protiviti®

Face the Future with Confidence

LEI DE PROTEÇÃO DE DADOS PESSOAIS

Agosto 2018

Internal Audit, Risk, Business & Technology Consulting

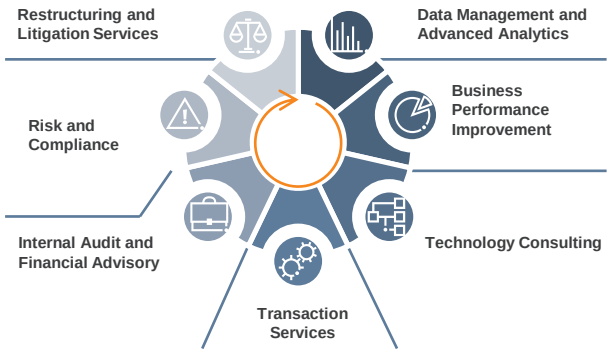
A PROTIVITI

PRESENÇA GLOBAL

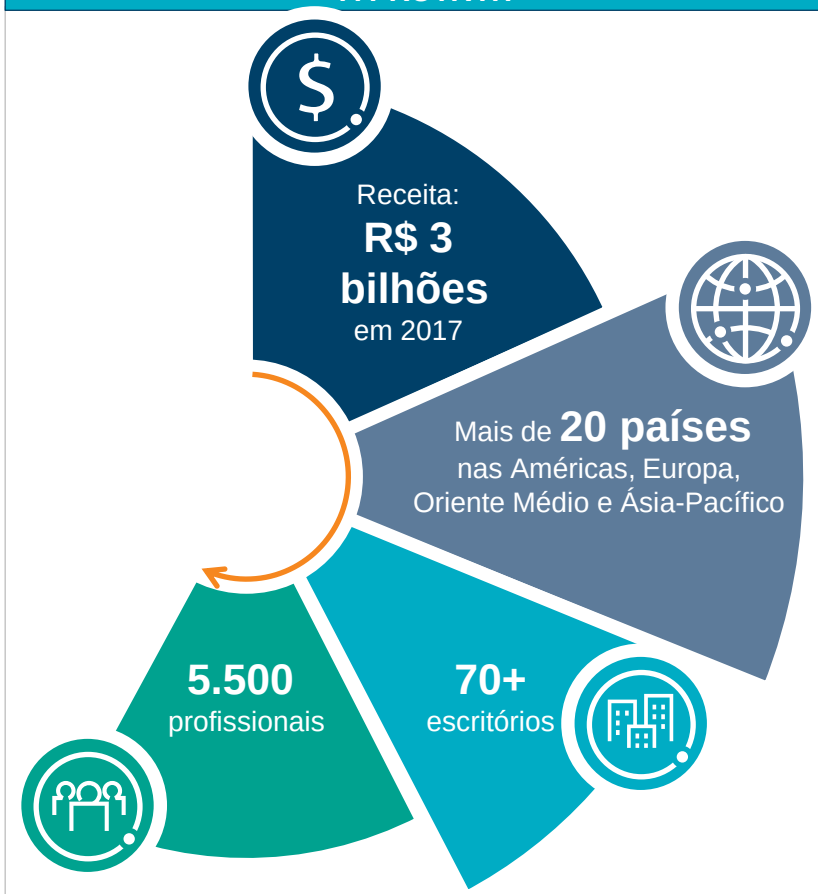
The Americas			Europe/Middle East/Africa			Asia-Pacific	
1. UNITED STATES Alexandria, VA Atlanta, GA Baltimore, MD Boston, MA Charlotte, NC Chicago, IL Cincinnati, OH Cleveland, OH Dallas, TX Denver, CO Ft. Lauderdale, FL Houston, TX	Kansas City, KS Los Angeles, CA Milwaukee, WI Minneapolis, MN New York, NY Orlando, FL Philadelphia, PA Phoenix, AZ Pittsburgh, PA Portland, OR Richmond, VA Sacramento, CA Salt Lake City, UT San Francisco, CA	San Jose, CA Seattle, WA Stamford, CT St. Louis, MO Tampa, FL Washington, D.C. Winchester, VA Woodbridge, NJ 2. ARGENTINA* Buenos Aires 3. BRAZIL* Rio de Janeiro São Paulo	4. CANADA Kitchener-Waterloo Toronto 5. CHILE* Santiago 6. MEXICO* Mexico City Monterrey 7. PERU* Lima 8. VENEZUELA* Caracas	9. FRANCE Paris 10. GERMANY Frankfurt Munich 11. ITALY Milan Rome Turin 12. THE NETHERLANDS Amsterdam	13. UNITED KINGDOM London 14. BAHRAIN* Manama 15. KUWAIT* Kuwait 16. OMAN* Muscat	17. QATAR* Doha 18. UNITED ARAB EMIRATES* Abu Dhabi Dubai 19. SAUDI ARABIA Riyadh 20. SOUTH AFRICA Johannesburg	21. AUSTRALIA Brisbane Canberra Perth Melbourne Sydney 22. CHINA Beijing Hong Kong Shanghai Shenzhen	23. INDIA Bangalore Mumbai New Delhi 24. JAPAN Osaka Tokyo 25. SINGAPORE Singapore

NOSSOS SERVIÇOS

A Protiviti ajuda empresas de todo o mundo a identificar, medir e navegar pelos riscos que enfrentam, dentro de seus setores e em todos os seus sistemas e processos, usando soluções comprovadas de valor agregado :



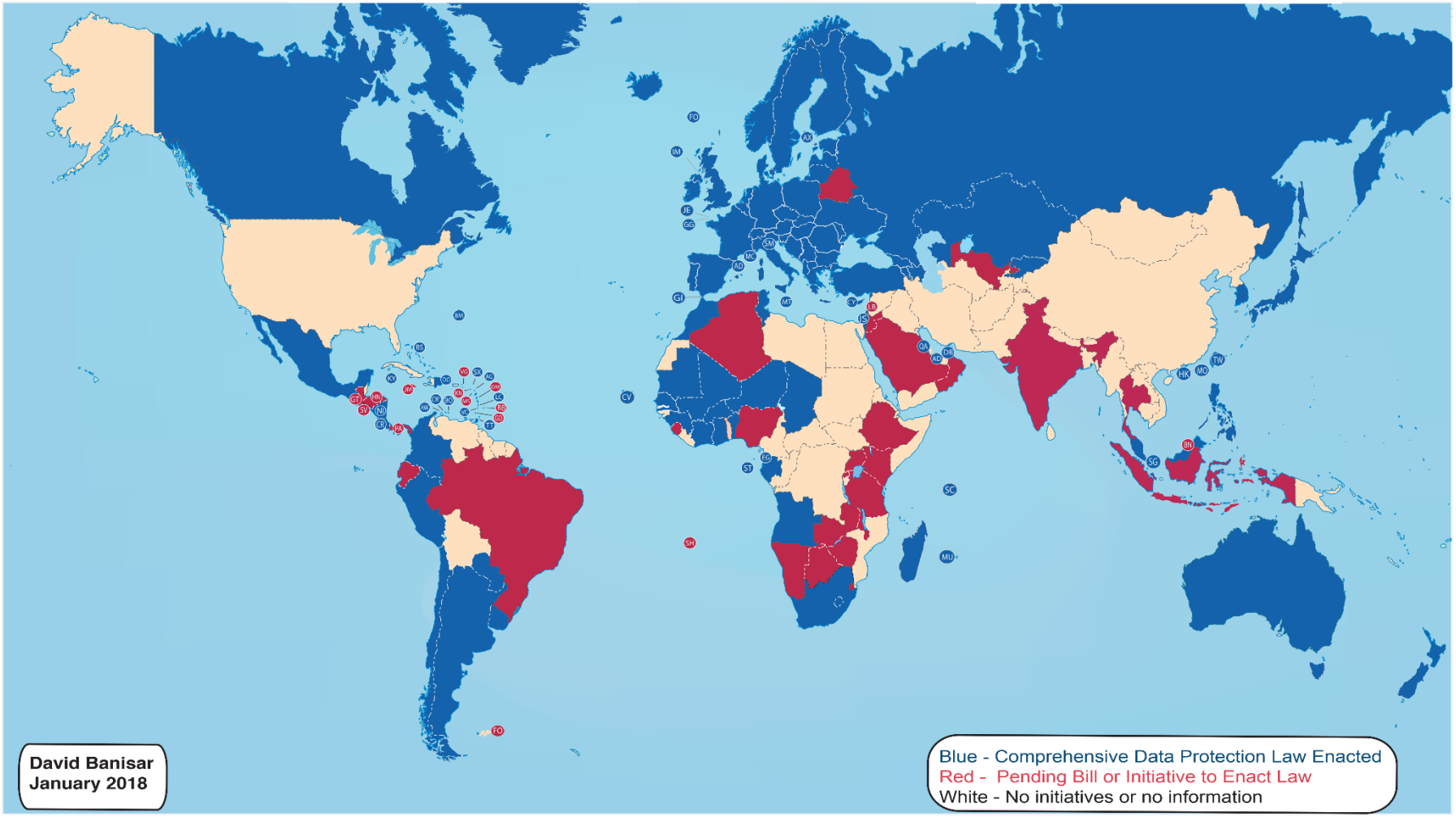
A PROTIVITI



A Protiviti (www.protiviti.com) é uma empresa global de consultoria que ajuda empresas a resolverem problemas em finanças, tecnologia, operações, governança, risco e auditoria interna

protiviti

LEIS DE PROTEÇÃO E PRIVACIDADE DE DADOS



protiviti

CENÁRIO REGULATÓRIO

Brasil

a Lei Geral de Proteção de Dados pessoais, que tramitava como Projeto de Lei da Câmara 53/2018. A lei disciplina a forma como informações são coletadas e tratadas, especialmente em meios digitais, como dados pessoais de cadastro ou até mesmo textos e fotos publicados em redes sociais. Caso seja constatada alguma irregularidade, a empresa pode receber uma série de sanções, entre as quais está prevista a ***multa diária de até 2% do faturamento, com limite de R$ 50 milhões***

União Européia

O regulamento geral de proteção de dados imporia uma legislação robusta e harmonizada em matéria de proteção de dados em toda a UE.

Asia

Cingapura, Malásia, Filipinas, Coréia do Sul e Taiwan introduziram, nos últimos cinco anos, regimes abrangentes de proteção de dados em suas respectivas jurisdições.

Estados Unidos

Nos últimos anos, o governo federal implementou uma supervisão mais rígida e promulgou requisitos específicos de gerenciamento e divulgação de riscos cibernéticos para os setores de saúde, defesa, energia e outros setores da indústria de infraestrutura crítica.

Africa do Sul

A Lei de Proteção de Informações Pessoais (Popi) da África do Sul, que entrou em vigor em novembro de 2013, regula como qualquer pessoa que processa informações pessoais deve manipular, manter e proteger essas informações.

Australia

A Lei de Privacidade (Enhancing Privacy Protection) de 2012 foi introduzida como uma emenda à Privacy Act 1988, uma lei australiana que regula o manuseio de informações pessoais sobre indivíduos.

protiviti

LEI GERAL DE PROTEÇÃO DE DADOS

- Todo tratamento de dados pessoais feito no Brasil **em "meios digitais" ou fora dele**
- Conceitua **dado pessoal** (informação relacionada à pessoa natural identificada ou identificável), **dado sensível** (em geral, aqueles que podem ser usados para causar dano ao titular, como dados sobre raça/etnia, religião, sexualidade, opinião política, genéticos e biométricos) e **dado anonimizado** (pessoais, relativos a um titular que não possa ser identificado).
- Uma empresa ou órgão público só poderá fazê-lo **se tiver o consentimento do titular** dos dados.
- O titular **pode retirar seu consentimento**, **pedir a exclusão ou a portabilidade** dos seus dados pessoais. Ele deve ser informado sobre por que um órgão público ou empresa está pedindo suas informações pessoais (princípio da finalidade), os quais devem ser limitados ao mínimo necessário para atingir o propósito informado (princípio da necessidade).
- A lei cobra que órgãos públicos organizem dados de forma que eles sejam "**interoperáveis**" e "**estruturados**", com o objetivo de torná-los padronizados e acessíveis.
- Qualquer empresa ou órgão público envolvido no tratamento de dados pessoais **deve ser responsabilizado em caso de violação à lei**. Em caso de vazamento ou qualquer outra falha de segurança que possa ter comprometido os dados pessoais sob sua responsabilidade**, o "órgão competente" deve ser comunicado** dentro de um prazo razoável.
- Multa diária de **até 2% do faturamento**, com limite de R$ 50 milhões
- Cria-se a Autoridade Nacional de Proteção de Dados, uma autarquia vinculada ao Ministério da Justiça que tem a obrigação de "zelar pela proteção dos dados pessoais", garantir o respeito à lei, fiscalizar e aplicar sanções e atender solicitações de titulares de dados sobre empresas e órgãos públicos.

ENQUANTO ISSO NO BRASIL

JURISTAS HOME BLOG FÓRUNS PARCEIROS CERTIFICAÇÃO DIGITAL JURISPRUDÊNCIAS

Direito da Tecnologia da Informação | Notícias

MPDF quer que Banco Inter pague indenização por vazamento de dados de clientes

Por **Juristas** - 01/08/2018 93 0

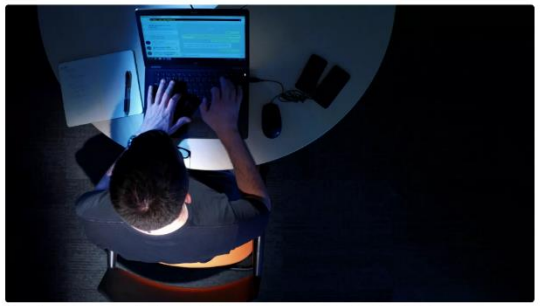
Banco Inter | Crédito: Banco Inter

O Ministério Público do Distrito Federal (MPDF) pediu a condenação do Banco Inter para o pagamento de R$ 10 milhões de indenização por danos morais coletivos. Segundo investigação do MPDF, o banco teria sido negligente com os dados de seus clientes, afirmando que o Inter não adotou as devidas providências para evitar o vazamento e roubo de dados de seus consumidores.

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 28/02/2018 05h25



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

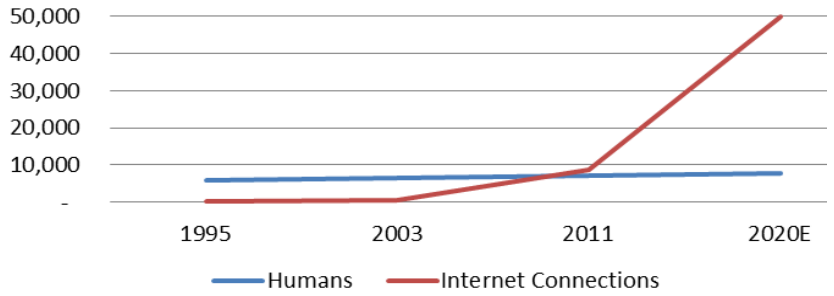
protiviti

INTERNET DAS COISAS - IOT

O número de dispositivos conectados à internet ultrapassou o número de seres humanos no planeta em 2011.

Em 2020, espera-se que os dispositivos conectados à internet cheguem a 50 bilhões.

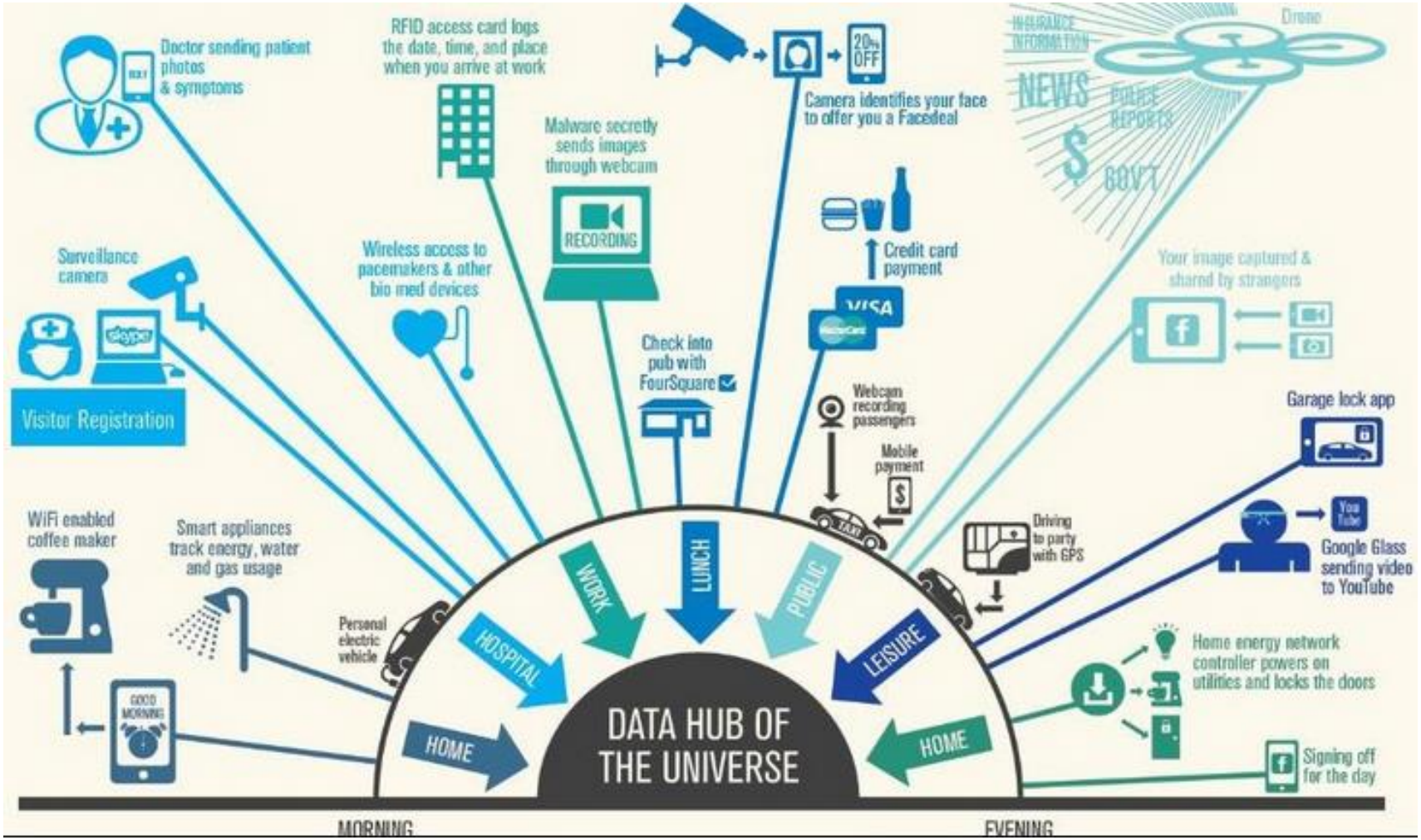
Seres Humanos versus Dispositivos Conectados à Internet



Graphic by Harbor Research

protiviti

EXTENSÃO DA INTERNET DAS COISAS



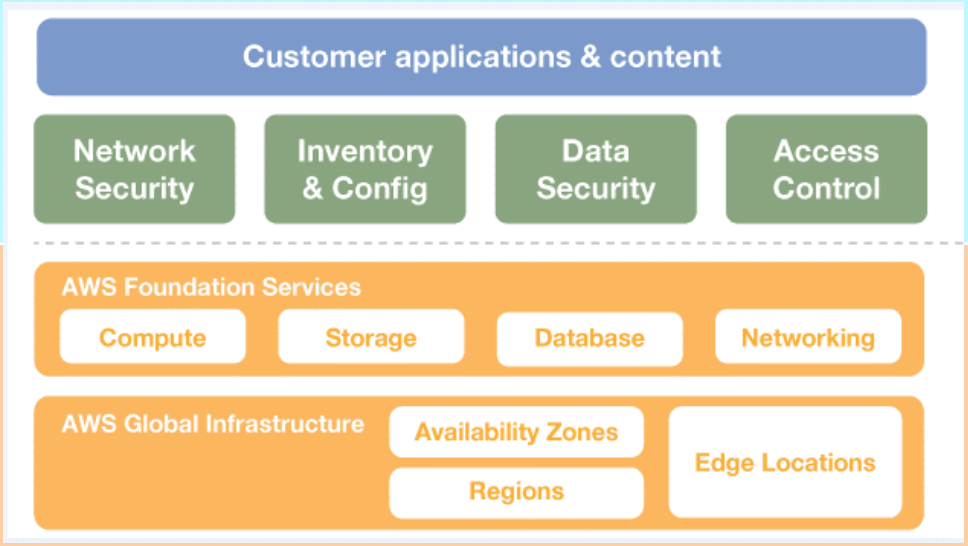
Fonte: http://www.privacyguidance.com/einfograph.html.

protiviti

CLOUD

Cliente

Modelo de provedor de Cloud (ex. AWS)



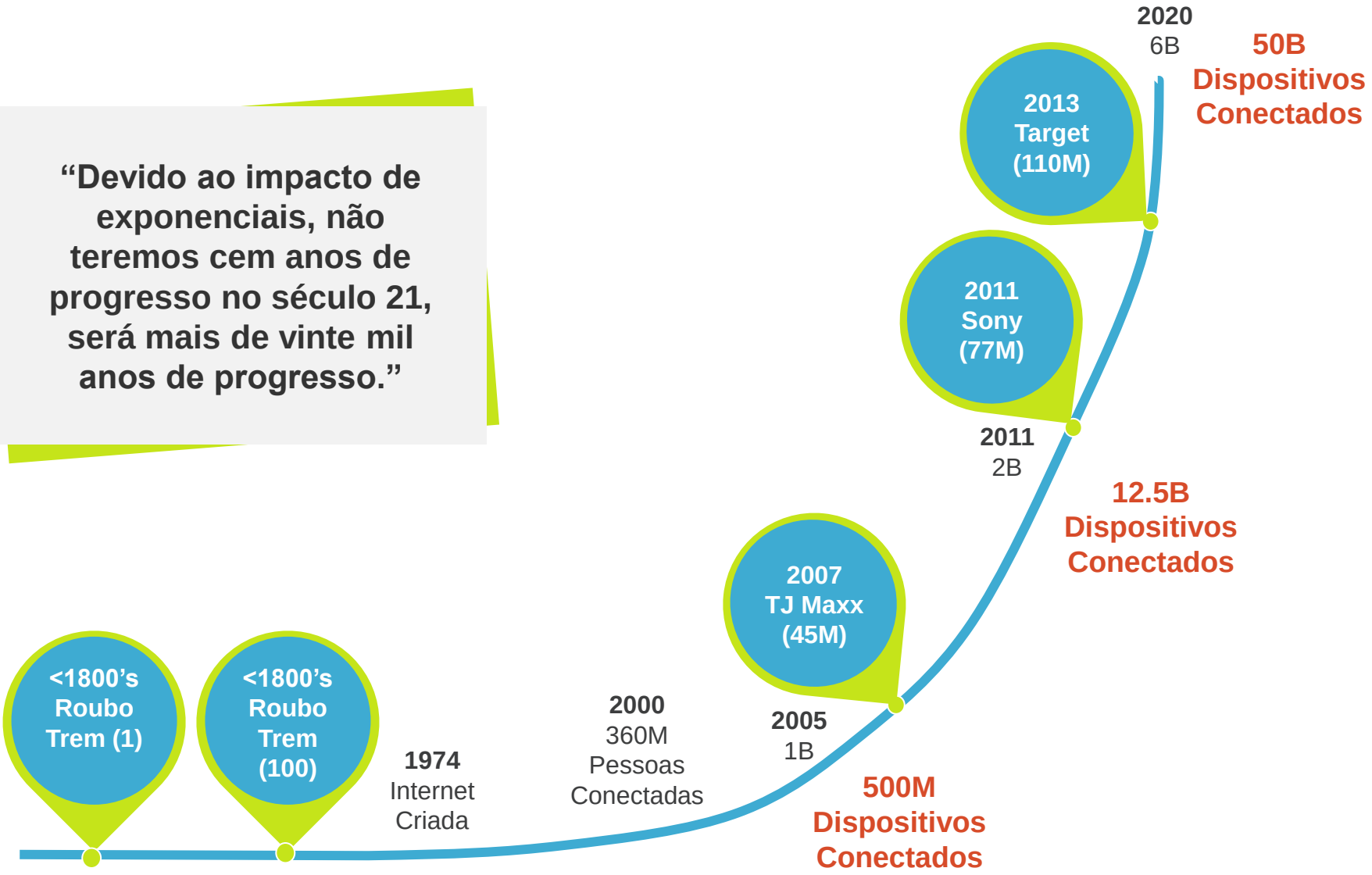
- Gerenciamento de acesso do usuário
- Uso de Conta Privilegiada e Gerenciamento de Chaves
- Registro e Monitoramento de Atividades
- Firewalls do sistema operacional, grupos de segurança, configuração de rede

Provedor

- Controles de Acesso Físico e Infraestrutura
- Instalações
- Desativação segura de hardware
- Segurança Ambiental
- Infraestrutura de virtualização e preocupações com disponibilidade

A ERA DOS INCIDENTES EXPONENCIAIS

“Devido ao impacto de exponenciais, não teremos cem anos de progresso no século 21, será mais de vinte mil anos de progresso.”



protiviti

INTERNET DAS COISAS: RISCOS

Fonte: Cisco

protiviti

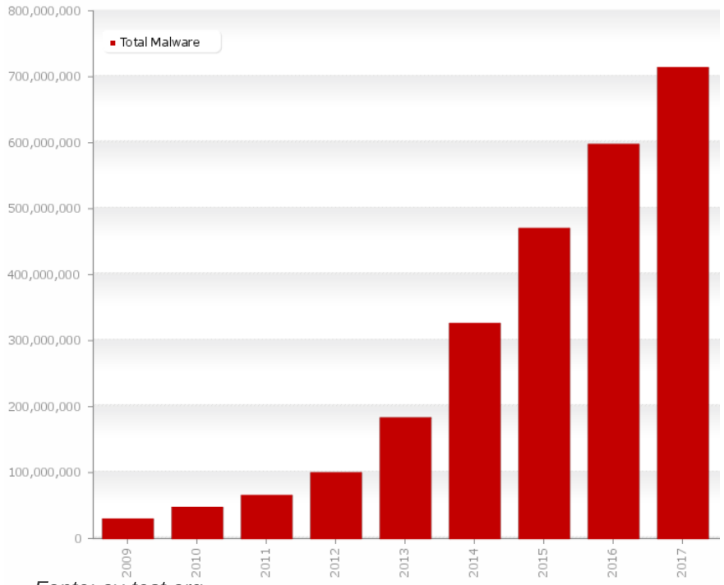
RISCOS CIBERNÉTICOS

MALWARE

MUNDO

x7

em 4 anos



Fonte: av-test.org,

CUSTOS DOS ATAQUES

Menos de 10% dos ataques são descobertos por meios internos.

2016	
US$ 4 million	*custo total do ataque*
US$ 158	*custo médio por registro atacado*
US$ 355	*... custo por registro para Healthcare*
US$ 172	*... custo por registro para o Varejo*
US$ 129	*... custo por registro para Transporte*
8 meses	*tempo médio desde a violação até a descoberta*
2.9%	*do faturamento comprometido por perda de negócios*
26%	*probabilidade de ataque nos próximos 24 meses*

Fonte: Ponemon Institute Cost of Data Breach Study

BRASIL

Prejuízos de **US$ 22 bilhões**

+62 milhões de brasileiros foram vítimas

Fonte: Norton Cyber Security Insights Report 2017

protiviti

CASOS NA UNIÃO EUROPÉIA

País/Lei	Data	Empresa	Multa	Razão
UK (ICO)	Jan 2013	Sony	250,000 GBP	Falha em impedir que dados pessoais de usuários do PlayStation sejam invadidos
UK (ICO)	Oct 2012	The Prudential	50,000 GBP	Misturando contas de dois clientes
UK (ICO)	May 2012	NHS Trust	325,000 GBP	Falha em impedir que dados pessoais confidenciais sejam vendidos no site de leilões da Internet
France (CNIL)	March 2011	Google	100,000 EUR	Coleta de dados de Wi-Fi e login / email durante suas operações do Street View
France (CNIL)	July 2011	Association Lexeek	10,000 EUR and injunction	Casos legais publicados on-line contendo nomes das partes
Spain (AEPD)	April 2007	Zeppelin Television	1,000,000 EUR	Incapacidade de proteger dados pessoais de 7000 requerentes do Big Brother
Netherlands (OPTA)	Dec 2011	DollarRevenue	1,000,000 EUR	Instalando o software adware / spyware em 22 milhões de computadores

Source: EU Case,

protiviti

GDPR – NOSSA EXPERIÊNCIA

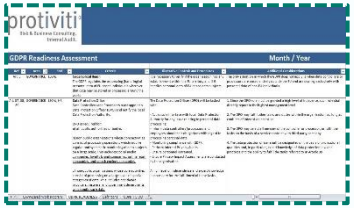
Atividades típicas de diversos projetos de GDPR

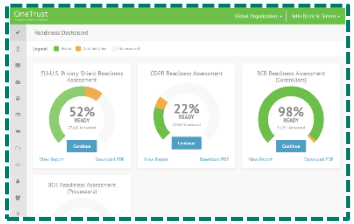
0 Descoberta e Planejamento

Inventário de fontes de dados com seu modelo de criticidade

1 Estado atual

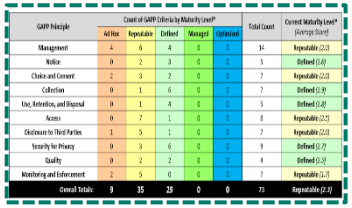
Análise do estado atual

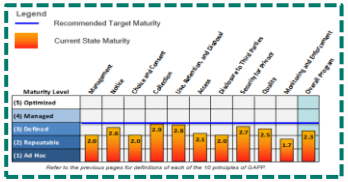




2 Análise de Gaps

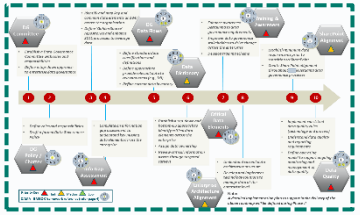
Resultados da análise





3 Desenho do plano

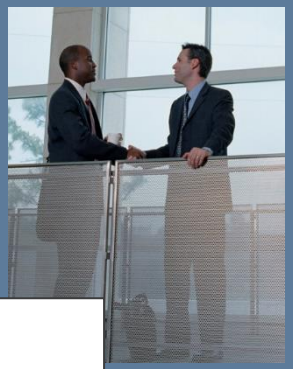
Roteiro de conformidade e relatório de suporte



protiviti

protiviti®
Risk & Business Consulting.
Internal Audit.

Obrigado!



Mauricio Fiss

protiviti®
Face the Future with Confidence

Face the Future with Confidence

Face the Future with Confidence

protiviti®