XIII Encuentro Iberoamericano de Protección de Datos

Lima, 6, 7 y 8 de mayo

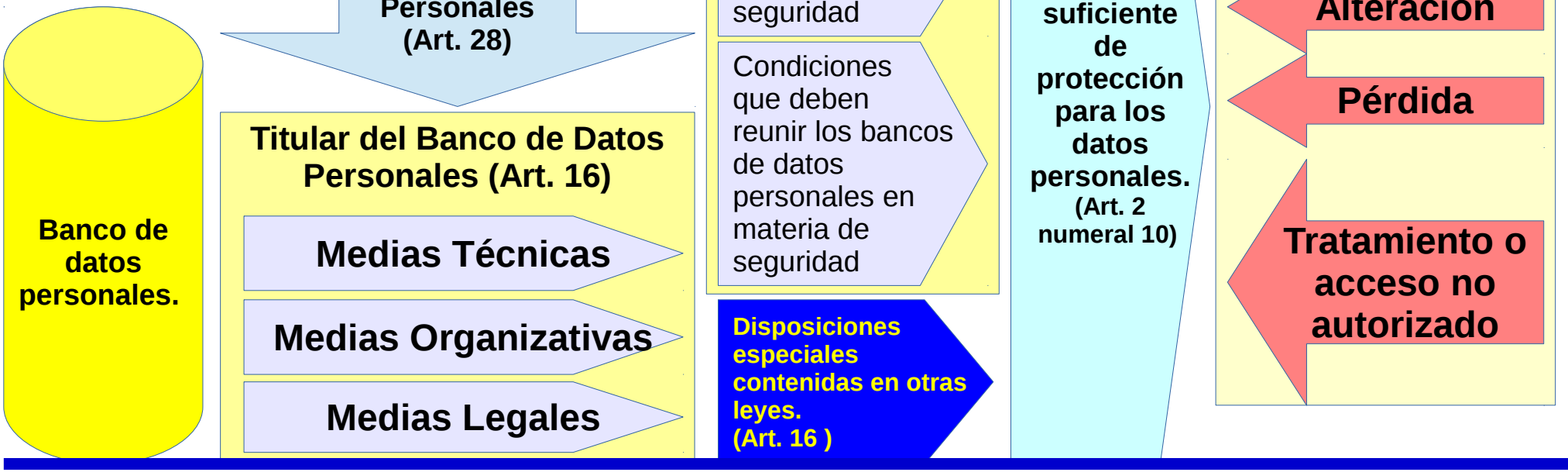
Protección de datos personales y medidas de seguridad de la información

PANEL 10

Carlos A. Horna Vallejos
carlos@gtdi.pe
@the_ska

GTDI
Tecnologías de la Información y Consultoría

Tratamiento de Datos personales (Aspectos de Seguridad)



Orientación y marco de trabajo ISO/IEC 29100

Enfoque y requisitos

ISO/IEC 27001

ISO/IEC 27005

DIRECTIVA DE SEGURIDAD

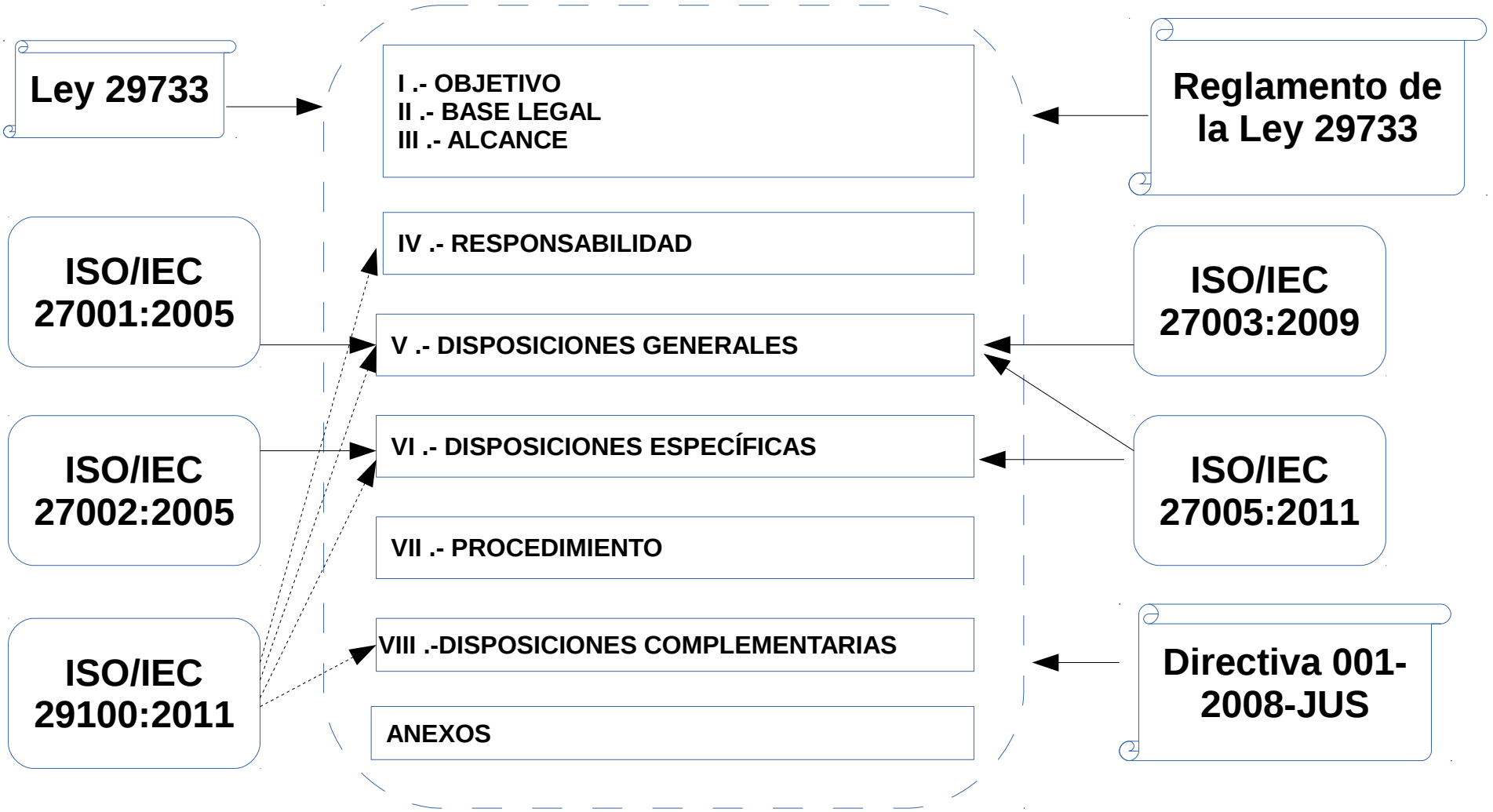
Autoridad Nacional de Protección de Datos Personales
APDP

Recomendaciones

ISO/IEC 27002

ISO/IEC 27003

- **Comentarios**
- **Directiva 001-2008-JUS**
- **R.M. 129-2012-PCM**


Ley 29733
I .- OBJETIVO
II .- BASE LEGAL
III .- ALCANCE
Reglamento de la Ley 29733
ISO/IEC 27001:2005
IV .- RESPONSABILIDAD
ISO/IEC 27003:2009
V .- DISPOSICIONES GENERALES
ISO/IEC 27002:2005
VI .- DISPOSICIONES ESPECÍFICAS
ISO/IEC 27005:2011
VII .- PROCEDIMIENTO
ISO/IEC 29100:2011
VIII .-DISPOSICIONES COMPLEMENTARIAS
Directiva 001-2008-JUS
ANEXOS

Documento maestro/ Cuaderno de seguridad (1.3.1.8)

Passwords (2.3.1.1)
c) Requerir el uso de contraseñas que contengan al menos 8 dígitos y que sean alfanuméricas (mayúsculas, minúsculas y números) y al menos incluyan un caracter especial

Posibilidad de mejora

MEDIDAS DE SEGURIDAD

1. DISPOSICIONES GENERALES

1.1 Categoría:

1.1.1 Para efectos de la presente directiva, se debe considerar la siguiente clasificación de categorías en el tratamiento de datos personales y el principio de proporcionalidad descrito en el artículo 7 de la Ley N° 29733 cuando no exista coincidencia exacta:

a) Básico, corresponde a la categoría de menor nivel e incluye a bancos de datos personales que:

- No contengan la información de más de cincuenta (50) personas.
- Número de datos personales no mayor a cinco (05). Por ejemplo nombres, apellidos, DNI, dirección y teléfono.
- No incluyen datos sensibles.
- Tienen como titular a una persona natural.

b) Simple, corresponde a bancos de datos personales que:

- No contengan la información de más de cien (100) personas.
- El periodo de tiempo del tratamiento para cumplir con la finalidad es inferior a un (01) año.

1.1.3 Matriz de apoyo para la selección de categoría en el tratamiento de datos personales.

ÍTEM	CRITERIO	BÁSICO	SIMPLE	INTERMEDIO	COMPLEJO	CRÍTICO
1	Volumen de registros, número de titulares de datos personales que consienten el tratamiento de sus datos. (Criterio utilizado para determinar las categorías).	Hasta 50	Hasta 100	Hasta 1000	Indeterminado	Indeterminado
2	Número de datos personales en banco de datos personales que no contienen datos sensibles. (Criterio utilizado para determinar el tipo básico).	Hasta 5	Más de 5	Más de 5	Más de 5	Más de 5
3	Finalidad del tratamiento de datos personales respaldada por ley o similar. (Criterio utilizado para determinar el tipo crítico).	No aplica	No aplica	No aplica	No aplica	Aplica
4	Periodo mayor a un (01) año o indeterminado para cumplir la finalidad (tiempo de tratamiento de los datos personales).	No aplica	No aplica	Aplica	Aplica	Aplica
5	Tipo de Titular del banco de datos personales: persona natural. (Criterio utilizado para determinar el tipo entre básico a intermedio).	Aplica	Aplica	Aplica	No aplica	No aplica
6	Tipo de Titular del banco de datos personales: persona jurídica. (Criterio utilizado para determinar la categoría entre simple a complejo).	No Aplica	Aplica	Aplica	Aplica	Aplica
7	Titular del banco de datos personales del tipo persona jurídica o entidad pública con múltiples localizaciones desde las cuales se tiene acceso al banco de datos personales o se realiza tratamiento de los datos personales. (Criterio utilizado para determinar la categoría complejo o crítico).	No Aplica	No aplica	No aplica	Aplica	Aplica
8	El banco de datos personales puede incluir datos sensibles. (Criterio utilizado para determinar la categoría entre Intermedio a crítico).	No Aplica	No aplica	Aplica	Aplica	Aplica

Anexos

- Contienen instrucciones que pueden ser utilizados como guía en la aplicación de la directiva.
- Incluye un ejemplo de declaración simple de cumplimiento con los principios de la Ley.
- Incluye una referencia al “Cuaderno de seguridad de datos personales”
- Incluye referencias hacia la utilización de otros documentos para:
  - Gestión de Riesgos
  - Evaluación de Impacto en la Privacidad (PIA)
  - Privacidad por Diseño (Privacy by Desgn)

NTP

Haga clic para ampliar la imagen

Código:	NTP-ISO/IEC 27001:2014
Título:	TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos
Publicado:	2014/12/01
Resumen:	Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización.
Reemplaza a:	NTP-ISO/IEC 27001:2008 (revisada el 2013)
I.C.S:	35.040 Conjuntos de caracteres y codificación de la información
Precio:	61.95
Descriptores:	Tecnología / información / técnicas / seguridad / sistema de gestión / requisitos /

ISO/IEC JTC 1/SC 27 IT Security techniques

Subcommittees/Working Groups:

Subcommittee/Working Group	Title
ISO/IEC JTC 1/SC 27/SWG-M	Special Working Group on Management *The convener can be reached through the secretariat*
ISO/IEC JTC 1/SC 27/SWG-T	Transversal Items *The convener can be reached through the secretariat*
ISO/IEC JTC 1/SC 27/WG 1	Information security management systems *The convener can be reached through the secretariat*
ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms *The convener can be reached through the secretariat*
ISO/IEC JTC 1/SC 27/WG 3	Security evaluation, testing and specification *The convener can be reached through the secretariat*
ISO/IEC JTC 1/SC 27/WG 4	Security controls and services *The convener can be reached through the secretariat*
ISO/IEC JTC 1/SC 27/WG 5	Identity management and privacy technologies *The convener can be reached through the secretariat*

Quick links

Work programme
(drafts and new work items of ISO/IEC JTC 1/SC 27)

Business plans

Working area on ISOTC and Public information folder

JTC/SC27

Secretaría

Germany (DIN)

Miembros plenos

Algeria (IANOR)
Argentina (IRAM)
Australia (SA)
Austria (ASI)
Belgium (NBN)
Brazil (ABNT)
Canada (SCC)
Chile (INN)
China (SAC)
Cyprus (CYS)
Czech Republic (UNMZ)
Côte d'Ivoire (CODINORM)
Denmark (DS)
Estonia (EVS)
Finland (SFS)
France (AFNOR)
Germany (DIN)
India (BIS)
Ireland (NSAI)
Israel (SII)
Italy (UNI)
Jamaica (BSJ)
Japan (JISC)
Kazakhstan (KAZMEMST)
Kenya (KEBS)
Korea, Republic of (KATS)
Luxembourg (ILNAS)
Malaysia (DSM)
Mauritius (MSB)
Mexico (DGN)
Netherlands (NEN)
New Zealand (SNZ)
Norway (SN)
Peru (INDECOPI)
Poland (PKN)
Romania (ASRO)
Russian Federation (GOST R)
Singapore (SPRING SG)
Slovakia (SOSMT)
Slovenia (SIST)
South Africa (SABS)
Spain (AENOR)
Sri Lanka (SLSI)
Sweden (SIS)
Switzerland (SNV)
Thailand (TISI)
The Former Yugoslav Republic of Macedonia (ISRM)
Ukraine (DTR)
United Arab Emirates (ESMA)
United Kingdom (BSI)
United States (ANSI)
Uruguay (UNIT)

Observadores

Belarus (BELST)
Bosnia and Herzegovina (BAS)
Costa Rica (INTECO)
El Salvador (OSN)
Ghana (GSA)
Hong Kong (ITCHKSAR) (Correspondent member)
Hungary (MSZT)
Iceland (IST)
Indonesia (BSN)
Iran, Islamic Republic of (ISIRI)
Lithuania (LST)
Morocco (IMANOR)
Palestine, State of (PSI) (Correspondent member)
Portugal (IPQ)
Saudi Arabia (SASO)
Serbia (ISS)
Swaziland (SWASA) (Correspondent member)
Turkey (TSE)

SC27 WG 5 Mission

Identity Management & Privacy Technologies

- Development and maintenance of standards and guidelines addressing security aspects of
  - *Identity management*
  - *Biometrics, and*
  - *Privacy*

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC 24761	Authentication context for biometrics	1st ed. 2009 Cor.1: 2013-03-01	*ISO/IEC 24761 specifies the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. It allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrolment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion.* *ISO/IEC 24761 also specifies the cryptographic syntax of an ACBio instance based on an abstract Cryptographic Message Syntax (CMS) schema.*
ISO/IEC 24745	Biometric information protection	1st ed. 2011	*ISO/IEC 24745 provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer.* *Additionally, it provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information.* *It does not include general management issues related to physical security, environmental security and key management for cryptographic techniques.*

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC 24760-1	A framework for identity management – Part 1: Terminology and concepts	1st ed. 2011 Freely available via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html	ISO/IEC 24760-1 • defines terms for identity management, and • specifies core concepts of identity and identity management and their relationships. To address the need to efficiently and effectively implement systems that make identity-based decisions ISO/IEC 24760 specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components which operate on behalf of individuals or organizations. ISO/IEC 24760 specifies fundamental concepts and operational structures of identity management with the purpose to realize information system management so that information systems can meet business, contractual, regulatory and legal obligations. Pat 1 of ISO/IEC 24760 specifies the terminology and concepts for identity management, to promote a common understanding in the field of identity management. It also provides a bibliography of documents related to standardization of various aspects of identity management.

WG 5 Products

Standard	Title	Status	Abstract
ISO/IEC 29100	Privacy framework	1st ed. 2011 Freely available via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html	*ISO/IEC 29100 provides a privacy framework which* • *specifies a common privacy terminology;* • *defines the actors and their roles in processing personally identifiable information (PII);* • *describes privacy safeguarding considerations; and* • *provides references to known privacy principles for IT.* *ISO/IEC 29100 is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.*
ISO/IEC 29115	Entity authentication assurance framework	1st ed. 2013	*ISO/IEC 29115 provides a framework for managing entity authentication assurance in a given context. In particular, it:* • *specifies 4 levels of entity authentication assurance (LoA);* • *specifies criteria and guidelines for achieving these 4 levels;* • *provides guidance for mapping other authentication assurance schemes to the 4 LoAs and for exchanging the results of authentication that are based on the 4 LoAs; and* • *provides guidance on mitigating authentication threats.*
ISO/IEC 29191	Requirements for partially anonymous, partially unlinkable authentication	1st ed. 2012	*ISO/IEC 29191 provides a framework and establishes requirements for partially anonymous, partially unlinkable authentication.* *The term 'partially anonymous, partially unlinkable' means that an a priori designated opener, and that designated opener only, can identify the authenticated entity.*

WG 5 Projects

Project	Title	Status
ISO/IEC 27018	Code of practice for PII protection in public clouds acting as PII processors	To be published as IS
ISO/IEC 24760-2	A framework for identity management – Part 2: Reference architecture and requirements	DIS Ballot
ISO/IEC 29190	Privacy capability assessment model	DIS Ballot
ISO/IEC 29146	A framework for access management	3rd CD
ITU-T X.1085 | ISO/IEC 17922	Telebiometric authentication framework using biometric hardware security module	1st CD
ISO/IEC 24760-3	A framework for identity management – Part 3: Practice	1st CD
ISO/IEC 29003	Identity proofing	4th WD
ISO/IEC 29134	Privacy impact assessment – Methodology	4th WD
ISO/IEC 29151	Code of practice for PII protection	3rd WD
Study Period	Age Verification	Extended
Study Period	A privacy-respecting identity management scheme using attribute-based credentials	Starting
Standing Document 2	Privacy references list	Freely available via www.jtc1sc27.din.de/en
Standing Document 4	Standards privacy assessment	To be published

Gracias por su atención

Carlos A. Horna Vallejos
carlos@gtdi.pe
@the_ska

GTDI
Tecnologías de la Información y Consultoría

http://www.gtdi.pe