PERÚ Ministerio de la Producción

INACAL
Instituto Nacional de Calidad

# NTP-ISO/IEC 29100:2021 Tecnología de la información. Técnicas de seguridad. Marco de referencia sobre privacidad. 1ª Edición


**GUSTAVO VALLEJO LA TORRE**
Miembro del CTN Codificación e Intercambio Electrónico de Datos

Siempre con el pueblo

# ÍNDICE / CONTENIDO

1 Ecosistema en la seguridad de la información

2 NTP-ISO/IEC 29100:2021 Marco de referencia sobre privacidad

3 Requisito 2: Términos y definiciones

4 Requisito 4: Elementos básicos

5 Requisito 5: Los principios sobre privacidad

6 Anexo A

1

# ECOSISTEMA EN LA SEGURIDAD DE LA INFORMACIÓN


INSTITUTO NACIONAL DE CALIDAD

# ECOSISTEMA SGSI

**01**

**NTP-ISO/IEC 27001:2014**
Sistemas de gestión de seguridad de la información. Requisitos

**NTP-ISO/IEC 27002:2017**
Código de prácticas para controles de seguridad de la información

**02**

**NTP-ISO/IEC 27003:2019**
Orientación

**NTP-ISO/IEC 27004:2018**
Seguimiento, medición, análisis y evaluación

**NTP-ISO/IEC 27005:2018**
Gestión de riesgos de la seguridad de la información

**NTP-ISO/IEC 27022**
Orientación sobre los procesos del SGSI

**03**

**Privacidad / Cloud**

**Auditoría**

**Incidentes**

**Seguridad de red / aplicaciones**

**…**

**04**

**NTP-ISO/IEC 29100**
Marco de referencia de privacidad

**ISO/IEC 29101**
Arquitectura de marco de referencia de privacidad

**ISO/IEC 29134**
Directrices para evaluación de impacto de privacidad

**ISO/IEC 29151**
Código de práctica para la protección de II

**ISO/IEC 29190**
Modelo de evaluación de capacidad de privacidad

# ECOSISTEMA SGSI

NTP-ISO/IEC 27001:2014

- Privacidad
- Cloud
- Incidentes
- Seguridad de red
- Seguridad de aplicaciones
- Ciberseguridad
- ...

2

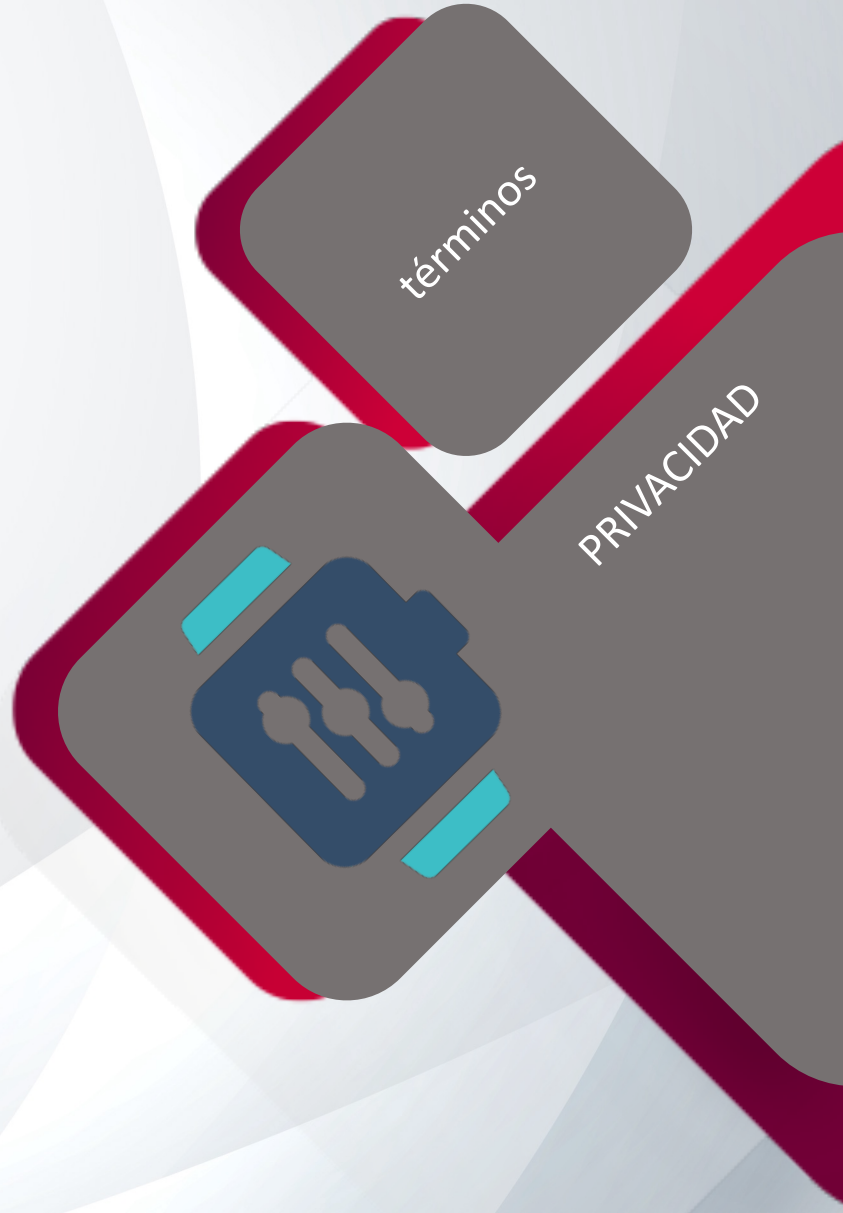
# NTP-ISO/IEC 29100
# MARCO DE REFERENCIA SOBRE LA PRIVACIDAD

INSTITUTO NACIONAL DE CALIDAD

# ESTRUCTURA NTP-ISO/IEC 29100

| | |
|---|---|
| 1 | Objeto y campo de aplicación |
| 2 | Términos y definiciones |
| 3 | Símbolo y términos abreviados |
| 4 | Elementos básicos del marco de privacidad |
| 5 | Los principios de privacidad de ISO/IEC 29100 |
| Anexo A | Correspondencia entre los conceptos ISO/IEC 29100 e ISO/IEC 27000 |

# REQUISITO 2:
# TÉRMINOS Y DEFINICIONES




INSTITUTO NACIONAL DE CALIDAD

# TÉRMINOS Y DEFINICIONES

IIP: Información de Identificación Personal

cualquier información que (a) pueda utilizarse para establecer un vínculo entre la información y la persona natural a la que se refiere dicha información, o (b) esté o pueda estar vinculada directa o indirectamente a una persona natural

| TITULAR IIP | CONTROLADOR IIP | PROCESADOR DE IIP |
|---|---|---|
| persona natural a quien se refiere la información de identificación personal (IIP) | interesado en la privacidad (o interesados en la privacidad) que determina los propósitos y los medios para procesar IIP que no sean personas naturales que usen datos para fines personales | interesado en la privacidad que procesa información de identificación personal (IIP) en nombre de y de acuerdo con las instrucciones de un controlador de IIP |

4

# REQUISITO 4:
# **ELEMENTOS BÁSICOS**

INSTITUTO NACIONAL DE CALIDAD

# ACTORES Y ROLES

- Titulares de IIP
- Controladores IIP
- Procesadores de IIP
- Terceros

# INTERACCIONES

| | Titular IIP | Controlador IIP | Procesador IIP | Tercera parte |
|---|---|---|---|---|
| Escenario a) | Proveedor IIP | Receptor IIP | - | - |
| Escenario b) | - | Proveedor IIP | Receptor IIP | - |
| Escenario c) | Proveedor IIP | - | Receptor IIP | - |
| Escenario d) | Receptor IIP | Proveedor IIP | - | - |
| Escenario e) | Receptor IIP | - | Proveedor IIP | - |
| Escenario f) | - | Receptor IIP | Proveedor IIP | - |
| Escenario g) | - | Proveedor IIP | | Receptor IIP |
| Escenario h) | - | - | Proveedor IIP | Receptor IIP |

# RECONICIMIENTO DE IIP

| Ejemplos |
| --- |
| Edad o necesidades especiales de personas naturales vulnerables<br>Denuncias de conducta criminal<br>Cualquier información recopilada durante los servicios de salud<br>Número de cuenta bancaria o tarjeta de crédito<br>Identificador biométrico<br>Estados de cuenta de tarjetas de crédito<br>Condenas penales o delitos cometidos<br>Informes de investigación criminal<br>Número de cliente<br>Fecha de nacimiento<br>Información de salud diagnóstica<br>Discapacidades Facturas del doctor<br>Archivos de sueldos y recursos humanos de los empleados<br>… |

# REQUISITOS DE PROTECCIÓN DE LA PRIVACIDAD

Ejemplos

**Factores legales y regulatorios**
- Leyes locales, nacionales e internacionales
- …

**Factores contractuales**
- Acuerdos entre varios actores diferentes
- …

**Factores de negocios**
- Características específicas de una aplicación prevista
- …

**Otros factores**
- Preferencias de privacidad de un Titular de IIP
- …

**Gestión de riesgos de privacidad**

# OTROS

## Políticas de privacidad

La alta gerencia de la organización involucrada en el procesamiento de IIP debería establecer una política de privacidad.

## Controles de privacidad

Identificar e implementar controles de privacidad para satisfacer los requisitos para protección de la privacidad identificados por el proceso de evaluación de riesgos de privacidad y su tratamiento

# REQUSITO 5:
# LOS PRINCIPIOS SOBRE PRIVACIDAD


INSTITUTO NACIONAL DE CALIDAD

# PRINCIPIOS SOBRE PRIVACIDAD

| | |
|---|---|
| 1 | El consentimiento y la elección |
| 2 | Propósito legítimo y específico |
| 3 | Límite en la recolección |
| 4 | Minimización de datos |
| 5 | Límites al uso, retención y divulgación |
| 6 | Exactitud y calidad |
| 7 | Apertura, transparencia y aviso |
| 8 | Participación individual y acceso |
| 9 | Rendición de cuentas |
| 10 | Seguridad de la información |
| 11 | Cumplimiento en privacidad |

6

# ANEXO A:
# CORRESPONDENCIA ENTRE LOS CONCEPTOS


INSTITUTO NACIONAL DE CALIDAD

# CORRESPONDENCIA ENTRE CONCEPTOS

| Conceptos de ISO/IEC 29100 | Conceptos de ISO/IEC 27000 |
|---|---|
| Interesado en la privacidad | Interesados |
| IIP | Activo de información |
| Violación de la privacidad | Incidente de seguridad de la información |
| Control de privacidad | Control |
| Riesgo a la privacidad | Riesgo |
| Gestión del riesgo a la privacidad | Gestión del riesgo |
| Requisitos de protección de la privacidad | Objetivos de control |

PERÚ Ministerio de la Producción

INACAL
Instituto Nacional de Calidad

INSTITUTO NACIONAL **DE CALIDAD**

# GRACIAS


## GUSTAVO VALLEJO LA TORRE

Miembro del CTN Codificación e Intercambio Electrónico de Datos


Siempre con el pueblo

PERÚ Ministerio de la Producción

INACAL
Instituto Nacional de Calidad

# NTP-ISO/IEC 27701:2020

## Extensión de ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información sobre privacidad. Requisitos y directrices.

**CARLOS HORNA VALLEJOS**
Miembro del CTN-EDI

Siempre con el pueblo

# ÍNDICE / CONTENIDO

1 Términos relevantes

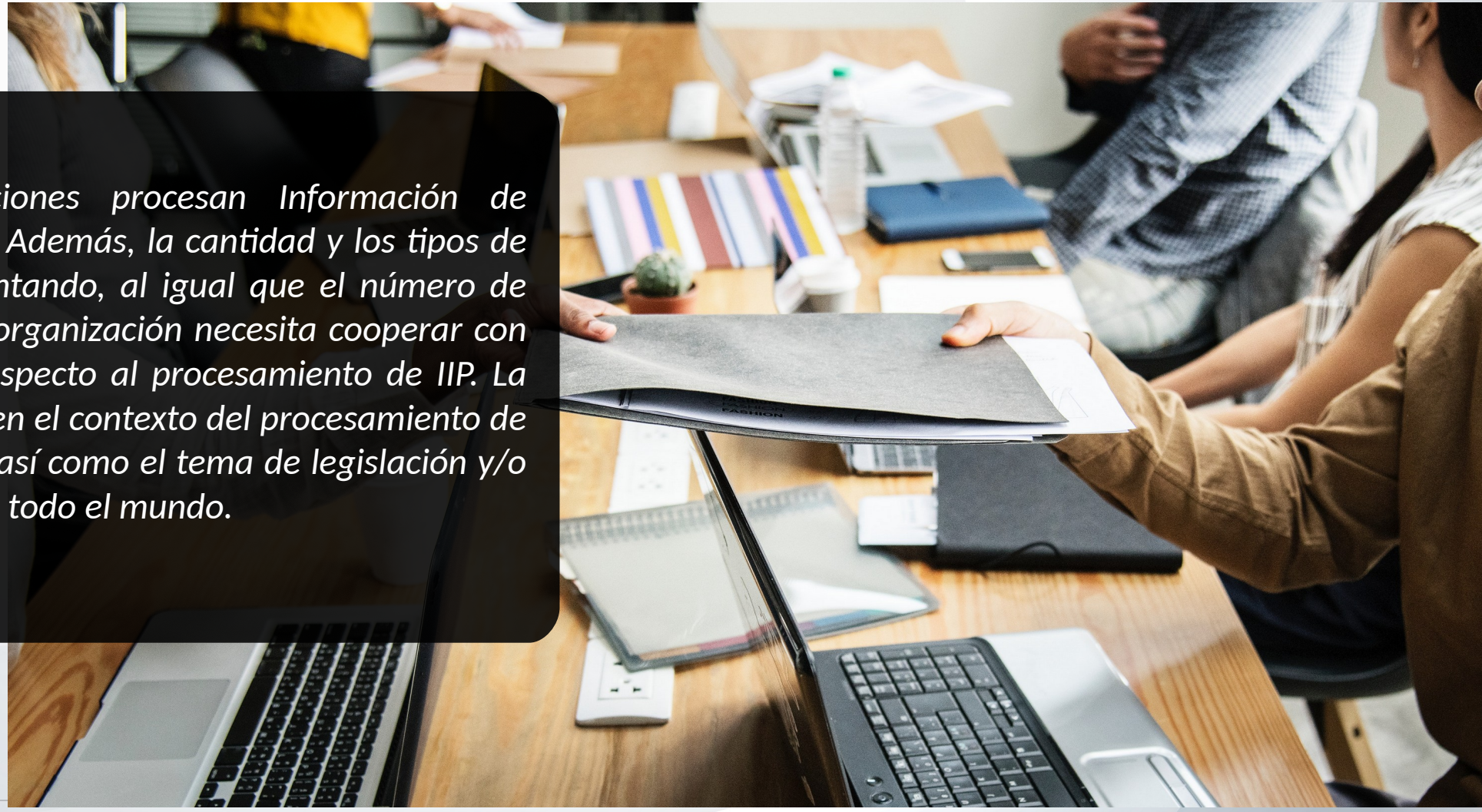
2 Estructura

3 Requisitos en PNTP-ISO/IEC 27701

4 Relación con ISO/IEC 27002

*Casi todas las organizaciones procesan Información de Identificación Personal (IIP). Además, la cantidad y los tipos de IIP procesados están aumentando, al igual que el número de situaciones en las que una organización necesita cooperar con otras organizaciones con respecto al procesamiento de IIP. La protección de la privacidad en el contexto del procesamiento de IIP es una necesidad social, así como el tema de legislación y/o regulación especializadas en todo el mundo.*

**NTP-ISO/IEC 27701:2020**




**NTP-ISO/IEC 27701:2020**

**Orientado a organizaciones de todo sector, tipo y tamaño. Especifica los requisitos relacionados con el SGIP y proporciona orientación para los controladores y procesadores de IIP que tienen la responsabilidad y la obligación de rendir cuentas por el procesamiento de IIP.**

1

# Términos relevantes

INSTITUTO NACIONAL DE CALIDAD

# Términos relevantes (1/2)

01

**Información de identificación personal IIP**
cualquier información que (a) pueda usarse para identificar al titular de PII con quien se relaciona dicha información, o (b) está o podría estar directa o indirectamente vinculado a un titular IIP

02

**Titular de IIP**
persona física a quien se refiere la información de identificación personal (IIP)

03

**Controlador de IIP**
interesado en la privacidad (o interesados en la privacidad) que determina los propósitos y los medios para procesar información de identificación personal (IIP) que no sean personas físicas que usen datos para fines personales

04

**Procesador de IIP**
interesado en la privacidad que procesa información de identificación personal (IIP) en nombre de y de acuerdo con las instrucciones de un controlador de IIP

# Términos relevantes (2/2)

**Controlador Conjunto de IIP**

El Controlador de IIP que determina los propósitos y medios del procesamiento conjunto de IIP con uno o más controladores de IIP diferentes.

**Sistema de Gestión de la Información sobre Privacidad (SGIP)**

Sistema de Gestión de seguridad de la Información que aborda la protección de la privacidad como lo potencialmente afectado por el procesamiento de IIP

2

# Estructura

INSTITUTO NACIONAL DE CALIDAD

# Estructura

1 Alcance

2 Referencias normativas

3 Términos, definiciones y abreviaciones

4 General

5 Requisitos específicos del SGIP relacionados con ISO/IEC 27001

6 Guía específica del SGIP relacionada con la ISO/IEC 27002

7 Orientación adicional a ISO/IEC 27002 para controladores IIP

8 Guía adicional ISO/IEC 27002 para procesadores IIP

Anexo A
SGIP - Objetivos de control y controles de referencia específicos (Controladores IIP)

Anexo B
SGIP - Objetivos de control y controles de referencia específicos (procesadores IIP)

Anexo C
Mapeo a ISO/IEC 29100

Anexo D
Mapeo al Reglamento General de Protección de Datos

Anexo E
Mapeo entre ISO / IEC 27018 e ISO / IEC 29151

Anexo F
Cómo aplicar ISO/IEC 27701 a ISO/IEC 27001 e ISO/IEC 27002

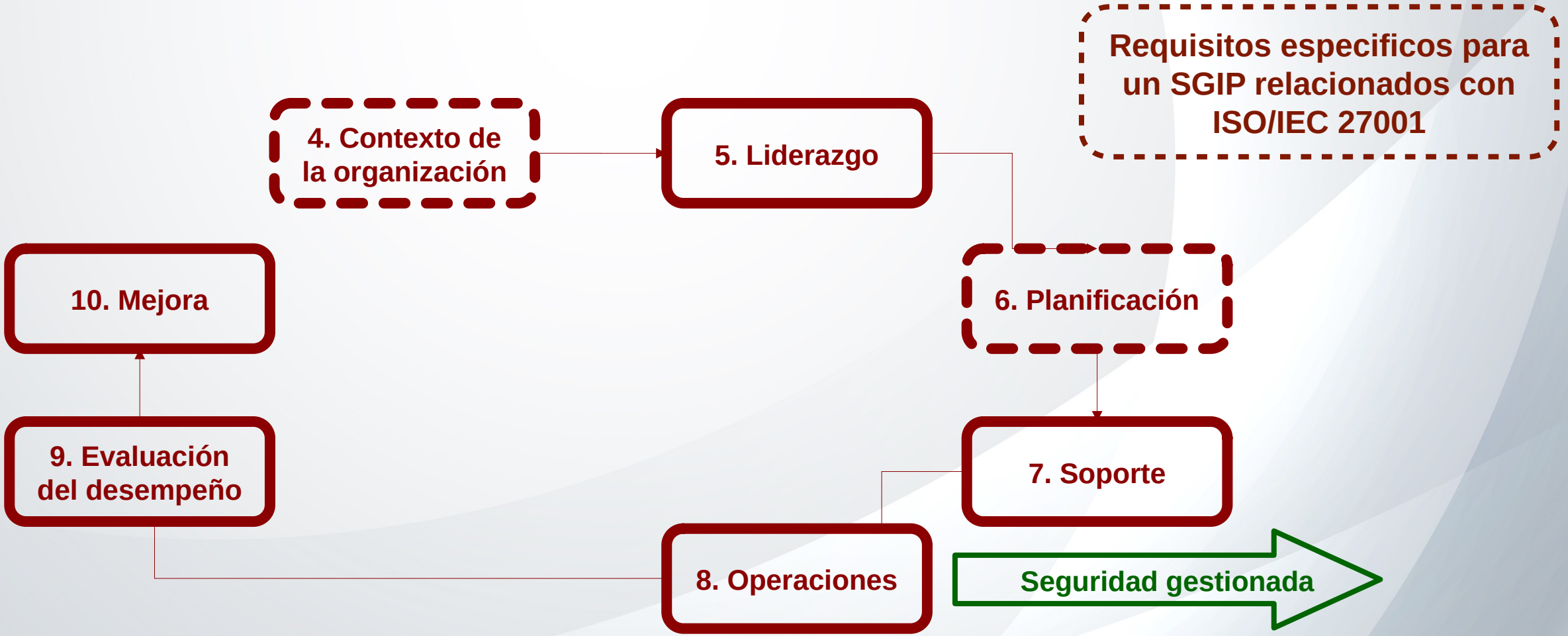
3

# Requisitos en NTP-ISO/IEC 27701

INSTITUTO NACIONAL DE CALIDAD

# Requisitos en NTP-ISO/IEC 27701

# Requisitos en NTP-ISO/IEC 27701



4

# Relación con ISO/IEC 27002

INSTITUTO NACIONAL DE CALIDAD

# Relación con ISO/IEC 27002 (1/7)

**PNTP-ISO/IEC 27701**

- 6 Guía específica del SGIP relacionada con la ISO/IEC 27002
- 7 Orientación adicional a ISO/IEC 27002 para controladores IIP
- 8 Guía adicional ISO/IEC 27002 para procesadores IIP

# Relación con ISO/IEC 27002 (2/7)


6.1 General
6.2 Políticas de seguridad de la información
6.3 Organización de la seguridad de la información
6.4 Seguridad de los recursos humanos
6.5 Gestión de activos
6.6 Control de acceso
6.7 Criptografía
6.8 Seguridad física y ambiental
6.9 Seguridad de las operaciones
6.10 Seguridad de las comunicaciones
6.11 Adquisición, desarrollo y mantenimiento de sistemas
6.12 Relaciones con los proveedores
6.13 Gestión de incidentes de seguridad de la información
6.14 Aspectos de seguridad de la información en la gestión de continuidad del negocio
6.15 Cumplimiento

# Relación con ISO/IEC 27002 (3/7)

**Ejemplo**

**6.2 Políticas de seguridad de la información**

**6.2.1 Lineamientos de gestión para la seguridad de la información**

**6.2.1.1 Políticas para la seguridad de la información**

Se aplica el control, la guía de implementación y otra información establecida en la ISO/IEC 27002:2013, 5.1.1 y la siguiente guía adicional:

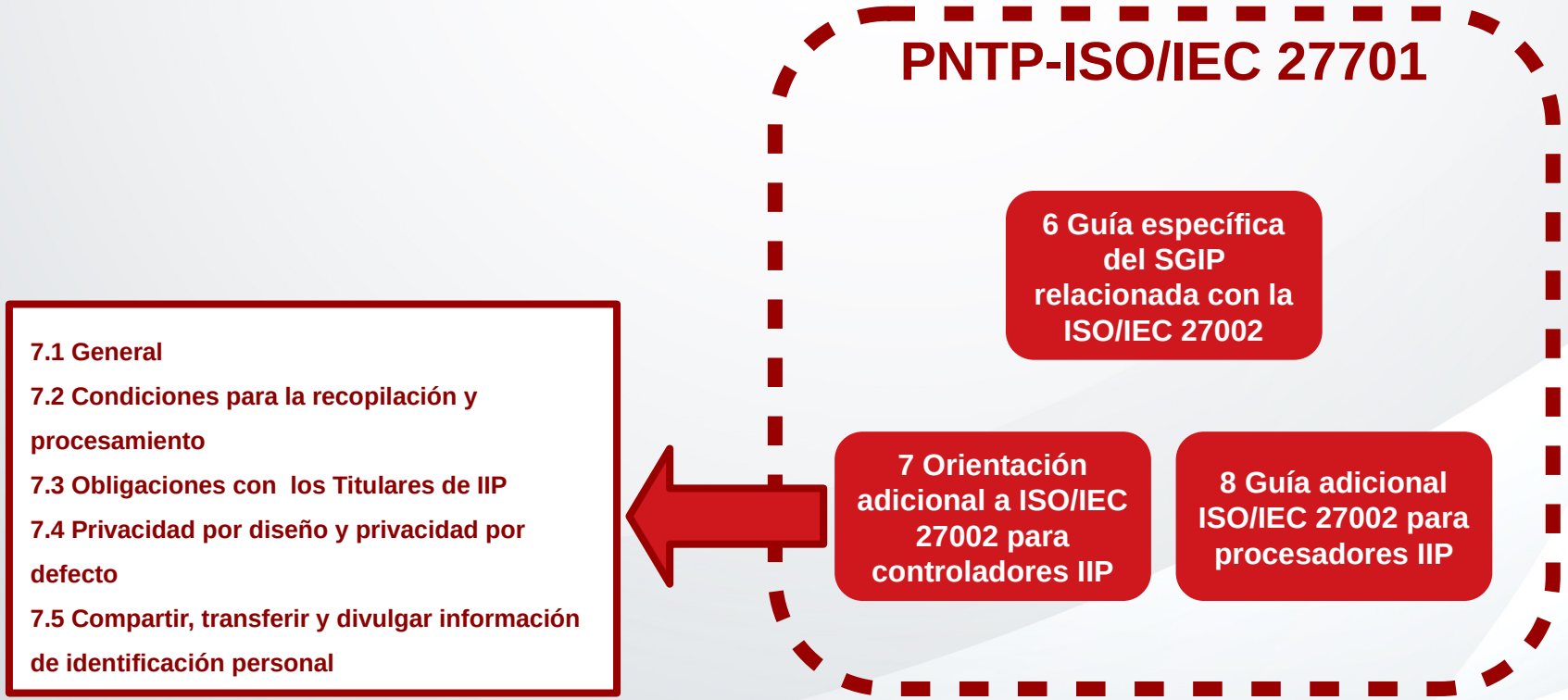
**Guía adicional para implementación de 5.1.1, Políticas para la seguridad de la información, de la ISO/IEC 27002:2013 es:**

Ya sea por el desarrollo de políticas de privacidad separadas, o incrementándolas en las políticas de seguridad de la información, la organización debería producir una declaración con respecto al apoyo y el compromiso de lograr el cumplimiento de la legislación y/o regulación de protección del IIP aplicable y con los términos contractuales acordados entre la organización y sus socios, sus subcontratistas y sus terceros aplicables (clientes, proveedores, etc.), que deberían asignar claramente las responsabilidades entre ellos.

**Otra información adicional para 5.1.1, Políticas para la seguridad de la información, de la ISO/IEC 27002:2013 es:**

Cualquier organización que procese IIP, ya sea un controlador de IIP o un procesador de IIP, debería considerar la legislación y/o regulación de protección de IIP aplicable durante el desarrollo y mantenimiento de las políticas de seguridad de la información.

# Relación con ISO/IEC 27002 (4/7)



# Relación con ISO/IEC 27002 (5/7)

**Ejemplo**

**7.3 Obligaciones a los Titulares de IIP**

Objetivo: Garantizar que los Titulares de IIP reciben información adecuada sobre el procesamiento de su IIP y cumplir con cualquier otra obligación aplicable a los Titulares de IIP relacionada según el procesamiento de su IIP.

**7.3.1 Determinar y cumplir las obligaciones con los Titulares de IIP**

**Control**

La organización debería determinar y documentar sus obligaciones legales, regulatorias y comerciales con los Titulares de IIP relacionadas con el procesamiento de su IIP y proporcionar los medios para cumplir con estas obligaciones.

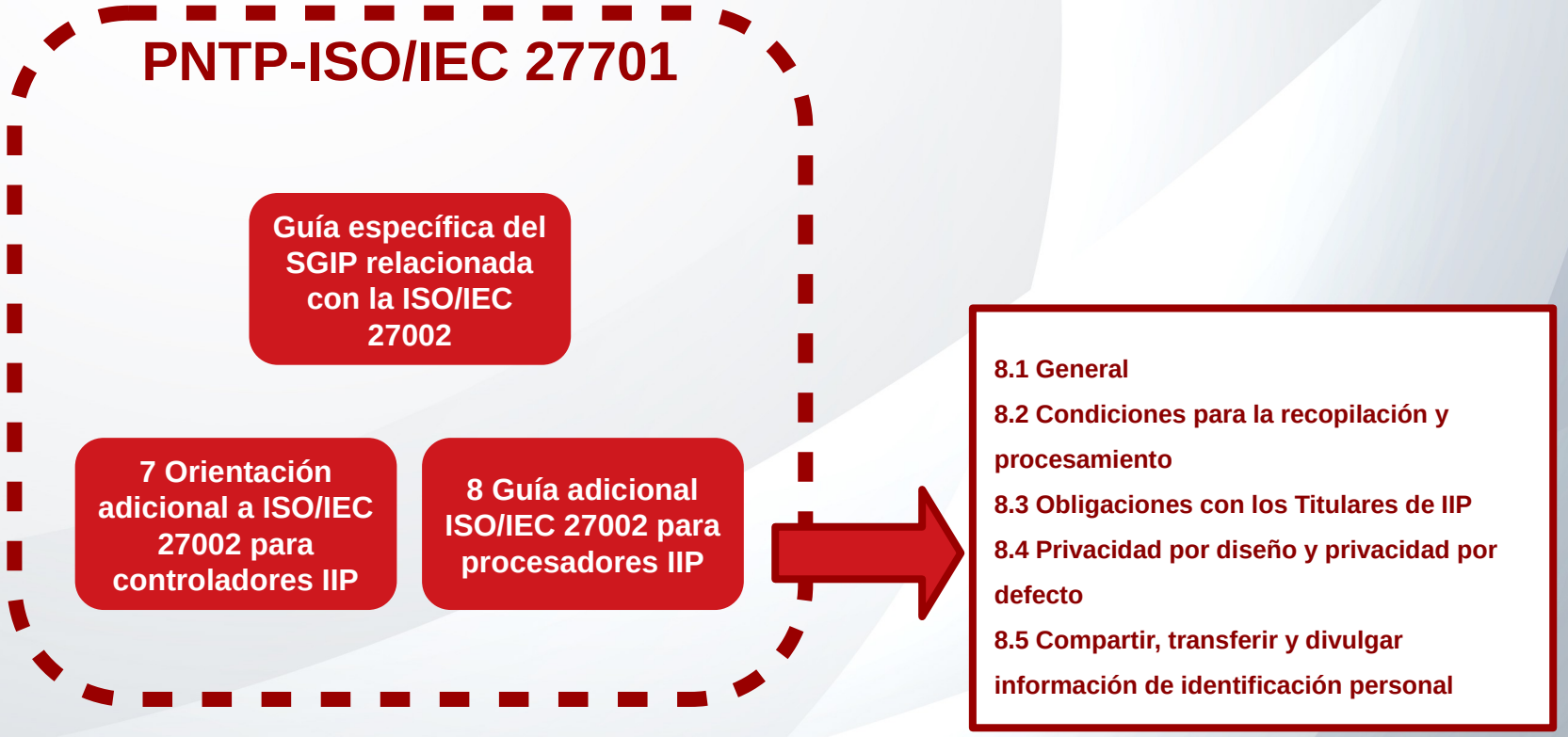
**Guía de implementación**

Las obligaciones con los Titulares de IIP y los medios para apoyarlos varían de una jurisdicción a otra.

La organización debería garantizar que proporcionan los medios adecuados para cumplir las obligaciones con los titulares de IIP de manera accesible y oportuna. Debería proporcionarse documentación clara al principal de la IIP en la que se describa en qué medida se cumplen las obligaciones con ellos y cómo, junto con un punto de contacto actualizado a donde pueda dirigir sus solicitudes.

El punto de contacto debería proporcionarse en una forma similar a que se utiliza para recopilar IIP y consentimiento (por ejemplo, si la IIP se recopila por correo electrónico o un sitio web, el punto de contacto debería ser por correo electrónico o el sitio web, no una alternativa como el teléfono o el fax).

# Relación con ISO/IEC 27002 (6/7)



# Relación con ISO/IEC 27002 (7/7)

**Ejemplo**

**8.3 Obligaciones con los Titulares de IIP**

Objetivo: Asegurar que los Titulares de IIP reciban la información apropiada sobre el procesamiento de su IIP y cumplir con cualquier otra obligación aplicable a los Titulares de IIP relacionada con el procesamiento de su IIP.

**8.3.1 Obligaciones con los Titulares de IIP**

**Control**

La organización debería proporcionar al cliente los medios para cumplir con sus obligaciones relacionadas con los Titulares de IIP.

**Guía de implementación**

Las obligaciones de un controlador IIP pueden definirse por legislación, por reglamento y/o por contrato. Estas obligaciones pueden incluir asuntos en los que el cliente utiliza los servicios de la organización para la implementación de estas obligaciones. Por ejemplo, esto puede incluir la corrección o eliminación de IIP de manera oportuna.
Cuando un cliente depende de la organización para obtener información o medidas técnicas para facilitar el cumplimiento de las obligaciones con los Titulares de IIP, la información relevante o las medidas técnicas deberían especificarse en un contrato.

PERÚ Ministerio de la Producción

INACAL Instituto Nacional de Calidad

INSTITUTO NACIONAL **DE CALIDAD**

# GRACIAS


**CARLOS A. HORNA VALLEJOS**

carlos@gtdi.pe


Siempre con el pueblo