

ISO 27000

Presentan:

Godinez Roblero Diana y Noé
Zúñiga Morales

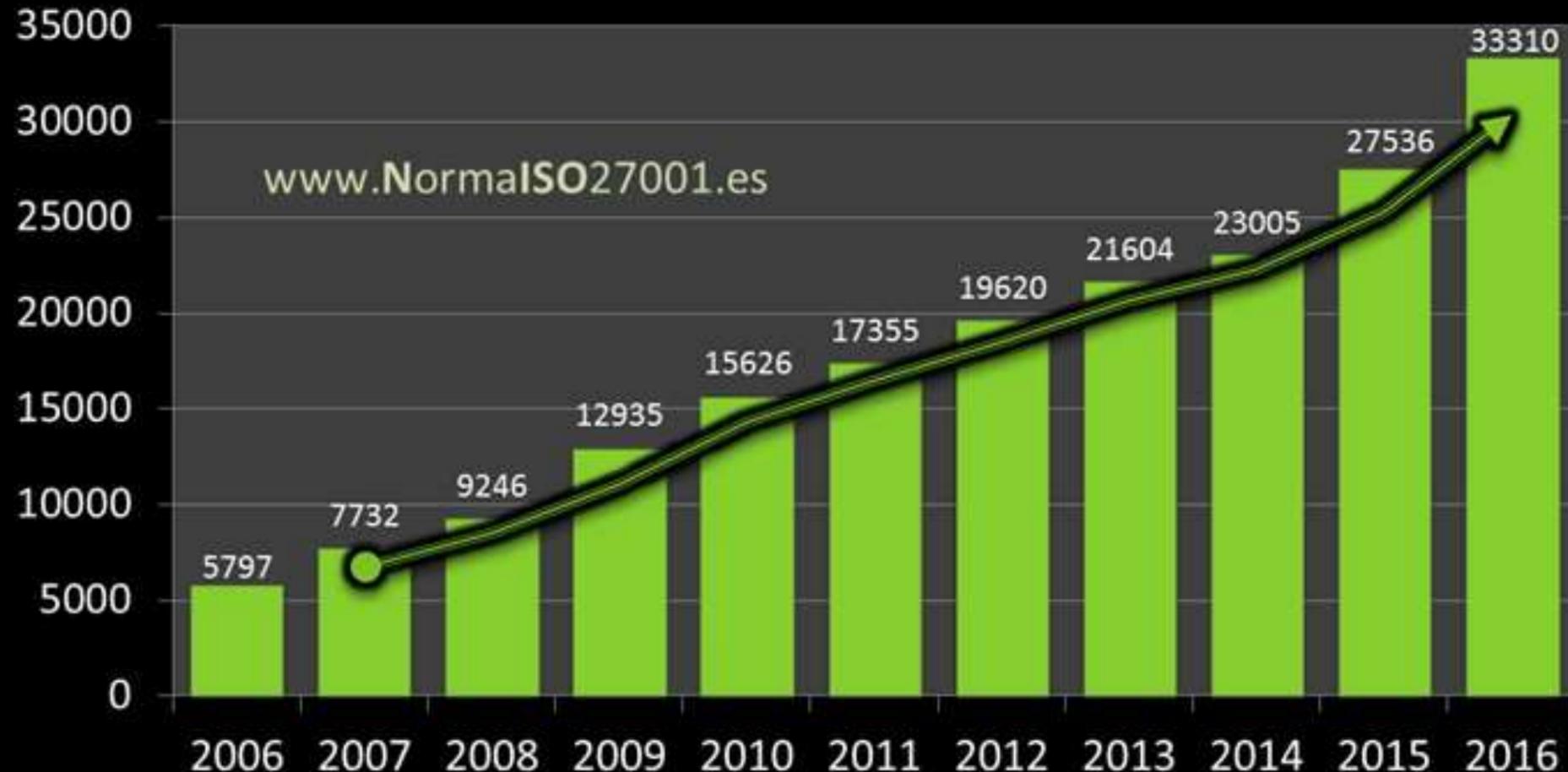
Propósito

Ayudar a la seguridad de la información
en una empresa

Norma a nivel mundial que hace referencia a la seguridad de la información en las organizaciones

ISO 27001

Certificados ISO 27001 en el mundo



www.NormalISO27001.es

SGSI según ISO 27001:2013

“Un Sistema de Gestión para la Seguridad de la Información se compone de una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información tomada como base los riesgos que afectan a la seguridad de la información en una empresa u organización”

¿Por qué implementar SGSI?

Mejora continua

- Desarrolla cultura de seguridad en la empresa

Ajustable a las necesidades

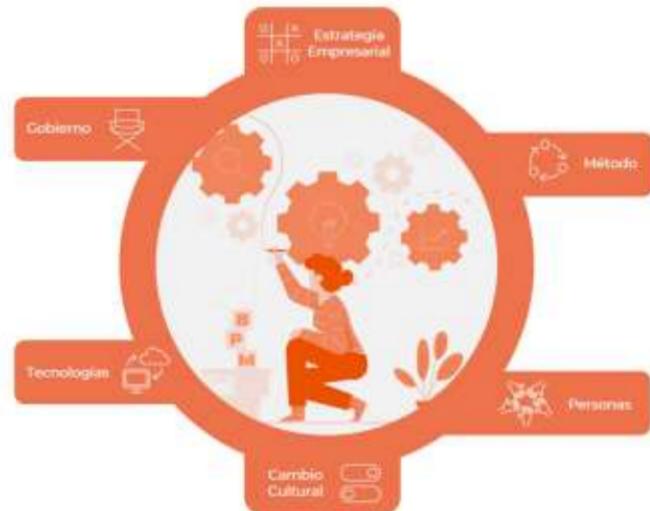
- Promueve el establecimiento de procesos de análisis de riesgo

Establece controles para la seguridad de la información

- Determinados por análisis científicos que permiten evaluar como las amenazas y los riesgos de seguridad informática afectan las necesidades de la empresa

Tipos de procesos

Procesos de Gestión

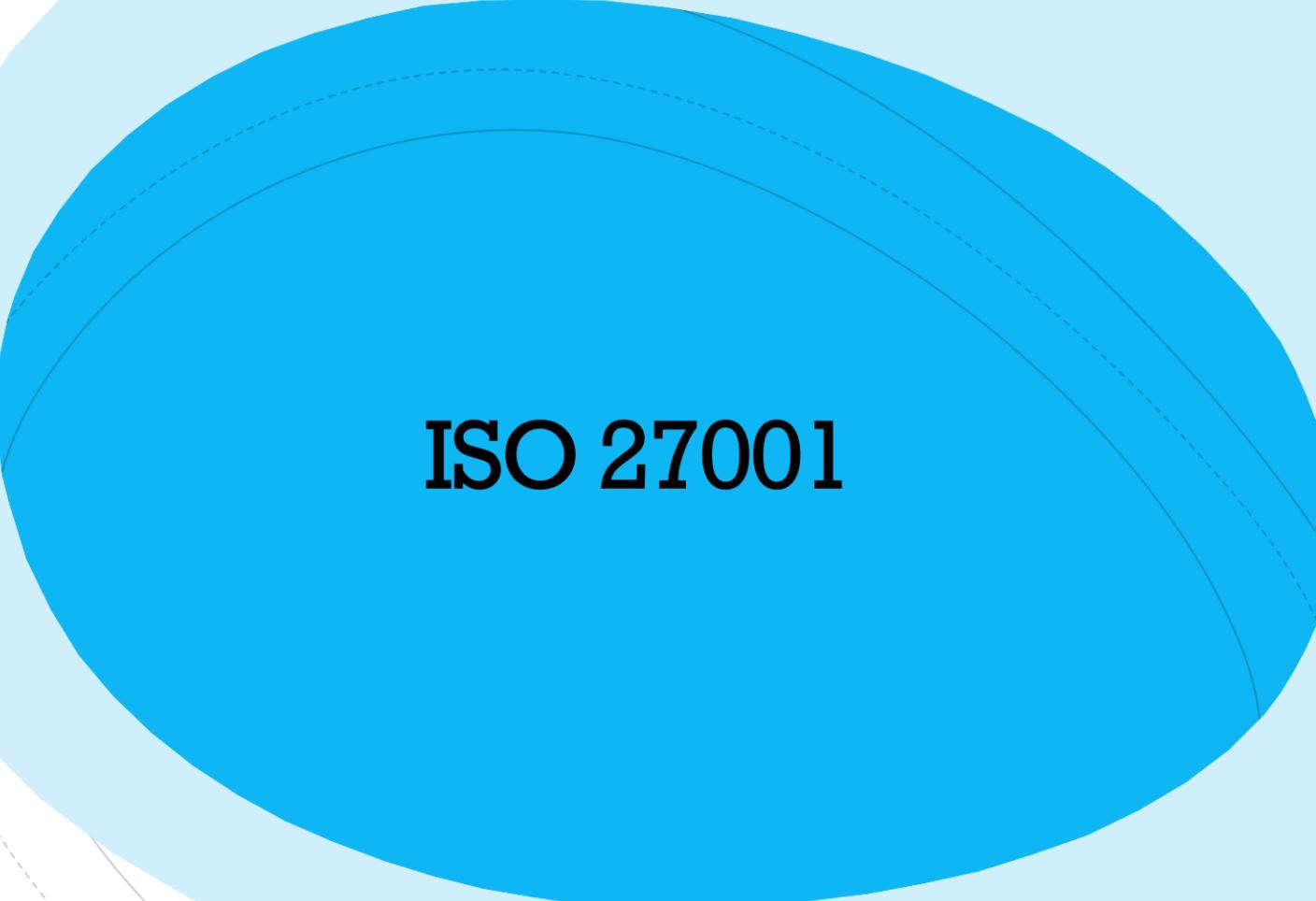


Procesos sobre la seguridad de la información



Estructuras Normativa ISO 27001

- ISO 27001 Requisitos para un sistema de Gestión (SGSI). Norma certificable que contiene los requisitos a implementar en un sistema de seguridad de la información
- ISO 27002 Guía de buenas prácticas para la implementación de un SGSI. Guía que proporciona controles o instrumentos de control pensados y diseñados específicamente para abordar problemas o peligros para seguridad de la información



ISO 27001

Flexibilidad. Las organizaciones encuentran la mejor forma de cumplir las normas que se adaptan a su necesidad

¿Qué es la norma ISO 27001?



Revisión de la norma ISO 27001:2013 introduce:

- Mayor énfasis en la gestión de riesgos
- Flexibiliza la elección de metodologías de análisis de riesgos
- Nuevo enfoque en la Selección de Controles d Seguridad

Revisión de la norma ISO 27001:2017

- Activos de información





ISO 27001

1. Objeto y campo de aplicación, definiendo el alcance del SGSI

- Aplicable a empresas de todos los tamaños
- Aplicar esta norma otorga mayores beneficios respecto a herramientas de gestión

2. Referencias normativas

- Ofrece visión genérica sobre los sistemas de SGSI, sobre metodología PDCA de todos los sistemas de Gestión
- Referencia normativa ISO/IEC 27000:2018 que aporta perspectivas generales de los SGSI

La recopilación de información en una auditoría

Entrevistas

Observación de
actividades

Revisión de
documentos

Recursos de información

Recopilación a través de un
muestreo apropiado y verificación

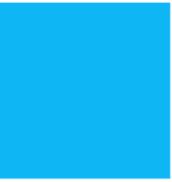
Evaluación contra criterios de
auditoría

Revisión

Conclusiones de la auditoría

Evidencia de auditoría

Hallazgos de auditoría



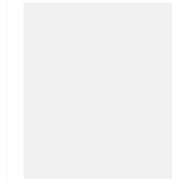
Auditoría

- Descripción de áreas físicas, unidades organizacionales, actividades y procesos



Autenticación

- Integridad, disponibilidad y confidencialidad



Autenticidad

- Pruebas de identidad. Entradas de ID de usuarios y contraseñas

Conformidad

Cumplimiento de requisitos

- **No conformidad menor.** Conformidad que no afecte la seguridad de la información, rendimiento, durabilidad, usos u operaciones efectivas o seguridad del producto
- **No conformidad mayor.** Conformidad no critica, que de lugar a fallas o reducir sustancialmente la seguridad de la información
- **No conformidad crítica.** No conformidad sobre la seguridad de la información que cause daño a las personas, su imagen o reputación

Objetivos de seguridad

Protección de intereses

- Disponibilidad de sistemas informáticos, utilizables cuando sean necesarios
- Confidencialidad de datos e información revelados
- Integridad de datos e información protegidos contra modificaciones no autorizadas

Preventivos	Detección	Correctivos	Compensación
Concienciación en la Seguridad	Sistemas de monitoreo de red	Actualización de Sistema Operativo	Copias de seguridad
Firewalls	IDS	Restaurar copias de respaldo	Servidor de respaldo en caliente
Anti virus	Anti virus	Anti virus	Aislamiento del servidor
Control de accesos	Detectores de Humos / Presencia	Mitigación de la vulnerabilidad	
IPS	IPS		

*Controles Preventivos Detección Correctivos
Compensación*

Objetivo de control

- Planificación de sistemas
- Implantación de sistemas estables
- Monitorización de sistemas, realizando mediciones reales de desempeño de objetivos
- Evaluación de desempeño, evaluando el cumplimiento de objetivos y estableciendo medidas de mejora

Liderazgo

Compromisos que debe ejercer la empresa en procesos de implantación de SGSI

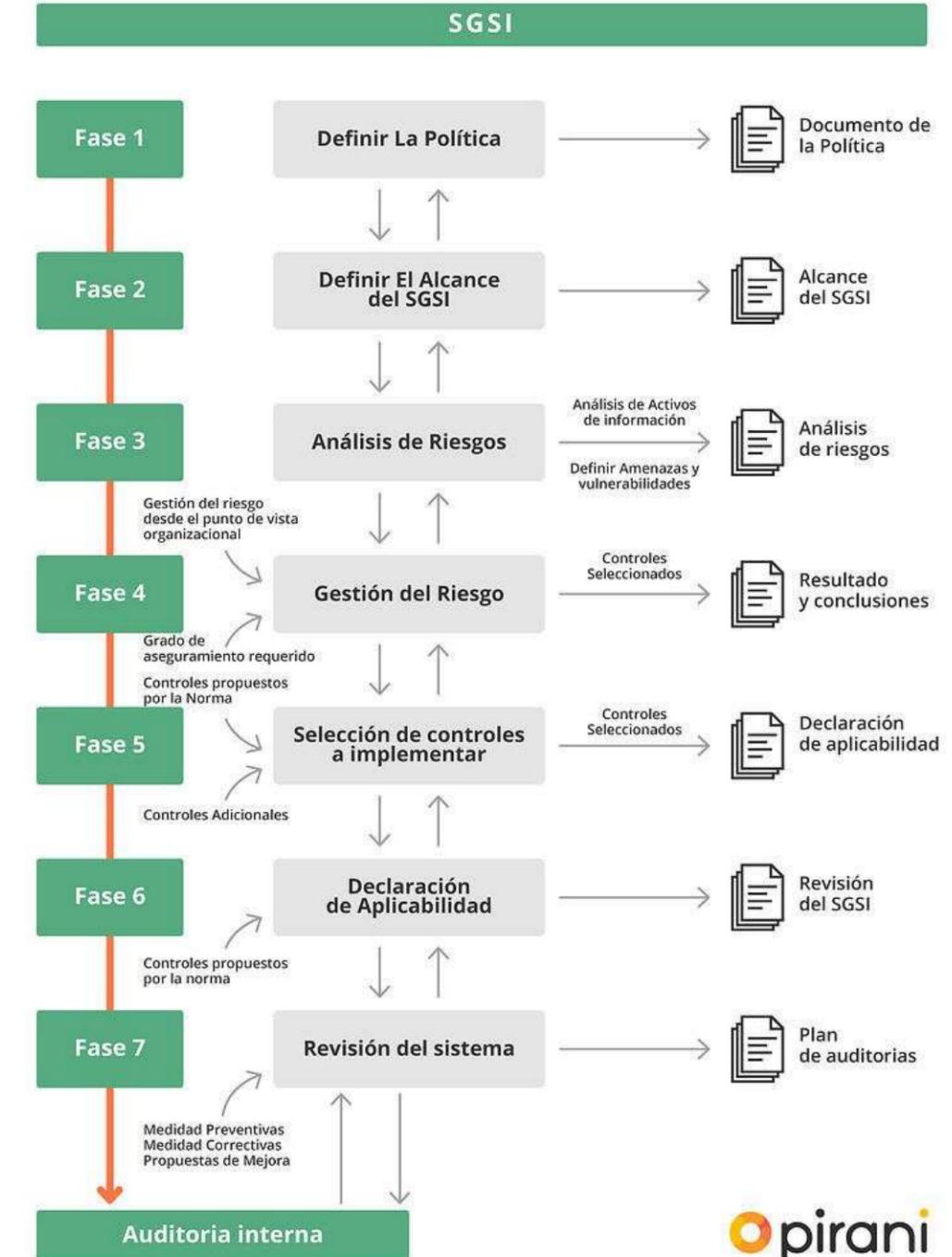
- Elaborar políticas de seguridad y establecer objetivos de la seguridad informática
- Comunicar los objetivos a la organización, definiendo las áreas de responsabilidad y roles correspondientes a seguridad informática

Planificación

Identificar las necesidades y expectativas que establezcan un plan de riesgos y actividades a realizar.

- Identificar las necesidades y expectativas de las partes interesadas
- Análisis de riesgos y oportunidades
- Evaluación de riesgos
- Plan de tratamiento de riesgos

Pasos para implementar ISO 27001

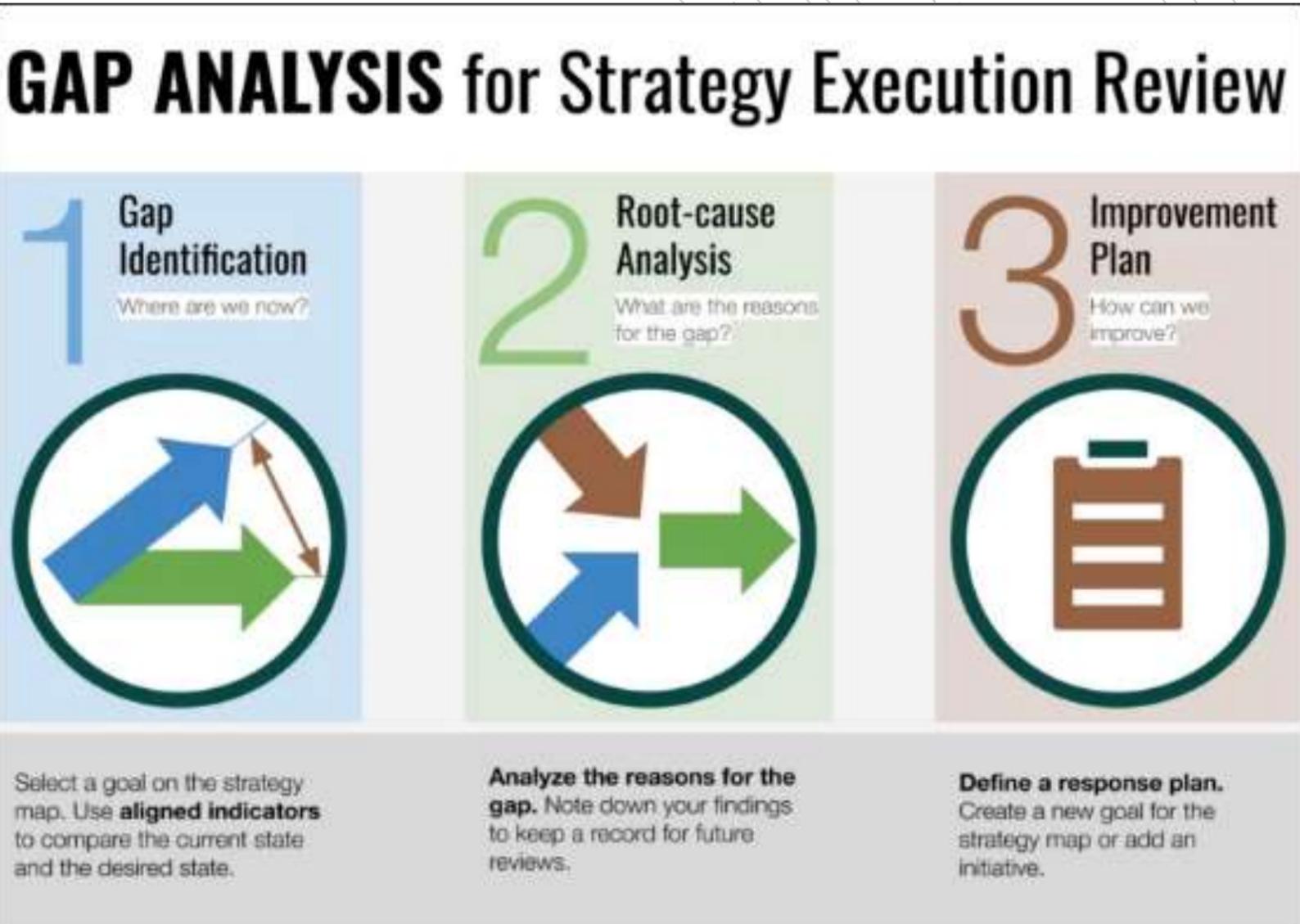


¿Para qué sirve un SGSI?



Fase 1. Auditoria inicial ISO 27001 GAP ANALYSIS

- Análisis de cumplimiento de los requisitos de la norma ISO 27001 y sus controles



Fase 2. Análisis del contexto de la organización y determinación del alcance

Establece el contexto del SGSI en cumplimiento de los requisitos de la clausula 4 de ISO 27001, contexto de la organización

1. Comprende la organización y su contexto
2. Comprender las necesidades y expectativas de las partes interesadas
3. Determinación del Alcance del sistema de Gestión

Contexto de la organización



Fase 3. Elaboración de la política. Objetivos del SGSI

Elaboración de políticas

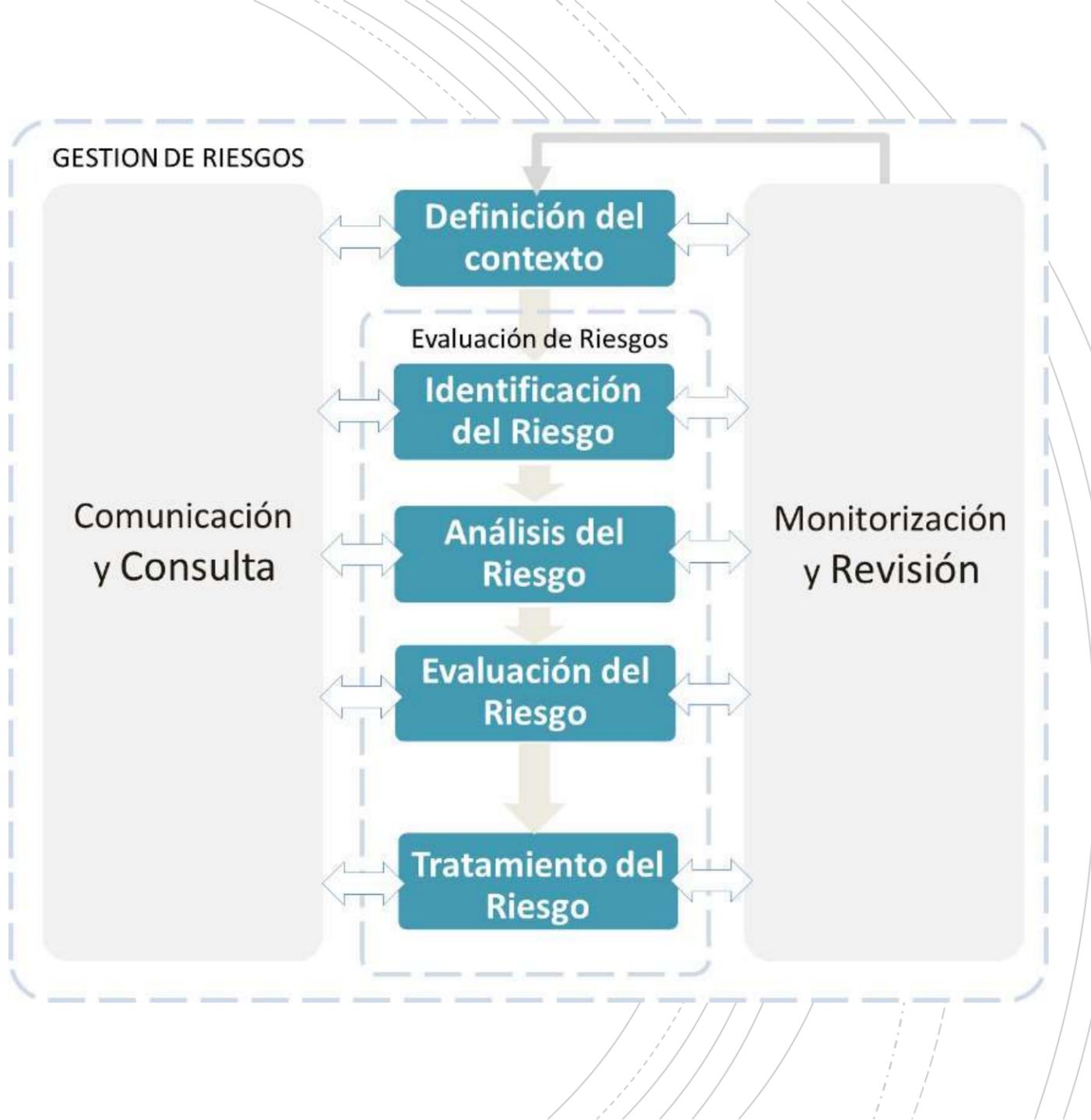
1. Redactar políticas de acuerdo a las necesidades de cada organización. Se considera el tamaño, la estructura y las actividades de la organización.
2. La política de la seguridad de la información debe tener en cuenta el objetivo de cada organización. Los objetivos se ven desde dos perspectivas: objetivos comerciales y objetivos de seguridad de la información
3. La política del SGSI debe demostrar que se tiene en cuenta los requisitos de las partes interesadas.
4. Comunicación de políticas a las partes interesadas
5. Propiedad de la política

Objetivos de seguridad del SGSI

1. Protección de activos de información
2. Autenticación
3. Autorización
4. Integridad de la información
 - Integridad de datos
 - Integridad del sistema
 - Irrenunciabilidad de transacción (No repudio)
 - Confidencialidad
5. Autoría de actividades de seguridad

Fase 4. Planificación del SGSI

- Inventario de activos
- Catalogo de amenazas
- Valoración de las amenazas para la seguridad de la información
- Análisis de riesgos
- Evaluación de riesgos
- Plan de tratamiento de riesgos
- Selección de controles: Declaraciones de aplicabilidad

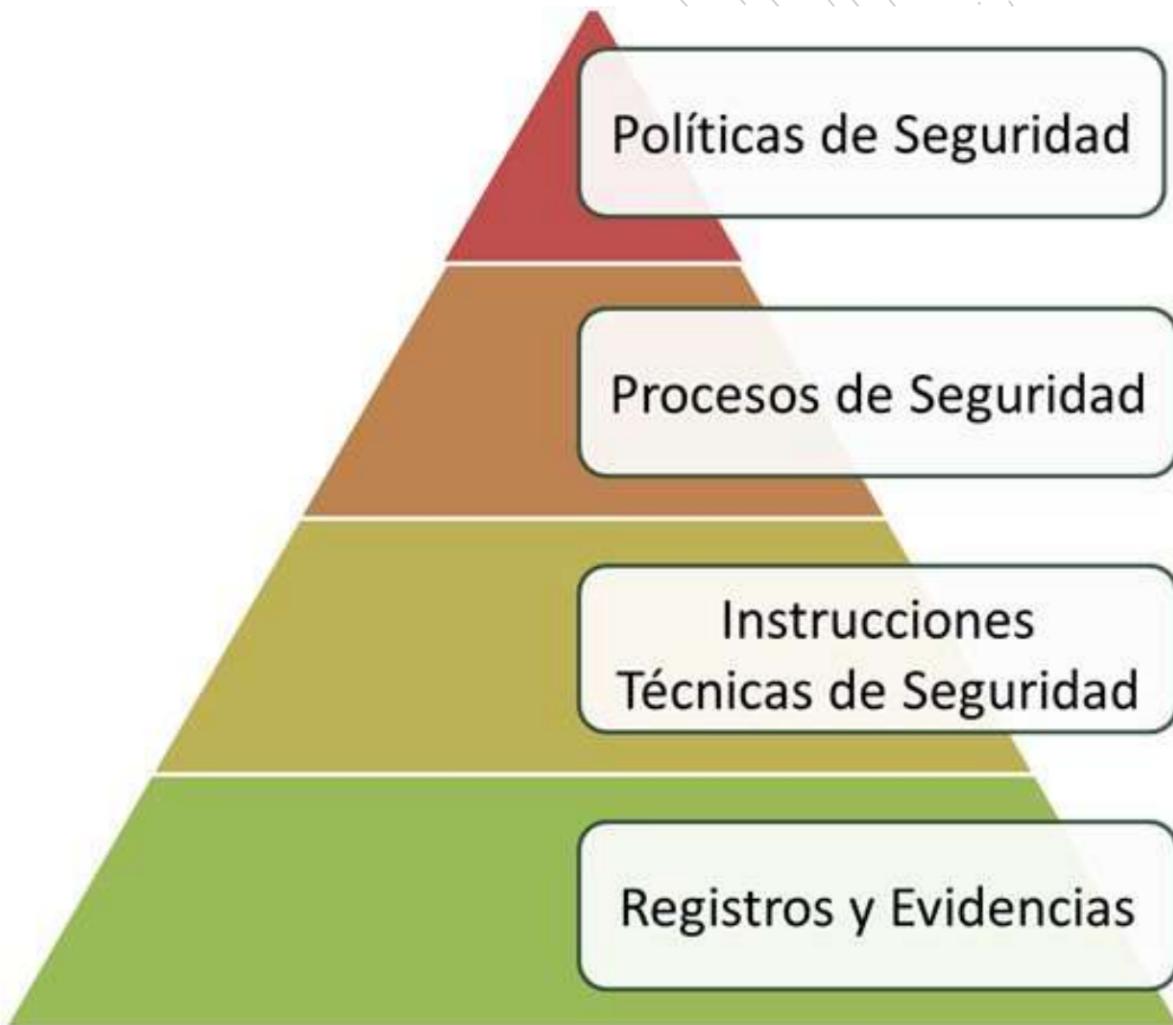


Fase 5. Documentación del SGSI

Importancia de documentar

- Garantiza la repetición en el tiempo de proceso
- Establece procesos de mejora

La documentación del SGSI se puede estructurar en:



Fase 6. Implementando un SGSI



Fase 7. Comunicación y sensibilización SGSI

¿Cómo documentar el plan de comunicación del SGSI?

- Análisis de objetivos y de la complejidad de la organización
- **Nivel 1.** Estructura de la organización en la cultura de la seguridad informática
- **Nivel 2.** Los valores de una organización y la seguridad de la información

Creación de cultura de seguridad informática en las organizaciones

- Toma de conciencia
- Punto de partida

CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN



*Comunicacion de valores y cultura de la Seguridad
de la Información*

Fase 8. Auditoria interna según ISO 27001

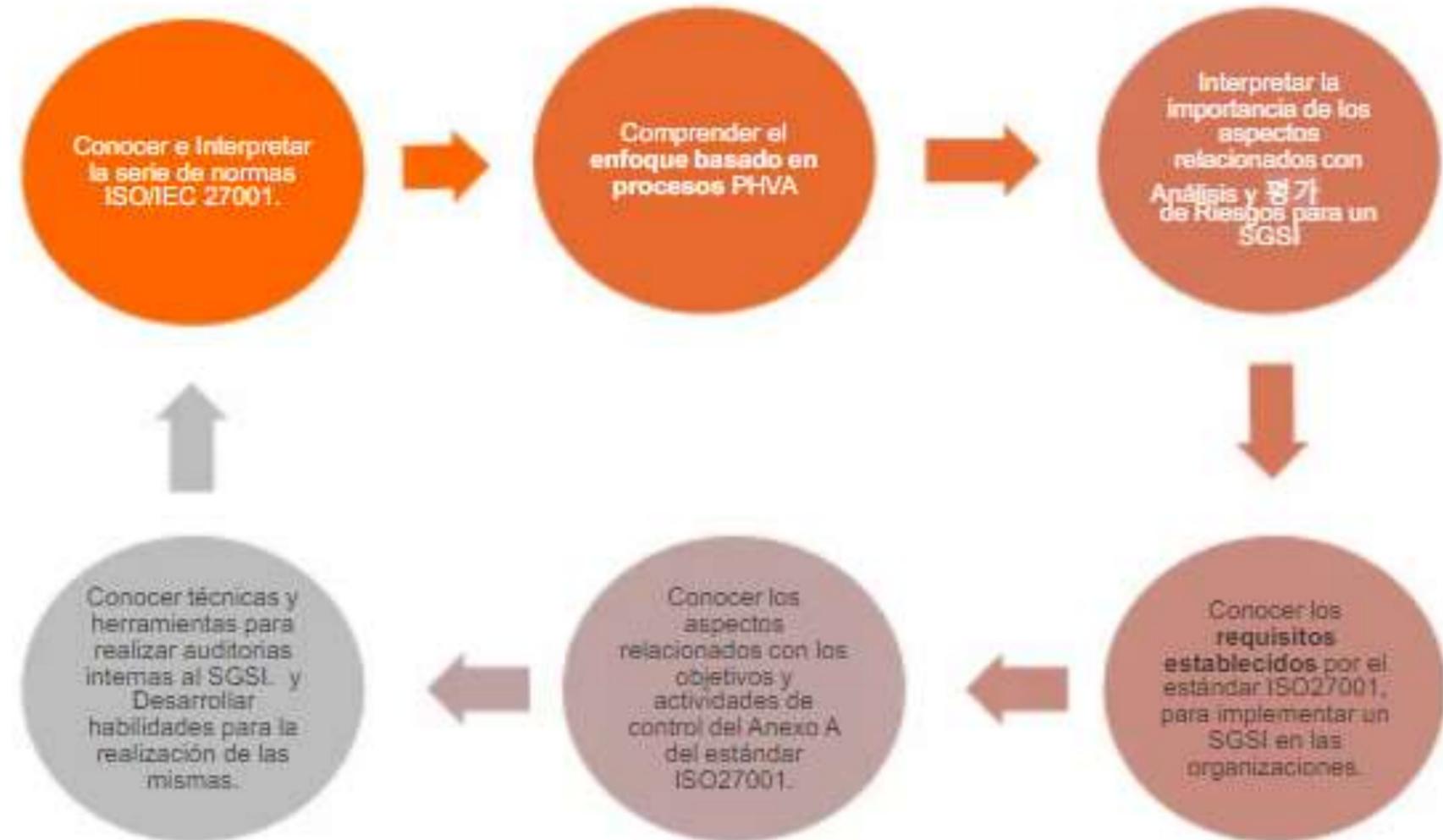
¿Cómo elegir un auditor interno?

- Antes de elegir un auditor debe definirse primero que debe desarrollar el auditor
- Conocer y preparar la certificación

Beneficios de una auditoria interna

- Sirve como recordatorio de la importancia y prioridad del cumplimiento de los requisitos sobre la seguridad de la información

OBJETIVOS



Fase 9. Revisión por la dirección según ISO 27001

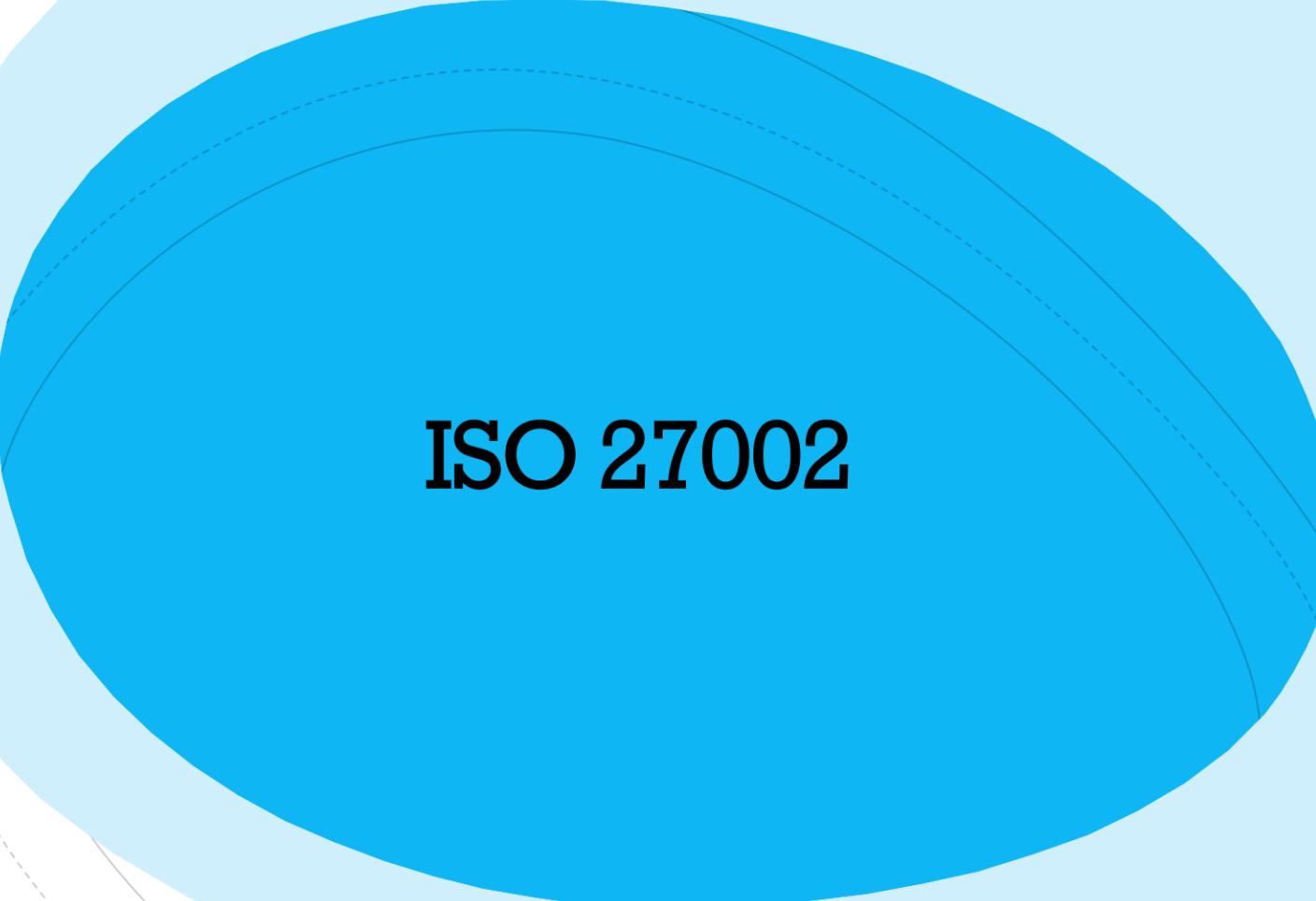
- Las revisiones por parte de la dirección de las organizaciones debe considerarse dentro de los proceso de mejora continua

Ciclo PDCA en ISO/IEC 27001:2013

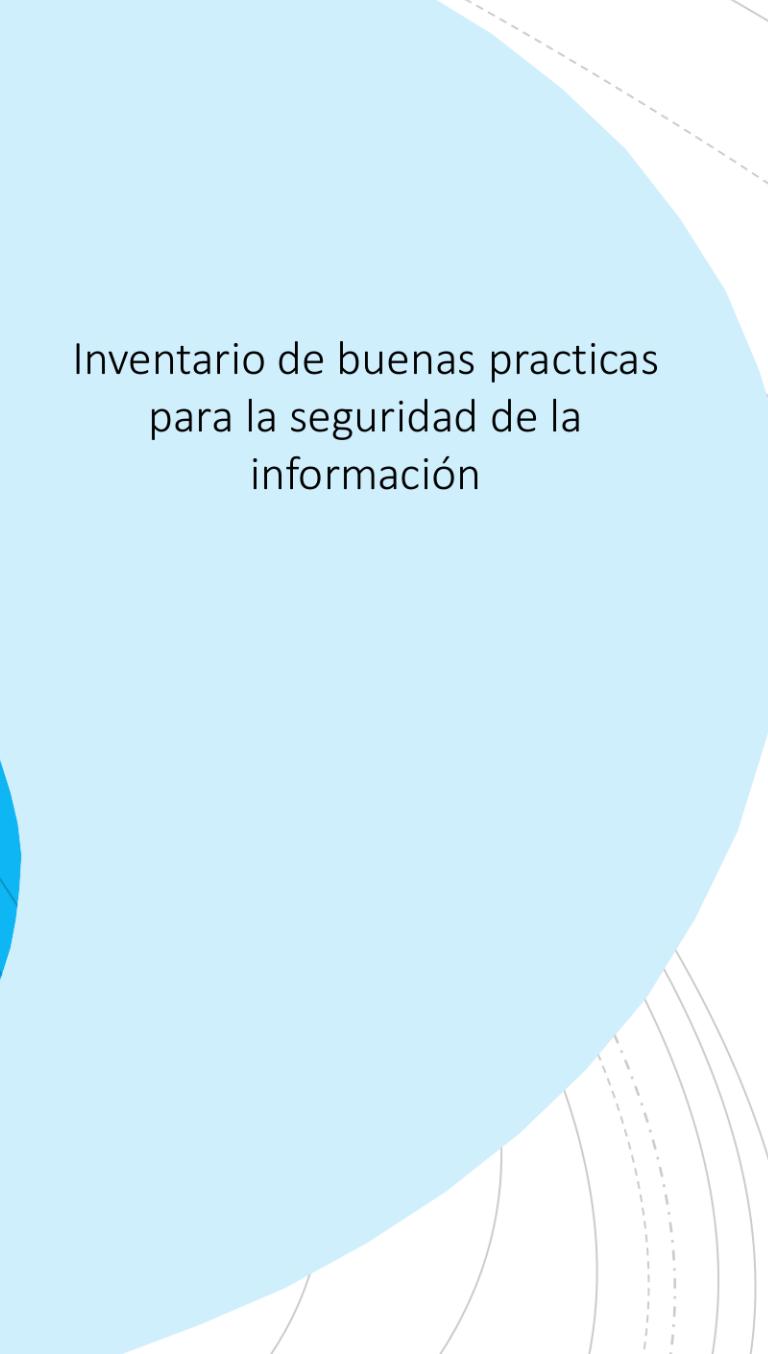


Fase 10. Proceso de certificación ISO 27001

- Auditoria de certificación ISO 27001 Fase 1. Análisis de la documentación
- Auditoria de certificación ISO 27001 Fase 2. Se revisa la implementación del SGSI
 - Evidencia
 - Entrevistas
 - Concienciación
 - Auditoria interna
 - Sección de un auditor
 - Revisión del plan de auditoría
 - Preparación para la entrevista



ISO 27002



Inventario de buenas prácticas
para la seguridad de la
información

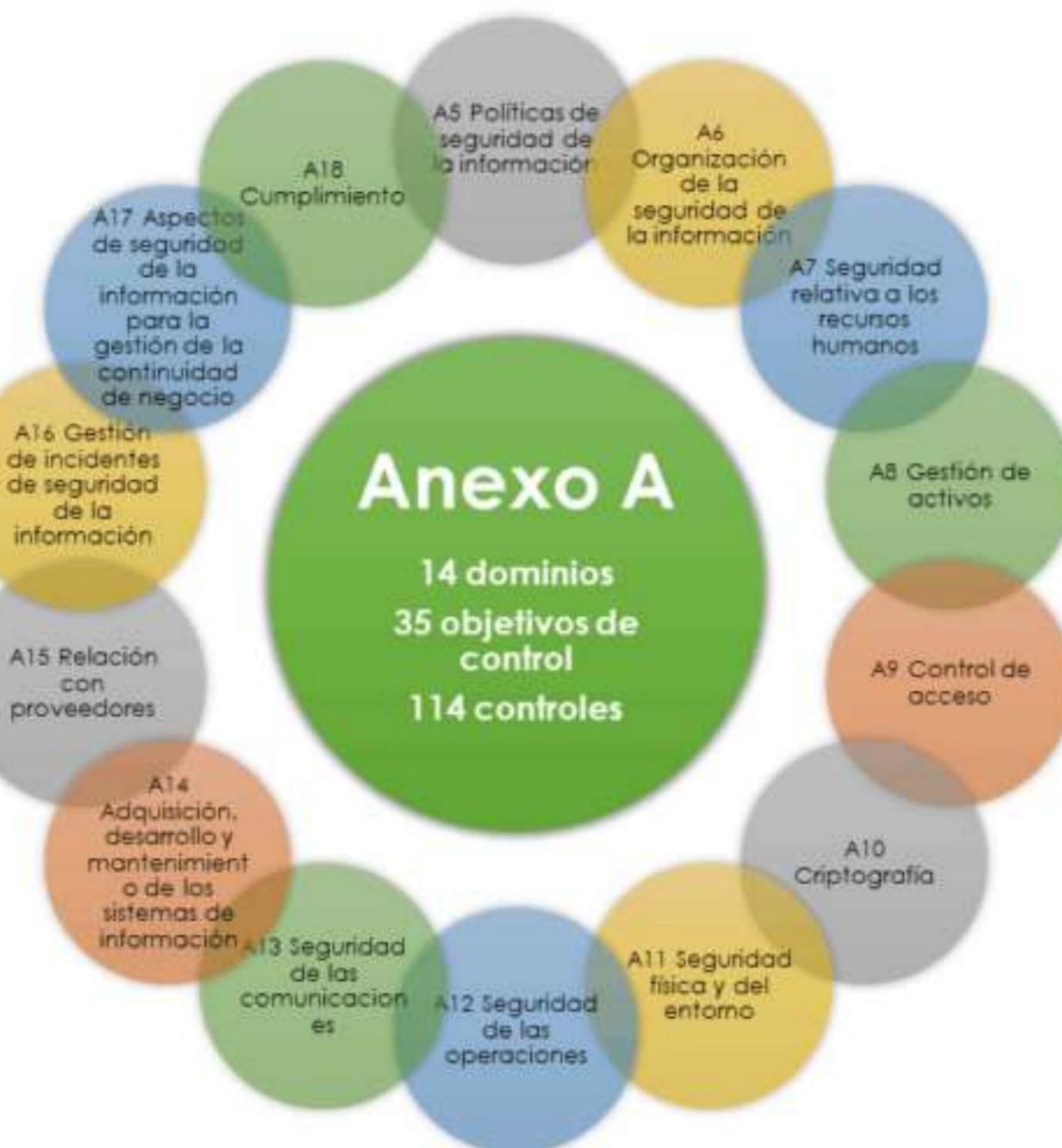


Los controles se consideran categorías, o bien, pueden localizarse dentro de los objetivos

Estructura de la ISO 27002

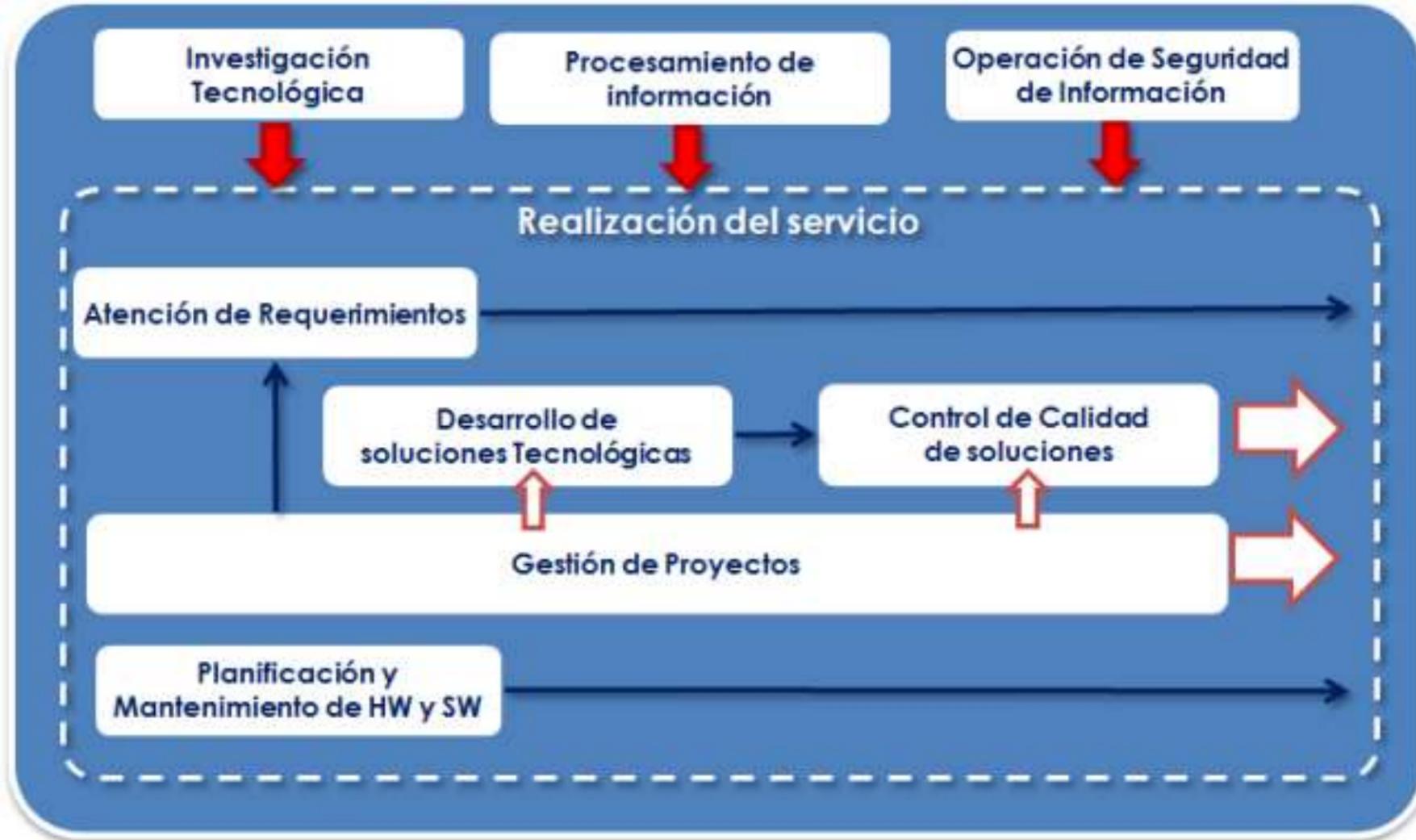
Anexo A

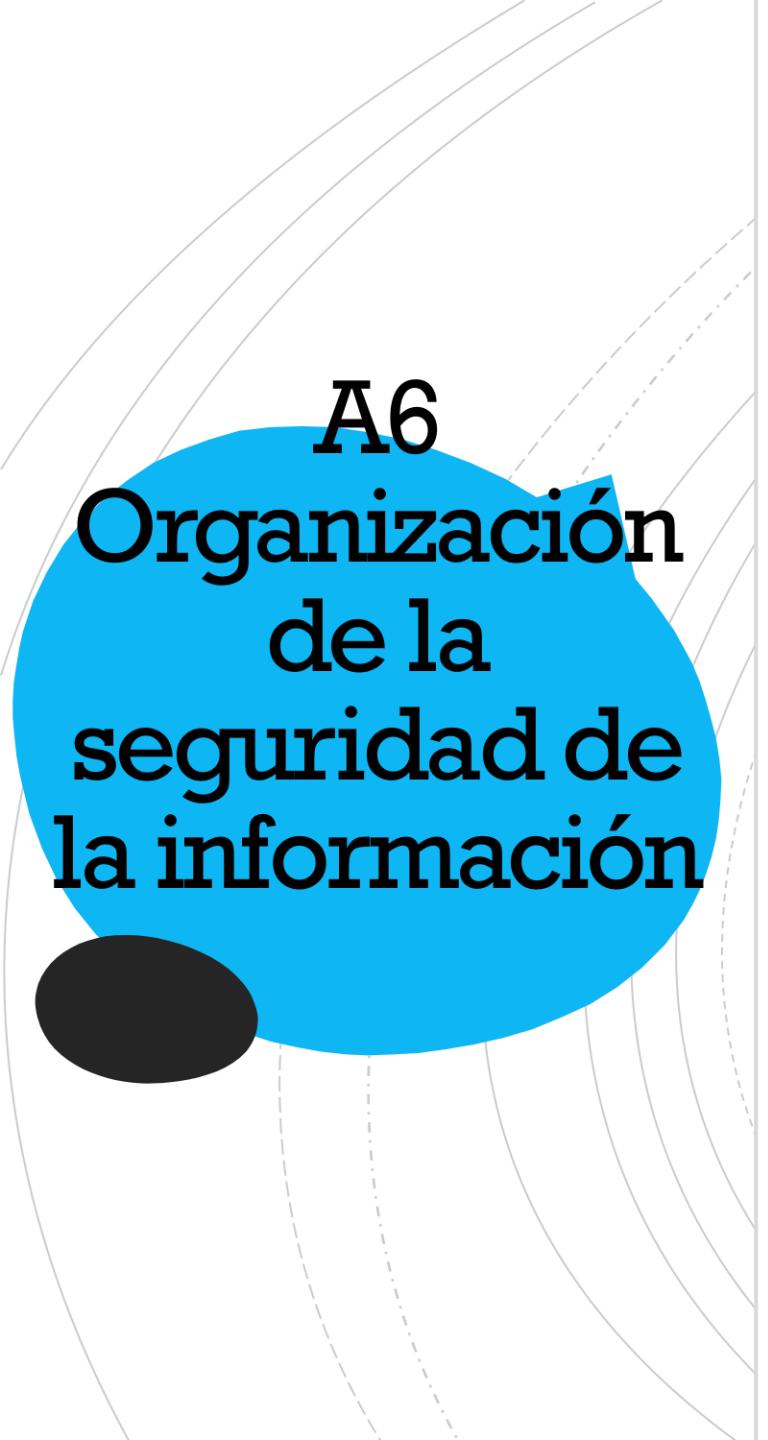
**14 dominios
35 objetivos de control
114 controles**



A5 Políticas de seguridad de la información

Mapa de proceso tecnológicos incluidos en el SGSI





A6

Organización de la seguridad de la información

Objetivos

- 6.1 Organización interna. Establecer marco de gestión que inicie y controle la implementación y las operaciones de seguridad de la información dentro de la organización
 - 6.1.1 Funciones y responsabilidades de la seguridad de la información
 - 6.1.2 Separación de funciones
 - 6.1.3 Contacto con autoridades
 - 6.1.4 Contacto con grupos de interés especial
 - 6.1.5 Seguridad de la información en la gestión de proyectos
- 6.2 Dispositivos móviles y teletrabajo. Garantiza la seguridad del teletrabajo y el uso de dispositivos móviles
 - 6.2.1 Política de dispositivos móviles
 - 6.2.2 Teletrabajo



A7 Seguridad relativa a los recursos

Nivel	Órgano/Departamento	Aportación/Implicación	Miembros
Estratégico	Comité de Dirección	Visión estratégica Aportación de recursos	<ul style="list-style-type: none">• CEO.• Director Financiero.• Director Servicios de Reciclaje de Acero.• Director Servicios de Reciclaje de Aluminio.• Director Tecnologías de la Información.
	Comité de Seguridad de la Información	Liderazgo Gestión del riesgo Comunicación	<ul style="list-style-type: none">• CEO.• Director Financiero.• Director Servicios de Reciclaje de Acero.• Director Servicios de Reciclaje de Aluminio.• Director Tecnologías de la Información.• Responsable de Seguridad.• Posibles invitados según temática.
Táctico	Responsable de Seguridad de la Información	Coordinación y Gestión Lenguaje común	<ul style="list-style-type: none">• Responsable de Seguridad.
	Departamento de Tecnologías de la Información	Implanta en los SI los controles de seguridad	<ul style="list-style-type: none">• Director de Tecnologías de la Información.• Service Managers.• Proveedores de servicio de TI.
Operativo	Recursos Humanos	Informa sobre los cambios de personal y aplica procedimientos disciplinarios	<ul style="list-style-type: none">• Personal del departamento de Recursos Humanos.
	Legal	Colabora en definición de normas y políticas	<ul style="list-style-type: none">• Personal del departamento de Legal.
	Personal general	Confidencialidad y uso adecuado de los recursos	<ul style="list-style-type: none">• Personal de la organización• Personal de proveedores de servicios con acceso a información de la organización



A8 Gestión de activos

Objetivos

1. Responsabilidad de los activos. Identificar activos y definir las protecciones adecuadas
2. Clasificación de la información. Asegura que la información reciba los niveles de protección adecuados de acuerdo a su nivel de importancia dentro de la organización
3. Manejo de los soportes

Estrategia de Gestión y Planificación de Activos

- Política de gestión de activos
- Estrategia de gestión de activos
- Análisis de la demanda
- Planificación Estratégica
- Planes de gestión de activos

Planificación de la Gestión de Activos "Toma de decisiones"

- Toma de decisiones para inversión de capital
- Tomas de decisiones en Operaciones y Mantenimiento
- Costo del ciclo de vida y optimización de Valor
- Estrategia y Optimización de recursos
- Estrategia y Optimización de Paradas
- Estrategias de sustitución de Activo

Actividades del Ciclo de Vida

- Normas Técnicas y Legislación
- Creación de activos y adquisición
- Ingeniería de Sistemas
- Gestión de activos
- Entrega del Mantenimiento
- Ingeniería de Confiabilidad y Análisis de Causa Raíz
- Operaciones de Activos
- Gestión de Recursos
- Gestión de Paradas & Overhaul
- Respuesta a Incidentes
- Racionalización y eliminación de activos

Conocimiento de Activos

- Estrategia de información de activos
- Estándares de Conocimiento de activos
- Sistemas de Información de Activos
- Los datos de activos y de conocimiento

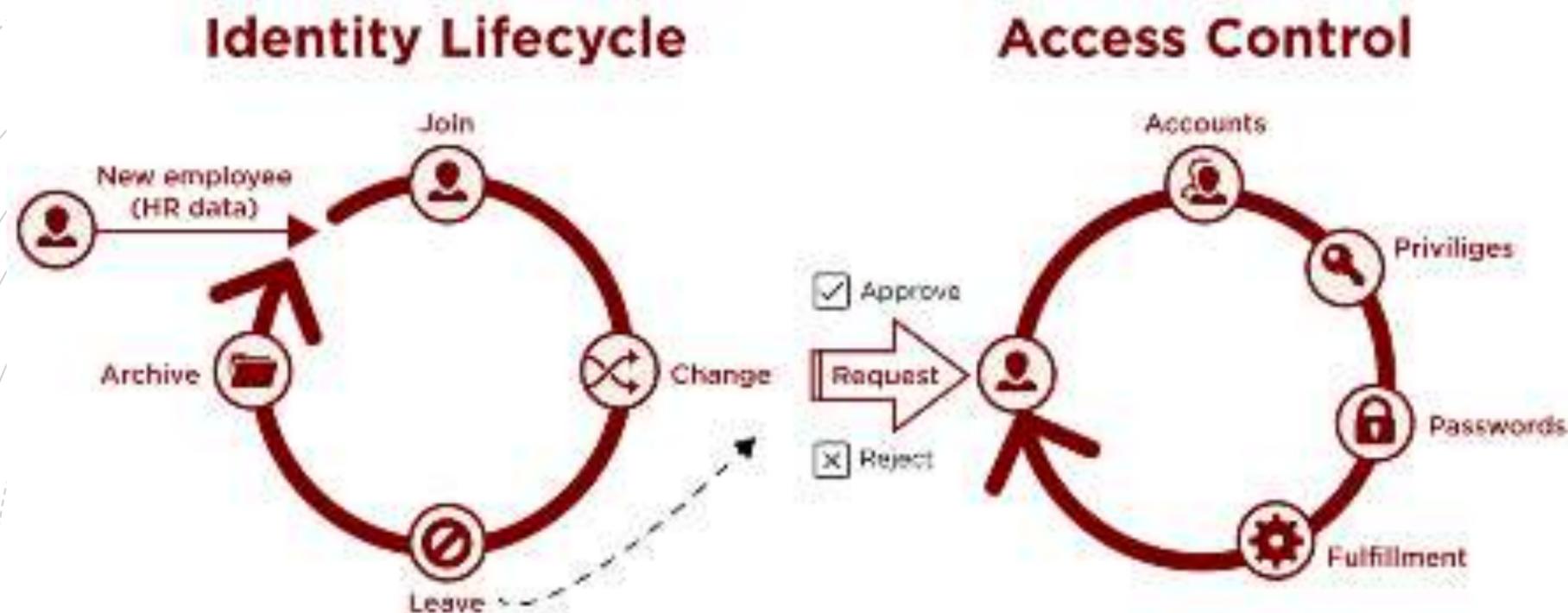
Organización y Personas Facilitadores

- Contratos y Gestión de Proveedores
- Liderazgo de Gestión de Activos
- Estructura organizativa y cultura
- Competencia y Comportamiento

Revisión & Riesgo

- La calidad, Evaluación de Riesgos y Gestión
- Planes de Contingencia y Análisis de Resistencia
- Desarrollo Sostenible
- Clima y Cambio Climático
- Activos y Sistemas de Rendimiento y Monitorización de la Salud
- Activos y Sistemas de Gestión de Cambio
- Revisión de la Gestión, Auditoría y Aseguramiento
- Prácticas de Contabilidad
- Interesados

A9 Control de acceso





A10 Criptografía

Controles de criptografía

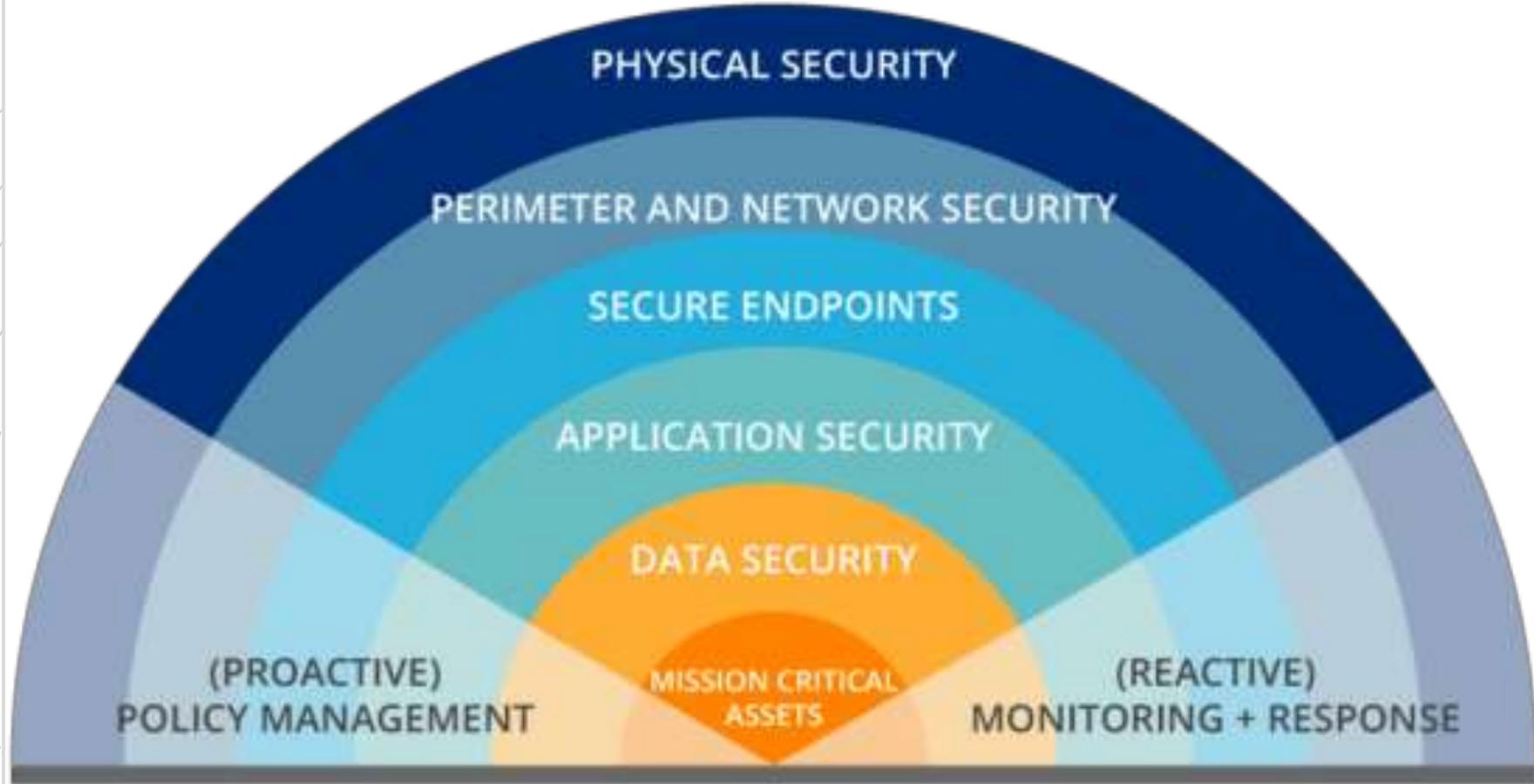
Políticas sobre el empleo de controles criptográficos

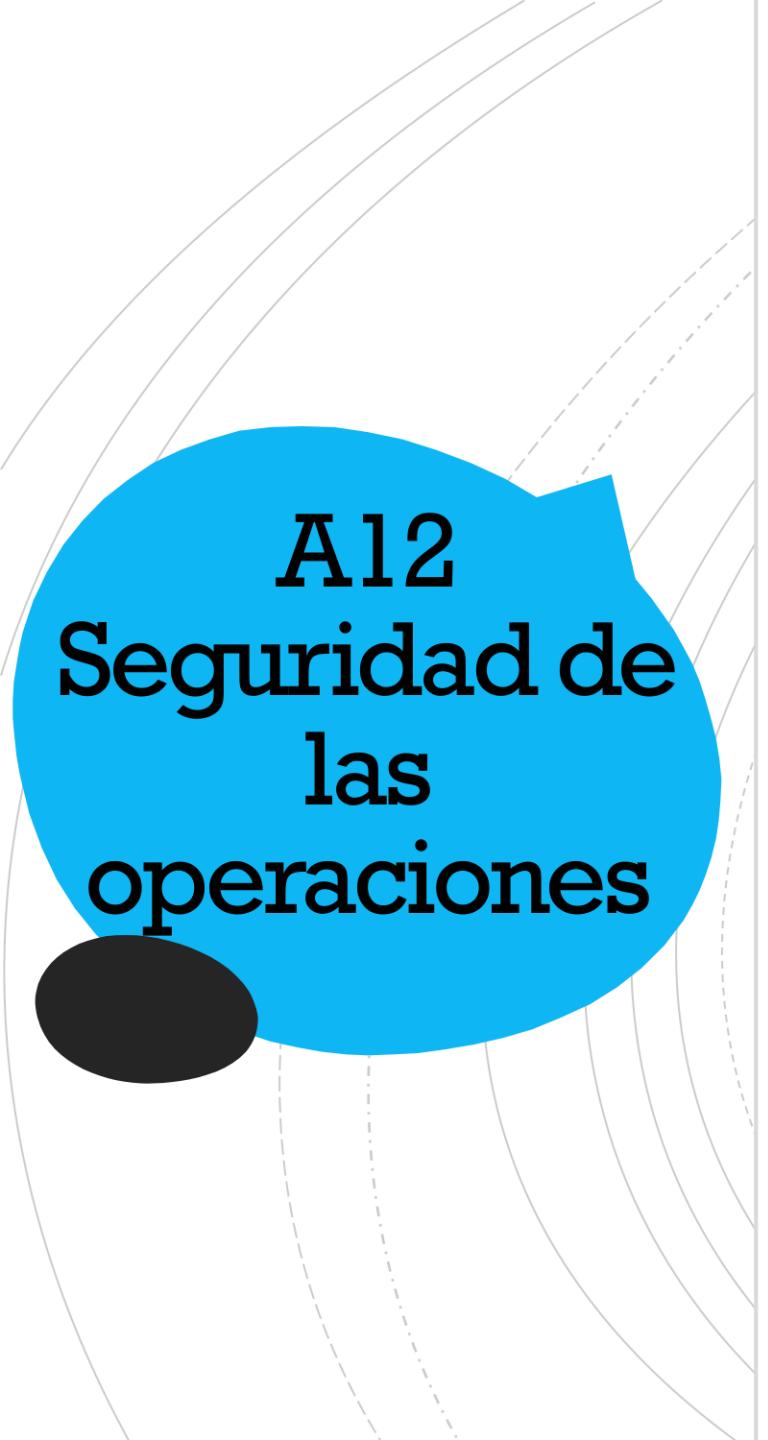
- Enfocados en la protección de la información en caso de que algún intruso acceda físicamente a la información. Identifica:
 - Las circunstancias en que es necesario aplicar claves criptográficas
 - Los medios a emplear
 - Gestión, mantenimiento y actualización de los medios empleados

Gestión de claves

- Mantiene la gestión de claves criptográficas utilizadas por los medios de cifrado, las claves deben cumplir con el ciclo de vida completo:
 - Generación
 - Uso y protección
 - Distribución
 - Renovación o destrucción

All Seguridad física y del entorno



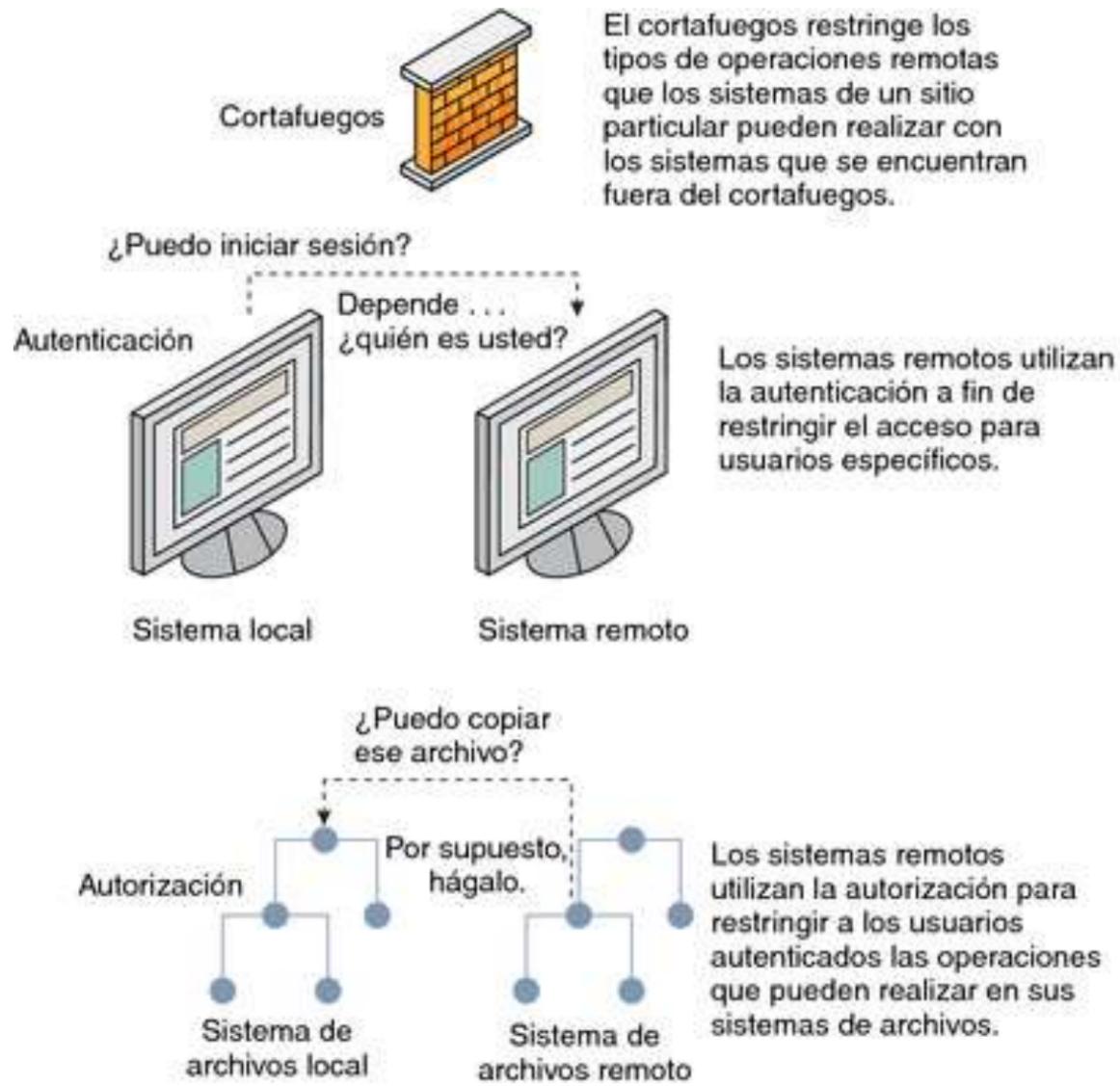


A12 Seguridad de las operaciones

Objetivos

- Procedimientos operacionales y responsabilidades. Asegura la operación correcta y segura de instalaciones de procesamiento de información
- Protección ante software malicioso. La información y las instalaciones de procesamiento de información se encuentran protegidos contra el código malicioso
- Respaldo. Registra eventos y genera evidencia
- Registros y supervisión
- Control de software en la producción. Integridad de los sistemas operativos
- Gestión de vulnerabilidades técnicas.
- Consideraciones sobre la auditoria de sistemas de información. Minimiza impactos de auditorias en sistemas operativos

A13 Seguridad de las comunicaciones



A14

Adquisición, desarrollo y mantenimiento de los sistemas de información

- Aplica controles para la seguridad de la información durante el ciclo de vida del sistema informático
- Garantiza la seguridad de la información integrando sistemas durante el ciclo de vida
- La seguridad de la información es diseñada e implementada dentro del ciclo de vida del desarrollo
- Garantiza la protección de los datos utilizados para las pruebas



A15 Relación con proveedores

Establecimiento de condiciones para el uso de activos

- Seguridad de la información en relaciones con los proveedores. Protección de activos de las organizaciones, siendo accesibles para los proveedores
- Gestión de entrega de servicios por terceros. Busca mantener un nivel apropiado de seguridad de la información y entrega de servicios acorde a los acuerdos con terceros

A16 Gestión de incidentes de la seguridad de la información



A17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

- Planificación de la continuidad de la seguridad de información
- Implementación de la continuidad de seguridad de la información
- Verifica, revisa y evalúa la continuidad de la seguridad de la información
- Garantiza la disponibilidad de las instalaciones de procesamiento de información



A18 Cumplimiento

Políticas, normas y legislaciones

- Identificación de legislaciones aplicables y requisitos contractuales
- Derecho de propiedad intelectual
- Protección de registros
- Regulación de controles criptográficos
- Revisión de cumplimiento técnico
- Cumplimiento de políticas y normas de seguridad