CSTIC 2018

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Seguridad de la Información

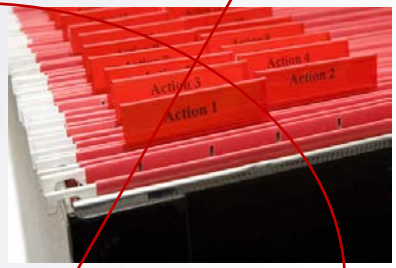
Evolución desde un modelo técnico a la gestión de la seguridad

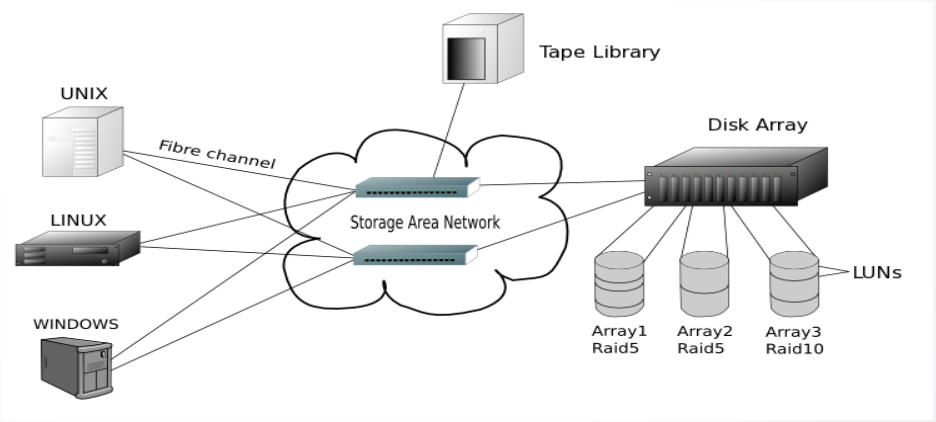
Miguel A. Guzmán

FREMAP

Índice

Evolución





Tecnología
Dependencia
Total

Riesgos Potenciales

?

- Procesos y procedimientos inconsistentes
- Pruebas insuficientes de aplicaciones (Desarrollo, Implantación)
- Operaciones con facultades excesivas para un rol operativo

Accidente Error	Riesgos Naturales
Ataque Interno	Ataque Externo
Normativa Legal	Tecnología

- Fuego
- Inundación
- Atmosféricos
- Sísmicos

- Empleados descontentos
- Intereses personales

- Hacking
- Vulnerabilidades de la tecnología

- RGPD
  - Coste implantación
  - Infracciones

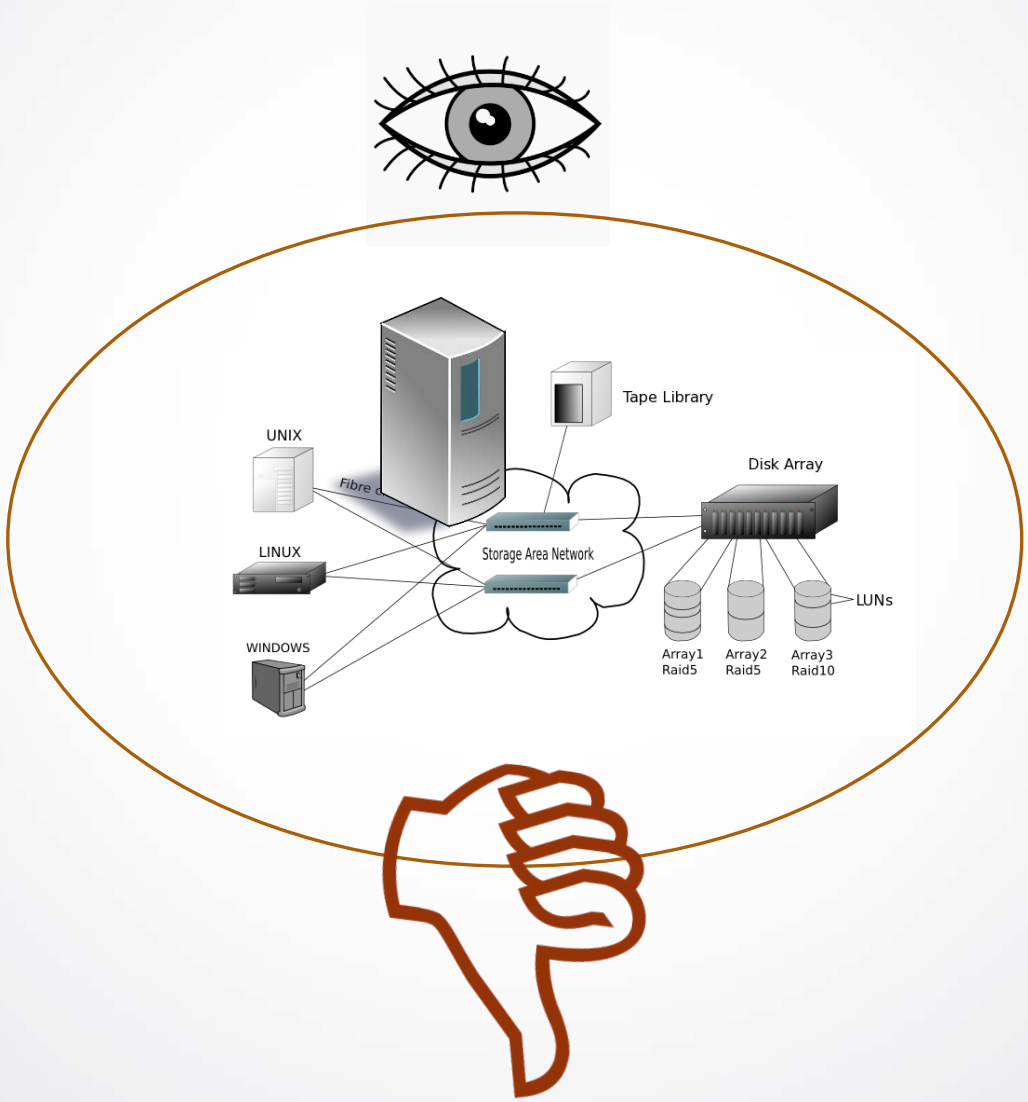
- Evolución constante

Impacto en la actividad

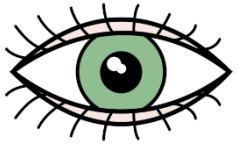
Ser conscientes de las consecuencias…..

Disponibilidad Integridad Confidencialidad	Cese parcial, temporal	Duración o momento Asumible
	Cese total, temporal	
	Cese parcial, temporal	Duración o momento **NO** Asumible
	Cese total, temporal	
	Pérdida de información	Cese del Negocio
	Pérdida de recursos	

Proteger el Negocio - Alcance



Proteger el Negocio - Alcance



Dirección

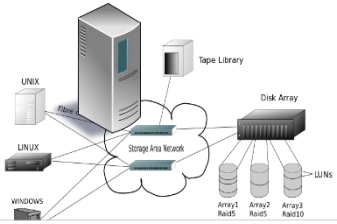
Estructura/Procesos

Áreas Funcionales

Áreas Operativas

Infraestructuras

TI



Grupos de Interés

Estrategia

Política de Seguridad de la Información	Dirección Liderazgo - Compromiso
Modelo de Gestión	- Responsable de Seguridad - Comité de Seguridad
Metodología	- Requisitos de seguridad - Análisis de Riesgos - Planes de acción
Auditoría	- Interna - Externa
Incidencias	- Comunicación - Gestión
Certificación	- Buenas prácticas

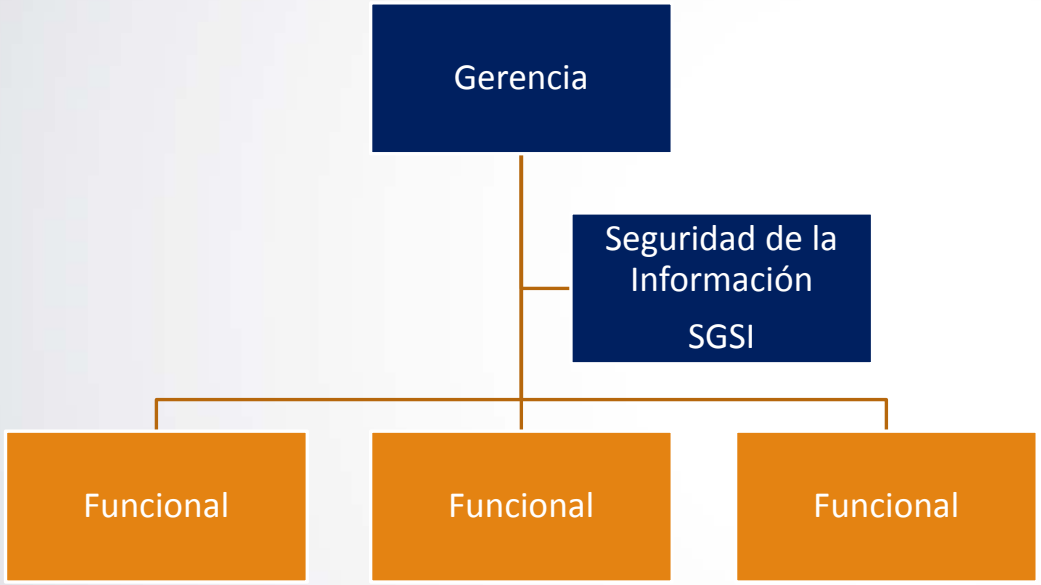
Política de Seguridad de la Información

- **Establecida por iniciativa de la Dirección**
- Orientada a los objetivos de la empresa y estándares SGSI
- Protección de todos los activos de información
- Compromiso de cumplimiento y mejora

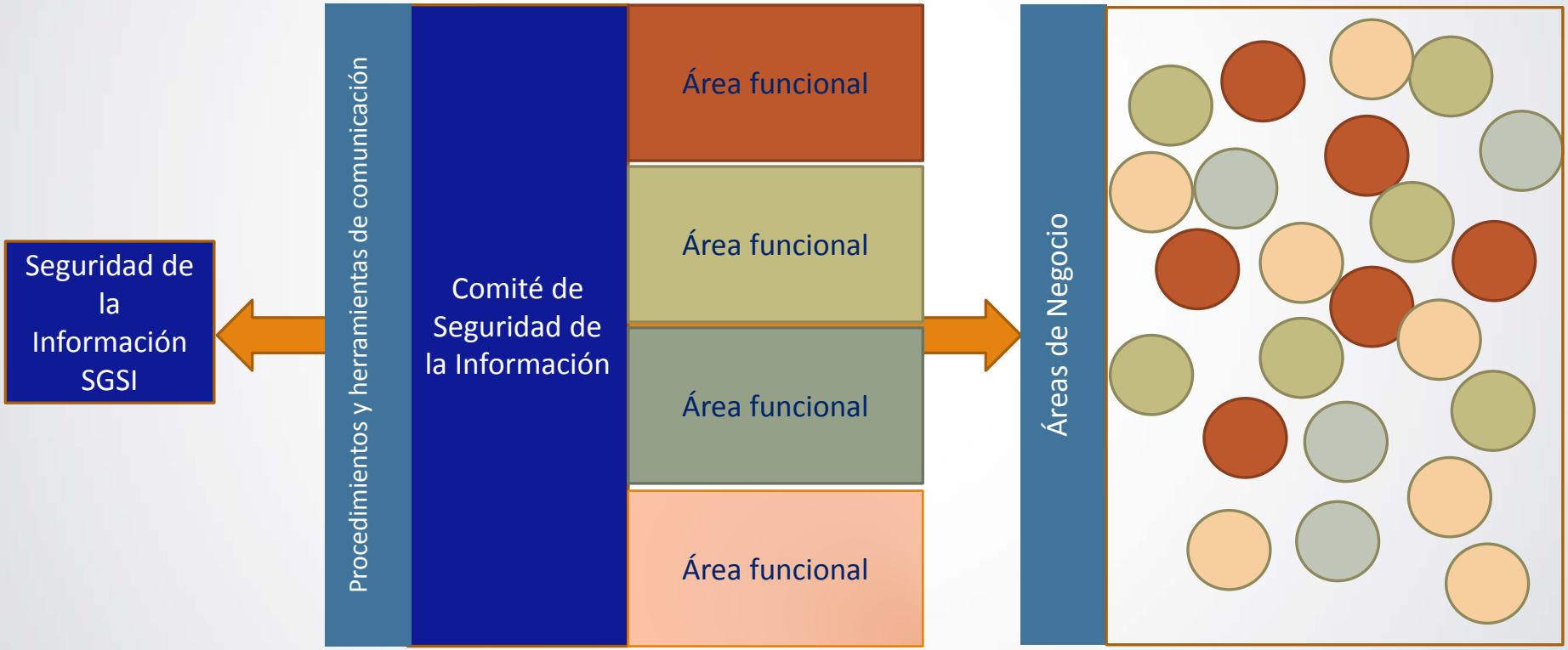
Acceso y comunicación:

- Accesible todo el personal
- Plan de comunicación, reforzando la obligación de cumplimiento
- Disponible para las partes interesadas

Modelo FREMAP | BS 7799 | ISO/IEC 17799 | ISO/IEC 27001



- Dependencia de la Gerencia
- Medios
- Ámbito de actuación global
- Plan de implantación reforzado

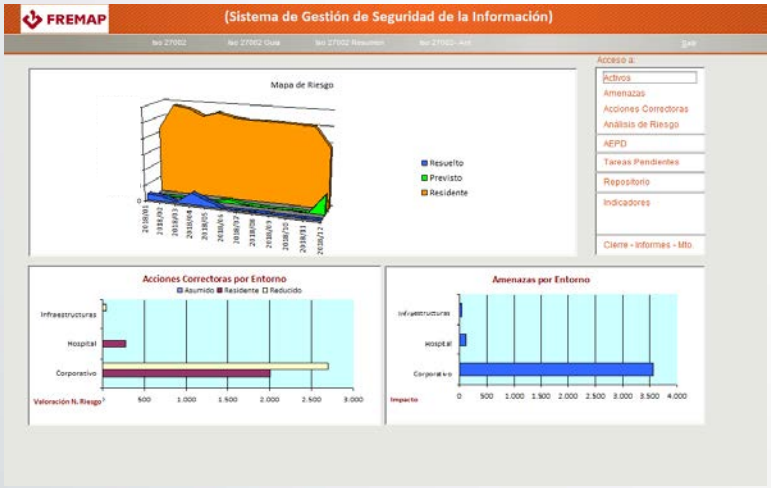

Seguridad de la Información SGSI
Procedimientos y herramientas de comunicación
Comité de Seguridad de la Información
Área funcional
Área funcional
Área funcional
Área funcional
Áreas de Negocio

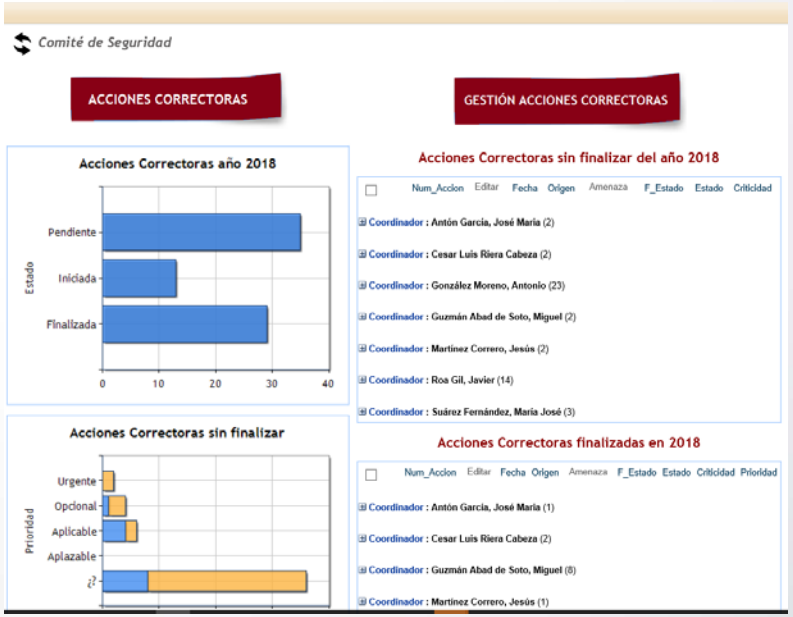
Seguridad de la Información

- Estrategia de seguridad
- Presidencia del Comité de S.
- Políticas, normas, instrucciones
- Gestión de incidencias
- Gestión del riesgo
- Informes a Gerencia

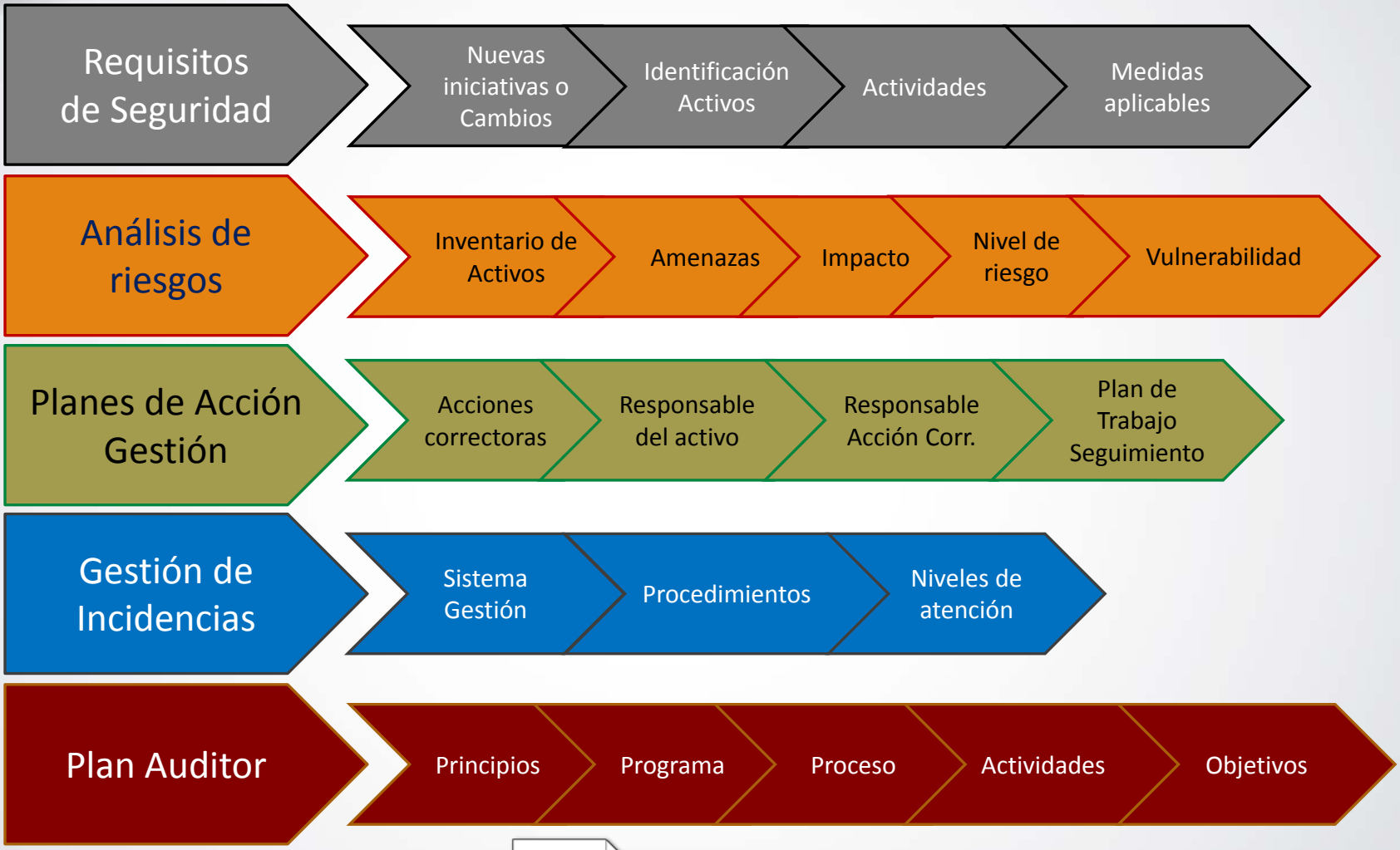
Comité de Seguridad

- Establecer y revisar la política
- Propuestas de mejora
- Información y formación
- Supervisión de los requisitos
- Gestión de los planes de acción





Implantación
Metodología I



Documentación
- Controlada
- actualizada

Implantación
Metodología II

- **Política**
  ISO/IEC 27001
- **SGSI**
  Sistema de Gestión de Seguridad de la Información
- Seguridad de la Información
- Comité de Seguridad de la Información
- Metodología y Procesos
- Auditoría
- Documentación

?

ISO/IEC 27001

¿Estamos preparados?

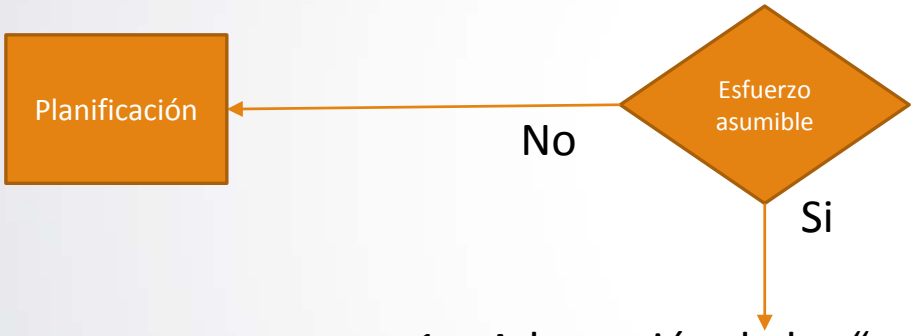
Certificación: ¿parcial o total?

- ✓ SGSI implantado
- ✓ Maduro (experiencia)
- ✓ Procedimientos optimizados
- ✓ Auditoría conforme al plan
- ✓ Planes de acción
- ✓ Seguimiento de los planes
- ✓ Actualización de políticas

Gestión orientada a procesos

Escenario apropiado – Certificación total

- **PROCESO**
  1. Revisión por entidad certificadora (GAP Analysis)
  2. Análisis del informe de situación.
  3. Valoración del coste técnico y organizativo
  4. Toma de decisión



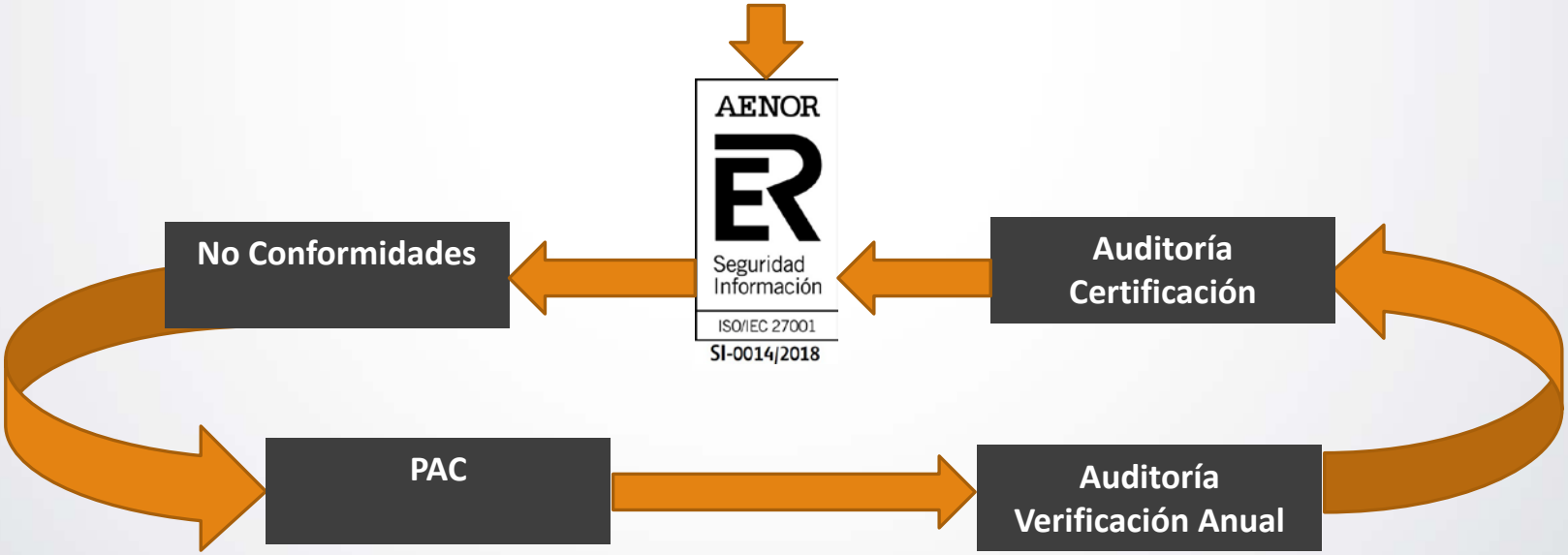
1. Adecuación de las “no conformidades” identificadas y recomendaciones del GAP
2. Planificación de la auditoría
3. Proceso de certificación

GAP Analysis

- Révisión rápida
- Modelo de gestión
- 27001

Certificación

- Revisión en detalle
- Modelo de gestión
- 27001
- Controles 27002



Ciclo de tres años

Valor añadido

Imagen

- Mayor confianza para empresas y personas
- Mejor valoración de procesos de contratación pública
- Mejor valoración de ofertas comerciales

Reglamento General de Protección de datos 2016/679 del Parlamento Europeo y del Consejo de 27 de abril

Obligaciones generales:

- Medidas de seguridad
  - **La adhesión a códigos de conducta o a <u>un mecanismo de certificación</u>** podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.
  - Protección desde el diseño y por defecto
  - Seudonimización, minimización, cifrado, disponibilidad, integridad, confidencialidad, resiliencia, contingencias, evaluación y valoración regular de las medidas
  - Notificación de brechas de seguridad
  - Evaluación de impacto

Reglamento General de Protección de datos 2016/679 del Parlamento Europeo y del Consejo de 27 de abril

- Adhesión a código de conducta o certificación
  - ISO/IEC 27001
- Diseño por defecto
  - Requisitos de seguridad
- Medidas de seguridad
  - ISO/IEC 27002
- Evaluaciones de impacto
  - Requisitos de seguridad
  - Análisis de riesgos

AENOR
Seguridad Información
ISO/IEC 27001
SI-0014/2018

FREMAP

Gracias por su atención

EFQM Recognised for excellence 5 star

900 61 00 61
www.fremap.es