



**Ensino a distância**  
**Aprendizado Contínuo**  
**Liberdade**  
**Colaborativismo**

- \* **Vídeo aulas**
- \* **Documentações**
- \* **Dicas**



[youtube.com/projetoroot](https://youtube.com/projetoroot)

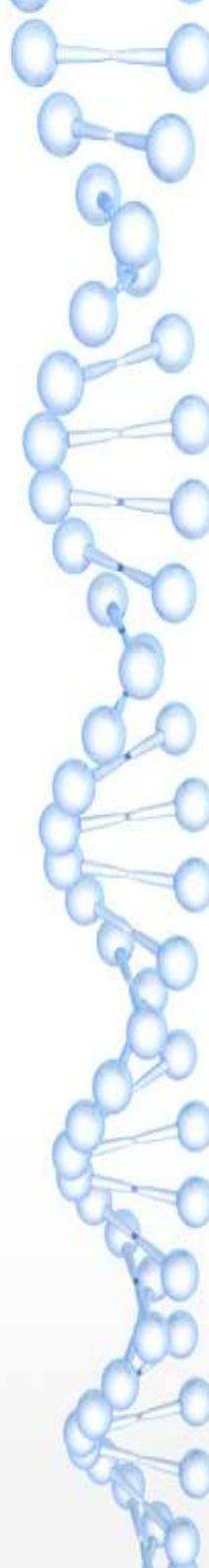
- [diegocosta@projetoroot.com.br](mailto:diegocosta@projetoroot.com.br)
- [www.projetoroot.com.br](http://www.projetoroot.com.br)
- [youtube.com/projetoroot](http://youtube.com/projetoroot)
- [facebook.com/projetoroot](http://facebook.com/projetoroot)
- [wiki.projetoroot.com.br](http://wiki.projetoroot.com.br)

•  
Diego Costa  
CEO – Projeto Root

- Especialista em Segurança da Informação – Faculdade de Tecnologia SENAC – Porto Alegre - RS
- Tecnólogo em Redes de Computadores – Faculdade de Tecnologia SENAC – Pelotas - RS
- Criador de conteúdos online na área de tecnologia e idealizador do canal no Youtube Projeto Root
- Analista de Segurança da Informação.







# (IN)Segurança na INternet

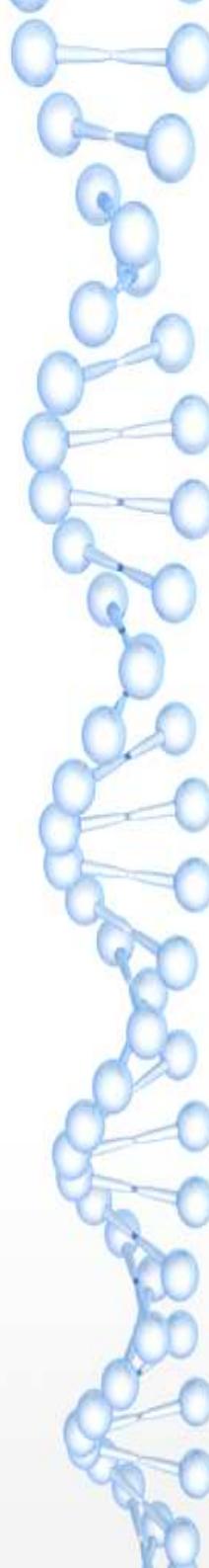


O que faço na internet ?

- Quem está lá ... ?
- Quais os riscos de uma navegação descuidada?
- A empresa que trabalho pode sofrer danos com o meu descuido?
- Posso mudar este cenário?

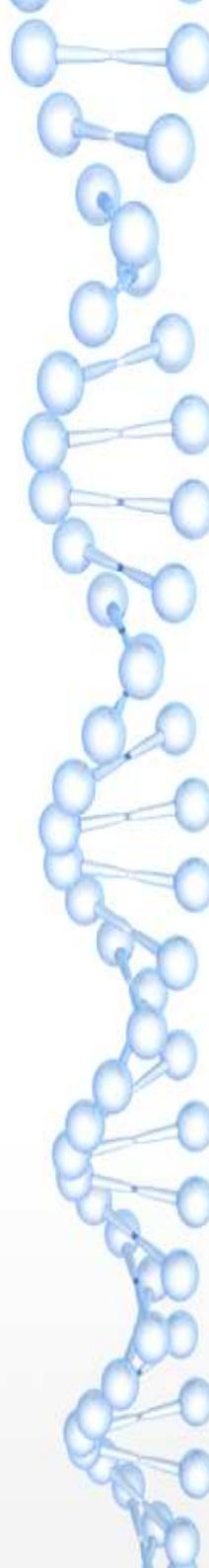
# Minha casa, sua casa?





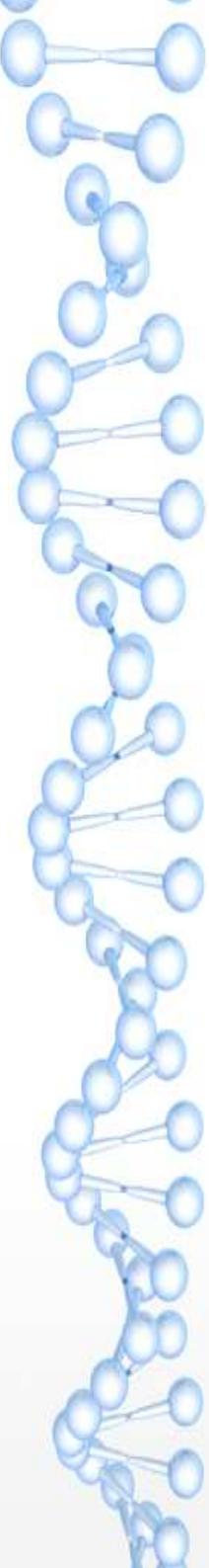
# Você sabe como a internet funciona?





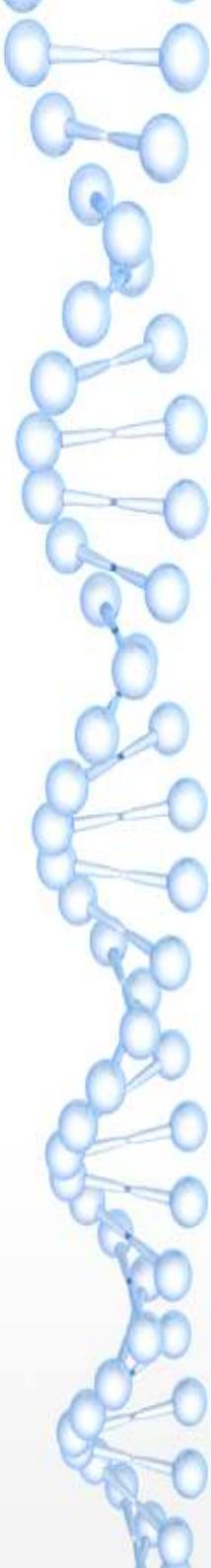
Será mesmo que ela é como você imagina?





# **Perigos na navegação**

- \* Invasão de computadores e dispositivos informáticos;
- \* Perdas e/ou vazamento de dados sensíveis ;
- \* Extorsão/Golpes;
- \* Fake News;
- \* Aproveitamento/Uso de informações privilegiadas;
- \* Prejuízos inestimáveis ao afetado.



# Mas isso todo mundo sabe, né?

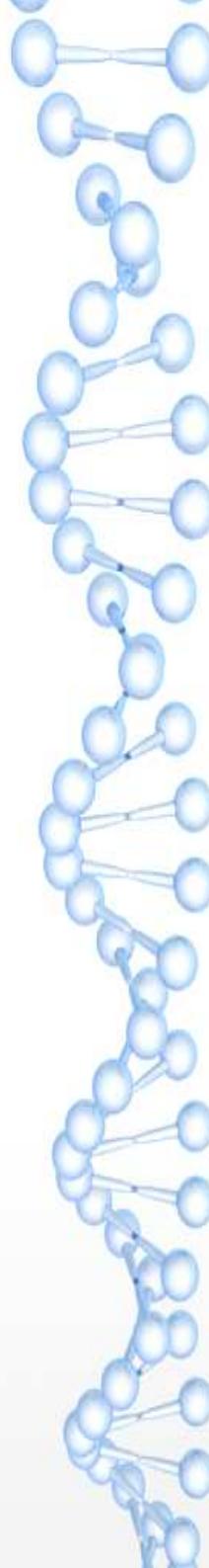
Vivemos em um mundo pós Edward Snowden

Sabemos ou deveríamos saber que **empresas** como:

- \* Facebook
- \* Google
- \* Microsoft
- \* Yahoo
- \* etc...

Fazem **bilhões** de dólares em lucro com:

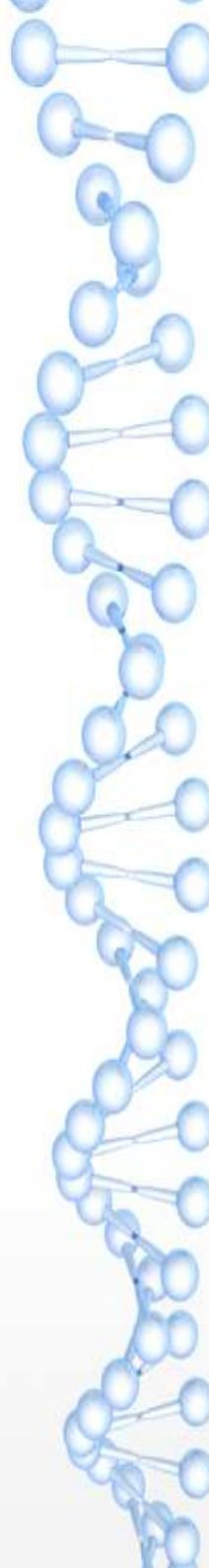
- \* Nossos perfis de navegação
- \* Nossas orientações (religiosas, políticas, sexual, ideológicas,etc..)
- \* Nossas compras (online e offline)
- \* Nossas localizações ( Check-IN, maps, marcações )
- \* etc...



# Mas como isso é possível?

Apenas com o maior bem (ativo) que você tem.





# Mas como? eu não ...

Será que não?



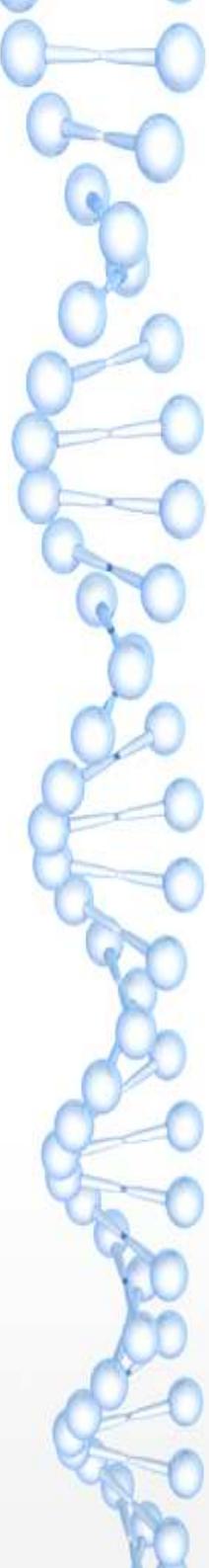
CURTIR



COMENTAR



COMPARTILHAR

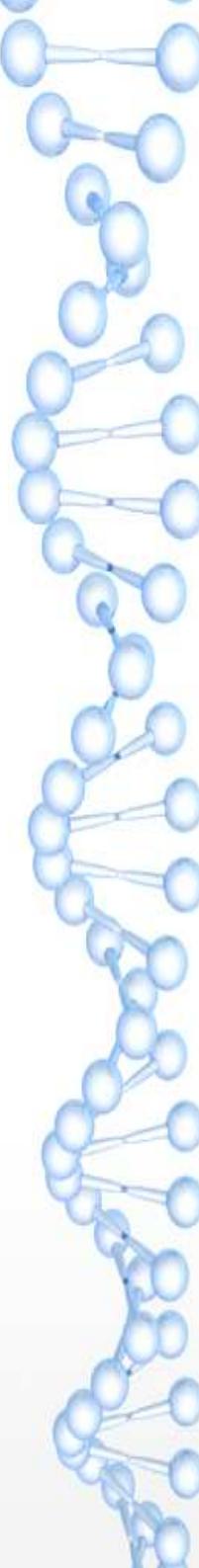


# Não, comigo não ...

Tem certeza?



# Mas quem é esse tal Snowden?



**MENU** | **G1** **MUNDO**

17/03/2016 17h34 - Atualizado em 17/03/2016 18h18

## Edward Snowden cita grampo de Dilma no Twitter

'Dilma ainda faz chamadas não criptografadas', diz ex-analista da NSA. Snowden cita caso de 2013 quando presidente foi alvo de escuta dos EUA.

Do G1, em São Paulo

O ex-consultor da Agência de Segurança Nacional (NSA) Edward Snowden postou nesta quinta-feira (17) no Twitter uma mensagem em que cita o grampo telefônico envolvendo o ex-presidente Luiz Inácio Lula da Silva e a presidente Dilma Rousseff.

"Going dark" é um conto de fadas: três anos após as manchetes de escuta de @dilmabr ela ainda está fazendo chamadas não criptografadas", diz a mensagem acompanhada de uma colagem de manchetes da imprensa americana de setembro de 2013 e desta quinta.

 **Edward Snowden**   
@Snowden



"Going dark" is a fairy tale: 3 years after @dilmabr wiretap headlines, she's still making unencrypted calls. [#opsec](#)

AP September 1, 2013, 11:43 PM

## Report: NSA spied on Brazilian, Mexican presidents

Tweeted by CNN Internatio... Mar 17, 2016

**BBC** | **Menu**

**NEWS | BRASIL**

Notícias | Brasil | Internacional | Economia | Saúde | Ciência | Tecnologia | Aprenda Inglês

## EUA espionaram Petrobras, dizem papéis vazados por Snowden

08 setembro 2013

f t g+ Compartilhar

**Novos documentos da Agência de Segurança Nacional dos Estados Unidos (NSA) vazados pelo ex-analista da agência Edward Snowden indicam que a Petrobras também teria sido espionada pelos americanos.**

A informação vem uma semana após notícias de que a presidente do Brasil, Dilma Rousseff, teria sido espionada pela agência.

Nome da Petrobrás aparece em treinamento sobre como invadir redes de dado privadas

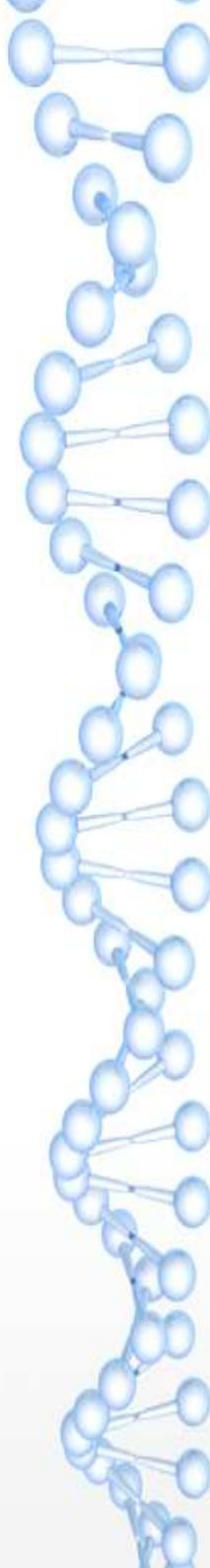


Reuters

O teor dos documentos sobre a Petrobras foi revelado em reportagem do programa *Fantástico*, da TV Globo.

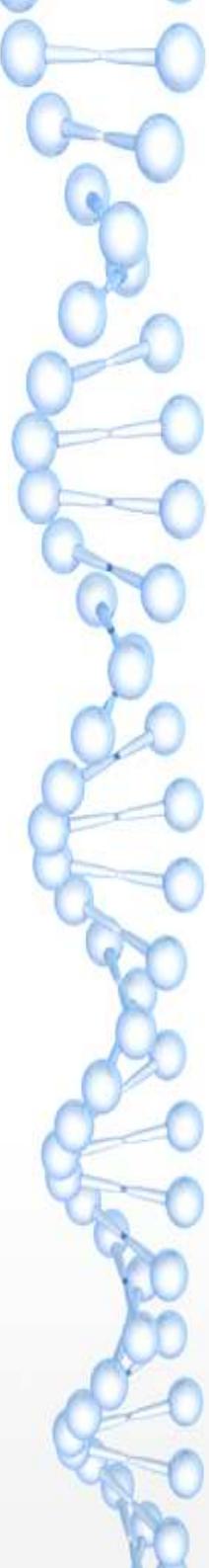
Segundo a reportagem, a tecnologia envolvendo a exploração em alta profundidade na camada pré-sal poderia ter sido o alvo da espionagem. Consultada, a Petrobras disse que não fará comentários.

O nome da Petrobras aparece em um documento usado em um treinamento de agentes da NSA, sempre segundo a reportagem.



# **SNOWDEN: TRAITOR OR PATRIOT?**





# Não iremos discutir se ele é ou não.

Mas que o mundo da Segurança da informação mudou com sua chegada, mudou...

- \* **Leis que preveem crimes neste segmento**

- Carolina Dieckmann - **Lei 12.737/2012**
- Marco Civil da Internet - **Lei N° 12.965/14**
- GDPR - Regulamento Geral de Proteção de Dados

- \* Cursos/Treinamentos/Eventos

- \* Entendimento das Normas da família ISO/IEC 27.000 (\*)

- \* Elaboração de Políticas de Segurança da Informação (PSI)

- \* Elaboração dos Planos de Continuidade do Negócio (PCN)

# Mas estamos no Brasil ...

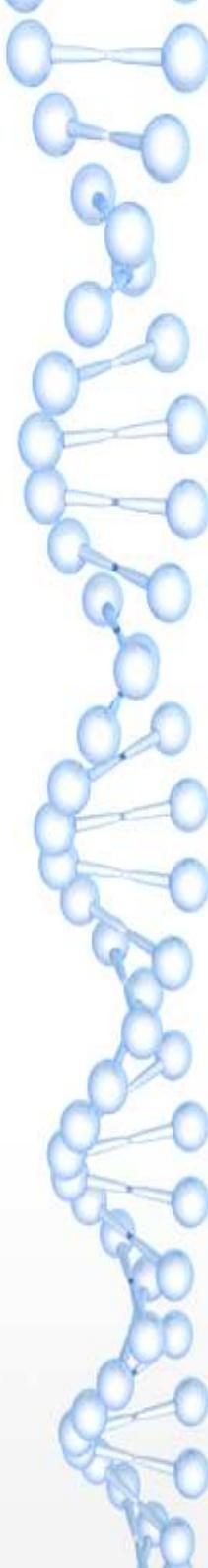
Não seremos afetados por isso...

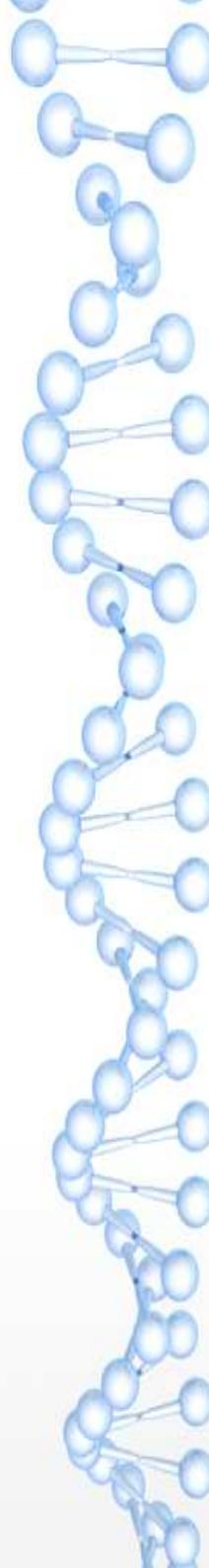


CenturyLink Global Network



© 2017 CenturyLink. All Rights Reserved. Map information above is current as of October 2017. Information is subject to change. Contact CenturyLink for updates or details. CenturyLink's global network is made up of owned, leased access and iRU segments, which are not distinguished on this map. CenturyLink engages in-region carriers to provide services in some markets.

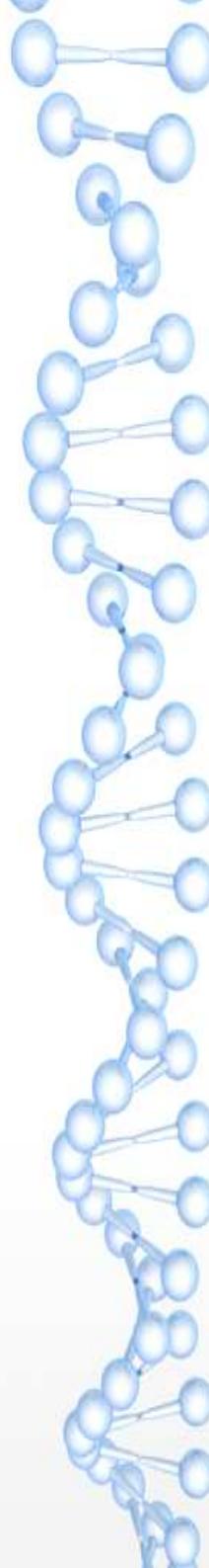




# Qual destes serviços estão operando no BR?

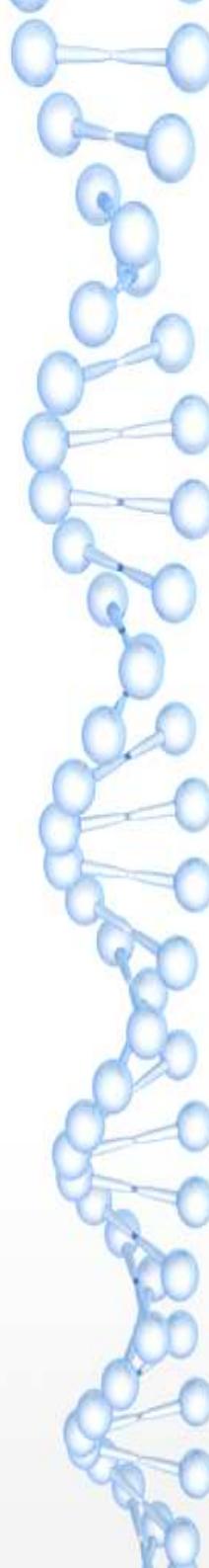
Quem aqui tem conta em uma destas redes?



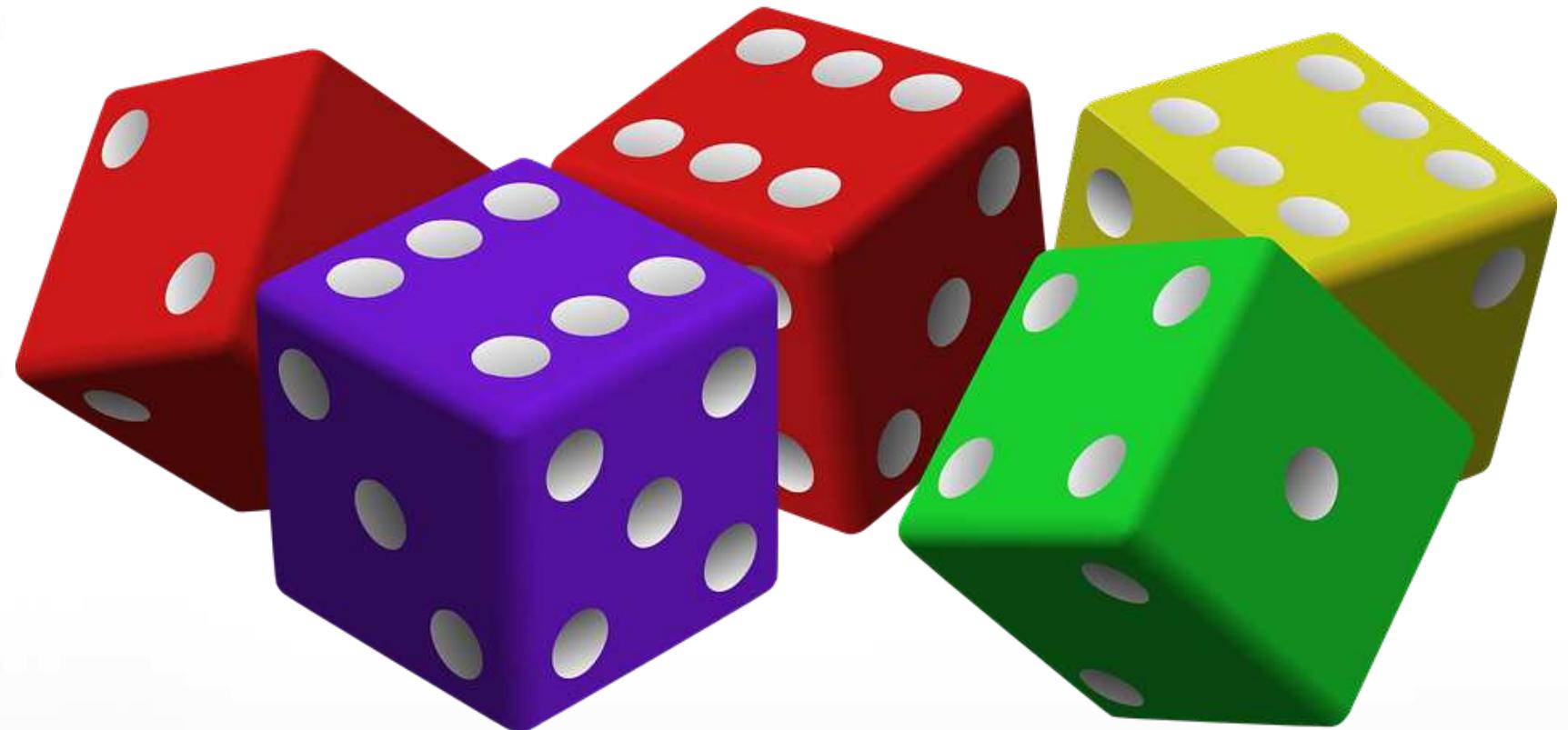


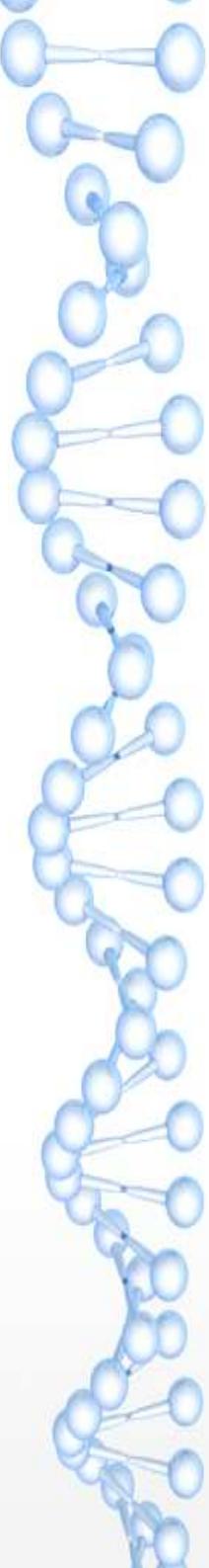
Alguns dos senhores tiveram que pagar \$\$ para ter acesso a rede?





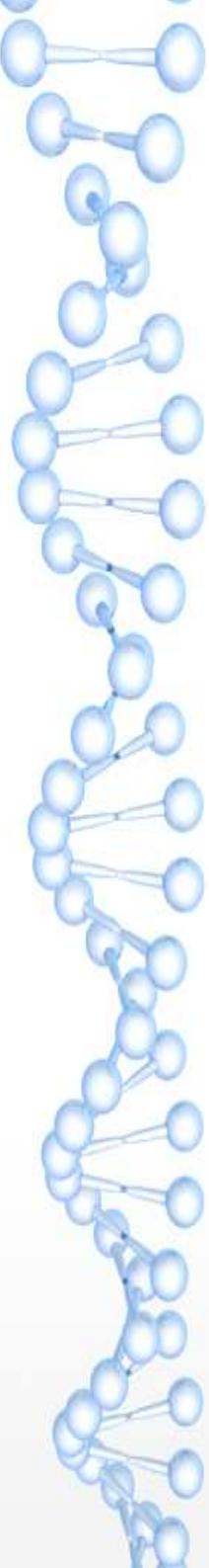
Vocês têm certeza?





# Tudo bem, mas como posso ter mais segurança na Internet?

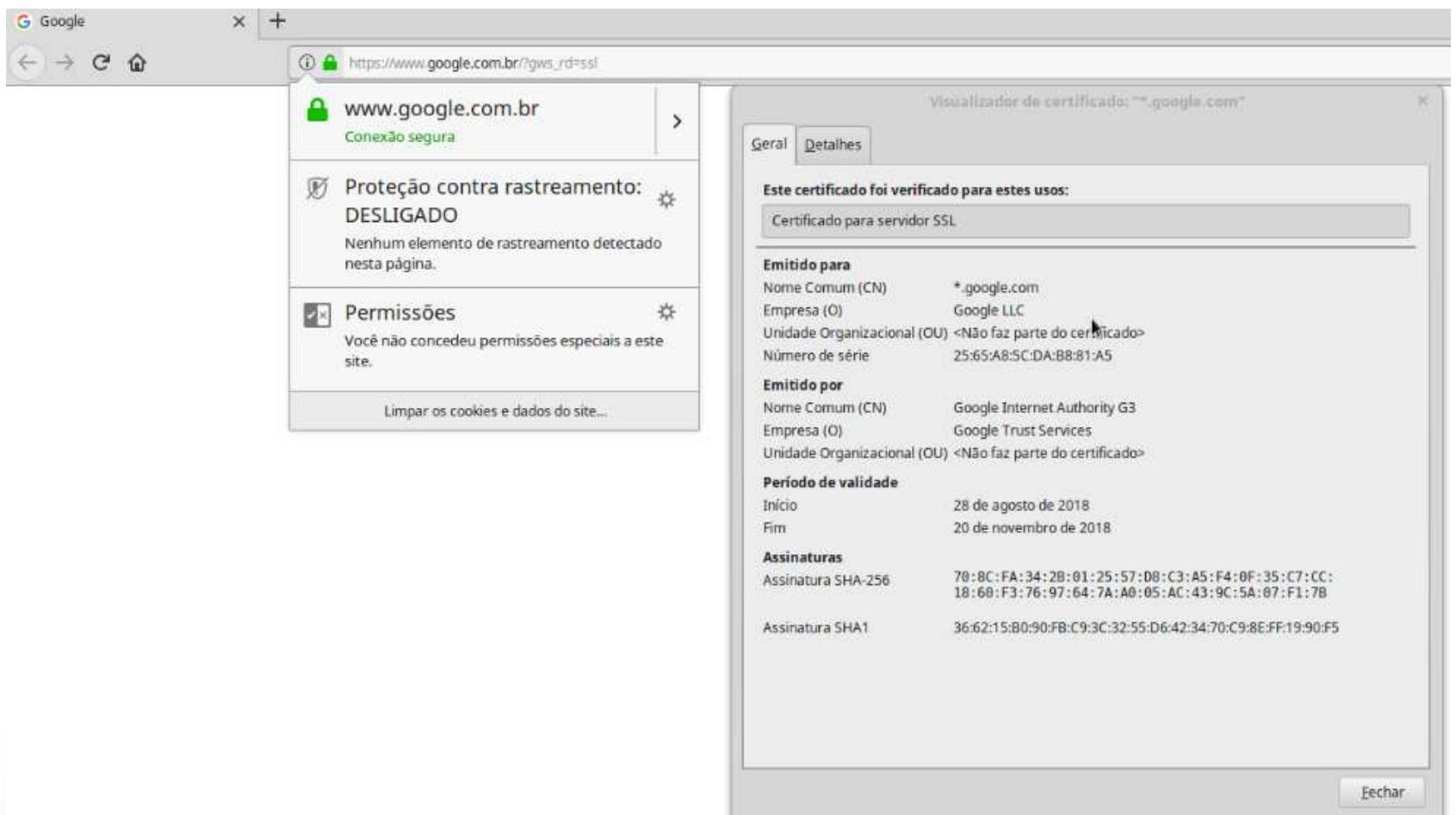
- \* Pesquise sobre a fonte antes de clicar no link ;
- \* Troque suas senhas com frequência e use duplo fator de autenticação;
- \* Senhas são pessoais e intransferíveis (segredo contado, deixa de ser segredo ... não é mesmo?)
- \* Senhas não são compartilháveis ...**  
nem com: amigos, familiares, esposas/os, filhos, gatos,cachorros, periquitos.... )
- \* Se existe uma norma/política SIGA, afinal se ela foi entregue/lida ou solicitada a você, logo tem um objetivo.



# Cadeado Verde = Seguro?



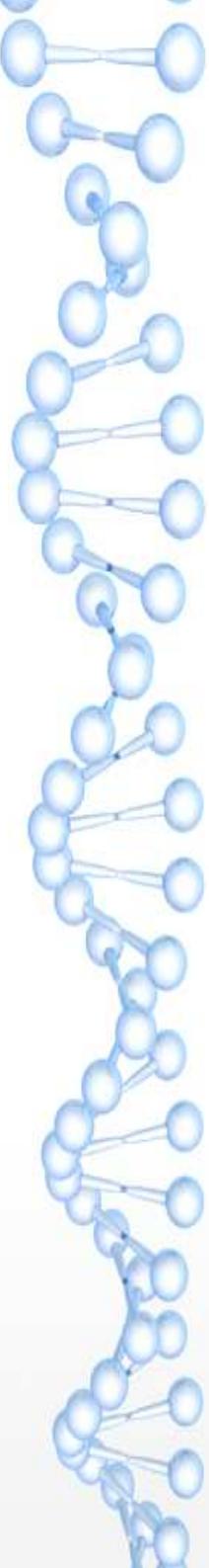
# Cadeado Verde = Seguro?



# Senhas são difíceis de decorar

prefiro 12345 ou senha como senha...





# Use duplo fator!

O que é isso?

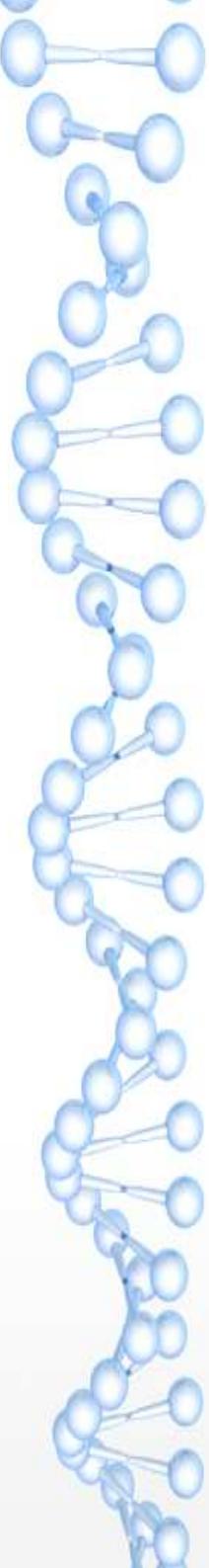


Na minha empresa tem um TXT

Salvo tudo lá e depois mando por...



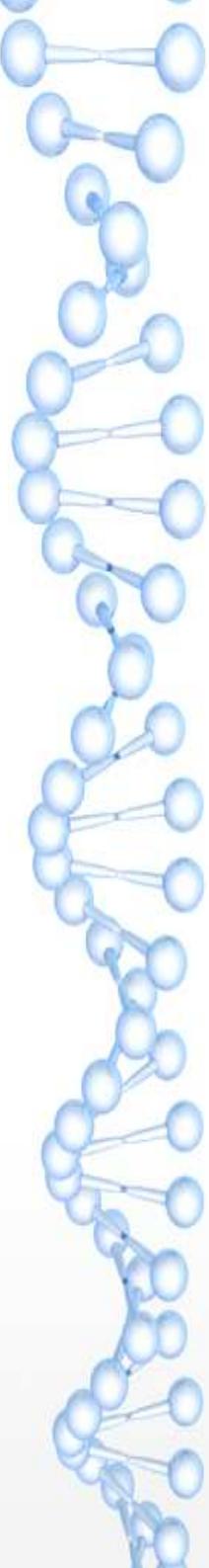
Senhas Colaborativas com TeamPass



# Use duplo fator!

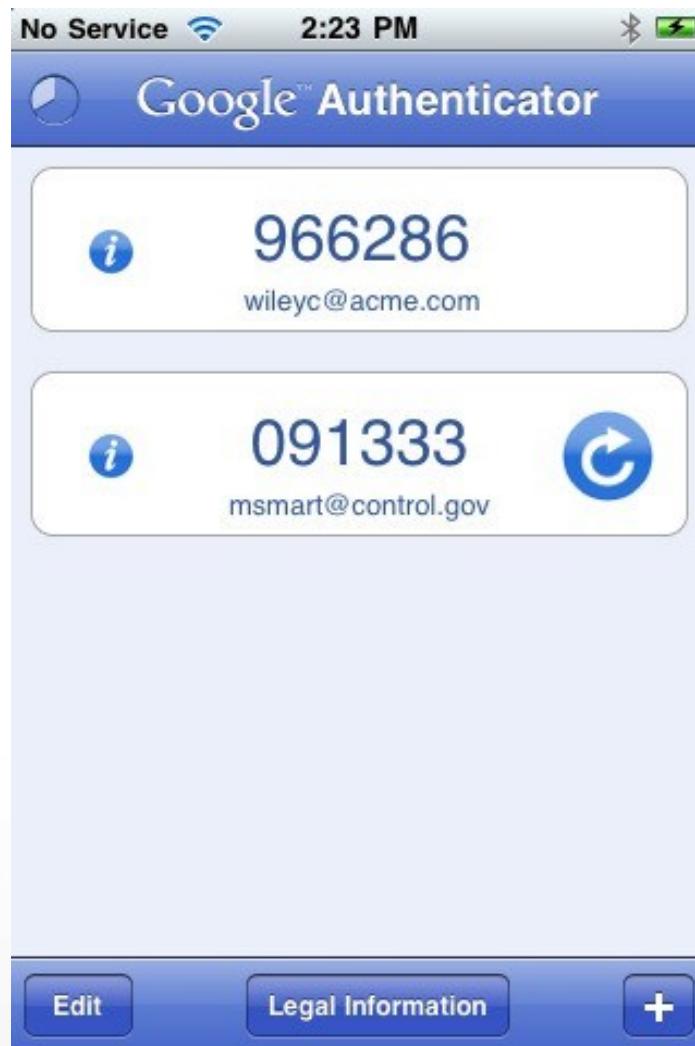
O que é isso?





# Softwares/App

## Google Auth

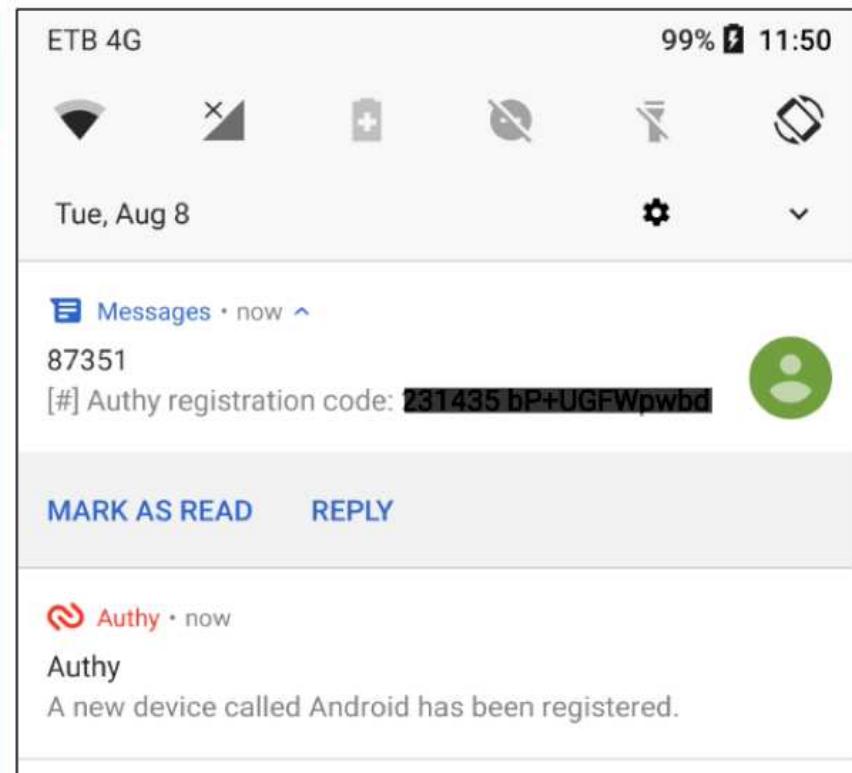
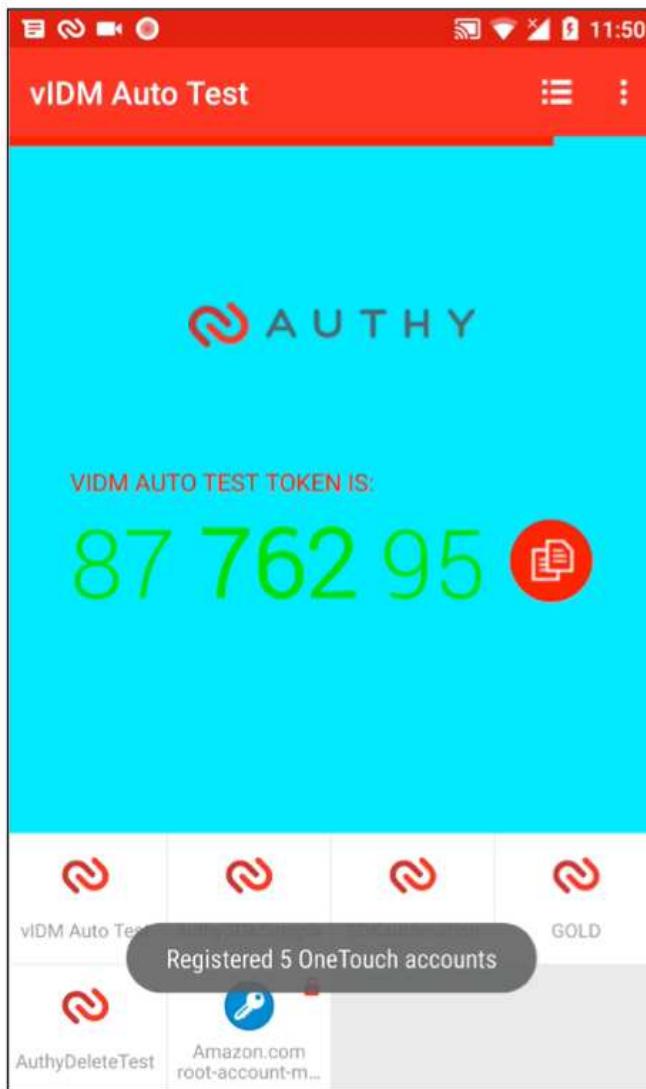


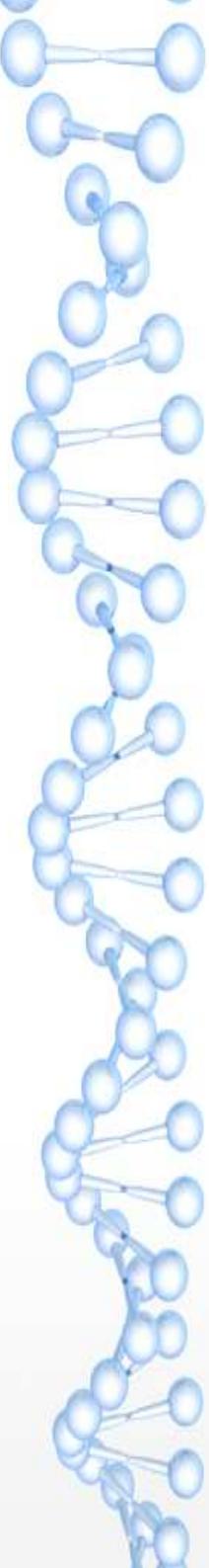
Número Randômico – Altera a cada X tempo

Usuário @ Serviço/Site/Sistema

# Softwares/App

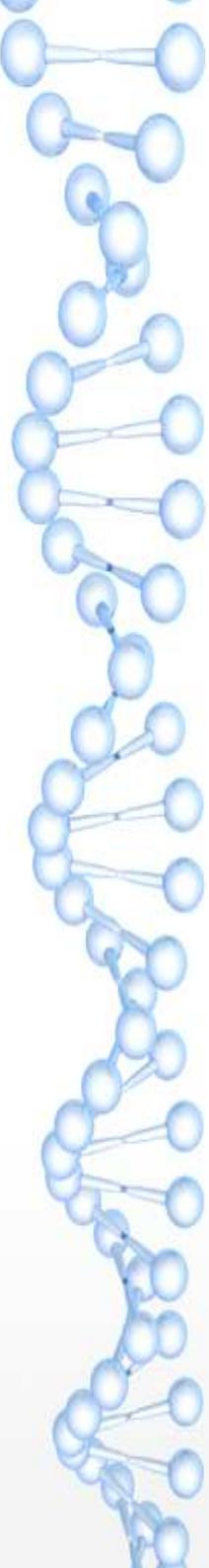
Authy





# Então tudo é resolvido com a senha?

- \* **Não;**
- \* Uma **senha segura** já é um indício de preocupação com a segurança da informação;
- \* O principal **vetor de ataque** Hacker/Cracker começa com conhecimento do alvo, entre as atividades destaca-se quais os serviços que o mesmo está cadastrado e se o mesmo possui senhas fracas.



# Tipos de ataques na internet

- \* **Vírus** (menos relevante atualmente) ;
- \* **Golpes** (Cartões de créditos, dados, etc..);
- \* **Fishing** (páginas ou e-mails simulando sites oficiais);
- \* **Malware** (Código criado para diversos fins, o mais comum é fazer de seu dispositivo um zumbi );
- \* **Ransomware** ( Sequestro de dados, sistemas, etc.. );
- \* **Whatsapp** (wishing);
- \* **Vulnerabilidades** em sistemas e/ou hardwares.

# Alguns ataques na internet

G1

ECONOMIA

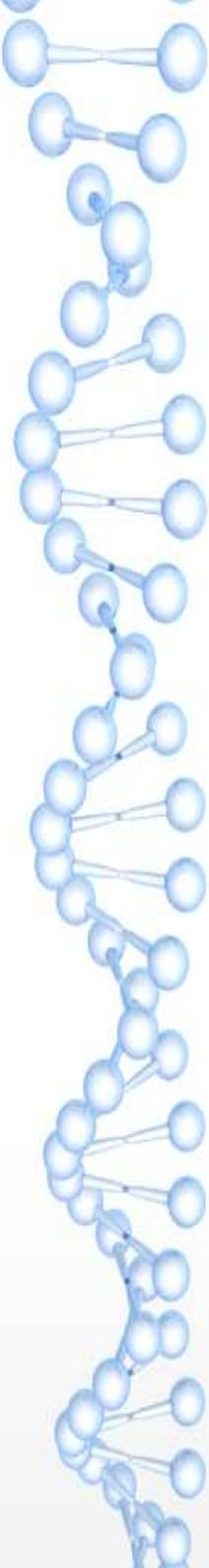
BLOG DO ALTIERES ROHR

## Como os golpistas ganham dinheiro com as fraudes no WhatsApp?

09/06/2018 08h00 · Atualizado há 4 meses



Criminosos se aproveitam de acordos de publicidade para faturar com golpes no WhatsApp — Foto: Altieres Rohr/Especial para o G1



# Alguns ataques na internet

Home > Segurança > Hacker

## Mais de 185 mil roteadores da TP-Link estão sujeitos a vulnerabilidade

Por Eduardo Hayashi | 04 de Maio de 2018 às 12h00

### TUDO SOBRE



TP-Link

**ATUALIZAÇÃO (04/05):** A TP-Link entrou em contato com a redação do Canaltech e informou que sua equipe de engenheiros e pesquisadores já está desenvolvendo uma correção para a vulnerabilidade presente no roteador TL-WR740N. Ainda de acordo com a empresa, a atualização de firmware deve ser disponibilizada ainda neste mês de maio. Enquanto o update não chega, a companhia solicita que os clientes façam a alteração do usuário e senha padrão do equipamento para impedir o acesso de pessoas não autorizadas.

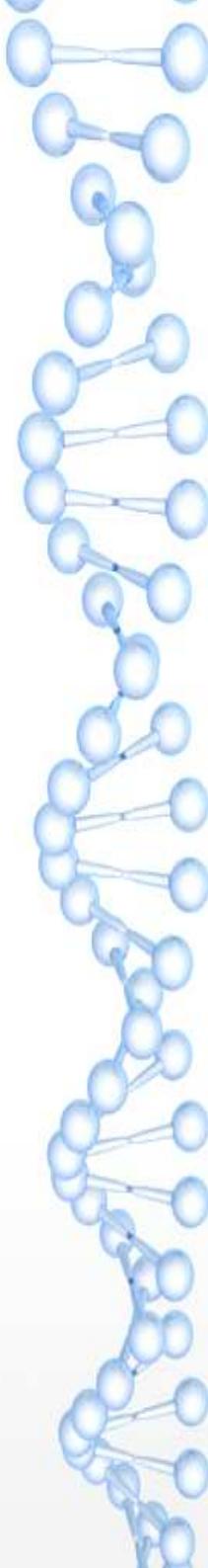
### Nota original

Uma vulnerabilidade crítica de segurança foi identificada em roteadores TP-Link, afetando mais de 185 mil aparelhos da empresa.

Participe do nosso [GRUPO CANALTECH DE DESCONTOS](#) do [Whatsapp](#) e do [Facebook](#) e garanta sempre o menor preço em suas compras de produtos de tecnologia.

De acordo com a publicação do pesquisador de segurança digital Tim Carrington, os roteadores da série TL-WR740N possuem uma brecha que viabiliza a execução remota de códigos, sendo esta uma óbvia porta de entrada para possíveis invasões.

Durante a análise do código-fonte do TL-WR740N, o especialista descobriu que a falha é muito semelhante à que foi encontrada no modelo TL-WR940N, uma vez que ambos os equipamentos de rede compartilham de códigos semelhantes.



# Alguns ataques na internet

techtudo

DOWNLOADS

## TP-Link libera lista de roteador afetados por falha no Wi-Fi com WPA2

Fabricante prepara atualizações de firmware para os produtos e faz recomendações de segurança.

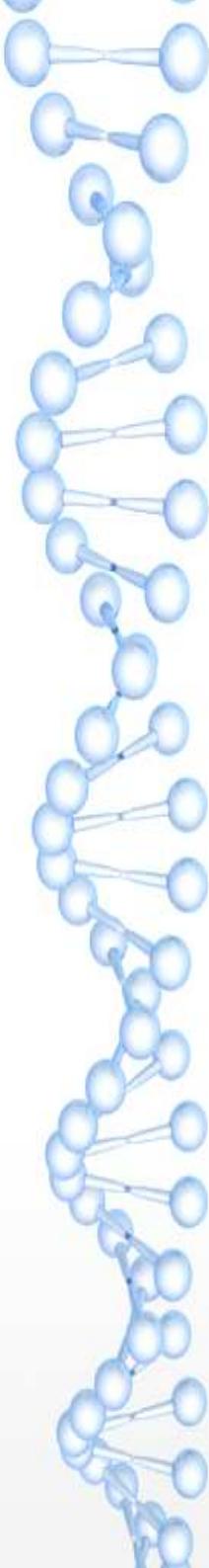
Por Filipe Garrett, para o TechTudo

19/10/2017 14h19 · Atualizado há 11 meses



A **TP-Link** emitiu uma nota oficial reconhecendo que parte de seus produtos é afetada pela vulnerabilidade KRACKs, que permite a invasores a **capacidade de interceptar informações em redes Wi-Fi**. Além disso, a marca identificou os modelos de roteadores e outros equipamentos de rede sem fio que podem ser alvo bem-sucedidos de ataques em WPA2, salientando que todos esses aparelhos receberão atualizações de firmware para eliminação do problema dentro das próximas semanas.





# Alguns ataques na internet

techtudo

INFORMÁTICA

## Criminosos usaram falha em roteadores D-Link para roubar dados bancários

Falha ocorreu entre 8 de junho e 10 de agosto; a recomendação é atualizar o firmware e trocar a senha

Por Igor Nishikiori, para o TechTudo

14/08/2018 14h51 · Atualizado há 1 mês



Cibercriminosos exploraram uma falha nos roteadores da marca **D-Link** para possivelmente roubar dados de clientes de bancos brasileiros, afirmou a empresa de segurança digital Radware. Segundo a empresa de proteção na web **ESET**, a vulnerabilidade permitiu aos golpistas manipularem o servidor DNS dos dispositivos conectados aos roteadores, redirecionando o usuário a páginas falsas do **Banco do Brasil** e do **Itaú**, prática conhecida como **hijacking** (sequestro, em inglês).

Anúncio fechado por Google

# Alguns ataques na internet

tecnoblog

TECNOCAST REVIEWS CUPONS CURSOS ASSISTENTE DE COMPRAS ANUNCIE



## 280 mil roteadores foram invadidos para minerar criptomoeda, a maioria no Brasil

Roteadores da MikroTik foram infectados com minerador de criptomoeda; falha foi corrigida em abril mas ainda é usada



Por Felipe Ventura  
11/09/2018 às 17h24

NEWS

Já conhece a nova extensão do Tecnoblog?

Baixe Agora

Mais de 280 mil roteadores da MikroTik estão infectados com um minerador de **criptomoeda**. A mesma falha de segurança está sendo usada em diferentes ataques, que atingem principalmente o Brasil. Ela já foi corrigida em abril, mas muita gente não instalou a atualização.

- Roteadores da MikroTik estão desviando tráfego; Brasil é um dos mais afetados

O pesquisador Troy Mursch catalogou [64 versões diferentes](#) dessa invasão, que usa o navegador web para minerar criptomoeda. A mais recente delas afeta quase 6.500 dispositivos, 4.500 deles no Brasil.



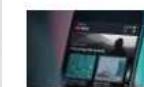
DOMAIN.COM

**SAVE 25%**  
on domains, websites,  
email, & more

Use Code: **GETSTARTED**

**GET STARTED**

### Em Destaque



YouTube Music Premium e YouTube Premium removem...



iPhone XS, XS Max, XR, Watch Series 4: o resumo dos...



Novo padrão de placas de carro começa a ser usado no...



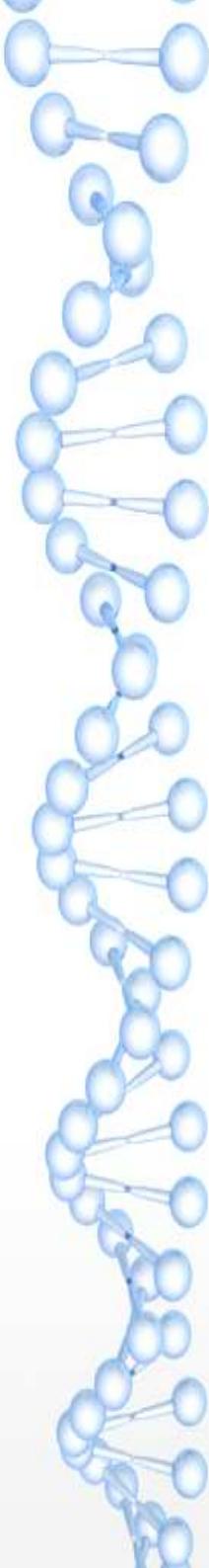
TV Sony X905F: escolha pela Imagem



Dez anos de Google Chrome: como o navegador dominou o...



O que é a falha Foreshadow que afeta processadores...



# Alguns ataques na internet

≡ MENU



TECNOLOGIA E GAMES

29/01/2013 14h25 - Atualizado em 05/02/2013 19h26

## Brecha vaza na web imagens gravadas por sistemas de segurança

Problema pode afetar 18 fabricantes de gravadores digitais (DVRs). Segundo especialista, 58 mil sistemas estariam expostos.

Altieres Rohr  
Especial para o G1

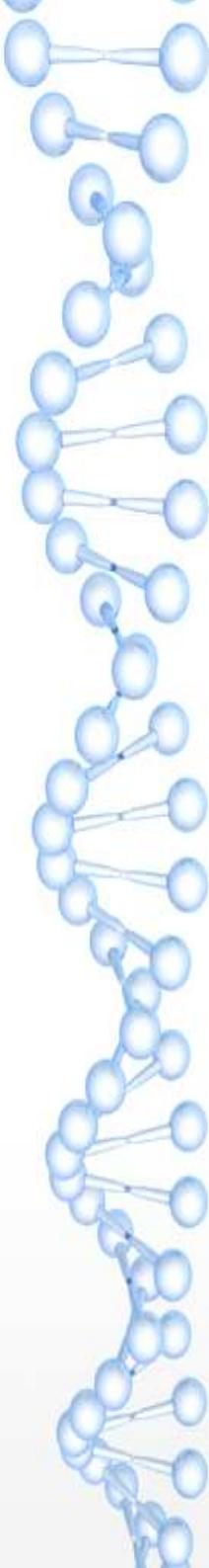


Sistemas de gravação digital, usados para a segurança de estabelecimentos, por exemplo, podem ser hackeados (Foto: Divulgação)

Um pesquisador de segurança que usa o apelido de "someLuser" descobriu uma vulnerabilidade em sistemas de gravação digital (DVR, na sigla em inglês) comumente usados em conjunto com câmeras de segurança em circuitos fechados de televisão (CFTV). A falha permite descobrir a senha do aparelho, o que dá acesso total às imagens gravadas, permitindo inclusive alterá-las ou removê-las da memória do dispositivo.

A vulnerabilidade está presente em um software fornecido por uma empresa chinesa chamada Ray Sharp. Segundo o especialista em segurança H. D. Moore, 18 fabricantes diferentes fazem uso do sistema chinês.

Os fabricantes, porém, ainda não confirmaram a falha.



# Alguns ataques na internet

## Smart-TVs em alto risco de invasão

11/01/2016 Autor: David B.Svaiter - Sócio-Diretor da área de S.I. & Criptografia da Big Blue

As Smart-TV's rodando o sistema operacional Android fornecem funcionalidades adicionais aos usuários, além de TVs normais, mas também criam um risco de segurança, conforme a Trend Micro revela.

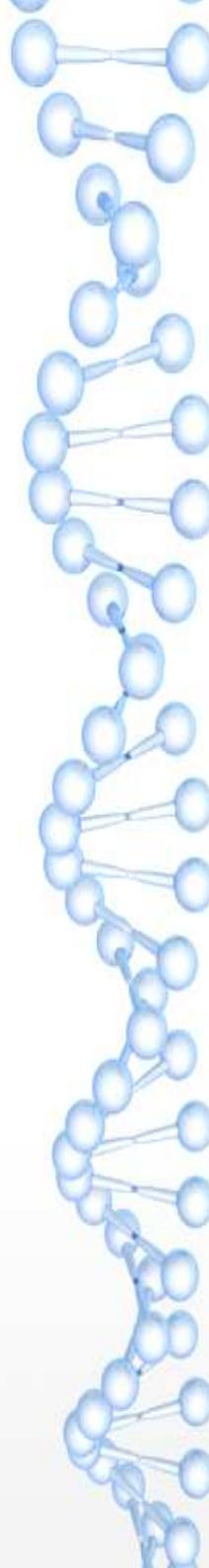
A Internet das Coisas (IoT) está em rápido crescimento e as TVs Inteligentes representam uma peça central neste crescimento, até porque elas são mais do que dispositivos de visualização passiva, já que podem executar aplicativos Android.

Um post no blog de autoria de Ju Zhu (da TrendMicro) explica que alguns dos aplicativos mais populares no Smart TVs permitem aos usuários assistir a canais de outras partes do mundo, mas também quebrar a segurança. De acordo com o pesquisador de segurança, alguns desses aplicativos contêm uma *backdoor* que abusa de uma falha em versões mais antigas do Android. A vulnerabilidade ([CVE-2014-7911](#)) é encontrado no Android anterior da versão Lollipop 5.0 (variando de 1.5 a Cupcake KitKat 4.4.2) e permite a um invasor executar código arbitrário em dispositivos comprometidos.



O problema é que muitas das *Smart TV's* de hoje executam versões mais antigas do Android, o que significa que elas são afetadas pela falha de segurança. A Trend Micro descobriu TVs vulneráveis de marcas como Changhong, Konka, Mi, Philips, Panasonic e Sharp, mas diz que outros dispositivos que executam versões mais antigas do Android também estão em risco, mesmo se esses aplicativos são usados principalmente em TVs.





# Alguns ataques na internet

## TV BOX PIRATAS ATACADOS POR VIRUS PARA MINERAR CRIPTOMOEDAS

Por Richard Lima - fevereiro 28, 2018

2750

f Compartilhar no Facebook

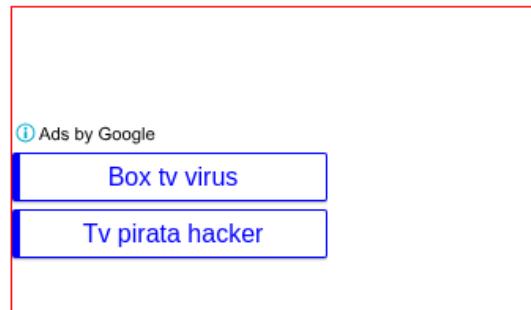
t Tweet

g+ G+

p

c Curtir 25

t Tweet



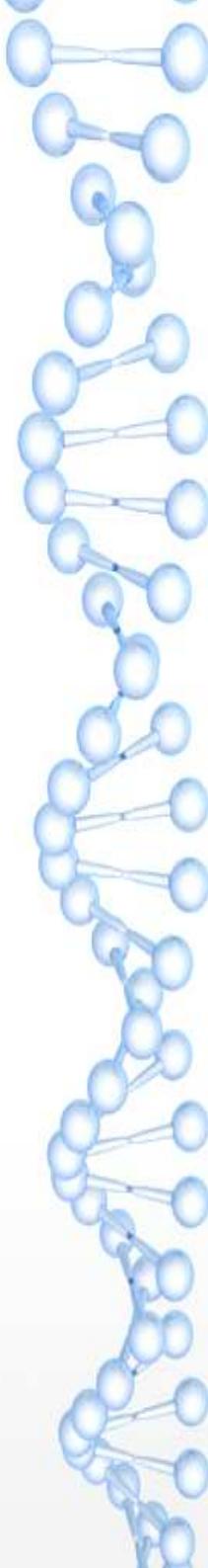
Hoje a internet estava cheia de matérias sobre Smart TVs atacadas por vírus para minerar criptomoedas para hackers, fui dar um conferida nas matérias e vi que a vulnerabilidade estava nas Smart TVs com firmware feito com o sistema operacional Android TV, aí pensei, opa, peraí, sistema operacional Android... Android TV... Android TV Box... TV Box para tv pirata, será??? Vou verificar.

Pois é... é.

O negócio tá mesmo complexo quando se fala em conectar qualquer aparelho à internet por que a galera que entende de invadir sistemas pouco seguros para instalar programas que escravizam estes aparelhos para trabalhar para eles está cada dia mais esperta e mais ousada.

As Smart TVs tem um sistema teoricamente um pouco mais seguro pois recebem versões certificadas do Android TV onde são feitas poucas modificações para implementar o layout e aplicativos da marca que vai usar o Android TV em suas televisões, agora quando se trata dos TV Box que usam versões do Android sem certificação... Aí o negócio complica.

Quando se fala nessa nova onda de virus para minerar criptomoedas nenhum dispositivo conectado à internet está à salvo, mas o caso das TV Box merecem especial atenção.



# Alguns ataques na internet

## Vulnerabilidade no Uconnect permite hackers controlarem carros da Fiat, Jeep e Chrysler

21/07/2015 13:43 | João Gabriel | @joao\_gan | Reportar erro

◀ POST ANTERIOR

Alcatel Onetouch lança o IDOL 3 no Brasil

Trilha sonora de The Last of Us será lançada amanhã em dis



0

Like

Share

Tweetar

G+

Dois hackers anunciaram que vão divulgar nas próximas semanas uma vulnerabilidade que encontraram no sistema conectado da Fiat Chrysler, o Uconnect, que aparece em veículos levando a marca Jeep, Dodge e Ram também. São aproximadamente 471.000 carros afetados que podem ser remotamente controlados pelos invasores, inclusive em partes críticas, como os freios, o volante e a transmissão.

# Alguns ataques na internet

G1

DISTRITO FEDERAL

## Netshoes ligará para 2 milhões de clientes afetados por vazamento de dados

Ligações serão feitas a partir de 8 de março. Medida foi adotada após reunião da empresa com Ministério Público do DF.

Por G1 DF e TV Globo

28/02/2018 05h25 · Atualizado há 7 meses



Hackers conseguiram dados de quase 2 milhões de contas no site — Foto: Reprodução/Fantástico

O site de comércio eletrônico Netshoes informou, por meio de nota, que os quase 2 milhões de consumidores de todo o país atingidos pelo **vazamento de dados** serão contatados por telefone a partir de 8 de março. Depois dessa data, a empresa terá mais 30 dias úteis para finalizar as ligações.

# Alguns ataques na internet

veja

Palavras cruzadas Eleições 2018 Pesquisas Eleitorais Dólar PIS/Pa

Economia

## Boa Vista SCPC apura possível vazamento de dados de milhões de brasileiros

A empresa reúne informações como CPF, e-mail, endereço e histórico financeiro dos brasileiros

Por Redação

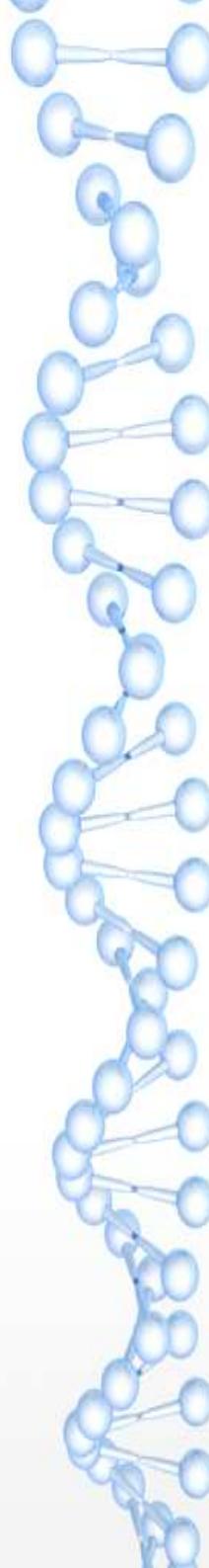
3 set 2018, 23h25 - Publicado em 3 set 2018, 19h42



Grupo hacker questiona o direito da Boa Vista SCPC de ter os dados pessoais de brasileiros "mesmo que eles não possuam dívidas" (//iStock)

A Boa Vista SCPC, empresa de análise de crédito, investiga uma possível invasão

# Alguns ataques na internet



**tecnoblog** TECNOCAST REVIEWS CUPONS CURSOS ASSISTENTE DE COMPRAS ANUNCIE

Still looking for a domain name?  
**SAVE 25%** Use Code: SEARCH GET STARTED

Início » Segurança » Facebook obriga 90 milhões de usuários a fazer login de novo após invasão

## Facebook obriga 90 milhões de usuários a fazer login de novo após invasão

Facebook diz que foi hackeado através do recurso "Ver como", agora desativado, e não confirma vazamento de dados

Por Felipe Ventura  
28/09/2018 às 14h01

NEWS

Já conhece a nova extensão do Tecnoblog? [Baixe Agora](#)

O Facebook sofreu um ataque em sua rede de computadores que afetou 50 milhões de pessoas. A rede social deslogou 90 milhões de usuários, forçando-os a fazer login de novo, mas ainda não sabe se houve vazamento de dados. Os hackers usaram uma falha que permitia assumir controle do perfil dos outros.

- [Como recuperar a senha do Facebook](#)
- [Como recuperar uma conta do Facebook sem o e-mail de cadastro](#)



### Em Destaque



Dez anos de Android: como surgiu o sistema móvel mais...

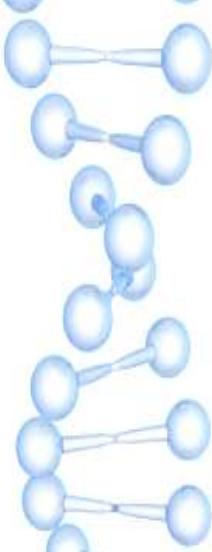


YouTube Music Premium e YouTube Premium removem...



iPhone XS, XS Max, XR, Watch Series 4: o resumo dos...

44



# Alguns ataques na internet

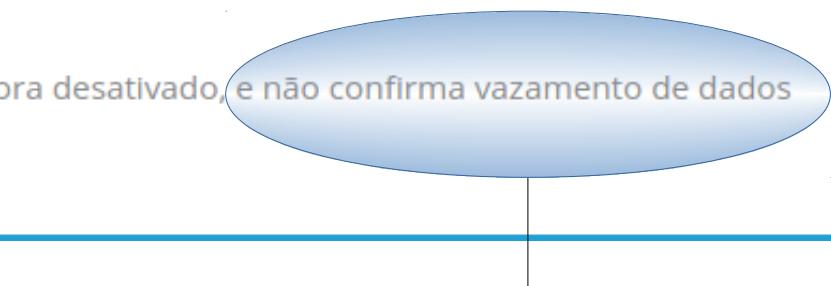
## **Facebook obriga 90 milhões de usuários a fazer login de novo após invasão**

Facebook diz que foi hackeado através do recurso "Ver como", agora desativado, e não confirma vazamento de dados



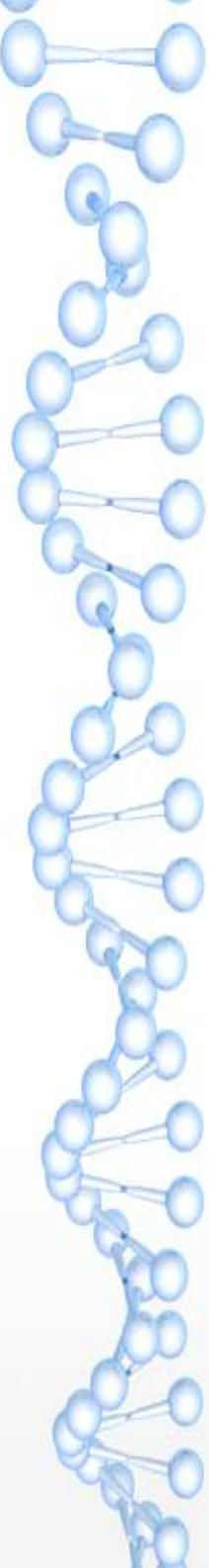
Por [Felipe Ventura](#)  
28/09/2018 às 14h01

NEWS



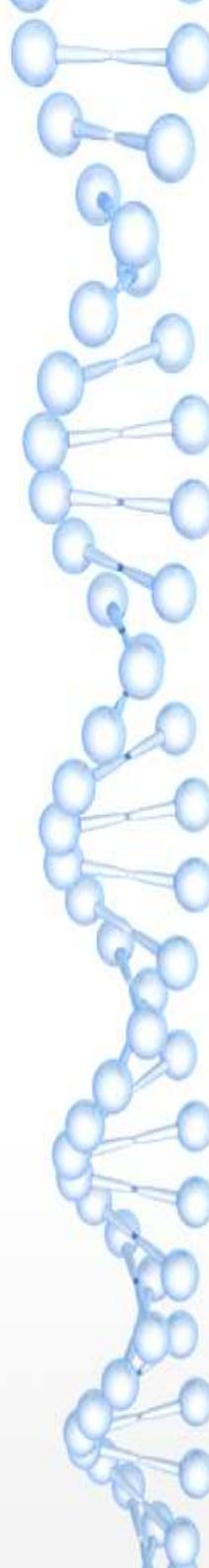
Será?





# Alguns dos métodos

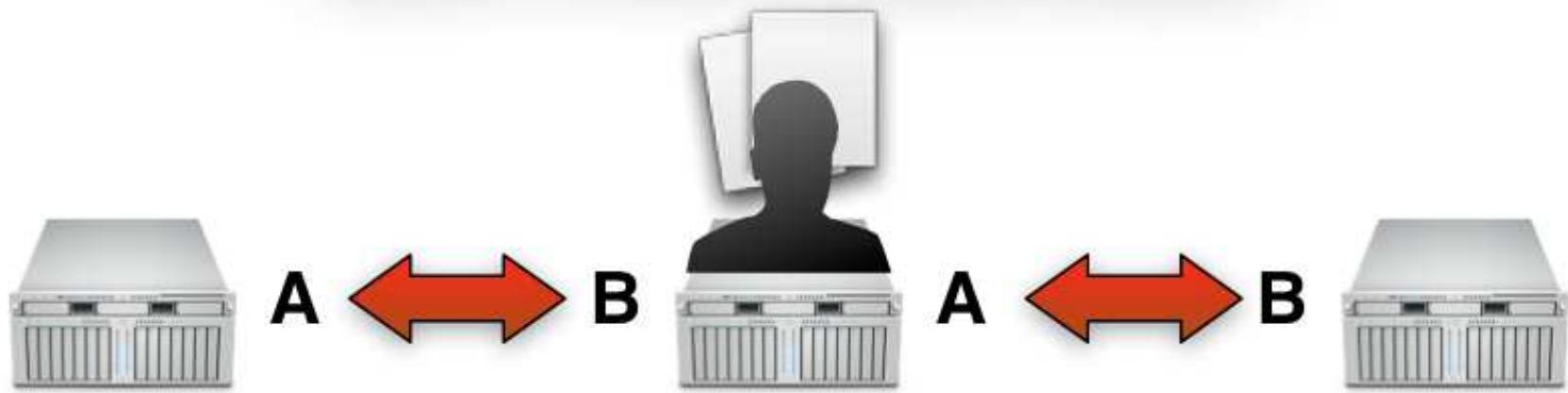
- \* SQL Injection
- \* **Senhas fracas**
- \* Keyloggers
- \* Vulnerabilidades novas (Zero Day)
- \* **MiTM (Man in The Middle)**
- \* ARP Spoofing/Poison
- \* **Engenharia Social**



# Alguns dos métodos

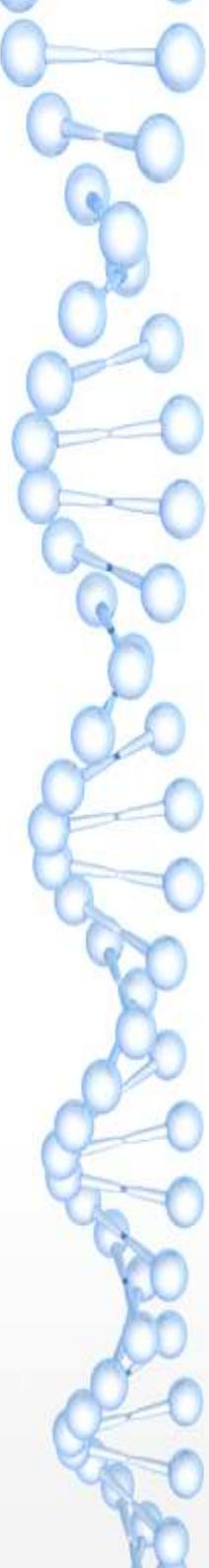


Man-in-the-middle attack



# Algumas soluções para correção de vulnerabilidades nos roteadores



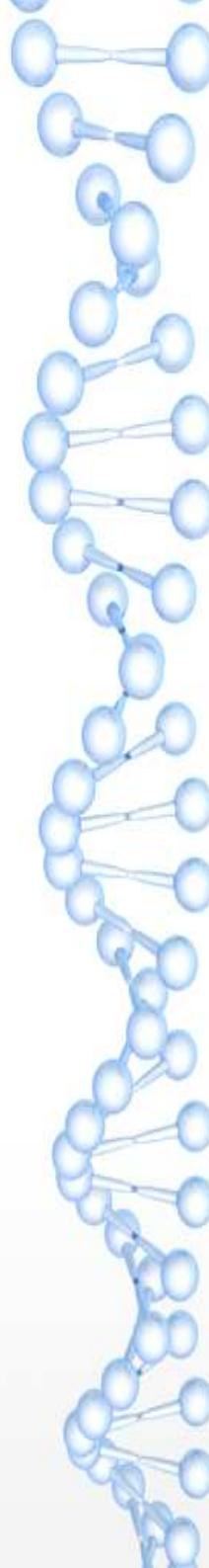


# Cultura de Seg Info

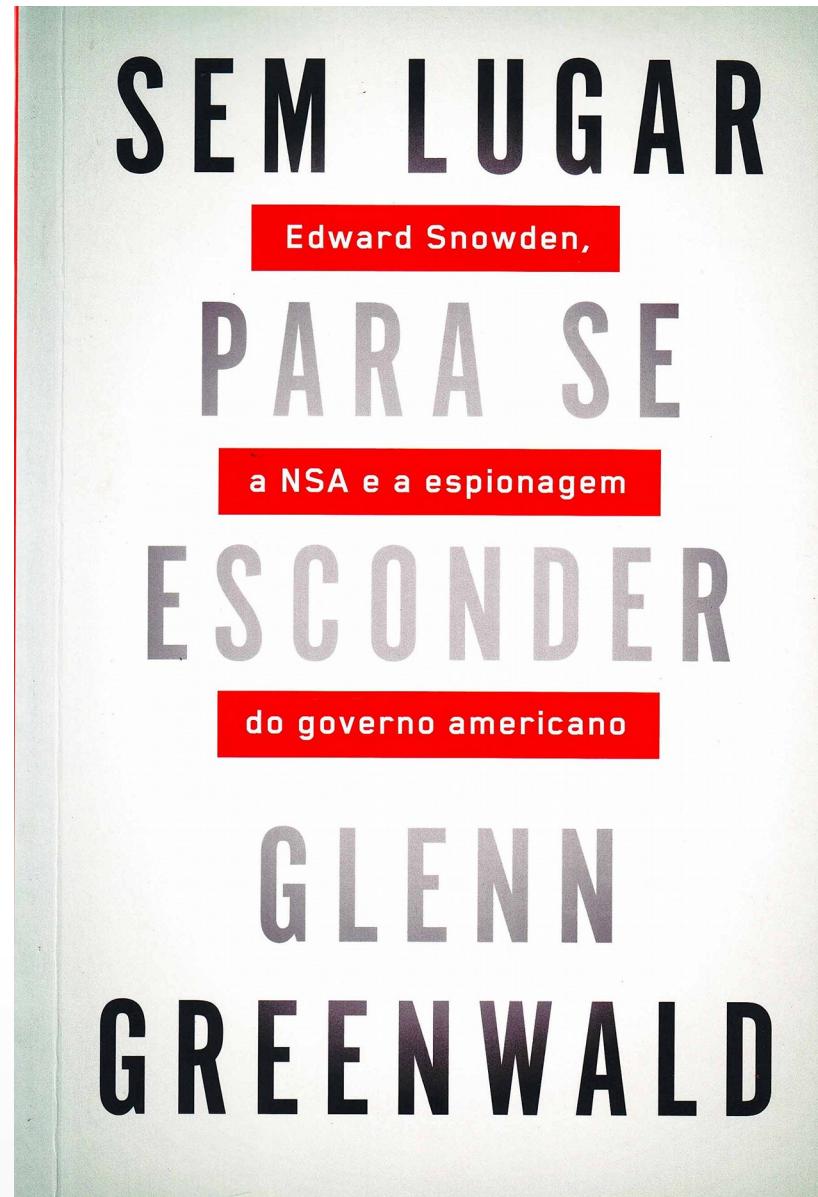
- \* Senhas **seguras**;
- \* **Seguir** Políticas de Segurança;
- \* Sempre estar **atento** as notícias;
- \* Manter uma **documentação** (não TXT) de senhas/acessos;
- \* **Participar/promover** eventos de Segurança da Informação;
- \* Ter a TI como aliada e qualquer dúvida **solicitar** ajuda;
- \* Ser um usuário de tecnologia **proativo** no que diz respeito as ameaças;
- \* Sempre manter todo e qualquer **sistema atualizado** (não só antivírus) .

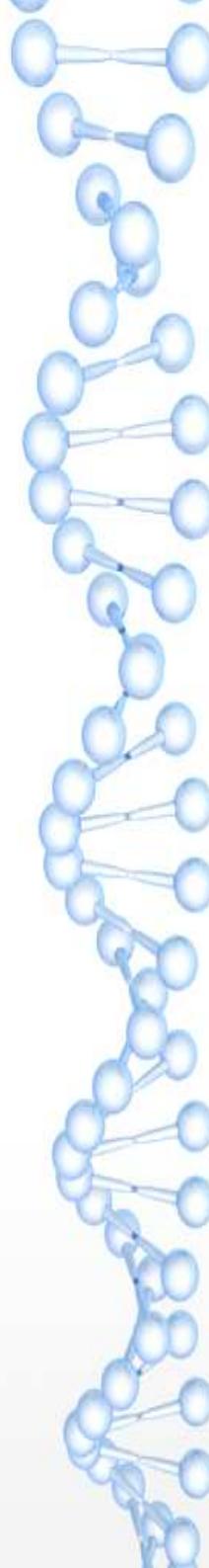
# INTERNET DAS COISAS



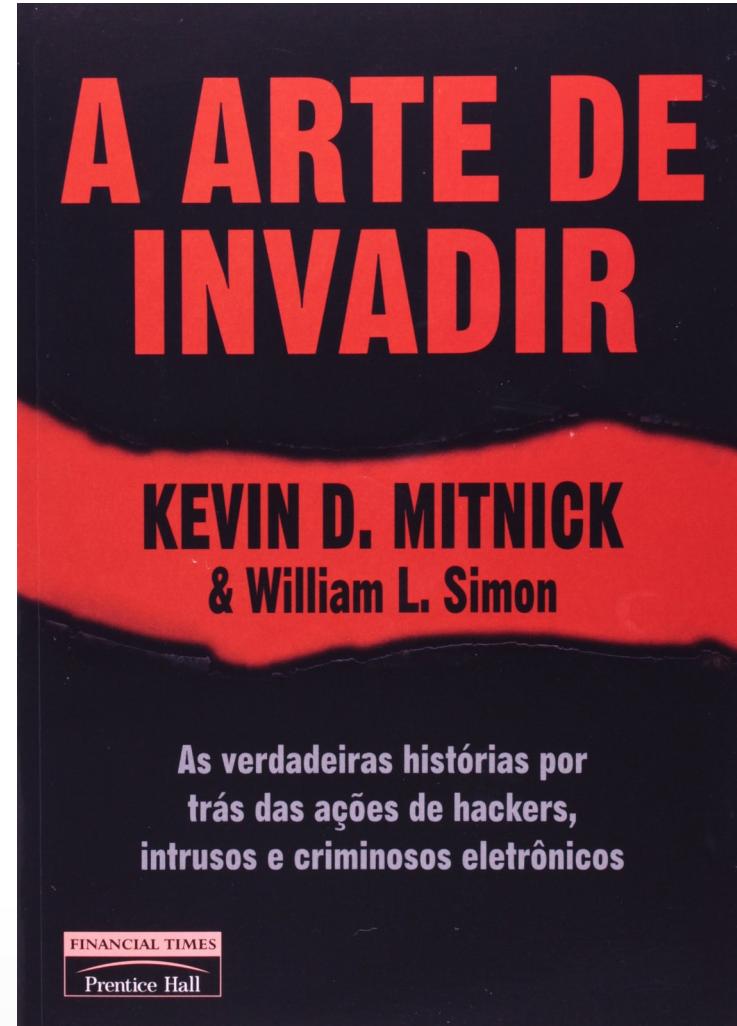
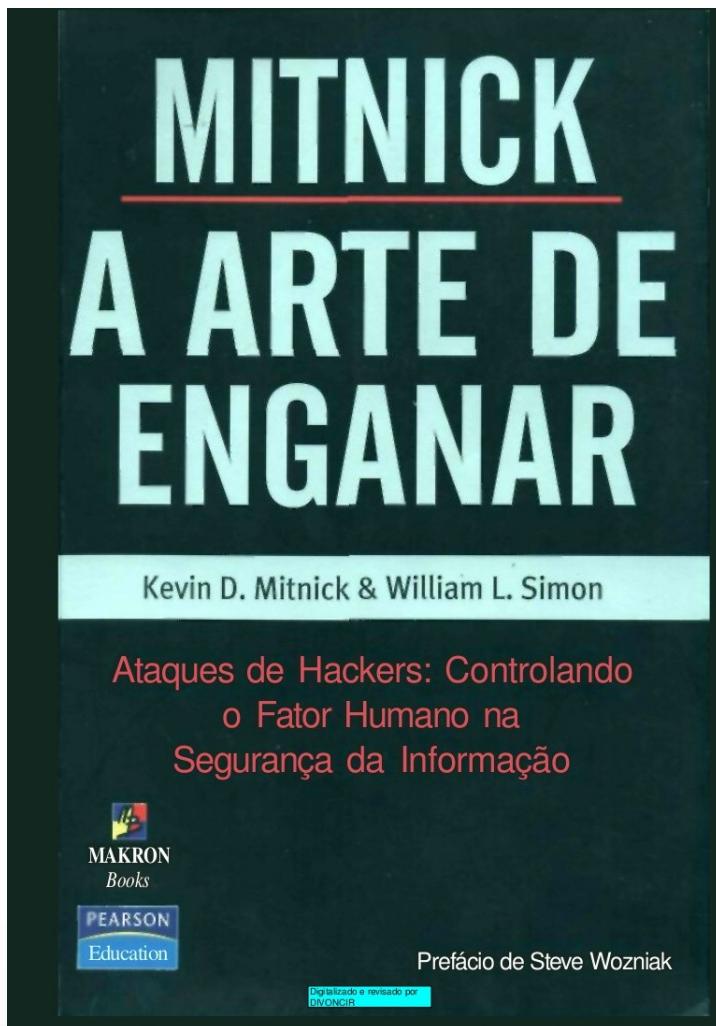


# Indicações - Livros





# Indicações - Livros



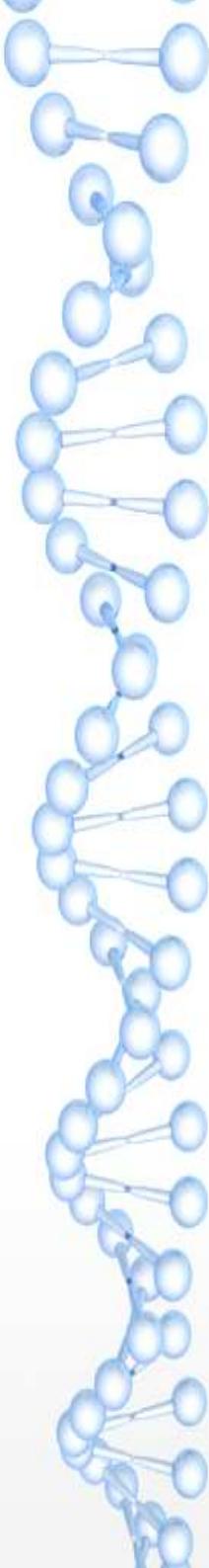
# Indicações - PodCast



The screenshot shows the homepage of the Segurança Legal Podcast website. At the top right is the logo, which features a stylized padlock icon with a keyhole and the text "PODCAST SEGU RANÇA LEGAL". Below the logo is a navigation bar with links: AGRADECIMENTOS, APOIE, ARTIGOS, ASSINE, CRÉDITOS, FALE CONOSCO, LISTA DE EPISÓDIOS, QUEM SOMOS, SUAS SUGESTÕES, and VLOG. Below the navigation bar are five episode thumbnails, each with a small image and a caption:

- Episódio #169 – Uso de dados por farmácias
- Episódio #168 – Resumo de Notícias Especial
- Episódio #167 – Seguro contra haters
- Episódio #166 – Resumo de Notícias
- Episódio #165 – Criminalização do Revenge Porn

[www.segurancalegal.com](http://www.segurancalegal.com)



PODCAST  
**SEGURANÇA  
LEGAL**  
www.segurancalegal.com

## Episódio #169 – Uso de dados por farmácias

7 de setembro de 2018

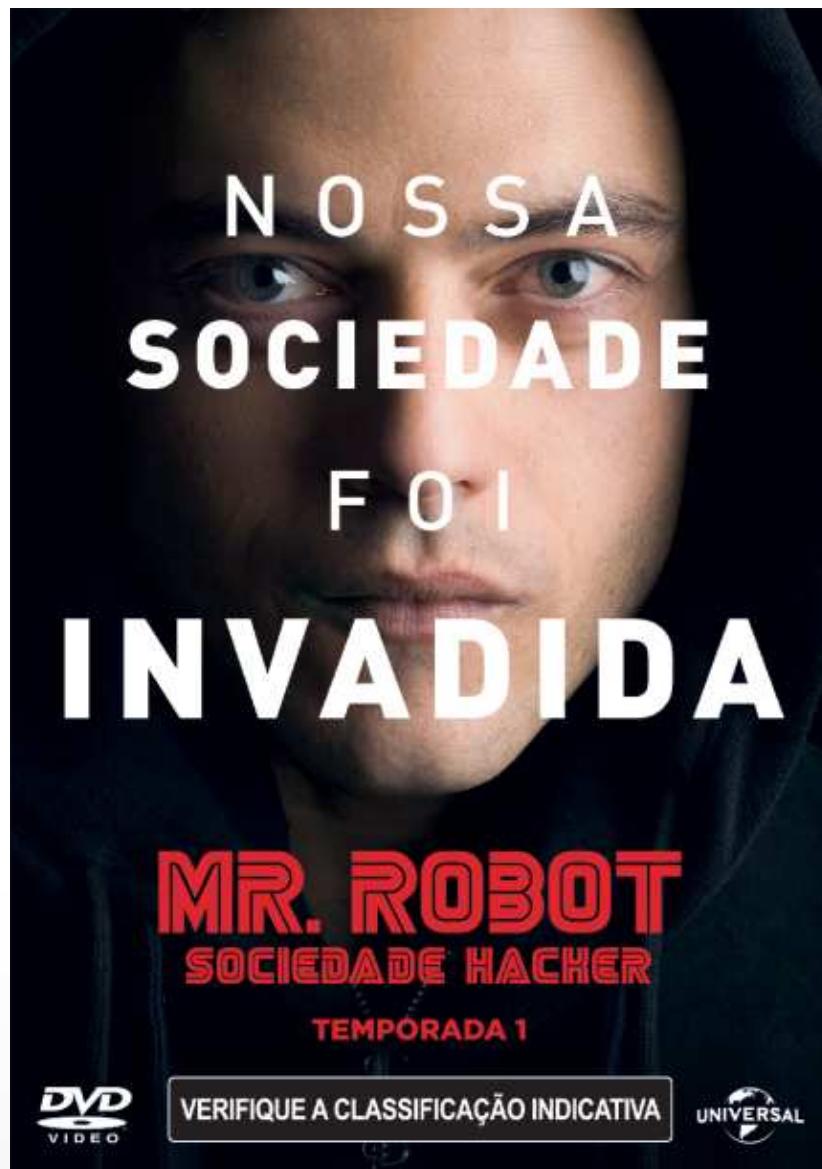
Neste episódio vamos conversar com o Davi Teófilo e a Luíza Brandão sobre a representação do IRIS acerca do uso de dados pessoais pelas farmácias.

*Ajude o Segurança Legal a continuar existindo. Visite nossa campanha de financiamento coletivo e nos apoie!*

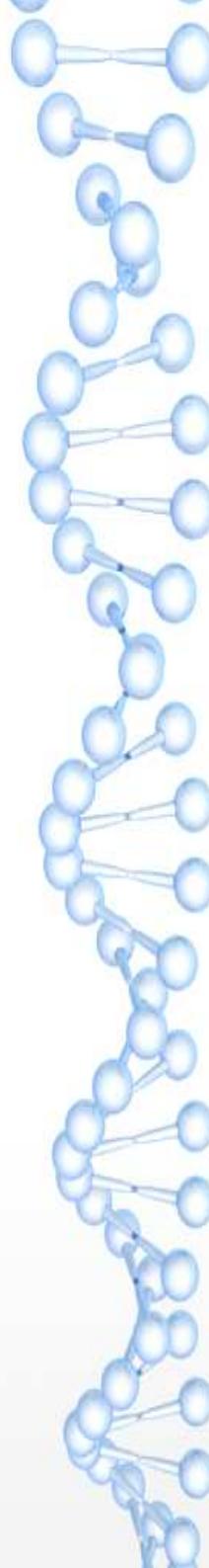
# Indicações - Filme

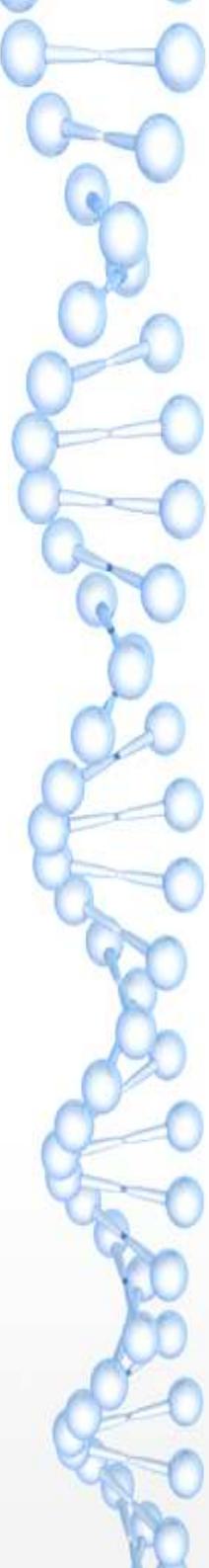


# Indicações - Séries

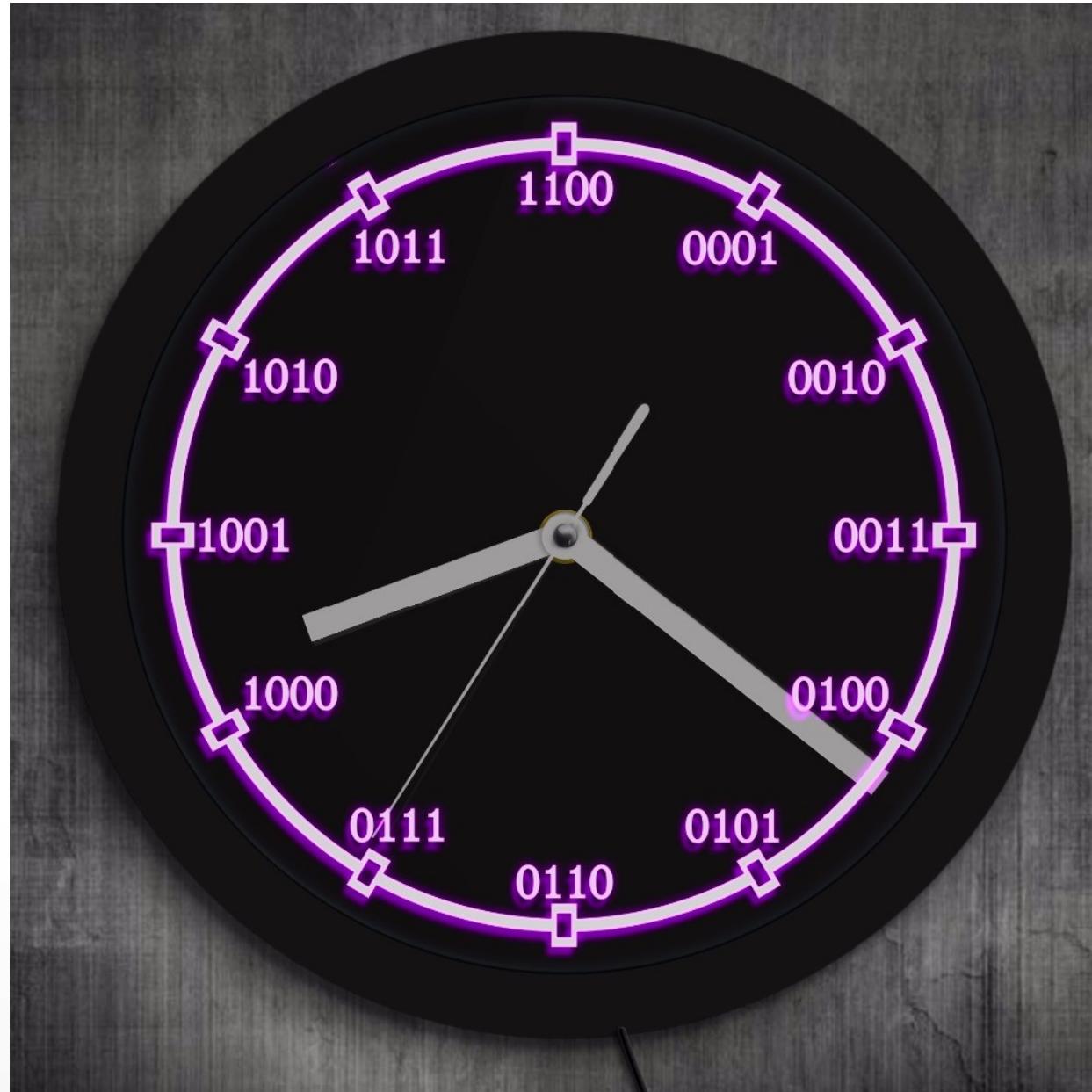








# Temos tempo ainda?





**TREND**  
**MICRO**<sup>TM</sup>



**Ensino a distância**  
**Aprendizado Contínuo**  
**Liberdade**  
**Colaborativismo**

- \* **Vídeo aulas**
- \* **Documentações**
- \* **Dicas**



[youtube.com/projetoroot](https://youtube.com/projetoroot)

# Perguntas?

- [diegocosta@projetoroot.com.br](mailto:diegocosta@projetoroot.com.br)
- [www.projetoroot.com.br](http://www.projetoroot.com.br)
- [youtube.com/projetoroot](http://youtube.com/projetoroot)
- [facebook.com/projetoroot](http://facebook.com/projetoroot)
- [wiki.projetoroot.com.br](http://wiki.projetoroot.com.br)

•  
Diego Costa  
CEO – Projeto Root