

16^a
**CONFERÊNCIA
ANUAL 2019**

O Mundo Digital
na Próxima Década

***Conformidade com o RGPD
recorrendo a normas internacionais***

Luís Azevedo, itSMF Portugal

Reitoria da Universidade Nova de Lisboa
3 de Outubro 2019

Patrocínio Platinum

claranet

easyVISTA™

Patrocínio Ouro

apcer

bmc

Rumos

RGPD => GERIR SEGURANÇA + GERIR PRIVACIDADE

GERIR SEGURANÇA: assegurar a confidencialidade, integridade, disponibilidade e resiliência dos dados e informações dos titulares.

GERIR PRIVACIDADE: assegurar o cumprimento dos princípios de privacidade e a operacionalização das regras específicas do RGPD e restante legislação relativa à proteção de dados pessoais.

GERIR SEGURANÇA => ISO/IEC 27001 – Requisitos SGSI

4 Contexto da organização	7 Suporte
4.1 Compreender a organização e o seu contexto	7.1 Recursos
4.2 Compreender as necessidades e expectativas das partes interessadas ...	7.2 Competência
4.3 Determinar o âmbito do sistema de gestão de segurança da informação	7.3 Consciencialização
4.4 Sistema de gestão de segurança da informação	7.4 Comunicação
5 Liderança	7.5 Informação documentada.....
5.1 Liderança e comprometimento	8 Operação
5.2 Política	8.1 Planeamento e controlo operacional
5.3 Funções, responsabilidades e autoridades na organização	8.2 Avaliação do risco de segurança da informação
6 Planeamento	8.3 Tratamento do risco de segurança da informação
6.1 Ações para endereçar riscos e oportunidades	9 Avaliação de desempenho
6.1.1 Generalidades	9.1 Monitorização, medição, análise e avaliação.....
6.1.2 Avaliação do risco de segurança da informação	9.2 Auditoria interna
6.1.3 Tratamento do risco de segurança da informação	9.3 Revisão pela gestão
6.2 Objetivos de segurança da informação e planeamento para os alcançar .	10 Melhoria
	10.1 Não conformidade e ação corretiva
	10.2 Melhoria contínua

Anexo A (normativo) Objetivos de controlo e controlos de referê

GERIR SEGURANÇA => ISO/IEC 27001 – Requisitos SGSI

4 Contexto da organização	7 Suporte
4.1 Compreender a organização e o seu contexto	7.1 Recursos
4.2 Compreender as necessidades e expectativas	7.2 Competência
4.3 Determinar o âmbito do sistema de gestão	7.3 Conscientização
4.4 Sistema de gestão de segurança da informação	7.4 Comunicação
5 Liderança	7.5 Informação documentada
5.1 Liderança e comprometimento	7.6 Gestão de documentos e de registros
5.2 Política	8.1 Planeamento do controlo operacional
5.3 Funções, responsabilidades e autoridades na organização	8.2 Avaliação do risco de segurança da informação
6 Planeamento	8.3 Tratamento do risco de segurança da informação
6.1 Ações para endereçar riscos e oportunidades	9 Desempenho
6.1.1 Generalidades	9.1 Medição, medição, análise e avaliação
6.1.2 Avaliação do risco de segurança da informação	9.2 Auditoria interna
6.1.3 Tratamento do risco de segurança da informação	9.3 Gestão de não conformidade e de ações corretivas
6.2 Objetivos de segurança da informação e planeamento para os alcançar	10.1 Não conformidade e ação corretiva
6.3 Avaliação de conformidade	10.2 Melhoria contínua

(re)avaliar riscos de segurança

aplicar / ajustar controlos de segurança

GERIR SEGURANÇA => ISO/IEC 27002 – Orientações p/Controlos

4 Structure of this standard	12 Operations security
4.1 Clauses.....	12.1 Operational procedures and responsibilities.....
4.2 Control categories.....	12.2 Protection from malware.....
5 Information security policies	12.3 Backup.....
5.1 Management direction for information security.....	12.4 Logging and monitoring.....
6 Organization of information security	12.5 Control of operational software.....
6.1 Internal organization.....	12.6 Technical vulnerability management.....
6.2 Mobile devices and teleworking.....	12.7 Information systems audit considerations.....
7 Human resource security	13 Communications security
7.1 Prior to employment.....	13.1 Network security management.....
7.2 During employment.....	13.2 Information transfer.....
7.3 Termination and change of employment.....	14 System acquisition, development and maintenance
8 Asset management	14.1 Security requirements of information systems.....
8.1 Responsibility for assets.....	14.2 Security in development and support processes.....
8.2 Information classification.....	14.3 Test data.....
8.3 Media handling.....	15 Supplier relationships
9 Access control	15.1 Information security in supplier relationships.....
9.1 Business requirements of access control.....	15.2 Supplier service delivery management.....
9.2 User access management.....	16 Information security incident management
9.3 User responsibilities.....	16.1 Management of information security incidents and improvements.....
9.4 System and application access control.....	17 Information security aspects of business continuity management
10 Cryptography	17.1 Information security continuity.....
10.1 Cryptographic controls.....	17.2 Redundancies.....
11 Physical and environmental security	18 Compliance
11.1 Secure areas.....	18.1 Compliance with legal and contractual requirements.....
11.2 Equipment.....	18.2 Information security reviews.....

GERIR SEGURANÇA => ISO/IEC 27002 – Orientações p/Controlos

A.5.1.1	Policies for information security	<i>Control</i> A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
---------	-----------------------------------	---

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an “information security policy” which is approved by management and which sets out the organization’s approach to managing its information security objectives.

Information security policies should address requirements created by:

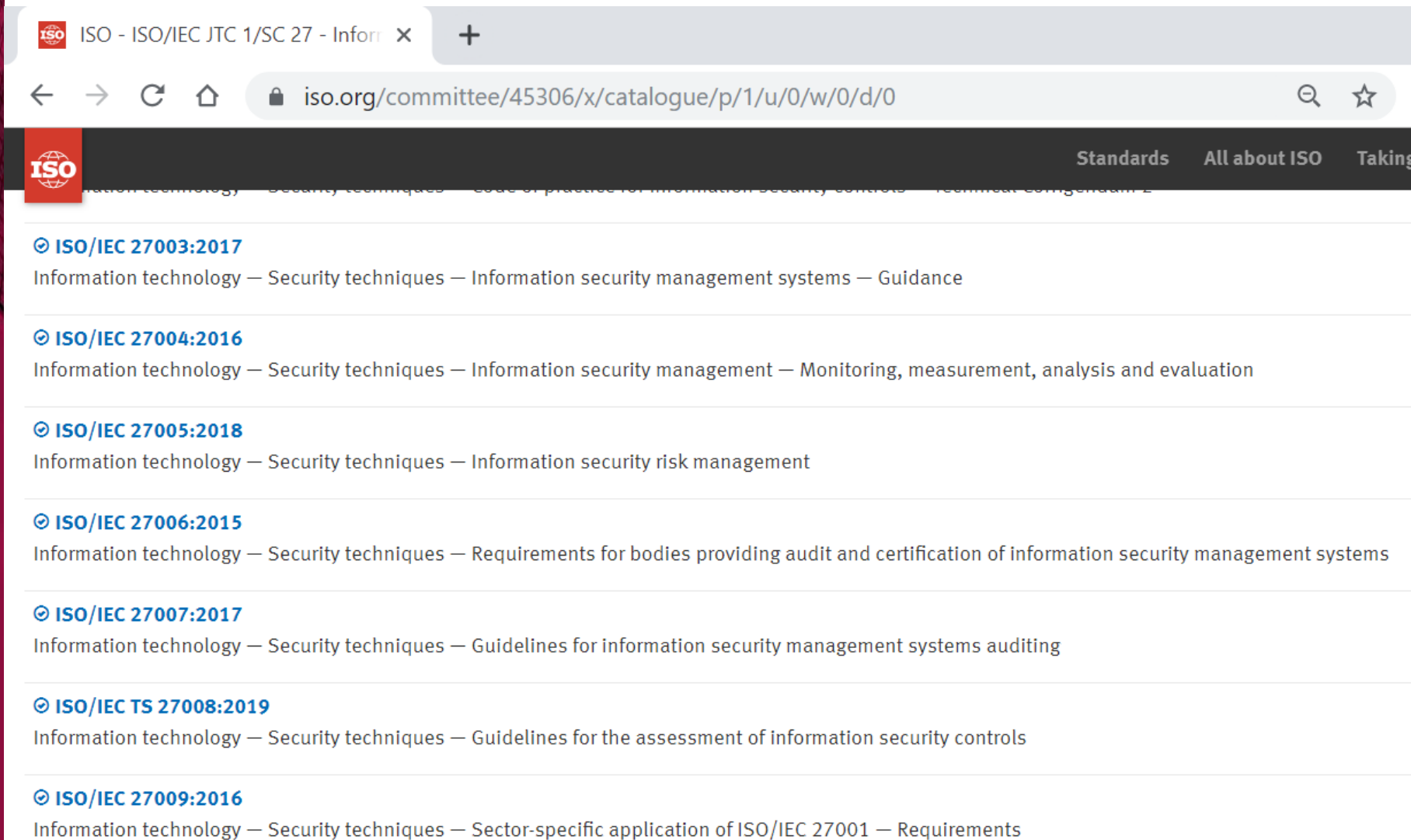
- a) business strategy;
- b) regulations, legislation and contracts;
- c) the current and projected information security threat environment.

The information security policy should contain statements concerning:

- a) definition of information security objectives and principles to guide all activities relating to

Conformidade com o RGPD recorrendo a normas internacionais

GERIR SEGURANÇA => Outras orientações ...



The screenshot shows a web browser window with the URL iso.org/committee/45306/x/catalogue/p/1/u/0/w/0/d/0. The page displays a list of ISO/IEC standards under the heading "Information technology — Security techniques".

- [ISO/IEC 27003:2017](#)
Information technology — Security techniques — Information security management systems — Guidance
- [ISO/IEC 27004:2016](#)
Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
- [ISO/IEC 27005:2018](#)
Information technology — Security techniques — Information security risk management
- [ISO/IEC 27006:2015](#)
Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- [ISO/IEC 27007:2017](#)
Information technology — Security techniques — Guidelines for information security management systems auditing
- [ISO/IEC TS 27008:2019](#)
Information technology — Security techniques — Guidelines for the assessment of information security controls
- [ISO/IEC 27009:2016](#)
Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

ISO/IEC 29100 privacy framework

This International Standard provides a high-level framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems.

It is general in nature and places organizational, technical, and procedural aspects in an overall privacy framework.

This International Standard is intended to enhance existing security standards by adding a focus relevant to the processing of PII.

Use of this International Standard will (...) improve organizations' privacy programs through the use of best practices.

ISO/IEC 29100 privacy framework

4 Basic elements of the privacy framework	5 The privacy principles of ISO/IEC 29100
4.1 Overview of the privacy framework	5.1 Overview of privacy principles
4.2 Actors and roles	5.2 Consent and choice
4.3 Interactions	5.3 Purpose legitimacy and specification
4.4 Recognizing PII	5.4 Collection limitation
4.5 Privacy safeguarding requirements	5.5 Data minimization
4.6 Privacy policies	5.6 Use, retention and disclosure limitation
4.7 Privacy controls	5.7 Accuracy and quality
	5.8 Openness, transparency and notice
	5.9 Individual participation and access
	5.10 Accountability
	5.11 Information security
	5.12 Privacy compliance
	Annex A (informative) Correspondence between ISO/IEC 29100
	concepts and ISO/IEC 27000 concepts

Privacy Principles: GDPR ↔ ISO/IEC 29100

GDPR (Article 5)	ISO/IEC 29100 (Clause 5)
lawfulness, fairness and transparency	Consent and choice Openness, transparency and notice Individual participation and access
purpose limitation	Purpose legitimacy and specification
data minimisation	Collection limitation Data minimization Use, retention and disclosure limitation
accuracy	Accuracy and quality
storage limitation	Use, retention and disclosure limitation
integrity and confidentiality	Information security
accountability	Accountability Privacy compliance

ISO/IEC 27701 – Extensão da 27001 e 2 para gestão de privacidade

This document can be used by PII controllers (including those that are joint PII controllers) and PII processors (including those using subcontracted PII processors and those processing PII as subcontractors to PII processors).

An organization complying with the requirements in this document will generate documentary evidence of how it handles the processing of PII.

Such evidence can be used to facilitate agreements with business partners where the processing of PII is mutually relevant. This can also assist in relationships with other stakeholders.

The use of this document in conjunction with ISO/IEC 27001 can, if desired, provide independent verification of this evidence.

This document was initially developed as ISO/IEC 27552.

ISO/IEC 27701 + 27001 + 27002 => Requisitos + Orientações

4 General	7 Additional ISO/IEC 27002 guidance for PII controllers
4.1 Structure of this document	7.1 General
4.2 Application of ISO/IEC 27001:2013 requirements	7.2 Conditions for collection and processing
4.3 Application of ISO/IEC 27002:2013 guidelines	7.3 Obligations to PII principals
4.4 Customer	7.4 Privacy by design and by default
5 PIMS-specific requirements related to ISO/IEC 27001	7.5 PII sharing, transfer, and disclosure
5.1 General	8 Additional ISO/IEC 27002 guidance for PII processors
5.2 Context of the organization	8.1 General
5.3 Leadership	8.2 Conditions for collection and processing
5.4 Planning.....	8.3 Obligations to PII principals
5.5 Support	8.4 Privacy by design and by default
5.6 Operation	8.5 PII sharing, transfer, and disclosure
5.7 Performance evaluation	Annex A (normative) PIMS-specific reference control objectives and controls (PII Controllers).....
5.8 Improvement	Annex B (normative) PIMS-specific reference control objectives and controls (PII Processors).....
6 PIMS-specific guidance related to ISO/IEC 27002	Annex C (informative) Mapping to ISO/IEC 29100.....
	Annex D (informative) Mapping to the General Data Protection Regulation.....
	Annex E (informative) Mapping to ISO/IEC 27018 and ISO/IEC 29151.....
	Annex F (informative) How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002.....

ISO/IEC 27701 + 27001 + 27002 => Requisitos + Orientações

Sistema de Gestão de Informação de Privacidade		
	Sistema de Gestão de Segurança da Informação (27001 + 27002)	Extensão para Gestão de Privacidade (27701)
Requisitos Certificáveis	27001 – 4 a 10: Requisitos para o sistema de gestão (incluindo gestão dos riscos) de segurança da informação	5 - Requisitos adicionais específicos de privacidade para a 27001
	27001 - Anexo A (A.5 a A.18): Objetivos de controlo e controlos de segurança da informação	Anexos A e B: Objetivos de controlo e controlos, adicionais, específicos para a privacidade, para Responsáveis pelo Tratamento e “Subcontratantes”
Orientações Práticas	27002 – 5 a 18: Orientações para implementação e melhoria dos controlos de segurança da informação da 27001	6 - Orientações de privacidade adicionais para implementação e melhoria dos controlos de segurança da informação da 27002
		7 e 8 - Orientações para implementação e melhoria dos controlos específicos de privacidade da 27701, para Responsáveis pelo Tratamento e “Subcontratantes”

ISO/IEC 27701 + 27001 + 27002 => Requisitos + Orientações

Sistema de Gestão de Informação de Privacidade	
	<p>Sistema de Gestão de Informação de Privacidade (27701)</p> <p>Sistema de Gestão de Informação de Privacidade (27701)</p>
Requisitos Certificáveis	<p>27001 – 4 a 10: Requisitos de gestão (incluindo requisitos adicionais específicos de privacidade para a 27001)</p>
	<p>27001 - Anexos A (A.5 a A.18): Objetivos de controlo e controlos de segurança da informação</p> <p>Anexos A e B: Objetivos de controlo e controlos, adicionais, e específicos para a privacidade, para Responsáveis pelo Tratamento e “Subcontratantes”</p>
Orientações Práticas	<p>27002 – 5 a 10: Orientações para implementação e melhoria da segurança da informação</p> <p>Orientações de privacidade adicionais para implementação e melhoria dos controlos de segurança da informação da 27002</p>
	<p>27002 – 11 a 18: Orientações para implementação e melhoria dos controlos específicos de privacidade da 27701, para Responsáveis pelo Tratamento e “Subcontratantes”</p>

(re)avaliar riscos de segurança e de privacidade

aplicar / ajustar controlos de segurança e de privacidade

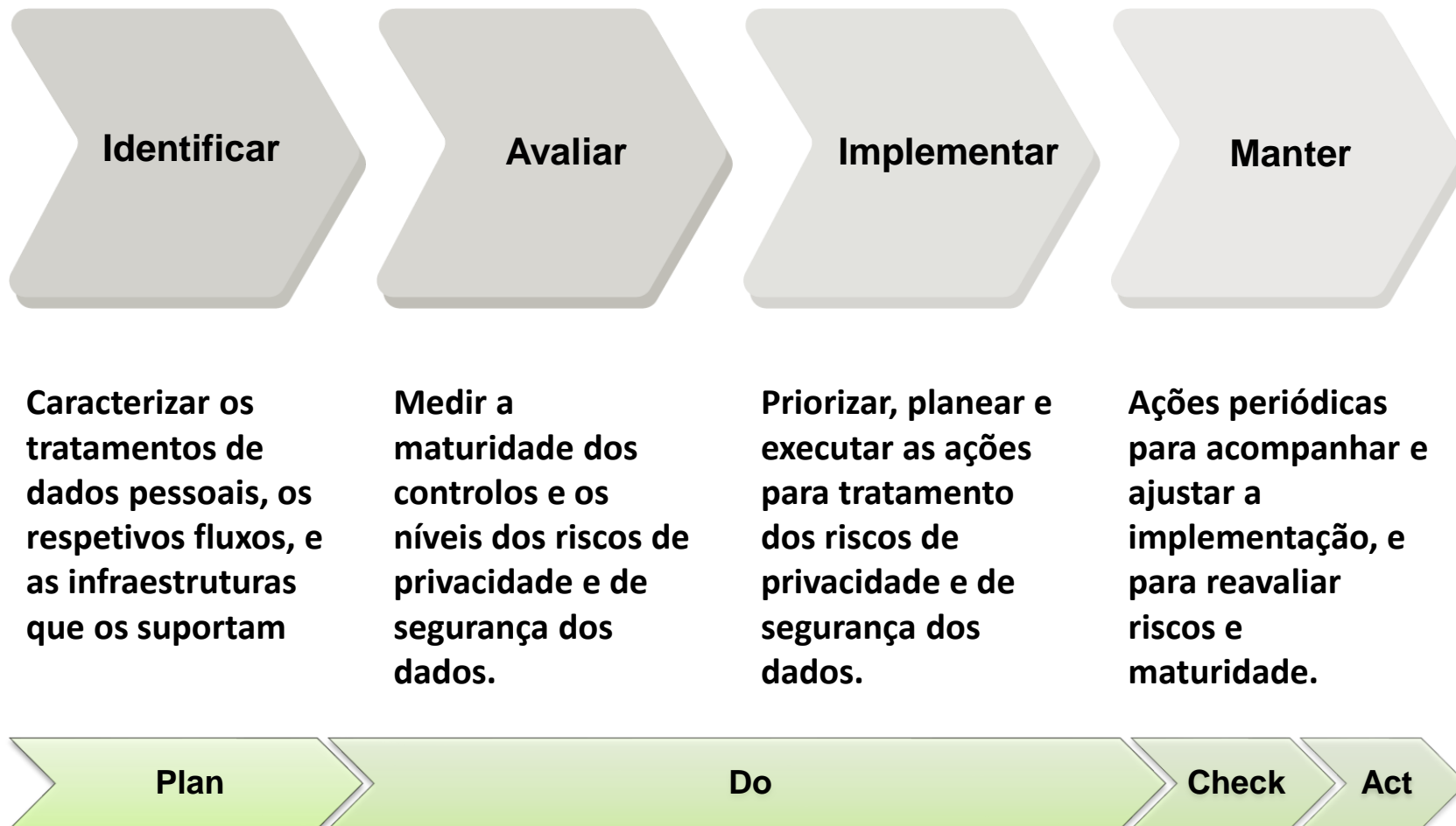
ISO/IEC 29134 => Orientações para avaliar riscos de privacidade

- *A privacy impact assessment (PIA) is an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information (PII) and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk.*
- *The organization conducting a PIA process may wish to directly adapt the process guidance below to its specific PIA scale and scope or as one possible alternative to select a suitable risk-based management system, such as ISO/IEC 27001, and integrate into it appropriately adapted elements of the guidance below, including the use of the PIA report (see Clause 7) to treat the privacy risks it identifies.*

ISO/IEC 29134 => Guidelines for privacy impact assessment

5 Preparing the grounds for PIA.....	7 PIA report.....
5.1 Benefits of carrying out a PIA.....	7.1 General.....
5.2 Objectives of PIA reporting.....	7.2 Report structure.....
5.3 Accountability to conduct a PIA.....	7.3 Scope of PIA.....
5.4 Scale of a PIA.....	7.4 Privacy requirements.....
6 Guidance on the process for conducting a PIA.	7.5 Risk assessment.....
6.1 General.....	7.6 Risk treatment plan.....
6.2 Determine whether a PIA is necessary (threshold analysis).....	7.7 Conclusion and decisions.....
6.3 Preparation of the PIA.....	7.8 PIA public summary.....
6.4 Perform the PIA.....	Annex A (informative) Scale criteria on the level of impact and on the likelihood.....
6.5 Follow up the PIA.....	Annex B (informative) Generic threats.....
	Annex C (informative) Guidance on the understanding of terms used....
	Annex D (informative) Illustrated examples supporting the PIA process.

Abordagem para Conformidade com o RGPD



16^a
E CONFERÊNCIA
ANUAL 2019

O Mundo Digital
na Próxima Década

Obrigado