itSMF
The IT Service Management Forum
Portugal

Conformidade com o RGPD recorrendo a normas internacionais

Luís Azevedo, itSMF Portugal

Reitoria da Universidade Nova de Lisboa
3 de Outubro 2019

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

GERIR SEGURANÇA => ISO/IEC 27001 – Requisitos SGSI

(re)avaliar riscos de segurança

aplicar / ajustar controlos de segurança

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

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

A.5.1.1	Policies for information security	*Control* 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;

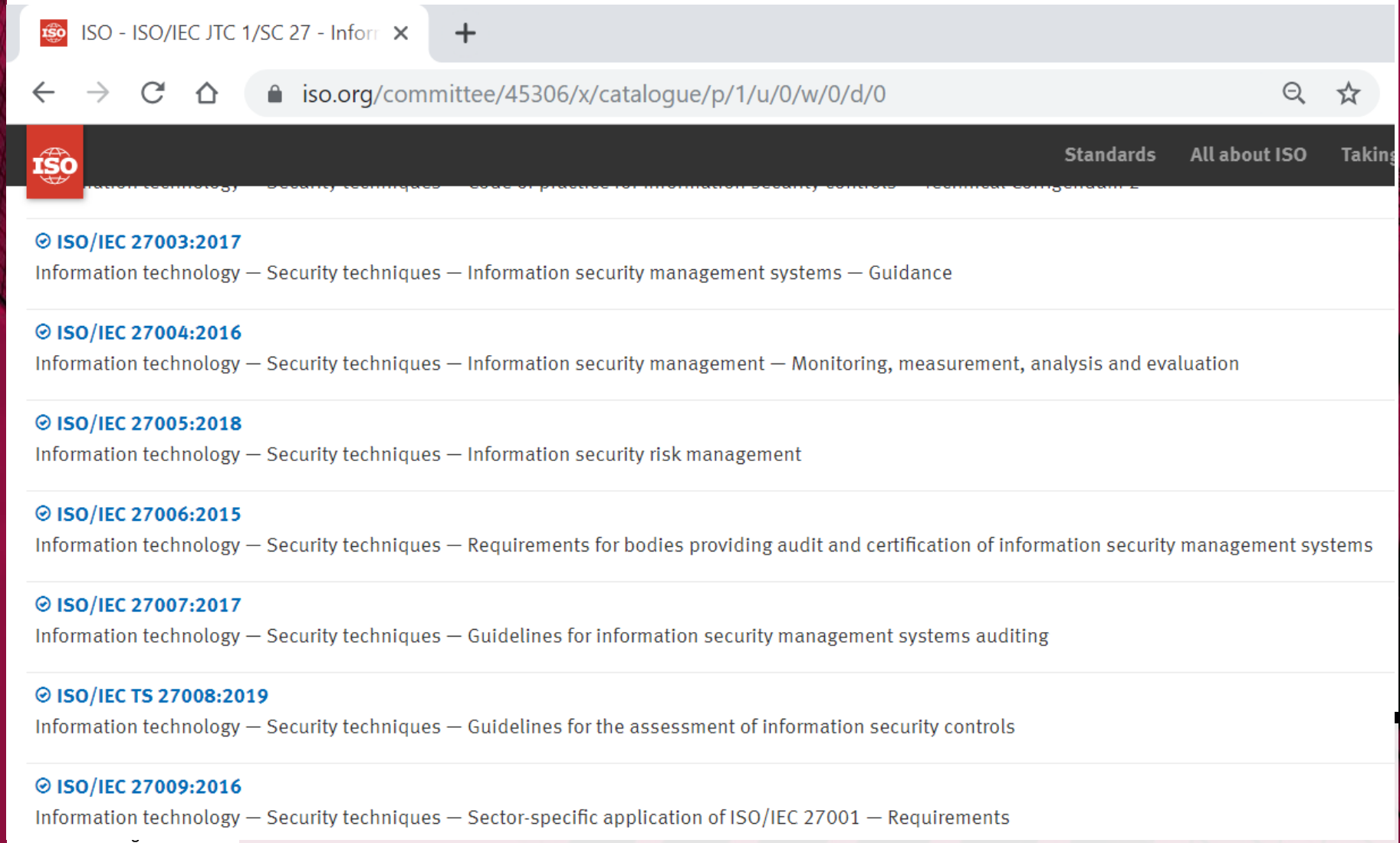
b) regulations, legislation and contracts;

c) the current and projected information security threat environment.

The information security policy should contain statements concerning:

Conformidade com o RGPD recorrendo a normas internacionais

GERIR SEGURANÇA => Outras orientações …



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

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

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	
	Sistema de Gest… Informação	**…ão para Gestão de Privacidade (27701)**
Requisitos Certificáveis	27001 – 4 a 10: R… gestão (inclu… o seg… ça d…	…uisitos adicionais específicos de …ivacidade para a 27001
	27001 - Anex… A (A.5 a A.18): Objetivos de controlo e …ntrolos de segurança da informação	Anexos A e … Objetivos de controlo e controlos, adicionais, e… ecíficos para a privacidade, para Resp… sáveis pelo Tratamento e "Subcontratantes"
Orientações Práticas	27002 – 5 a … implementação e m… segurança da in…	…nta…es de privacidade adicionais para …ação e melhoria dos controlos de …rança da informação da 27002
		- Orientações para implementação e …lhoria dos controlos específicos de …idade da 27701, para Responsáveis pelo Tratamento e "Subcontratantes"

(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

Abordagem para Conformidade com o RGPD

Identificar	Avaliar	Implementar	Manter
Caracterizar os tratamentos de dados pessoais, os respetivos fluxos, e as infraestruturas que os suportam	Medir a maturidade dos controlos e os níveis dos riscos de privacidade e de segurança dos dados.	Priorizar, planear e executar as ações para tratamento dos riscos de privacidade e de segurança dos dados.	Ações periódicas para acompanhar e ajustar a implementação, e para reavaliar riscos e maturidade.

Plan	Do	Check	Act

16ª CONFERÊNCIA ANUAL 2019

O Mundo Digital na Próxima Década

Obrigado

itSMF
The IT Service Management Forum
Portugal

luis.azevedo@itsmf.pt
www.linkedin.com/in/luisazevedo