Gestão de Riscos e Proteção de Dados Pessoais

Rodrigo D. P. Gomes

RODRIGO DIAS DE PINHO GOMES

rodrigo@pinhogomes.com.br - Instagram @prof_rdpg

Advogado.

Membro titular do Conselho Municipal de Proteção de Dados e Privacidade – RJ.

Presidente da Comissão de Proteção de Dados da OAB-RJ.

Membro da Comissão de Proteção de Dados do Conselho Federal da OAB.

Doutor em Direito Civil pela UERJ.

Data Protection Officer.

PINHO GOMES

ADVOGADOS

pine data officer

ICO reprimands NHS Lanarkshire for sharing patient data via WhatsApp

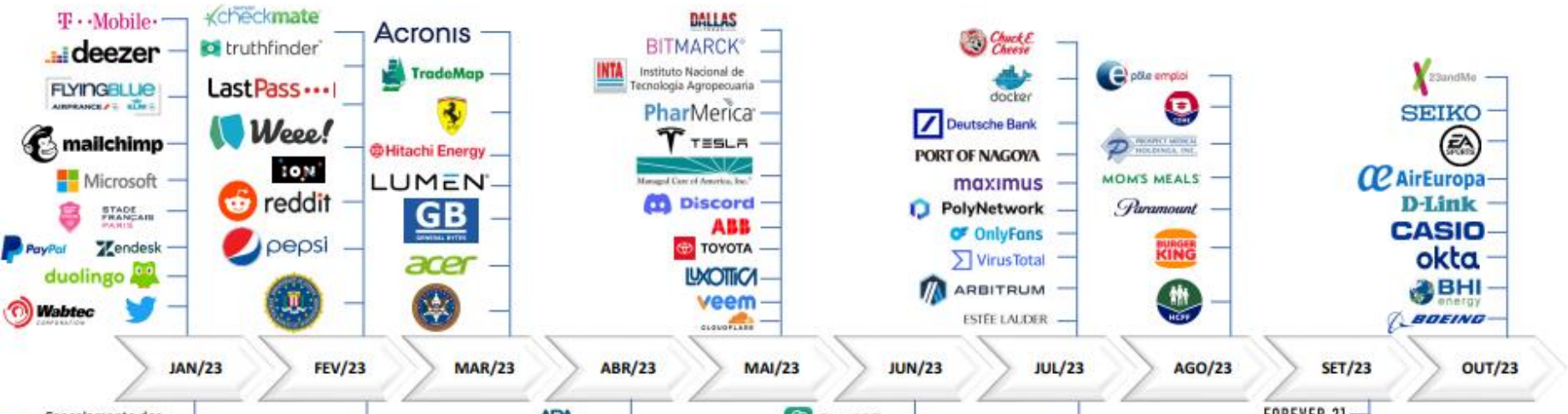
Date
01 August 2023

Type
News

The Information Commissioner's Office (ICO) has issued a reprimand to NHS Lanarkshire, following staff's unauthorised use of WhatsApp to share patients' personal data over the course of two years.

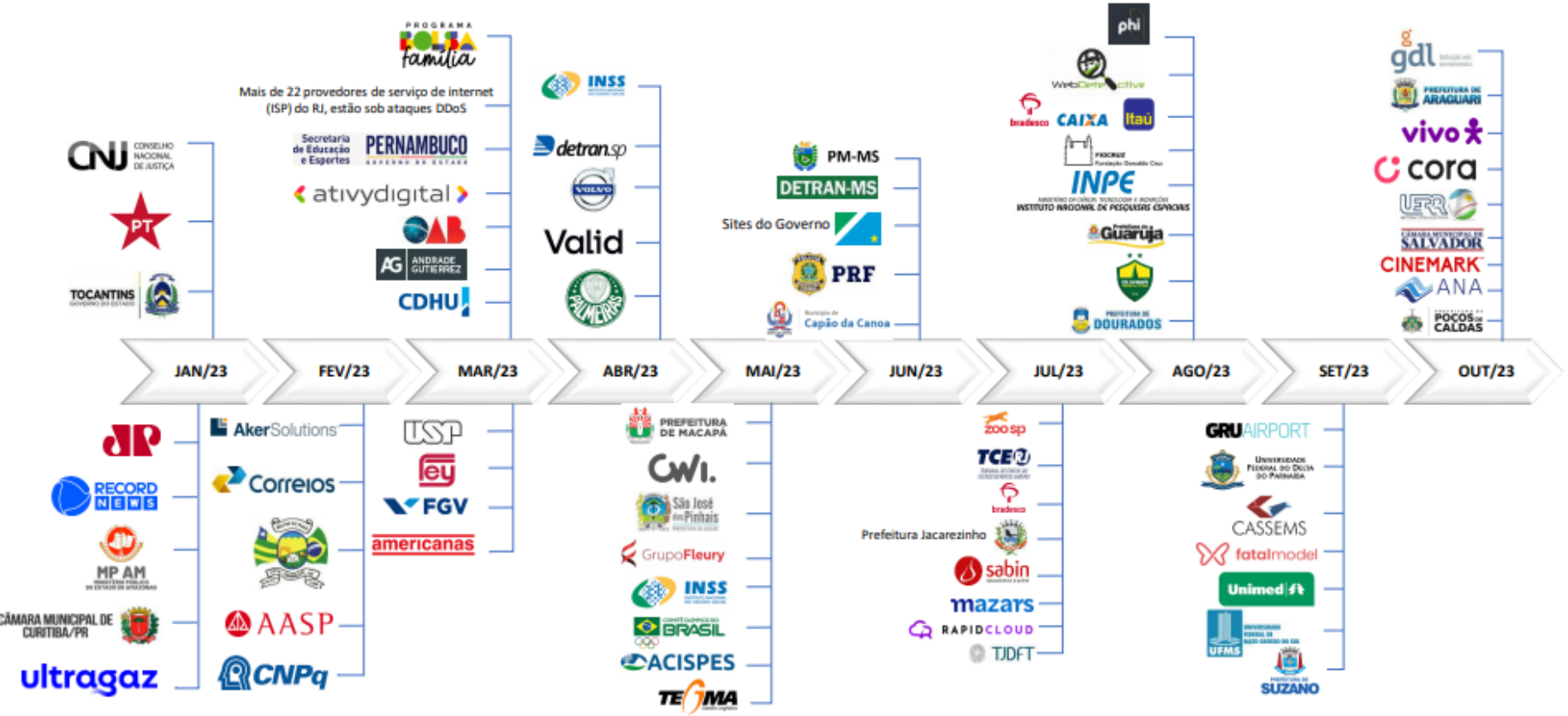
https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/08/ico-reprimands-nhs-lanarkshire-for-sharing-patient-data-via-whatsapp/

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*



- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*



- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade

IBRASPD

Incidente de Segurança com Dados Pessoais

Multa de €3,5 milhões foi aplicada devido a uma avaliação de risco inadequada, que permitiu um ataque cibernético com grande impacto nos dados de 1,35 milhão de clientes.

Redes Eléctricas Inteligentes, S.A.U.

AEPD (Spain) - EXP202205206


Probabilidade
x
Impacto
=
Riscos

Tabela 4 Parâmetros Escalares

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

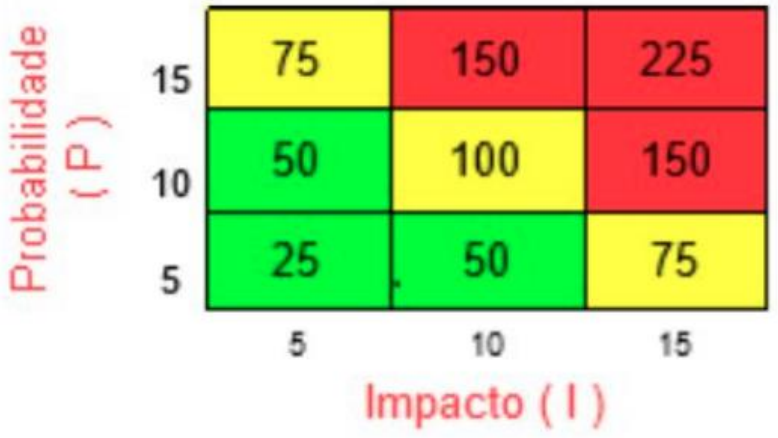


Figura 2 Matriz Probabilidade x Impacto

Fonte: Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD)

- Medidas necessárias
- Nível de prioridade
- Responsável
- Nível de complexidade
- Custo
- Prazo

Avaliação de Riscos

Comparar

Confrontar os riscos com os critérios

Priorizar

Determinar quais riscos requerem tratamento

Decidir

Selecionar as opções de tratamento adequadas

Foco nas Incertezas

1. **Identificar**
   Reconhecer as incertezas que podem afetar os objetivos.

2. **Analisar**
   Compreender as causas e os impactos potenciais das incertezas.

3. **Responder**
   Desenvolver estratégias para lidar com as incertezas identificadas.

Melhoria Contínua

1

Monitoramento

Acompanhar a evolução dos riscos e a eficácia das medidas adotadas.

2

Análise Crítica

Avaliar periodicamente o desempenho do sistema de gestão de riscos.

3

Aprendizado

Incorporar lições aprendidas e adotar melhores práticas de forma contínua.

Gestão de Riscos Organizacionais

- Cultura Organizacional

Incorporar a gestão de riscos como parte da mentalidade e nos comportamentos.

- Governança e Liderança

Garantir o compromisso e o direcionamento da alta direção.

- Processos e Sistemas

Alinhar a gestão de riscos aos processos e sistemas existentes.

Criação e Proteção de Valor

1

Aumento de Eficiência

Identificar e mitigar riscos para melhorar a eficiência operacional.

2

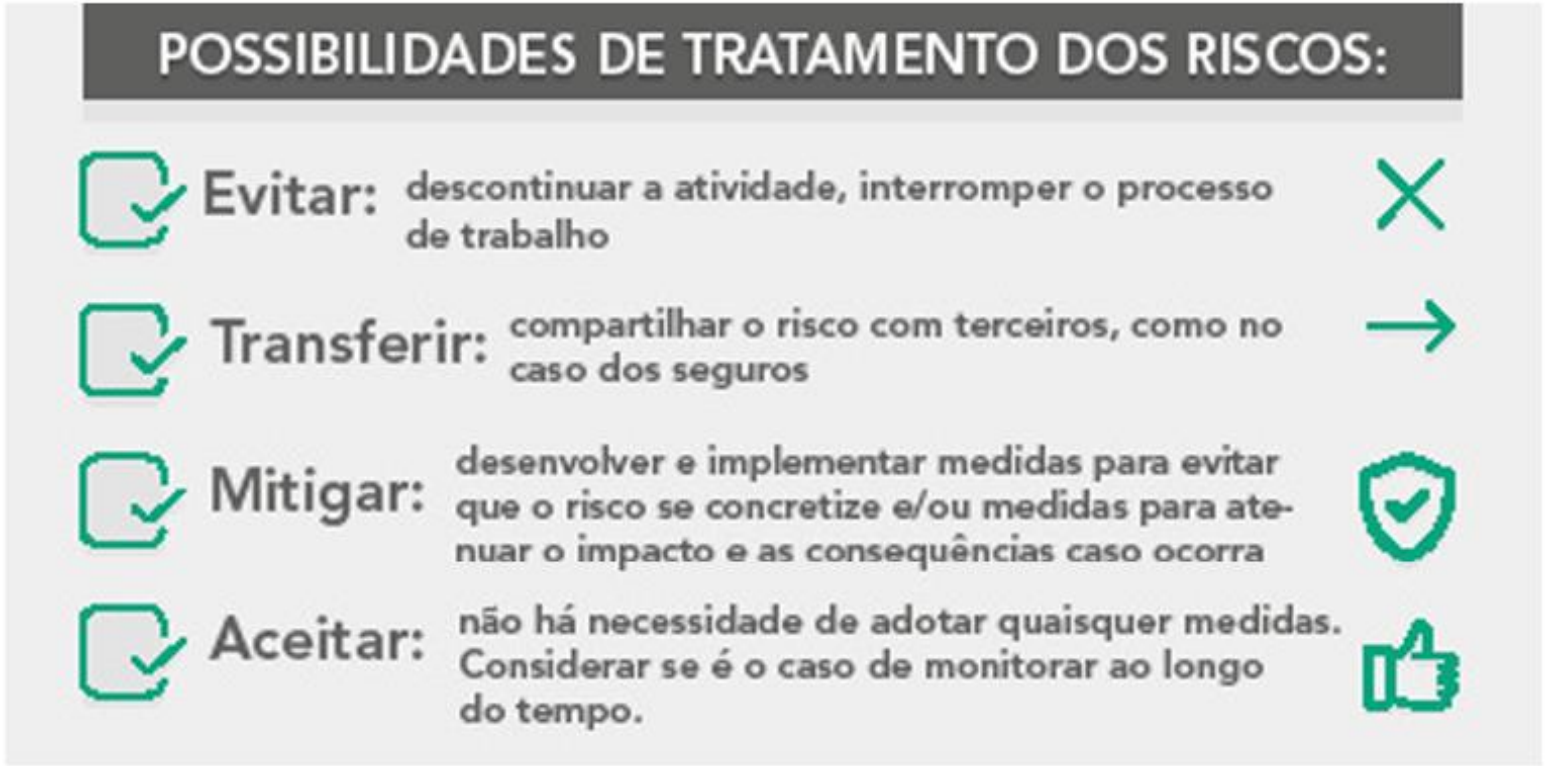
Vantagem Competitiva

Gerenciar riscos de forma proativa = vantagem competitiva.

3

Otimização de Resultados

Equilibrar riscos e oportunidades para maximizar os resultados.



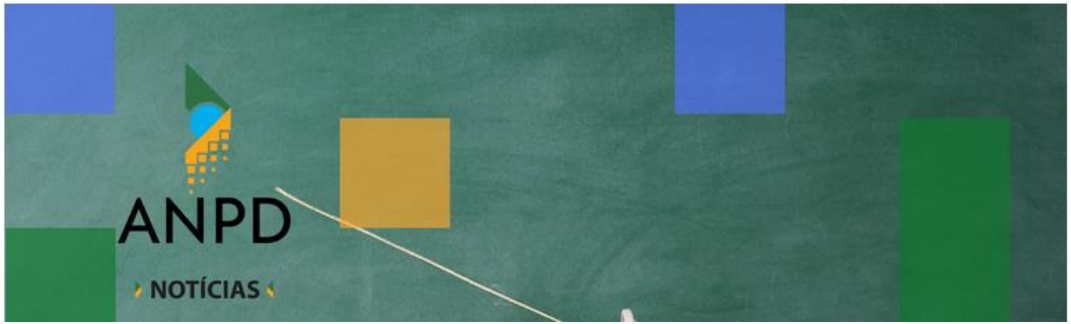
https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/

FISCALIZAÇÃO

ANPD conclui processo sancionador contra órgão público

Coordenação-Geral de Fiscalização da ANPD concluiu processo administrativo sancionador contra o IAMSPE de São Paulo

Publicado em 06/10/2023 16h50 | Atualizado em 06/10/2023 22h10



FISCALIZAÇÃO

ANPD sanciona mais um órgão público

Coordenação-Geral de Fiscalização concluiu que a Secretaria de Saúde de Santa Catarina cometeu quatro infrações à legislação em vigor, sendo três graves

Publicado em 18/10/2023 10h07 | Atualizado em 30/10/2023 10h05

STF: ADI 6.649 - DF

Tratamento de dados por órgãos públicos que viole as normas legais e constitucionais

Resp. Civil Estado

Direito de regresso

Improbidade adm

Sanções disciplinares

Segurança

Art. 6, VII

utilização de medidas **técnicas e administrativas aptas a proteger os dados pessoais** de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Findings

Brazil

Get the 2020 password list

https://nordpass.com/most-common-passwords-list/

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	123456	< 1 Second	1,003,925
2	123456789	< 1 Second	326,815
3	Brasil	< 1 Second	154,075
4	12345	< 1 Second	143,513
5	102030	< 1 Second	106,217
6	senha	10 Seconds	103,500
7	12345678	< 1 Second	85,937

Prevenção

Art. 6, VIII

Adoção de medidas para **prevenir a ocorrência de danos** em virtude do tratamento de dados pessoais - ***Privacy by design***.

Privacy by design

Art. 46. Os agentes de tratamento devem adotar **medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais** de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

(...)

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas **desde a fase de concepção do produto ou do serviço até a sua execução**.

DarkSide ransomware

The New York Times

Colonial Pipeline chief says an oversight let hackers into its system.

Cybercriminals gained access via an old virtual private network, allowing them to paralyze a critical U.S. fuel artery.

Give this article

This article is part of our Daily Business Briefing

Joseph Blount, the chief executive of Colonial Pipeline, told a Senate committee on Tuesday that the company believes cybercriminals accessed its computer systems via a virtual private network that was no longer used.
Andrew Caballero-Reynolds/Agence France-Presse — Getty Images

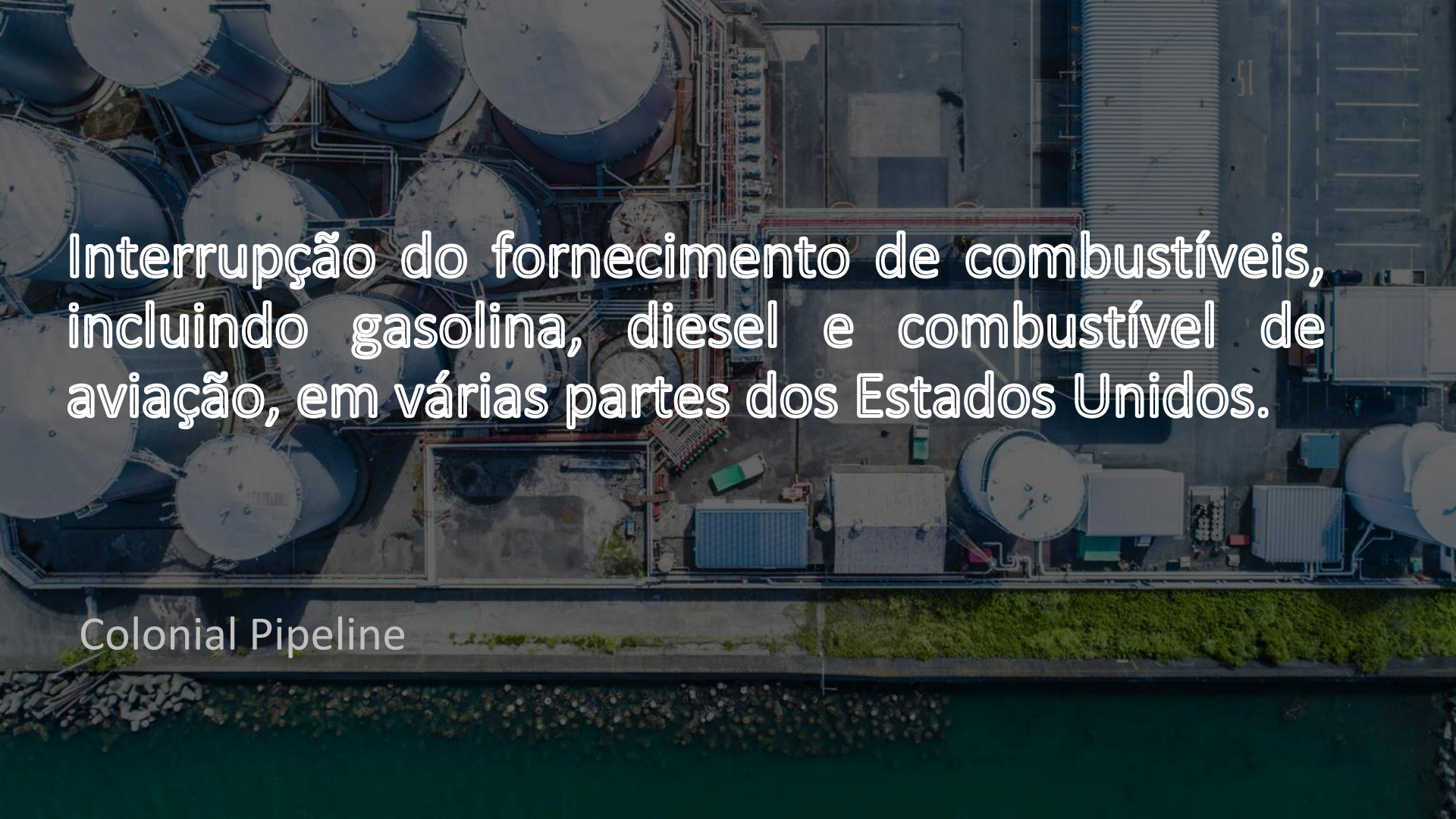
By Clifford Krauss

Published June 8, 2021 Updated June 9, 2021

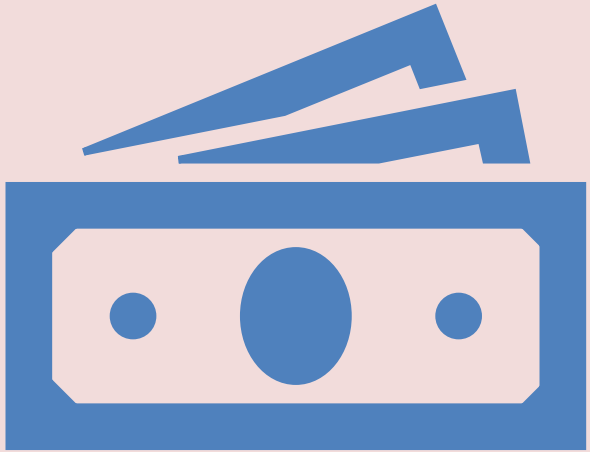
https://www.nytimes.com/2021/06/08/business/colonial-pipeline-hack.html

V.P.N.

não exigia autenticação multifator (MFA)


Interrupção do fornecimento de combustíveis, incluindo gasolina, diesel e combustível de aviação, em várias partes dos Estados Unidos.
Colonial Pipeline

4,4 milhões de dólares



Accountability

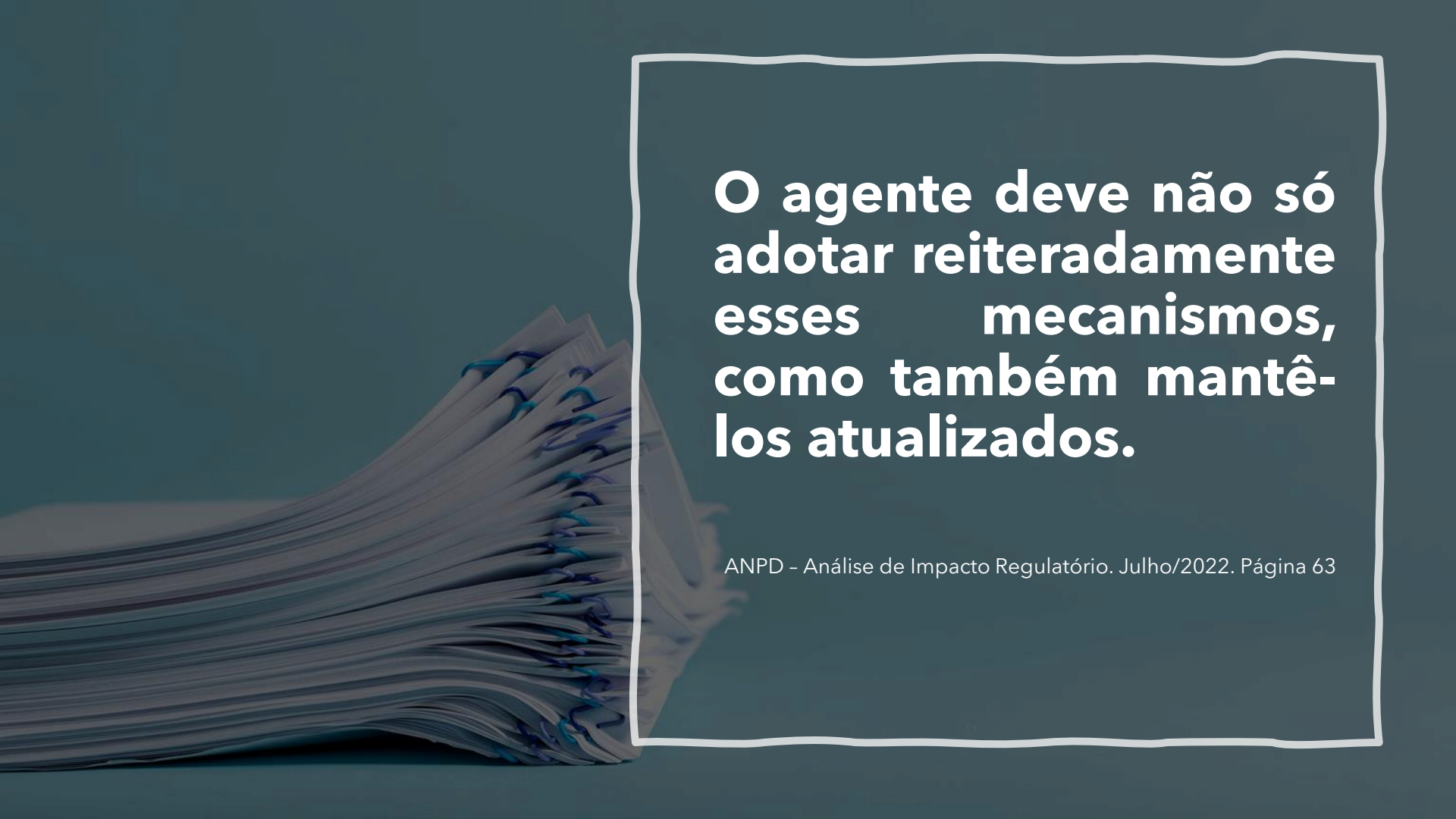
RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS - Art. 6, X.

Demonstração, pelo agente, da **adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas** de proteção de dados pessoais e, inclusive, da **eficácia dessas medidas**.

Parâmetros e Critérios Sanções Administrativas

Art. 52 § 1°

- Garantida a ampla defesa - (CF Art 5 LV)
- Gravidade e a natureza das infrações e dos direitos pessoais afetados
- Boa-fé do infrator
- Vantagem auferida
- Condição econômica do infrator
- Reincidência
- Grau do dano
- Cooperação do infrator
- Adoção de mecanismos de minimização do dano
- Adoção de política de boas práticas e governança
- Pronta adoção de medidas corretivas
- Proporcionalidade entre a gravidade da falta e a intensidade da sanção



O agente deve não só adotar reiteradamente esses mecanismos, como também mantê-los atualizados.

ANPD – Análise de Impacto Regulatório. Julho/2022. Página 63

Protocolo: **816431**
Data: **02/08/2022**
Título: **RESOLUÇÃO Nº 91**
Página(s): **a**

RESOLUÇÃO SEGOVI Nº 91 DE 1º DE AGOSTO DE 2022

Regulamenta o Programa de Governança em Privacidade e Proteção dos Dados Pessoais - PGPPDP no âmbito da Administração Pública Municipal, em conformidade com o art. 50, § 2º da Lei Geral de Proteção de Dados Pessoais - LGPD.

O SECRETÁRIO MUNICIPAL DE GOVERNO E INTEGRIDADE PÚBLICA, no uso das atribuições que lhe são conferidas pela legislação em vigor, e

CONSIDERANDO o disposto no inciso LXXIX, do art. 5º, da Constituição da República Federativa do Brasil de 1988, incluído pela Emenda Constitucional nº 115, de 10 de janeiro de 2022, o qual estabelece que é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;

CONSIDERANDO o disposto na Lei Federal nº 13.709, Lei Geral de Proteção de Dados Pessoais - LGPD;

CONSIDERANDO o disposto no Decreto Rio nº 49.558, de 06 de outubro de 2021, que *estabelece os procedimentos iniciais a serem adotados pela Administração Pública Municipal visando à construção de uma cultura de proteção de dados pessoais e dá outras providências* , em especial seu art. 3º, parágrafo único, segundo a qual caberá à Secretaria Municipal de Governo e Integridade Pública - SEGOVI propor as medidas de governança necessárias à implementação do Programa de Proteção de Dados no âmbito da PCRJ,

I - Termo de Uso;

II - Termo de Consentimento;

III - Inventário de Dados Pessoais;

IV - Orientações do Controlador para o Operador;

V - Plano de Análise de Riscos;

VI - Plano de Adequação;

VII - Aviso de Privacidade e Política de Privacidade;

VIII - Política de Cookies;

IX - Plano de Resposta aos Incidentes de Proteção de Dados Pessoais;

X - Relatório de Incidente de Proteção de Dados Pessoais;

XI - Política de Controle de Acessos;

XII - RIPD;

XIII - Proposta de Cronograma de Identificação e de Mapeamento dos Instrumentos Jurídicos

XIV - Cronograma de Implementação do PGPPDP.


POLICIES
STANDARDS
TRANSPARENCY
REQUIREMENTS
DPO
RULES
REGULATIONS
LAW
GOVERNANCE

ANPD Autoridade Nacional de Proteção de Dados

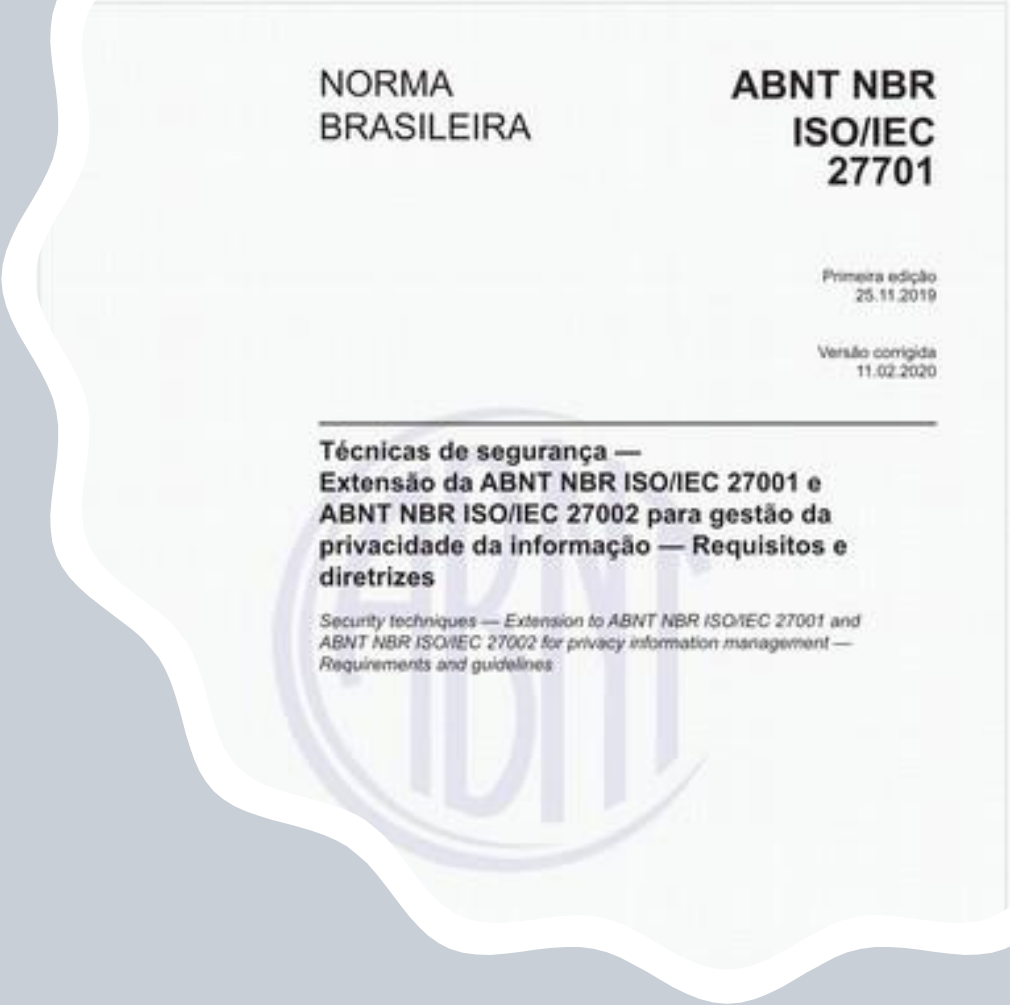
"74. (...) Como boa prática, considera-se **importante que o encarregado tenha liberdade** na realização de suas atribuições. (...)

76. Também é importante observar que a LGPD não proíbe que o encarregado seja apoiado por uma equipe de proteção de dados. Ao contrário, considerando as boas práticas, é importante que o encarregado tenha **recursos adequados para realizar suas atividades**, o que pode incluir recursos humanos. Outros recursos que devem ser considerados são tempo (prazos apropriados), finanças e infraestrutura"

GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO - https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf

item 6.3.1.1 ABNT NBR ISO/IEC 27701:2019

- **Independência**
- **Liberdade**
- Reportar ao **nível gerencial apropriado**


NORMA
BRASILEIRA

ABNT NBR
ISO/IEC
27701

Primeira edição
25.11.2019

Versão corrigida
11.02.2020

Técnicas de segurança —
Extensão da ABNT NBR ISO/IEC 27001 e
ABNT NBR ISO/IEC 27002 para gestão da
privacidade da informação — Requisitos e
diretrizes

Security techniques — Extension to ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for privacy information management — Requirements and guidelines

Carregando o piano? notas sobre o encarregado de dados no setor público

Rodrigo Dias de Pinho Gomes e Rafael A. F. Zanatta

Os desafios e complexidades enfrentados pela função do Encarregado pela Proteção de Dados Pessoais na coisa pública é diretamente proporcional à relevância do cargo para o respeito e cumprimento às regras trazidas pela LGPD.

quinta-feira, 22 de julho de 2021

(Imagem: Arte Migalhas)

https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos

MANUAL DE GESTÃO DE RISCOS DO TCU

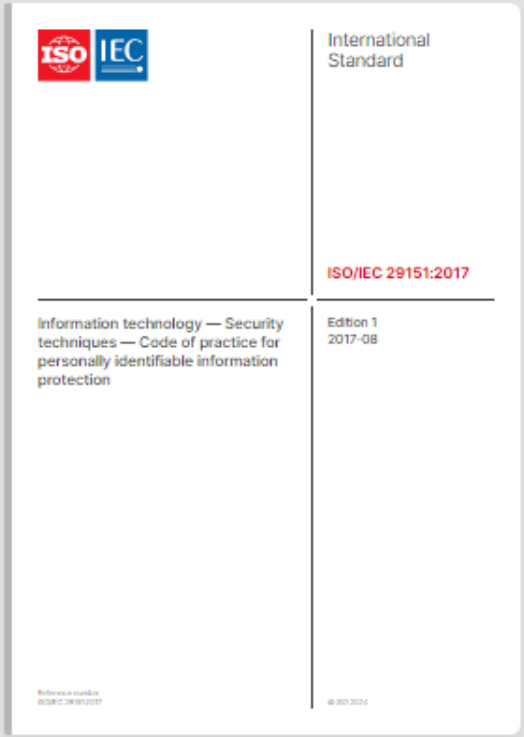
https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/manual-de-gestao-de-riscos/

National Institute of Standards and Technology
U.S. Department of Commerce

NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0

16 de janeiro de 2020

https://doi.org/10.6028/NIST.CSWP.01162020pt



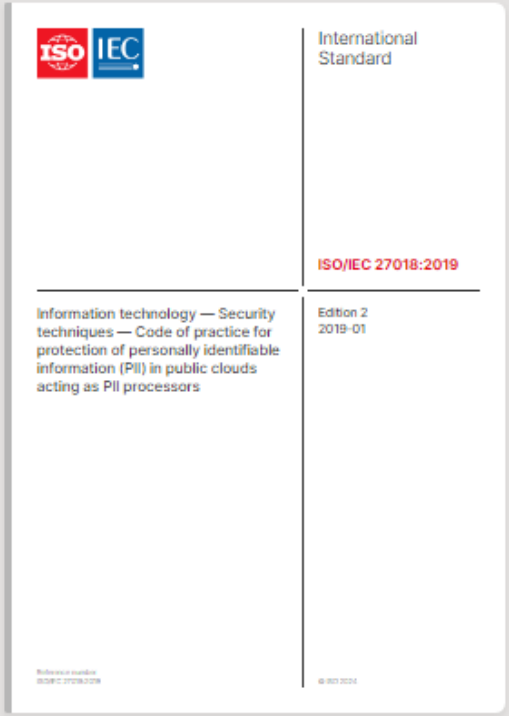
ISO/IEC 29151:2017

Information technology — Security techniques — Code of practice for personally identifiable information protection

Published (Edition 1, 2017)

This standard was last reviewed and confirmed in 2023. Therefore this version remains current.

https://www.iso.org/standard/62726.html



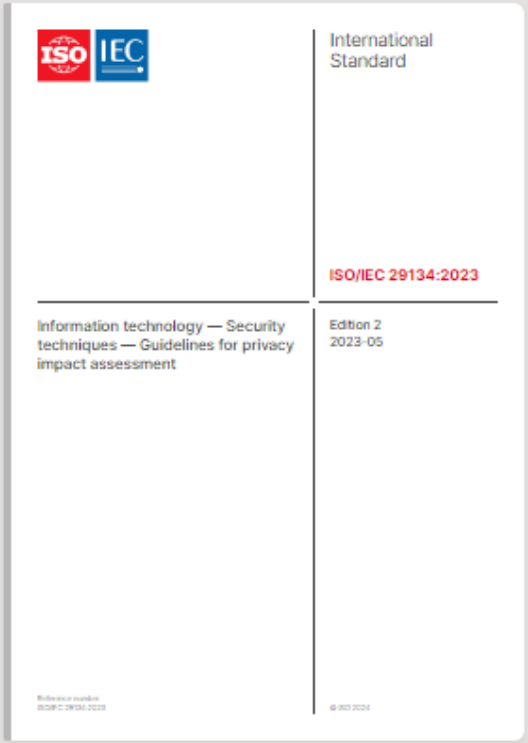
ISO/IEC 27018:2019

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Published (Edition 2, 2019)

→ Expected to be replaced by ISO/IEC DIS 27018 within the coming months.

https://www.iso.org/standard/76559.html

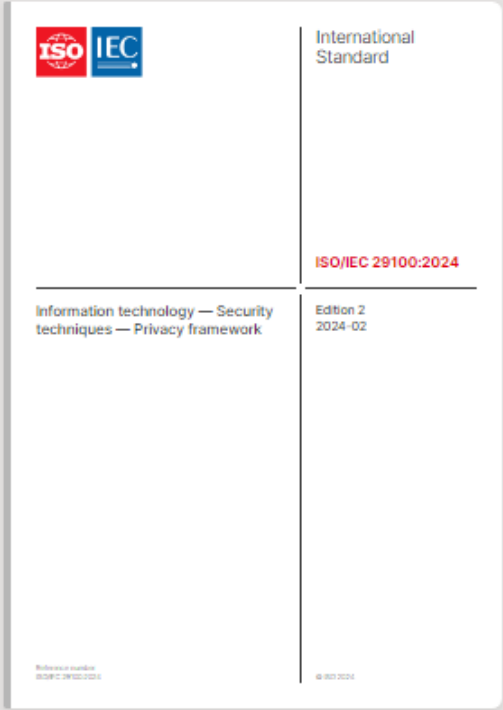


ISO/IEC 29134:2023

Information technology — Security techniques — Guidelines for privacy impact assessment

Published (Edition 2, 2023)

https://www.iso.org/standard/86012.html



ISO/IEC 29100:2024

Information technology — Security techniques — Privacy framework

Published (Edition 2, 2024)

https://www.iso.org/standard/85938.html

OBRIGADO!

Instagram @prof_rdpg

PINHO GOMES
ADVOGADOS

RODRIGO DIAS DE PINHO GOMES
21 99577 5776 21 2283 5062
WWW.PINHOGOMES.COM.BR
RUA DO CARMO N° 8, 12°ANDAR - CENTRO
RIO DE JANEIRO - RJ - CEP 20.011-020

ESCRITÓRIO CARBONO NEUTRO
United Nations FRAMEWORK CONVENTION ON CLIMATE CHANGE

pine data officer