Organiza:

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Partners Estratégicos:

Telefónica

GOVERTIS
Advisory Services

Introducción práctica a la ISO 27701:2019
Nuevo estándar internacional de protección de datos

Borja Romano Arenas

Information, Security & Risk Consultant
GOVERTIS Advisory Services, S.L.

Presentación

Borja Romano Arenas

Ingeniería Técnica Informática de Sistemas por la Universidad de Oviedo.

Auditor líder para:

- Sistemas de Gestión de Calidad (ISO 9001) IRCA
- Sistemas de Gestión de Seguridad de la Información (ISO 27001) IRCA
- Esquema Nacional de Seguridad (ENS)
- Sistemas de Gestión de Continuidad de Negocio (ISO 22301) IRCA
- Sistemas de Gestión Emergencias (ISO 22320) por Applus+
- Sistemas de Gestión de Servicios de Tecnologías de la Información (ISO 20000)

Más de 10 años de experiencia en consultoría y auditoría de Sistemas de Gestión de Seguridad de la Información, Calidad, Servicios de TI, Emergencias, Desarrollo de Software, Medio ambiente, Continuidad de Negocio…

LOPD, RGPD, LOPDGDD, Esquema Nacional de Seguridad…

Índice

- Presentación
- Introducción
  - Historia
  - Conceptos
  - Relación ISO 27001, ISO 27002 e ISO 27701
- Análisis ISO 27701
  - Estructura
  - Cláusulas
    - 27001
    - 27002
    - Responsables
    - Encargados
- Implantación ISO 27701

Introducción

Historia

Gestión de la Seguridad de la Información
Información de privacidad

Introducción

Historia

1995
- BS 7799-1
- Buenas prácticas

1998
- BS 7799-2
- Certificable

1999
- BS 7799-1
- Revisión

2000
- ISO/IEC 17799
- ISO en base a BS 7799-1

2004
- UNE 71502

2005
- **ISO/IEC 27001**
- Revisión ISO/IEC 17799

Introducción

Historia

2007
- Nueva versión ISO/IEC 27001
- ISO/IEC 17799 pasa a llamarse ISO 27002

2011
- ISO/IEC 29100 - Framework Privacidad

2013
- Revisión ISO/IEC 27001 e ISO/IEC 27002

2016
- RGPD

2017
- Revisión ISO/IEC 27001 e ISO/IEC 27002
- ISO/IEC 29151 – Buenas prácticas privacidad

2018
- LOPDGDD

2019
- ISO/IEC 27701
- Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad

Introducción

Historia

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.*

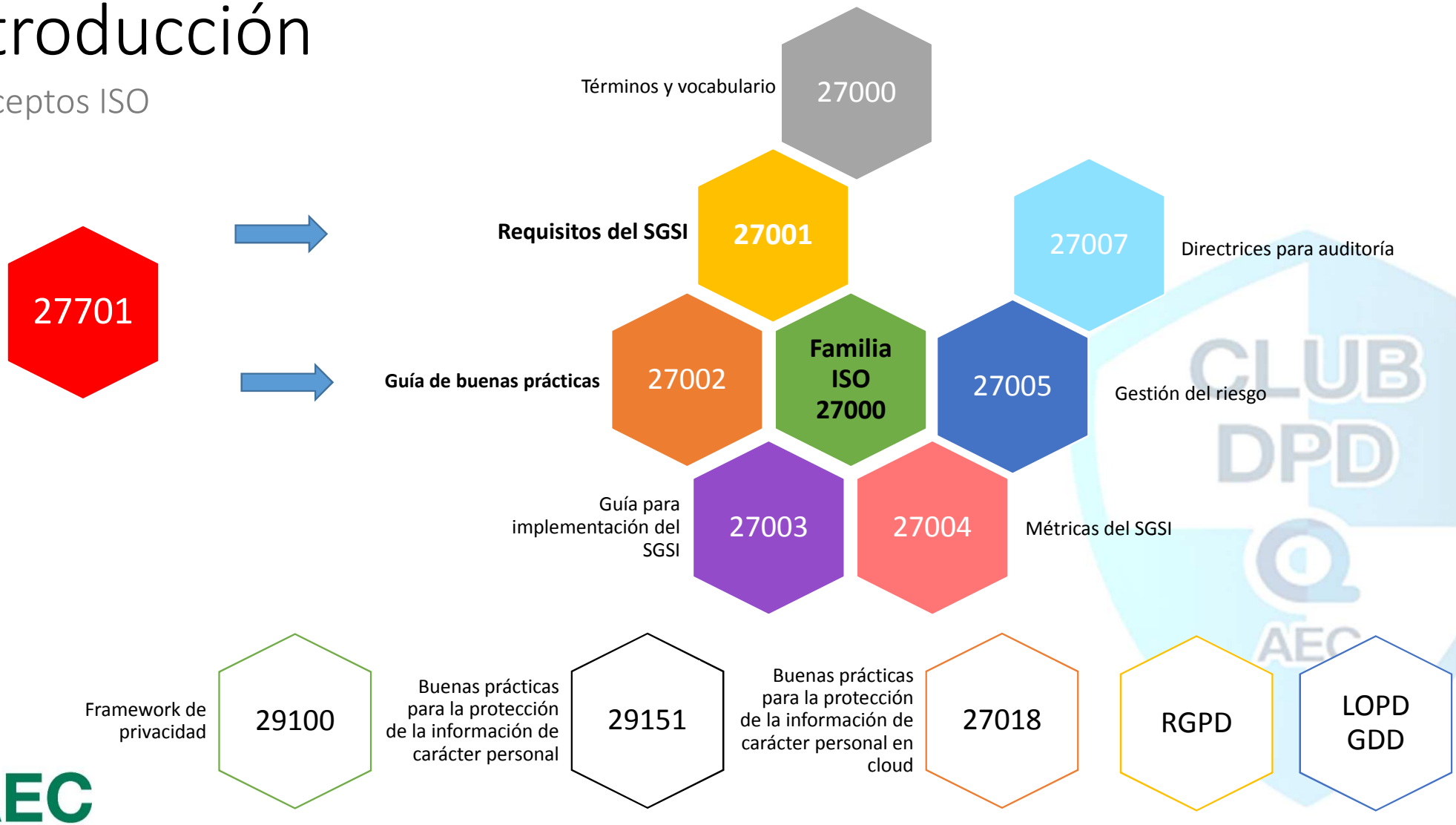
Introducción

Conceptos

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

Introducción

Conceptos ISO



Introducción

Conceptos 27701

- 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 ISO 27701 / 29100

- **Personally Identifiable Information (IIP)**: Información de Identificación Personal (IIP), se corresponde con la denominación de "Datos Personales" de la LOPDGDD o al concepto de "Datos de carácter personal" de la antigua LOPD
- **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.
- **IIP Principal:** Interesado
- **IIP Controller:** Responsable del tratamiento
- **IIP Processor:** Encargado del tratamiento
- **Third parties:** Terceras partes que reciben la IIP de los responsables y los encargados.

Introducción

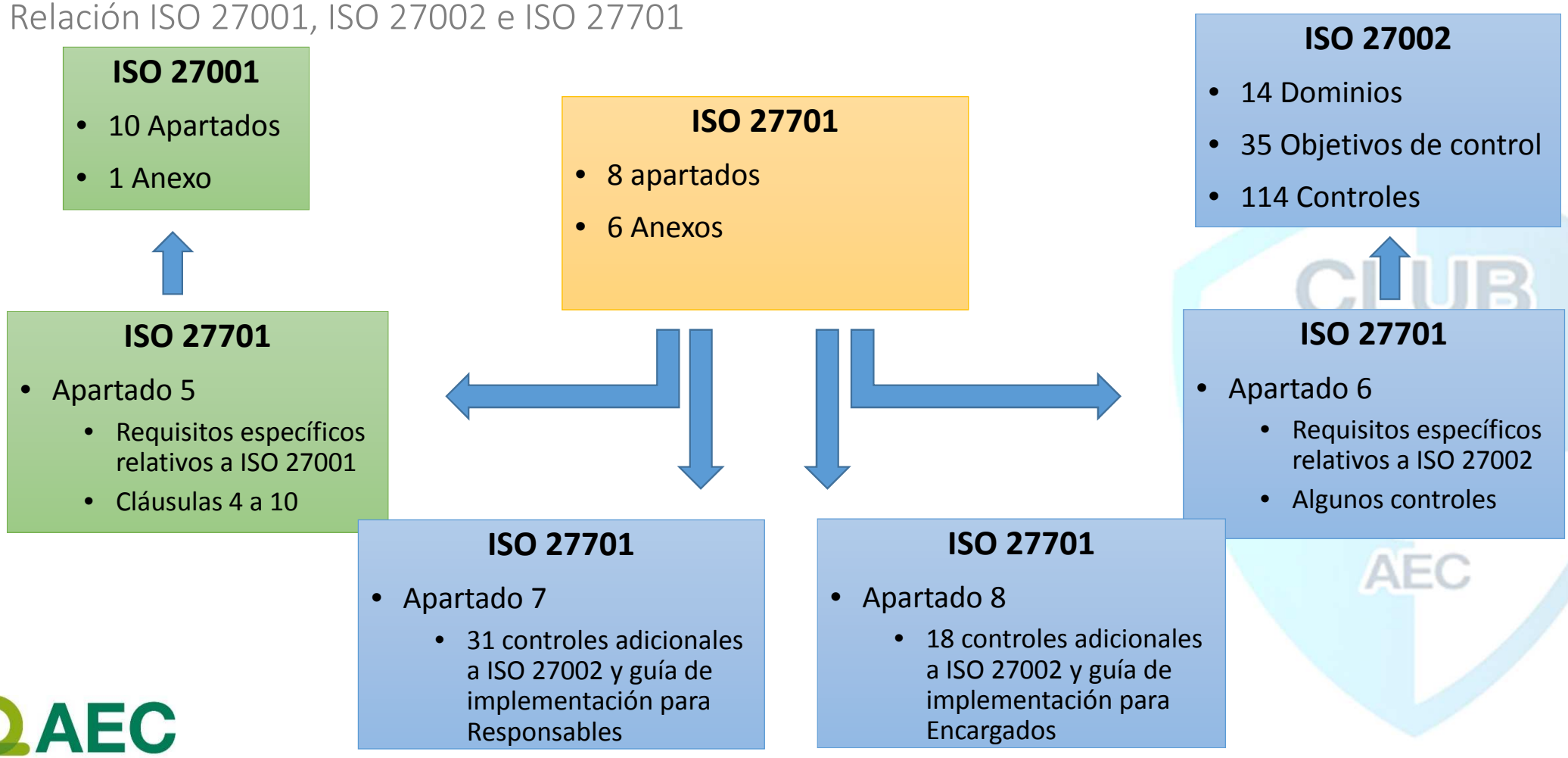
Relación ISO 27001, ISO 27002 e ISO 27701

Gestión de la Seguridad de la Información / Privacidad
ISO 27001 / ISO 27701

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

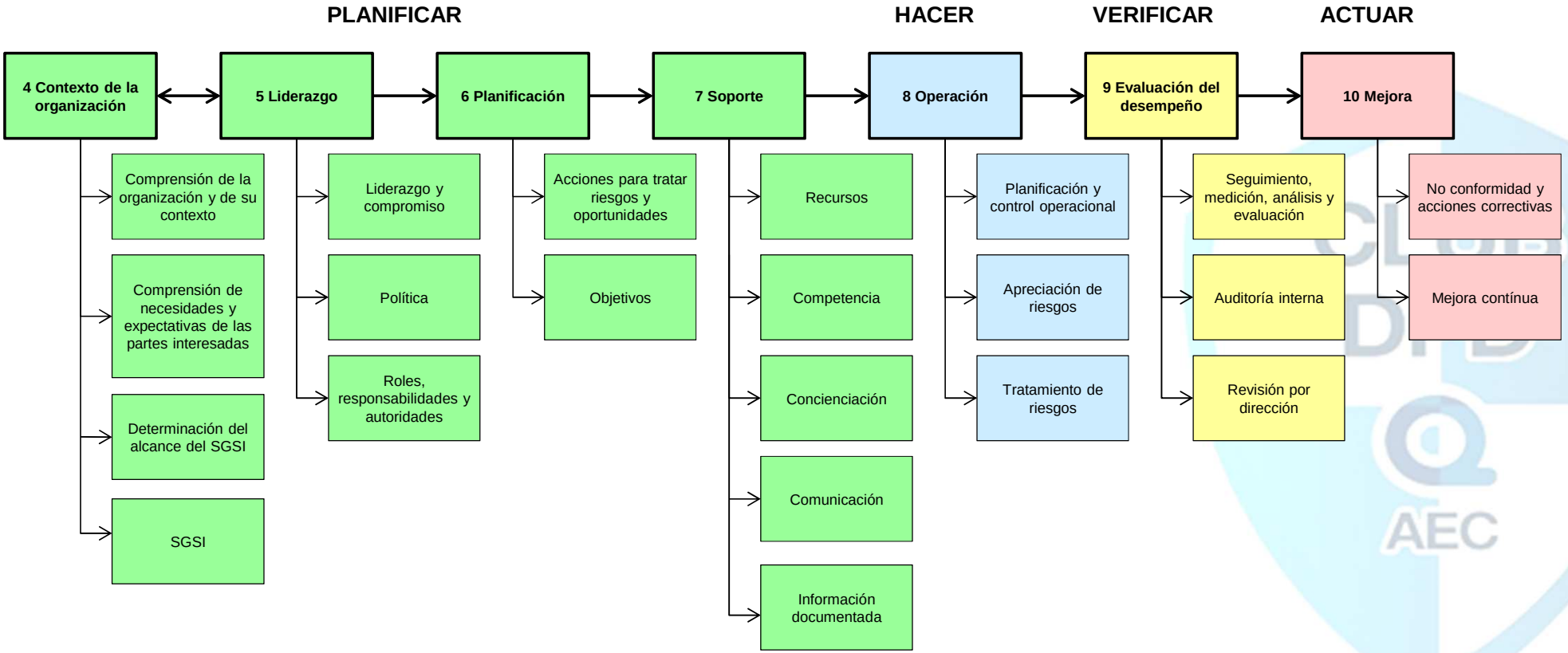
Introducción

Relación ISO 27001, ISO 27002 e ISO 27701



Introducción

Relación ISO 27001, ISO 27002 e ISO 27701 – Estructura ISO 27001



Introducción

Relación ISO 27001, ISO 27002 e ISO 27701 – Estructura ISO 27002

Análisis ISO 27701

Estructura, mapeo y cláusulas

Gestión de Información de Privacidad
ISO 27701

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Análisis ISO 27701

Estructura

La ISO 27701 aborda requerimientos y recomendaciones adicionales a las normas ISO/IEC 27001 e ISO/IEC 27002 (sistemas de gestión de seguridad de la información y código de practica de controles de seguridad de la información) para incorporar aspectos específicos referidos a privacidad, transformando el Sistema de gestión de seguridad de la información en un nuevo Sistema de Gestión de Información de Privacidad.

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Generalidades
5. Requisitos específicos de SGIP relacionados con ISO / IEC 27001
6. Orientaciones específicas de SGIP relacionadas con ISO / IEC 27002
7. Guía adicional ISO / IEC 27002 para controles de Información de Identificación Personal (IIP)
8. Guía adicional ISO / IEC 27002 para procesos de Información de Identificación Personal (IIP)

- Anexos

Análisis ISO 27701

Cláusulas

Cláusula 5:

En esta cláusula se establece la correspondencia con los apartados **4 al 10 de la norma ISO 27001**, **ampliando** los requerimientos sobre protección de la información específicamente para el apartado **4** sobre el **contexto** organizacional y el apartado **6** relativo a la **planificación de la gestión de riesgos**, no aportando necesidades adicionales en el resto de los apartados.

Análisis ISO 27701

Ejemplo de cláusula de ISO 27701 con requisitos adicionales a ISO 27001

4.1 Comprensión de la organización y su contexto

ISO 27001

La organización debe **determinar las cuestiones externas e internas** que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su Sistema de Gestión de la **Seguridad de la Información**.

ISO 27701

La organización **determinará su función como Responsable y/o Encargado** del tratamiento.
La organización debe **determinar las cuestiones externas e internas** que son pertinentes para su propósito y que afectan a su capacidad para lograr los resultados previstos de su Sistema de Gestión de **Información de Privacidad**. Por ejemplo, estos pueden incluir:

- legislación de privacidad aplicable;
- reglamentos aplicables;
- decisiones judiciales aplicables;
- contexto organizativo, gobernanza, políticas y procedimientos aplicables;
- decisiones administrativas aplicables;
- requisitos contractuales aplicables.

Cuando la organización actúe en **ambos roles** (por ejemplo, un Responsable y Encargado del tratamiento), se deben determinar estos roles segregados, cada uno de los cuales es objeto de un **conjunto separado de controles**.

Análisis ISO 27701

Ejemplo de cláusula de ISO 27701 con requisitos adicionales a ISO 27001

6.1.2.c.1 Apreciación de riesgos de seguridad de la información

ISO 27001

La organización debe **definir y aplicar un proceso de apreciación de riesgos de seguridad de la información**, que identifique los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el alcance del sistema de gestión de la seguridad de la información

ISO 27701

La organización aplicará el proceso de evaluación del riesgo de seguridad de la información para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad, **dentro del ámbito del SGIP**.
La organización aplicará el proceso de **evaluación de riesgos de privacidad** para identificar **los riesgos relacionados con el procesamiento de IIP**, dentro del ámbito del SGIP.
La organización **garantizará** a lo largo de los procesos de evaluación de riesgos que la **relación entre la seguridad de la información y la protección de la IIP se gestionan adecuadamente**.

NOTA: La organización puede aplicar un proceso integrado de evaluación de riesgos de privacidad y seguridad de la información o dos separadas para la seguridad de la información y los riesgos relacionados con el procesamiento de IIP.

Análisis ISO 27701

Cláusulas

Cláusula 6:

Este apartado **amplía** los requerimientos establecidos en la guía de buenas prácticas **ISO 27002** y los controles establecidos en el Anexo A de la ISO 27001.

Se amplían los requisitos sobre la protección de la información en algunos **controles del 5 al 18**, con excepción del control 17 (Seguridad de la información en la continuidad del negocio) donde no se establecen medidas adicionales a las ya existentes.

Análisis ISO 27701

Ejemplo de cláusula de ISO 27701 con requisitos adicionales a ISO 27002

6.1.1 Roles y responsabilidades en seguridad de la información

ISO 27001

La asignación de **responsabilidades** relativas a seguridad de la información debería realizarse de acuerdo con las **políticas de seguridad de la información**.

Deberían identificarse las **responsabilidades** para la **protección de activos** individuales así como para llevar a cabo procesos de seguridad específicos.

Deberían definirse las **responsabilidades** para **las actividades de gestión de riesgos** de seguridad de la información y, en particular, para la **aceptación de riesgos residuales**.

Estas responsabilidades deberían **completarse, dónde sea necesario**, con una guía más detallada para ubicaciones e instalaciones de tratamiento de información específicas.

Se deberían definir las **responsabilidades** locales para la **protección de los activos** y para llevar a cabo **procesos de seguridad específicos**.

Análisis ISO 27701

Ejemplo de cláusula de ISO 27701 con requisitos adicionales a ISO 27002

6.1.1 Roles y responsabilidades en seguridad de la información

ISO 27701

La organización debe designar un **punto de contacto**, para su uso por parte del **interesado**

La organización debe **designar** a una o más personas **responsables** de desarrollar, implementar, mantener y supervisar un **programa de gobierno y privacidad** en toda la organización, para garantizar el cumplimiento de todas las leyes y reglamentos relativos al tratamiento de Información de Identificación Personal.

La persona responsable **deberá**, en su caso:

- ser **independiente** e informar directamente al nivel de gestión adecuado de la organización con el fin de garantizar una gestión eficaz de los riesgos de privacidad;
- participar en la **gestión** de todas las cuestiones relacionadas con el tratamiento de IIP;
- ser **experto** en legislación, regulación y práctica en materia de protección de datos;
- ser **punto de contacto** para las autoridades de supervisión;
- **informar** a los directivos de alto nivel y a los empleados de la organización de sus obligaciones con respecto al tratamiento de IIP;
- proporcionar **asesoramiento** con respecto a las evaluaciones de impacto en la privacidad realizadas por la organización.

Análisis ISO 27701

Cláusulas

Cláusula 7:

Determina **controles adicionales** y la guía de implementación de estos para los Responsables del tratamiento.

En total con **4 objetivos de control y 31 controles**.

Análisis ISO 27701

Controles de ISO 27701 para Responsables del tratamiento

A.7.2 Condiciones de recogida y tratamiento

- Identificar y documentar la finalidad
- Identificar la base legal
- Determinar cuándo y cómo debe ser obtenido el consentimiento
- Obtener y recoger el consentimiento
- Evaluación de impacto
- Contratos de Encargado de Tratamiento
- Corresponsable del tratamiento
- Registros (evidencias)

Análisis ISO 27701

Controles de ISO 27701 para Responsables del tratamiento

A.7.3 Obligaciones con los interesados

- Determinar, documentar y cumplir con las obligaciones con los interesados
- Determinar información para los interesados
- Proporcionar información a los interesados
- Proporcionar mecanismo para modificar o retirar consentimiento
- Proporcionar mecanismo para oponerse tratamiento
- Acceso, rectificación, cancelación y/o supresión
- Informar a terceros
- Proveer portabilidad de los datos
- Gestión de solicitudes de los interesados
- Automatización

Análisis ISO 27701

Controles de ISO 27701 para Responsables del tratamiento

A.7.4 Privacidad por diseño y privacidad por defecto

- Limitar la recogida
- Limitar el tratamiento
- Precisión y calidad
- Objetivos de minimización
- Disociación y eliminación al final del procesamiento
- Archivos temporales
- Retención
- Eliminación
- Controles en transmisiones

Análisis ISO 27701

Controles de ISO 27701 para Responsables del tratamiento

A.7.5 Intercambio de PII, transferencia y divulgación

- Identificar la base para la transferencia de entre jurisdicciones
- Países y organizaciones internacionales entre las que se puede transferir la IIP
- Registros de transferencia de IIP
- Registro de divulgaciones de IIP a terceras partes

Análisis ISO 27701

Ejemplo de control de ISO 27701 para Responsables del tratamiento

7.2.4 Obtener y registrar el consentimiento

Control

La organización debe **obtener y registrar el consentimiento de los interesados** de acuerdo con un **proceso documentado.**

Guía de implementación

La organización debe obtener y registrar el consentimiento de los interesados de tal manera que pueda proporcionar, previa solicitud, **evidencia de los detalles del consentimiento proporcionado** (por ejemplo, cuándo se ha aportado el consentimiento, la identificación del interesado y la declaración de consentimiento).

El consentimiento debe ser:

- **libremente** dado;
- **específico para el propósito** del tratamiento; y
- **inequívoco y explícito**.

Análisis ISO 27701

Cláusulas

Cláusula 8:

Este apartado establece **controles adicionales** y una recomendación de implantación para los **Encargados del tratamiento.**

En total con **4 objetivos de control y 18 controles**.

Análisis ISO 27701

Ejemplo de controles de ISO 27701 para Encargados del tratamiento

8.2.4 Instrucción infractora

Control

La organización (ET) debe **informar** al cliente (RT) si, en su opinión, una instrucción de tratamiento **infringe** legislación y/o regulación.

Guía de implementación

La capacidad de la organización para verificar si la instrucción infringe la legislación y/o la regulación puede depender de el contexto tecnológico, sobre la propia instrucción y sobre el contrato entre la organización y el cliente.

Análisis ISO 27701

Anexos

Anexo A
Objetivos de control y controles para Responsables del tratamiento

Anexo B
Objetivos de control y controles para Encargados del tratamiento

Anexo C
Mapeo con ISO/IEC 29100

Anexo D
Mapeo con artículos del RGPD

Anexo E
Mapeo con ISO/IEC 27018 (Cloud) e ISO/IEC 29151 (Buenas prácticas para IIP)

Anexo F
Información sobre cómo extender ISO 27001/27002 con la 27701

Análisis ISO 27701

Ejemplo en el Anexo F

6.1.2 Evaluación del riesgo de seguridad de la información

La organización definirá y aplicará un proceso de evaluación de riesgos de privacidad y seguridad de la información que:

a) establezca y mantenga criterios de seguridad de la información y riesgo de privacidad que incluyan:
   1. los criterios de aceptación del riesgo; y
   2. criterios para realizar evaluaciones de riesgos de privacidad y seguridad de la información;

b) garantiza que las sucesivas evaluaciones de los riesgos de privacidad y seguridad de la información produzcan resultados coherentes, válidos y comparables;

c) identifica los riesgos de seguridad de la información y privacidad

Implantación ISO 27701

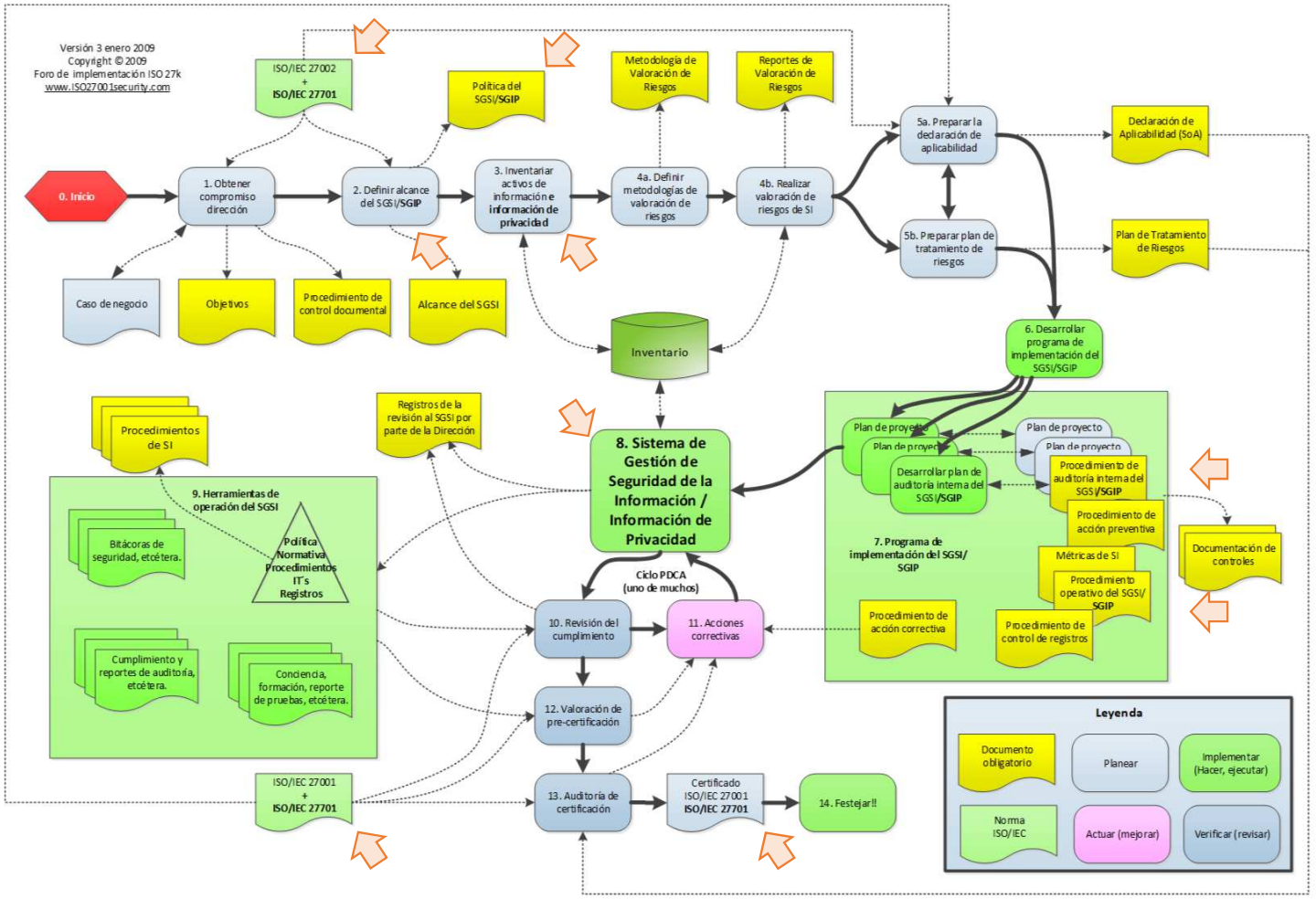
Diferentes casos

Gestión de Información de Privacidad
ISO 27701

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Implantación ISO 27701

Casos de implantación



AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

GRACIAS

por la atención

Preguntas

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD