

Tecnologia de  
identidade digital  
e criptografia  
no mundo *paperless*



Sergio Leal





maior portal de notícias  
sobre certificação digital





- ✓ Colunista e membro do conselho editorial do CryptID.
- ✓ Especialista em Certificação Digital e Arquitetura Corporativa
- ✓ Trabalha com criptografia e certificação Digital desde o início da década de 90, tendo ocupado posições de destaque em empresas líderes em seu segmento como Modulo e CertiSign.
- ✓ Criador da 'ittru': Primeira solução de certificação digital mobile no mundo.
- ✓ Bacharel em Ciências da Computação pela UERJ desde 1997.
- ✓ Certificações:
- ✓ Project Management Professional (desde 2007)
- ✓ TOGAF 9.1 Certified



Business?

# Digital Disruption



1975  
Filmes 90%  
Câmeras  
85%

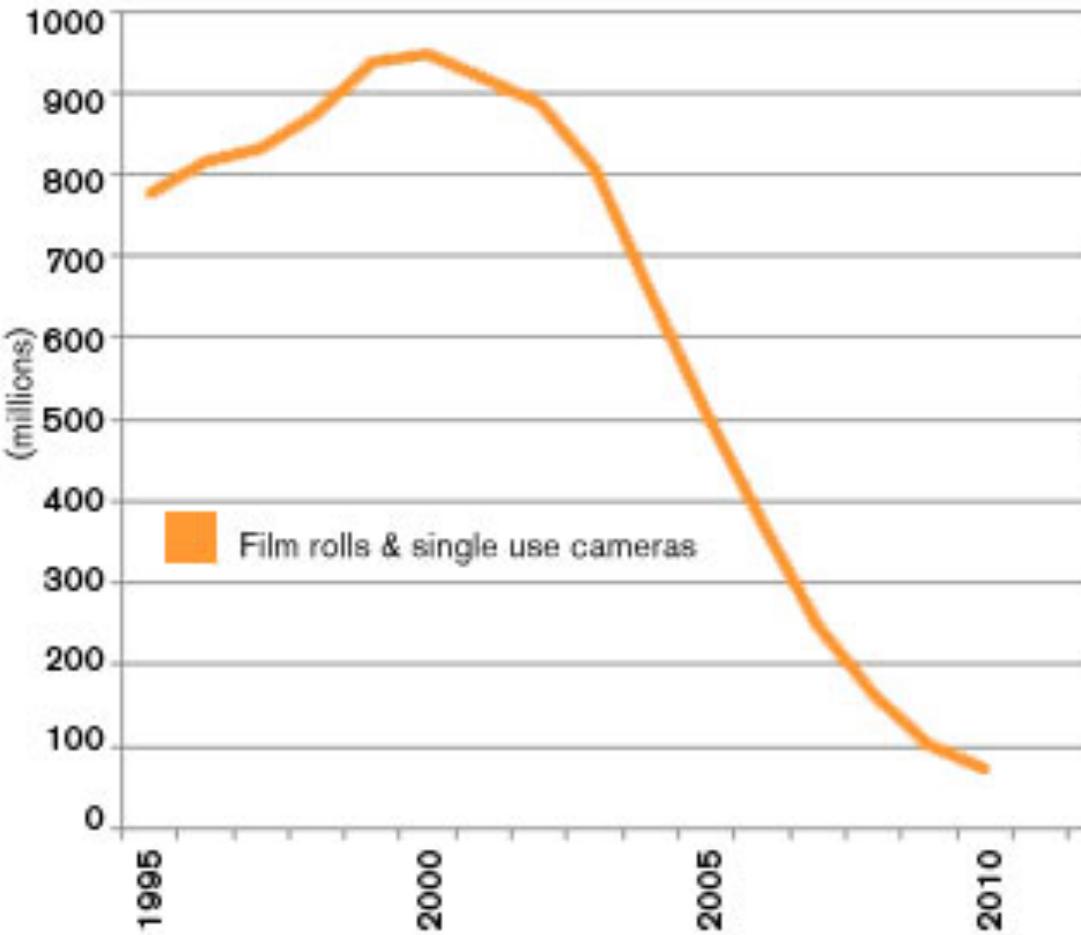


1975  
Invenção da  
Câmera  
Digital

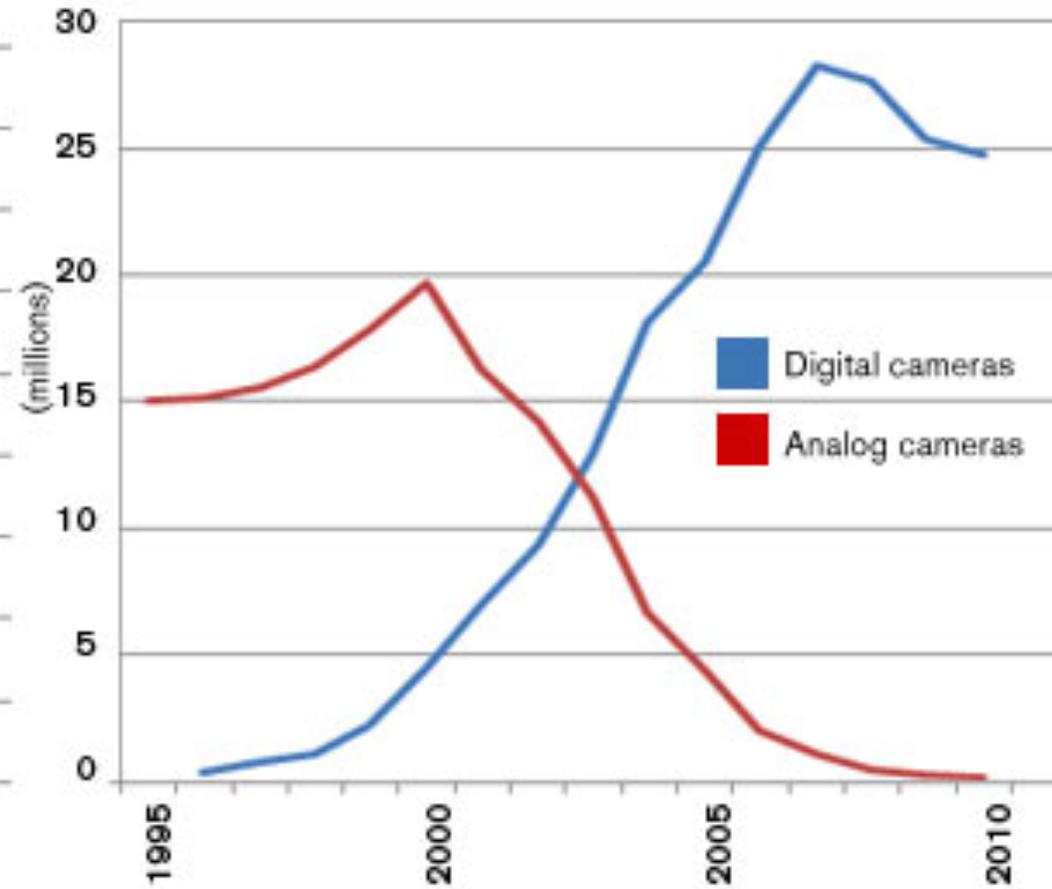


# Decline of Film

## Film rolls sold



## Camera sales





# 52% of the Fortune 500 firms since 2000 are gone

52% das empresas Fortune 500

De 2000 sumiram!



"Você pode ignorar a realidade, mas não pode ignorar as consequências de ignorar a realidade"

Ayn Rand



- ✓ *Contexto*
  - ✓ *Empresas e Serviços*
  - ✓ *Pessoas*
- ✓ *Identidade Digital*
- ✓ *Sigilo*
- ✓ *Conclusões*





U B E R



airbnb



WhatsApp

NETFLIX



“Software  
vai devorar  
o mundo”

Marc Andreessen



ANDY GREENBERG SECURITY 07.24.15 12:30 PM

SHARE

f SHARE 16368

t TWEET 1473

p PIN

# AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

Após hack de Jeep, Chrysler faz Recall

De 1,4 milhões de veículos

para consertar bug



# Lucro da GM cai 88% no 1º tri após custos com recall em massa COMENTE

Do UOL, em São Paulo 24/04/2014 | 12h52



Ouvir texto Imprimir Comunicar erro

A General Motors informou nesta quinta-feira (24) que o seu lucro no primeiro trimestre caiu 88% após um recall em massa, devido a defeito na chave de ignição de veículos.

Mas os resultados ainda superaram as expectativas em função das vendas de picapes da montadora na América do Norte.

O lucro líquido da GM no primeiro trimestre caiu para US\$ 108 milhões, ou US\$ 0,06 por ação, ante US\$ 873 milhões, ou US\$ 0,58 dólar, no mesmo período do ano passado. O trimestre mais recente incluiu custos de recall de US\$ 0,48 por papel.

A receita subiu 1,4% na comparação anual, para US\$ 37,4 bilhões, mas abaixo dos US\$ 38,4 bilhões estimados por analistas.

O recall de milhões de veículos teve custo de US\$ 1,3 bilhão e o defeito foi associado a 13 mortes. Defensores da segurança e alguns legisladores pediram que a GM estabelecesse um fundo de compensação para as vítimas.



SHARE

f SHARE  
1817

t TWEET  
1160

p PIN

COMMENT  
142

# RESEARCHERS HACKED A MODEL S, BUT TESLA'S ALREADY RELEASED A PATCH



Pesquisadores hackearam um modelo S

mas Tesla já publicou um patch

ECMSHOW  
2015  
INFORMATION  
LEADERS FORUM

# The Tesla Model S demolishes Consumer Reports' rating system

By Bill Howard on August 28, 2015 at 8:24 am | 111 Comments

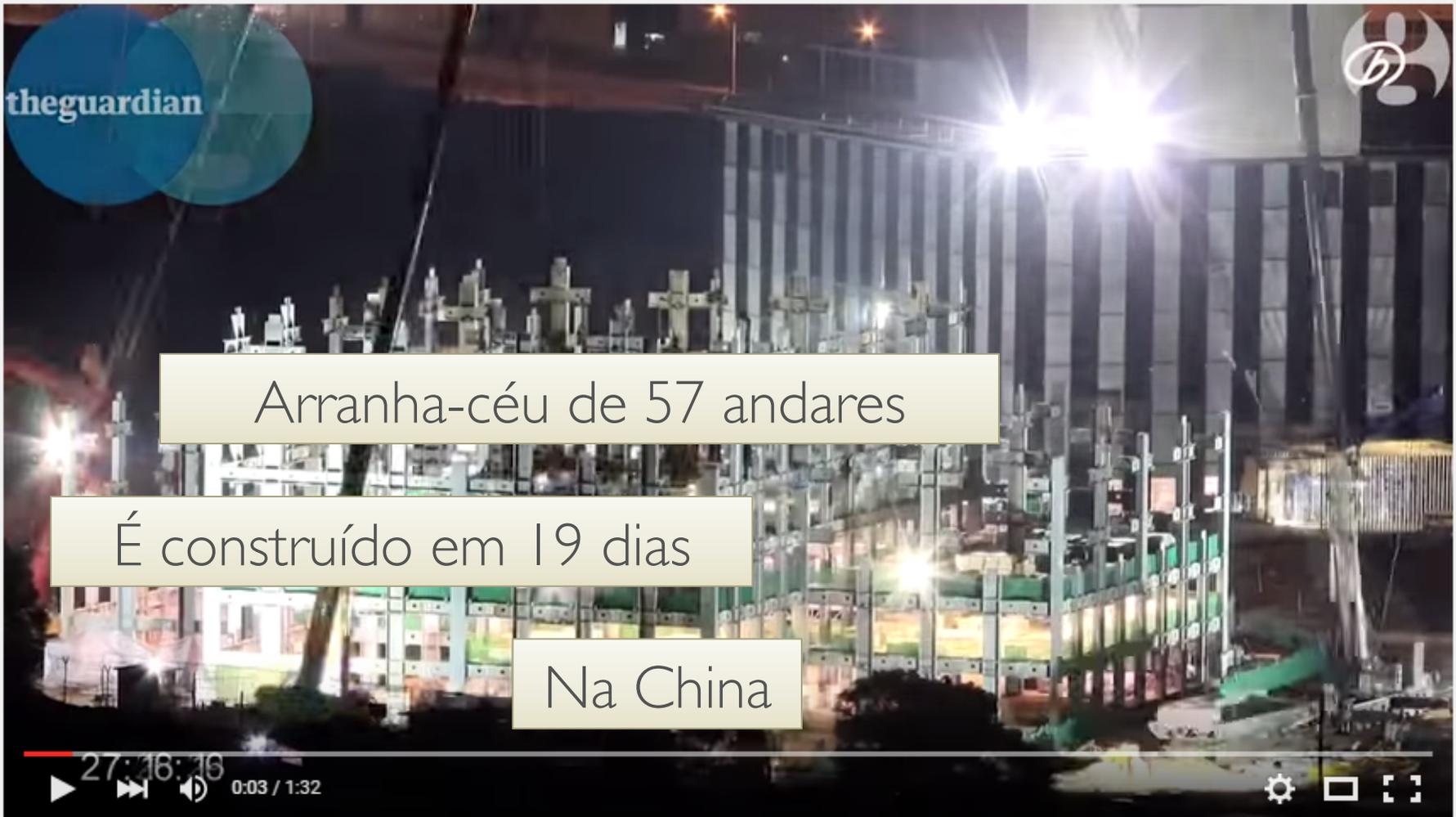


Modelo S da Tesla demole

o sistema de notas

da *Consumer Reports*





Arranha-céu de 57 andares

É construído em 19 dias

Na China

Chinese build 57-storey skyscraper in 19 days – timelapse



Geração	1940	1950	1960	1970	1980	1990	2000	2010
Baby Boomers	■	■						
Geração X			■	■				

Gerações Analógicas

Geração	1940	1950	1960	1970	1980	1990	2000	2010
Baby Boomers	■	■						
Geração X				■	■			
Geração Y					■	■		

Geração Internet



Geração	1940	1950	1960	1970	1980	1990	2000	2010
Baby Boomers	■	■						
Geração X			■					
Geração Y					■	■		
Geração Z							■	■

Geração  
Mobile /  
YouTube

# Identidade Digital



# A compreensão humana

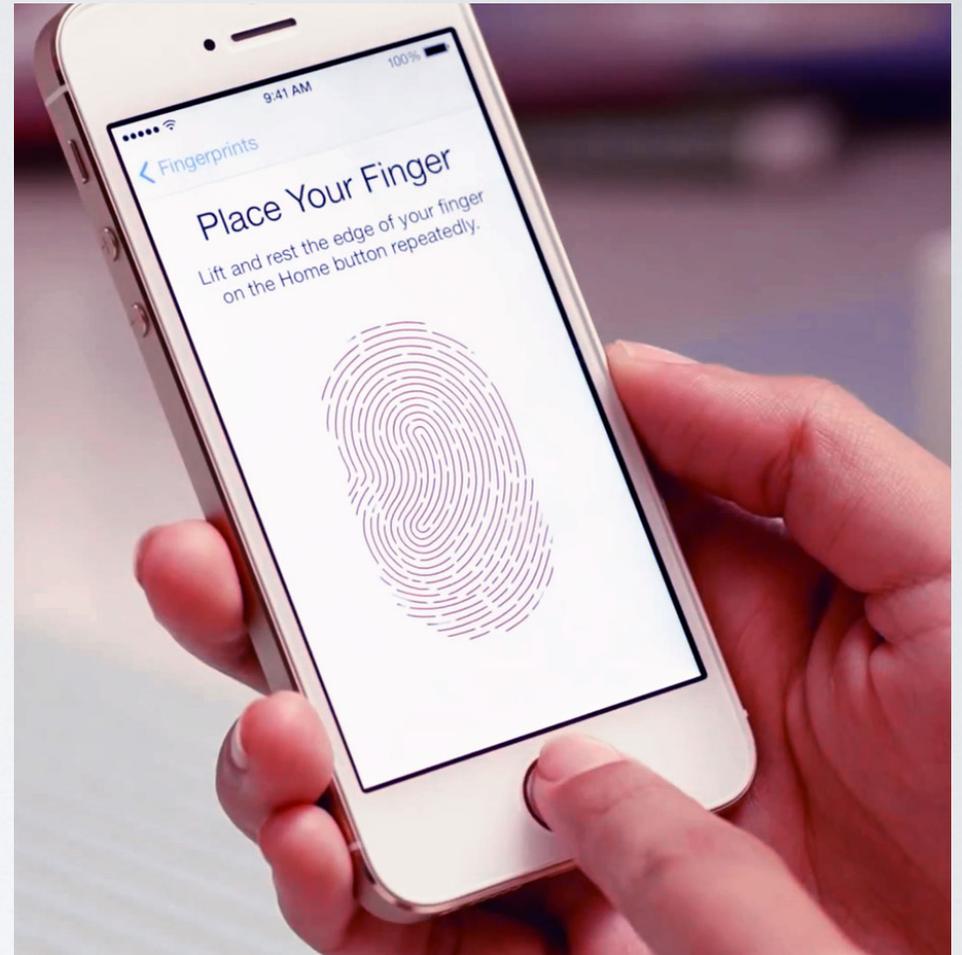


# Senhas descartáveis



Credenciais para múltiplos serviços

# Biometria



# Biometria

## This 7-Year-Old Hacked Apple's Touch ID In The Simplest Way

NEWS James Peckham 13:26, 3 Dec 2014



Garoto de 7 anos hackeou

O TouchId da Apple do

A se jeito mais simples

ne fingerprint

# Biometria

- ✓ Não permite múltiplas identidades;
- ✓ Independe da vontade;
- ✓ Não pode ser alterada;
- ✓ Sensores podem ser caros;



# Autenticação Federada

f t in BI Intelligence Events

[Sign-in](#) v [Edition](#) v

Username or Email

Password

Remember me

[Login](#) [Register](#)

[Forgot your username or password?](#)

CONNECT WITH

t f g+



# Autenticação Federada

- ✓ Rastreamento de atividades



# Internet das Coisas



# Segurança em camadas

TRENDING: Back to School · Working STEM students may be forced to leave U.S. · Resources/White Papers

**COMPUTERWORLD** Popular Now: [dropdown] [Twitter] [LinkedIn] [Facebook] [Google+] [RSS]

Home > Security > Cybercrime & Hacking

NEWS

## Sony hackers targeted employees with fake Apple ID emails

**Hackers da Sony atacaram funcionários com e-mails falsos de Apple ID**

**MORE LIKE THIS**

- Sony hack: Never underestimate the stupid criminals
- The Irari rules for declaring cyberattack 'sophisticated'

on IDG Answers → How to backup PS4 internal drive to external 2TB HDD when I'm getting "file..."

IDG.tv



# Como se sente?

PREPARE FOR THE DAY  
EVERYONE FEARS.

Witness the rebirth of the legend in this retelling of the infamous horror film that terrified audiences everywhere. After the supposed death of her son at Camp Crystal Lake, a mother begins to take vengeance into her own hands by slaughtering the teenage counselors who let him drown. After her death at the hands of one of the teens, her son returns to continue her bloody legacy. They were warned. They are doomed. And on Friday the 13th, nothing will save them!

NEW LINE CINEMA PRESENTS IN ASSOCIATION WITH MICHAEL BAY A PLATINUM DUNES/ NEXT ENTERTAINMENT PRODUCTION  
"FRIDAY THE 13TH" JARED PADALECKI DANIELLE PANABAKER AMANDA RIGHETTI TRAVIS VAN WINKLE DEREK MEARS AARON YOO WILLA FORD  
AND NANA VISITOR AS PAMELA VOORHEES EDITED BY KEN BLACKWELL DIRECTOR OF PHOTOGRAPHY DANIEL C. PEARL  
EXECUTIVE PRODUCERS SEAN S. CUNNINGHAM TOBY EMMERICH BRIAN WITTEN  
PRODUCED BY ANDREW FORM BRAD FULLER MICHAEL BAY WRITTEN BY DAMIAN SHANNON AND MARK SWIFT DIRECTED BY MARCUS NISPEL

NOT AUTHORIZED FOR SALE OR RENTAL OUTSIDE THE USA AND CANADA. This copyrighted product has been manufactured and distributed by Warner Home Video, a Warner Bros. Home Entertainment Company, and is authorized for sale or rental for private home use in the USA and Canada ONLY. The sale or rental of this product outside of the USA and Canada has NOT been authorized by Warner Home Video, and is in direct violation of its written terms of trade. Federal Law provides severe civil and criminal penalties for the unauthorized distribution, reproduction or exhibition of copyrighted motion pictures, videotapes or videodisks.

FRIDAY THE 13TH Package Design and Supplementary Material Compilation (C) 2009 Warner Bros. Entertainment Inc. Distributed by Warner Home Video, 4000 Warner Blvd., Burbank, CA 91522. All Rights Reserved. "Dolby" and the "DD" symbol are trademarks of Dolby Laboratories Licensing Corporation.

WIDESCREEN VERSION PRESENTED IN A LETTERBOX WIDESCREEN FORMAT PRESERVING THE "SOFT" ASPECT RATIO OF ITS ORIGINAL THEATRICAL EXHIBITION. ENHANCED FOR WIDESCREEN TV'S.

**R RESTRICTED**  
FOR STRONG BLOOD/VIOLENCE, SOME GRAPHIC SEXUAL CONTENT, LANGUAGE AND DRUG MATERIAL  
Bonus Material/Trailer Not Rated.

PROOF OF PURCHASE 33330A  
PROOF OF PURCHASE 33330B  
ISSN 0-7907-9200-4  
0 185393 35302 5

WIDESCREEN EDITION

# FRIDAY THE 13<sup>TH</sup>

WELCOME TO CRYSTAL LAKE



# Certificação Digital

- ✓ Não depende da compreensão humana;
- ✓ Permite operar “n para n”;
- ✓ Permite múltiplas identidades;
- ✓ Não pode ser usado ‘dormindo’;
- ✓ Pode ser alterada;
- ✓ Não pode ser rastreado;



# Validade Jurídica



## Presidência da República Casa Civil Subchefia para Assuntos Jurídicos

### MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

**O PRESIDENTE DA REPÚBLICA**, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

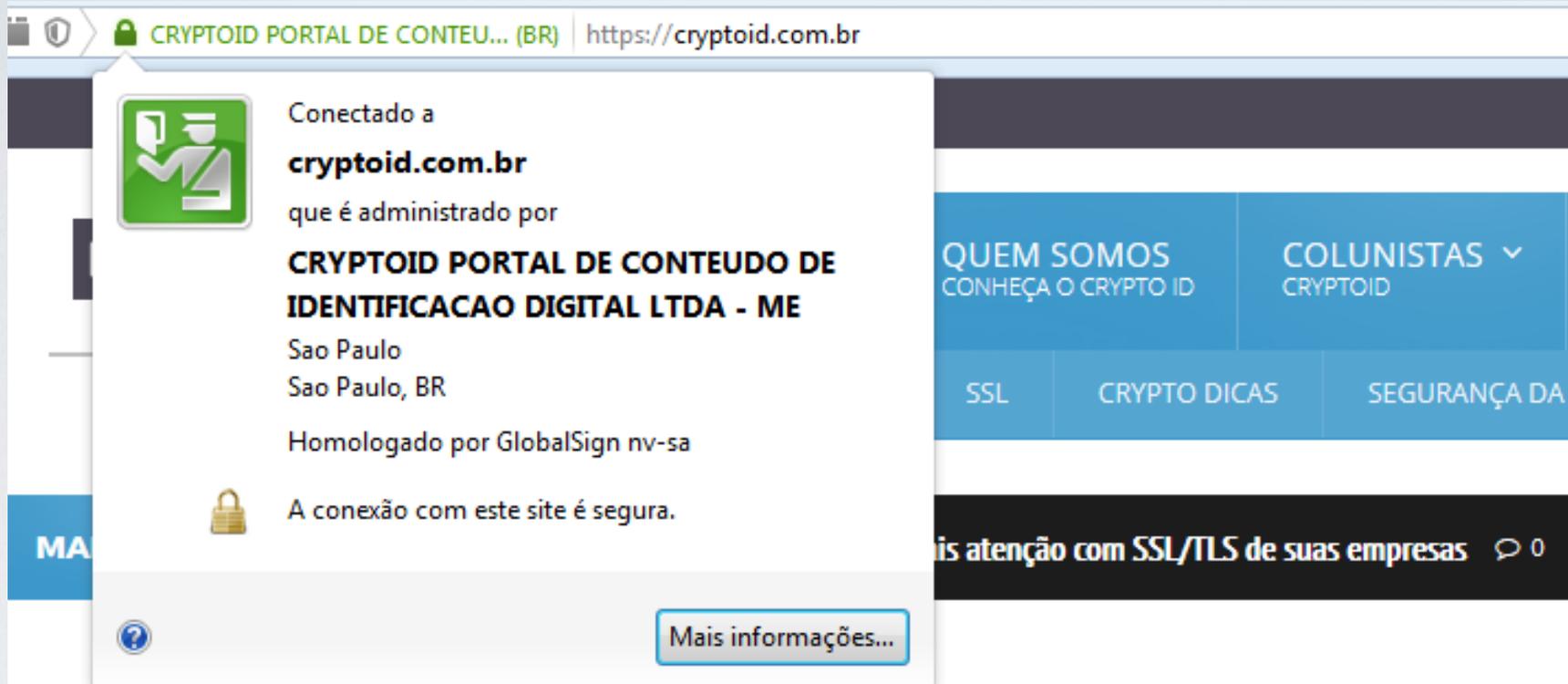
§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.



# ○ SSL/TLS é popular!



The image shows a browser window with a security notification overlay. The notification is for the website **cryptoid.com.br**, which is administered by **CRYPTOID PORTAL DE CONTEUDO DE IDENTIFICACAO DIGITAL LTDA - ME** in São Paulo, BR. It states that the connection is secure and homologated by GlobalSign nv-sa. The background website has a blue header with navigation links: **QUEM SOMOS** (CONHEÇA O CRYPTO ID), **COLONISTAS** (CRYPTOID), **SSL**, **CRYPTO DICAS**, and **SEGURANÇA DA**. A black banner at the bottom of the page reads **is atenção com SSL/TLS de suas empresas**.

Conectado a  
**cryptoid.com.br**  
que é administrado por  
**CRYPTOID PORTAL DE CONTEUDO DE IDENTIFICACAO DIGITAL LTDA - ME**  
Sao Paulo  
Sao Paulo, BR  
Homologado por GlobalSign nv-sa

A conexão com este site é segura.

Mais informações...





## Aplicação

Applet Java

Active X

Java (JRE)

Navegador

MS-CAPI / PKCS#11 / MS-CGN

Sistema Operacional

PC/SC

Driver (USB)

USB

Driver (PC/SC)

Leitora

Driver (ISO7816)

## Cartão

## Aplicação

Applet Java

Active X

Java (JRE)

Navegador

MS-CAPI / PKCS#11 / MS-CGN

Sistema Operacional

PC/SC

Driver (USB)

USB

Driver (PC/SC)

Leitora

Driver (ISO7816)

## Cartão

## Aplicação

Applet Java

Active X

Java (JRE)

Navegador

MS-CAPI / PKCS#11 / MS-CGN

Sistema Operacional

PC/SC

Driver (USB)

USB

Driver (PC/SC)

Leitora

Driver (ISO7816)

## Cartão

## Aplicação

Applet Java

Active X

Java (JRE)

## Navegador

MS-CAPI / PKCS#11 / MS-CGN

Sistema Operacional

PC/SC

Driver (USB)

USB

Driver (PC/SC)

Leitora

Driver (ISO7816)

## Cartão

## Aplicação

Applet Java

Active X

Java (JRE)

Navegador

MS-CAPI / PKCS#11 / MS-CGN

Sistema Operacional

PC/SC

Driver (USB)

USB

Driver (PC/SC)

Leitora

Driver (ISO7816)

## Cartão

## Aplicação

Applet Java

Active X

Java (JRE)

Navegador

MS-CAPI / PKCS#11 / MS-CGN

## Sistema Operacional

PC/SC

Driver (USB)

USB

Driver (PC/SC)

Leitora

Driver (ISO7816)

## Cartão

## Aplicação

Applet Java

Active X

Java (JRE)

Navegador

MS-CAPI / PKCS#11 / MS-CGN

Sistema Operacional

PC/SC

Driver (USB)

USB

Driver (PC/SC)

Leitora

Driver (ISO7816)

## Cartão



## Aplicação

Applet Java

Active X

Java (JRE)

Navegador

MS-CAPI / PKCS#11 / MS-CGN

Sistema Operacional

PC/SC

Driver (USB)

USB

Driver (PC/SC)

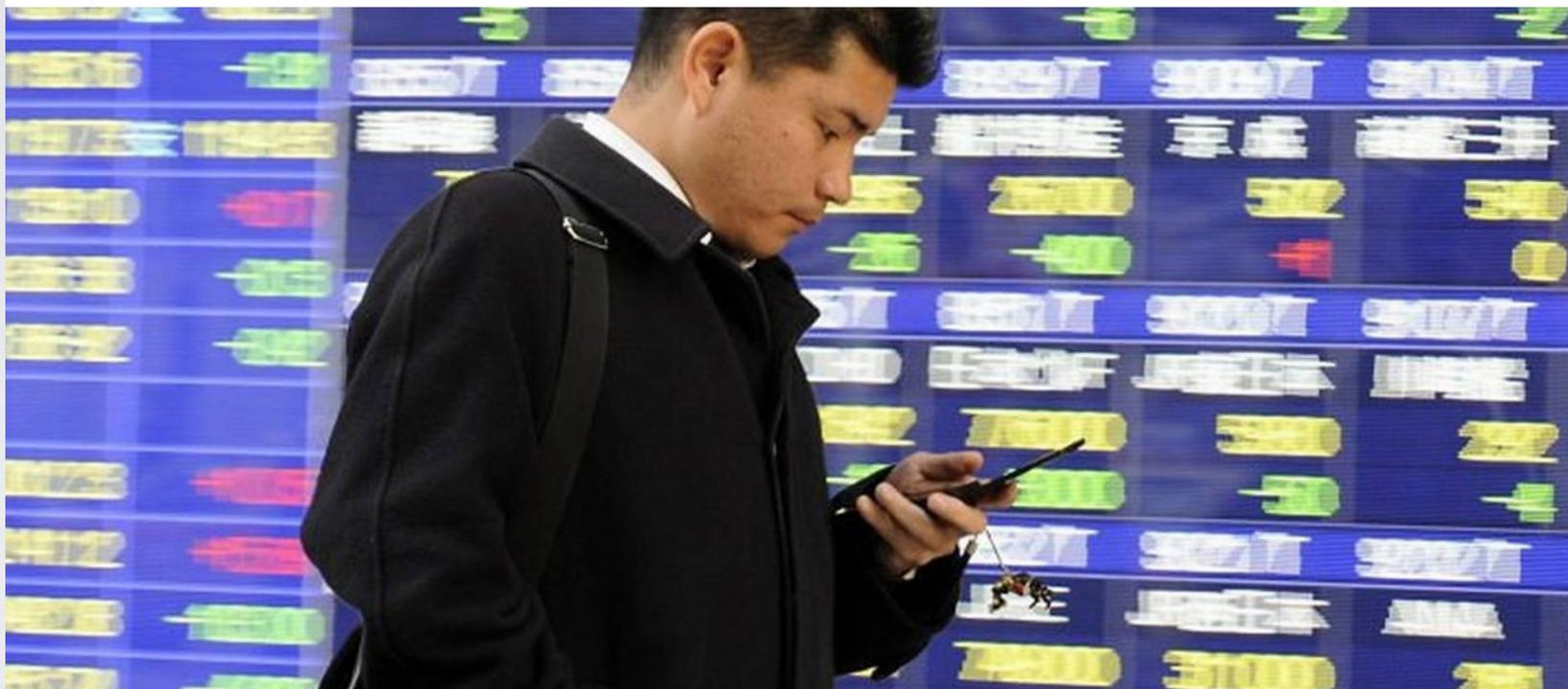
Leitora

Driver (ISO7816)

Cartão

# Programa criado por cariocas simplifica acesso a certificados digitais

POR CARLOS ALBERTO TEIXEIRA ///  
21/02/2010 0:00 / ATUALIZADO 01/11/2011 2:00



Com a ajuda do telefone celular, o processo de certificação bolado pela Timewarp com o Ittru parece mais simples que os métodos tradicionais Crédito: AFP Photo -



ARQUIVO CRYPTO ID COLUNISTAS DESTAQUES SERGIO LEAL

# Você conhece a Web Cryptography API da W3C?



<http://oglobo.globo.com/sociedade/tecnologia/programa-criado-por-cariocas-simplifica-acesso-certificados-digitais-3051035>



ARQUIVO CRYPTO ID CERTIFICAÇÃO DIGITAL DESTAQUES LEGISLAÇÃO, RECURSOS E NORMAS

## Hackers invadem Ibama e com certificado digital liberam venda de madeira



<https://cryptoid.com.br/arquivo-cryptoid/hackers-invadem-ibama-e-com-certificado-digital-liberam-venda-de-madeira/>

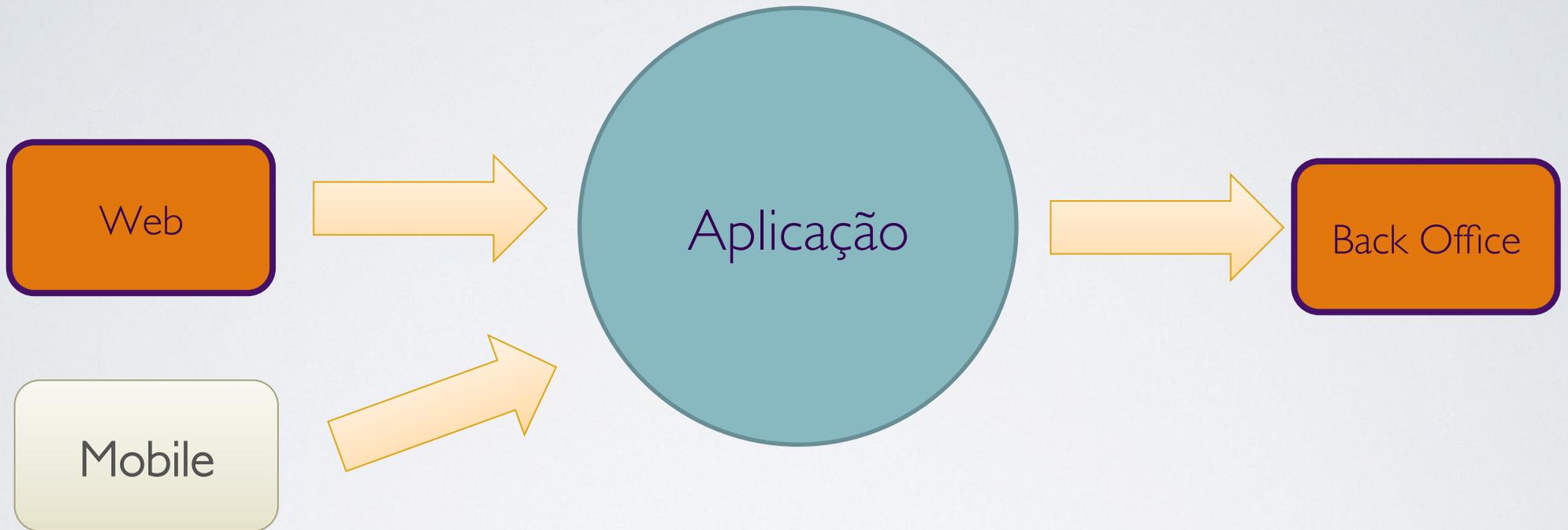
# Como Começa?



# Arquitetura Web



+ Mobile



○ que encontramos?



# Como é?



PKCS#11

MSCAPI

PC/SC

CAAdES  
XAdES  
PAdES  
CMS  
XMLDSig

SigningTime  
Countersignature



# Software Livre



Software Livre para assinatura digital

- ✓ Segue padrões ICP-Brasil
- ✓ ADRB 1.0 e 2.1
- ✓ Orientado a serviço
- ✓ Multi browser, multi OS
- ✓ Substitui o CAPICOM
- ✓ Integrável a qualquer aplicativo web
- ✓ Java, .NET, PHP..
- ✓ Pode ser usado em aplicativos desktop
- ✓ Oferece ActiveX
- ✓ Applet (PKCS#11 e MSCAPI)

<http://bluecryst.al>



# Software Livre

projeto-siga / siga

Watch 20 Star 3 Fork 13

## Assinatura Digital

Markenson edited this page on 21 Aug 2014 · 1 revision

Conselho da Justiça Federal, TRF da Segunda Região, JFRJ, JFES, TJERJ, TJEPA, TRT 23 Região, UFF

## Página que reúne informações sobre assinatura digital no siga.

### Intro

O SIGA-D  
finalidade

### Detal

- ✓ Produção de documentos digitais – Processos Administrativos ou Expedientes,
- ✓ Trâmite e arquivamento,
- ✓ Workflow, Gestão de Identidade, Gestão de Conhecimento,
- ✓ Altamente aderente ao eArq.

Pages 44

Find a Page...

Home

AP 6] [DEV] Gerenciamento  
Modo Standalone (Com  
Locker)

AP 6][Hmg][Prod] Utilização do  
ambiente em modo Domain

cessando Base Teste

resentando autoridades  
rtificadoras no SIGA 3.x

oache\_HTTP\_Server\_  
onfiguracoes

ECMSHOW  
2015  
INFORMATION  
LEADERS  
FORUM

# E o Governo?

## PJe supera marca dos 5 milhões de processos eletrônicos

25/08/2015 - 10h03



TWEETAR

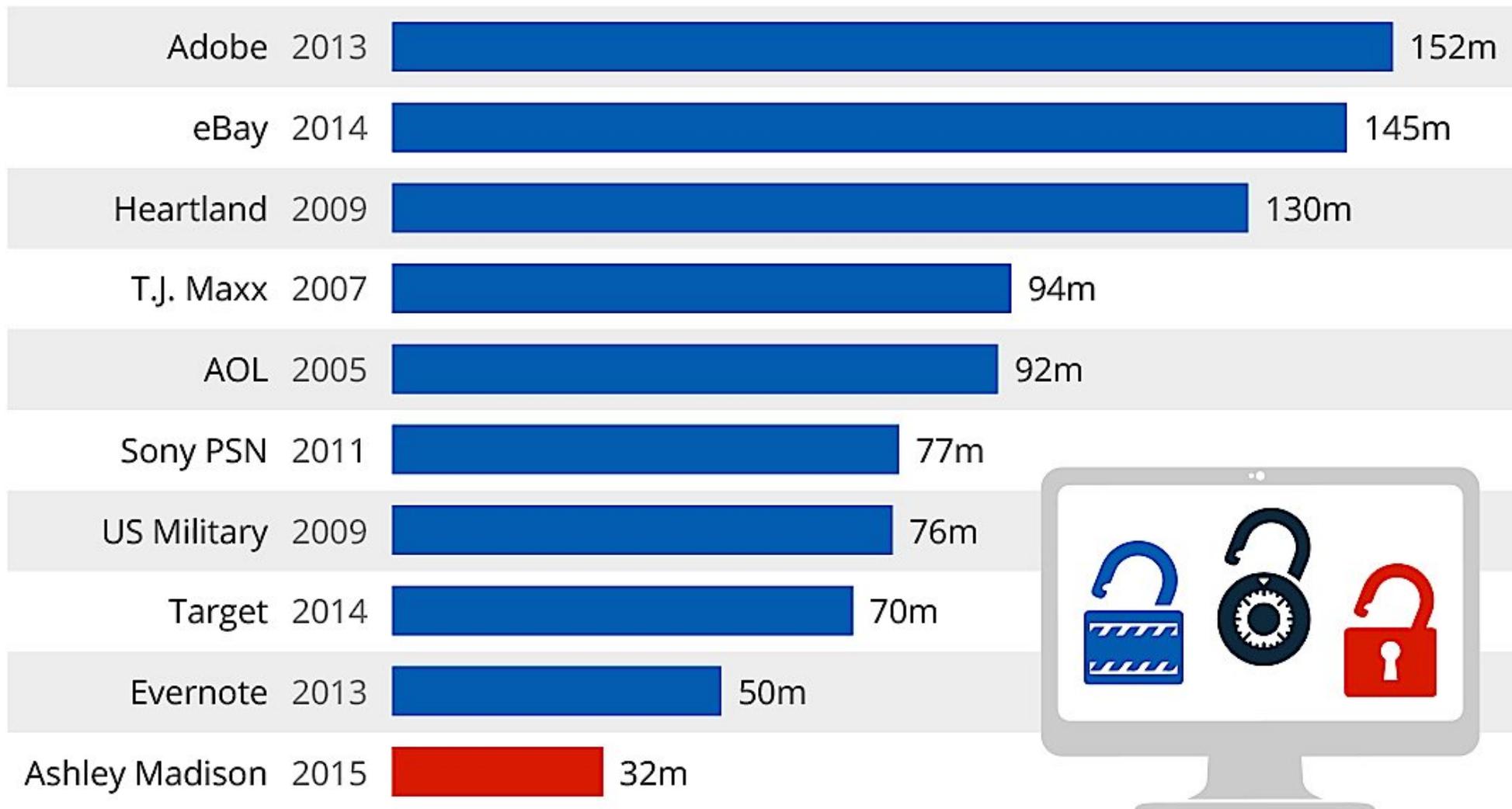


COMPARTILHAR



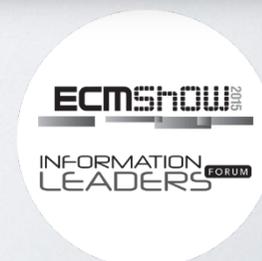
# Sigilo





**BUSINESS INSIDER**

Source: Media reports **statista**



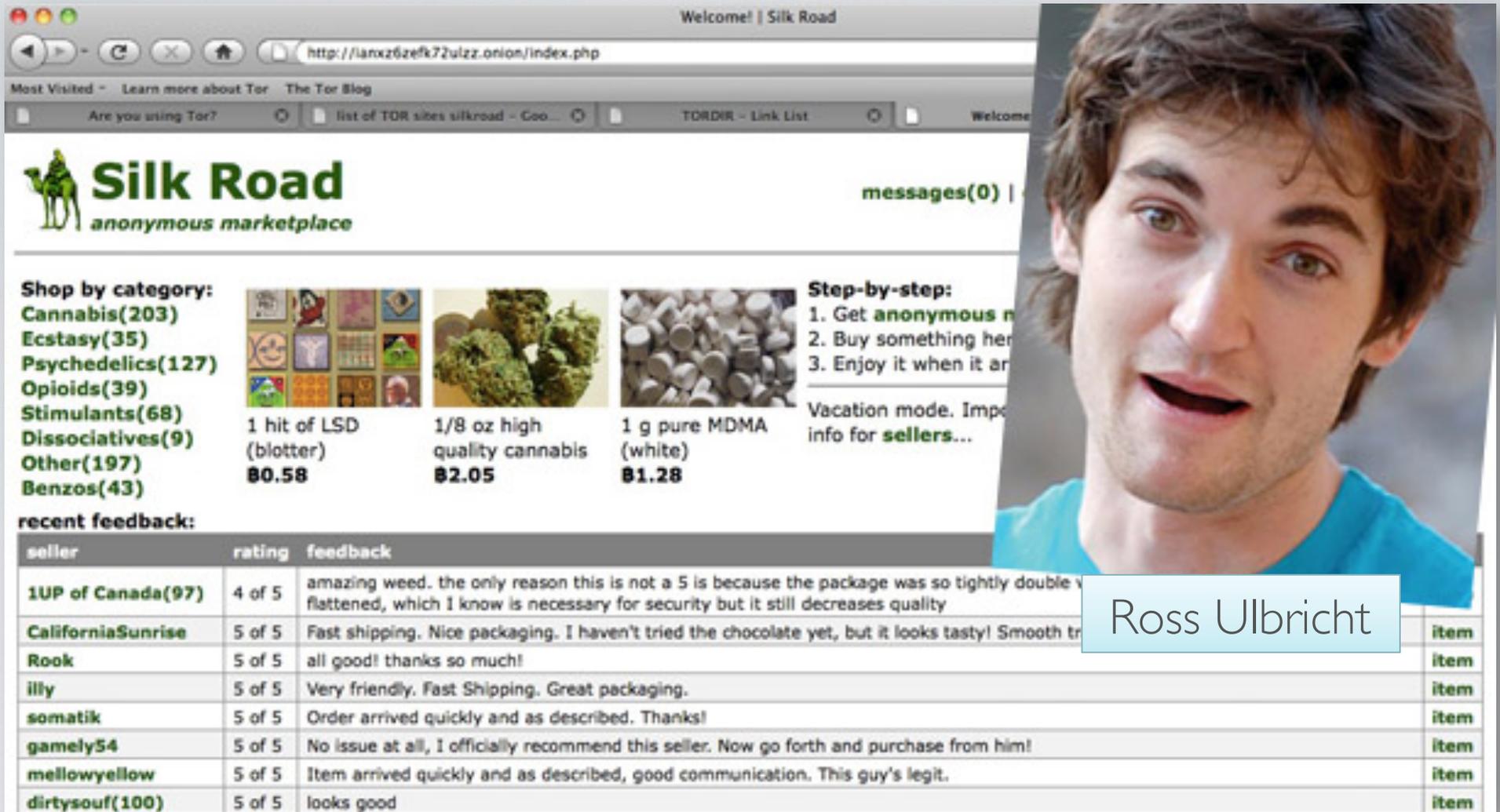


*“Criptografia é única solução para escapar da espionagem”*

Edward Snowden



# Nem os criminosos



Most Visited - Learn more about Tor The Tor Blog

Are you using Tor? list of TOR sites silkroad - Goo... TORDIR - Link List Welcome

## Silk Road

anonymous marketplace

messages(0) |

**Shop by category:**  
Cannabis(203)  
Ecstasy(35)  
Psychedelics(127)  
Opioids(39)  
Stimulants(68)  
Dissociatives(9)  
Other(197)  
Benzos(43)

**recent feedback:**

seller	rating	feedback	
<b>1UP of Canada(97)</b>	4 of 5	amazing weed. the only reason this is not a 5 is because the package was so tightly double v flattened, which I know is necessary for security but it still decreases quality	
<b>CaliforniaSunrise</b>	5 of 5	Fast shipping. Nice packaging. I haven't tried the chocolate yet, but it looks tasty! Smooth tr	<a href="#">item</a>
<b>Rook</b>	5 of 5	all good! thanks so much!	<a href="#">item</a>
<b>illy</b>	5 of 5	Very friendly. Fast Shipping. Great packaging.	<a href="#">item</a>
<b>somatik</b>	5 of 5	Order arrived quickly and as described. Thanks!	<a href="#">item</a>
<b>gamely54</b>	5 of 5	No issue at all, I officially recommend this seller. Now go forth and purchase from him!	<a href="#">item</a>
<b>mellowyellow</b>	5 of 5	Item arrived quickly and as described, good communication. This guy's legit.	<a href="#">item</a>
<b>dirtysof(100)</b>	5 of 5	looks good	<a href="#">item</a>

**Step-by-step:**  
1. Get **anonymous** n  
2. Buy something her  
3. Enjoy it when it ar

Vacation mode. Impo  
info for **sellers**...

Ross Ulbricht

Obrigado!

Sergio Leal (sergio.leal@ittru.com)



<http://bluecryst.al>

