

12 MARZO 2021

II CONGRESO DE  
SEGURIDAD DE LA  
INFORMACIÓN Y  
CIBERSEGURIDAD

# “Gestión de la Privacidad”

**Speaker:**

LEOCADIO MARRERO TRUJILLO

**Linkedin**

[www.linkedin.com/in/leocadio-marrero](https://www.linkedin.com/in/leocadio-marrero)



SOCHISI.CL/ENVIVO





- 1. Lead Auditor ISO 27001 Sistemas de Gestión de Seguridad de la Información-BSI
- 2. Auditor ISO 27017 Seguridad en entornos Cloud-BSI
- 3. Auditor y Auditor Implementador ISO 27701 Sistemas de Gestión de Seguridad de la Privacidad- BSI.
- 4. RISK MANAGER ISO 31000 Sistemas de Gestión de Riesgos- PECB
- 5. Gestión y Gobierno de la Ciberseguridad usando NIST CFM.
- 6. CIBER SECURITY FOUNDATION CSFPC
- 7. LEAD CYBERSECURITY PROFESSIONAL CERTIFICATE LCSPC
- 8. Profesor homologado de la Fundación Incyde y Director de programas de formación.
- 9. Profesor en la Escuela de Prácticas Jurídicas del Colegio de Abogados de Las Palmas.
- 10. Académico del Diplomado de Gestión y Gobierno de la Ciberseguridad en USACH.
- 11. Especialista en Protección de Datos Personales. AENOR
- 12. DPO/DPD del ICALPA, Consejo Canario de Colegios de Abogados, COIICO, COAATGC y otras entidades.
- 13. Especialista en Ciberseguridad Industrial en SGCI y Auditoría. Categoría Profesional Nivel Verde del CCI y Coordinador para Canarias del CCI.
- 14. Miembro fundador de APEP, Asociación Profesional Española de la Privacidad; del ISMS FORUM SPAIN y miembro del CCI, Centro de Ciberseguridad Industrial. Miembro de ISACA MADRID,
- 15. CIBERCOOPERANTE del INCIBE.
- 16. Consultor especialista en G.R.C.- Gobierno, Riesgo y Cumplimiento.
- 17. Gestión y Gobierno de la Ciberseguridad en COBIT2019.
- 18. Implementador Líder ISO 27001.



**LA PRIVACIDAD ES PODER.  
LO QUE LA GENTE NO SABE,  
NO PUEDE ARRUINARLO.**

@JustMe



***“La privacidad es colectiva, como el medio ambiente. Si no cuidas tus datos, otros sufren las consecuencias”***

*Carissa Véliz. Filósofa*

*Véliz es profesora de Ética, Filosofía Moral y Filosofía de la Mente en la Universidad de Oxford. Estudió Filosofía en la Universidad de Salamanca, terminó la carrera en la Universidad de Toronto y cursó un máster de Filosofía en la Universidad de Nueva York. Se doctoró en Oxford, donde también realizó una investigación postdoc relacionada con la privacidad*

**SOCHISI.CL/ENVIVO**

En el año 2015, cada día, se generaban en el mundo 6 megabytes de datos por persona. Los números son impactantes y cada año aumentan exponencialmente.

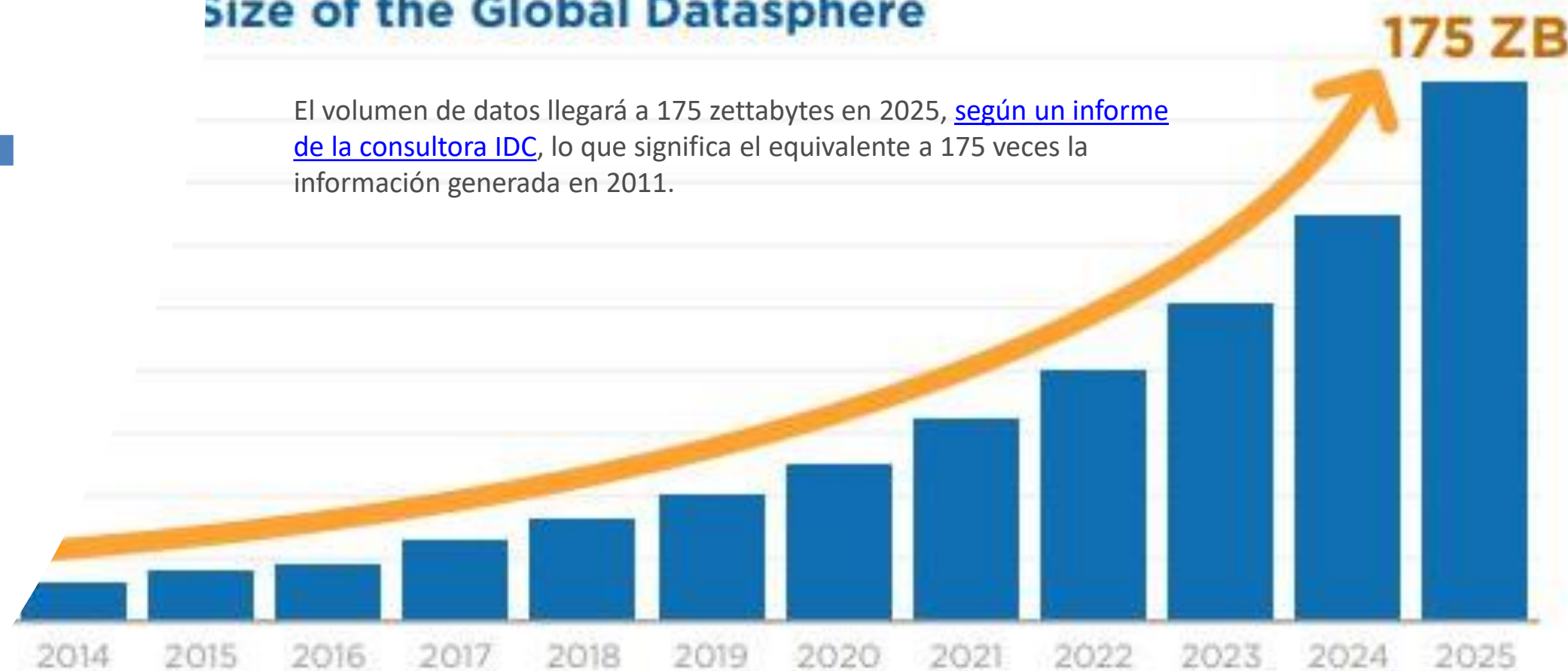
**2020**

**2015**

Se espera que para el 2020, por cada persona en el mundo se producirá 1.7 MB de datos cada segundo y que cada año se duplicará la cantidad de datos producidos en el año anterior

## Size of the Global Datasphere

El volumen de datos llegará a 175 zettabytes en 2025, [según un informe de la consultora IDC](#), lo que significa el equivalente a 175 veces la información generada en 2011.

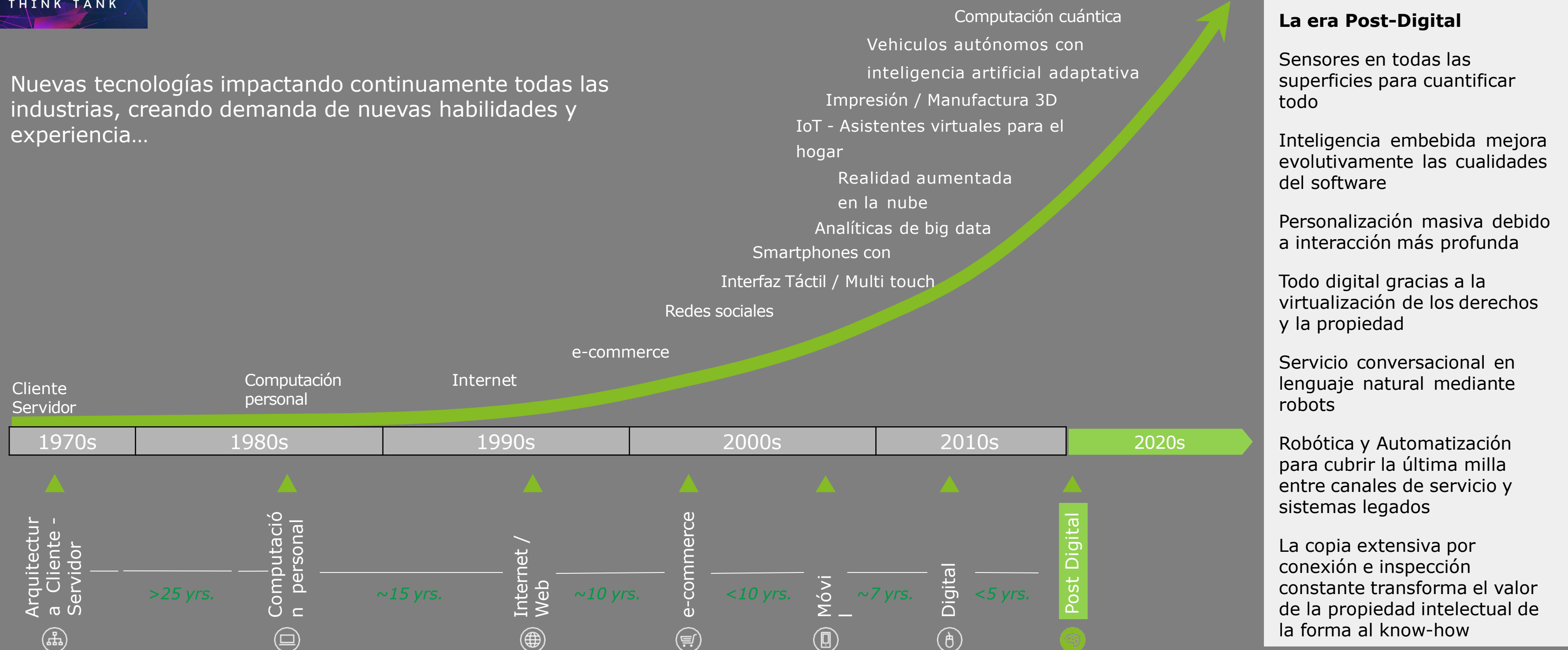


Source: Data Age 2025, sponsored by Seagate with data from IDC Global DataSphere, Nov 2018



# Continuas innovaciones tecnológicas

Nuevas tecnologías impactando continuamente todas las industrias, creando demanda de nuevas habilidades y experiencia...












Los 10 trabajos más demandados en 2010 no existían en 2004. 65 % de los niños graduados en USA trabajarán en cargos que aún no se han inventado

Para 2020, 100 millones de consumidores comprarán mediante realidad aumentada y más de 20% de las marcas abandonarán sus aplicaciones móviles

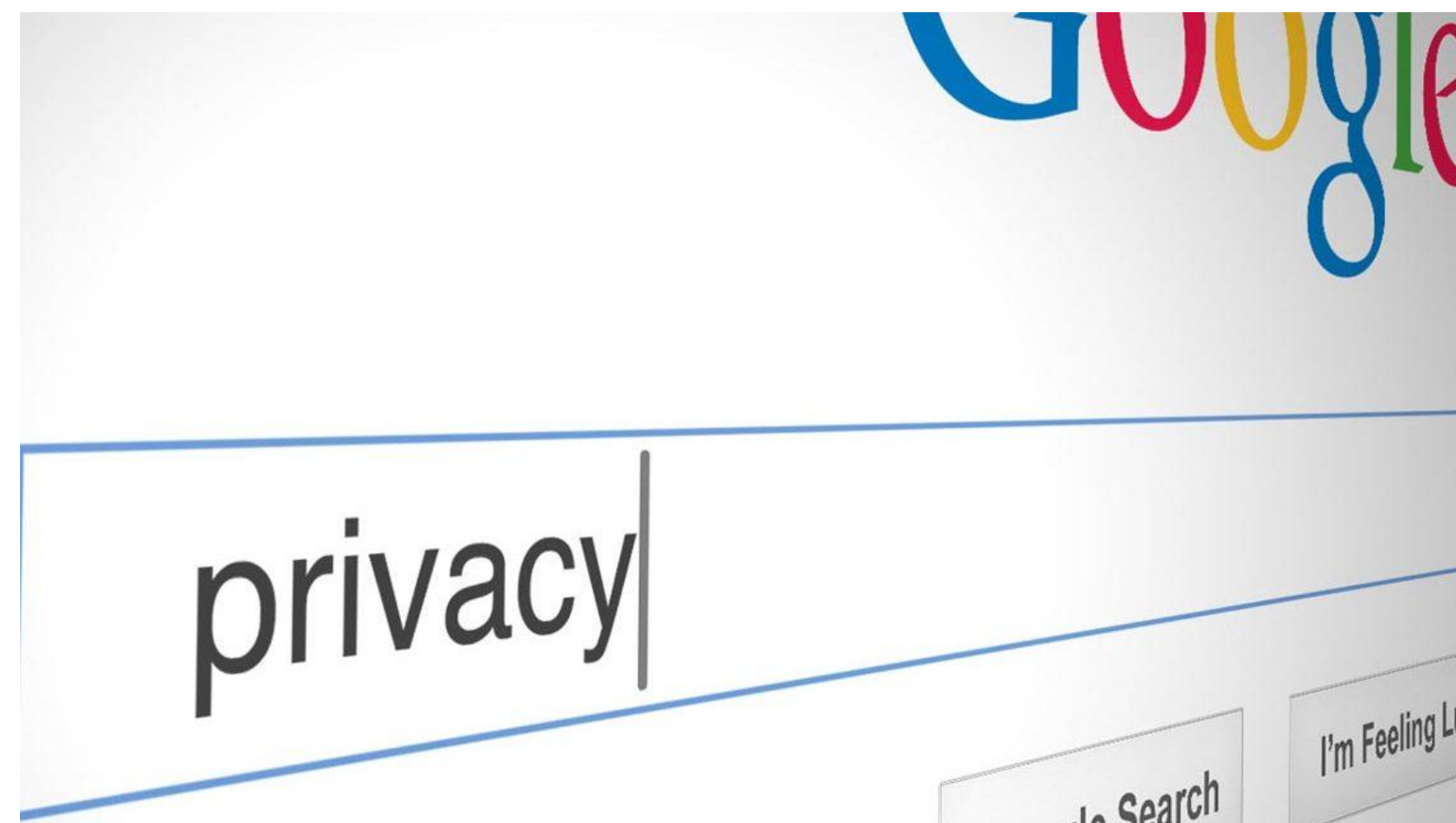
En los próximos 10 años, 30% de los trabajos en Bancos serán remplazados por Automatización de Procesos y Tecnologías Cognitivas

# Los próximos 10 años marcarán puntos de quiebre para varias tecnologías

Una investigación del Foro Económico Mundial muestra que entre 10 y 20 transiciones ocurrirán en los próximos 10 años

	AÑO PROMEDIO EN EL CUAL SE ESPERA EL PUNTO DE QUIEBRE						
2018	2021	2022	2023	2024	2025	2026	
							
<ul style="list-style-type: none"> <li>Almacenamiento para todos</li> </ul>	<ul style="list-style-type: none"> <li>Robots y Servicios</li> </ul>	<ul style="list-style-type: none"> <li>IoT</li> <li>Wearables</li> <li>3D Printing</li> </ul>	<ul style="list-style-type: none"> <li>Tecnologías implantables en humanos</li> <li>Súper computadora de bolsillo</li> </ul>	<ul style="list-style-type: none"> <li>Computación omnipresente</li> <li>Hogar 100% conectado</li> <li>Diagnóstico de la salud humana</li> </ul>	<ul style="list-style-type: none"> <li>3D en productos para cliente final</li> <li>Inteligencia artificial en puestos ejecutivos</li> </ul>	<ul style="list-style-type: none"> <li>Automóviles autónomos</li> <li>Ciudades inteligentes</li> <li>Toma de decision final por una Inteligencia Artificial</li> </ul>	
Hay transofrmaciones profundas que están ocurriendo rapidamente en la Sociedad humana cmo resultado de la evolución tecnológica							
Tecnologías Implantables					Revolución sensorial		
 El primer teléfono móvil implantable disponible comercialmente en 2023					 1 billón de sensores estará conectado a Internet en 2022		
El hogar conectado					Ciudades inteligentes		
 50% del tráfico de Internet será generado por los aparatos electrodomésticos en 2024					 La primera ciudad con más de 50.000 habitantes y sin semáforos en 2026		
Visión como nuevo artefacto					AI entra en el mundo corporativo		
 10% de las gafas de lectura se conectará					 La primera máquina de inteligencia artificial (AI) en una Junta Directiva por 2026		
Blockchain					Robótica y servicios		
 10% del producto interno bruto global (PIB) almacenado en la tecnología blockchain en 2027					 El primer fármaco robótico en los Estados Unidos en 2021		

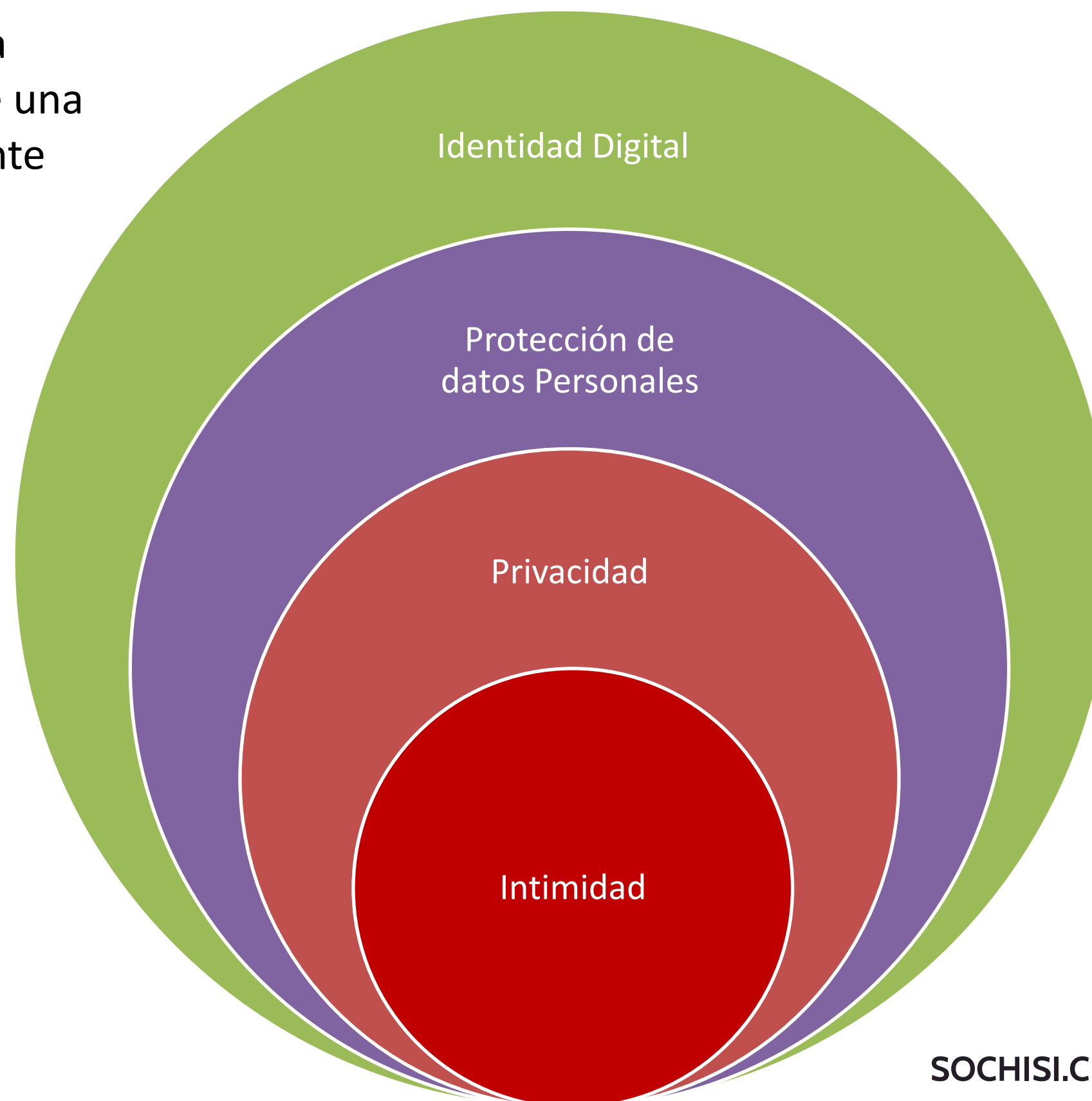
- En los tiempos que corren, el ámbito de **la privacidad y la protección de datos** se presenta como **uno de los principales desafíos** a los que se enfrenta nuestra sociedad. A nadie se le escapa el hecho de que cada vez se digitaliza nuestra vida diaria en mayor proporción, desde el ámbito de nuestro ocio y tiempo libre (redes sociales o servicios de mensajería instantánea), hasta el aspecto profesional y de relaciones con nuestra empresa y los organismos de la Administración Pública.





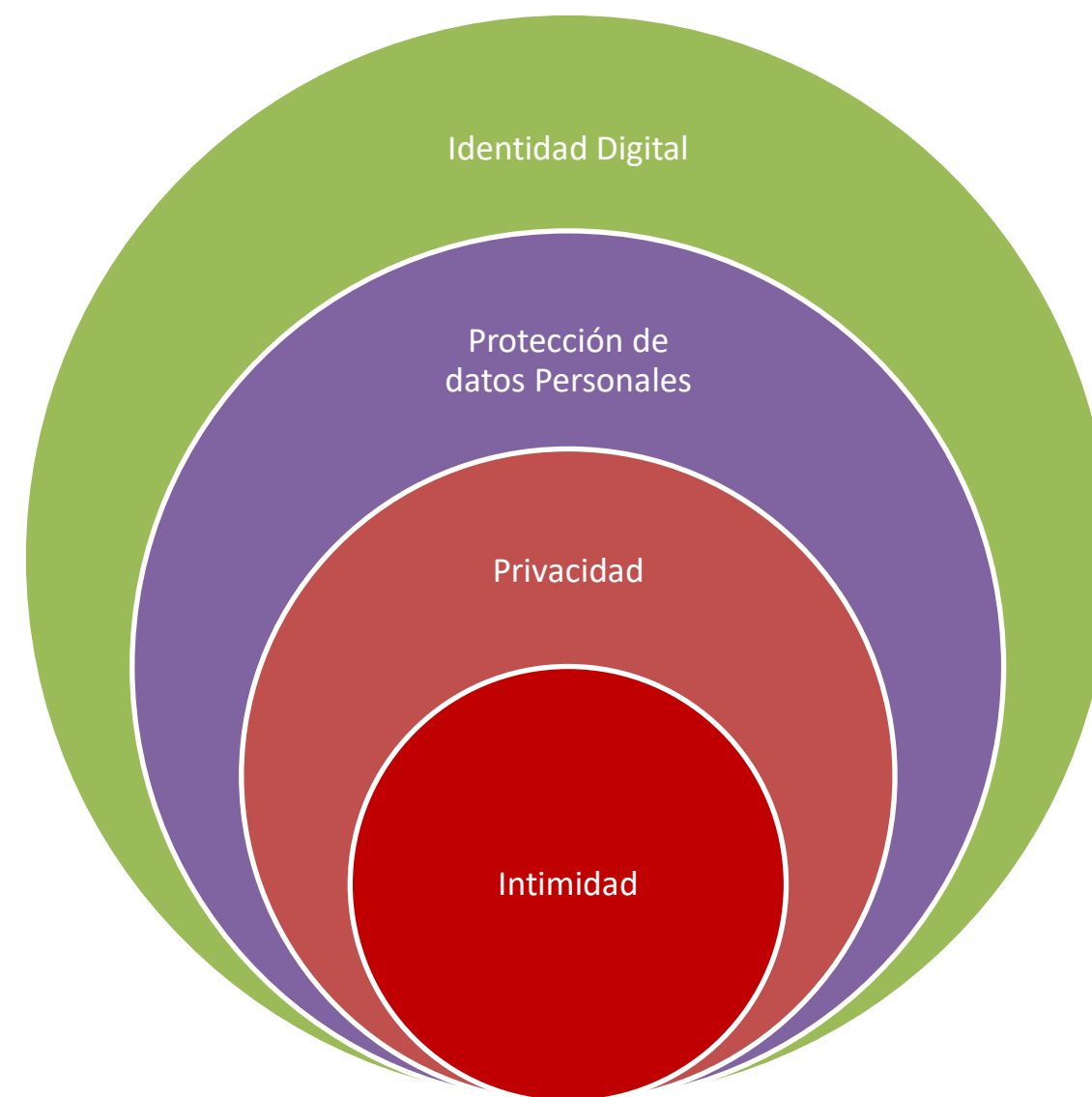
Según el diccionario de la RAE, por **intimidad** se debe entender una “zona espiritual íntima reservada de una persona o de un grupo, especialmente de una familia”.

Y, **privacidad** es el “ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión”.



La **Privacidad** es la parte mas profunda de la vida de una persona, que comprende sus sentimientos, vida familiar o relaciones de amistad. Según dicta el articulo 12 de la Declaración Universal de los Derechos Humanos:

*“Nadie será objeto de injerencias arbitrarias en **su vida privada**, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”\**



\* Art. 12 de la Declaración Universal de los Derechos Humanos



- Podríamos concluir que **los asuntos íntimos son privados, pero que no todos los asuntos privados son íntimos**. Hecha esta distinción, es el momento en el que entra en juego el derecho a la protección de datos de carácter personal.



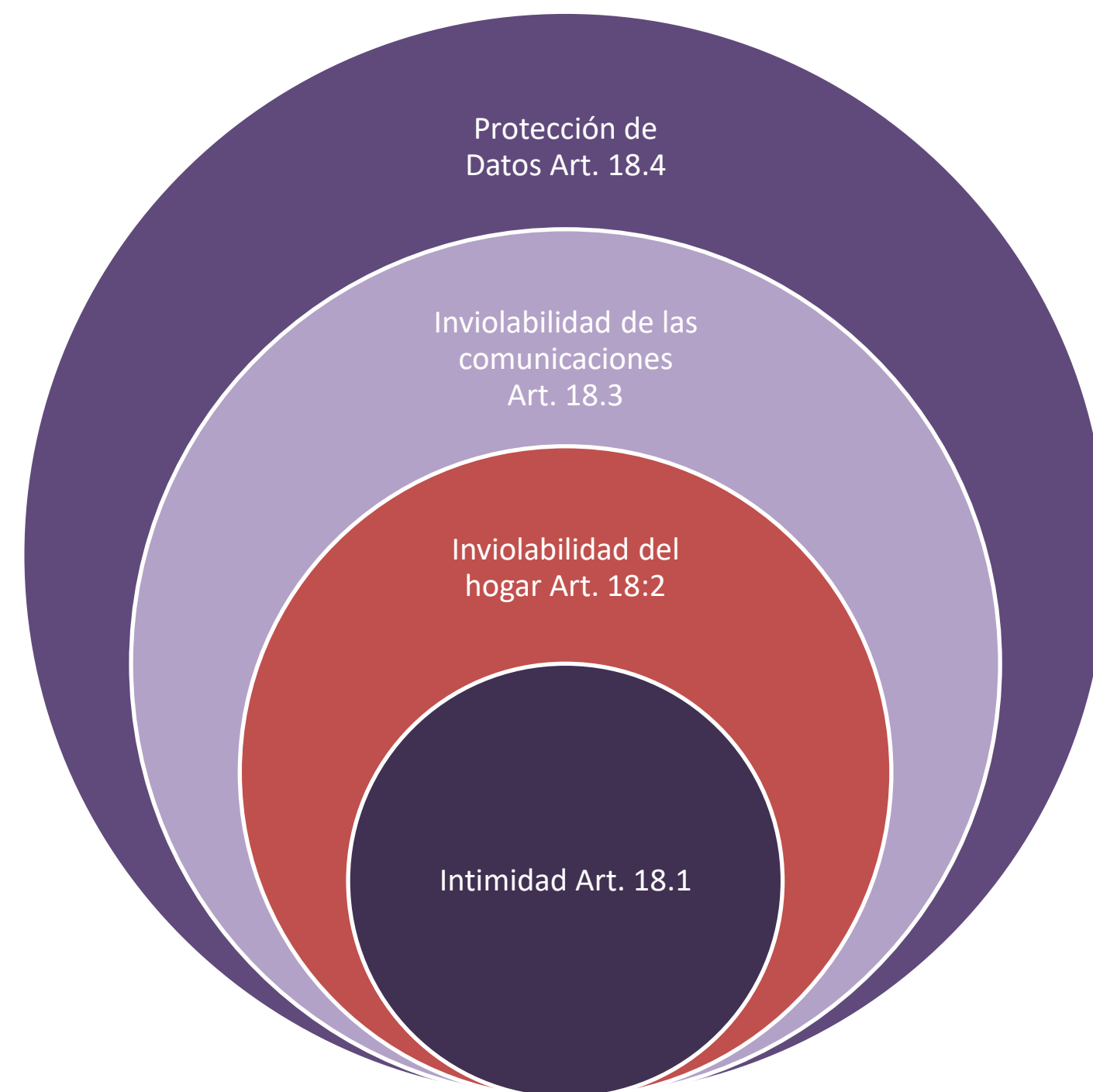
# INTIMIDAD vs PRIVACIDAD



Existe un elemento que es común tanto en el concepto de intimidad como en el de privacidad: el **tratamiento de la información personal**. La información es, entonces, el elemento fundamental, la materia de la que están formadas privacidad e intimidad. Y hablar de tratamiento de información es hablar de informática.

Son tres los derechos que protegen la esfera íntima del individuo.

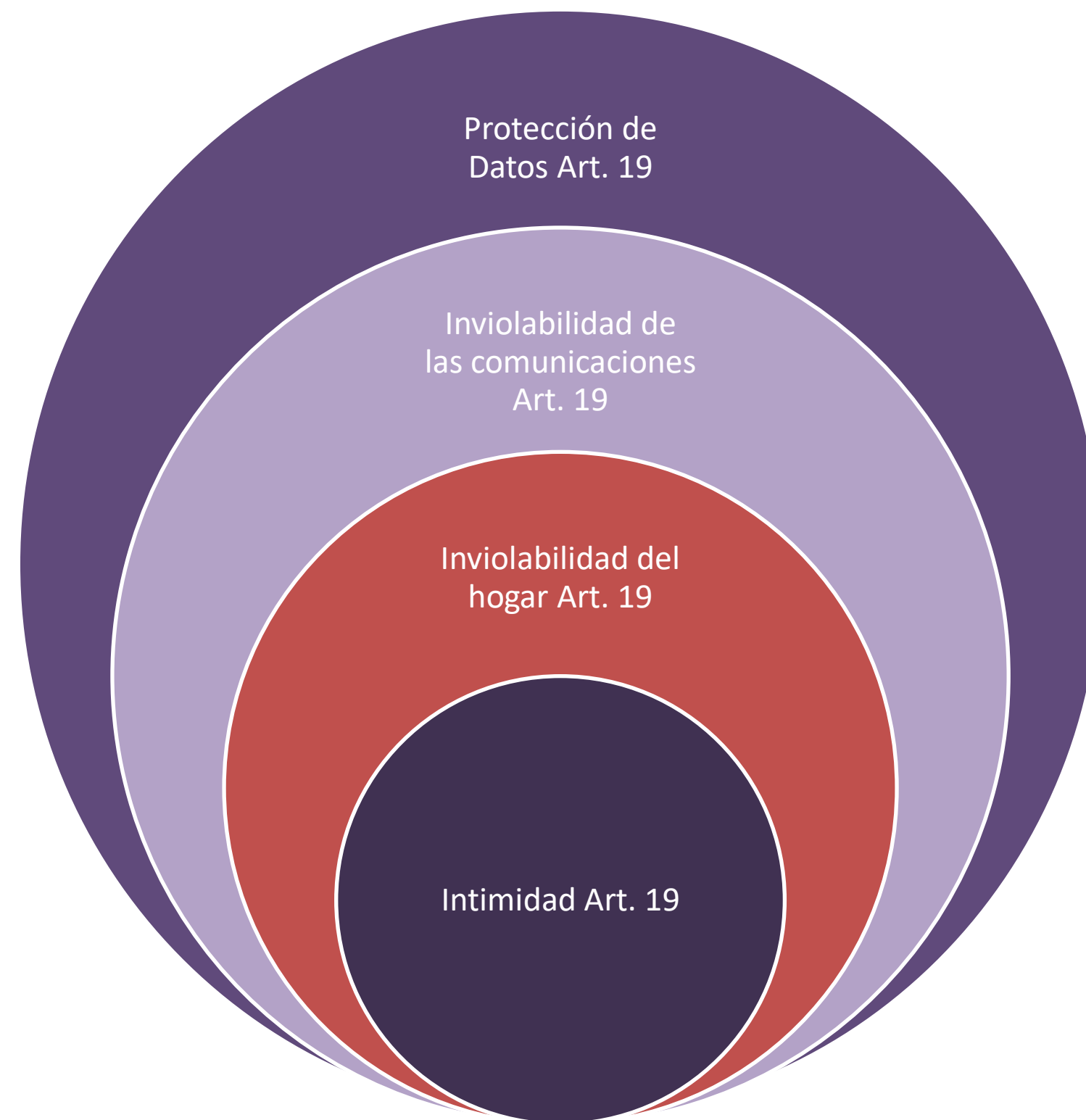
Si antes decíamos que no todo lo privado es íntimo pero todo lo íntimo es privado, ahora añadimos que no todos los datos personales son íntimos o privados, pero **todos son susceptibles de protección**.



\* Constitución Española de 1978

Por ejemplo, el **NIF (RUT/RUN)** de una persona no es un dato íntimo, ni siquiera privado, pero es un dato personal sobre el que el individuo tiene la capacidad de decidir a quién se lo proporciona. Sobre los datos que aparecen en una **cuenta bancaria** recae también el derecho a la protección, y además pueden ofrecernos una versión íntima del individuo. La **afiliación política** de una persona o su historial sanitario nos llevan un paso más allá, nos hablan de su esfera íntima.

No puede hablarse de un **límite exacto** que delimite dónde empieza y acaba cada derecho; la protección de datos surge en cualquier tratamiento de información personal, sea del carácter que sea, y abarca tanto la esfera de lo íntimo como de lo privado.



Art.19 de la Constitución de Chile

4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley;

5º.- La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley;



# Privacidad: Contexto

```
object to mirror  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True
```

```
selection at the end -add  
mirror_ob.select= 1  
mirror_ob.select=1  
context.scene.objects.active  
("Selected" - str(notify  
mirror_ob.select = 0  
= bpy.context.selected_objects  
data.objects[one.name].select  
print("please select exactly 1")
```

```
-- OPERATOR CLASSES -----
```

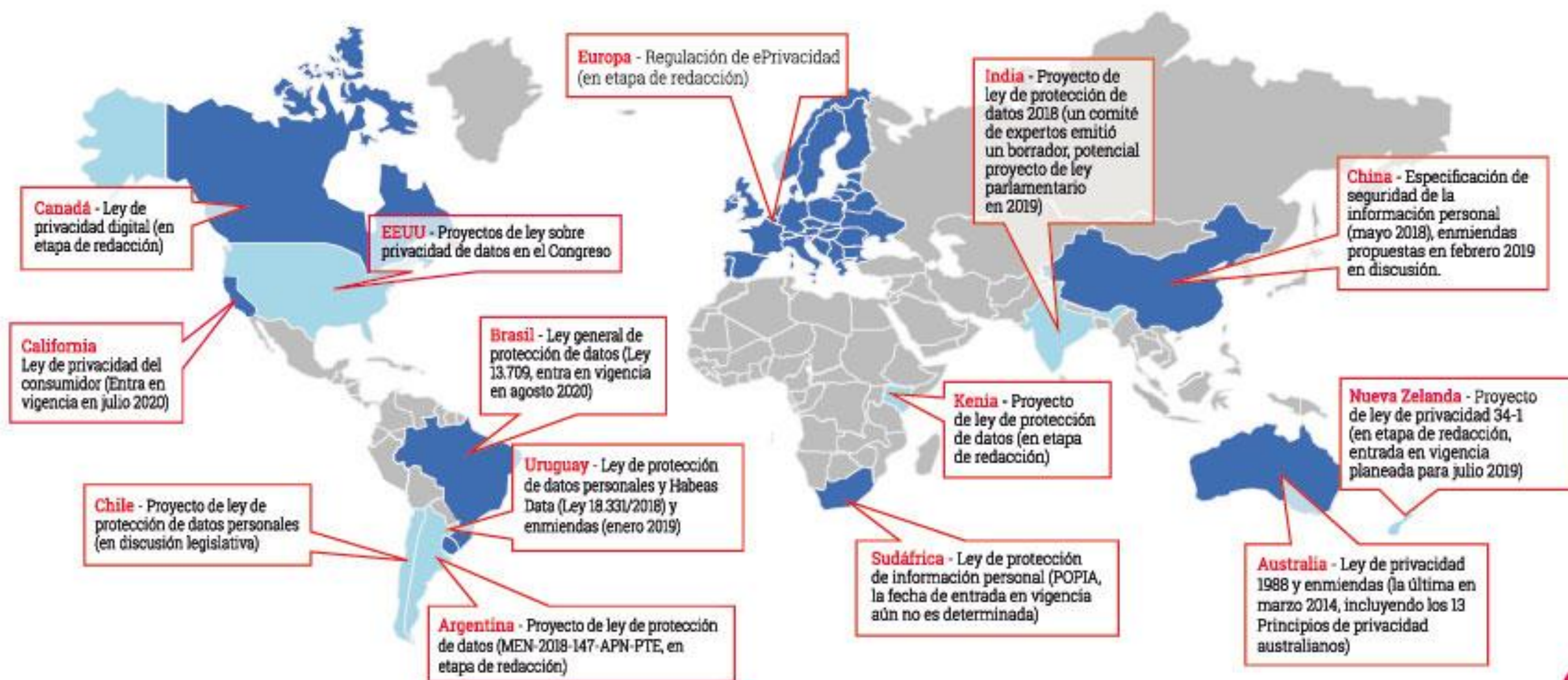
```
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"
```

```
is not
```



# Privacidad: Antecedentes

## Desarrollos legislativos más recientes en mercados claves\*



\* Focalizado solo en ciertos mercados claves para avisadores globales. No es una lista exhaustiva de todos los desarrollos legislativos en todos los países.



# Privacidad: Antecedentes

## Comparación con el marco de referencia del GDPR

- ✓ Marco de referencia es similar\* al GDPR
- ✗ Marco de referencia no es similar\* al GDPR

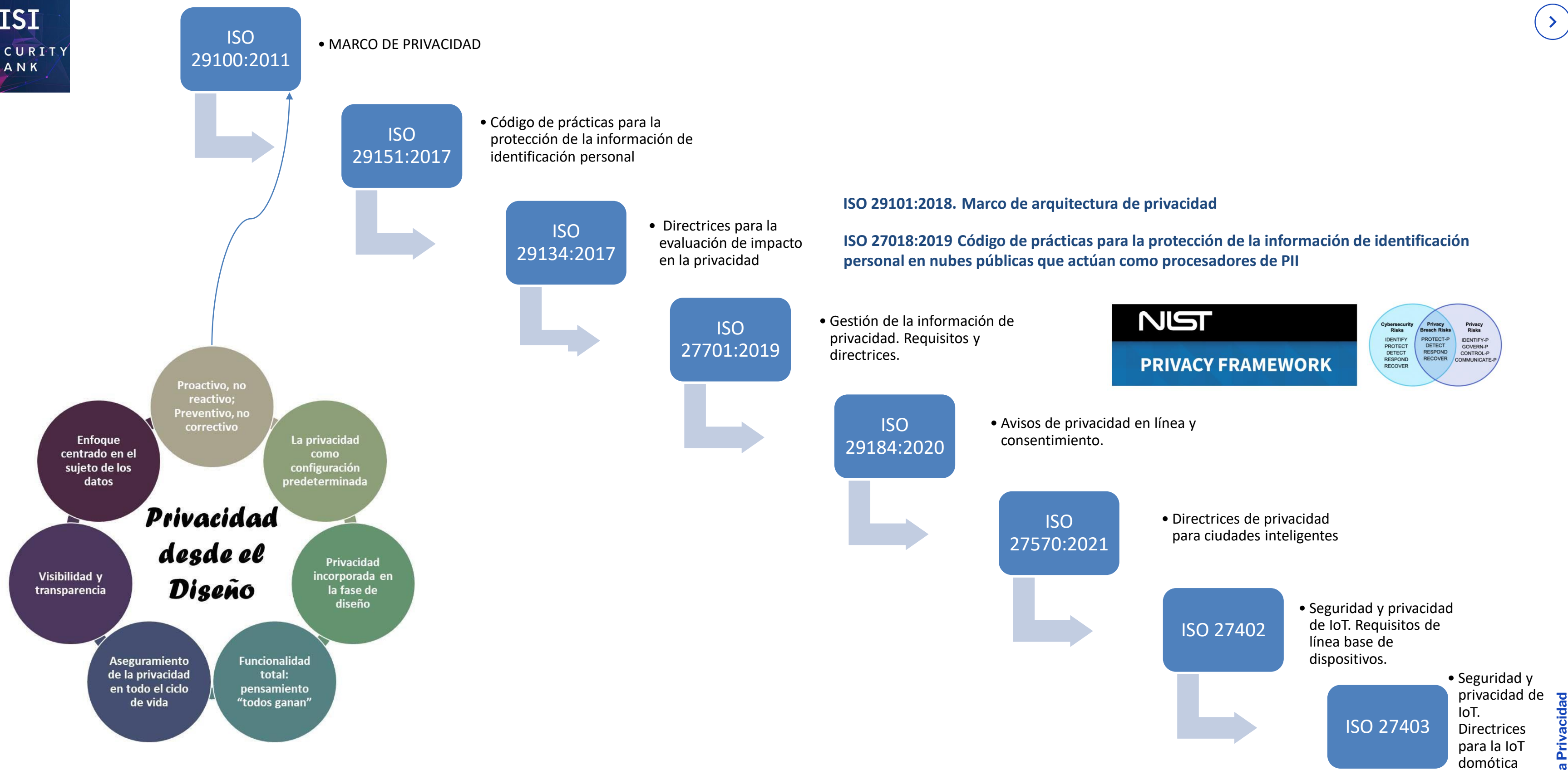
	ARG		AUS	BRA		CAN	CHL		CHN	IND	KEN	NZL		ZAF	URY		USA	
	Actual	Propuesta	Actual	Actual	Futuro	Actual	Actual	Propuesta	Actual Propuesta	Actual	Propuesta	Actual	Propuesta	Futuro	Previo	Actual	Actual (Federal)	Calidormia (CCPAI)
Alcance extra territorial	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓
Base para el procesamiento	✓	✓	✓	✗	✓	✗	✗	✓	✓	✗	✓	✗	✗	✓	✓	✓	✗	✗
Datos de niños	✗	✓	✗		✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗	✓	✓
Notificación de violación de datos	✗	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✓
Derecho al olvido	✗	✓	✗	✗	✓	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓
Sanciones	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
Agencia de protección de datos	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗
Evaluación de impacto	✗	✓	✗	✗	✓	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗



# Singularidad de la ISO 27701











ALGO SE ESTÁ MOVIENDO, EL NIVEL DE CONCIENCIA ESTÁ AUMENTANDO, LAS LEGISLACIONES SE ESTÁN ADECUANDO A LOS REQUERIMIENTOS DE LOS CIUDADANOS Y LOS MARCOS DE GESTIÓN SON PRUEBA DE ELLO.

INDEPENDIENTEMENTE DEL NIVEL DE MADUREZ, ESTAMOS ANTE UN MOVIMIENTO QUE VA A SEGUIR PROGRESIONES GEOMÉTRICAS EN LOS PRÓXIMOS AÑOS.

# Introducción. Historia

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)



Del RGPD a la ISO 27701

## Artículo 24 del RGPD:

*La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un **mecanismo de certificación aprobado** a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.*

## Artículo 42 del RGPD:

*Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de **mecanismos de certificación** en materia de protección de datos y de sellos y marcas de protección de datos a fin de **demostrar el cumplimiento** de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.*



# Introducción. Historia





## ARTÍCULO 32 DEL RGPD/GDPR

### Seguridad del tratamiento

•Teniendo en cuenta el ***estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas***, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la **seudonimización** y el **cifrado** de datos personales;
- b) la capacidad de garantizar la **confidencialidad, integridad, disponibilidad y resiliencia** permanentes de los sistemas y servicios de tratamiento;
- c) la capacidad de **restaurar la disponibilidad** y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- d) un proceso de **verificación, evaluación y valoración regulares** de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

•Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

# Introducción: Tres características. La 1ª

zadara

*Almacenamiento empresarial definido por software de última generación.*

Intereses organizacionales: 100% se centra en...

Intereses de las personas no entran en sus...



Zadara ha determinado un ALCANCE en 27001 alineado con sus objetivos de negocio. Esa certificación no abarca a toda la organización ni a todos sus procesos.

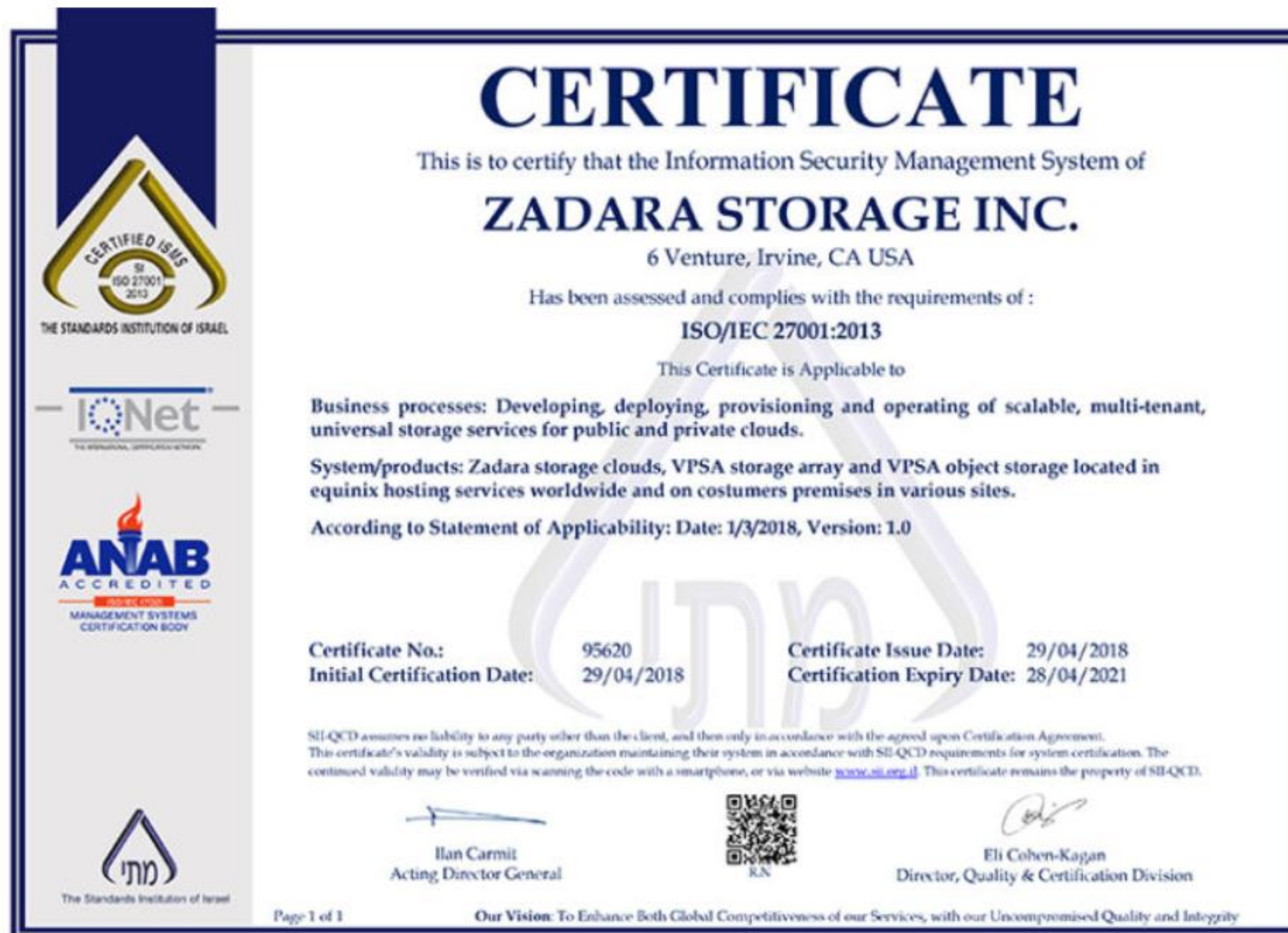


Pero la privacidad no se puede encapsular a un proceso o servicio, como sí en 27001. Es transversal a toda la organización porque en todos ellos, de una manera u otra, transita los datos personales.





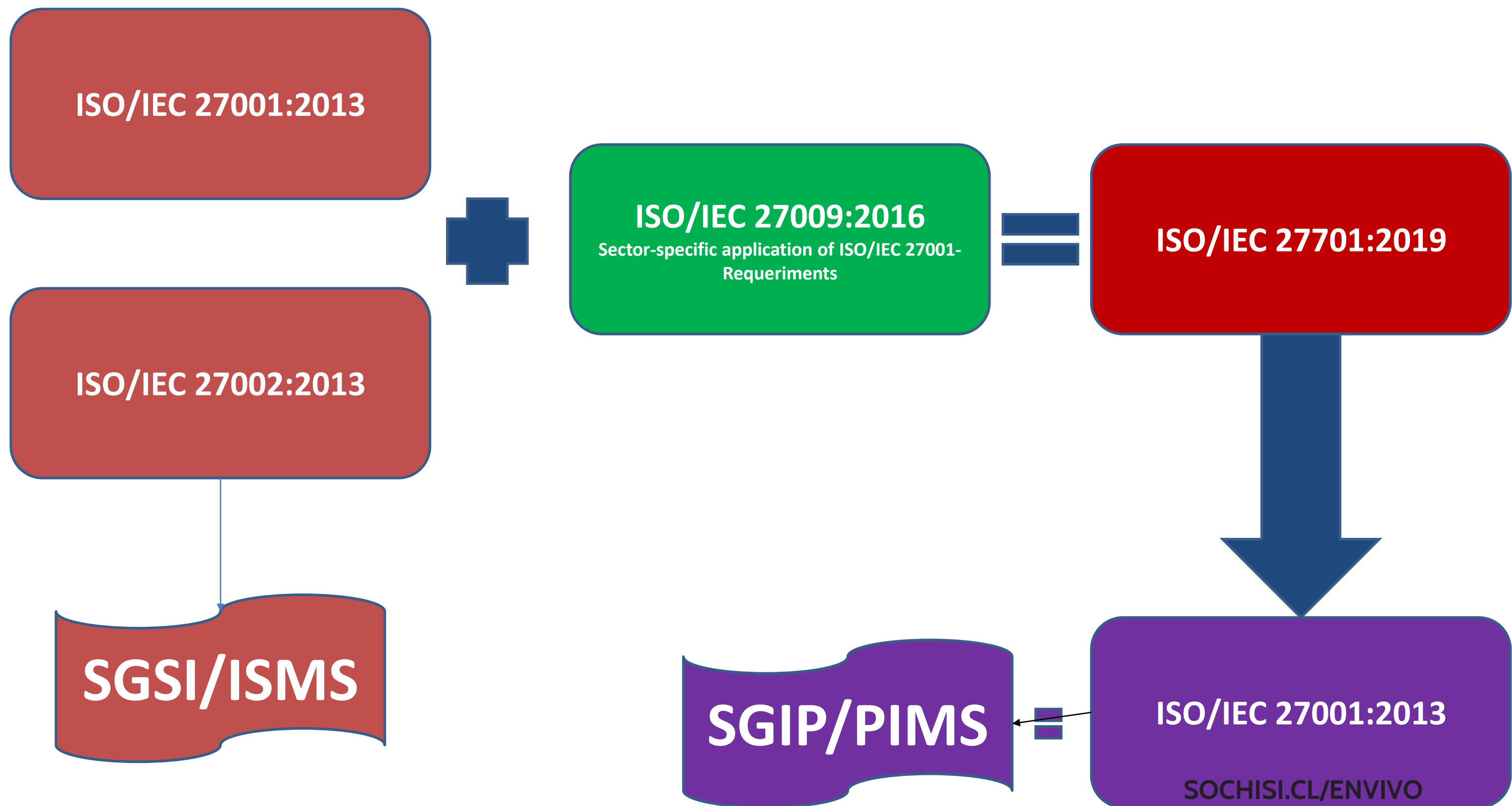
## Introducción: Tres características. 2ª





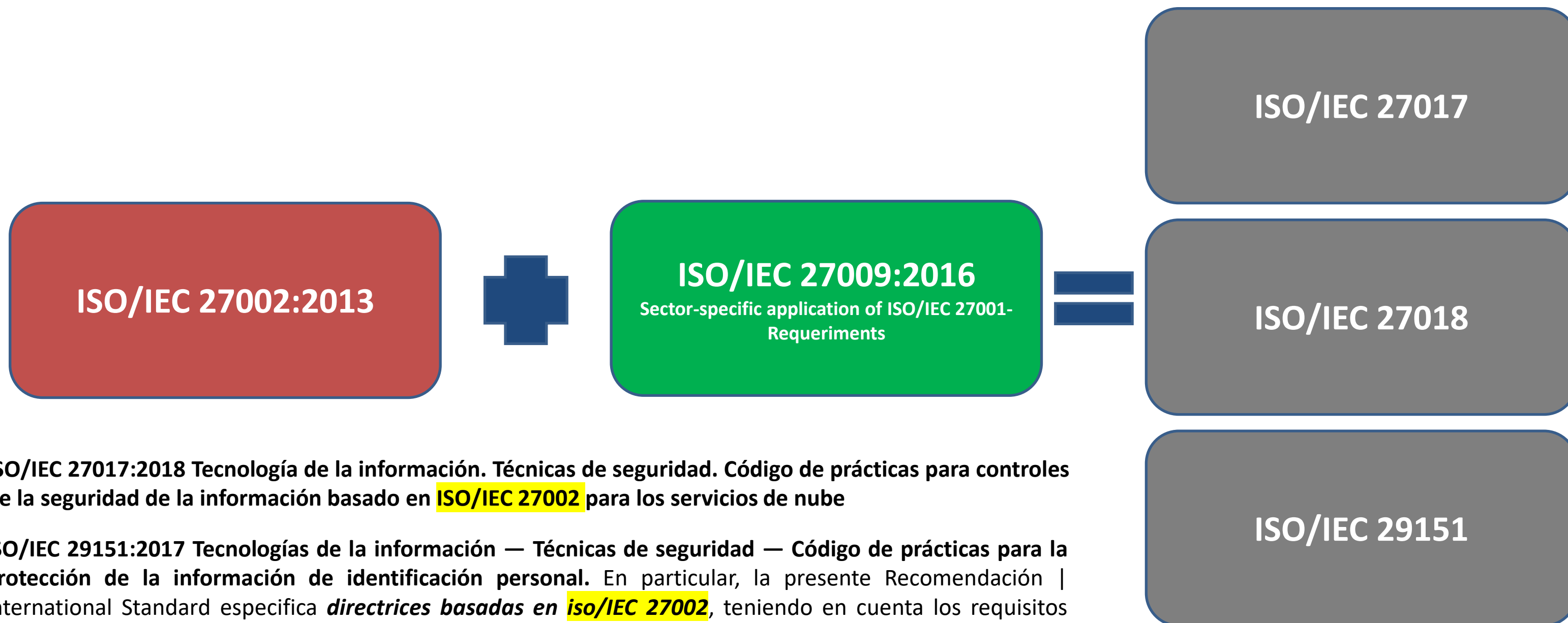


## Introducción: Tres características. 3ª





# Introducción: Tres características. 3ª



ISO/IEC 27017:2018 Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de la seguridad de la información basado en **ISO/IEC 27002** para los servicios de nube

ISO/IEC 29151:2017 Tecnologías de la información — Técnicas de seguridad — Código de prácticas para la protección de la información de identificación personal. En particular, la presente Recomendación | International Standard especifica *directrices basadas en iso/IEC 27002*, teniendo en cuenta los requisitos para el procesamiento de PII que pueden ser aplicables en el contexto de los entornos de riesgo de seguridad de la información de una organización.

ISO/IEC 27018:2019. Tecnología de la información — Técnicas de seguridad — Código de prácticas para la protección de la información de identificación personal (PII) en nubes públicas que actúan como procesadores pii. En particular, este documento especifica *directrices basadas en iso/IEC 27002*, teniendo en cuenta los requisitos reglamentarios para la protección de la PII que pueden ser aplicables en el contexto de los entornos de riesgo de seguridad de la información de un proveedor de servicios en la nube pública.





# Introducción. Conceptos

Gestión de la Seguridad de la Información  
Familia ISO 27000 / ISO 27701

INTERNATIONAL  
STANDARD

**ISO/IEC  
27701**

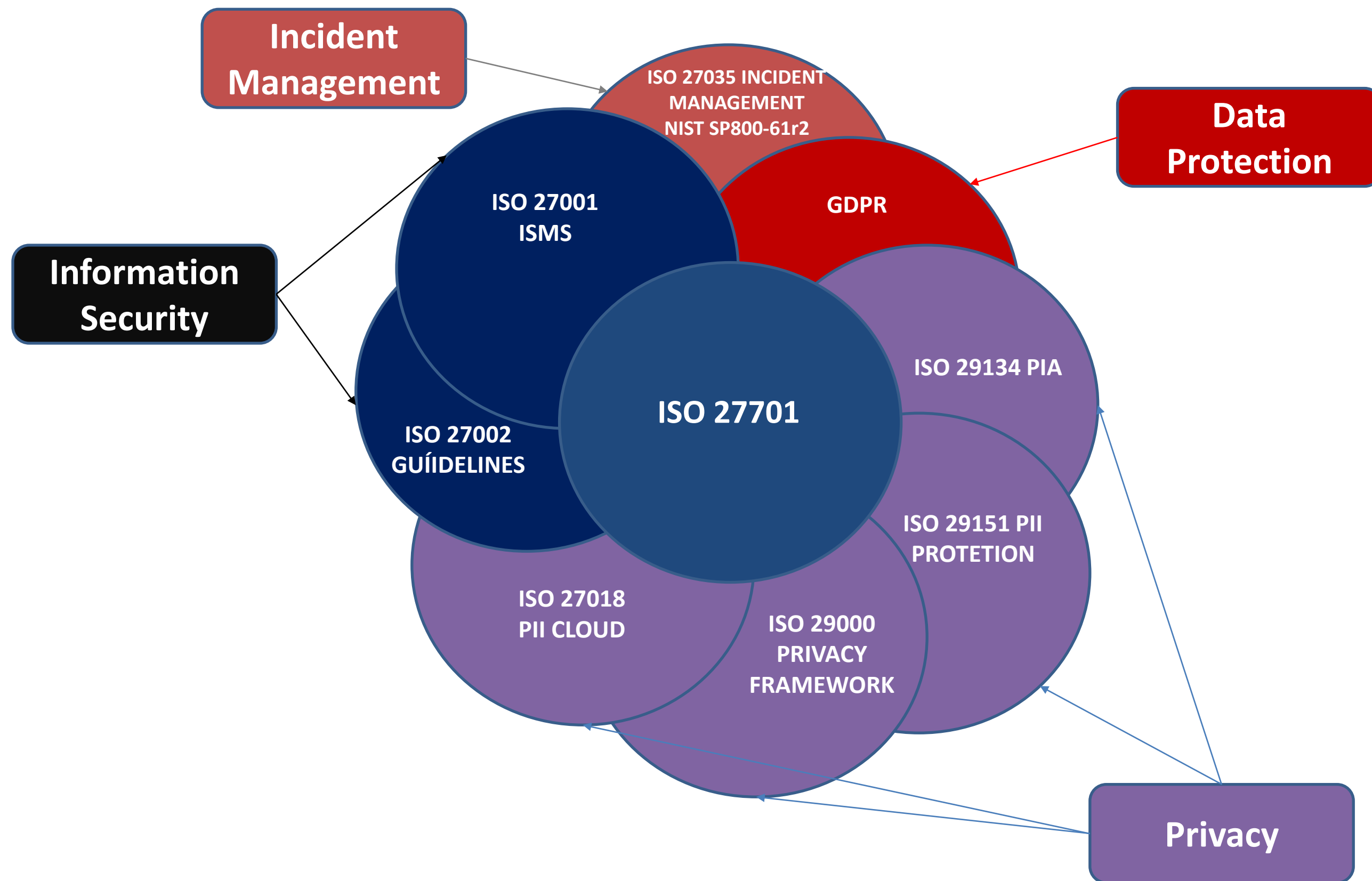
First edition  
2019-08

---

**Security techniques — Extension to  
ISO/IEC 27001 and ISO/IEC 27002 for  
privacy information management —  
Requirements and guidelines**

*Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC  
27002 au management de la protection de la vie privée — Exigences  
et lignes directrices*

# Introducción. Conceptos







# Introducción. Conceptos

- ISO/IEC 27701 incorpora **requerimientos adicionales para el SGSI** de modo que cubra también los aspectos específicos **sobre privacidad** y que puedan extender el sistema de gestión para que la organización genere **evidencias de un adecuado cumplimiento** de las leyes y regulaciones en materia de privacidad o protección de datos personales.
- El **resultado** de la aplicación de ISO/IEC 27701 será la **transformación de un SGSI en un SGIP** que aporte valor a la organización no solo en la protección de la información organizacional sino en el cumplimiento de sus responsabilidades sobre privacidad, tanto si se trata de un responsable como si se trata de un encargado de tratamiento.

# Introducción. Conceptos

Conceptos ISO 27701 / 29100

ISO 27701 toma algunas de sus definiciones clave de ISO 29100, que utiliza términos que difieren de algunas otras fuentes. Es útil comprenderlos y cómo se relacionan con su entorno legal y regulatorio.

- **Información de Identificación Personal (PII):** Información de Identificación Personal (IIP), se corresponde con la denominación de “**Datos Personales**” del RGPD.
- **Privacy Information Management System (PIMS):** *Sistema de Gestión de Información de Privacidad* (SGIP), pero que debe estar en alineación directa con el Sistema de Gestión de Seguridad de la Información (SGSI) de ISO 27001.
- **Principal de PII:** Interesado. ‘*Sujeto de datos*’ en el GDPR. ISO 29100 define esto como una "persona física con quien se relaciona la información de identificación personal (PII)" (Cláusula 2.11)
- **Controlador de PII:** Responsable del tratamiento. ‘*Controlador de datos*’ en el GDPR. ISO 29100 define esto como el “interesado en la privacidad (o interesados en la privacidad) que determina los propósitos y medios para procesar la información de identificación personal (PII) que no sean personas físicas que usan datos para propósitos personales” (Cláusula 2.12)
- **Procesador de PII:** Encargado del tratamiento. ‘*Procesador de datos*’ en el GDPR. ISO 29100 define esto como el "interesado en la privacidad que procesa la información de identificación personal (PII) en nombre y de acuerdo con las instrucciones de un controlador de PII"
- **Third parties:** Terceras partes que reciben la IIP de los responsables y los encargados.



# Introducción. Conceptos

Términos tal como aparecen en ISO/IEC 27701	Términos alternativos
Sistema de gestión de información de privacidad (PIMS)	Sistema de gestión de información personal (PIMS)
Información de identificación personal (PII)	Información personal
Principal PII	Sujeto de datos (Titular de los datos)
<u>Privacidad por diseño</u>	Protección de datos por diseño.
<u>Privacidad por defecto</u>	Protección de datos por defecto
Controlador PII	Controlador (Responsable del Tratamiento)
Procesador PII	Procesador (Encargado del Tratamiento)

# INTRODUCCIÓN. BENEFICIOS







# ESTRUCTURA



# ESTRUCTURA

## ESTRUCTURA PRINCIPAL DE ISO 27701:

Cláusula	Descripción
1	Alcance
2	Referencias normativas
3	Términos y definiciones
4	General
5	Requisitos de PIMS relacionados con ISO/IEC 27001
6	Orientación PIMS relacionada con ISO/IEC 27002
7	Orientación para los controladores PII
8	Orientación para procesadores PII

1	Scope .....	1
2	Normative references .....	1
3	Terms, definitions and abbreviations .....	1



# ESTRUCTURA

## EXPLICACIONES DE ANEXOS EN ISO 27701:

Anexo	Descripción
A	Objetivos de control de referencia para controladores/Responsables de Tratamientos
B	Objetivos de control de referencia para procesadores/Encargados de Tratamientos.
C	Asignación a ISO/IEC 29100
D	Mapeo al RGPD/GDPR
E	Asignación a ISO/IEC 27018 e ISO 29151
F	Cómo aplicar ISO/IEC 27701 a ISO/IEC 27001 e ISO/IEC 27002

37

Orientación de la Cláusula 6	Cláusula 7 de iso/IEC 27701	Controles del Anexo A	Aplicable a controllers de PII
	Cláusula 8 de iso/IEC 27701	Controles del Anexo B	Aplicable a procesadores PII



# ESTRUCTURA

## MAPPING DE ISO/IEC 27701 CON ISO/IEC 29100 Privacy Framework:

ISO/IEC 29100 es un marco de privacidad que tiene 11 principios que se dan a continuación.

1	Consentimiento y elección
2	Propósito de legitimidad y especificación
3	Limitación de cobro
4	Minimización de datos
5	Limitación de uso, retención y divulgación
6	Precisión y calidad
7	Apertura, transparencia y aviso
8	Participación y acceso individuales
9	Responsabilidad
10	Seguridad de la información
11	Cumplimiento de la privacidad

ISO/IEC 27701 tiene sus diferentes controles aplicables a los controladores PII y al procesador PII. Estos controles se asignan a diferentes principios de privacidad enunciados en el marco de privacidad ISO/IEC 29100.

ISO/IEC 27701 Anexo C (Asignación a ISO/IEC 29100)	Cláusula 7 de iso/IEC 27701	Controles del Anexo A	Aplicable a los controladores PII
	Cláusula 8 de iso/IEC 27701	Controles del Anexo B	Aplicable a procesadores PII





# ESTRUCTURA

## MAPEO DE ISO/IEC 27701 CON GDPR:

El Anexo D de la NORMA/IEC 27701 proporciona la cartografía con el Reglamento General de Protección de Datos. Por lo tanto, el cumplimiento de los requisitos de ISO/IEC 27701 también ayuda a cumplir los requisitos para el RGPD.

Sin embargo, es importante señalar que el Anexo D de la ISO/IEC 27701 es de carácter informativo y que corresponde a la diligencia de organización determinar las obligaciones legales que les son aplicables y cómo deben cumplirse.

La adopción e implementación de ISO/IEC 27701 puede ayudar a reducir el riesgo de privacidad garantizando los derechos de los principios de PII y la implementación de controles de privacidad. Esto protege posteriormente a las organizaciones de posibles violaciones de datos que puedan causar más riesgo para la reputación de la empresa y la insatisfacción del cliente.

El establecimiento exitoso, el mantenimiento y la mejora continua de este sistema de gestión pueden cosechar los beneficios de una mayor ventaja competitiva, confianza del cliente y confianza en la forma en que una organización se comporta en la protección de los derechos de privacidad de sus principales de PII

# ESTRUCTURA

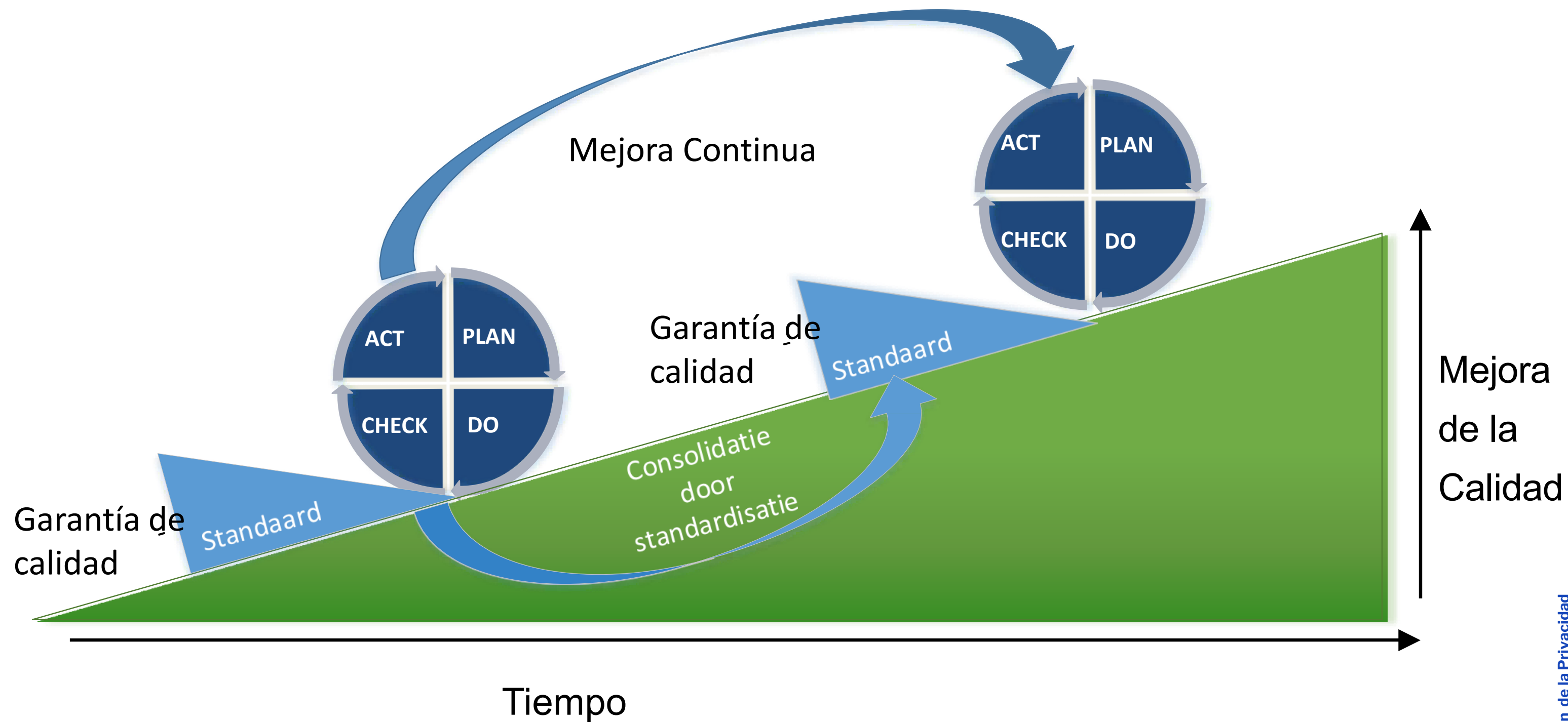
## PRINCIPIO BÁSICO DE ISO: PDCA





# ESTRUCTURA

## PDCA

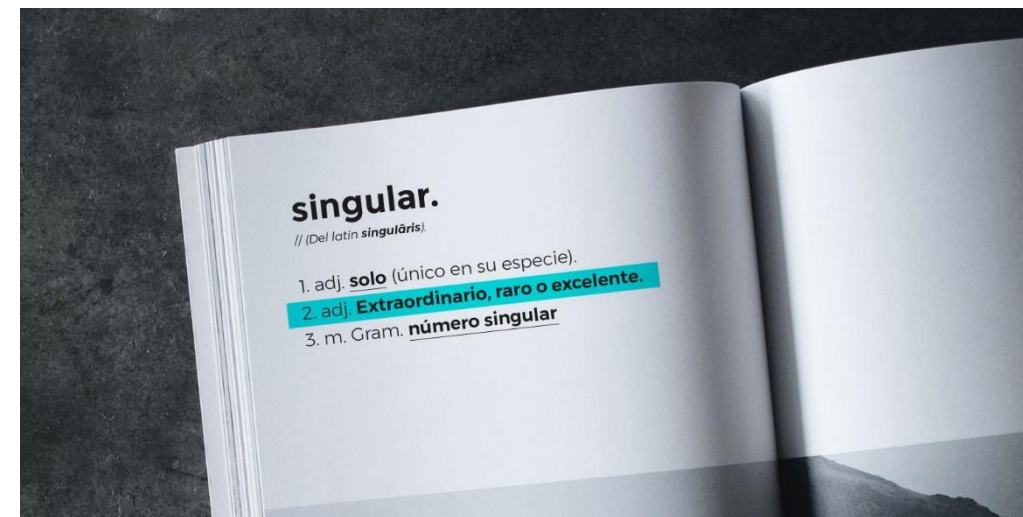




# GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. FAMILIA ISO 27000/ISO 27701



# INTRODUCCIÓN



## 5.1 Generalidades

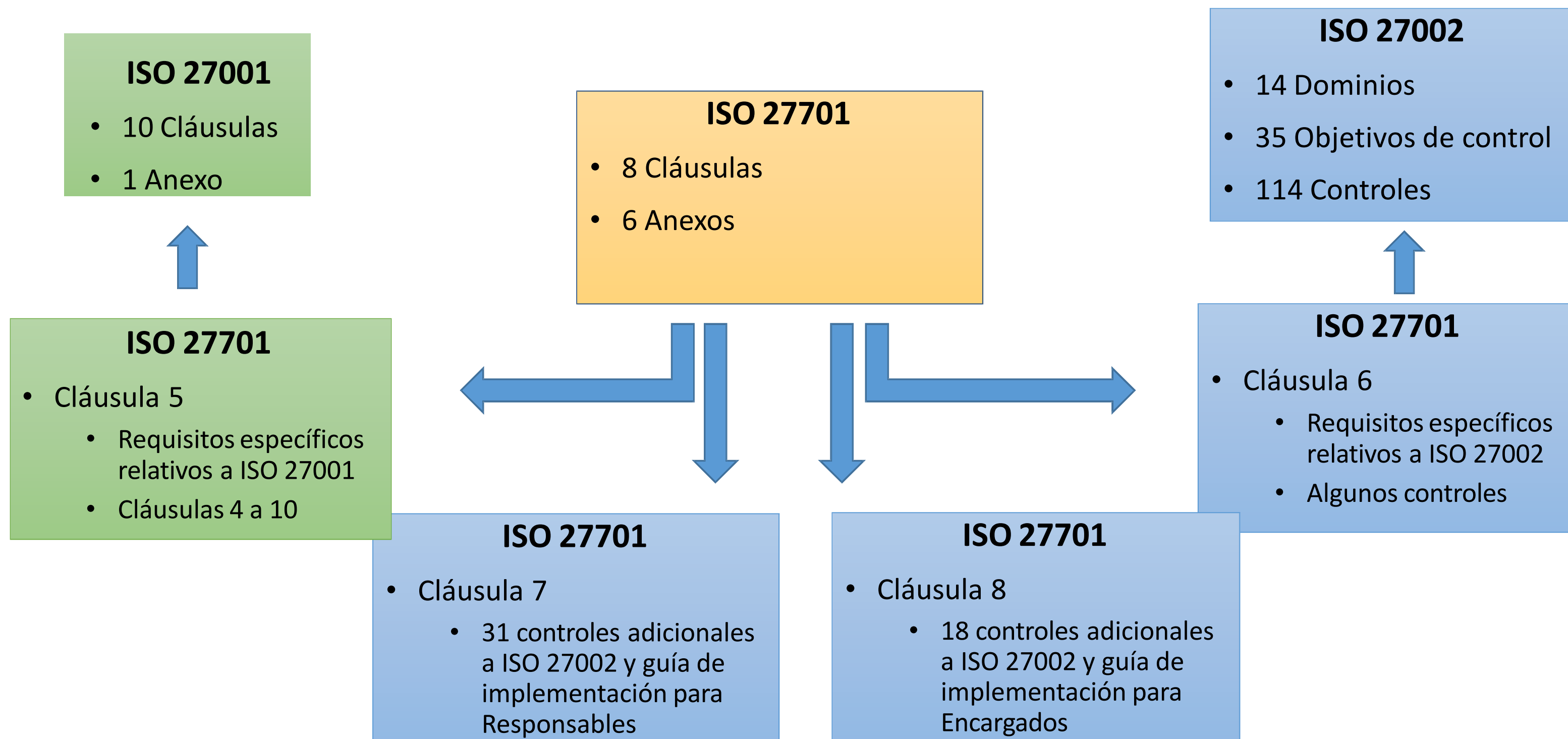
Los requisitos de ISO/IEC 27001:2013 que mencionan la "seguridad de la información" debe **extenderse** a la protección de la privacidad como potencialmente afectada por el procesamiento de IIP.

NOTA: En la práctica, donde se usa "seguridad de la información" en la ISO/IEC 27001:2013, se aplica en su lugar "**seguridad de la información y privacidad**" (véase Anexo F)

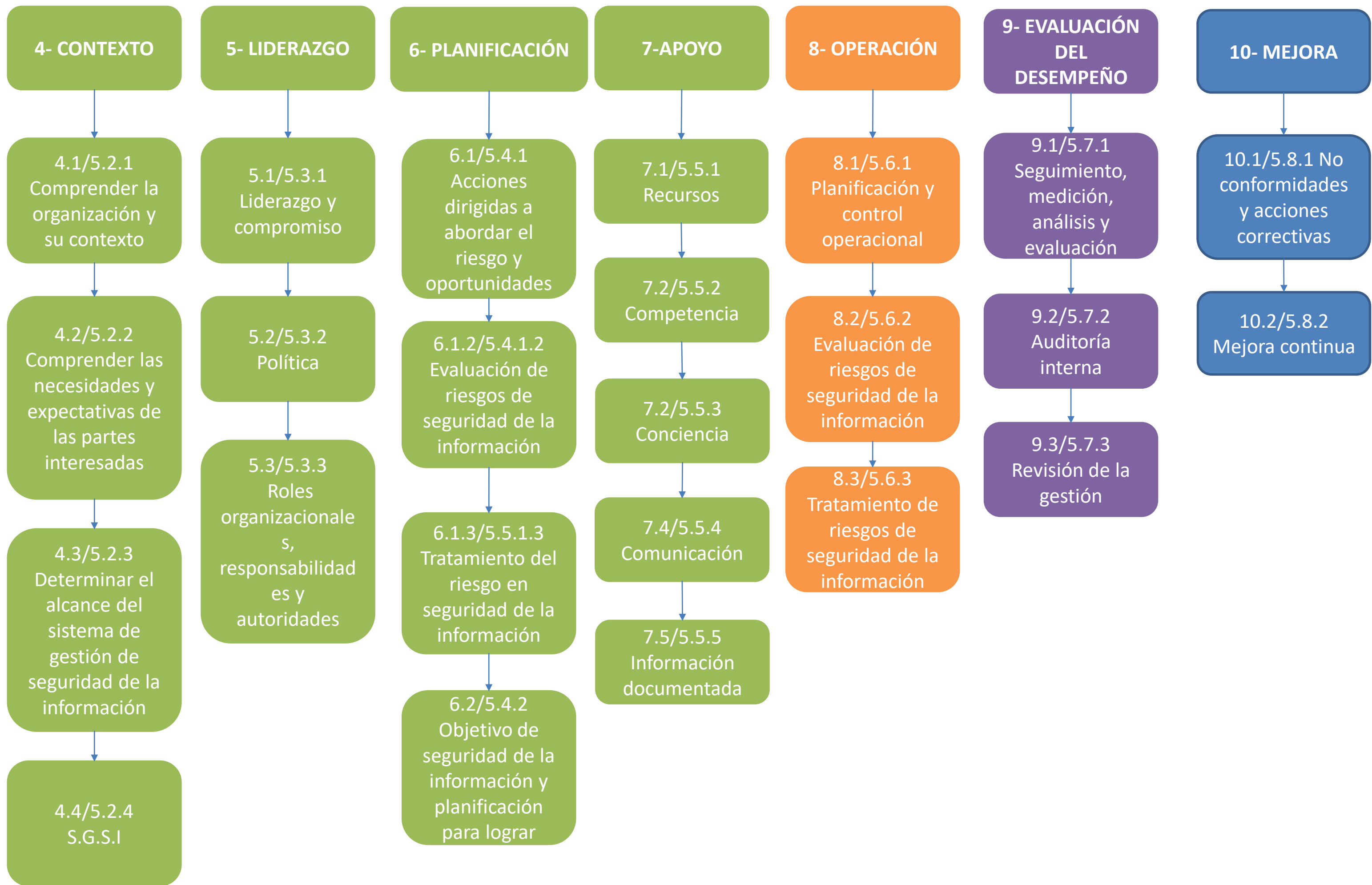
\* Esta nota modifica toda la norma, todas sus cláusulas. Pero hay requisitos adicionales que se incorporan a la cláusula 4 y a la 6

# Introducción

Relación ISO 27001, ISO 27002 e ISO 27701









# INTRODUCCIÓN

Asignación de ISO27701 a ISO27001

Requisitos de ISO27001 (ISO27701 Cláusula 5)

ISO27701	Tema	ISO27001	Observación
5.2	Contexto de la organización	4	Modificado
5.3	Liderazgo	5	Directo
5.4	Calendario	6	Modificado
5.5	Apoyo	7	Directo
5.6	Operación	8	Directo
5.7	Evaluación del desempeño	9	Directo
5.8	Mejora	10	Directo



# INTRODUCCIÓN

Asignación de ISO27701 a ISO27002  
Requisitos de ISO27002 (ISO27701 Cláusula 6)

ISO27701	Tema	ISO27002	Observación
6.2	Políticas	5	Modificado
6.3	Organización	6	Modificado
6.4	HORA	7	Modificado
6.5	Gestión de activos	8	Modificado
6.6	Control de acceso	9	Modificado
6,7	Criptografía	10	Modificado
6,8	Físico y medio ambiente	11	Modificado





# INTRODUCCIÓN

Asignación de ISO27701 a ISO27002

Requisitos de ISO27002 (ISO27701 Cláusula 6)

ISO27701	Tema	ISO27002	Observación
6,9	Operaciones	12	Modificado
6,10	Comunicaciones	13	Modificado
6.11	Adquisición, desarrollo y mantener.	14	Modificado
6.12	Proveedores	15	Modificado
6.13	Gestión de incidentes	16	Modificado
6.14	Continuidad del negocio	17	Directo
6.15	Cumplimiento	18	Modificado

# IMPLANTACIÓN ISO 27701







*“La privacidad es mucho más que una simple obligación de cumplimiento. Constituye un derecho humano fundamental y un imperativo empresarial para construir y mantener la confianza de los clientes”, comenta Harvey Jang, Vicepresidente y Director de Privacidad en Cisco.*

**SOCHISI.CL/ENVIVO**



12 MARZO 2021

# ¡Muchas Gracias!

“GESTIÓN DE LA PRIVACIDAD”

**Speaker:**

LEOCADIO MARRERO TRUJILLO

**Linkedin**

[www.linkedin.com/in/leocadio-marrero](https://www.linkedin.com/in/leocadio-marrero)

---

SOCHISI.CL/ENVIVO

**II CONGRESO DE  
SEGURIDAD DE LA  
INFORMACIÓN Y  
CIBERSEGURIDAD**



**SOCHISI**

DIGITAL SECURITY  
THINK TANK