



FORMAÇÃO  
PROFISSIONAL DE  
**PRIVACIDADE**  
DE DADOS (LGPD)



# FORMAÇÃO PROFISSIONAL DE **PRIVACIDADE** DE DADOS (LGPD)



Realização



Apoadores



Módulo

---



# Segurança e Boas Práticas *Teórica & Prática*



**Presidente da ANPPD**

@davisalvesphd



**Segurança da Informação, Data Protection Officer (DPO), Chief Information Security Officer (CISO - ISO-27001 Professional, ITIL® Expert, System Administrator (ICS MCSA®), Ethical Hacker, Cyber Security & Cloud Computing Certified.**

- ❖ Professor na UNIP/USCS/UFSCar/Daryus/Faculdade Impacta
- Tecnólogo em Redes de Computadores
- Pós-graduado em Gerenciamento de Projetos
- Mestre em Administração com foco em TI
- Doutor em Administração com foco em TI  
Ph.D pela Florida Christian University nos Estados Unidos.

# Em qual parte da lei estamos?

## CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS

Artigos 46 ao 51

Seção I - Da Segurança e do Sigilo de Dados – artigos 46 ao 49

Seção II - Das Boas Práticas e da Governança – artigos 50 e 51



# Seção I

---

## Da Segurança e do Sigilo de Dados

# Adoção de medidas

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.

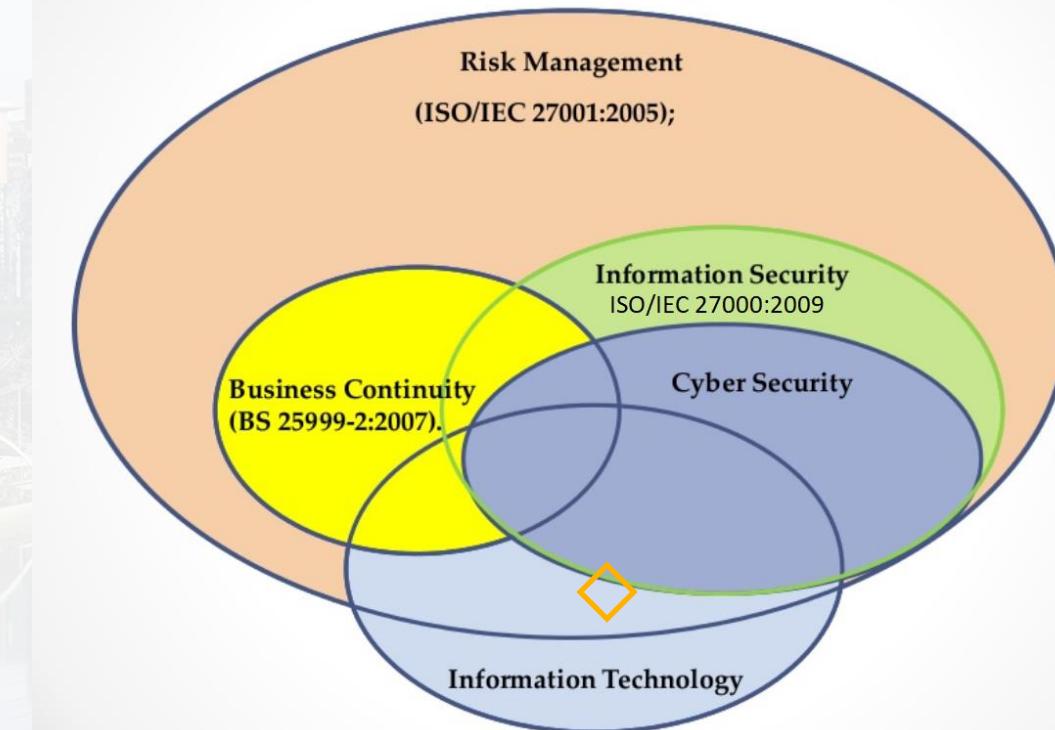
Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

# Adoção de medidas

## Segurança da Informação

### 3 Tipos de Medidas de Segurança:

- ✓ SEGURANÇA FÍSICA
- ✓ SEGURANÇA TÉCNICA
- ✓ SEGURANÇA ORGANIZACIONAL

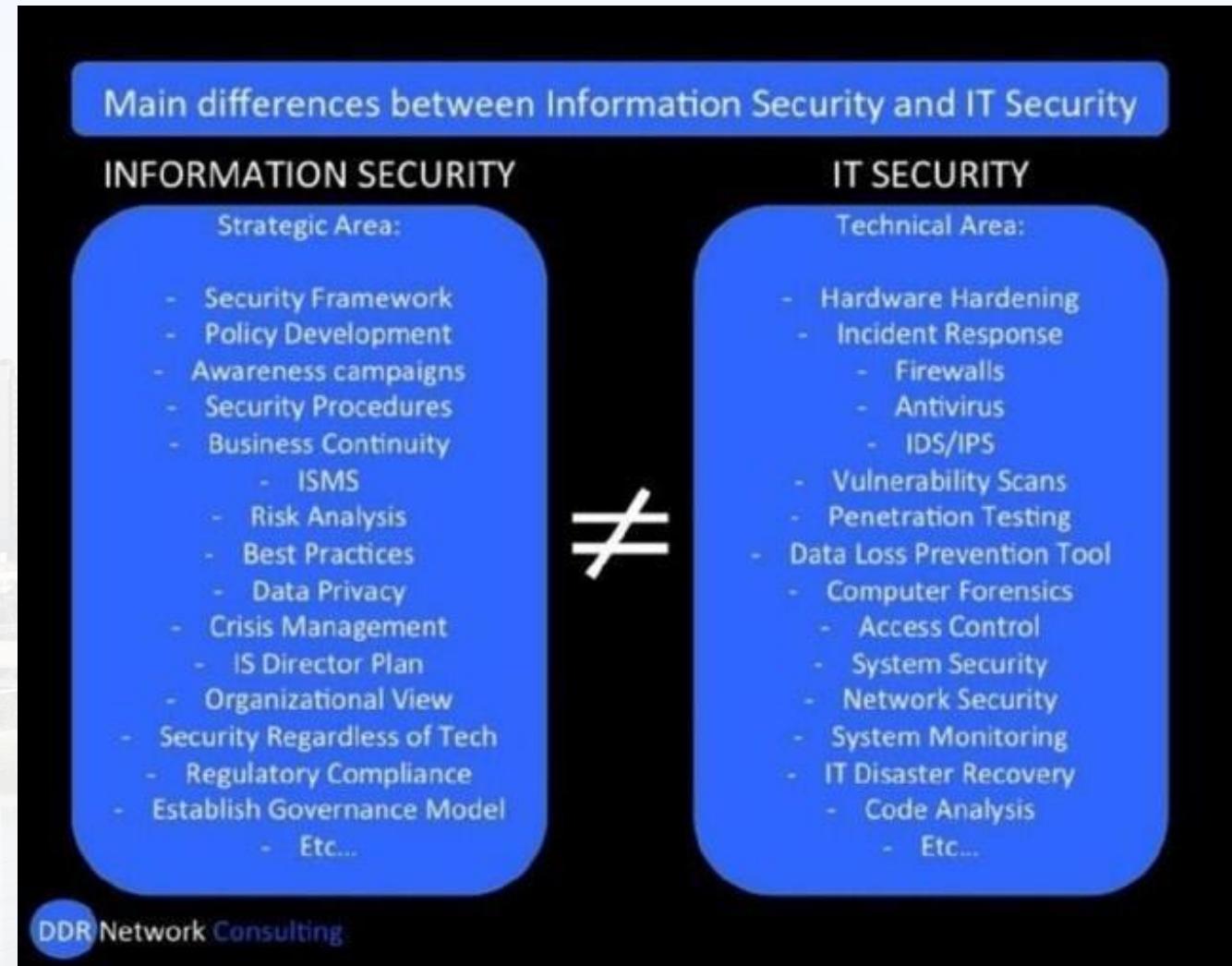


# Adoção de medidas

## Segurança da Informação

### 3 Tipos de Medidas de Segurança:

- ✓ SEGURANÇA FÍSICA
- ✓ SEGURANÇA TÉCNICA
- ✓ SEGURANÇA ORGANIZACIONAL



# Comunicação do incidente de segurança

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

- § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

- I - a descrição da natureza dos dados pessoais afetados;
- II - as informações sobre os titulares envolvidos;
- III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- IV - os riscos relacionados ao incidente;
- V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

## Seção II

# Das Boas Práticas e da Governança



# Modelos para Governança

## Modelo de Competência BPM

Habilidades Competências

Analista de Processos

Conhecimento Experiência

BPM CBOK

Certificação

CBPA  
Certified Business Process Associate

Arquiteto de Processos

BPM  
Experiência em Projeto

CBPP  
Certified Business Process Professional

Arquiteto Chefe de Processos

BPM  
Experiência em Transformação

CBPL  
Certified Business Process Leader



Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular **regras de boas práticas e de governança** que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Art. 50. § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

- I - implementar programa de governança em privacidade que, no mínimo:
  - a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
  - b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
  - c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
  - d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

Art. 50. § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

- I - implementar programa de governança em privacidade que, no mínimo:
  - e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
  - f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
  - g) conte com planos de resposta a incidentes e remediação; e
  - h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

# Objetivos de controles da ISO 27001

Controles são todas as medidas administrativas, processuais e tecnológicas a serem adotadas



Implantação do SGSI

Políticas de Segurança

Organização da Informação

Gestão de Ativos

Controle de Acessos

Criptografia

Segurança Física e Ambiental

Segurança das Operações

Aquisição de Sistemas,  
Desenvolvimento e Manutenção

Transferência de Informações

Relação com Fornecedores

Gestão de Incidentes de Segurança

Continuidade do Negócio

Cumprimento de requisitos legais e  
contratuais

- No § 1º do Artigo 50 da LGPD diz que tanto o controlador quanto o operador devem estabelecer regras de boas práticas de segurança em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.



Direitos reservados – Uso exclusivo para estudo e exemplificação do modelo. Permitido reprodução com citação da fonte.

# Cyber-ataques em tempo real



# Já tive dados pessoais vazados?

The screenshot shows a web browser window with the URL <https://haveibeenpwned.com/>. The page has a dark blue header with navigation links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below the header is a large white button with the text '';--have i been pwned?'. Underneath it, a subtext reads 'Check if you have an account that has been compromised in a data breach'. A search form contains a text input 'email address' and a button 'pwned?'. Below the search area, there's a call-to-action for password generation: 'Generate secure, unique passwords for every account' with a link to 'Learn more at 1Password.com'. The main content area displays four large numbers: '454 pwned websites', '9,760,722,439 pwned accounts', '112,905 pastes', and '135,168,575 paste accounts'. At the bottom, there are two sections: 'Largest breaches' and 'Recently added breaches', each listing several breached services with their respective account counts.

email address **pwned?**

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

454	9,760,722,439	112,905	135,168,575
pwned websites	pwned accounts	pastes	paste accounts

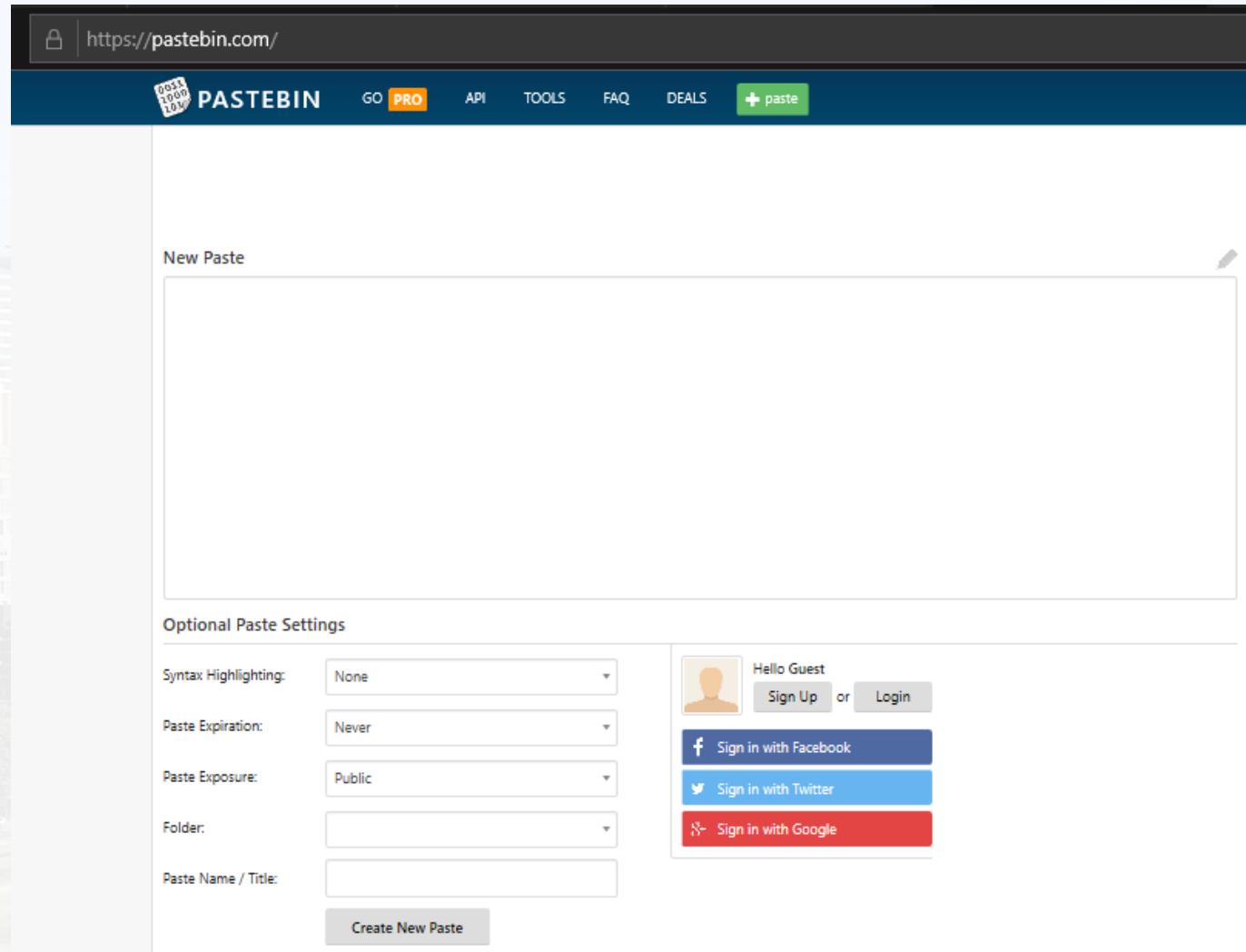
**Largest breaches**

	772,904,991 Collection #1 accounts
	763,117,241 Verifications.io accounts
	711,477,622 Onliner Spambot accounts
	622,161,052 Data Enrichment Exposure From

**Recently added breaches**

	25,692,862 Mathway accounts
	3,589,795 Zoomcar accounts
	68,693,853 Lead Hunter accounts
	9,705,172 Wishbone (2020) accounts

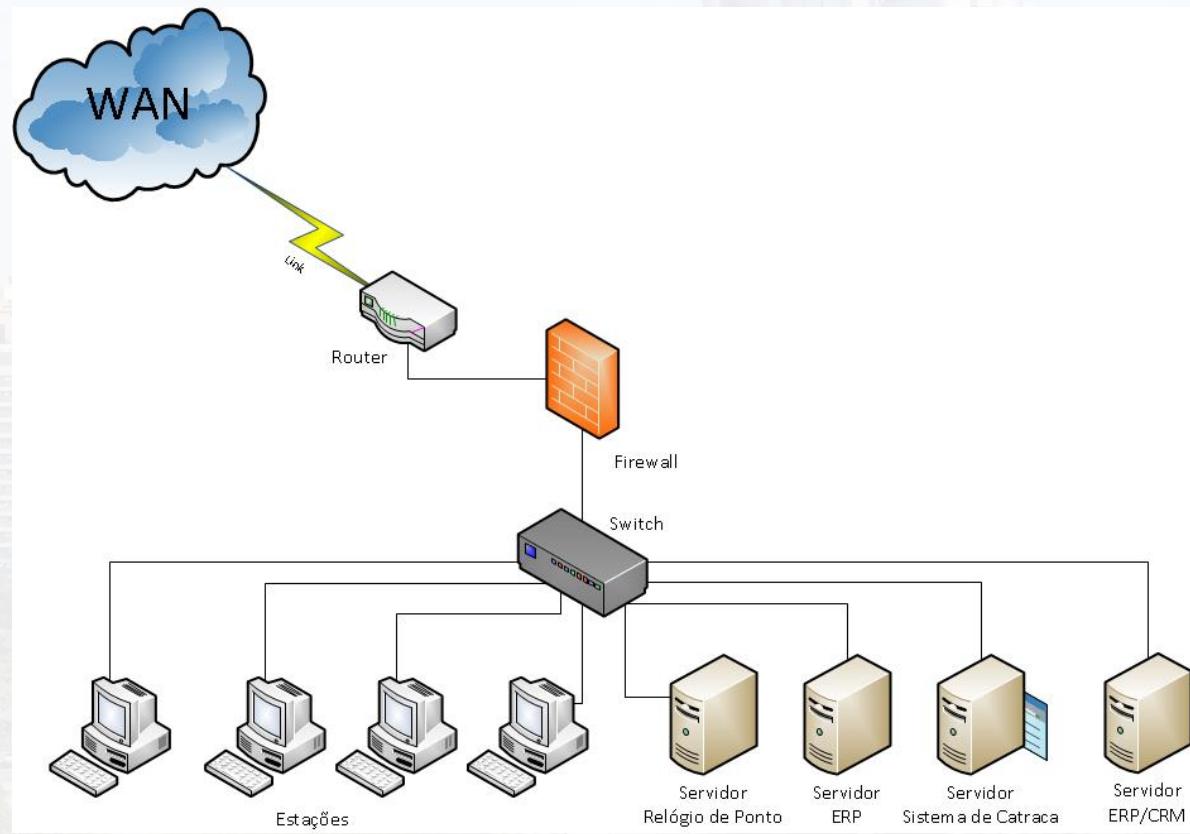
# Para onde vão os dados pessoais vazados?



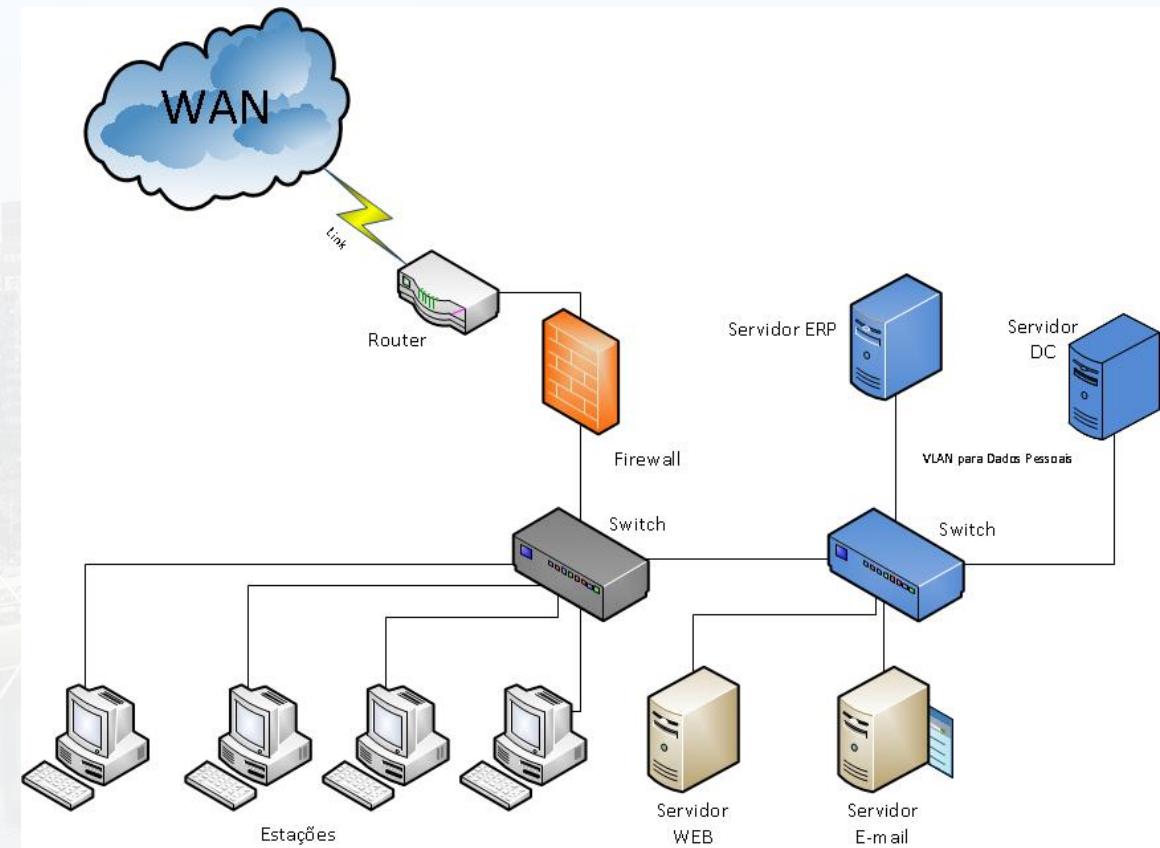
The screenshot shows the Pastebin website at <https://pastebin.com/>. The page has a dark header with a lock icon, the URL, and the Pastebin logo. Below the header is a navigation bar with links for GO PRO, API, TOOLS, FAQ, DEALS, and a green '+ paste' button. The main content area is titled 'New Paste' and contains a large text input field. Below this is a section for 'Optional Paste Settings' with dropdown menus for Syntax Highlighting (None), Paste Expiration (Never), Paste Exposure (Public), and Folder. There is also a text input for Paste Name / Title and a 'Create New Paste' button. To the right of these settings is a user profile section for 'Hello Guest' with 'Sign Up' and 'Login' buttons, and social media sign-in options for Facebook, Twitter, and Google.

# Segurança em Topologias de Redes de Computadores

## Topologia Tradicional

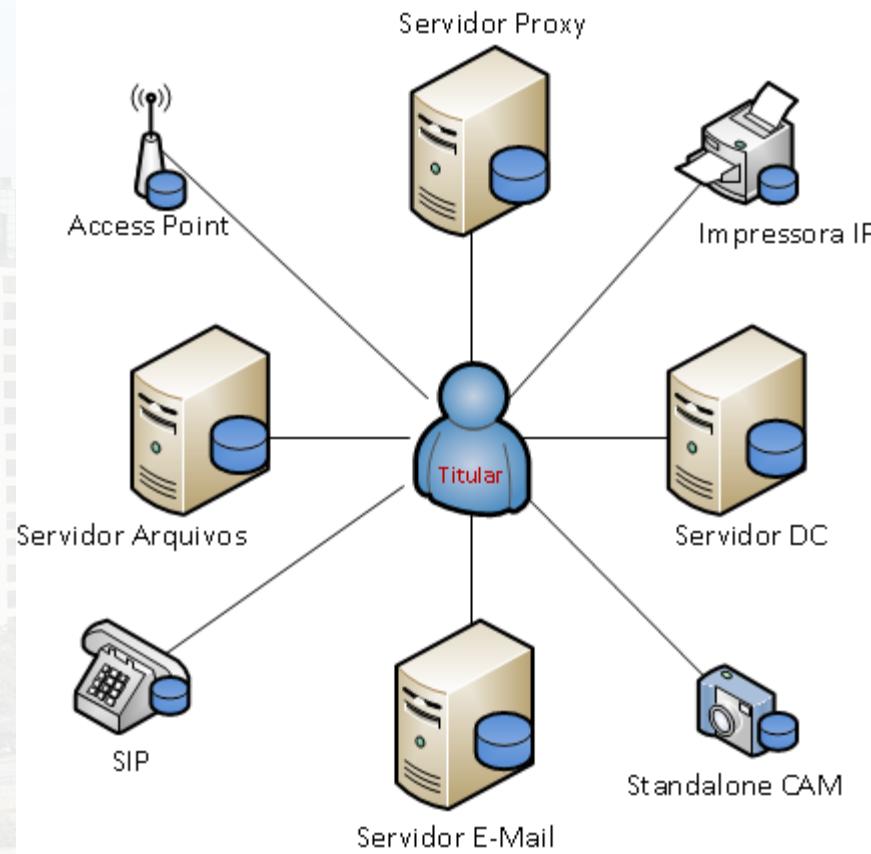


## Topologia com Dados Pessoais

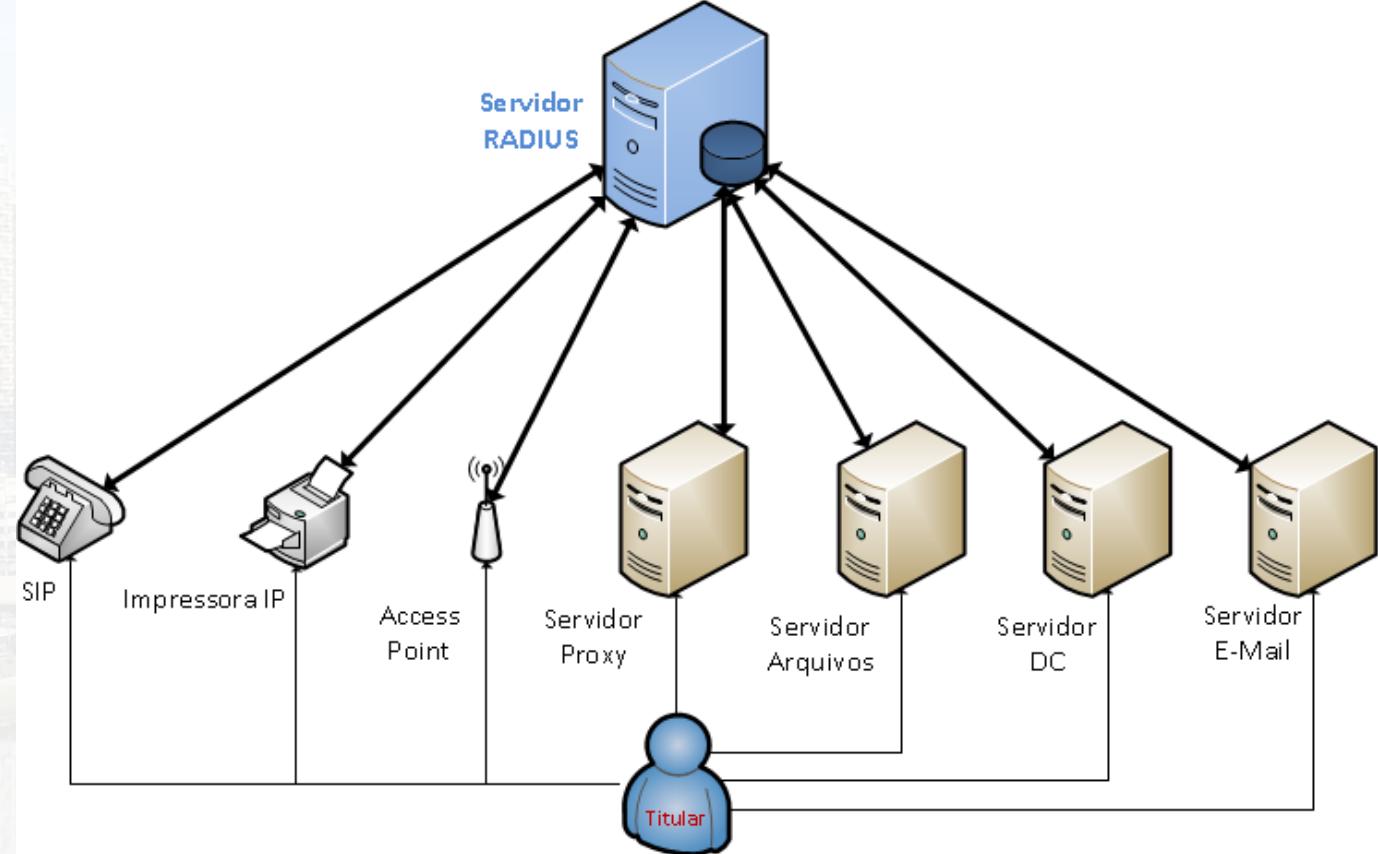


# Segurança em Topologias de Redes de Computadores

## Topologia Tradicional



## Topologia com Dados Pessoais



# Tabela de Medidas de Segurança por ATIVO

*Exemplo: Proteção para um Servidor de Rede com Dados Pessoais*

Segurança Organizacional	- Cadastro dos usuários autorizados	- Assinatura Digital	- Auditoria de Conteúdo	- Destinação para empresa autorizada
Segurança Técnica	- Usar com senha	- VPN	- Criptografia	- Sanitização de Dados
Segurança Física	- Usar em local seguro	- Link dedicado	- Rack de Telecom	- Triturar
Medidas de Seg. da Informação vs Ciclo de Vida da Informação →	<b>Manuseio</b>	<b>Transporte</b>	<b>Armazenamento</b>	<b>Descarte</b>
	<i>Analista Segurança</i>		<i>Administrador de Redes</i>	<i>Analista Segurança</i>

# Direitos do Titular

Estudo de Caso Público: ANPPD.org

The screenshot shows a web browser window with the URL <https://anppd.org/cadastro>. The page is titled "FICHA DE CADASTRO" (Registration Form). It includes fields for First Name, Last Name, Email, Password, Confirmation, LinkedIn Profile Link, State selection, and a photo upload section. A red box highlights the photo requirements: "Padrão de foto: Traje social sem gravata, braços cruzados, fundo branco, foto da parte superior do corpo." Below the photo section, there's a dropdown for committee participation and a question about public profile visibility with "Sim" and "Não" options. A large blue "CRIAR" (Create) button is at the bottom.

ANPPD  
Associação Nacional dos Profissionais de Privacidade de Dados

FICHA DE CADASTRO  
Minimizada  
(Art. 6, III - LGPD)

PRIMEIRO NOME

ÚLTIMO NOME

E-MAIL

SENHA

CONFIRMAÇÃO DA SENHA

LINK DO PERFIL DO LINKEDIN

Estado

INSIRA SUA FOTO DE PERFIL

Browse... No file selected.

Padrão de foto:  
Traje social sem gravata, braços cruzados, fundo branco, foto da parte superior do corpo.

Selecionar o comitê que deseja participar

DESEJA DEIXAR SEU PERFIL PÚBLICO?

Sim  Não

CRIAR

# Segurança LGPD nos Portais WEB

Estudo de Caso Público:  
ANPPD.org

The screenshot shows a user profile page for ANPPD.org. At the top, there's a navigation bar with links for INÍCIO, QUEM SOMOS, NOTÍCIAS, EVENTOS, CONTATO, PARECERES TÉCNICOS, and a search bar labeled 'PESQUISAR'. Below the navigation is the ANPPD logo and a photo of a man in a suit. On the left, there's a sidebar with links for Alterar foto, Comitê Diretivo (highlighted in black), Cartão Digital, Editar Perfil, Alterar Senha, FAQ, Eventos, Biblioteca ANPPD, Situação Financeira, and Excluir cadastro. The main content area contains fields for Nome (Davis), Último Nome (Alves), E-mail (Davis@e-davis.net), LinkedIn (https://www.linkedin.com/in/davisalvesphd), Estado (São Paulo), and a dropdown for 'PERFIL PÚBLICO?' (Sim). There's also a field for 'Link validador do instituto:' with the URL https://app.exeed.pro/holder/badge/26476. At the bottom, there's a 'Certificado' section with a 'Browse...' button and a placeholder 'No file selected.' A digital certificate from EXIN for 'Data Protection Officer' is displayed.

# Segurança LGPD nos Portais WEB

Estudo de Caso Público:  
ANPPD.org



The screenshot shows a web browser window for https://anppd.org/user. The header includes social media links (Facebook, Instagram, LinkedIn, YouTube, Twitter), a search bar, and navigation tabs for MEMBROS, ÁREA DO ASSOCIADO, and SOLICITAR CONVITE. The main content area features the ANPPD logo and a navigation menu with links to INÍCIO, QUEM SOMOS, NOTÍCIAS, EVENTOS, CONTATO, PARECERES TÉCNICOS, and PESQUISAR. A large image of a man in a suit is displayed. Below the image are buttons for Alterar foto, Comitê Diretivo, and Cartão Digital. At the bottom of the page are links for Editar Perfil, Alterar Senha, FAQ, Eventos, Biblioteca ANPPD, Situação Financeira, and Excluir cadastro.

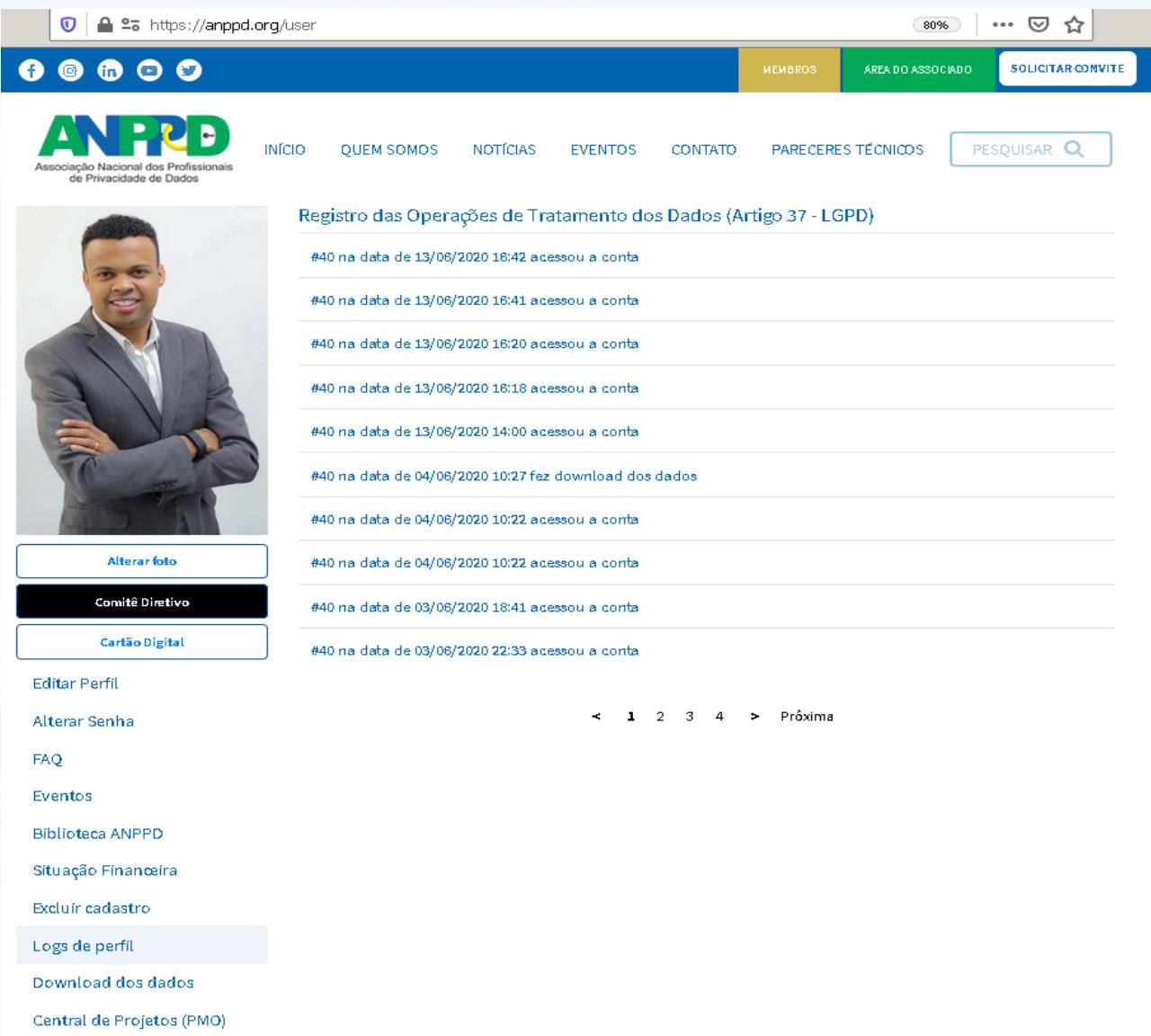
Direito de Eliminação dos Dados (Artigo 18, VI - LGPD)

Deseja excluir permanentemente seu cadastro da ANPPD? Esta ação é irreversível!

[Apagar](#)

# Segurança LGPD nos Portais WEB

Estudo de Caso Público:  
ANPPD.org



The screenshot shows a user profile page for ANPPD.org. At the top, there's a navigation bar with links for INÍCIO, QUEM SOMOS, NOTÍCIAS, EVENTOS, CONTATO, PARECERES TÉCNICOS, and a search bar labeled 'PESQUISAR'. Below the navigation is the ANPPD logo and the text 'Associação Nacional dos Profissionais de Privacidade de Dados'. To the left of the main content area is a large photo of a man in a suit with his arms crossed. Below the photo are several buttons: 'Alterar foto' (Change photo), 'Comitê Diretivo' (Directors Committee) which is highlighted in black, and 'Cartão Digital'. On the right side, under the heading 'Registro das Operações de Tratamento dos Dados (Artigo 37 - LGPD)', there is a list of data processing activities:

- #40 na data de 13/06/2020 16:42 acessou a conta
- #40 na data de 13/06/2020 16:41 acessou a conta
- #40 na data de 13/06/2020 16:20 acessou a conta
- #40 na data de 13/06/2020 16:18 acessou a conta
- #40 na data de 13/06/2020 14:00 acessou a conta
- #40 na data de 04/06/2020 10:27 fez download dos dados
- #40 na data de 04/06/2020 10:22 acessou a conta
- #40 na data de 04/06/2020 10:22 acessou a conta
- #40 na data de 03/06/2020 18:41 acessou a conta
- #40 na data de 03/06/2020 22:33 acessou a conta

At the bottom of the page, there are navigation links: 'Editor Perfil', 'Alterar Senha', 'FAQ', 'Eventos', 'Biblioteca ANPPD', 'Situação Financeira', 'Excluir cadastro', 'Logs de perfil' (which is highlighted in light blue), 'Download dos dados', and 'Central de Projetos (PMO)'. There are also page navigation arrows and a 'Próxima' (Next) button.

# Segurança LGPD nos Portais WEB

Estudo de Caso Público:  
ANPPD.org

The screenshot shows a web browser window for https://anppd.org/user. The header includes social media links, a logo for ANPPD (Associação Nacional dos Profissionais de Privacidade de Dados), and navigation menu items: INÍCIO, QUEM SOMOS, NOTÍCIAS, EVENTOS, CONTATO, PARECERES TÉCNICOS, and PESQUISAR. A 'MEMBROS' button is highlighted in yellow. A 'SOLICITAR CONVITE' button is also visible. Below the header, there's a large image of a man in a suit with his arms crossed. To the left of the image are buttons for 'Alterar foto', 'Comitê Diretivo', and 'Cartão Digital'. To the right, a section titled 'Direito de Portabilidade (Artigo 18, V - LGPD)' contains a message: 'Deseja fazer download dos seus dados?' followed by a red 'Download' button. A modal dialog box titled 'Abrir "1592077609.zip"' is displayed, showing file details: '1592077609.zip' (type: WinRAR ZIP archive (107 KB), de: https://cms.anppd.org). It asks 'O que o Firefox deve fazer?' with options: 'Abrir com o:' (selected, set to WinRAR archiver (aplicativo padrão)), 'Salvar arquivo (D)', and a checkbox for 'Fazer isso automaticamente nos arquivos como este de agora em diante.' Buttons for 'OK' and 'Cancelar' are at the bottom.

# Por onde começar a Política de Segurança?

Download PDF:

<https://www.instagram.com/p/B8MHW99J>

ANI/

The image shows the front cover of a white document titled 'Guia de implementação do SGSI' (ISO-27001 Project Plan). At the top is the ANPPD logo (green letters 'ANPPD' with a yellow 'P') and the text 'Associação Nacional dos Profissionais de Privacidade de Dados'. Below the title is a subtitle 'Plano de Projeto para os Requisitos da ISO-27001'. A large green and yellow shield graphic is centered on the cover. The text 'NOTA: O objetivo deste documento é ajudá-lo a reconhecer as atividades relacionadas ao estabelecimento de um SGSI. Este documento não deve ser considerado como consultoria profissional para estabelecer ou implementar um SGSI. O uso deste guia não garante uma implementação bem sucedida nem uma implementação pronta para certificação. Se você deseja implementar um SGSI, considere contratar um consultor profissional especializado na Implementação do SGSI.' is visible. At the bottom, it says 'ANPPD - Comitê de Conteúdo contato@anppd.org' and 'MODELO PARA DOMÍNIO PÚBLICO'.

The image shows the table of contents page of the same document. It features the ANPPD logo at the top right. The table of contents lists 15 numbered steps for SGSI implementation, each with a short description. Step 15 is 'Apêndices'. At the bottom, it says 'ANPPD - Comitê de Conteúdo contato@anppd.org' and 'MODELO PARA DOMÍNIO PÚBLICO'.

Índice
Visão geral de um SGSI
1. Adquira uma cópia dos padrões ISO / IEC
2. Obtenha suporte de gerenciamento
3. Determine o escopo do SGSI
4. Identifique a legislação aplicável
5. Defina um método de avaliação de risco
6. Crie um inventário de ativos de informações para proteger
7. Identifique os riscos
8. Avalie os riscos
9. Identifique objetivos e controles aplicáveis
10. Estabelecer políticas e procedimentos para controlar risco
11. Aloque recursos e treine a equipe
12. Monitore a implementação do SGSI
13. Prepare-se para a auditoria de certificação
14. Peça ajuda
15. Apêndices



**Davis Alves, Ph.D**

- Segurança da Informação
  - Presidente da ANPPD
- <https://instagram.com/davisalvesphd>

## Segurança e Boas Práticas *Teórica & Prática*



PERGUNTAS?