A importância da Segurança da Informação e os impactos da LGPD

Eliézer Zarpelão

Eliézer Zarpelão

Co-Fundador e Arquiteto de Software - ZarpSystem
Professor – UNAERP
Embaixador – Google Developer Group Campinas
Técnico em Informática - COTUCA / Unicamp
Graduação em Sistemas de Informação - ICMC / USP
Especialização em Eng. de Software - IC /Unicamp
Mestrado - IC / Unicamp (em curso)

Qual foi a última vez que você trocou a senha do seu e-mail?

_

95% dos brasileiros usam senhas fracas para proteção de dados.

Estamos seguros #sqn

23% Seu nome ou o nome de alguém da família

14% Seu aniversário

9% Palavras relacionadas ao seu hobby

8% O nome do seu animal de estimação

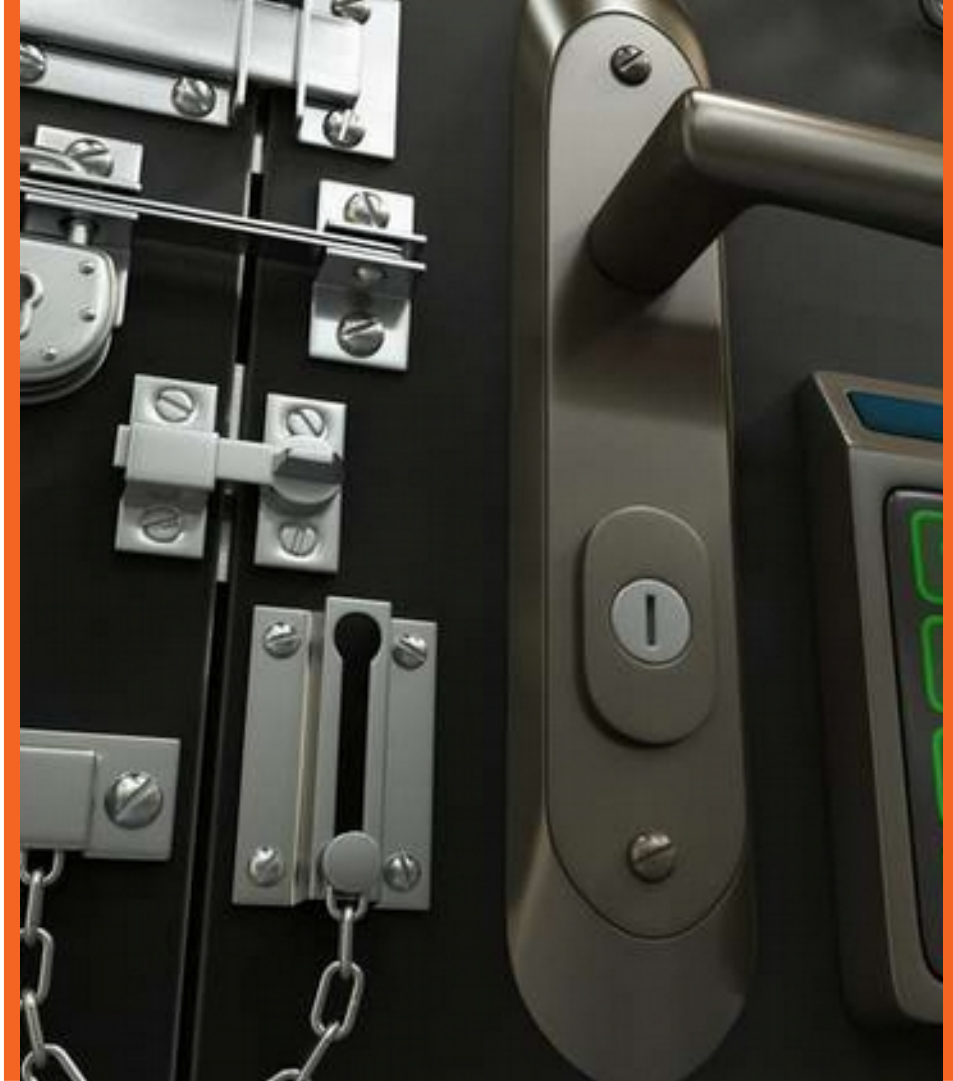
6% O nome do seu livro ou filme favorito

5% Nomes de celebridades

4% O nome do site, no qual usa a senha

3% Dados do endereço residencial

Fonte: Pesquisa AVAST



O que é Segurança da Informação?

DICS

Dado

Palavra
Imagem
Número

Informação

Organização
Processamento

Conhecimento

Idéia
Interpretação

Sabedoria

Aplicação
Contexto

Os prejuízos por incidentes envolvendo informações podem ser incalculáveis e até decretar o **fim de uma organização.**

Você nunca verá

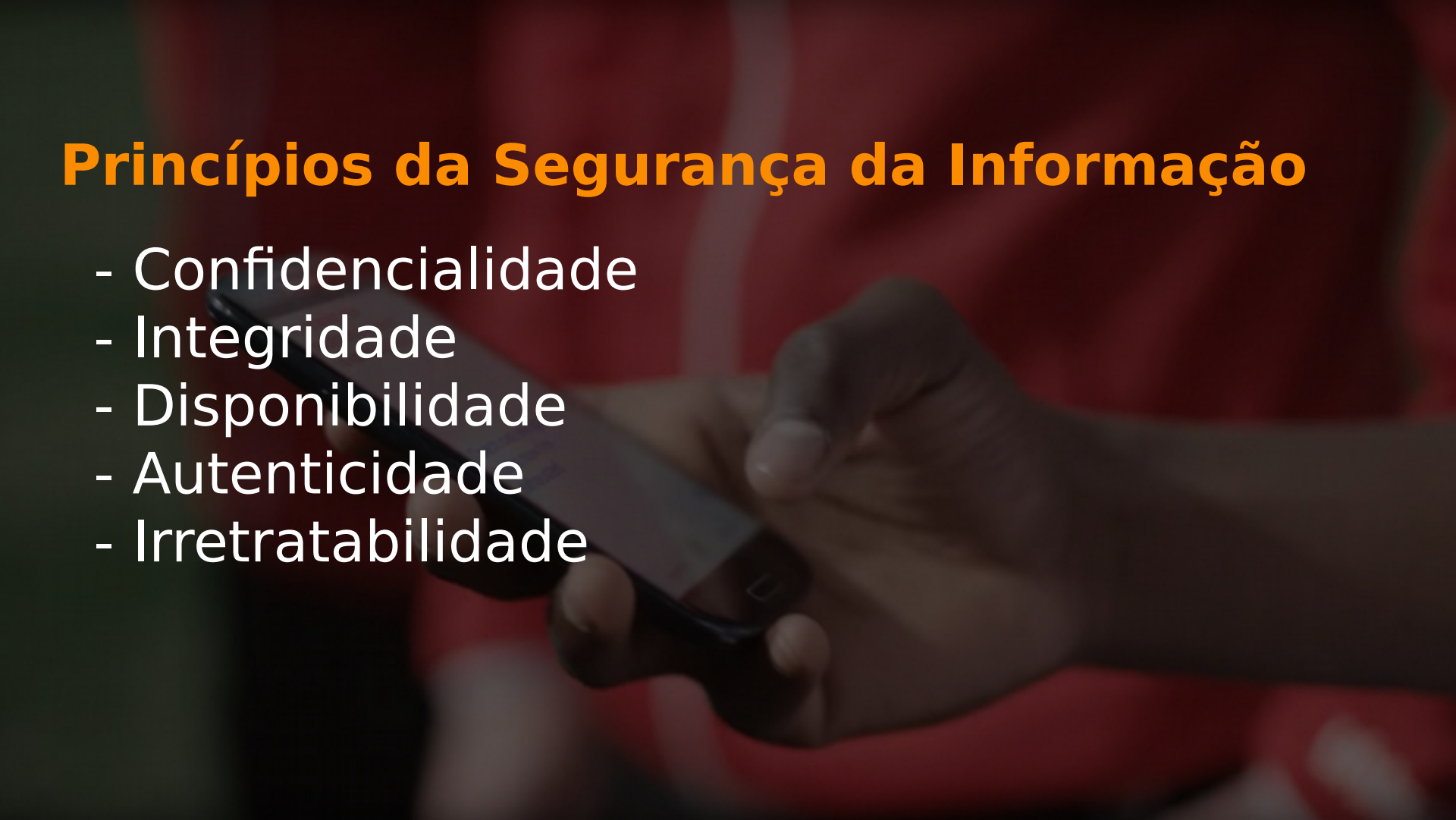
Roberto Carlos de bermuda

Cabeça de bacalhau

Entrevistado do Ibope

Sistema 100% seguro


CAN'T GET HACKED
IF YOU DON'T USE A COMPUTER



Princípios da Segurança da Informação

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Irretratabilidade

Confidencialidade

É uma característica da informação que diz respeito ao **direito de acesso**.

Garantir que a informação esteja **acessível** apenas para pessoas/ organizações que tenham **permissão de acesso**, prevenindo, assim, **revelação não autorizada**.

Integridade

É uma característica da informação que diz respeito à sua **exatidão**.

Garantir que a informação seja alterada somente por pessoas **autorizadas** e em situações que efetivamente demandem a **alteração legítima**.

Autenticidade

Diz respeito à **certeza da origem** da informação.

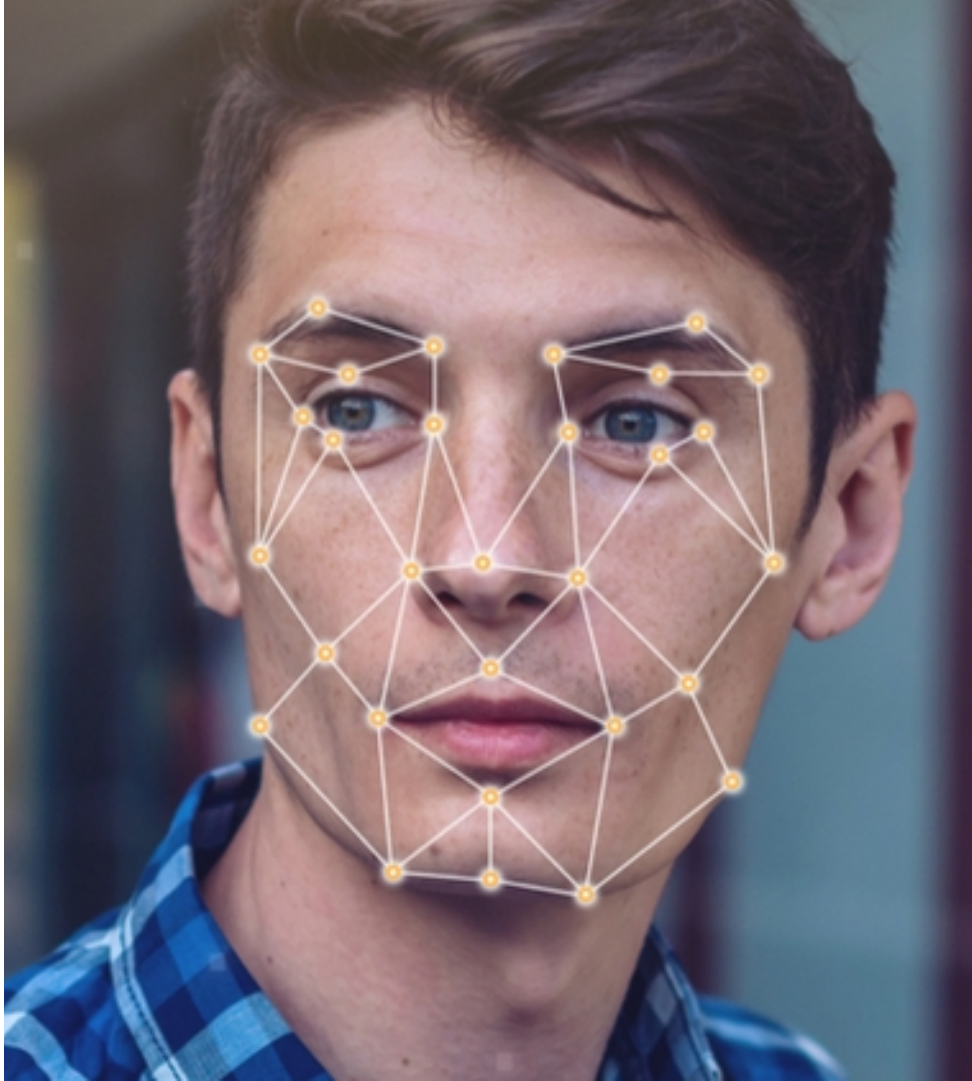
Garantir que a informação **provem** da fonte anunciada e que não foi alvo de **mutação** ao longo de sua transmissão


SO YOU'RE SAYING I
MUST OPEN AN ATTACHMENT
FOR MY CASH REFUND ?
imgflip.com

Irretratabilidade

Diz respeito à garantia de que o autor de determinada ação **não possa negar** tal ação.

Garantir meios que identifique inequivocamente o autor de uma ação.



Disponibilidade

Garantir que a informação esteja **disponível**, sempre que necessário, aos usuários e/ou sistemas associados que tenham direito de acesso a ela.

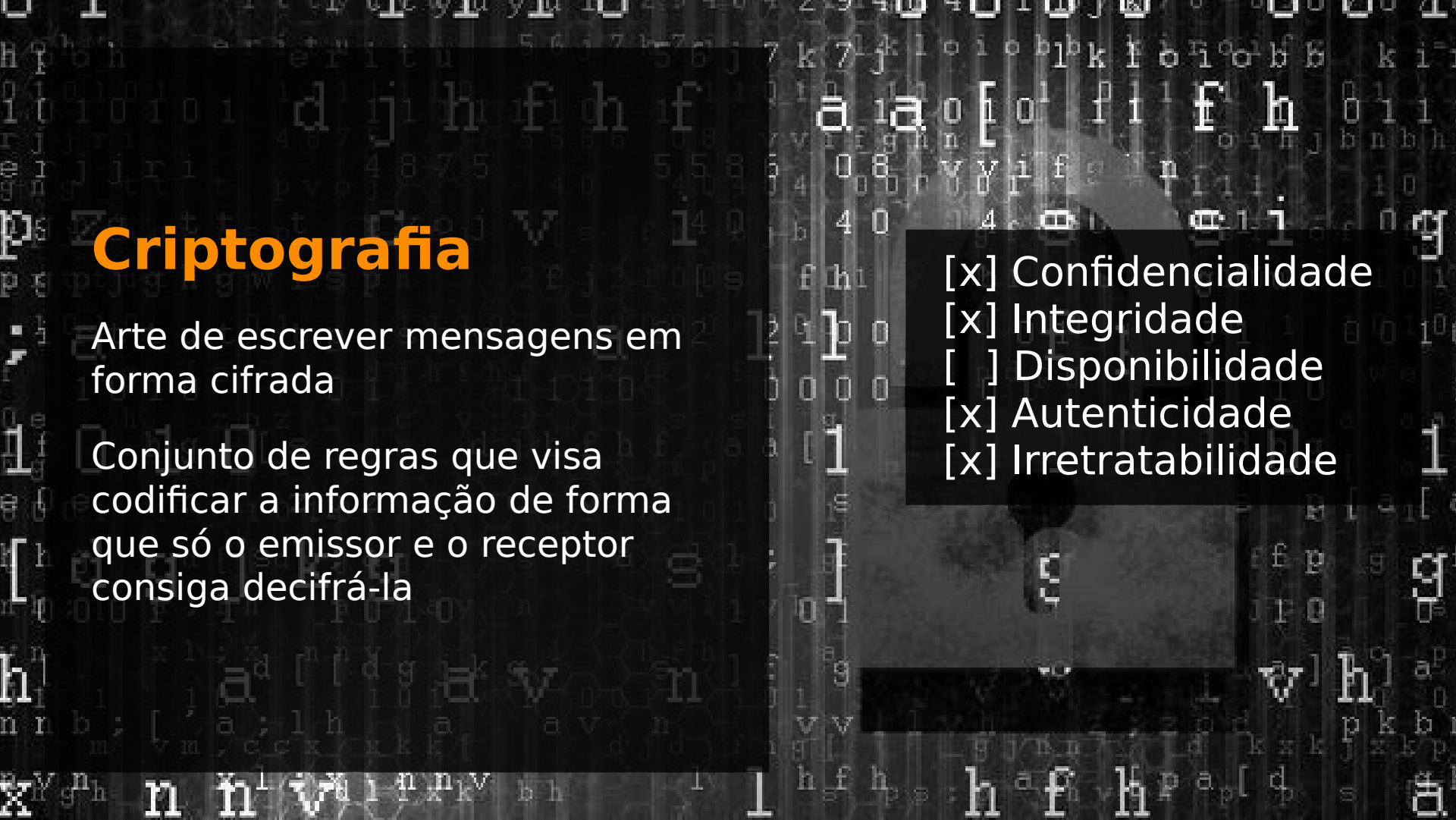
Como podemos garantir a segurança da informação?

(ou no mínimo mitigar os riscos)

Criptografia

Arte de escrever mensagens em forma cifrada

Conjunto de regras que visa codificar a informação de forma que só o emissor e o receptor consiga decifrá-la



[x] Confidencialidade
[x] Integridade
[ ] Disponibilidade
[x] Autenticidade
[x] Irretratabilidade

Tipos de Chaves

Simétricas

A mesma chave é utilizada tanto pelo emissor quanto por quem recebe a informação.

Não é recomendado uso para informações sensíveis

Assimétricas

Uma chave privada e outra pública.
Pública: chave de codificação e enviada a quem for lhe mandar informações.
Privada: chave secreta para a decodificação.


INFORMATION SECURITY IS
EVERYONE'S RESPONSIBILITY
imgflip.com

Governo de São Paulo confirma vazamento de dados de inscritos no ProAC

Dados de mais de 28 mil candidatos do programa de cultura de São Paulo são expostos na Internet

Por Beatriz Cardoso, da Redação

25/10/2019 10h22 · Atualizado há 57 minutos

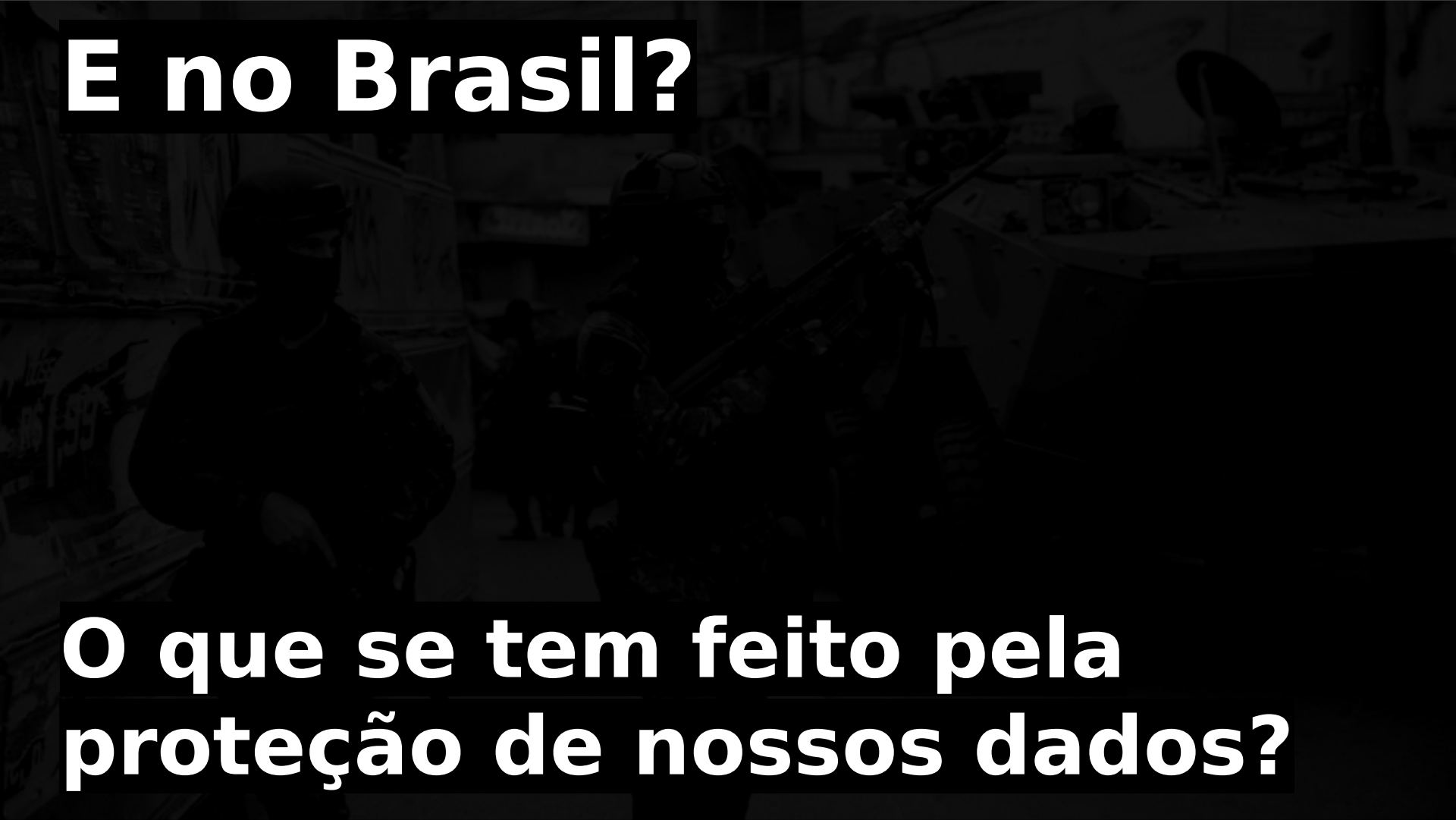
InfoMoney

Vazamento

Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros

Falha de segurança dava acesso ao banco de dados de todas as unidades do Detran do país. Todos os brasileiros com CNH tiveram seus dados vazados

E no Brasil?



O que se tem feito pela proteção de nossos dados?

Lei Geral de Proteção de Dados Pessoais

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Principais pontos da LGPD

- Aplicada a **todos** os setores da economia;
- Possui aplicação **extraterritorial**, ou seja, toda empresa que tiver negócios no país deve se adequar a ela;
- Necessário o **consentimento** do usuário para coletar informações pessoais;
- Os titulares podem retificar, cancelar ou até solicitar a exclusão desses dados;
- Criação da Autoridade Nacional de Proteção aos Dados (**ANPD**);
- **Notificação** obrigatória de qualquer incidente;
- Inspirada na **GDPR** (UE)


Cambridge
Analytica
fakebook

FACEBOOK PAGA A MAIOR MULTA JÁ REGISTRADA POR VIOLAÇÃO DE DADOS PESSOAIS

DA REDAÇÃO 24 DE JULHO DE 2019

Empresa vai pagar US$ 5 bilhões. Terá de criar estrutura executiva especializada em privacidade e independente, que não obedecerá ao CEO e fundador, Mark Zuckerberg

CAMBRIDGE ANALYTICA

Um exemplo de compartilhamento de dados pessoais aconteceu com a consultoria Cambridge Analytica. A FTC também processou a empresa, seu antigo CEO e o desenvolvedor. A acusação é de que eles usavam táticas enganosas para coletar informação pessoal de milhões de usuários do Facebook para traçar seus perfis de orientação política e impactá-los com propaganda eleitoral.

http://www.telesintese.com.br/facebook-paga-a-maior-multa-ja-registrada-por-violacao-de-dados-pessoais/

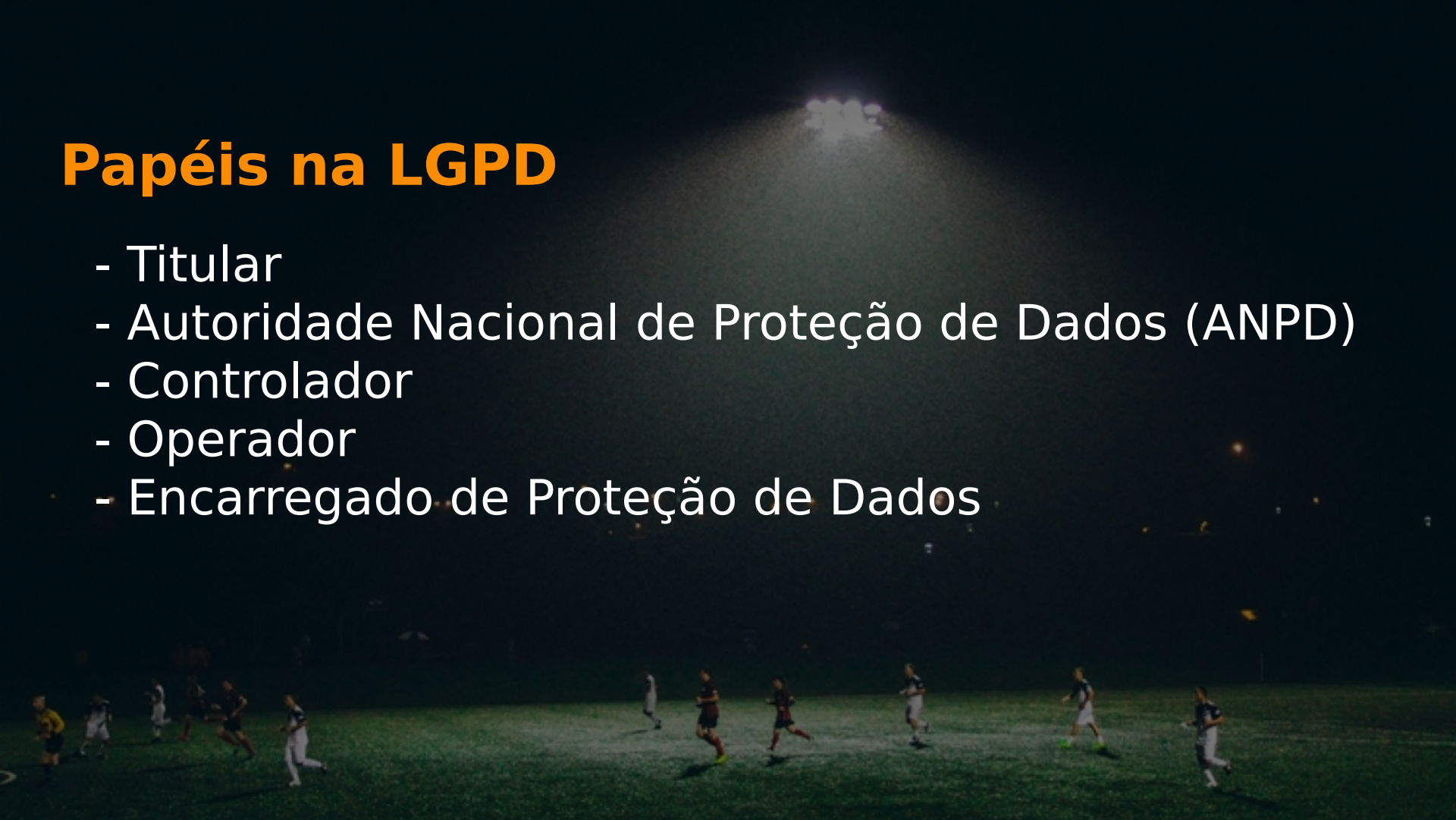
O que são dados pessoais?

Dados pessoais

Qualquer informação relacionada a pessoa natural identificada ou identificável

Dados Pessoais Sensíveis

- Opinião Política
- Origem Racial
- Origem Étnica
- Dados genéticos
- Convicção Religiosa
- Dados Biomédicos
- Dado referente à saúde ou à vida sexual
- Filiação a sindicato ou a organização de caráter religioso, filosófico ou político



Papéis na LGPD

- Titular
- Autoridade Nacional de Proteção de Dados (ANPD)
- Controlador
- Operador
- Encarregado de Proteção de Dados

Titular

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Autoridade Nacional de Proteção de Dados

- Órgão Federal
- Zelar pela proteção dos dados pessoais
- Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade
- Aplicar sanções em caso de tratamento de dados feito de forma irregularração legítima.

Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Conhecimentos em Segurança da informação, tecnologia e compliance.

Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Encarregado de Proteção de Dados

Pessoa indicada pelo controlador e operador para atuar como **canal de comunicação** entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Data Protection Officer

https://www.infranewstelecom.com.br/controlador-operador-encarregado-quem-e-quem-na-lgpd/

Ciclo de vida dos dados

https://www.xpositum.com.br/ciclo-de-vida-dos-dados-e-lgp

O que a LGPD entende por tratamento de dados?

Tratamento de Dados

- Coleta
- Produção
- Recepção
- Classificação
- Utilização
- Acesso
- Reprodução
- Transmissão
- Distribuição
- Processamento
- Arquivamento
- Armazenamento
- Eliminação
- Avaliação ou controle da informação
- Modificação
- Comunicação
- Transferência
- Difusão
- Extração

10 PRINCÍPIOS DO TRATAMENTO DE DADOS – Art 7º

Finalidade	Adequação	Necessidade	Livre Acesso	Qualidade dos dados
Transparência	Segurança	Prevenção	Não Discriminação	Responsabilização e Prestação de Contas

Incidentes de Segurança (Data Breach)

Quando comunicar?
- Incidente de segurança que possa acarretar risco ou dano relevante aos Titulares
- Em prazo razoável
- À ANPD e aos titulares afetados

Conteúdo mínimo da comunicação:
- Descrição da natureza dos dados
- Informações sobre os titulares envolvidos
- Medidas técnicas e de segurança de proteção adotadas
- Riscos relacionados ao incidente
- Motivo da demora caso comunicação não imediata
- Medidas adotadas para reverter ou mitigar

Sanções

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

https://idec.org.br/noticia/veja-10-coisas-que-mudarao-na-sua-vida-com-lei-de-dados-pessoais

O que muda na sua vida?

- O fim dos “termos de uso que ninguém lê”
- Mais controle do usuário sobre seus próprios dados
- Mais controle sobre como farmácias usam seu CPF e dados de saúde
- Mecanismos claros em caso de vazamentos de dados pessoais
- Suas emoções não poderão ser coletadas e vendidas em espaços abertos
- Portabilidade de dados pessoais
- Condomínios residenciais precisarão discutir sobre reconhecimento da digital para controlar a entrada no prédio
- Sem obscuridades: os consumidores terão livre acesso a sua pontuação de crédito, como ela foi calculada e quais dados foram utilizados
- Fim da bonança dos testes de internet
- Diferenciação de preços em compra online somente com consentimento do consumidor

https://idec.org.br/noticia/veja-10-coisas-que-mudarao-na-sua-vida-com-lei-de-dados-pessoais

O que muda na sua vida [+T.I.]

Códigos carregam propostas políticas
- Estabelecem permissões e restrições
- Logo regulam o [ciber]espaço

Privacy by Design (PbD)
- Construir a cultura protetiva à privacidade no desenho dos produtos
- Ex: é adequado que aplicativos de lanterna coletem dados de geolocalização?

Machine Learning

Atualizar seus termos de uso
- Deixar claro para o usuário o tipo de informação a ser coletada dele, bem como a finalidade desse uso

Anonimizar os dados obtidos dos usuários
- Dado deixa de ser Pessoal

Utilização de bases de dados públicas

Atenção com troca de dados entre empresas e parceiras

FATO ou FAKE???

- A Lei Geral de Proteção de Dados não terá eficácia real
  - **FAKE!** ANPD irá zelar pelo cumprimento da lei
- A Lei Geral de Proteção de Dados revogará as outras normas envolvendo proteção de dados em vigor no Brasil
  - **FAKE!** Continuam valendo Marco Civil da Internet, a Lei do Cadastro Positivo, o Código de Defesa do Consumidor, dentre outras.
- A LGDP abrange somente os dados de pessoas naturais
  - **FATO!**
- A LGPD somente protege os dados pessoais que circulam no meio digital
  - **FAKE!** Visa a proteção tantos dos dados mantidos em meios físicos quanto digitais

https://www.marinho.adv.br/post/29-10-mitos-e-verdades-sobre-a-lei-geral-de-protecao-de-dados

FATO ou FAKE???

- A implementação desta lei na minha empresa será simples e rápida
  - **FAKE ^ 1024**
- Em caso de incidentes envolvendo dados pessoais, as únicas penalidades que posso receber são as administrativas
  - **FAKE!** Também poderão ser alvos de ações judiciais demandadas pelos titulares dos dados pessoais, em razão de possíveis danos morais ou materiais sofridos
- Advertências e multa de até 2% do faturamento da pessoa jurídica, limitada a R$ 50 milhões por infração, são algumas das sanções administrativas que a Autoridade nacional poderá aplicar em caso de descumprimento dos dispositivos da lei
  - **FATO!**

https://www.marinho.adv.br/post/29-10-mitos-e-verdades-sobre-a-lei-geral-de-protecao-de-dados

FATO ou FAKE???

- Na Europa, diversas multas já foram aplicadas pelo fato das empresas não estarem em compliance com a lei
  - **FATO!**
- Minha empresa é de pequeno porte e por este motivo não preciso me adequar
  - **FAKE!** Não importa o porte da empresa! Agravante: Afetará compartilhamento de dados
- Um documento afirmando que a organização está em compliance com a LGPD será suficiente para afastar qualquer penalidade decorrente da sua violação
  - **FAKE!** Mudança de cultura + Engajamento!

https://www.marinho.adv.br/post/29-10-mitos-e-verdades-sobre-a-lei-geral-de-protecao-de-dados

Mantenha-se informado!!!

@podcastdt – Direito e Tecnologia
https://podtail.com/pt-BR/podcast/direito-e-tecnologia/

Escola Virtual
https://www.escolavirtual.gov.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)
https://www.cert.br/

Obrigado!!!!

ezarpelao@unaerp.br

eliezer.zarpelao@gmail.com

https://www.linkedin.com/in/eliezerzarpelao/