



ISO/IEC 27001

Gestión de la seguridad de la información

Ing. Marco Antonio Paredes Poblano

2do. Congreso Internacional para la Acreditación en el Sector Salud



¿Qué es información?

Conjunto de datos organizados en poder de una entidad que poseen valor para la misma.

**La información
puede estar**

- **escrita**
- **en imágenes**
- **oral**
- **impresa en papel**
- **almacenada electrónicamente**
- **Proyectada**
- **enviada por correo, fax o e-mail**
- **transmitida en conversaciones**
- **nube**



Seguridad de la información

Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.



Confidencialidad

- **La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.**

Integridad

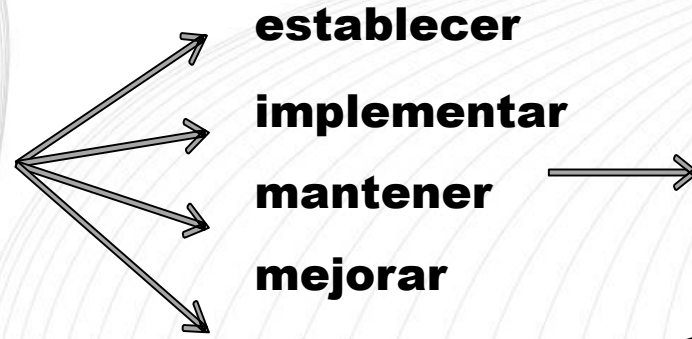
- **Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.**

Disponibilidad

- **Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.**



Norma internacional que establece requisitos para



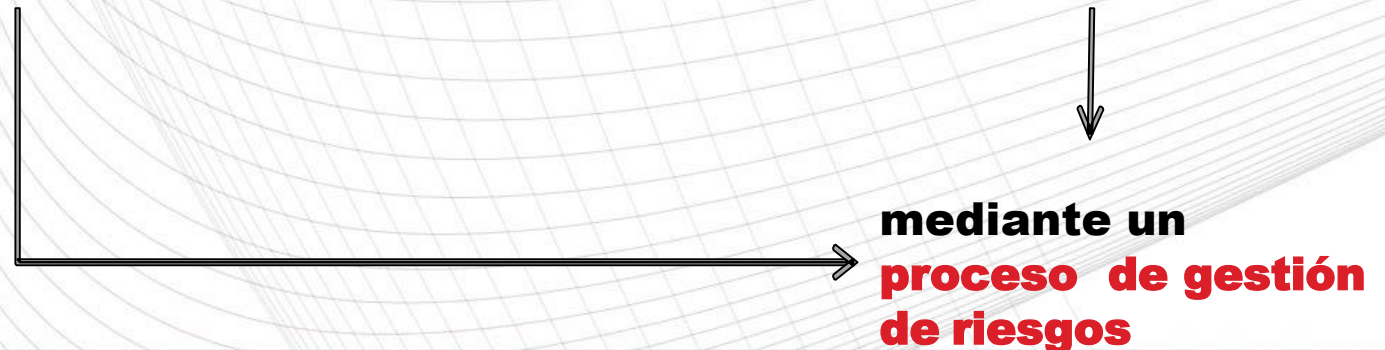
un sistema de gestión de seguridad de la información (SGSI)

brinda la **confianza sobre la gestión adecuada de los riesgos a las partes interesadas**

preserva la

- **confidencialidad**
- **integridad**
- **disponibilidad**

de la información





¿Qué es un SGSI?

Dado el conocimiento del *ciclo de vida* de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI

Evolución



**ISO
27002**

1992

**Code of
Practice
for Information
Security
Management**
Gobierno
Británico

BSI 7999

British
Standards
Institute (BSI)

1999

BSI 7999
British
Standards
Institute
(BSI)

**ISO
27799**

2000

**ISO/IEC
17779**
ISO

2002

**ISO
27001**

BSI 7999-2
British
Standards
Institute
(BSI)

2005

**ISO/IEC
17779**
ISO

2005

**ISO/IEC
27001**
ISO

2007

**ISO/IEC
27002**
ISO
2007

2013

**ISO/IEC
27002**
ISO
2016

2013

**ISO/IEC
27001**
ISO

Familia ISO 27000



ISO/IEC 27000:2014

**Fundamentos
y vocabulario**



**ISO/IEC
27001:2013
Requisitos
para
certificación**



**ISO/IEC
27002:2013
Mejores
prácticas**



**ISO/IEC
27003:2010
Guía de
implementaci-
ón**



**ISO/IEC
27004:2009
Recomendacio-
nes sobre
medidas de
seguridad**



**ISO/IEC
27005:2011
Recomendacion
es proceso de
gestión de
riesgos**



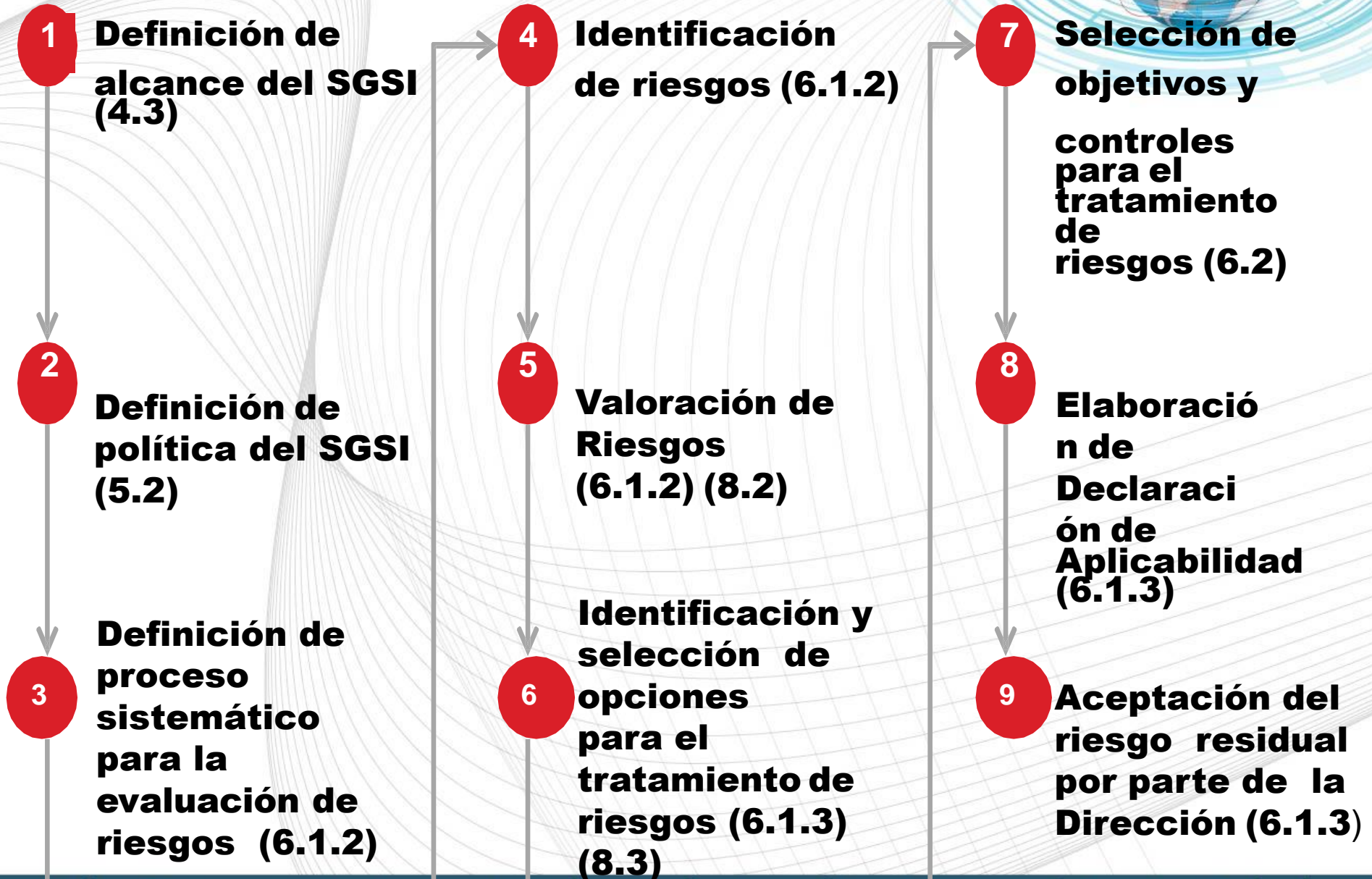
**ISO/IEC
27006:2011
Requisitos
acreditación
organismos
de
certificación**



**ISO/IEC
27007:2011
Directrices
para auditar
un SGSI**



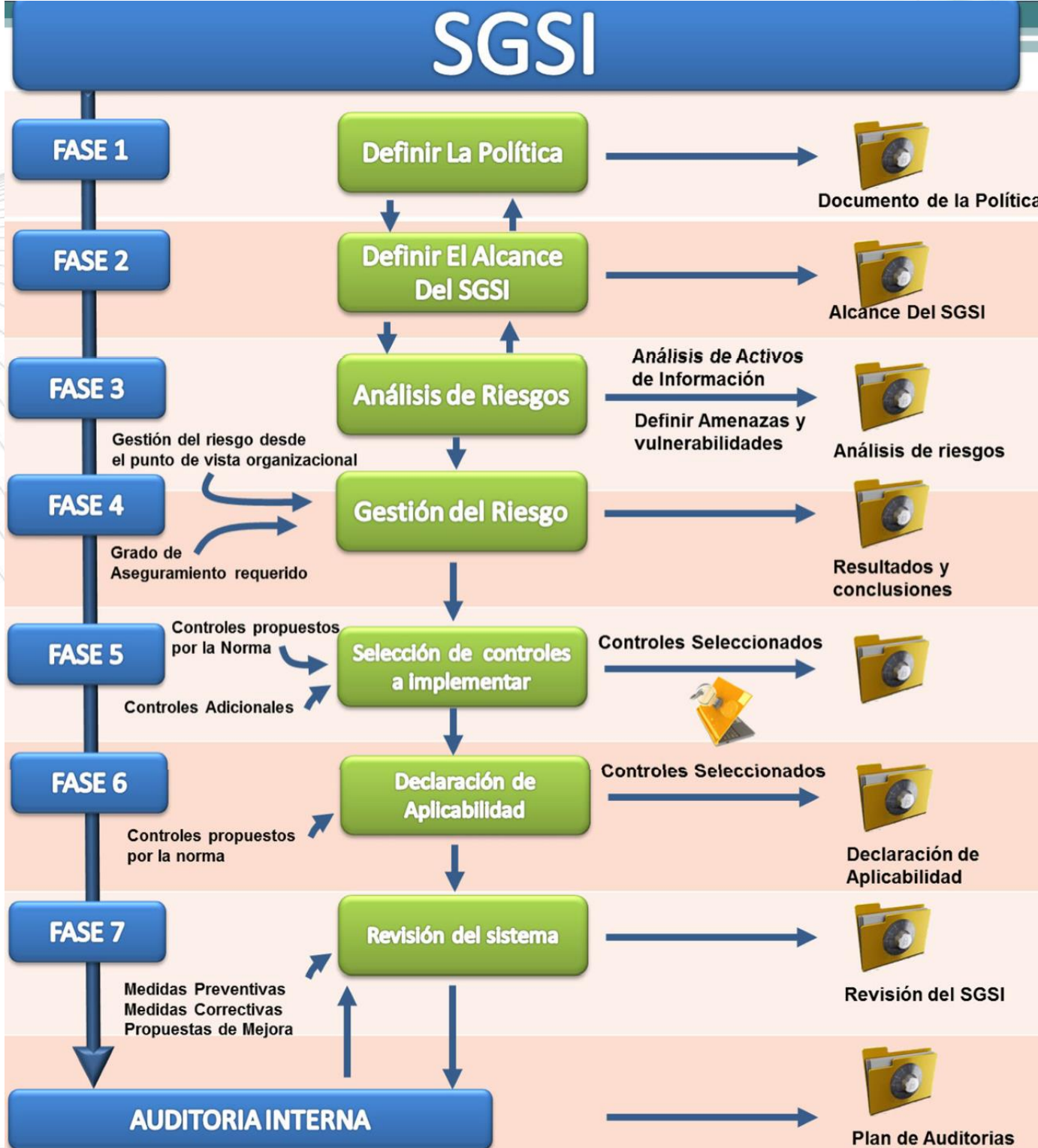
Establecimiento de un SGSI



Cambio: anexo SL



- **adopción del Anexo SL (lo que era antes la Guía ISO 83) dentro del SGSI. Es importante mencionar que este anexo describe los lineamientos para un sistema de gestión genérico; ayudando a las empresas que por alguna razón deben certificar múltiples normas de sistemas de gestión. De esta forma ISO 27001 cumple con los requisitos comunes a todo sistema de gestión, facilitando la implementación y auditoría de varios sistemas en la misma organización.**





Documentos*	Capítulo de ISO 27001:2013
Alcance del SGSI	4.3
Políticas y objetivos de seguridad de la información	5.2, 6.2
Metodología de evaluación y tratamiento de riesgos	6.1.2
Declaración de aplicabilidad	6.1.3 d)
Plan de tratamiento del riesgo	6.1.3 e), 6.2
Informe de evaluación de riesgos	8.2
Definición de funciones y responsabilidades de seguridad	A.7.1.2, A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos operativos para gestión de TI	A.12.1.1
Principios de ingeniería para sistema seguro	A.14.2.5
Política de seguridad para proveedores	A.15.1.1
Procedimiento para gestión de incidentes	A.16.1.5
Procedimientos de la continuidad del negocio	A.17.1.2
Requisitos legales, normativos y contractuales	A.18.1.1



Registros*	Capítulo de ISO 27001:2013
Registros de capacitación, habilidades, experiencia y calificaciones	7.2
Resultados de supervisión y medición	9.1
Programa de auditoría interna	9.2
Resultados de las auditorías internas	9.2
Resultados de la revisión por parte de la dirección	9.3
Resultados de acciones correctivas	10.1
Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	A.12.4.1, A.12.4.3

Ventajas de implantar un SGSI basado en la ISO 27001



- ✓ **Garantizar la confidencialidad, integridad y disponibilidad de información sensible.**
- ✓ **Disminuir el riesgo, con la consiguiente reducción de gastos asociados.**
- ✓ **Reducir la incertidumbre por el conocimiento de los riesgos e impactos asociados.**
- ✓ **Mejorar continuamente la gestión de la seguridad de la información.**
- ✓ **Garantizar la continuidad del negocio.**
- ✓ **Aumento de la competitividad por mejora de la imagen corporativa.**
- ✓ **Incremento de la confianza de las partes interesadas.**



- ✓ **Aumento de la rentabilidad, derivado de un control de los riesgos.**
- ✓ **Cumplir la legislación vigente referente a seguridad de la información.**
- ✓ **Aumentar las oportunidades de negocio.**
- ✓ **Reducir los costos asociados a los incidentes.**
- ✓ **Mejorar la implicación y participación del personal en la gestión de la seguridad.**
- ✓ **Posibilidad de integración con otros sistemas de gestión como ISO 9001, ISO14001, OHSAS 18001, entre otros.**
- ✓ **Mejorar los procesos y servicios prestados.**
- ✓ **Aumentar de la competitividad por mejora de la imagen corporativa.**



Más allá de los cambios en el estándar, lo más importante es tener en cuenta que todas las organizaciones son diferentes y los requerimientos impuestos por la norma deben ser interpretados de acuerdo al contexto de cada empresa.

Conclusiones



La implantación de un SGSI basado en ISO 27001, supone el conocimiento de la organización en su conjunto y de los riesgos a los que se encuentra expuesta, de manera que se asuman y se trabaje en su minimización y control de manera sistemática, para mejorar continuamente.

La ISO 27001 es perfectamente integrable con otros sistemas de gestión como ISO 9001, ISO 14001 u OHSAS, entre otras. Esta integración se hace más sencilla con esta nueva versión ISO 27001:2013

Ya está vigente la nueva versión ISO 27001:2013 que sustituye a la anterior ISO 27001:2005.

La ISO 27001 permite una operativa basada en la seguridad y la excelencia en el tratamiento de la información en la organización, que se traducen en un mejor servicio con una menor inversión



Preguntas ??