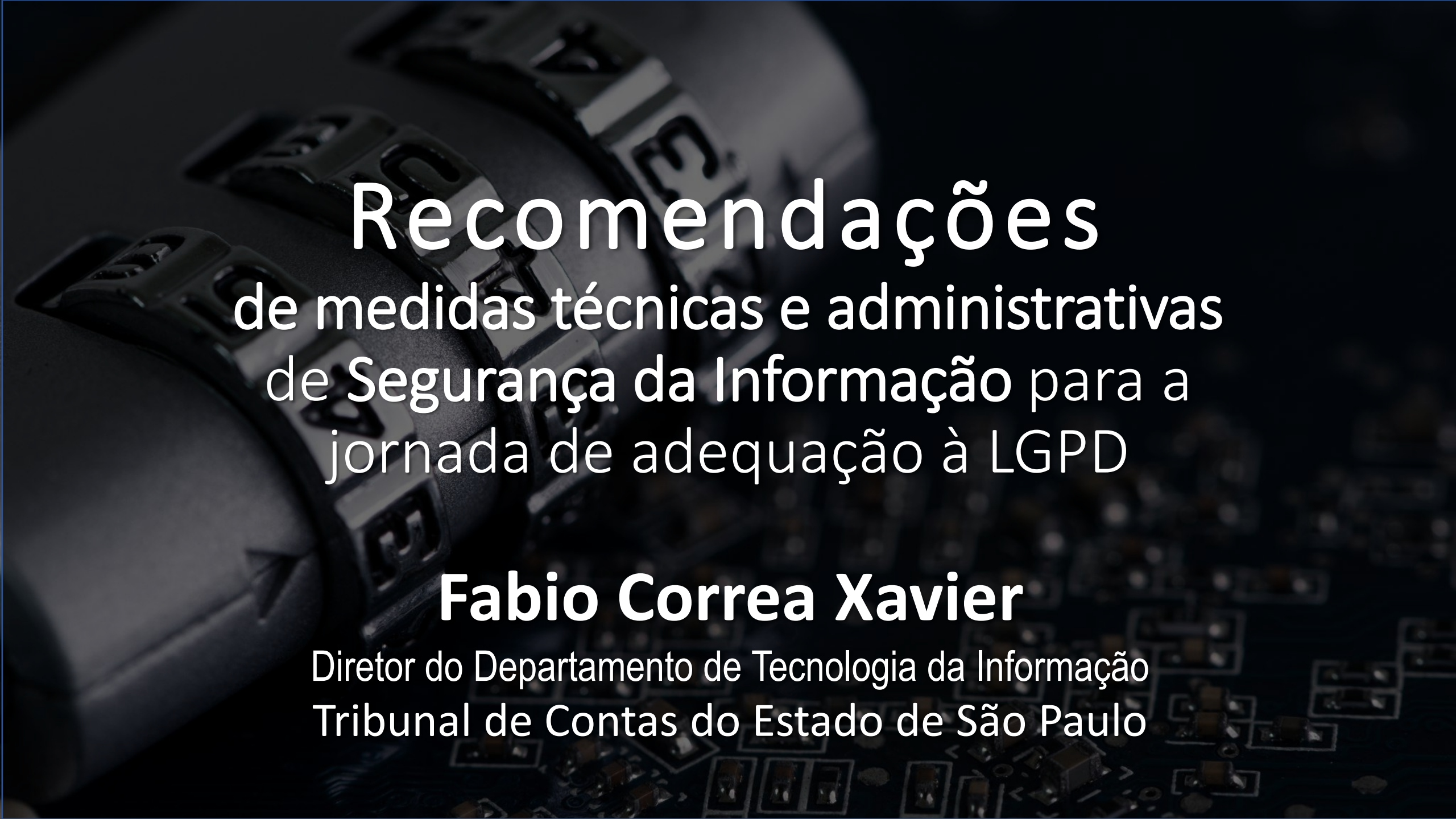


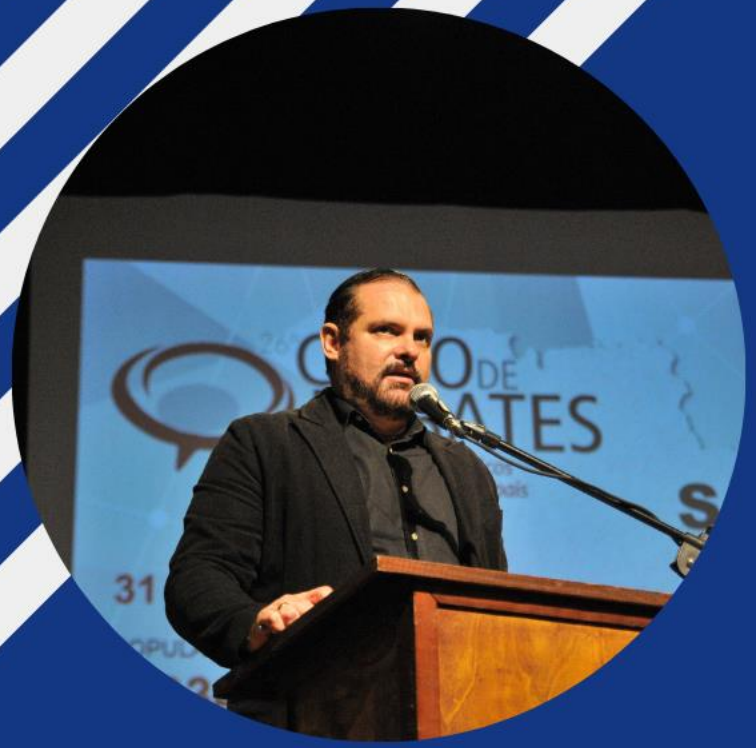
Recomendações

de medidas técnicas e administrativas de **Segurança da Informação** para a jornada de adequação à LGPD

Fabio Correa Xavier

Diretor do Departamento de Tecnologia da Informação

Tribunal de Contas do Estado de São Paulo



Fábio Correa Xavier

CIO do TCESP | Professor
Colunista MIT Technology Review Brasil
Mestre em Ciência da Computação

fabio@tce.sp.gov.br
https://www.linkedin.com/in/fabiocorreaxavier
@fabiocx
fabioxavier.com.br

+30 ANOS

EXPERIÊNCIA PROFISSIONAL
EM GESTÃO, GOVERNANÇA E TECNOLOGIA DA INFORMAÇÃO

MIT Technology Review — Publicado por TEC

COLUNISTA MIT TECHNOLOGY REVIEW
mittechreview.com.br/author/fabio-xavier/

JOTA

ARTIGOS PARA O PORTAL JOTA
www.jota.info/autor/fabio-correa-xavier

Migalhas

ARTIGOS PARA O PORTAL MIGALHAS
www.migalhas.com.br/autor/fabio-correa-xavier


1 ataque a cada 41 dias
STF
SUPREMO
TRIBUNAL FEDERAL
STJ
SUPERIOR
TRIBUNAL DE JUSTIÇA
JFPE
JUSTIÇA FEDERAL
EM PERNAMBUCO
TRF
1ª REGIÃO
JUSTIÇA
FEDERAL
TRF3
TJRS
CÂMARA MUNICIPAL
DE TERESINA/PI
anp
Agência Nacional
TJDFT
Prefeitura de
Porto Alegre
TCEPR
MINISTÉRIO
DA SAÚDE
Somos todos
GOIÁS

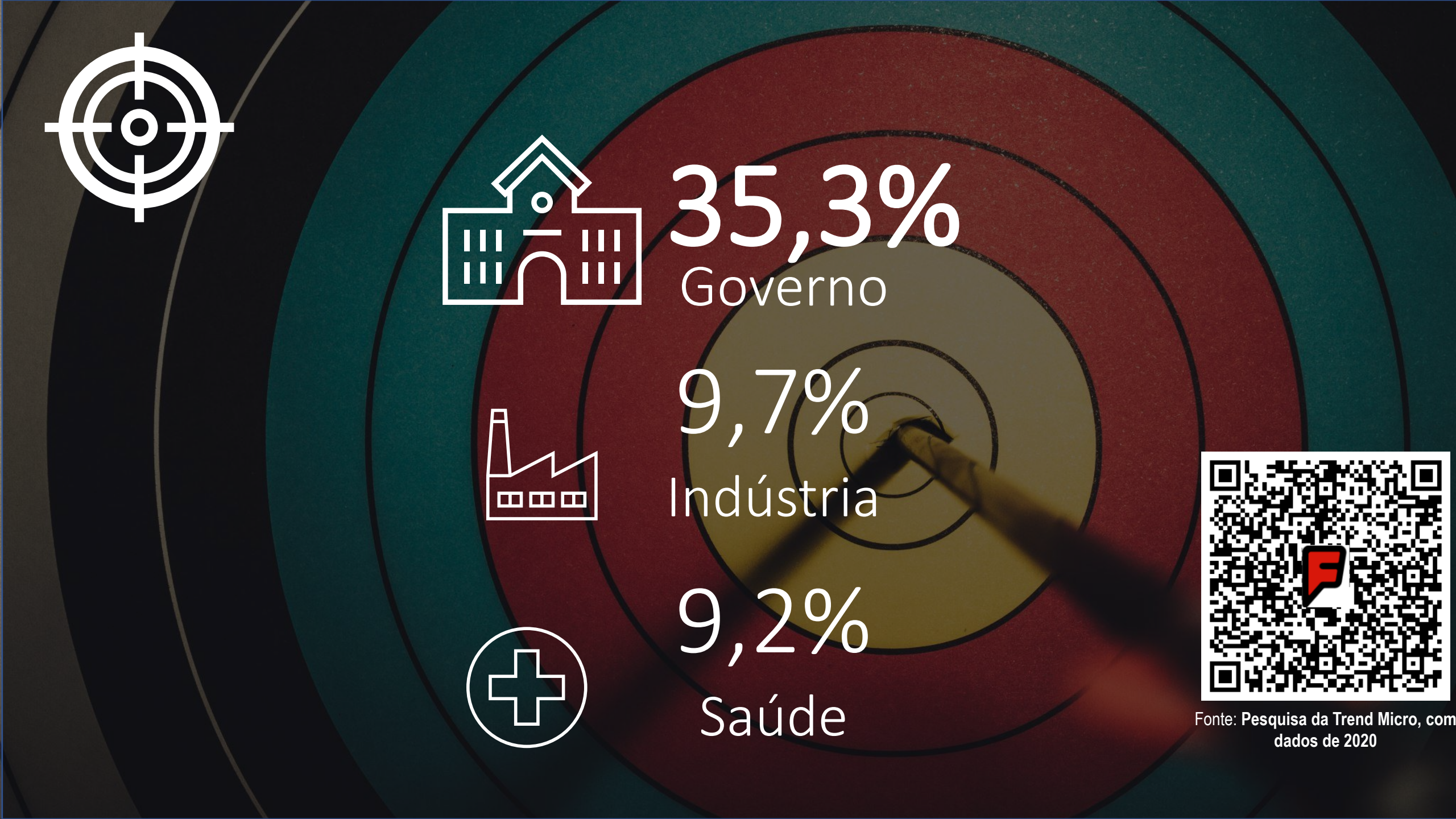
Em 2021

US$ 6 trilhões

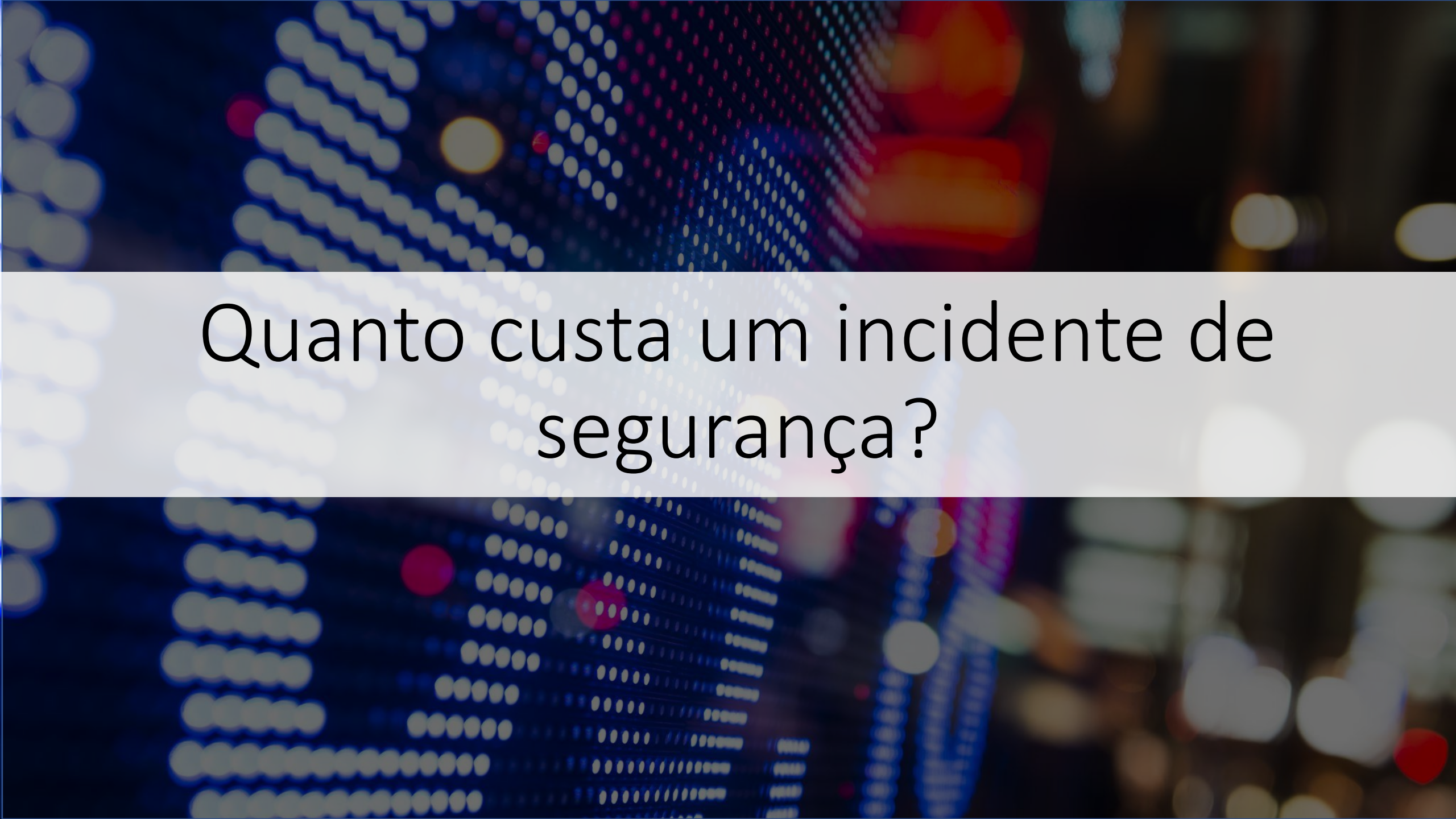
Prejuízo global com ataques cibernéticos

Fonte: Consultoria Roland Berger

https://bit.ly/3ucPkSf



Fonte: **Pesquisa da Trend Micro, com dados de 2020**



Quanto custa um incidente de segurança?

Custo médio por país

US$ 4,35 milhões
Média mundial (4,24)

US$ 9,44 milhões
USA (9,05)

US$ 1,38 milhões
Brasil (1,08)

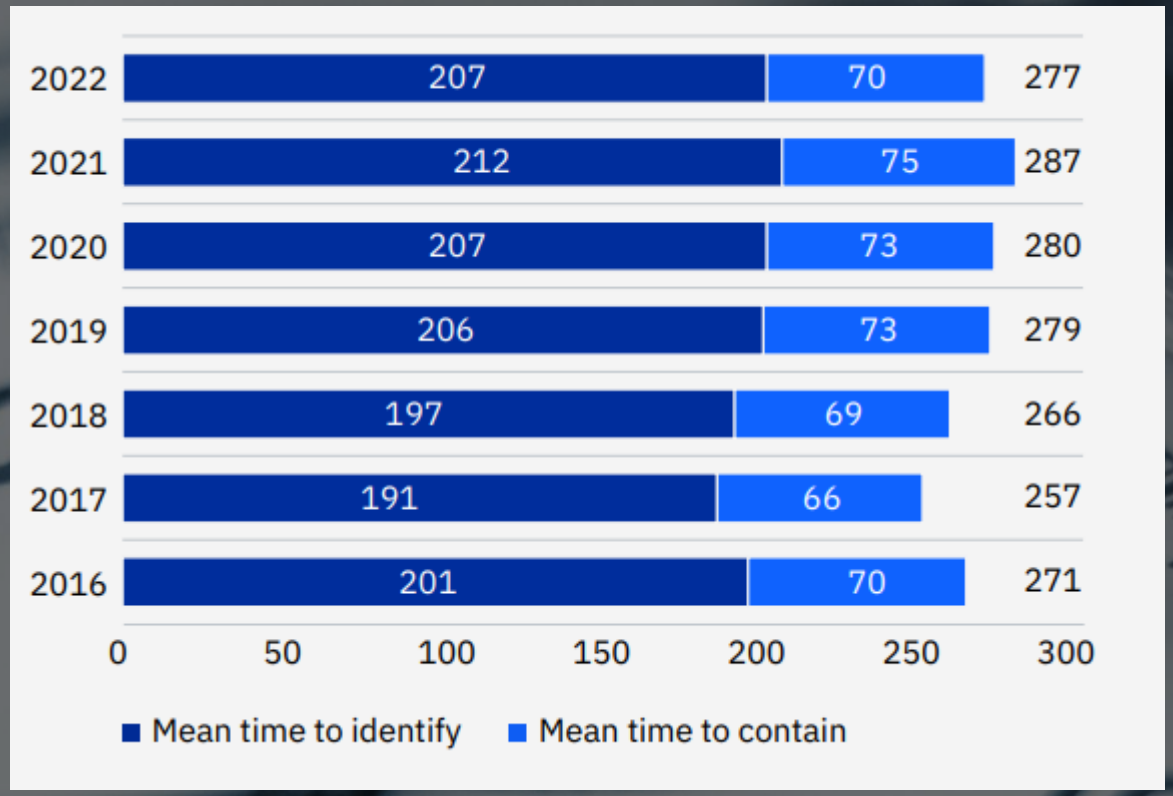
Custo médio por setor

US$ 10,10 milhões
Saúde (9,23)

US$ 5,97 milhões
Financeiro (5,72)

US$ 2,07 milhões
Governo (1,93)

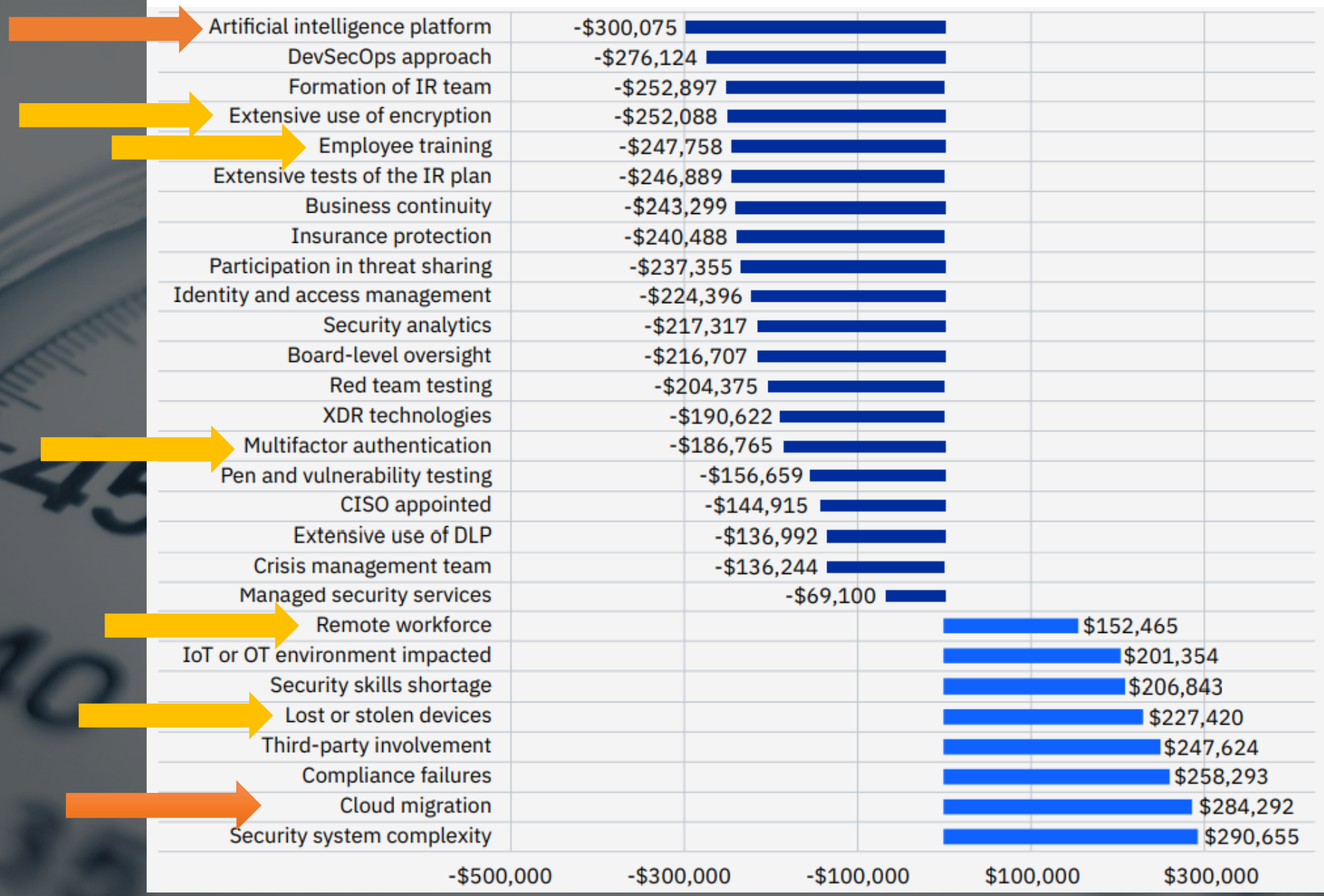
Tempo médio para identificar e mitigar incidentes



Tempo é dinheiro!

+200 dias => + US$ 1,12 milhões

Fatores chave que impactam o custo médio de um incidente



Atividades relacionadas à identificação e mitigação de um incidente de segurança

(i)

Detecção e escalonamento

- atividades forenses e de investigação
- serviços de avaliação e auditoria
- gerenciamento de crise e
- comunicação aos executivos e conselhos das organizações

(ii)

Negócios perdidos

- perda de receita em função da indisponibilidade dos sistemas
- custo da perda de clientes e de não aquisição de novos clientes (leads)

40%
custo

(iii)

Notificação

- atividades de notificação do incidente à autoridades e titulares dos dados

(iv)

Ações pós-incidente

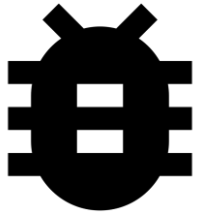
- reparação do incidente junto a autoridades de regulação e titulares
- despesas legais
- multas regulatórias
- emissão de novos cartões
- descontos em produtos
- recuperação de imagem

Fonte: *Cost of a Data Breach Report* 2022, Ponemon Institute

Causas dos incidentes de segurança

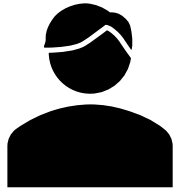
Ataques Maliciosos

52% no geral
47% no Brasil



Falhas de Sistemas

25% no geral
28% no Brasil



Erro Humano

23% no geral
25% no Brasil

Fonte: *Cost of a Data Breach Report* 2020, Ponemon Institute
https://bit.ly/39ErsOc

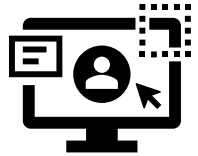
Principais vetores de ataques

E-mail *phishing*

E-mails falsos com o objetivo de roubar credenciais

Protocolo RDP

Protocolo Remote Desktop (RDP) é aquele que permite o acesso remoto a computadores por meio da Internet e que ficou muito comum em tempos de pandemia



Vulnerabilidades de softwares

Especialmente de sistemas operacionais, que permitem acesso ao computador da vítima para espalhar o *ransomware*.

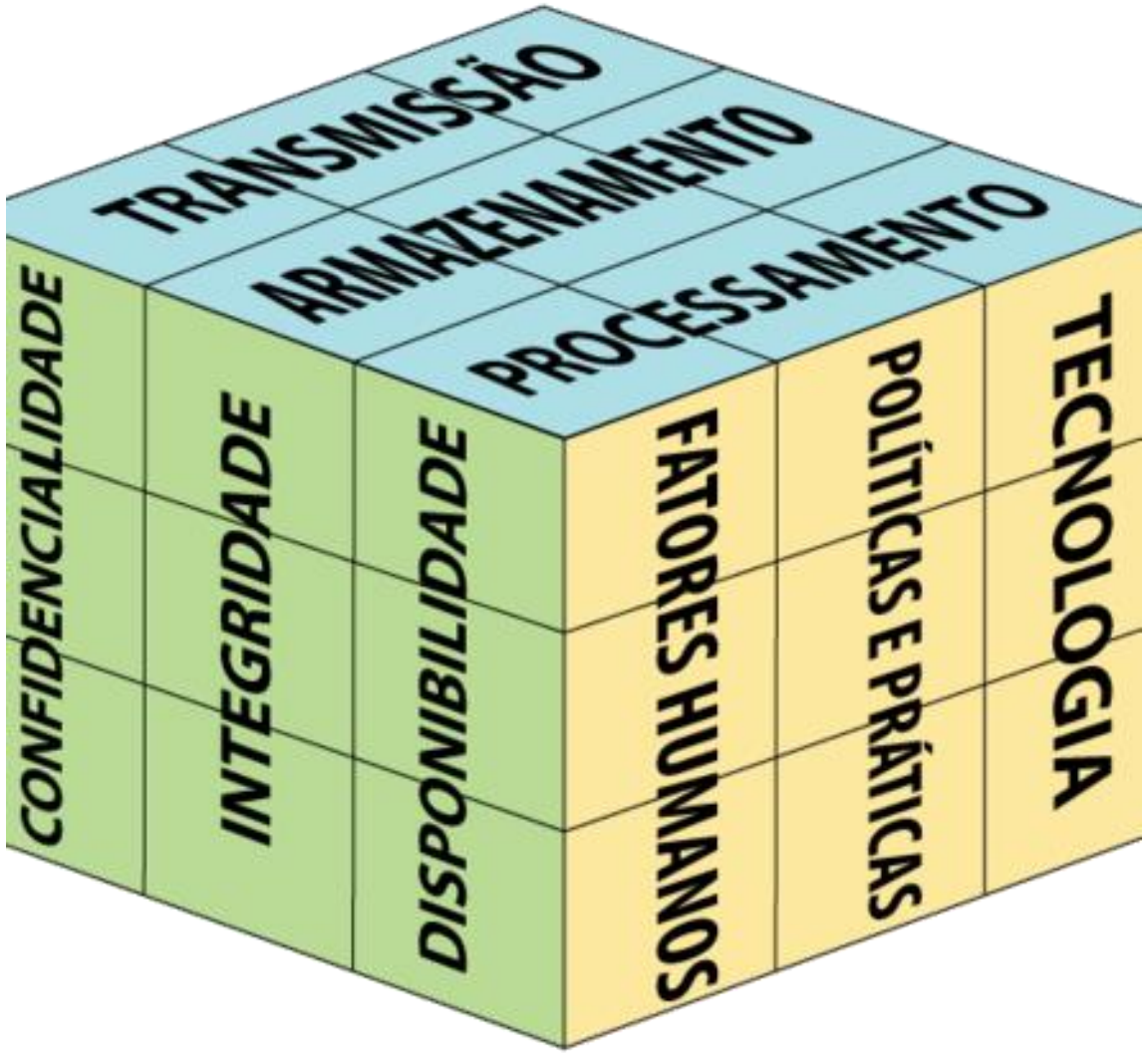
Fonte: *o IC3[10] (Internet Crime Complaint Center), ligado ao FBI, em meu artigo "***Ransomware: pagar ou não pagar, eis a questão"** https://bit.ly/3odpsF0

O que podemos fazer?

Cubo da Segurança de Cibernética

John McCumber, um especialista em segurança cibernética, desenvolveu uma estrutura chamada Cubo McCumber ou o cubo de segurança cibernética.

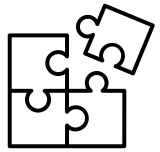
Esse cubo é usado para gerenciar a proteção de redes, domínios e da Internet.



Pilares da Segurança da Informação - CID

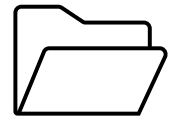
Confidencialidade

A propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.



Integridade

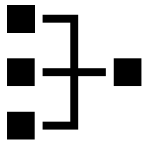
A propriedade de salvaguarda na exatidão e completeza de ativos, garante que a informação não sofra alteração indevida.



Disponibilidade

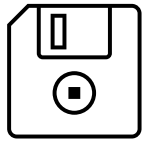
A propriedade de estar acessível e utilizável quando demandada por uma entidade autorizada.

Estado da Informação



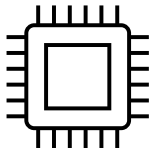
Transmissão

Dados sendo enviados de um dispositivo para outro



Armazenamento

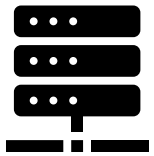
Dados em repouso, que estão em um dispositivo de armazenamento, sem utilização por usuários ou processos



Processamento

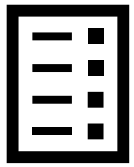
Dados sendo trabalhados durante a captação, cálculo/processamento ou saída

Contramedidas



Tecnologia

Tecnologias empregadas na segurança da informação



Políticas e Práticas

Processos, procedimentos e políticas que definem as boas práticas na realização de atividades, considerando a segurança da informação

Fator Humano

Conscientização e treinamento das pessoas, para que seja criada uma cultura de segurança da informação

TCESP
Tribunal de Contas
do Estado de São Paulo

Como minimizar os riscos de se tornar mais um refém virtual?

Boas práticas em relação às contramedidas

TCESP Tribunal de Contas do Estado de São Paulo

Tecnologia

Tecnologias empregadas na segurança da informação

1. **Manter e testar cópias de segurança** – offline – atualizadas de dados, sistemas e configurações e, claro, testar periodicamente essas cópias de segurança

2. Utilizar **autenticação multifator**

3. Manter **sistemas atualizados**, com últimos *patches* de correção e segurança aplicados

4. Manter **soluções de segurança adequadas e atualizadas**, de acordo com um bom plano de avaliação de riscos

5. Manter, revisar e executar periodicamente o **plano de resposta a incidentes e de continuidade de negócios**

Fonte: Artigo "**Ransomware: pagar ou não pagar, eis a questão"** https://bit.ly/3odpsF0

Boas práticas em relação às políticas

Políticas e Práticas

Processos, procedimentos e políticas que definem as boas práticas na realização de atividades, considerando a segurança da informação

1. Considerar a contratação de um **seguro de proteção** para incidentes de segurança e interrupção de negócios

2. Ter uma **equipe de resposta a incidentes** de segurança com experiência em eventos de *ransomware*

3. Estabelecer uma **política corporativa sobre pagamento do resgate (sim ou não),** avaliando a legalidade, bem como quando e como tal decisão deve ser tomada e os meios para aquisição de criptomoedas

4. Ter um **plano de ação detalhado** para o caso de um incidente com *ransomware*, incluindo a lista de pessoas, entidades e empresas que devem ser acionadas;

5. Avaliar a capacidade de **recuperação de cópias** de segurança em grande escala.

Fonte: Artigo "**Ransomware: pagar ou não pagar, eis a questão"** https://bit.ly/3odpsF0

Boas práticas em relação ao fator humano

TCESP Tribunal de Contas do Estado de São Paulo

Fator Humano

Conscientização e treinamento das pessoas, para que seja criada uma cultura de segurança da informação

1. Estabelecer um programa de **capacitação constante** em segurança da informação e proteção de dados
2. **Simulação de *phishing*** para identificação e orientação de pessoas mais vulneráveis a esse tipo de ataque
3. Palestras, eventos e orientação constante sobre as **principais vulnerabilidades, ameaças e ataques** recentes.

Fonte: Artigo "**Ransomware: pagar ou não pagar, eis a questão"** https://bit.ly/3odpsF0

TCESP
Tribunal de Contas
do Estado de São Paulo

Recomendações do Ponemon Institute

Ações para minimizar os riscos (1/2)

(i)

Automatização da segurança

Uso de soluções de Inteligência **Artificial e analytics**: organizações que implementaram completamente a automação de segurança tiverem um **custo médio 60% menor** que as empresas que não têm essa automação.

(ii)

Adoção do modelo de segurança "zero trust"

Assume-se que ninguém é confiável por padrão: "**nunca confie, sempre verifique**".

(iii)

Teste intensivo do plano de resposta a incidentes

Manter a equipe preparada e treinada para atuar com agilidade e de forma certeira quando um incidente realmente ocorrer.

(iv)

Uso de ferramentas para proteção e monitoramento de computadores e empregados remotos

Como soluções de UEM – *Unified endpoint management* – e IAM – *Identity and access management*.

Fonte: *Cost of a Data Breach Report* 2020, Ponemon Institute
https://bit.ly/39ErsOc

Ações para minimizar os riscos (2/2)

(i)

Programas de governança, gerenciamento de risco e compliance

Preparar-se estruturalmente para auditorias e para a realização de avaliações de risco para acompanhar o processo de conformidade com requisitos regulatórios e de segurança da informação.

(ii)

Minimização da complexidade dos ambientes de TI e segurança da informação

Utilização de soluções abrangentes com capacidade de lidar com sistemas distintos e híbridos, para ajudar as equipes de segurança a detectar incidentes em ambientes heterogêneos.

(iii)

Proteção de dados em ambientes de nuvem com políticas e tecnologias

Como classificação de dados e políticas de retenção, definindo de forma clara o ciclo de vida dos dados dentro da organização, dando maior visibilidade dessas informações e minimizando o volume de dados tratados, em harmonia com o **princípio da necessidade da LGPD.** Usar criptografia, se possível, e realizar testes de penetração de forma a identificar e corrigir vulnerabilidades.

(viii)

Utilização de serviços de segurança gerenciados

Especialmente se a organização não possuir uma equipe de segurança capacitada. Esse tipo de serviço possibilita um monitoramento ininterrupto do ambiente tecnológico, permitindo uma rápida intervenção no caso de um incidentes.

Padrões Técnicos de Segurança valorizados pelas autoridades europeias

TCESP Tribunal de Contas do Estado de São Paulo

1. Monitorar contas privilegiadas
2. Monitorar acesso e uso de BD com dados pessoais
3. Fazer o *hardening* de servidores
4. Usar criptografia em dados pessoais
5. Usar autenticação multifator
6. Ter rigoroso controle de acesso com base na necessidade
7. Realizar testes de invasão frequentes
8. Não armazenar senhas em texto claro
9. Registrar tentativas de login sem sucesso
10. Revisar códigos em busca de dados pessoais
11. Seguir padrão PCI DSS para processamento de dados de cartões

Fonte: Artigo: "Quais são os padrões técnicos mínimos exigidos pela LGPD?" https://bit.ly/3zIw1BA

Guia Orientativo ANPD

Segurança da Informação para Agentes de Tratamento de Pequeno Porte

Medidas Administrativas

I. **Política de Segurança da Informação** – mesmo que simplificada, diretrizes e regras
II. **Conscientização e Treinamento**
III. **Gerenciamento de Contratos** – inclusão de termos de confidencialidade para funcionários, fornecedores e clientes

Medidas Técnicas

I. **Controle de Acesso** – necessidade, senhas complexas, autenticação multifator
II. **Segurança dos dados pessoais armazenados** – necessidade e minimização da coleta, evitar uso de mídias externas, backup e criptografia
III. **Segurança das comunicações** – protocolos seguros, criptografia e tecnologia de proteção
IV. **Gerenciamento de vulnerabilidades**

Dispositivos Móveis

I. **Mesmos controles** para equipamentos corporativos
II. Autenticação **multifator**.
III. **Evitar** uso de dispositivos particulares
IV. Possibilidade de **apagar dados remotamente**

Nuvem

I. Contrato de **SLA** adequado que contemple a Segurança da Informação e Proteção de dados pessoais
II. autenticação **multifator**

Fonte: LGPD: as recomendações para Micro e Pequenas Empresas

https://bit.ly/3o7LYh1

Boas práticas do mercado

Marco Civil da Internet
Decreto 8.771/16
Esse decreto define, por exemplo, a previsão de utilização de sistemas de **autenticação de dois fatores** e uso de **criptografia**.

Normas ABNT ISO/IEC

27001
Define os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um **Sistema de Gestão da Segurança da Informação** (SGSI), com foco nas necessidades e particularidades de cada organização

27002
Estipula as **melhores práticas** para apoiar a implantação do SGSI, incluindo a seleção, implementação e o gerenciamento de **controles**, com base em **análise de risco** da organização

27003
Diretrizes para **implantação do SGSI**

27004
Métricas e controles alinhados à 27002

27005
Trata do processo de **gestão de riscos** de segurança da informação

27006
Diretrizes para o **credenciamento de organizações e certificação de SGSI**

27035
Resposta e gerenciamento de **Incidentes**

27102
Diretrizes para **seguro cibernético**

27103
Uso do SGSI criar uma **estrutura de segurança cibernética**

27550
Diretrizes de engenharia de privacidade no **ciclo de vida de sistemas**

27701
Trata da **gestão da privacidade** no contexto da organização

31000
Traz recomendações para **gerenciar os riscos**

Para começar...

Regra de Pareto

3 ações que podem resolver 80% dos incidentes

Manter softwares Atualizados

"as 10 vulnerabilidades mais exploradas para o comprometimento de sistemas e redes governamentais são conhecidas e possuem correções, algumas há mais de 5 anos."

Hardening de SO e dispositivos

"especialmente para mudar configurações de fábrica alterando, por exemplo, usuário e senhas amplamente conhecidas e desabilitando protocolos inseguros ou não utilizados"

Melhorar processo de autenticação

"sistemas que utilizam apenas senhas como forma de autenticação são alvos mais fáceis para golpes digitais. Uma forma de melhorar a segurança dos sistemas é utilizar múltiplos fatores de autenticação"

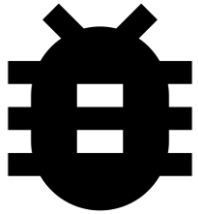
Fonte: CETIC.br, detalhado em meu artigo:
Regra de Pareto para a Segurança Digital: 3 ações que mitigam 80% dos ataques
https://bit.ly/2WcBanG

Não esquecer o fator humano!

Causas dos incidentes

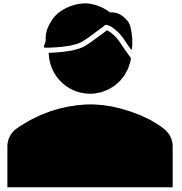
Ataques Maliciosos

52% no geral
47% no Brasil



Falhas de Sistemas

25% no geral
28% no Brasil



Erro Humano

23% no geral
25% no Brasil

Fonte: *Cost of a Data Breach Report* 2020, Ponemon Institute
https://bit.ly/39ErsOc

Principais vetores de *Ransomware*

E-mail *phishing*

E-mails falsos com o objetivo de roubar credenciais

Fonte: *o IC3[10] (Internet Crime Complaint Center), ligado ao FBI, em meu artigo "***Ransomware: pagar ou não pagar, eis a questão"** https://bit.ly/3odpsF0

Protocolo RDP

Protocolo Remote Desktop (RDP) é aquele que permite o acesso remoto a computadores por meio da Internet e que ficou muito comum em tempos de pandemia

Vulnerabilidades de softwares

Especialmente de sistemas operacionais, que permitem acesso ao computador da vítima para espalhar o *ransomware*.

“

O **elo humano** é constantemente **negligenciado** em ações institucionais. Em relação à LGPD, é essencial que a instituição promova **treinamentos, capacitação, sensibilização e campanhas constantes** para servidores, contratados, jurisdicionados e parceiros que versem sobre **segurança da informação**, **privacidade** e cuidados necessários com o tratamento dos dados pessoais.

”

Obrigado!

Fabio Correa Xavier

Diretor do Departamento de TI do TCESP

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

https://twitter.com/fabiocx

www.fabioxavier.com.br

"That's all Folks!"