Entenda como o Termo de Referência ANPPD/RGB contribuiu para o Acórdão 1384/2022 emitido pelo TCU alinhado com a ISO-27701

Avanços da LGPD no Setor Público

Davis Alves, Ph.D
Presidente da ANPPD
Data Protection Officer
Segurança da Informação

Início: 04/11/22 (6ª feira)
Horário: 10h00 às 11h00 (fuso de Brasília)

Associação Nacional dos Profissionais de Privacidade de Dados

Palestrante de hoje:

Prof. Davis Alves, Ph.D
Data Protection Officer
Segurança da Informação

@davisalvesphd

- Presidente da ANPPD – Associação Nacional dos Profissionais de Privacidade de Dados.
- Coordenador do GT-1 – Subsídios para Política Nacional de Proteção de Dados do CNPD/ANPD
- Servidor Público desde 2014 na área de Redes de Computadores na Universidade Municipal de São Caetano do Sul (USCS).

Segurança da Informação, ITIL® Expert · Data Protection Officer (DPO) · LGPD Specialist · CISO · ISO-27001 Professional · ICS MCSA® · Cloud Computing · Cyber Security · Ethical Hacker · Psicanalista · Instrutor oficial do EXIN® · Coordenador (GT1) & Membro do Conselho Nacional de Proteção de Dados (CNPD/ANPD) nomeado pelo Presidente da República do Brasil.

- Professor no Ensino Superior: UNIP/USCS/UFSCar/Daryus
- Professor no Mestrado e Doutorado: Florida Christian University
- **Tecnólogo** em Redes de Computadores e Internet
- **Pós-graduado** em Gerenciamento de Projetos
- **Extensão** em Gestão de TI pela FGV/SP
- **Mestre** em Administração com foco em TI
- **Doutor** em Administração com foco em TI Ph.D pela Florida Christian University nos Estados Unidos.

Colunista Jovem Pan

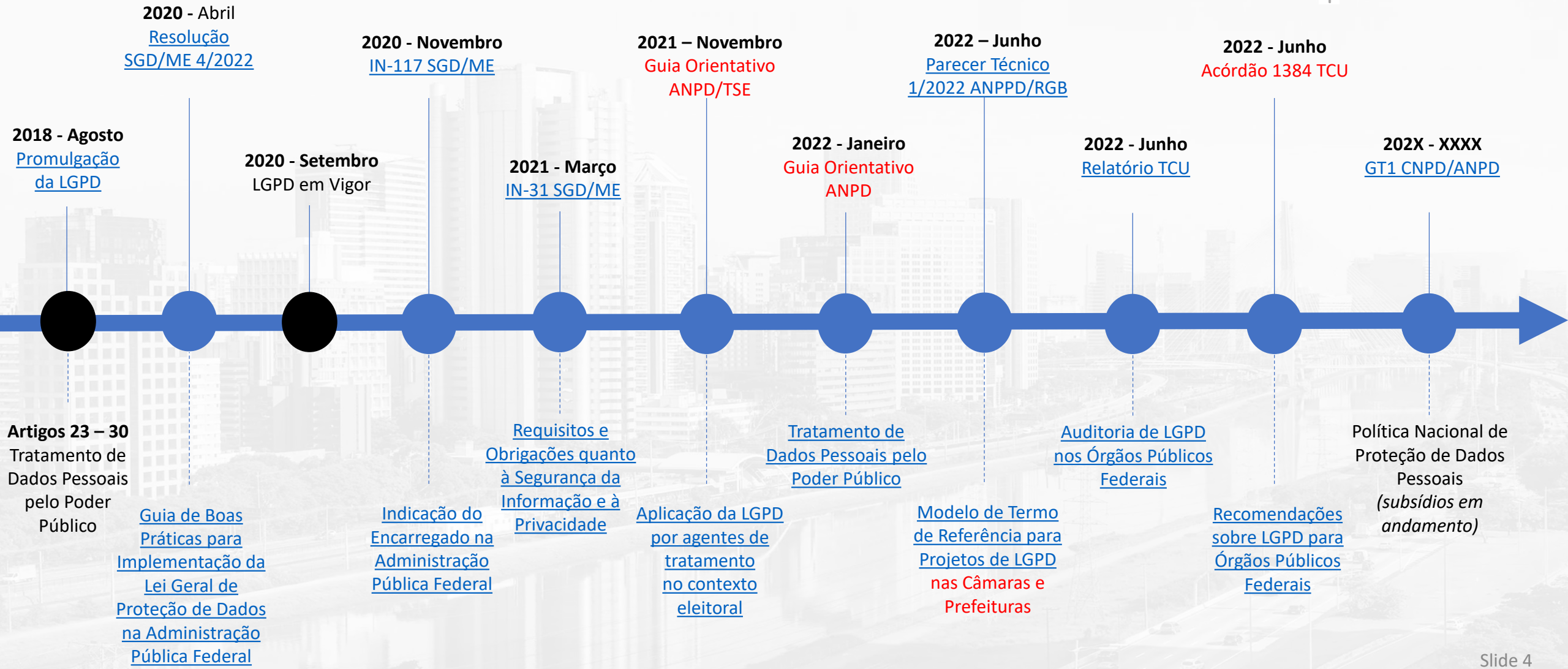
Associação Nacional dos Profissionais de Privacidade de Dados

Conteúdo programático

- Os Avanços da LGPD para o Setor Público – 2018 à 2022
- Desafios da LGPD no Setor Público
- Proposta do Termo de Referência para Projetos de LGPD nas Câmaras e Prefeituras
- Acórdão 1384/2022 TCU - Como adequar a LGPD no Setor Público
- A Norma ISO-27701 oficial para o Setor Público
- A Política Nacional de Proteção de Dados subsídios pelo GT-1 do CNPD
- Pesquisa ANPPD 2022: Panorama dos DPOs no Brasil

Os Avanços da LGPD para o Setor Público – 2018 à 2022

Prof. Davis Alves, Ph.D



Desafios da LGPD no Setor Público

1. Autoridades públicas do executivo (prefeitos, secretários, ministros, etc...) desconhecem a lei
2. Não saber qual setor/secretaria/departamento será o responsável pelo projeto de LGPD (coord.)
3. “Várias leis que existem, as prefeituras não seguem”
4. Falácias: “Essa lei não vai pegar” “Órgão público ninguém fiscaliza direito”
5. Prefeitos não saber o que e como será fiscalizado (ANPD, MP, TCE)
6. Prefeitos esperando “os outros” começarem para terem um modelo
7. Verbas limitadas e/ou não suficientes para projetos de LGPD
8. Prefeituras não sabem o que devem exigir nas licitações
9. Empresas em concorrências com preços impraticáveis (para mais ou para menos)
10. Prefeitos inseguros e com receio para dedicar verbas para projetos de LGPD
11. Licitações do tipo “Menor Preço” garantir as entregas necessárias
12. Não saber avaliar se as empresas concorrentes estão aptas tecnicamente para projetos de LGPD
13. Capacitação em LGPD dos servidores públicos para validar as entregas das empresas ganhadoras
14. Não saber se “esta sendo enganado” pelas empresas ganhadoras das licitações

Brainstorm/Consulta Pública:

“Prefeituras sem projetos de LGPD e com dados vazados devem tornar o prefeito inelegível?”

Lembre-se: Proteção de Dados & Privacidade agora são constitucionais!

Referências para Precificação – Projeto Completo

- ✓ Modelo de "BASELINE" e adaptável
- ✓ Segue modelos científicos de adequação à privacidade (SGPD)
- ✓ O SGPD é reconhecido na Europa para o GDPR (lei equivalente)
- ✓ Convalidado no Brasil por especialistas em LGPD (ANPPD) e para o setor público (RGB)
- ✓ Artigos obrigatórios da LGPD identificados com a norma aplicável
- ✓ Vinculo entre SGPD + LGPD + ISO-27001 + ISO-27701
- ✓ Cada atividade possui referencia com as melhores práticas e normas internacionais para proteção de dados e governança: ISO-27001, ISO-27701, ITIL, COBIT, entre outras (Art. 50 – LGPD)

Fase	Descrição	Referência Base
Fase 01	Preparação	**Art. 50, §2, I, a – LGPD**
Fase 02	Organização	**Art. 6, II – LGPD**
Fase 03	Implementação	**Art. 46 – LGPD**
Fase 04	Governança	**Art. 50 – LGPD**
Fase 05	Avaliação e Melhoria	**Art. 50, §2, I, d & f – LGPD**
Fase 06	Serviço de Gestão da Privacidade (DPOaaS)	**Art. 41, §2 – LGPD**

Descrição	Referência Base (administrativa)	Referência Complementar (técnica)
• Realizar análise de privacidade	Art. 50, §2, I – LGPD	ISO-9001, ISO-27701, ISO-29134

Art. 50. Os controladores e operadores, no âmbito de suas competências ou por meio de **associações**, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização. (LGPD)

Referências para Precificação – Projeto Completo

Modelo oficial ANPPD e RGB de **Termo de Referência para uso nos Projetos de Adequação à Lei Geral de Proteção de Dados (LGPD) dos municípios brasileiros**. Esse modelo foi elaborado conforme estudos técnicos e diretrizes do Tribunal de Contas da União (TCU) disponível para o **Termo de Referência** (tcu.gov.br - http://www.tcu.gov.br/arquivosrca/001.003.011.htm), referências normativas da Lei de Licitações e Contratos Administrativos (Lei 14.133/2021), além da Lei da Modalidade e Pregão (Lei 10.520/2002). A estruturação do escopo técnico segue o modelo (*framework*) europeu DPMS/SGPD - Sistema de Gestão de Proteção de Dados, convalidado no Brasil pelas comissões técnicas da Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD) e Rede Governança Brasil (RGB), referências aos dispositivos da LGPD além das normas e boas práticas internacionais para demonstração do comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente à proteção de dados pessoais. (Art. 50, § 2º, I – LGPD, 2018)

Versão 1.0 01/06/2022
Parecer Técnico ANPPD Nº 01/2022 publicado oficialmente em:
https://anppd.org/parecer/parecer-tecnico-012022-termo-de-referncia-para-projetos-de-lgpd

REDE GOVERNANÇA BRASIL
DA GOVERNANÇA À ESPERANÇA

ANPPD
Associação Nacional dos Profissionais de Privacidade de Dados

MODELO OFICIAL – PARECER TÉCNICO Nº 01/2022

TERMO DE REFERÊNCIA:
PROJETOS DE ADEQUAÇÃO À
LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Proposta com os elementos necessários para uso em licitações de Projetos de Adequação à Lei 13.709/2018 – LGPD nas câmaras e prefeituras brasileiras.

Resumo:

Proposta de Termo de Referência para uso nos Projetos de Adequação à Lei Geral de Proteção de Dados (LGPD) dos municípios brasileiros. Esse modelo foi elaborado conforme estudos técnicos e diretrizes do Tribunal de Contas da União (TCU) disponível para o Termo de Referência (tcu.gov.br), referências normativas da Lei de Licitações e Contratos Administrativos (Lei 14.133/2021), além da Lei da Modalidade e Pregão (Lei 10.520/2002). A estruturação do escopo técnico segue o modelo (*framework*) europeu DPMS/SGPD - Sistema de Gestão de Proteção de Dados, convalidado no Brasil pelas comissões técnicas da Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD) e Rede Governança Brasil (RGB), referências aos dispositivos da LGPD além das normas e boas práticas internacionais para demonstração do comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente à proteção de dados pessoais. (Art. 50, § 2º, I – LGPD, 2018).

Versão 1.0
01/06/2022
Parecer Técnico ANPPD Nº 01/2022 publicado oficialmente em:
https://anppd.org/parecer/parecer-tecnico-012022-termo-de-referncia-para-projetos-de-lgpd

Acórdão 1384/2022 TCU - LGPD no Setor Público

Junho de 2022

Download PDF: https://portal.tcu.gov.br/data/files/B4/25/78/27/D9C818102DFE0FF7F18818A8/038.172-2019-4-AN - auditoria_ Lei Geral de Protecao de Dados.pdf

Acórdão 1384/2022	ABNT NBR ISO/IEC 27701:2019	DIRETRIZ
Identificação de Normativos Correlatos	Item 5.2.1	Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 7.1, junto com a interpretação especificada em 5.1, se aplicam.
Contratos firmados com os Operadores	Item 7.2.6	Convém que a organização determine as responsabilidades e respectivos papéis para o tratamento de DP (incluindo a proteção do DP e os requisitos de segurança) com qualquer controlador conjunto de DP.
Ocorrência de Tratamento de Dados Pessoais	Item 7.2.7	Convém que a organização determine as responsabilidades e respectivos papéis para o tratamento de DP (incluindo a proteção do DP e os requisitos de segurança) com qualquer controlador conjunto de DP.

* Recomendações para o SGD/ME

Acórdão 1384/2022 TCU - LGPD no Setor Público

Junho de 2022

Download PDF: https://portal.tcu.gov.br/data/files/B4/25/78/27/D9C818102DFE0FF7F18818A8/038.172-2019-4-AN - auditoria_ Lei Geral de Protecao de Dados.pdf

Acórdão 1384/2022	ABNT NBR ISO/IEC 27701:2019	DIRETRIZ
Política de Classificação da Informação	Item 6.5.2	Convém que o sistema de classificação da informação da organização considere explicitamente DP como parte do esquema que ela implementa. Considerar DP dentro de todo o sistema de classificação é importante para entender qual DP a organização trata (por exemplo, tipo, categorias especiais), onde tal DP é armazenado e os sistemas pelos quais ele pode fluir
Política de Proteção de Dados Pessoais	Item 6.2.1.1	O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 5.1.1

* Recomendações para o SGD/ME

Acórdão 1384/2022 TCU - LGPD no Setor Público

Junho de 2022

Download PDF: https://portal.tcu.gov.br/data/files/B4/25/78/27/D9C818102DFE0FF7F18818A8/038.172-2019-4-AN - auditoria_ Lei Geral de Protecao de Dados.pdf

Acórdão 1384/2022	ABNT NBR ISO/IEC 27701:2019	DIRETRIZ
Plano de Capacitação	Itens 5.5.2 e 5.5.3	Os requisitos estabelecidos na ABNT NBR ISO/IEC 27001:2013, 7.2, junto com a interpretação especificada em 5.1, se aplicam.
Política de Privacidade	Itens 7.3.2 e 7.3.3	Convém que a organização determine e documente a informação a ser fornecida aos titulares de DP, relativa ao tratamento de seus DP, e o tempo de tal disponibilização
Atendimento dos Direitos dos Titulares	Item 7.3	Para assegurar que os titulares de DP sejam providos com informações apropriadas sobre o tratamento de seus DP e para atender quaisquer outras obrigações aplicáveis aos titulares de DP, relativas aos tratamentos de seus DP.

* Recomendações para o SGD/ME

Acórdão 1384/2022 TCU - LGPD no Setor Público

Junho de 2022

Download PDF: https://portal.tcu.gov.br/data/files/B4/25/78/27/D9C818102DFE0FF7F18818A8/038.172-2019-4-AN - auditoria_ Lei Geral de Protecao de Dados.pdf

Acórdão 1384/2022	ABNT NBR ISO/IEC 27701:2019	DIRETRIZ
Procedimentos internos mais céleres (fast track) e controles simplificados para o uso compartilhado de dados pessoais	Item 7.5	Convém que a organização identifique e documente as bases relevantes para a transferência de DP entre jurisdições.
Controles para o compartilhamento de dados pessoais com terceiros	Item 7.5	Convém que a organização identifique e documente as bases relevantes para a transferência de DP entre jurisdições.
Plano de Resposta a Incidentes	Item 6.13	convém que a organização estabeleça responsabilidades e procedimentos para a identificação e registro de violações de DP

* Recomendações para o SGD/ME

Acórdão 1384/2022 TCU - LGPD no Setor Público

Junho de 2022

Download PDF: https://portal.tcu.gov.br/data/files/B4/25/78/27/D9C818102DFE0FF7F18818A8/038.172-2019-4-AN - auditoria_ Lei Geral de Protecao de Dados.pdf

Acórdão 1384/2022	ABNT NBR ISO/IEC 27701:2019	DIRETRIZ
Controle de acesso de usuários em sistemas	Itens 6.6.2.1 e 6.6.2.2	Convém que procedimentos para registro e cancelamento de usuários que administrem ou operem sistemas e serviços que tratam DP considerem a situação onde o controle de acesso do usuário para aqueles usuários esteja comprometido, como a corrupção ou o comprometimento de senhas ou outros registros de dados de usuários
Registro de Eventos	Item 6.9.4.1	Convém que um processo seja implementado para analisar criticamente os registros de eventos (*logs)* usando processos contínuos de alerta e monitoramento automatizados, ou também manualmente, onde convém que tal análise crítica seja desempenhada em uma periodicidade especificada e documentada, visando identificar irregularidades e propor esforços de remediação
Criptografia	Item 6.7	Convém que a organização forneça informações para o cliente em relação às circunstâncias em que ela usa a criptografia para proteger os DP que ela trata. Convém que a organização também forneça informações para o cliente sobre quaisquer capacidades que ela fornece, que possam atender ao cliente, aplicando sua própria proteção de criptografia

Acórdão 1384/2022 TCU - LGPD no Setor Público

Junho de 2022

Download PDF: https://portal.tcu.gov.br/data/files/B4/25/78/27/D9C818102DFE0FF7F18818A8/038.172-2019-4-AN - auditoria_ Lei Geral de Protecao de Dados.pdf

Acórdão 1384/2022	ABNT NBR ISO/IEC 27701:2019	DIRETRIZ
Controle de acesso de usuários em sistemas	Itens 6.6.2.1 e 6.6.2.2	Convém que procedimentos para registro e cancelamento de usuários que administrem ou operem sistemas e serviços que tratam DP considerem a situação onde o controle de acesso do usuário para aqueles usuários esteja comprometido, como a corrupção ou o comprometimento de senhas ou outros registros de dados de usuários
Registro de Eventos	Item 6.9.4.1	Convém que um processo seja implementado para analisar criticamente os registros de eventos (*logs)* usando processos contínuos de alerta e monitoramento automatizados, ou também manualmente, onde convém que tal análise crítica seja desempenhada em uma periodicidade especificada e documentada, visando identificar irregularidades e propor esforços de remediação
Criptografia	Item 6.7	Convém que a organização forneça informações para o cliente em relação às circunstâncias em que ela usa a criptografia para proteger os DP que ela trata. Convém que a organização também forneça informações para o cliente sobre quaisquer capacidades que ela fornece, que possam atender ao cliente, aplicando sua própria proteção de criptografia

A Norma ISO-27701 oficial para o Setor Público

Norma Técnica

Código	ABNT NBR ISO/IEC 27701:2019 Versão Corrigida:2020

ABNT CERTIFICA ESSA NORMA

Identica a :	ISO/IEC 27701:2019
Data de Publicação :	25/11/2019
Título :	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
Título Idioma Sec. :	Security techniques — Extension to ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for privacy information management — Requirements and guidelines
Nota de Título :	Esta versão corrigida da ABNT NBR ISO/IEC 27701:2019 incorpora a Errata 1, de 11.02.2020.
Comitê :	ABNT/CB-021 Tecnologias da Informação e Transformação Digital
Páginas :	82
Status :	Em Vigor
Idioma :	Português
Organismo :	ABNT - Associação Brasileira de Normas Técnicas
Preço (R$) :	309,40
Objetivo :	Este documento especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização.

Novembro de 2019

Adquirir: ABNT Catalogo

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

A Política Nacional de Proteção de Dados · GT-1 do CNPD

Art. 55-J. Compete à ANPD:

III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:

I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

PRESIDÊNCIA DA REPÚBLICA
CONSELHO NACIONAL DE PROTEÇÃO DE DADOS E DA PRIVACIDADE

PORTARIA CNPD Nº 01, DE 01 DE ABRIL DE 2022

Institui Grupo de Trabalho dedicado à proposição de diretrizes estratégicas e ao fornecimento de subsídios para elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

https://www.gov.br/anpd/pt-br/cnpd-2/portarias-gts-2.pdf

Davis Alves (Coordenador do GT-1) ------- ANPPD
Marta Medeiros ---------- Ministério da Economia
Claudio Rocha ---------- Agência Nacional do Petróleo
Debora Sirotheau ---------- Setor Laboral
Rodrigo Lange ---------- Ministério da Justiça
Marcos Pinto ---------- Ministério da C. e Tecnologia
Fabio Andrade ---------- Setor Empresarial

A Política Nacional de Proteção de Dados · GT-1 do CNPD

PRESIDÊNCIA DA REPÚBLICA
CONSELHO NACIONAL DE PROTEÇÃO DE DADOS E DA PRIVACIDADE

LGPD

É fiscalizada pela...

ANPD

Atuando conforme a...

Política Nacional Proteção de Dados

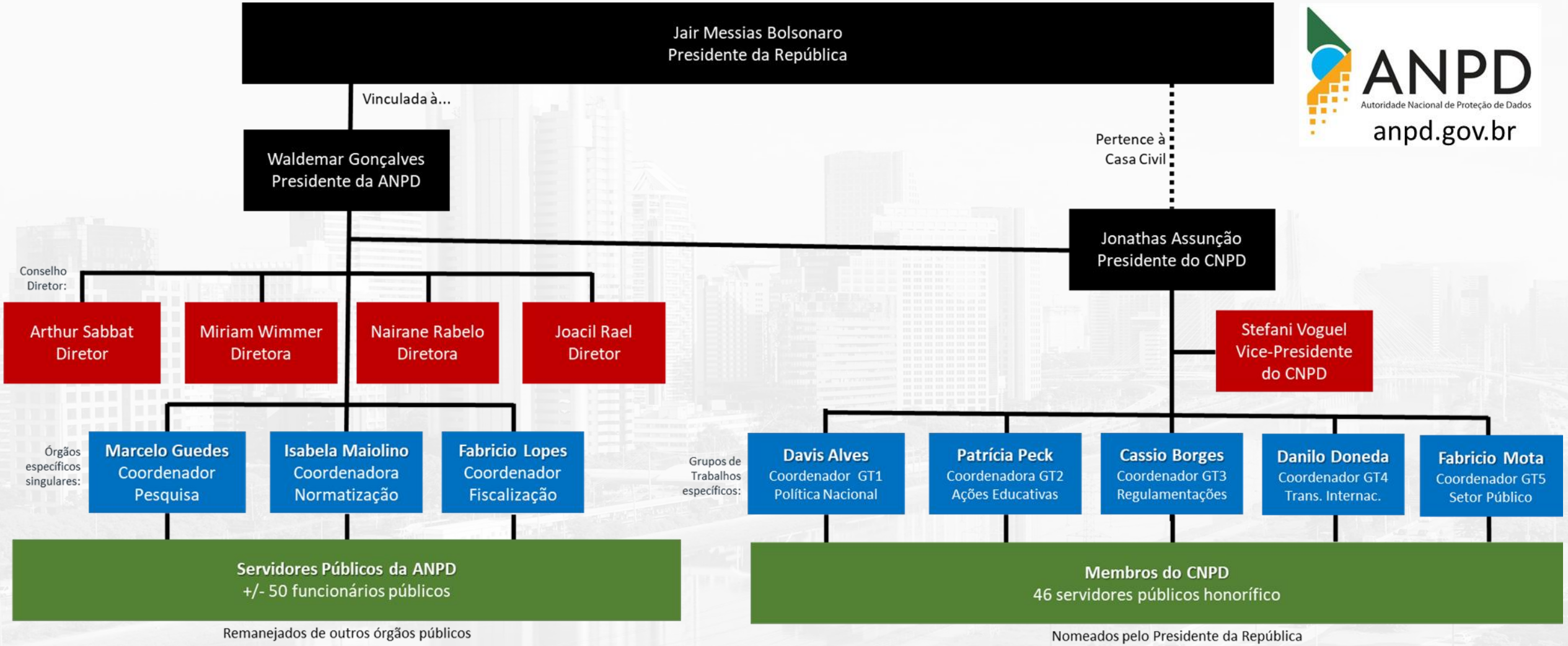
Toda a...

População Brasileira & Órgãos Públicos

A LGPD é fiscalizada pela ANPD, orientando conforme Política Nacional de Proteção de Dados toda a Sociedade Brasileira e Órgãos Públicos

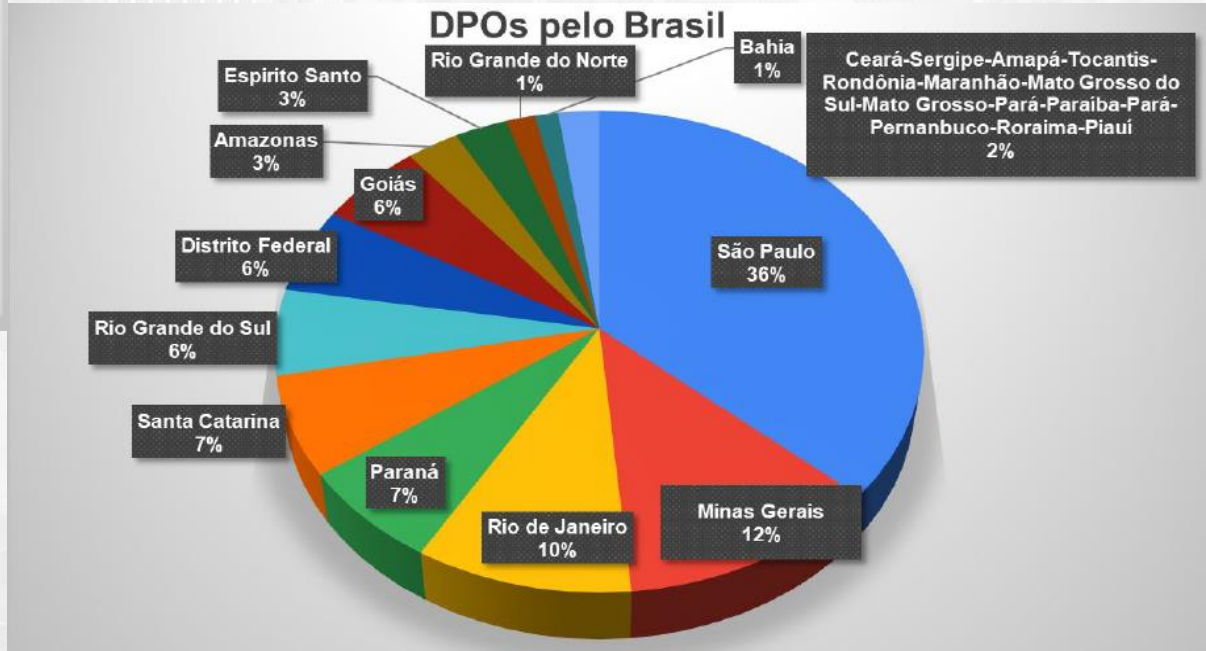
* Possível posicionamento da PNPDPP

A Estrutura da ANPD



Composição da ANPD (www.gov.br)

Perfil dos DPOs no Brasil



Dados: ANPPD (2022)
Publicado em: https://lgpdmagazine.com.br

** LIVRO ** Disponível!

amazon

CLIQUE AQUI

Realização:

TI exames

Prof. Davis Alves, Ph.D
ICS MCSA | ITIL® Expert

Presidente da ANPPD
Membro do Conselho Nacional (CNPD)
Data Protection Officer
Ethical Hacker & CyberSec

LIVRO: Encarregados/DPO

Comentar "PRESENTE" em:
https://instagram.com/davisalvesphd

Minicurso
LGPD no Setor Público

anppd.org

Prof. Davis Alves, Ph.D
ICS MCSA | ITIL® Expert

Presidente da ANPPD
Membro do Conselho Nacional (CNPD)
Data Protection Officer
Ethical Hacker & CyberSec

Encarregados | Data Protection Officers - DPOs exigidos pela LGPD - Lei Geral de Proteção de Dados - 13.709/2018 BR

SEJA MEMBRO:
➔ https://anppd.org/cadastro

Esteja entre os melhores!

anppd.org

Presidente da ANPPD
Membro do Conselho Nacional (CNPD)
Data Protection Officer
Ethical Hacker & CyberSec

Prof. Davis Alves, Ph.D
ICS MCSA | ITIL® Expert

Encarregados | Data Protection Officers - DPOs exigidos pela LGPD - Lei Geral de Proteção de Dados - 13.709/2018 BR

SEJA MEMBRO:

➔ https://anppd.org/cadastro