Organiza:

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Partners Estratégicos:

GOVERTIS
Advisory Services

Telefónica

Organiza: AEC Asociación Española para la Calidad

Partners Estratégicos: Govertis Advisory Services, Telefónica

# ISO 27.701:2019.
# El nuevo estándar en Protección de Datos.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Agenda.

- **Contexto de la norma.**
- **Cláusula 4.** Requisitos generales de la norma **ISO 27701.**
- **Cláusula 5.** Requisitos del SGPD relacionados con la norma **ISO 27001.**
- **Cláusula 6.** Requisitos del SGPD relacionados con la norma **ISO 27002.**
- **Cláusula 7.** Controles adicionales para Responsables de tratamiento.
- **Cláusula 8.** Controles adicionales para Encargados de tratamiento.
- Anexos.
- Ruta desde ISO 27001 hacia la certificación ISO 27.701.

# Definición de términos ISO 27701 / 29100.

- **Personally Identifiable Information (PII)**: 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 Datos Personales (SGIDP), pero que debe estar en alineación directa con el Sistema de Gestión de Seguridad de la Información (SGSI) de ISO 27001.
- **PII Principal:** Interesado
- **PII Controller:** Responsable del tratamiento
- **PII Processor:** Encargado del tratamiento
- **Third parties:** Terceras partes que reciben la PII de los responsables y los encargados.

# La certificación en el contexto RGPD.

## Artículo 24 Responsabilidad del responsable del tratamiento.

*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 Certificación.

*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.*

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Finalidad de la certificación.

- Permite fuera de Europa disponer de un SG convalidable con el RGPD.
- Es un mecanismo para formalizar la demostración del cumplimiento.
- El funcionamiento se orienta a resultados y cumplimiento de objetivos.
- Define la construcción de “procesos de gestión” que garantizan la responsabilidad proactiva.

Organiza:
Partners Estratégicos:

# Encaje de ISO 27.701

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Estructura de la norma ISO 27701.

| Cláusula | Titulo |
|---|---|
| 1 | Alcance |
| 2 | Normativas de referencia. |
| 3 | Términos, definiciones y abreviaturas. |
| 4 | General. |
| 5 | Requisitos específicos de los SGPD relativos a **ISO 27001**. |
| 6 | Requisitos específicos de los SGPD relativos a **ISO 27002**. |
| 7 | Medidas adicionales a los Responsables de tratamiento. |
| 8 | Medidas adicionales a los Encargados de tratamiento. |
| Anexo A (Normativo) | Objetivos de control y controles específicos para los Responsables de tratamiento. |
| Anexo B (Normativo) | Objetivos de control y controles específicos para los Encargados de tratamiento. |
| Resto Anexos | Anexos C a F (Informativos): Mapeos de ISO 27701 con ISO 29100, el RGPD, la ISO 27018 e ISO 29151. |

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Agenda.

- Contexto de la norma.
- **Cláusula 4. Requisitos generales de la norma ISO 27701.**
- **Cláusula 5.** Requisitos del SGPD relacionados con la norma **ISO 27001.**
- **Cláusula 6.** Requisitos del SGPD relacionados con la norma **ISO 27002.**
- **Cláusula 7.** Controles adicionales para Responsables de tratamiento.
- **Cláusula 8.** Controles adicionales para Encargados de tratamiento.
- Anexos.
- Ruta desde ISO 27001 hacia la certificación ISO 27.701.

Organiza: AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
Partners Estratégicos: GOVERTIS Advisory Services, Telefónica

# Cláusula 4. Requisitos generales de la norma ISO 27701.

- Este apartado 4.1 de propósito general describe cómo se extiende la norma **ISO 27701** sobre la norma **ISO 27001**.
- Sirve para contextualizar el encaje de **ISO 27701 con las normas ISO 27001 e ISO 27002**.
- El subapartado 4.2 indica qué cláusulas de la norma **ISO 27001** serán ampliadas.
- El subapartado 4.3 indica qué objetivos de control y controles de la norma **ISO 27002** serán modificados.
- El apartado 4.4 describe qué debe entenderse por “cliente” en esta norma.
  - Relaciones entre interesados.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Agenda.

- Contexto de la norma.
- Cláusula 4. Requisitos generales de la norma ISO 27701.
- **Cláusula 5. Requisitos del SGPD relacionados con la norma ISO 27001.**
- **Cláusula 6.** Requisitos del SGPD relacionados con la norma **ISO 27002.**
- **Cláusula 7.** Controles adicionales para Responsables de tratamiento.
- **Cláusula 8.** Controles adicionales para Encargados de tratamiento.
- Anexos.
- Ruta desde ISO 27001 hacia la certificación ISO 27.701.

# Cláusula 5.

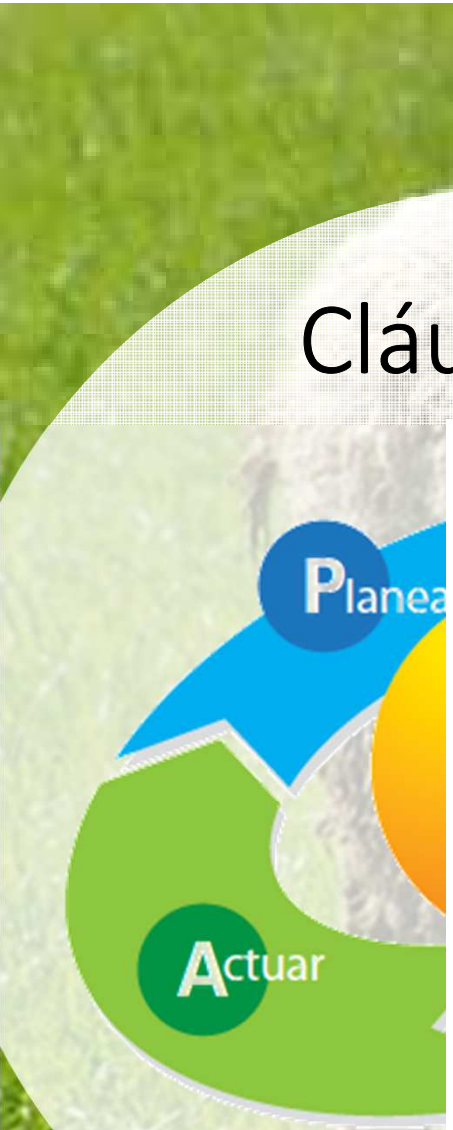




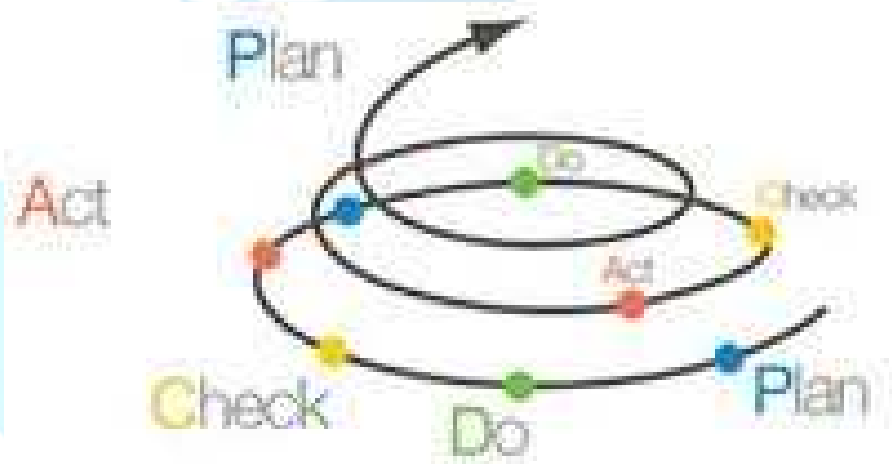

**Table 1 — Location of PIMS-specific requirements and other information for implementing controls in ISO/IEC 27001:2013**

| Clause in ISO/IEC 27001:2013 | Title | Subclause in this document | Remarks |
|---|---|---|---|
| 4 | Context of the organization | 5.2 | Additional requirements |
| 5 | Leadership | 5.3 | No PIMS-specific requirements |
| 6 | Planning | 5.4 | Additional requirements |
| 7 | Support | 5.5 | No PIMS-specific requirements |
| 8 | Operation | 5.6 | No PIMS-specific requirements |
| 9 | Performance evaluation | 5.7 | No PIMS-specific requirements |
| 10 | Improvement | 5.8 | No PIMS-specific requirements |

NOTE The extended interpretation of "information security" according to 5.1 always applies even when there are no PIMS-specific requirements.

# Cláusula 5 de la norma ISO 27701.

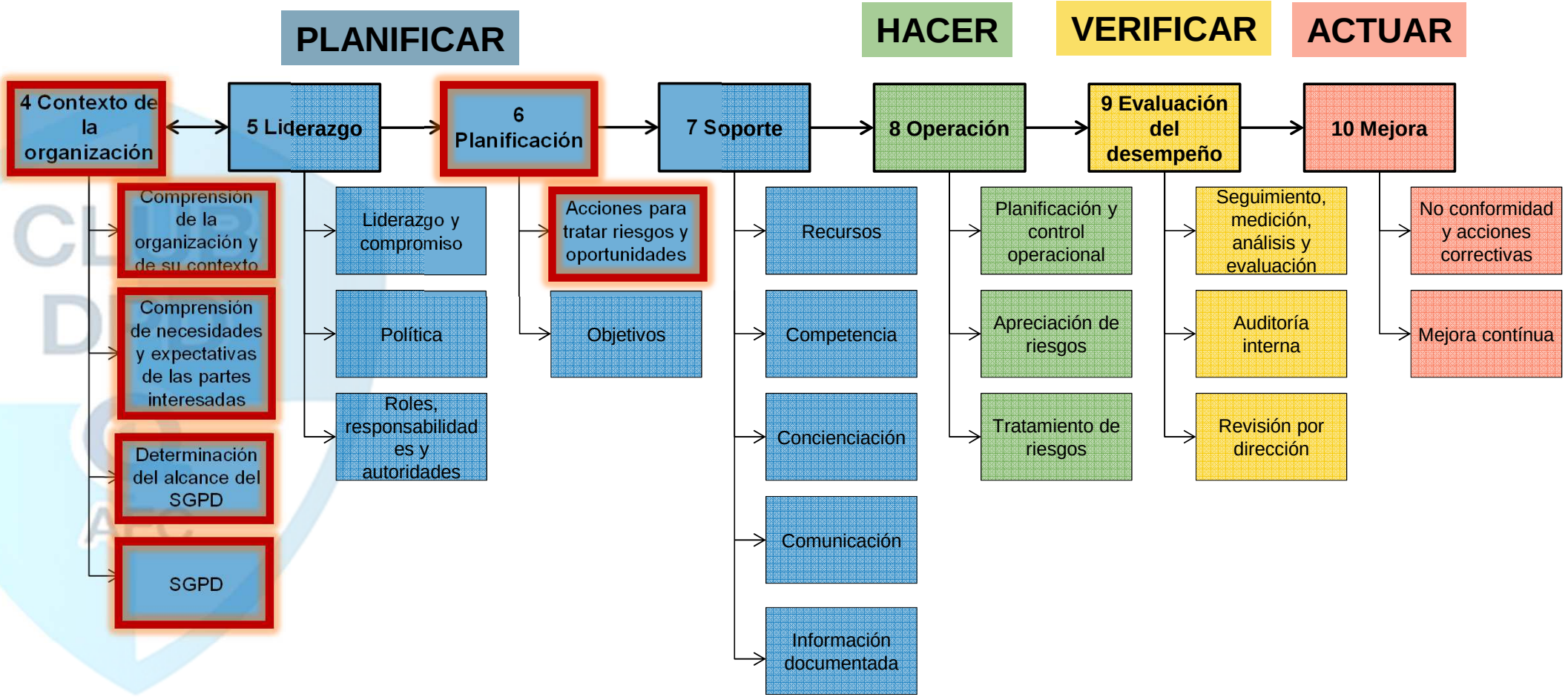
- El **Apartado 5-ISO 27701** asume que se empleará el contenido de la norma **ISO 27001** (Basado en el anexo SL) para construir un Sistema de Gestión).




| FASE PDCA | Apartado de la norma ISO 27001:2013 |
|---|---|
| **Plan** | *4-Context* |
| | *5-Leadership* |
| | *6-Planning* |
| | *7-Support* |
| **Do** | *8-Operation* |
| **Check** | *9-Performance Evaluation* |
| **Act** | *10-Improvement* |

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Cláusula 5 de la norma ISO 27701.



Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# ¿Qué implica Cláusula 5 de la norma ISO 27701?.

- Establece los pilares de la responsabilidad proactiva y la demostración del cumplimiento basado en el ciclo PDCA.
- Obliga a definir una Política de Seguridad y Privacidad.
- Determina concretar los objetivos a alcanzar.
- Requiere la realización de auditorías internas del SGPD en intervalos planificados.
- Establece la necesidad de revisar el SGPD e informar a Dirección del cumplimiento de objetivos.
- Define un proceso de mejora continua.

# Modelo 3 LINEAS DE DEFENSA (3DL).

# Cláusula 5 de la norma ISO 27701.

- La documentación relativa a la cláusula 5 será similar a ISO 27001 con algunos cambios.

| FASE PDCA | Apartados de la norma ISO 27001 | Resultados documentados |
|---|---|---|
| **Plan** | *4-Context* | • *Documento de alcance según criterios ISO 27701.* |
| | *5-Leadership* | • *Política de seguridad y privacidad.*<br>• *Roles y responsabilidades en seguridad.* |
| | 6-Planning | • Metodología de análisis de riesgos.<br>• Informe de análisis de riesgos.<br>• Plan de tratamiento de riesgos.<br>• Objetivos de seguridad del SGPD.<br>• Declaración de aplicabilidad contemplando ampliación ISO 27701. |
| | *7-Support* | • *Concienciación y formación.*<br>• *Procedimiento de control de documentos y registros.* |
| **Do** | 8-Operation | • Actualización del análisis y plan de gestión del riesgo. |
| **Check** | 9-Performance Evaluation | • Procedimiento de gestión de objetivos.<br>• Procedimiento de auditoría<br>• Procedimiento de revisión por Dirección |
| **Act** | 10-Improvement | • Procedimiento de mejora continua |

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Agenda.

- Contexto de la norma.
- Cláusula 4. Requisitos generales de la norma ISO 27701.
- Cláusula 5. Requisitos del SGPD relacionados con la norma ISO 27001.
- **Cláusula 6. Requisitos del SGPD relacionados con la norma ISO 27002.**
- **Cláusula 7.** Controles adicionales para Responsables de tratamiento.
- **Cláusula 8.** Controles adicionales para Encargados de tratamiento.
- Anexos.
- Ruta desde ISO 27001 hacia la certificación ISO 27.701.

# Cláusula 6 de la norma ISO 27701.

**Capa organizativa**

**Capa Operativa**

**Table 2 — Location of PIMS-specific guidance and other information for implementing controls in ISO/IEC 27002:2013**

| Clause in ISO/IEC 27002:2013 | Title | Subclause in this document | Remarks |
|---|---|---|---|
| 5 | Information security policies | 6.2 | Additional guidance |
| 6 | Organization of information security | 6.3 | Additional guidance |
| 7 | Human resource security | 6.4 | Additional guidance |
| 8 | Asset management | 6.5 | Additional guidance |
| 9 | Access control | 6.6 | Additional guidance |
| 10 | Cryptography | 6.7 | Additional guidance |
| 11 | Physical and environmental security | 6.8 | Additional guidance |
| 12 | Operations security | 6.9 | Additional guidance |
| 13 | Communications security | 6.10 | Additional guidance |
| 14 | System acquisition, development and maintenance | 6.11 | Additional guidance |
| 15 | Supplier relationships | 6.12 | Additional guidance |
| 16 | Information security incident management | 6.13 | Additional guidance |
| 17 | Information security aspects of business continuity management. | 6.14 | No PIMS-specific guidance |
| 18 | Compliance | 6.15 | Additional guidance |

NOTE The extended interpretation of “information security” according to 6.1 always applies even when there is no PIMS-specific guidance.

Seguridad organizativa

Seguridad lógica

Seguridad física

Seguridad jurídica

# Cláusula 6 de la norma ISO 27701.

- Comienza indicando que cuando **ISO 27001** aparece el término “seguridad de la información” debe extenderse e incluir la protección de la privacidad.

| ÁREAS | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Objetivos de control | 1 | 2 | 3 | 3 | 4 | 1 | 2 | 7 | 2 | 3 | 2 | 1 | 2 | 2 |
| Controles | 2 | 7 | 6 | 10 | 14 | 2 | 15 | 14 | 7 | 13 | 5 | 7 | 4 | 8 |
| Modificados ISO **27701** | 1 | 2 | 1 | 6 | 3 | 1 | 2 | 3 | 2 | 5 | 1 | 2 | 0 | 4 |

# Ejemplo de modificación sobre control de ISO 27701.

## 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**.

### 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.

# Ejemplo de modificación sobre control de ISO 27701.

## 11.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla.

Comtrol 11.2.9

ISO 27701

### 6.8.2.8 Unattended user equipment

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.8 applies.

### 6.8.2.9 Clear desk and clear screen policy

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 11.2.9 and the following additional guidance applies:

**Additional implementation guidance for 11.2.9, Clear desk and clear screen policy, of ISO/IEC 27002:2013 is:**

The organization should restrict the creation of hardcopy material including PII to the minimum needed to fulfil the identified processing purpose.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Agenda.

- Contexto de la norma.
- Cláusula 4. Requisitos generales de la norma ISO 27701.
- Cláusula 5. Requisitos del SGPD relacionados con la norma ISO 27001.
- Cláusula 6. Requisitos del SGPD relacionados con la norma ISO 27002.
- **Cláusula 7. Controles adicionales para Responsables de tratamiento.**
- **Cláusula 8.** Controles adicionales para Encargados de tratamiento.
- Anexos.
- Ruta desde ISO 27001 hacia la certificación ISO 27.701.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Cláusula 7 de la norma ISO 27701.

- Determina **controles adicionales para RESPONSABLES DE TRATAMIENTO** y la guía de implementación a considerar.
- En total con **4 objetivos de control y 31 controles**.

| | | |
|---|---|---|
| Condiciones para la recogida y tratamiento de datos. | 8 | Controles desde A.7.2.1 a A.7.2.8 |
| Obligaciones del Responsable de tratamiento con el interesado. | 10 | Controles desde A.7.3.1 a A.7.3.10 |
| Privacidad por diseño y por defecto. | 9 | Controles desde A.7.4.1 a A.7.4.9 |
| Intercambios, transferencia y divulgación de datos personales. | 4 | Controles desde A.7.5.1 a A.7.5.4. |

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Cláusula 7 de la norma ISO 27701. Controles.

8

## Condiciones para la recogida y tratamiento de datos.

- A.7.2.1. Identificar y documentar la finalidad.
- A.7.2.2. Identificar fundamentos legales
- A.7.2.3. Determinar cuándo y cómo obtener consentimiento.
- A.7.2.4. Obtener evidencia del consentimiento.
- A.7.2.5. Evaluación de impacto de privacidad.
- A.7.2.6. Contratos con encargados de tratamiento.
- A.7.2.7. Corresponsables del tratamiento.
- A.7.2.8. Evidencias de cumplimiento del tratamiento de datos personales.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Cláusula 7 de la norma ISO 27701. Controles.

10

## Obligaciones del Responsable de tratamiento con el interesado.

- A.7.3.1. Determinar y cumplir con las obligaciones con el interesado.
- A.7.3.2. Determinar la información a suministrar a los interesados.
- A.7.3.3. Proporcionar información a los interesados.
- A.7.3.4. Mecanismos para modificar o retirar el consentimiento.
- A.7.3.5. Mecanismos para oponerse al tratamiento.
- A.7.3.6. Acceso, modificación o cancelación.
- A.7.3.7. Obligaciones del Responsable de tratamiento de informar a terceros.
- A.7.3.8. Proporcionar copias de los datos personales tratados.
- A.7.3.9. Atender solicitudes de los interesados.
- A.7.3.10. Entornos de decisiones automatizadas.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Cláusula 7 de la norma ISO 27701. Controles.

9

## Privacidad por diseño y por defecto.

- A.7.4.1. Limitaciones en la recogida.
- A.7.4.2. Limitaciones en el tratamiento.
- A.7.4.3. Exactitud y calidad.
- A.7.4.4. Objetivos de minimización del tratamiento.
- A.7.4.5. Psedoanonimización o eliminación al finalizar el tratamiento.
- A.7.4.6. Ficheros temporales.
- A.7.4.7. Retención.
- A.7.4.8. Disposición.
- A.7.4.9. Control en la transmisión de datos personales.

Organiza: AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
Partners Estratégicos: GOVERTIS Advisory Services, Telefónica

# Cláusula 7 de la norma ISO 27701. Controles.

4

## Intercambios, transferencia y divulgación de datos personales.

- A.7.5.1. Identificar la base legal para transferencias internacionales.
- A.7.5.2. Países y organizaciones internacionales a las que poder transferir datos personales.
- A.7.5.3. Registros de transferencias de datos personales.
- A.7.5.4. Registros de divulgación a terceros.

Organiza: AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
Partners Estratégicos: GOVERTIS Advisory Services · Telefónica

# Agenda.

- Contexto de la norma.
- Cláusula 4. Requisitos generales de la norma ISO 27701.
- Cláusula 5. Requisitos del SGPD relacionados con la norma ISO 27001.
- Cláusula 6. Requisitos del SGPD relacionados con la norma ISO 27002.
- Cláusula 7. Controles adicionales para Responsables de tratamiento.
- **Cláusula 8. Controles adicionales para Encargados de tratamiento.**
- Anexos.
- Ruta desde ISO 27001 hacia la certificación ISO 27.701.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Cláusula 8 de la norma ISO 27701.

- Determina **controles adicionales para ENCARGADOS DE TRATAMIENTO** y la guía de implementación a considerar.
- En total con **4 objetivos de control y 18 controles**.

| | | |
|---|---|---|
| Condiciones para la recogida y tratamiento de datos. | 6 | Controles desde A.8.2.1 a A.8.2.6 |
| Obligaciones del Encargado de tratamiento con el interesado. | 1 | Control A.8.3.1 |
| Privacidad por diseño y por defecto. | 3 | Controles desde A.8.4.1 a A.8.4.3 |
| Intercambios, transferencia y divulgación de datos personales. | 8 | Controles desde A.8.5.1 a A.8.5.8. |

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Cláusula 8 de la norma ISO 27701. Controles.

6

## Condiciones para la recogida y tratamiento de datos.

- A.8.2.1. Acuerdos con el cliente.
- A.8.2.2. Propósitos del tratamiento realizado para el Responsable.
- A.8.2.3. Usos para marketing y publicidad.
- A.8.2.4. Incumplimiento de instrucciones.
- A.8.2.5. Obligaciones del cliente.
- A.8.2.6. Evidencias de cumplimiento del tratamiento de datos personales.

Organiza: AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
Partners Estratégicos: GOVERTIS Advisory Services, Telefónica

# Cláusula 8 de la norma ISO 27701. Controles.

1

## Obligaciones del Encargado de tratamiento con el interesado.

- A.8.3.1. Obligaciones con el interesado.

Organiza: AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD
Partners Estratégicos: GOVERTIS Advisory Services, Telefónica

# Cláusula 8 de la norma ISO 27701. Controles.

3

## Privacidad por diseño y por defecto.

- A.8.4.1. Ficheros temporales..
- A.8.4.2.Devolución, transferencia o entrega.
- A.8.4.3. Control en la transmisión de datos personales.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Cláusula 8 de la norma ISO 27701. Controles.

8

## Intercambios, transferencia y divulgación de datos personales.

- A.8.5.1. Identificar la base legal para transferencias internacionales.
- A.8.5.2. Países y organizaciones internacionales a las que poder transferir datos personales.
- A.8.5.3. Registros de transferencias de datos personales.
- A.8.5.4. Registros de divulgación a terceros.
- A.8.5.5. Divulgaciones legales vinculantes de datos personales.
- A.8.5.6. Divulgaciones a terceros subcontratados que actúen como encargados.
- A.8.5.7. Contratación de terceros para realizar tratamientos de datos personales.
- A.8.5.8. Cambio de terceros para realizar tratamientos de datos personales.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Agenda.

- Contexto de la norma.
- Cláusula 4. Requisitos generales de la norma ISO 27701.
- Cláusula 5. Requisitos del SGPD relacionados con la norma ISO 27001.
- Cláusula 6. Requisitos del SGPD relacionados con la norma ISO 27002.
- Cláusula 7. Controles adicionales para Responsables de tratamiento.
- Cláusula 8. Controles adicionales para Encargados de tratamiento.
- **Anexos.**
- Ruta desde ISO 27001 hacia la certificación ISO 27.701.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Anexos de la norma ISO 27701.

- **Anexo A.** Tabla con objetivos de control y controles para Responsables del tratamiento.
- **Anexo B.** Tabla con objetivos de control y controles para Encargados del tratamiento
- **Anexo C.** Tabla con relaciones entre **ISO 27701** e ISO/IEC 29100
- **Anexo D.** Tabla con relaciones entre artículos del RGPD e **ISO 27701**
- **Anexo E. Tabla con relaciones entre** ISO/IEC 27018 (Cloud) e ISO/IEC 29151 (Buenas prácticas para IIP) e **ISO 27701.**
- **Anexo F.** Información sobre cómo extender ISO 27001/27002 con **ISO 27701.**

# Anexo D. Relaciones entre ISO 27701 y RGPD.

- Permite ver con qué cláusulas de ISO 27701 se cumplen los diferentes artículos del RGPD.

**Annex D**
(informative)

**Mapping to the General Data Protection Regulation**

This annex gives an indicative mapping between provisions of this document and Articles 5 to 49 except 43 of the General Data Protection Regulation of the European Union. It shows how compliance to requirements and controls of this document can be relevant to fulfil obligations of GDPR.

However, it is purely indicative and as per this document, it is the organizations responsibility to assess its legal obligations and decide how to comply with them.

**Table D.1 — Mapping of ISO/IEC 27701 structure to GDPR articles**

| Subclause of this document | GDPR article |
|---|---|
| 5.2.1 | (24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8) |
| 5.2.2 | (31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5) |
| 5.2.3 | (32)(2) |
| 5.2.4 | (32)(2) |
| 5.4.1.2 | (32)(1)(b), (32)(2) |
| 5.4.1.3 | (32)(1)(b), (32)(2) |
| 6.2.1.1 | (24)(2) |
| 6.3.1.1 | (27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2) |
| 6.3.2.1 | (5)(1)(f) |
| 6.4.2.2 | (39)(1)(b) |

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Anexo D. Relaciones entre ISO 27701 y RGPD.

En relación al cumplimiento del RGPD en materia de “Seguridad de los datos personales”, el artículo 33 se distribuye por varios apartados de **ISO 27701** pero los artículos 33 y 34 se centran en el cumplimiento de los controles de gestión de incidentes.

- El cumplimiento de:
  - “Artículo 33.Notificación de una violación de la seguridad de los datos personales a la autoridad de control”
  - “Artículo 34 Comunicación de una violación de la seguridad de los datos personales al interesado”

**Queda delegado en el cumplimiento de los controles ISO 27701**:

- “13.1.1. Responsabilidades y procedimientos”,
- “13.1.2. Notificación de los eventos de seguridad de la información”
- “16.1.5 Respuesta a los incidentes de seguridad”.

# Anexo F. Cómo aplicar ISO 27701 sobre ISO 27001 e ISO 27002.

Este anexo describe cómo debe modificarse el contenido de la norma para que “seguridad de la información” se amplíe para incluir privacidad.

**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:

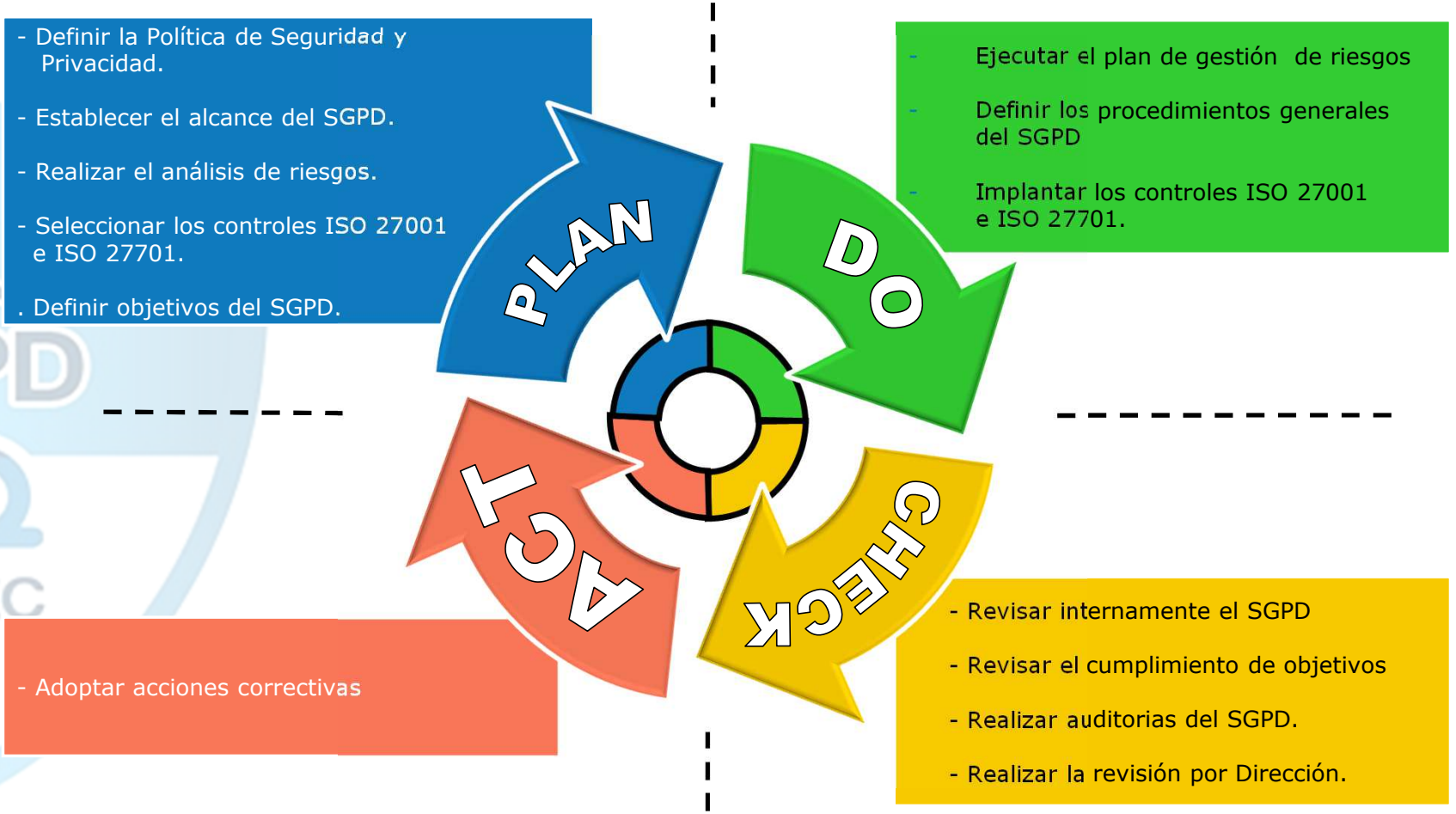
a) establezca y mantenga criterios de seguridad de la información y riesgo de privacidad que incluyan:
   1. los criterios de aceptación del riesgo; y
   2. criterios para realizar evaluaciones de riesgos de privacidad y seguridad de la información;
b) garantiza que las sucesivas evaluaciones de los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

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

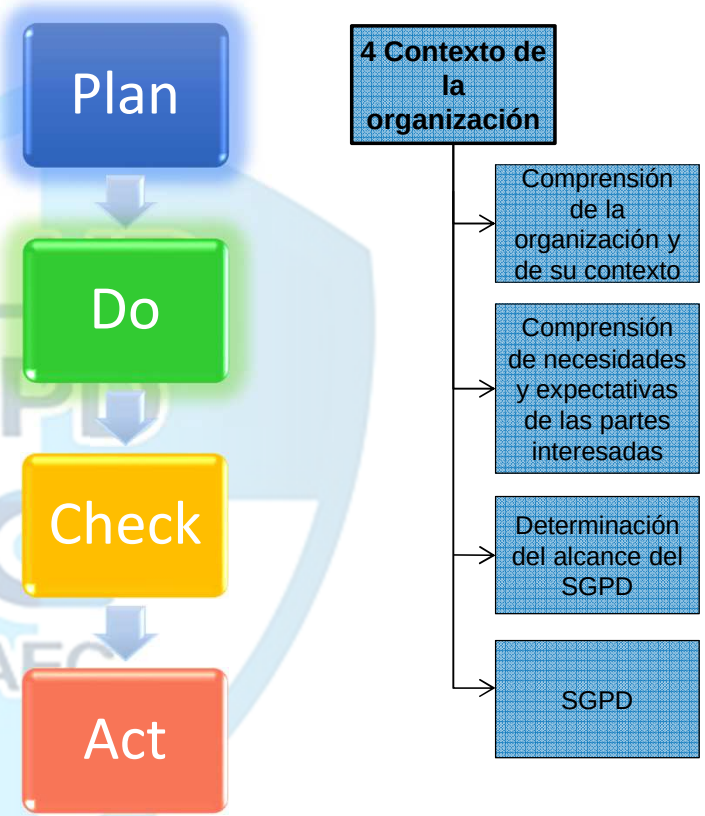
# Agenda.

- Contexto de la norma.
- Cláusula 4. Requisitos generales de la norma ISO 27701.
- Cláusula 5. Requisitos del SGPD relacionados con la norma ISO 27001.
- Cláusula 6. Requisitos del SGPD relacionados con la norma ISO 27002.
- Cláusula 7. Controles adicionales para Responsables de tratamiento.
- Cláusula 8. Controles adicionales para Encargados de tratamiento.
- Anexos.
- **Ruta desde ISO 27001 hacia la certificación ISO 27.701.**

# Planificar-Hacer-Verificar-Revisar



# Fase Planificar-PLAN.



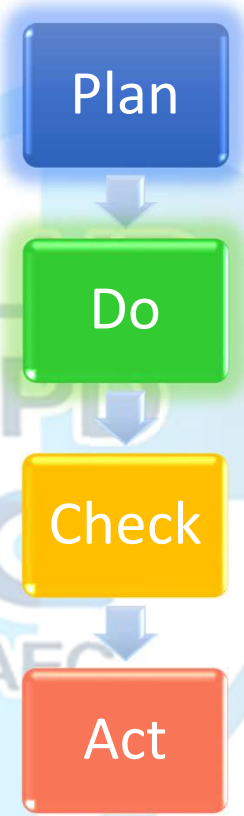

## 4. Contexto de la organización.

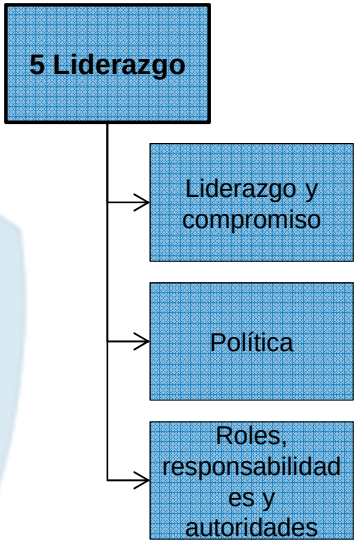
- Considerar los roles de la Organización:
  - Responsable de tratamiento
  - Encargado de tratamiento.
- Entender las necesidades de las partes interesadas.
- Definir y documentar el alcance del SGPD.

Evidencia documentada:

- Documento del alcance del SGPD.

# Fase Planificar-PLAN.




## 5. Liderazgo.

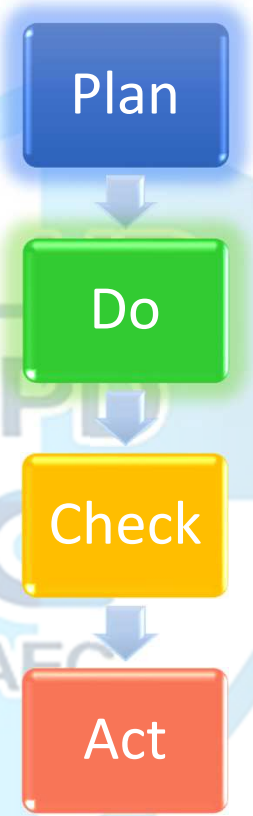
- Se definirá la Política de seguridad de la información y la privacidad.
- Se definen los roles y responsabilidades que forman parte del SGPD.

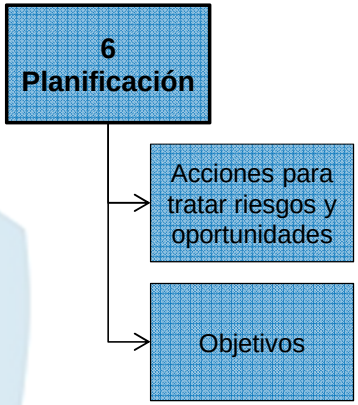
Evidencias documentadas:

- Política de seguridad de la información y privacidad.
- Roles y responsabilidades del SGPD.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Fase Planificar-PLAN.

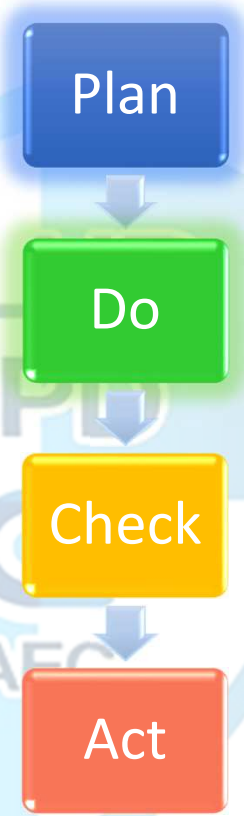


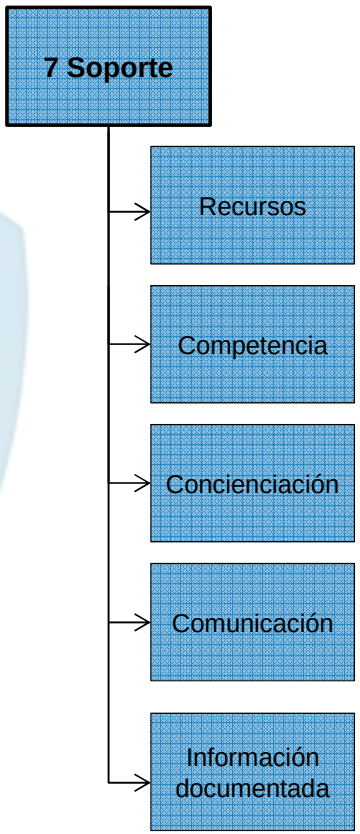




- Se realiza el proceso de gestión de riesgos del SGPD.
  - Se debe realizar el análisis de riesgos de los tratamientos incluidos en el alcance del SGPD.
  - Se define el plan de tratamiento de riesgos.
  - Se elabora la declaración de aplicabilidad.

Evidencias documentadas:
- Informe de análisis de riesgos.
- Plan de tratamiento de riesgos.
- Declaración de aplicabilidad.

# Fase Planificar-PLAN.



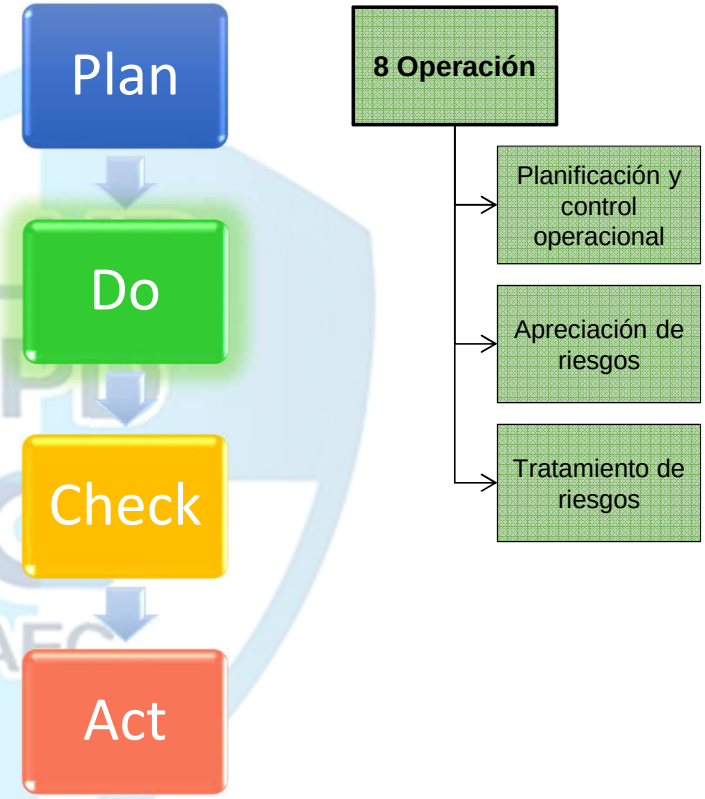

- Se debe garantizar la viabilidad del SGPD.
  - Es necesario asegurar que se alcanzan las competencias requeridas.
  - Se establecen las necesidades de formación.
  - Se define el plan de comunicación del SGPD.
  - Se establece el procedimiento de control de documentos.

Evidencias documentadas:

- Plan de formación.
- Plan de comunicación del SGPD.
- Procedimiento de control de documentación y registros.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Fase Hacer-DO.

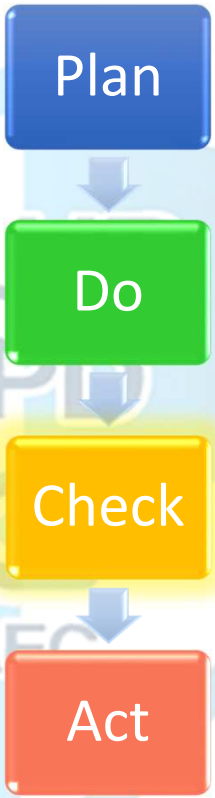


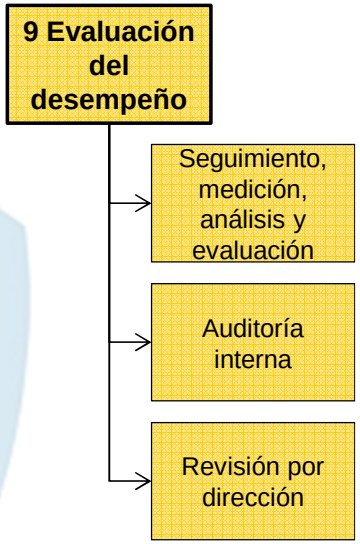




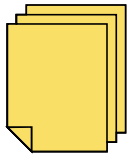
- Se debe poner en marcha lo establecido en el Plan de tratamiento de riesgos.
- Debe velarse por el cumplimiento de objetivos.

# Fase Verificar-CHECK.



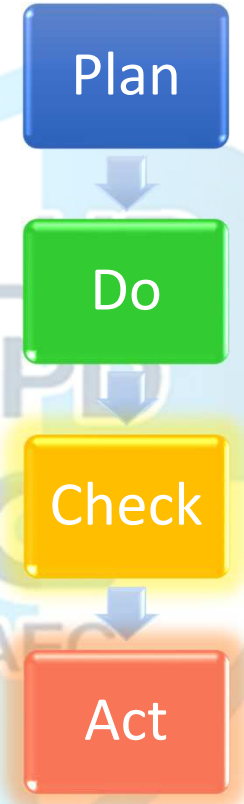

- Se establece el proceso de medición, monitorización y gestión del desempeño.
- Se determina el proceso de auditoría interna.
- Se define el proceso de revisión por Dirección.

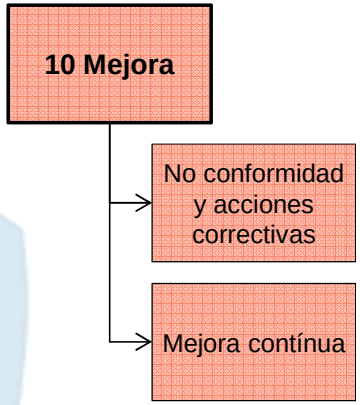


Evidencias documentadas:

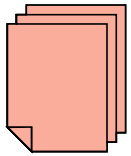
- Procedimiento de gestión de objetivos.
- Procedimiento de auditoría interna.
- Procedimiento de revisión por Dirección.

# Fase Actuar-ACT.




- Se establece el proceso de mejora continua.
  - Se debe determinar cómo se identifican no conformidades.
  - Se establece cómo se definen acciones correctoras.

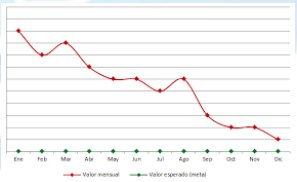


Evidencias documentadas:
- Procedimiento de mejora continua.

Organiza: AEC Asociación Española para la Calidad
Partners Estratégicos: Govertis Advisory Services, Telefónica

# Orientación a objetivos y resultados del SGPD.





- **OBJ-S1**: Atender el 90% de los ejercicios de derechos en menos de 10 días.
- **OBJ-S2:** Realizar una acción formativa por año que alcance al 100% de los empleados.
- **OBJ-S3:** Tiempo medio de respuesta para incidentes de seguridad < 4 horas.
- **OBJ-S4:** 95% de éxito en ejecución de copias de seguridad y sus pruebas.

Organiza: AEC Asociación Española para la Calidad

Partners Estratégicos: Gobertis Advisory Services · Telefónica

# ¿Opiniones sobre la norma ISO 27.701?

- Entre con su móvil en WWW.MENTI.COM usando el código que aparece en la página.

Organiza: AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Partners Estratégicos: GOVERTIS Advisory Services · Telefónica


Muchas gracias por participar en el Congreso.