



INICIO  
GRABACIÓN



**SANJOSÉ**  
FUNDACIÓN DE EDUCACIÓN SUPERIOR



# Arquitectura De TI

**Wilson Cárdenas Cr.**  
**Fundación de educación superior San Jose**  
**Semana 12**



# FUNDAMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE SGSI ISO 27001





# Contenido

## **Sistema de Gestión de Seguridad de la Información (SGSI)**

- Definición
- Enfoque en los procesos
- Visión general – Cláusulas 4 a 10
- Anexo A





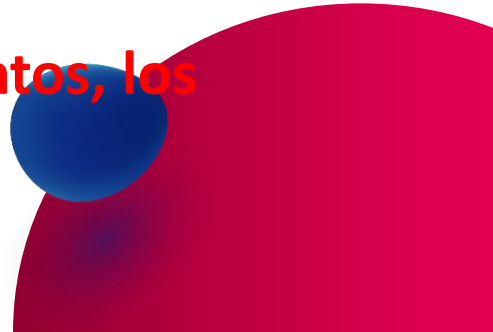
# Definición del SGSI

---

## ISO 27000, cláusula 3.2.1:

Un SGSI es un enfoque un en sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para conseguir los objetivos del negocio. Se basa en una evaluación del riesgo y de los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar los riesgos de manera eficaz. Analizar los requisitos para gestionar los riesgos de manera eficaz. Analizar los requisitos para la protección de los activos de información y aplicar controles adecuados para garantizarla protección de estos activos de información, según sea necesario, contribuye a la aplicación exitosa de un SGSI

**Nota: El Sistema de gestión consta de las Políticas, los Procedimientos, los lineamientos, las actividades y recursos asociados**





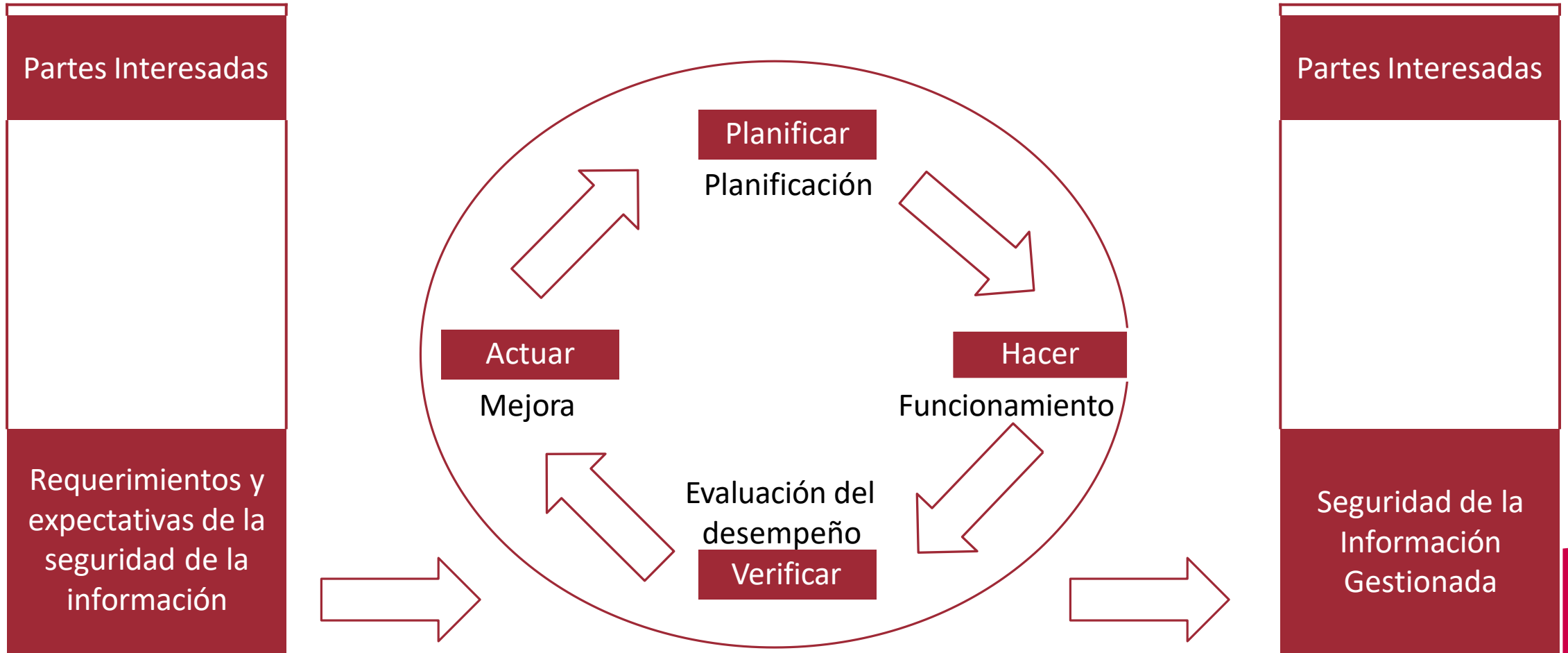
# Las definiciones relacionadas con el concepto de “SGSI” ISO 9000 e ISO 27000

---

- **Sistemas:** Conjunto de elementos interrelacionados o que interactúan (ISO 9000, 3.2.1).
- **Gestión:** Actividades coordinadas para dirigir y controlar un organización (ISO 9000, 3.2.6)
- **Sistemas de gestión:** Sistema para establecer la política y objetivos, y para alcanzar dichos objetivos (ISO 9000, 3.2.2)
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información (ISO 27000, 2.19)



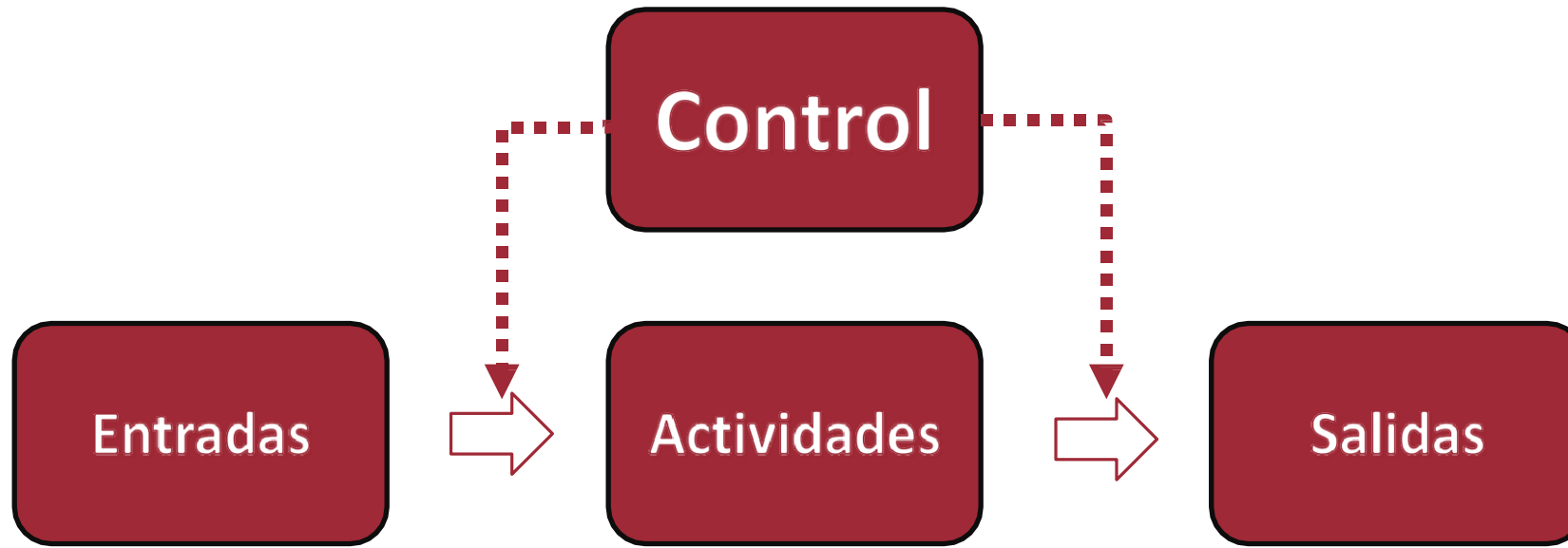
# Enfoque a Procesos





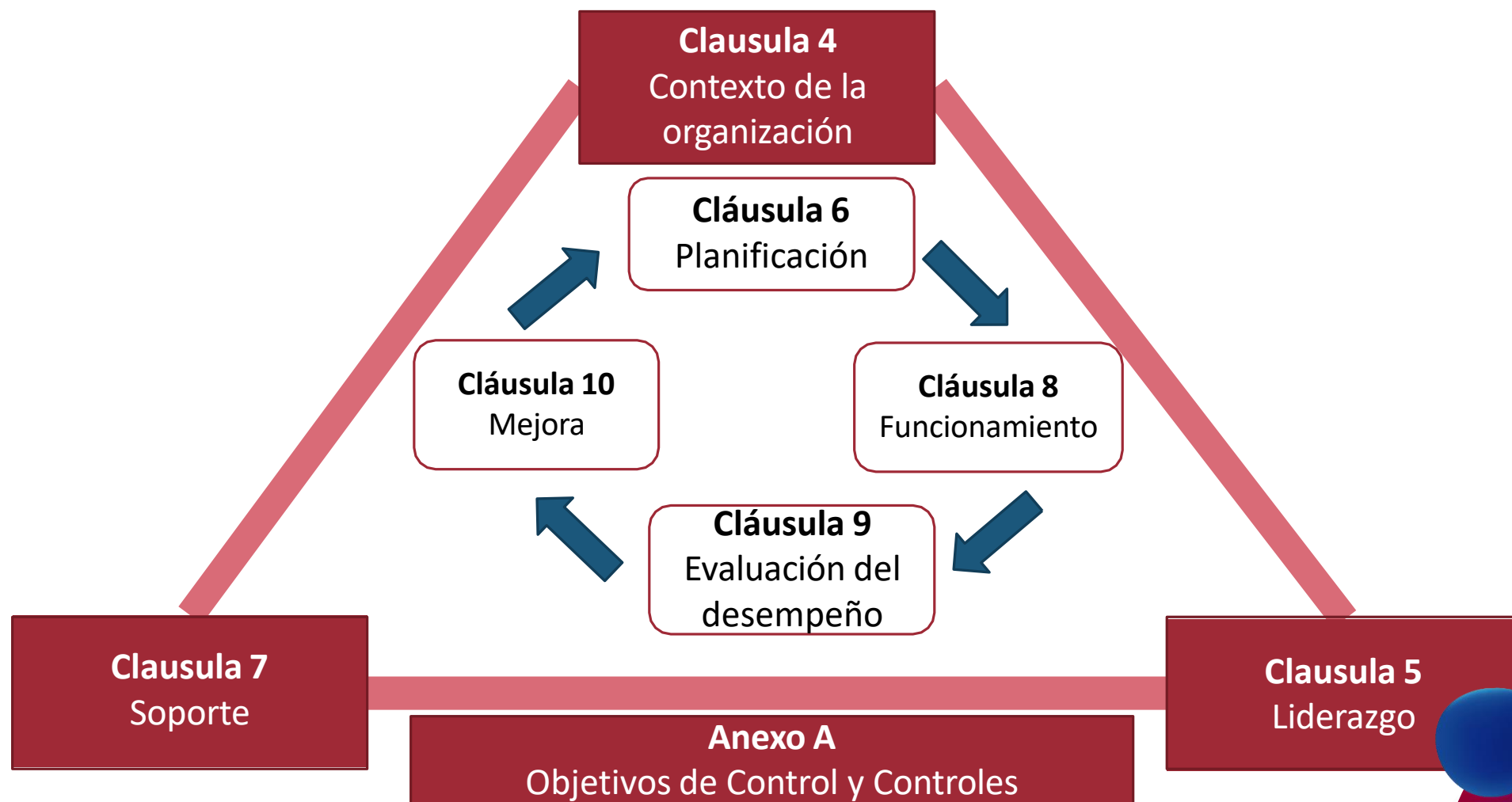
# Enfoque a Procesos

- La aplicación del enfoque de proceso variará de una organización a otra en función de su tamaño, complejidad y actividades
- A menudo las organizaciones identifican demasiados procesos





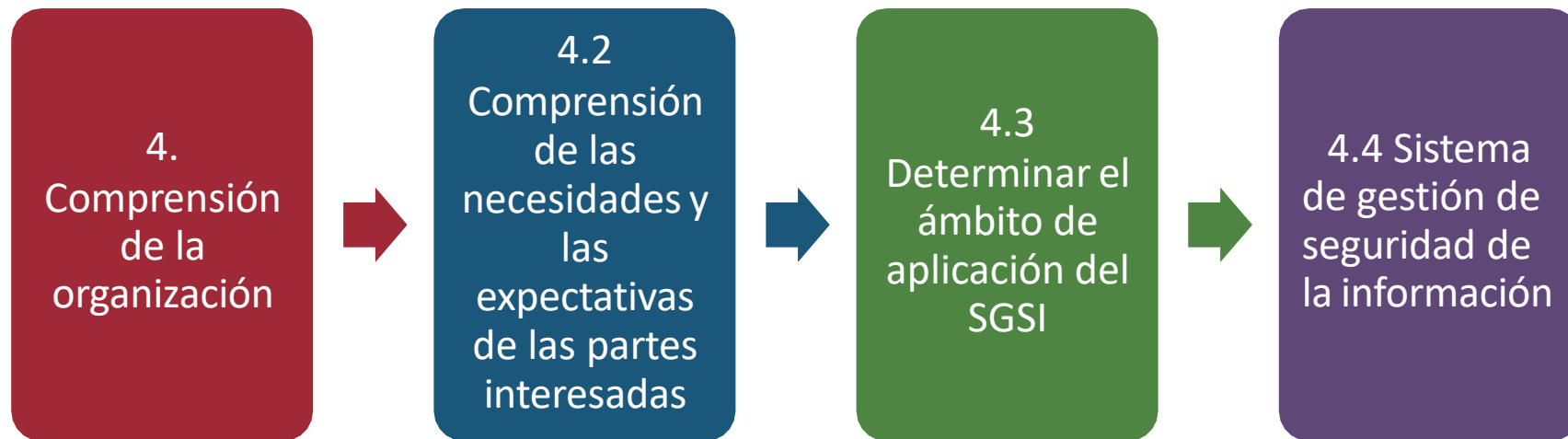
# Estructura de la norma ISO 27001



# Contexto de la organización



ISO 27001, cláusulas 4.1-4.4



# Liderazgo y Compromiso de la Dirección



ISO 27001, cláusulas 5.1

## Orientación estratégica

- Asegurarse de que el SGSI es compatible con la orientación estratégica de la organización
- Integrar los requisitos del SGSI en los procesos de negocio de una organización

## Hacer que los recursos estén disponibles

- La Dirección deberá determinar y proporcionar los recursos necesarios para el SGSI

## Comunicación

- La Dirección deberá comunicar la importancia de una buena Gestión de la Seguridad de la Información y el cumplimiento de los procesos del SGSI





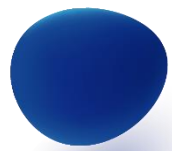
# Política de Seguridad de la Información

---

ISO 27001, cláusulas 5.2

- **La alta dirección debe establecer una política de seguridad de la información que:**
  - Sea apropiada para los fines de la organización
  - Proporcione un marco para establecer objetivos de seguridad de la información
  - Incluya un compromiso de cumplir los requisitos aplicables
  - Incluya un compromiso de mejora continua del SGSI
- **La política del SGSI deberá**
  - Estar disponible como información documentada
  - Ser comunicada dentro de la organización
  - Estar a disposición de todas las partes interesadas, según corresponda





# Funciones, Responsabilidades y Autoridades



ISO 27001, cláusula 5.3

- La alta dirección deberá asegurarse de que las responsabilidades y autoridades para funciones pertinentes sean asignadas y comunicadas dentro de la organización
- La alta gerencia deberá asignar la responsabilidad y autoridad para:
  - ❖ Garantizar que el sistema de gestión se establece y ejecuta en conformidad con los requisitos de la norma ISO 27001
  - ❖ Informar sobre la eficacia de la gestión del SGSI a la alta dirección





# Planificación



## ISO 27001, cláusula 6

Asegurar que el SGSI puede lograr resultados previstos, prevenir o reducir efectos no deseados, lograr mejoras continuas, planificar acciones para hacer frente a los riesgos y oportunidades, ponerlos en práctica y evaluar su eficacia

Determinar riesgos y oportunidades

Evaluación del riesgo de la Seguridad de la Información

Establecer y mantener criterios de riesgo, asegurarse de que las evaluaciones de riesgo repetidas producen resultados consistentes, validos y comparables, identificar los riesgos, analizar los riesgos, evaluar los riesgos

Seleccionar las opciones de tratamiento del riesgo, determinar los controles para aplicar las opciones, comparar los controles determinados, producir declaración de aplicabilidad, formular plan de tratamiento de riesgos, obtener la aprobación del plan y la aceptación de los riesgos residuales

Tratamiento de riesgos de la seguridad de la información

Objetivos de la Seguridad de la Información

Coherentes con la política de SI, mensurables, toman en cuenta los requisitos, la evaluación de riesgos y los resultados del tratamiento del riesgo, comunicados, actualizados. Lo que se va a hacer, ¿Qué recursos serán necesarios, quien será responsable, cuando se concluya, como se evaluarán los resultados?



# Apoyo

## ISO 27001, cláusula 7



La organización deberá determinar y proporcionar los recursos necesarios para el SGSI

### Recursos

### Competencia

La organización deberá asegurar tener personas competentes para realizar las tareas relacionadas con el SGSI

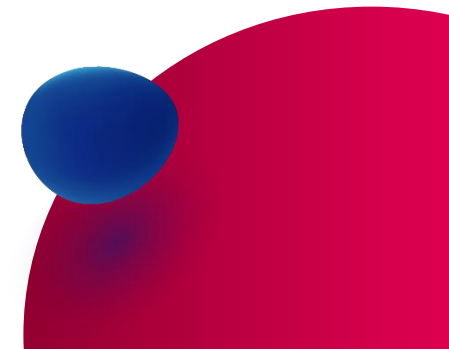
Las personas que realiza trabajo en el marco del control de la organización deberán ser conscientes de la política de SI, sus funciones en el SGSI y los requisitos para la organización

### Concientización

### Comunicación

La Organización deberá establecer, implementar y mantener mecanismos de comunicación con las partes interesadas internas y externas

El SGSI de la organización deberá incluir información documentada requerida por la ISO 27001 y registros para demostrar la eficacia del SGSI



# Información documentada

ISO 27001, cláusula 7,5



Se debe establecer un procedimiento para gestionar el ciclo de vida de los documentos


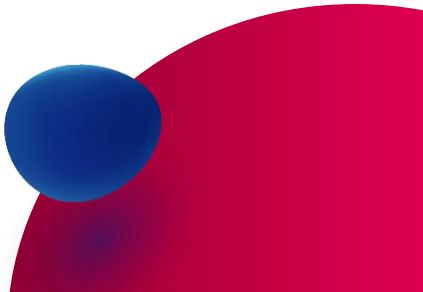


# Planificación operativa y control



---

ISO 27001, cláusula 8,1

- La organización deberá planificar, ejecutar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información, y aplicar las medidas determinadas para hacer frente a los riesgos y oportunidades. La organización también deberá implementar planes para alcanzar objetivos de seguridad de la información establecidos.
  - La organización deberá mantener información documentada en la medida en que sea necesario para tener confianza en que los procesos se han llevado a cabo como estaba previsto.
  - La organización deberá controlar los cambios programados, y analizar las consecuencias de los cambios fortuitos, tomando medidas para mitigar los posibles efectos adversos, según sea necesario.
  - La organización deberá asegurarse de que los procesos tercerizados son determinados y controlados.
- 
- 



# Evaluación y tratamiento del riesgo en seguridad de la información

---

ISO 27001, cláusulas 8,2 y 8,3

Deberá realizarse la evaluación de riesgos en la seguridad de la información



Deberá ser aplicado el plan de tratamiento del riesgo para la seguridad de la información





# Monitoreo y Revisión del SGSI

ISO 27001, cláusulas 9




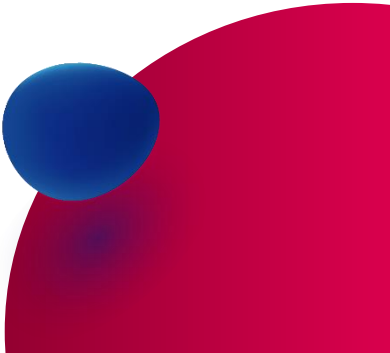
**Nota:** Cada una de estas acciones debe ser documentada y registrada



# Auditorías Internas del SGSI

---

ISO 27001, cláusulas 9.2

- La organización deberá llevar a cabo auditorías internas del SGSI a intervalos reguladores
  - Debe planificarse un programa de auditoría teniendo en cuenta la importancia de los procesos y alcances de auditoría, así como los resultados de auditorías anteriores
- 
- 



# Revisión del SGSI por la Dirección

ISO 27001, cláusulas 9,3

## Revisión por la Dirección de los elementos de entrada

1. Las acciones de seguimiento de las revisiones anteriores
  2. Los cambios en las cuestiones internas y externas que son relevantes para el SGSI
  3. No conformidades y acciones correctivas
  4. Seguimiento y resultados de la medición
  5. Resultados de la auditoría
  6. El cumplimiento de los objetivos de seguridad de la información
  7. Los comentarios de las partes interesadas
  8. Resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos
- Oportunidades para la mejora continua

## Revisión por la Dirección de los elementos de salida

1. Las decisiones relativas a las oportunidades de mejora continua
2. La necesidad de cambios en el SGSI



# Mejora del SGSI

---

ISO 27001, cláusulas 10

- La organización deberá mejorar continuamente la conveniencia, adecuación y eficacia del SGSI
- Cuando la disconformidad se produce, la organización deberá:
  - Reaccionar a la no conformidad
  - Evaluar la necesidad de adoptar medidas para eliminar las causas de no conformidades, a fin de que no se repita o se produzca en otros lugares
  - Aplicar las medidas necesarias
  - Revisar la eficacia de las medidas correctivas adoptadas
  - Realizar cambios en el SGSI



# Objetivos y controles de seguridad



ISO 27001, Anexo A

## ISO 27001

**Anexo A**  
(Lista de los objetivos y  
controles de seguridad)



## ISO 27002

Objetivos y controles

Recomendaciones para  
la implementación

Información  
Complementaria





# ISO 27002, Cláusulas

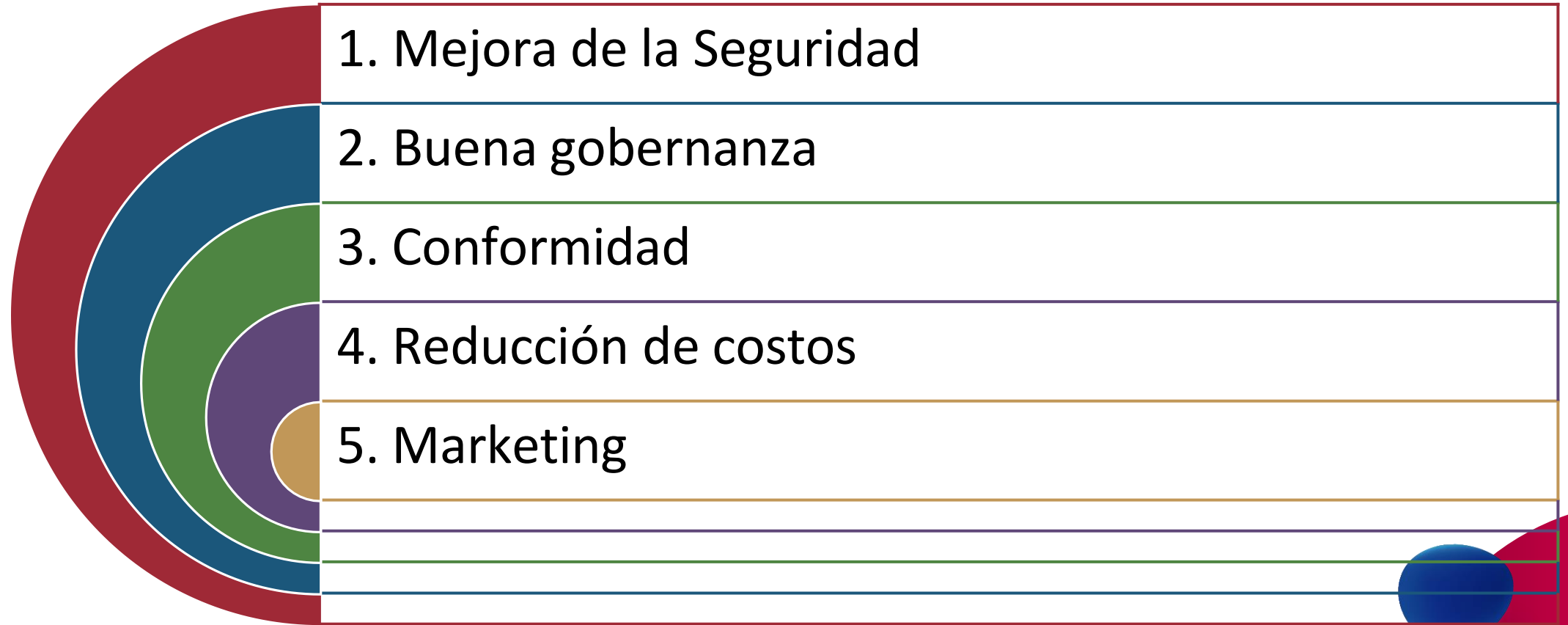
ISO 27001, Anexo A

A 5	Políticas de seguridad de la información
A 6	Organización de seguridad de la información
A 7	Seguridad de los recursos humanos
A 8	Gestión de activos
A 9	Control de accesos
A 10	Criptografía
A 11	Seguridad física y medioambiental
A 12	Seguridad de la operaciones
A 13	Seguridad de las comunicaciones
A 14	Adquisición de los sistemas, desarrollo y mantenimiento
A 15	Relaciones con los proveedores
A 16	Gestión de incidentes de seguridad de la información
A 17	Aspectos de seguridad de la información de la gestión de continuidad del negocio
A 18	Cumplimiento



# Ventajas de la ISO 27001


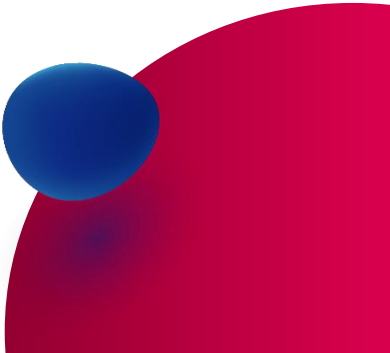
---





# Principios Fundamentales

---

1. Activo y activo de información
  2. Seguridad de la Información
  3. Confidencialidad, integridad y disponibilidad
  4. Vulnerabilidad, amenaza e impacto
  5. Riesgo para la seguridad de la información
  6. Objetivos y controles de seguridad
  7. Clasificación de controles de seguridad
- 
- 



# Información y activo

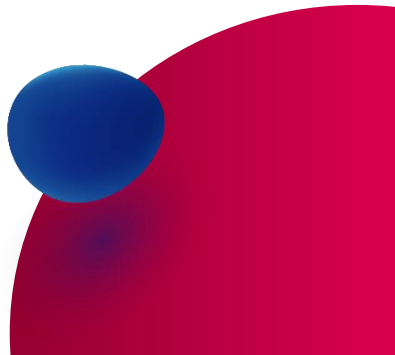
---

ISO 9000, cláusula 7.3.1; ISO 27000, cláusula 2,4

- **Información:** Datos significativos
- **Activo:** Cualquier bien que tiene valor para la organización

NOTA: hay muchos tipos de bienes, entre los que se incluyen:

- ❖ Información
- ❖ Software, tal como un programa de computación
- ❖ Físico, tal como un computador
- ❖ Servicios
- ❖ Las personas y sus calificaciones, competencia y experiencia
- ❖ Activos intangibles, tales como la reputación y la imagen





# Documento - Registro

---

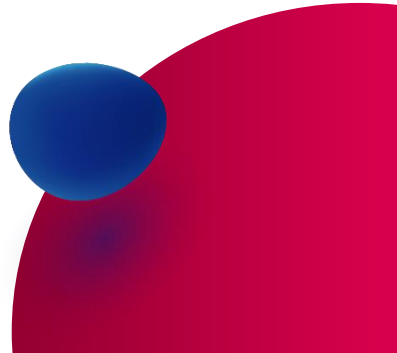
ISO 9000, cláusula 3,7

## Documento

- Información y su medio de soporte

## Registro

- Documento que indique los resultados obtenidos o proporcione evidencia de las actividades desempeñadas





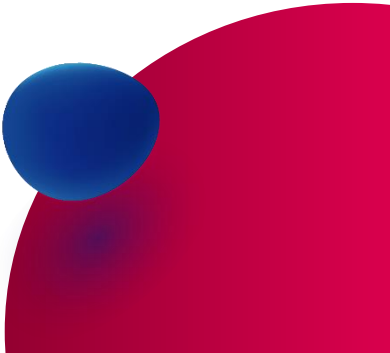


# Seguridad de la Información

---

ISO 27000, cláusula 2.3

- Preservación de la confidencialidad, integridad y disponibilidad de la información
- Nota: Por otra parte, también pueden participar otras propiedades, como la autenticidad, la responsabilidad, el no-repudio y la fiabilidad



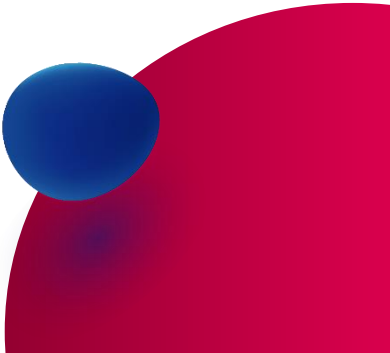


# Seguridad de la Información

---

Abarca todo tipo de información

- Impresa o escrita a mano
- Grabada con asistencia técnica
- Transmitida por correo electrónico o electrónicamente
- Incluida en un sitio web
- Mostrada en vídeos corporativos
- Mencionada durante las conversaciones
- Etc.



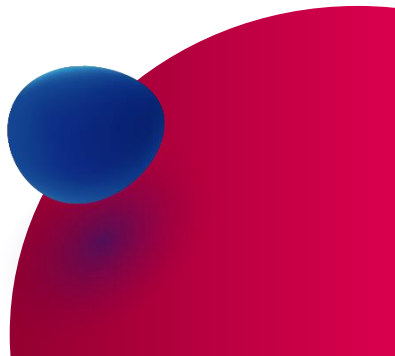


# Confidencialidad:

---

ISO 27000, cláusula 2.13

- La propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizado



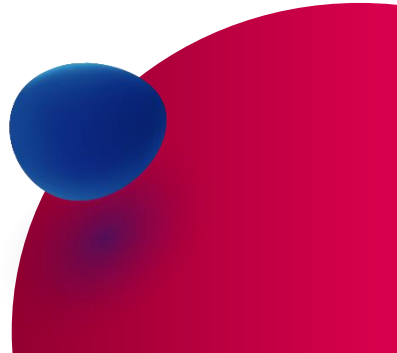


# Integridad

---

ISO 27000, cláusula 2.36

- La propiedad de proteger la exactitud y completitud de los activos



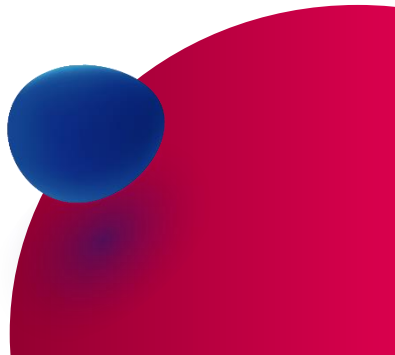


# Disponibilidad

---

ISO 27000, cláusula 2.10

- La propiedad de ser accesible y utilizable por una entidad autorizada



# Vulnerabilidad

---

ISO 27000, cláusula 2.81

La debilidad de un activo o de un control que puede ser explotada por una o mas amenazas



# Tipos de Vulnerabilidades



ISO 27005, Anexo D

Tipo de vulnerabilidad	Ejemplos
1 Hardware	Mantenimiento insuficiente
	Portabilidad
2 Software	No hay registros de inscripción
	Interfaces complicadas
3 Red	Falta de encriptación en las transferencias
	Unico punto de acceso
4 Personal	Formación insuficiente
	Falta de supervisión
5 Sitio	Sistema eléctrico inestable
	Sitio en un área susceptible a inundaciones
6 Estructura de la organización	Falta de separación de funciones
	No hay descripciones de puestos



# Amenazas

---



ISO 27000, cláusula 2.77

Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización





# Tipos de Amenazas



ISO 27005, Anexo C

Tipo de vulnerabilidad	Ejemplos
1 Daño físico	Fuego
	Daño por agua
2 Desastre Natural	Terremoto
	Inundación
3 Pérdida de servicios esenciales	Falta de aire acondicionado
	Corte de suministro eléctrico
4 Trastornos causados por la radiación	Radiación electromagnética
	Radiación térmica
5 Información comprometida	Escuchas telefónica
	Robo de documentos
6 Fallas técnicas	Falla del equipo
	Sobrecarga de la red

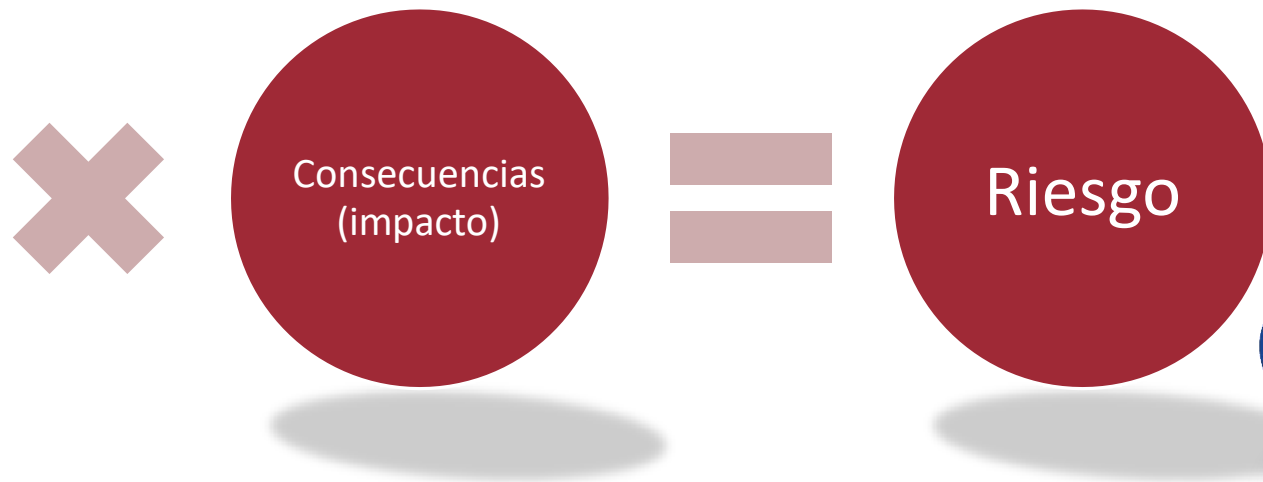
# Riesgo para la Seguridad de la Información



ISO 27000. cláusula 2,61

Potencialidad de que una amenaza explote una vulnerabilidad en un activo o grupo de activos y por lo tanto causará daño a la organización

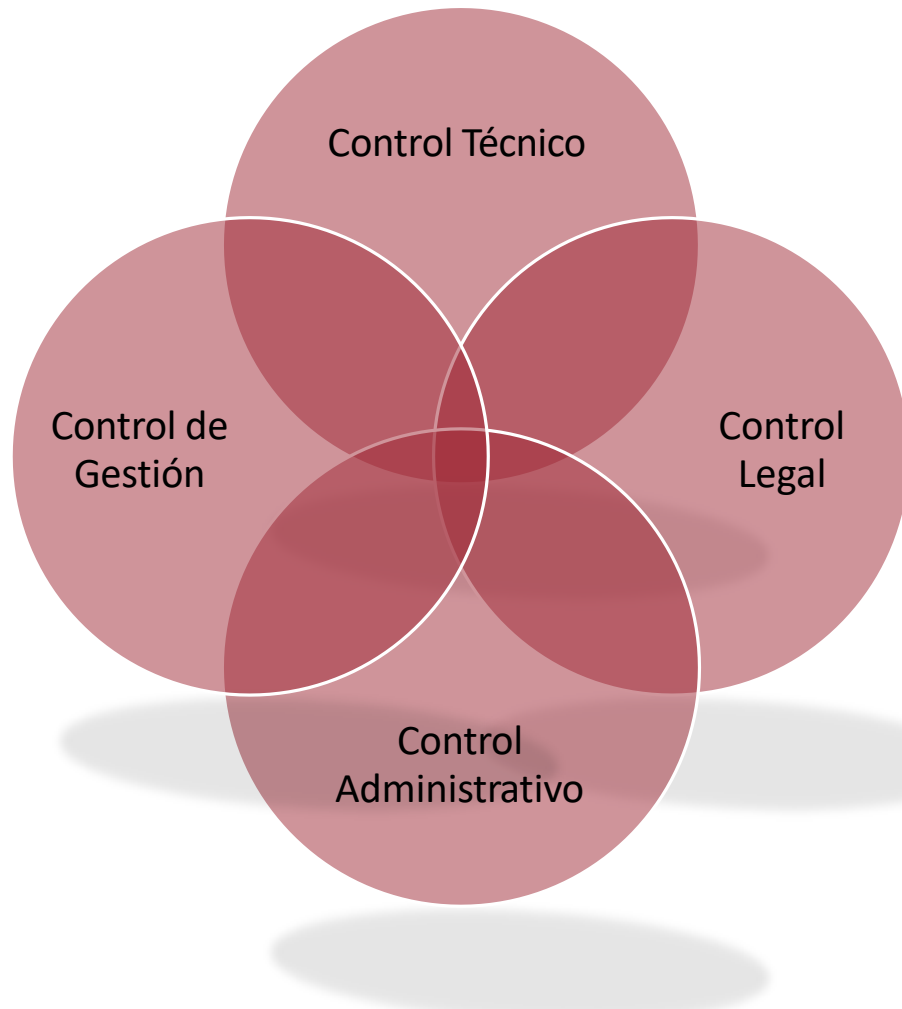
**Nota:** se mide en términos de una combinación de la probabilidad de un evento y sus consecuencias





# Objetivo de Control y Control

ISO 27000. cláusula 2.16-17



## Objetivo de Control

Declaración de describir lo que se quiere lograr como resultado de los controles de aplicación

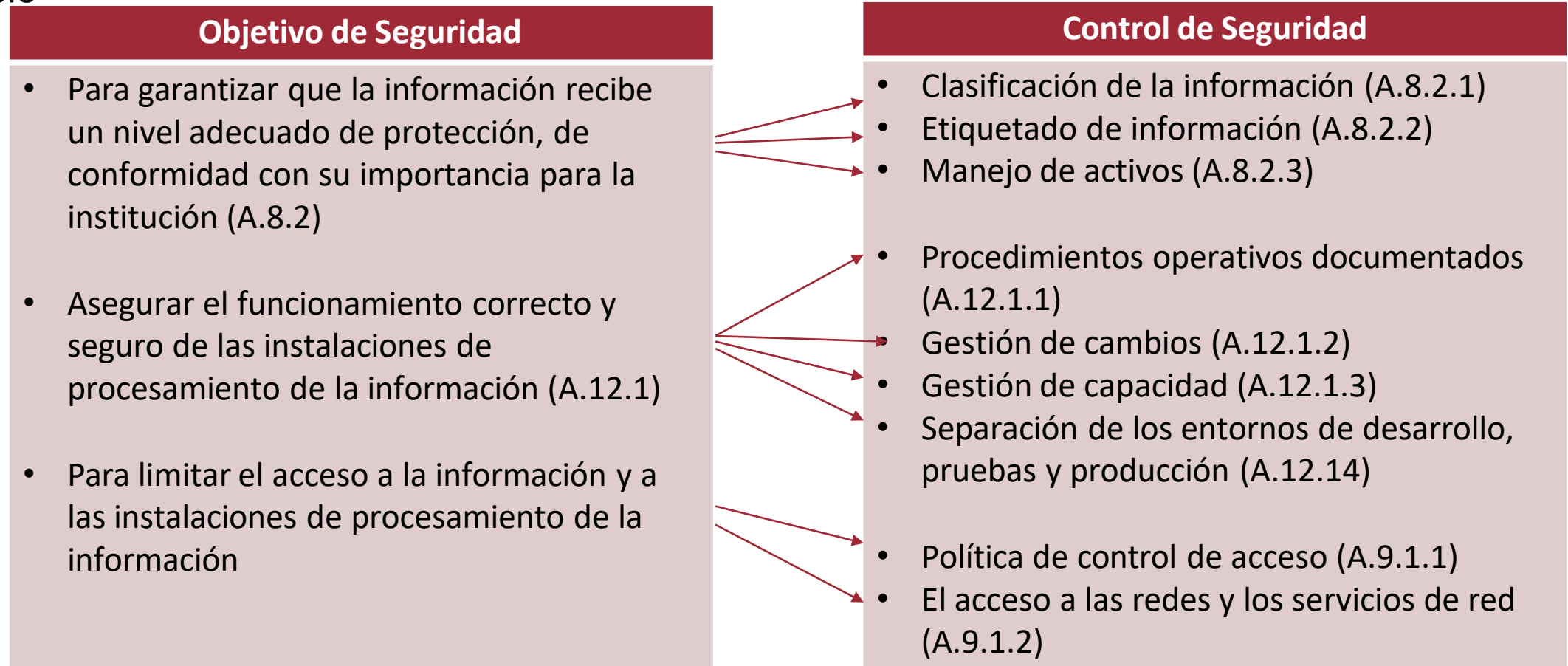
## Control

- Métodos para gestionar el riesgo
- Incluye las políticas, procedimientos, directrices y prácticas o estructuras organizativas
- Sinónimo: medida, contra medida, dispositivo de seguridad

# Relación entre los Objetivos y los Controles de Seguridad



Ejemplo





# Controles



## Clasificación



### Control Preventivo

Desalentar o prevenir la aparición de problemas

### Control de detección

- Buscar, detectar e investigar problemas

### Control Correctivo

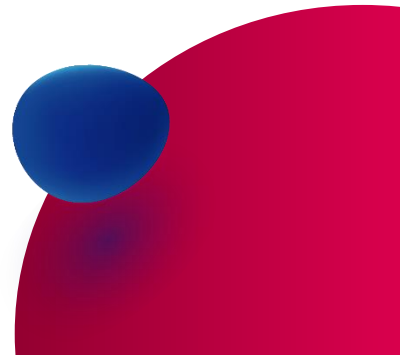
- Resolver problemas encontrados y prevenir la recurrencia



# Clasificación de controles de seguridad

## Ejemplos

Controles Preventivos	Controles Investigativos	Controles Correctivos
<ul style="list-style-type: none"><li>• Publicar una política de seguridad de la información</li><li>• Hacer firmar un acuerdo de confidencialidad</li><li>• Contratar solo personal calificado</li><li>• Identificar los riesgos procedentes de terceros</li><li>• Segregación de tareas</li></ul>	<ul style="list-style-type: none"><li>• Supervisar y revisar servicios de terceros</li><li>• Supervisar los recursos usados por sistemas<ul style="list-style-type: none"><li>• Activación de la alarma al detectar por ejemplo, fuego</li></ul></li><li>• Revisión de los derechos de acceso de los usuarios</li><li>• Análisis de los registros de auditoría</li></ul>	<ul style="list-style-type: none"><li>• Investigación técnica y jurídica (análisis) tras un incidente de seguridad</li><li>• Habilitar el plan de continuidad del negocio después de la ocurrencia de un desastre</li><li>• Aplicación de parches tras la identificación de vulnerabilidades técnicas</li></ul>







**FIN DE  
GRABACIÓN**