Frameworks para Proteção e Privacidade de Dados

Sobre o Palestrante

Fernando Fonseca, CISSP-ISSAP, CISM, ISO 27001 LA, CHFI, MCSE Security, Security+, ACE

- Instrutor desde 1993, certificado pela Microsoft, CA, Conectiva, EC-Council, PCI e EXIN
- Trabalha com Segurança da Informação desde 1999
- Professor em cursos de graduação e pós-graduação
- Presidente do capítulo Belo Horizonte da ISACA
- Ex-Vice-presidente do ISSA Brasil Chapter
- Palestrante e autor de artigos em diversas práticas de Segurança da Informação
- Sócio Diretor na Antebellum Capacitação Profissional
- Chief Visionary Officer e Data Protection Officer na Privally Management Software

LinkedIn br.LinkedIn.com/in/ferfon

Segurança da Informação

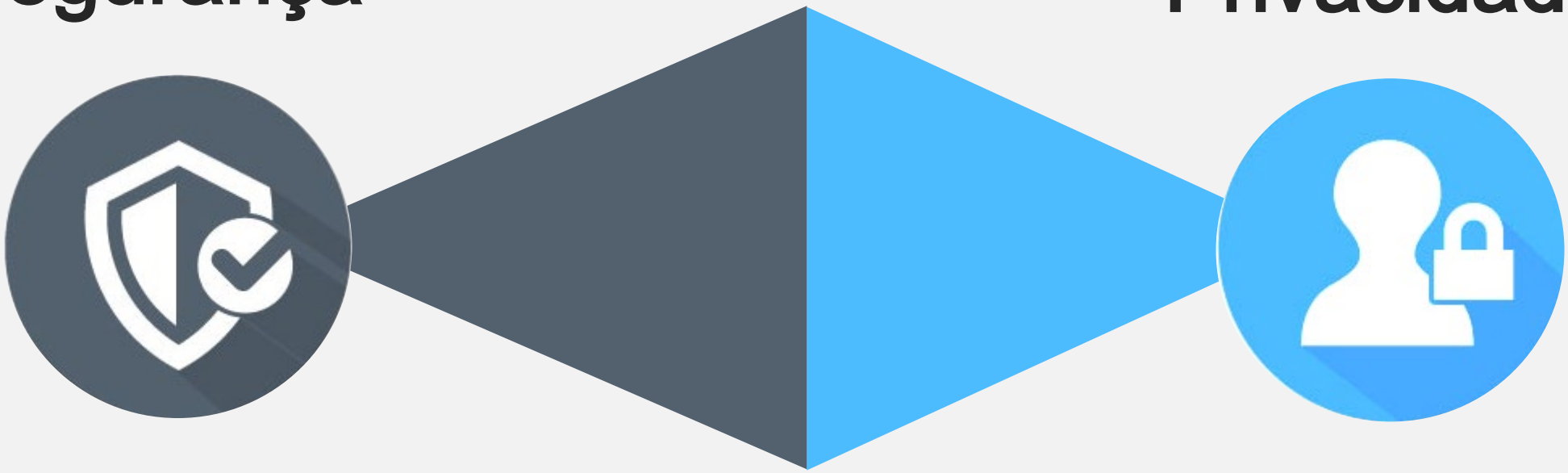
- Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
  - VII - segurança: **utilização de medidas técnicas e administrativas** aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
  - I - o modo pelo qual é realizado;
  - II - o resultado e os riscos que razoavelmente dele se esperam;
  - III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
  - Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, **ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano**.
- 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**.

Tu te tornas eternamente responsável por todos os dados que coletas

Segurança x Privacidade

Nome	Roberto Coinbra
E-mail	roberto@coinbrasa.com.br
CPF	222.449.876-90
Endereço	Rua do Bosque, 34 - São Paulo

Segurança



Privacidade

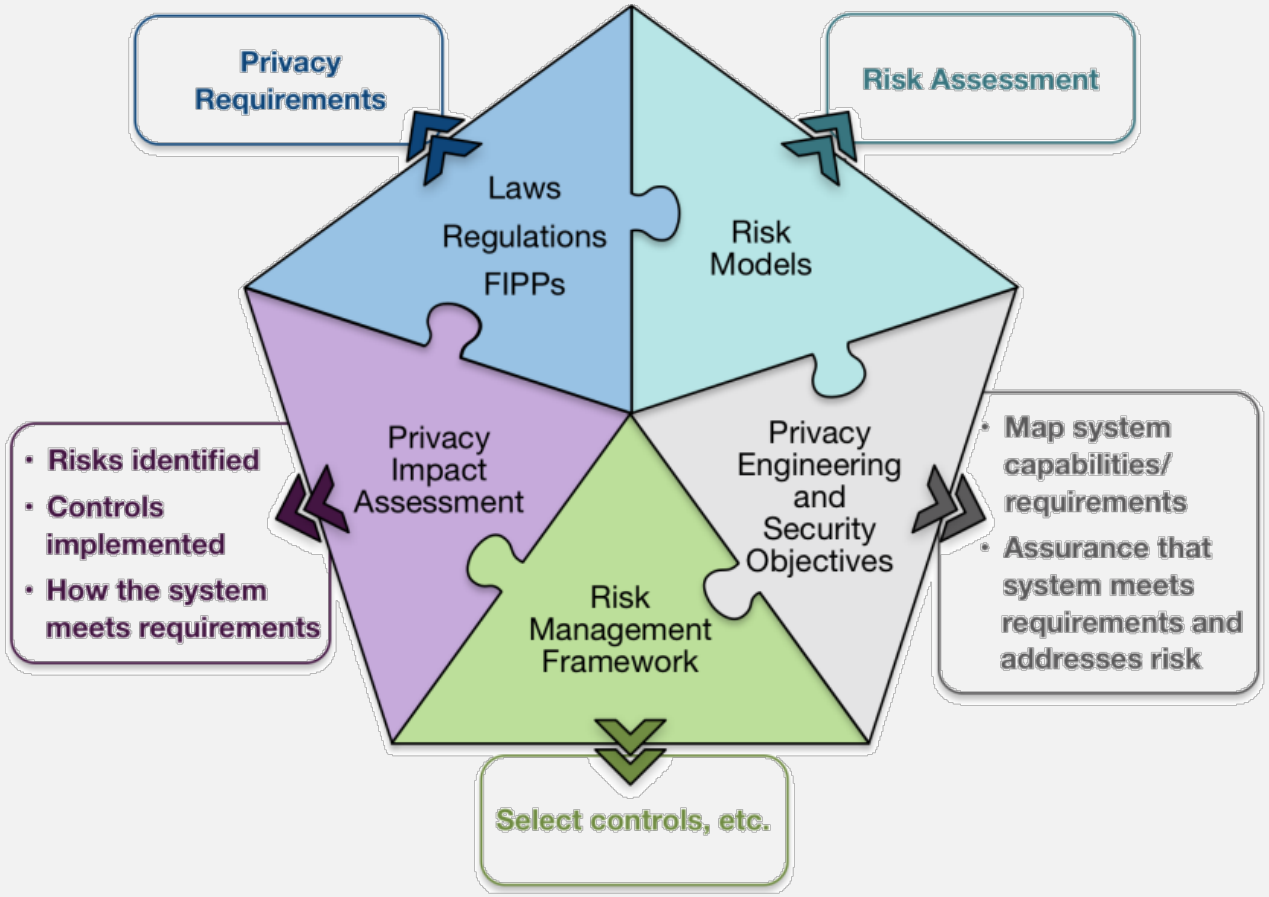
Ex. Esse dado está armazenado em um local seguro?

Ex. Posso processar e armazenar esse dado?

An Introduction to Privacy Engineering and Risk Management in Federal Systems

Chapter 2:
An Engineering Approach to Privacy

- 2.1 The Relationship Between Information Security and Privacy
- 2.2 Privacy Problems and Information Systems
- 2.3 Defining Privacy Engineering
- 2.3.1 The Applicability of Systems Engineering
- 2.3.2 The Utility of Risk Management

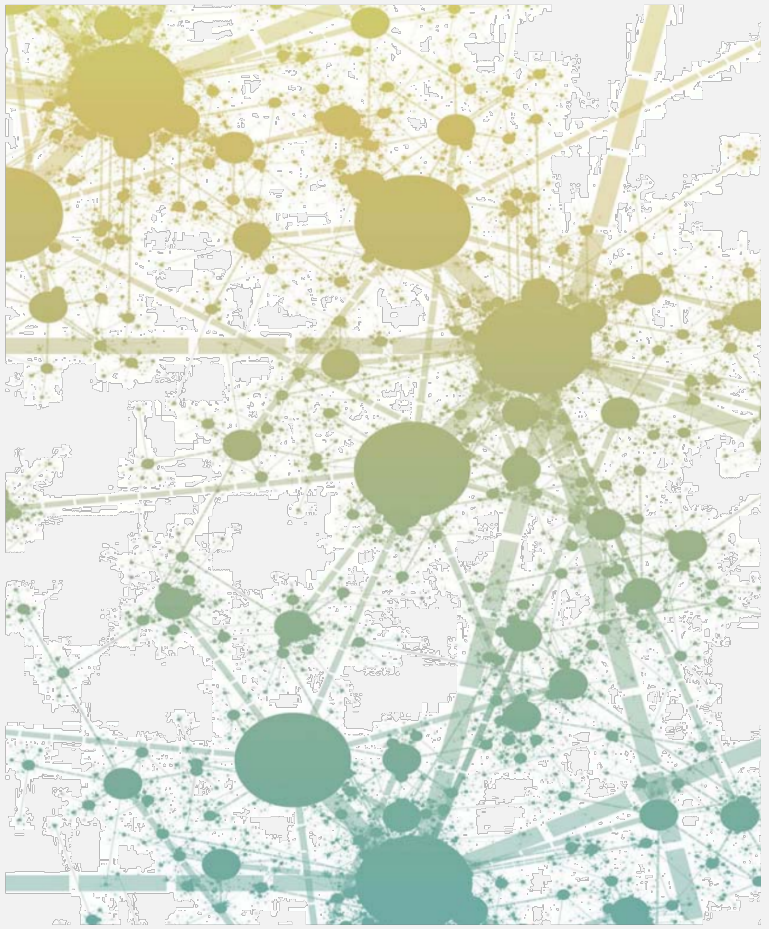


Chapter 3:
Tools for Privacy Engineering in Federal Information Systems

- 3.1 Introducing Privacy Engineering Objectives
- 3.1.1 Privacy Engineering Objectives and the FIPPs
- 3.2 Introducing a Privacy Risk Model
- 3.2.1 Privacy Risk Factors
- 3.2.2 Privacy Risk Characteristics

THE OECD PRIVACY FRAMEWORK

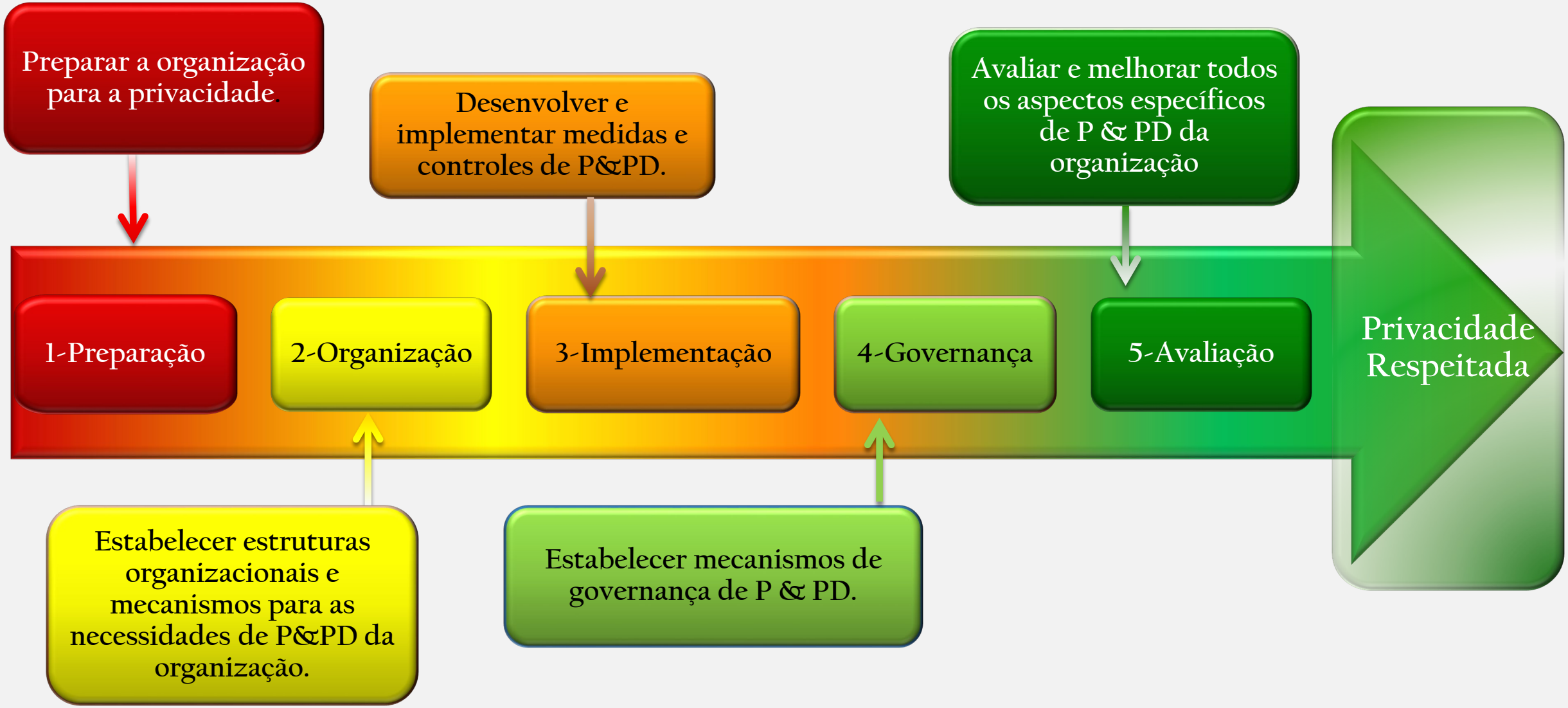
- Chapter 1. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)
- Chapter 2. Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)
- Chapter 3. Original Explanatory Memorandum to the OECD Privacy Guidelines (1980)
- Chapter 4. The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (2011)



Generally Accepted Privacy Principles

- GAPP can be used by organizations for the following:
  - Designing, implementing, and communicating privacy policy
  - Establishing and managing privacy programs
  - Monitoring and auditing privacy programs
  - Measuring performance and benchmarking
- Establishing and managing a privacy program involves the following activities:
- Strategizing. Performing privacy strategic and business planning.
  - Diagnosing. Performing privacy gap and risk analyses.
  - Implementing. Developing, documenting, introducing, and institutionalizing the program's action plan, including establishing controls over personal information.
  - Sustaining and managing. Monitoring activities of a privacy program.
  - Auditing. Internal or external auditors evaluating the organization's privacy program.

Fases de uma SGPD



Fonte: J. Kyriazoglou

Fase 1 – Preparação

Objetivos, passos e ações

Objetivos

- Analise os requisitos e necessidades de P&PD
- Coletar leis, regulamentos e normas relevantes
- Estabelecer um plano de ação

Passos e ações

1. Realizar análise de privacidade
2. Coletar de privacidade
3. Analisar o impacto da privacidade
4. Auditar e avaliações iniciais de dados
5. Estabelecer organização de governança de dados
6. Estabelecer fluxos de dados e inventário de dados pessoais
7. Estabelecer programa de P&PD
8. Desenvolver planos de implementação

Meta:

Preparar a organização para a privacidade.

Fase 2 – Organização

Fase 2 – Objetivos, passos e ações

Objetivos

- Projetar e configurar o programa P&PD
- Nomear um oficial de proteção de dados (DPO)
- Envolver-se e obter o compromisso de todas as partes interessadas relevantes

Meta:

Estabelecer estruturas organizacionais e mecanismos para as necessidades de P&PD da organização.

Passos e ações

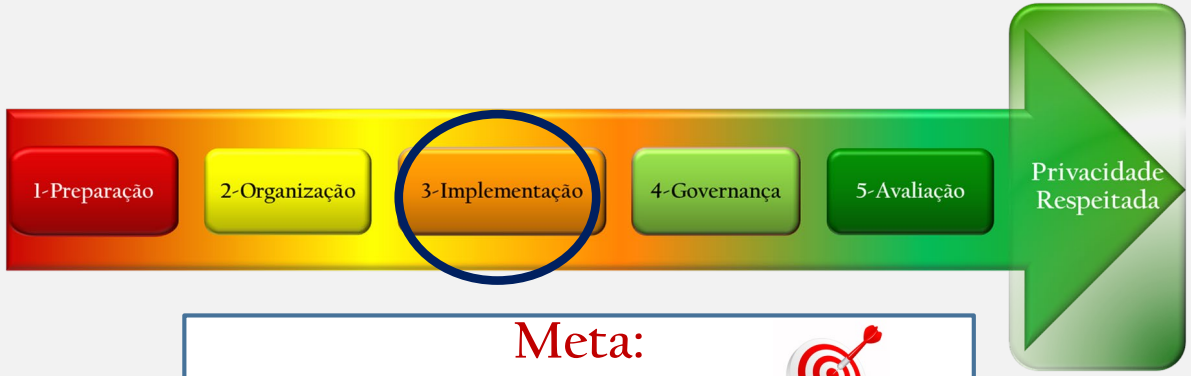
1. Gerenciar programa, políticas e mecanismos de governança de proteção de dados
2. Atribuir e gerenciar responsabilidades de privacidade e proteção de dados (RACI)
3. Gerenciar o envolvimento da gerência sênior em P&PD.
4. Gerenciar o comprometimento com a privacidade e proteção de dados
5. Gerenciar comunicações regulares para questões de privacidade e proteção de dados
6. Gerenciar o envolvimento das partes interessadas (stakeholders) em assuntos de P&PD
7. Implementar e operar sistemas computadorizados de proteção de dados

Fase 3 – Implementação

Implementação da proteção de dados e privacidade

Objetivos

- Projetar um sistema de classificação de dados;
- Desenvolver e implementar políticas, procedimentos e controles



Meta:

Desenvolver e implementar medidas de controles de P&PD.

Etapas e ações

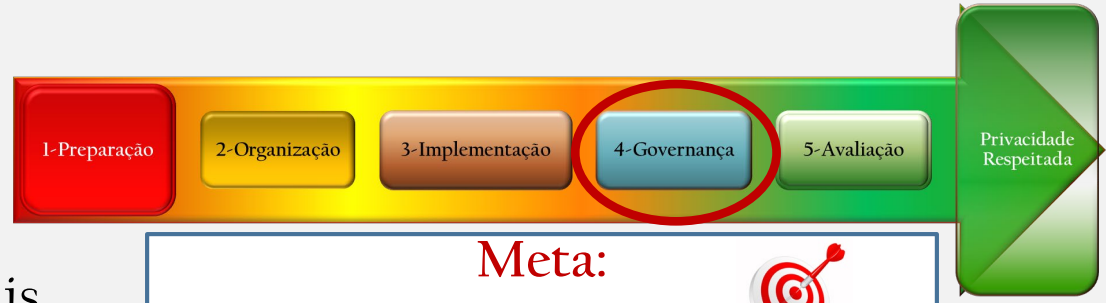
1. Desenvolver e implementar estratégias, planos e políticas;
2. Implementar procedimento de aprovação para processamento;
3. Registre bancos de dados para dados pessoais;
4. Desenvolver e implementar um sistema de transferência de dados transfronteiriço;
5. Executar atividades de integração;
6. Execute o plano de treinamento;
7. Implementar controles de segurança de dados.

Fase 4 – Governança

Objetivos, passos e ações

Objetivos

- Elaborar e configurar estruturas de governança; por exemplo.
- Programa de P&PD, oficial de proteção de dados, etc.
- Envolver e comprometer todas as partes interessadas relevantes
- Relatar todos os problemas de P&PD (processo contínuo)



Meta:

Estabelecer mecanismos de governança de P&PD

Passos e ações

1. Implementar práticas para gerenciar o uso de dados pessoais
2. Manter avisos de privacidade sobre dados pessoais
3. Executar um plano de solicitações, reclamações e retificação.
4. Executar uma avaliação de risco de proteção de dados e privacidade
5. Emitir relatórios de P&PD
6. Manter documentação
7. Estabelecer e manter um plano de resposta de violação de dados

Fase 5 – Avaliação

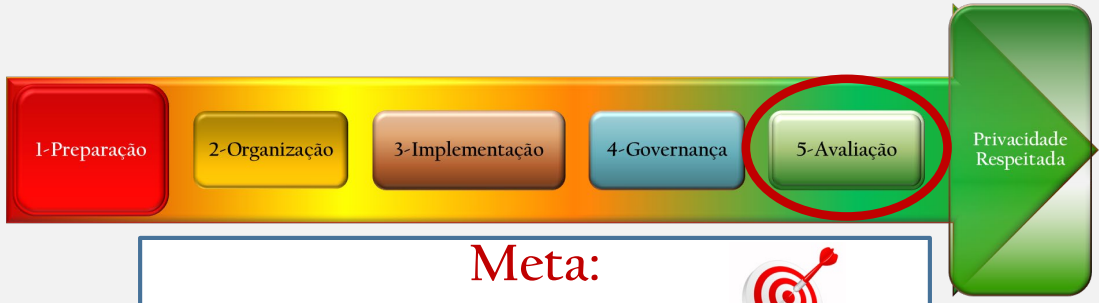
Objetivos, passos e ações

Objetivos

- Monitore a operação e a resolução de todas questões relacionados à privacidade
- Avaliar regularmente a conformidade com processos e políticas internas
- Melhorar a proteção de dados e medidas de privacidade

Passos e ações

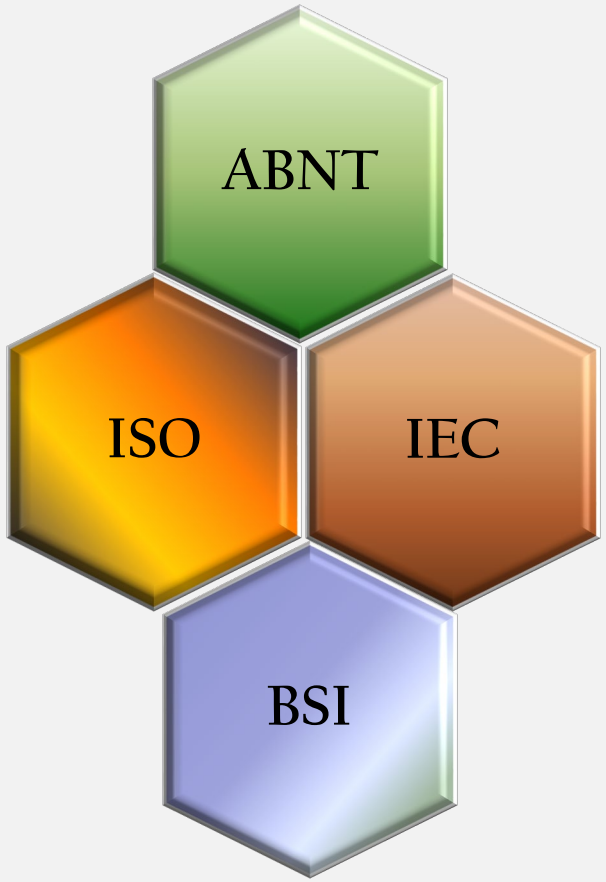
1. Realize a auditoria interna.
2. Contratar parte externa para avaliações
3. Realizar avaliações e estabelecer benchmarks
4. Execute um DPIA
5. Resolver riscos
6. Relatório Análise de riscos e resultados
7. Monitore leis e regulamentos

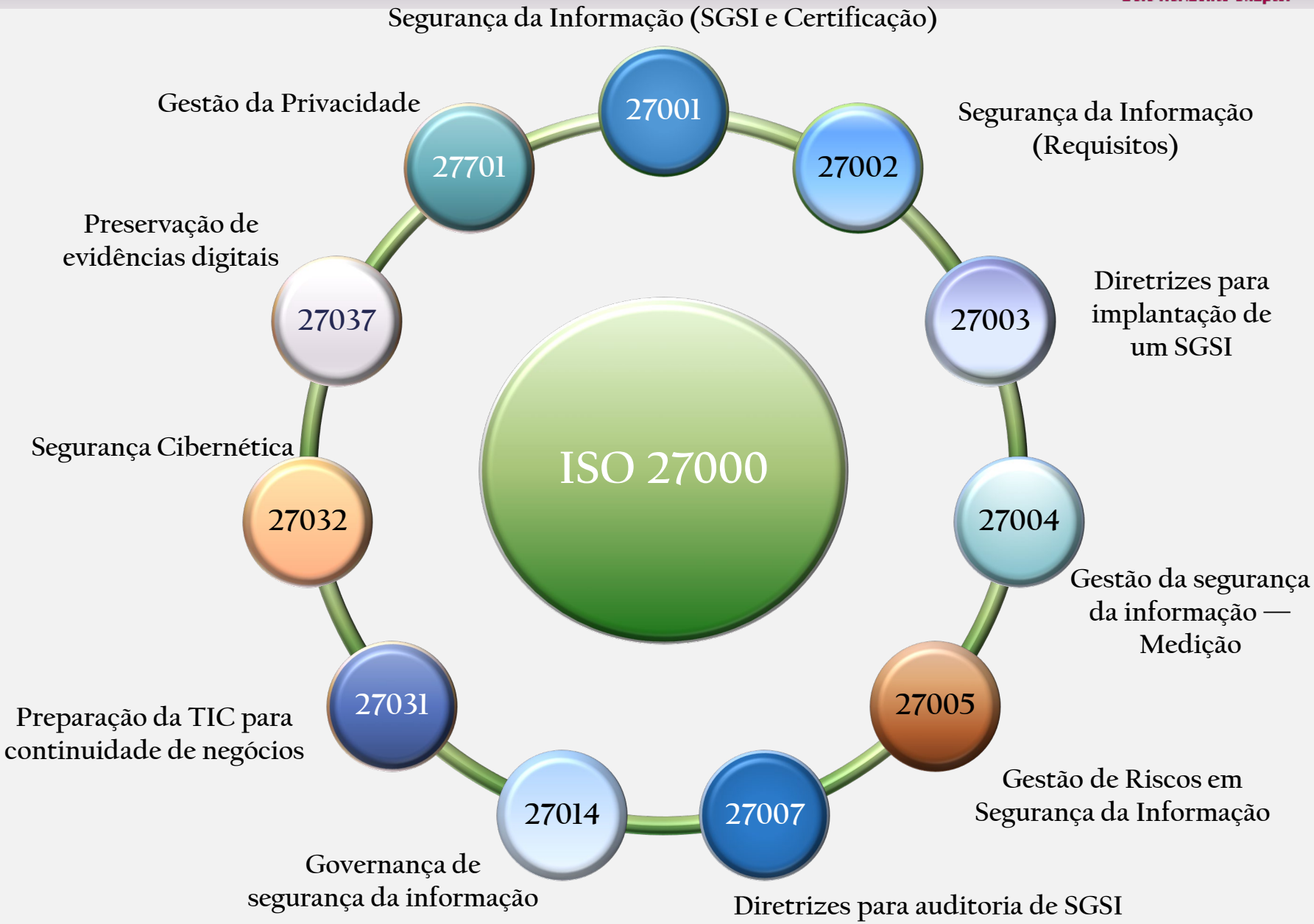


Meta:

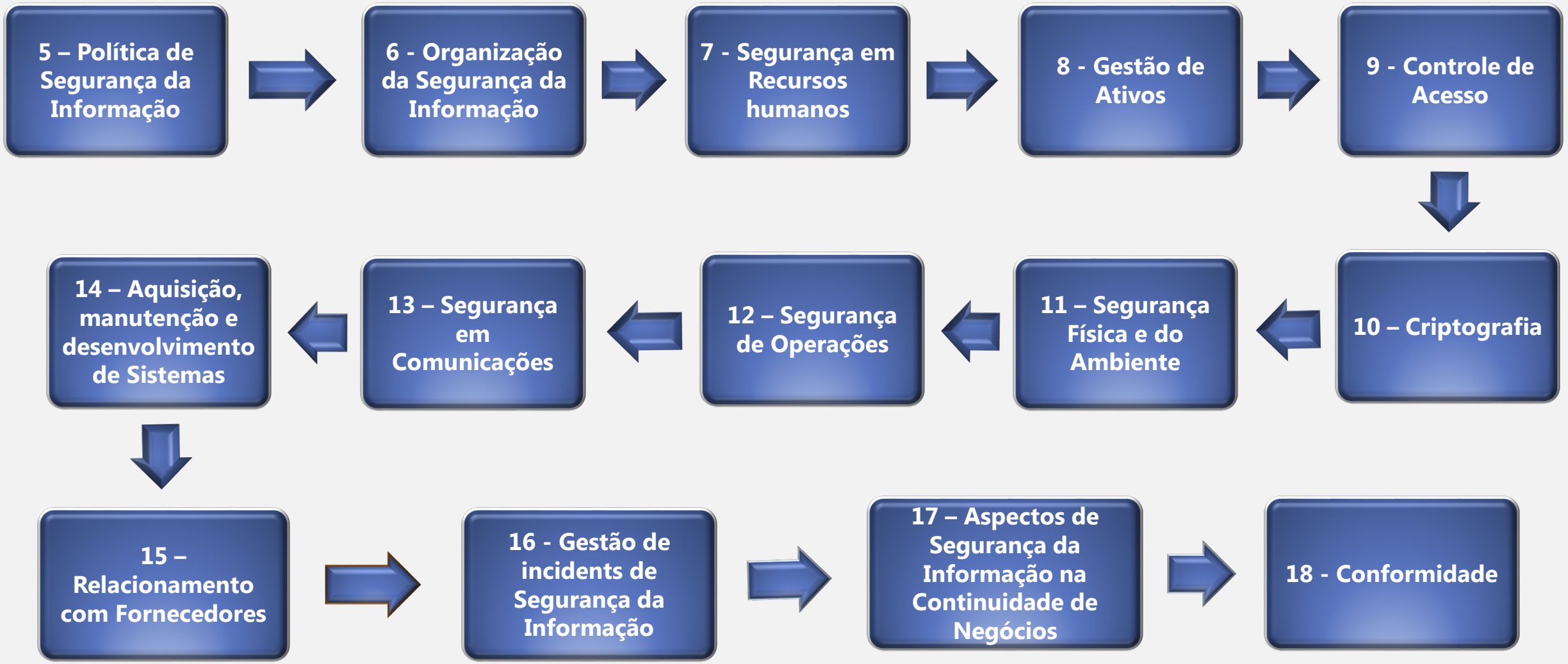
Avaliar e melhorar todos os aspectos específicos de P&PD da organização

A Família ISO 27000





Seções da ISO 27002



Norma de Referência - Não Auditável

ISO 27701 – Privacidade de Dados

ISO 27701
Privacidade de Dados

O SGSI da 27001, é projetado para permitir a adição de requisitos, sem a necessidade de desenvolver um novo Sistema de Gestão.

- ✓ A 27701 estabelece um Sistema de Gestão de Privacidade da Informação (SGPI) como uma extensão das 27001 e 27002 para a gestão da privacidade
- ✓ Depende das normas ISO 27001, 27002 e 29100 para sua implementação
- ✓ Amplia os requisitos da ISO 27001, levando em consideração a proteção da privacidade dos titulares de DP

ISO 27701
Privacidade de Dados

Exemplos de extensão de controles da ISO 27001

- ✓ Onde encontramos "segurança da informação" ISO 27001 devemos considerar “segurança da informação e privacidade"

6.5.3.3 - Transferência física de mídias

- ✓ O controle, as diretrizes para implementação e outras informações estabelecidas na ABNT NBR ISO/IEC 27002:2013, 8.3.3, e as seguintes diretrizes adicionais se aplicam.

As diretrizes adicionais para implementação do controle 8.3.3 são:

- ✓ .....
- ✓ Convém que a organização submeta a mídia física contendo DP a um procedimento de autorização antes de deixar as suas instalações e que assegure que o DP não seja acessível para qualquer outra pessoa que não o pessoal autorizado

ISO 27701
Privacidade de Dados

Exemplo de diretrizes adicionais da ISO 27002 através da ISO 27701:

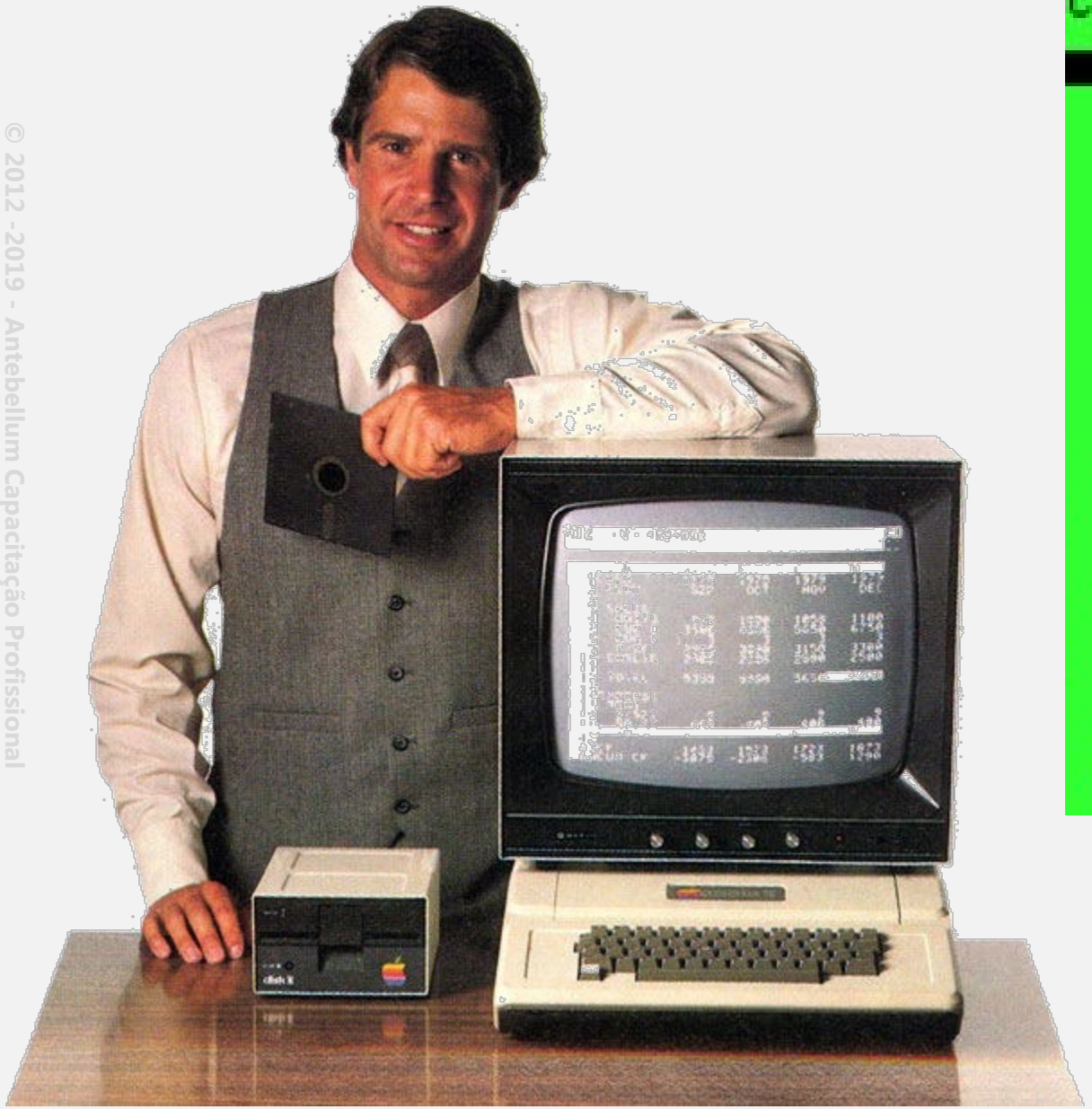
7.2 - Condições para coleta e tratamento

Objetivo: Determinar e documentar que o tratamento é lícito, com bases legais, conforme as jurisdições aplicáveis, e com propósitos legítimos e claramente estabelecidos.

7.2.1 - Propósito da identificação e documentação

- ✓ Controle: Convém que a organização identifique e documente os propósitos específicos pelos quais os DP serão tratados
- ✓ Diretrizes para implementação: Convém que a organização assegure que os titulares de DP entendam o propósito para os quais os seus DP serão tratados.

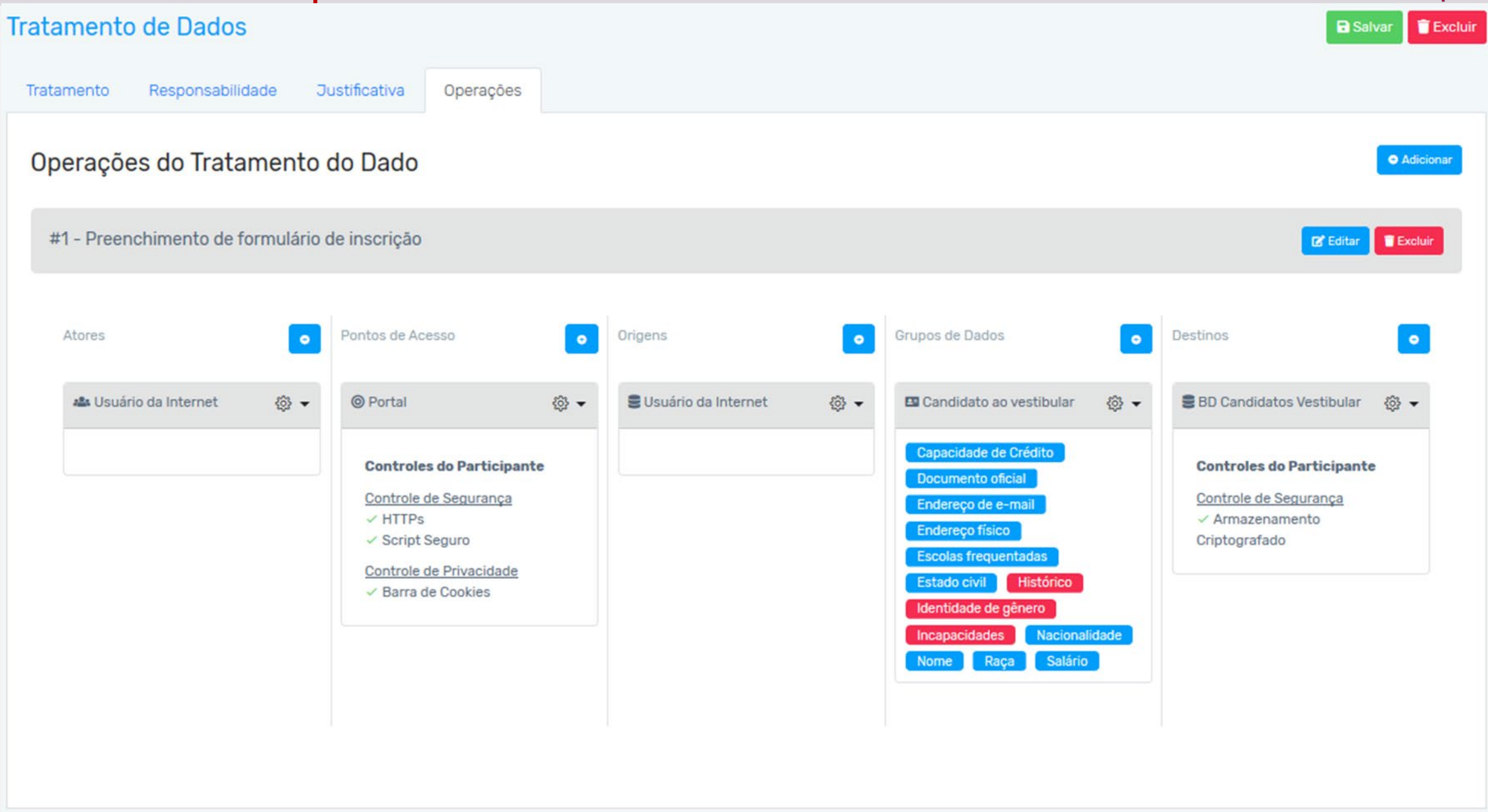
Planilhas foram criadas para Cálculos (Visicalc 1979)



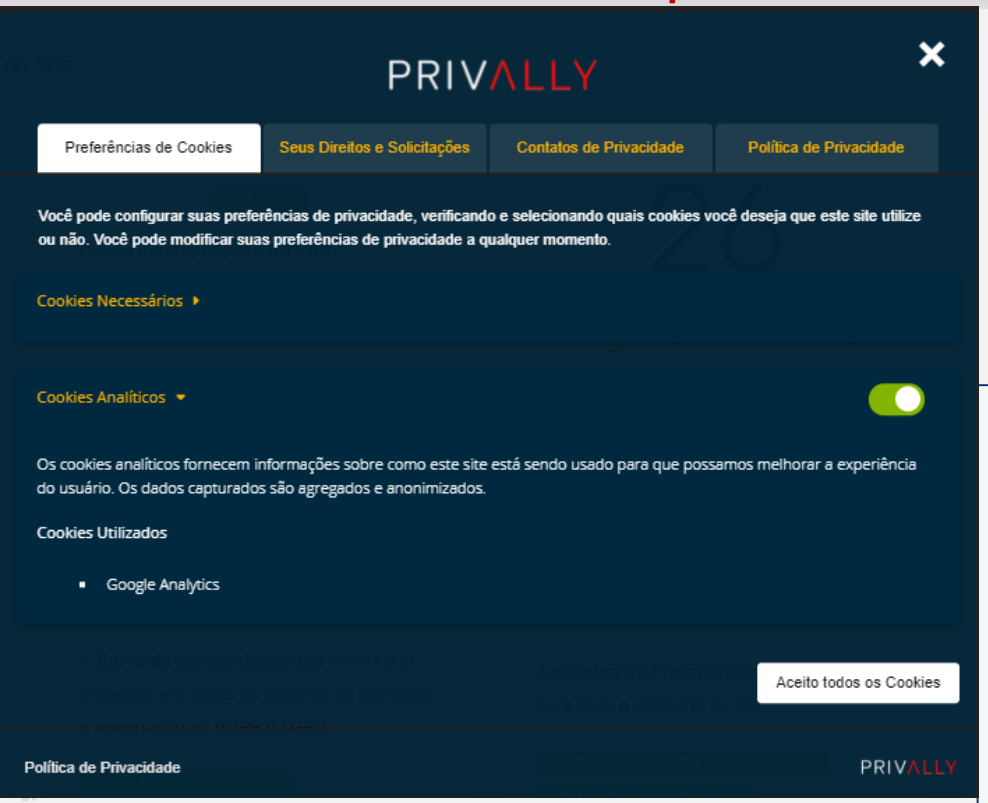
C11 (L) TOTAL C1
25

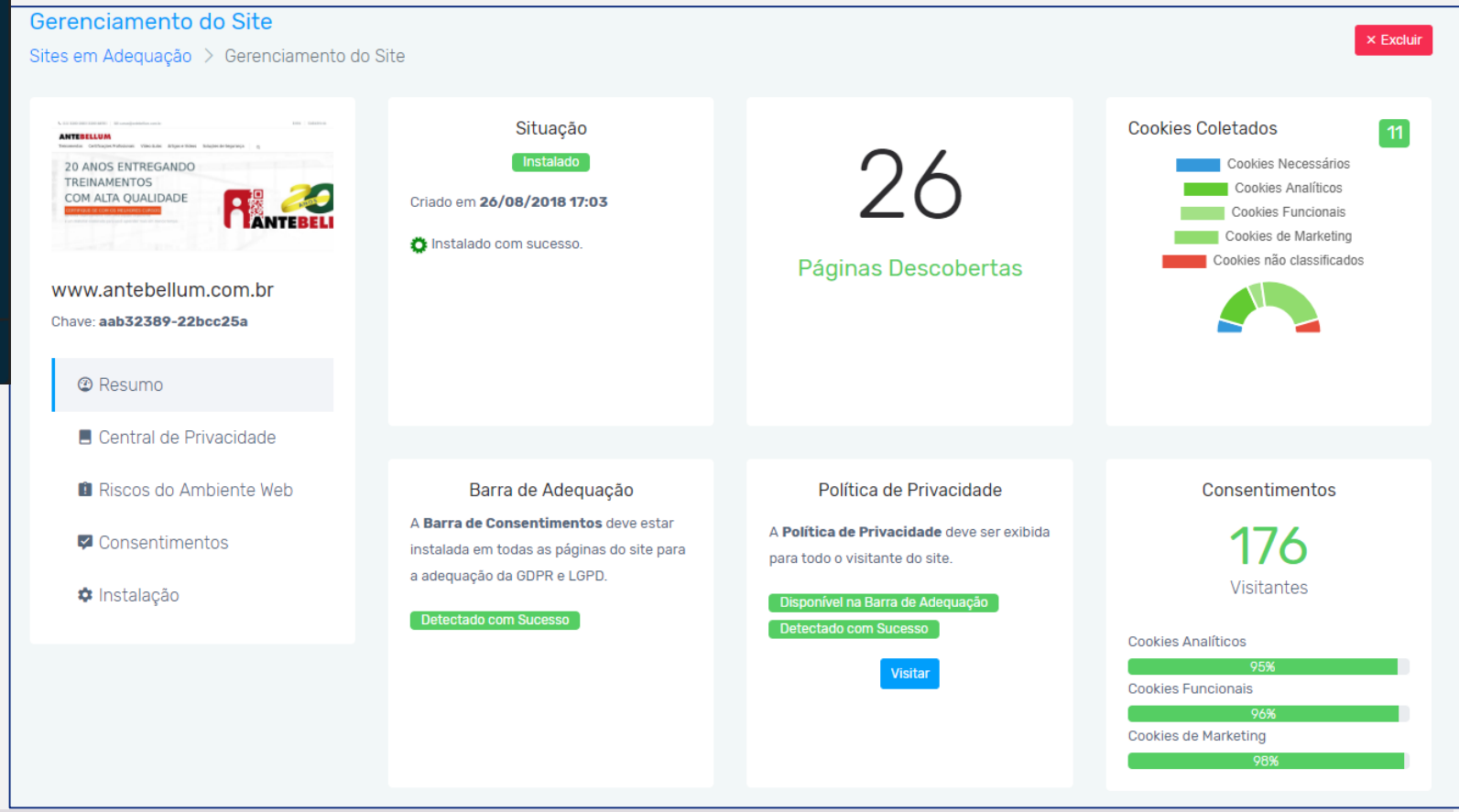
	A ITEM	B NO.	C UNIT	D COST
1				
2				
3	MUCK RAKE	43	12.95	556.85
4	BUZZ CUT	15	6.75	101.25
5	TOE TONER	250	49.95	12487.50
6	EYE SNUFF	2	4.95	9.90
7				
8			SUBTOTAL	13155.50
9			9.75% TAX	1282.66
10				
11			TOTAL	14438.16
12				
13				
14				
15				
16				
17				
18				
19				
20				

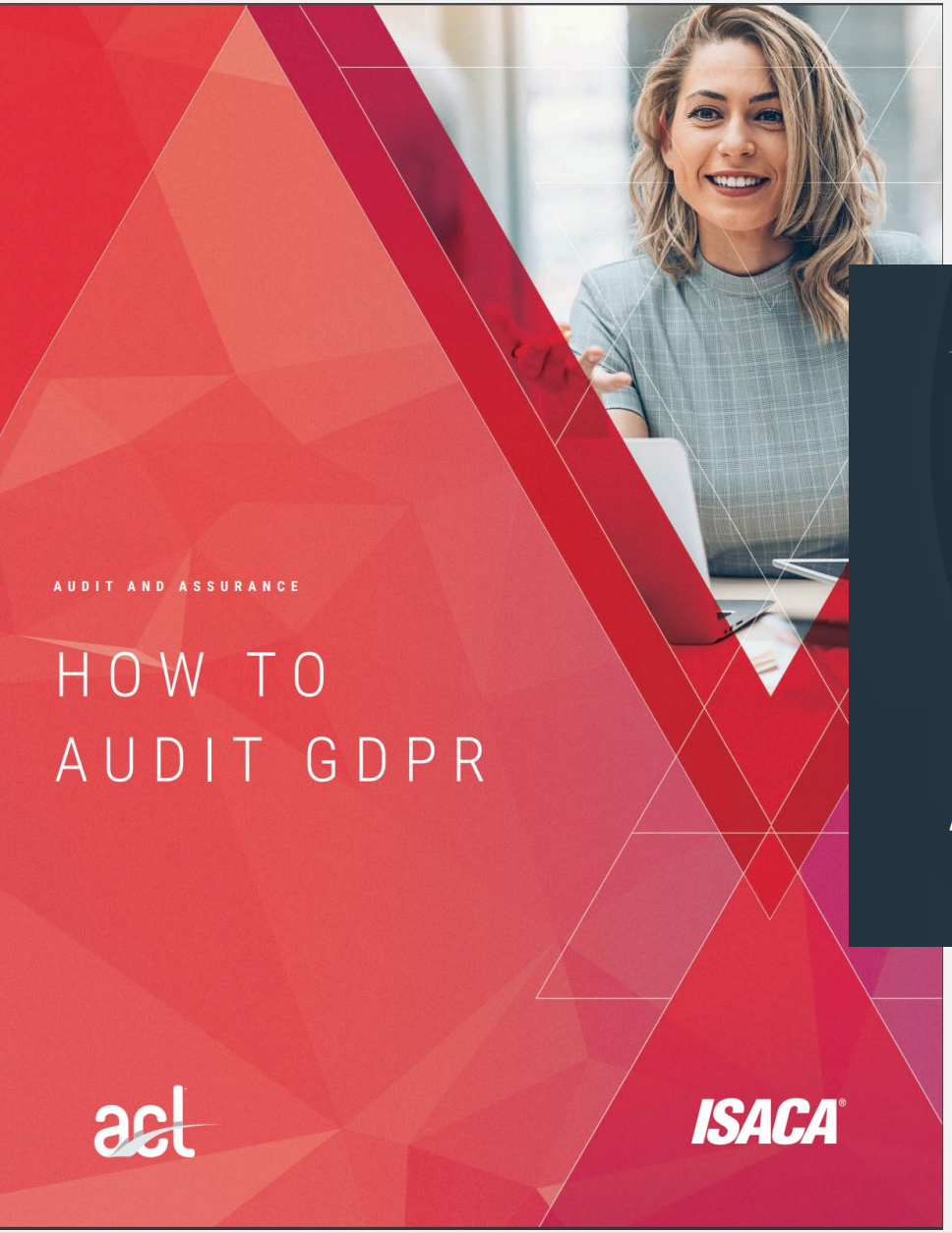
Precisamos de ferramentas específicas



Precisamos de ferramentas específicas






AUDIT AND ASSURANCE
HOW TO
AUDIT GDPR
acl
ISACA


ISACA
Trust in, and value from, information systems
5
Adopting GDPR Using
COBIT® 5


Figure 3– Steps to GDPR Compliance
1. Confirm Applicability
Assess the scope of GDPR and its applicability to the processing activities of the organization.
2. Catalog Key Requirements
Identify key compliance requirements necessary to achieve objectives.
3. Chart Compliance Program
Detail the road map of compliance activities necessary to meet GDPR requirements.
4. Conduct Privacy Assessment
Evaluate current data protection measures against GDPR requirements.
5. Conduct Security Assessment
Evaluate current security measures against GDPR requirements and industry best practices.
6. Classify Gaps
Identify and prioritize issues, risk and vulnerabilities.
7. Conduct Remediation
Organize and undertake resolution of identified privacy and security gaps.
8. Compute Performance
Evaluate the performance of the organization against compliance standards and outline lessons learned.

ISACA

GENERAL DATA PROTECTION REGULATION (GDPR) READINESS, ASSESSMENT & COMPLIANCE

INTERACTIVE LEARNING | RESOURCES | NEWS | ADVOCACY | ISACA.ORG

GDPR Compliance: The Information & Insights You Need to Avoid Penalties

The European Union's General Data Protect Regulation is a sweeping data protection law that affects all enterprises offering goods or services (regardless if payment is required) within the EU as well as any business retaining or processing information on any EU citizen. Given the global nature of digital commerce today, this regulation is having a global impact.

For enterprises, the cost of non-compliance can be high—the EU recently issued the first wave of rulings and penalties, with more likely to come. With potential penalties ranging up to 4% of a company's worldwide revenues for severe offenders, government authorities are clearly serious about ensuring the protection of personal information collected, stored and used by organizations.

Follow ISACA's world-class privacy guidance and learn how best to operate in a GDPR world and develop new enterprise best practices that can give your organization a competitive advantage in managing data protection.

Check out our extensive library of GDPR interactive learning, resources, news and advocacy!

FREE ONLINE GDPR ASSESSMENT RATES ENTERPRISE COMPLIANCE

IDENTIFY AND RESOLVE GAPS >

EXTEND YOUR GDPR KNOWLEDGE WITH CPE ON DEMAND

SIGN UP TODAY >

IMPLEMENTING THE GENERAL DATA PROTECTION REGULATION

PURCHASE THE E-BOOK >

GDPR INTERACTIVE LEARNING

Sign up and learn with others in an interactive environment at international conferences or through online webinars. Reserve your spot today!

VIEW OPTIONS

GDPR RESOURCE CENTER

As you develop a data protection strategy and plan for your enterprise, take advantage of the knowledge and thought leadership provided by ISACA's worldwide network of experts.

VIEW OPTIONS

GDPR NEWSROOM

Stay on top of the latest news and current events about GDPR, and see what ISACA thought leaders have to say about the importance of complying with this new regulatory development and the strategic opportunities it affords forward-thinking enterprises.

VIEW OPTIONS

GDPR ADVOCACY

ISACA is already acknowledged as a global thought leader in the information risk, governance and security space, providing relevant guidance and internationally recognized certifications. This, together with ISACA's strong European presence, means that ISACA is ideally positioned to provide practical and pragmatic guidance to assist organizations to prepare for the requirements of GDPR, particularly in the areas of privacy by design, appropriate security protection and the role of the Data Protection Officer.

VIEW OPTIONS

Certificações Profissionais (EXIN e IAPP)

Considerações Finais

That's All Folks!

www.linkedin/in/ferfon

fernnado@antebellum.com.br