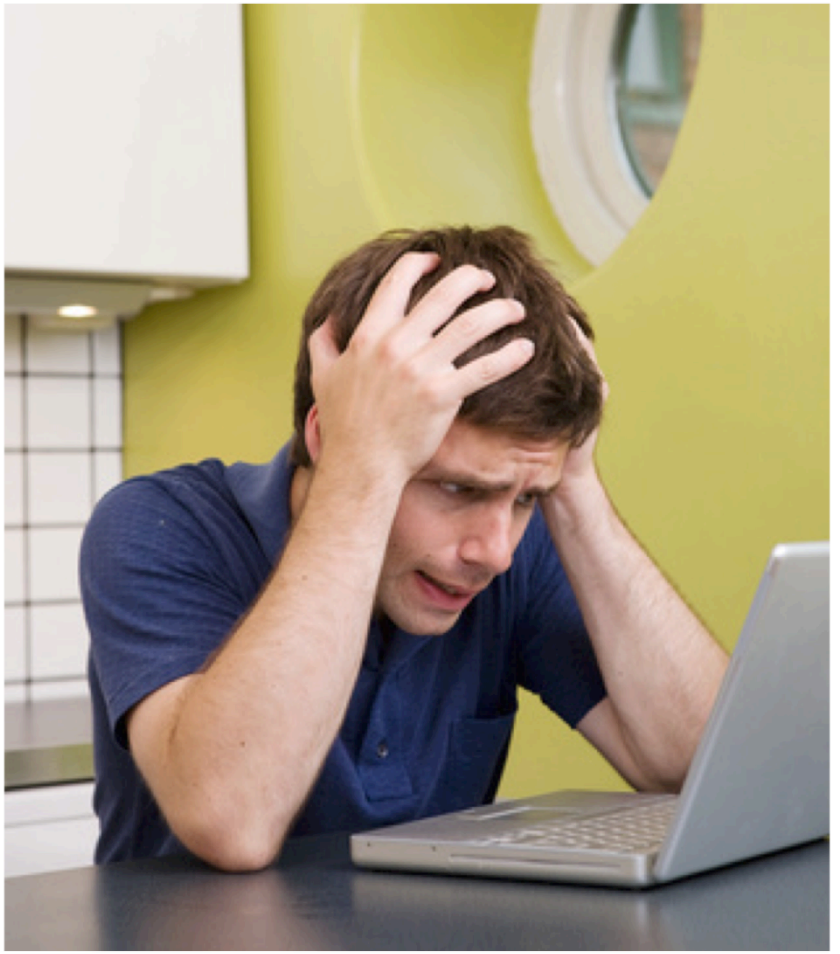

FCSCL
FUNDACIÓN CENTRO DE SUPERCOMPUTACIÓN
DE CASTILLA Y LEÓN
Implantación de la Norma ISO 27001 en un Centro de Supercomputación
JT RedIris 2010
Córdoba, 19 de noviembre de 2010
Antonio Ruiz Falcó – Director Técnico
antonio.ruizfalco@fcsc.es

- **El Problema de la seguridad**
- La norma ISO 27001 “Gestión de Seguridad de Sistemas de Información”
- Experiencia en la FCSCL

- Uno de cada 5 empleados deja a su familia y amigos usar sus portátiles corporativos para acceder a Internet. (21%).
- Uno de cada diez confiesa que baja algún tipo de contenido que no debiera mientras está en el trabajo.
- Dos tercios admiten tener conocimientos muy limitados en materia de seguridad.
- Un 5% dice que tienen acceso a areas de la red corporativa que no deberían tener.

Fuente: **McAffee.**



- Informe Penteo (2006):
  - Sólo un 21% de las organizaciones gestionan el Dpto. de SI con criterios de negocio
  - 31 % gestionan el dpto. de SI sólo con criterios tecnológicos
  - 48 % gestionan con criterios híbridos

- Conclusiones:
  - La Dirección de las organizaciones tiene una percepción más positiva de los CIOs que siguen criterios de Negocio. Les dan el rol de líderes contribuidores de negocio en un 58%
  - La Gestión de las TICs mejora el posicionamiento del dpto. de SI y del CIO
  - En un futuro los CIOS más gestores y menos tecnólogos

  (Encuesta a: 85 Directores de TICs, 36 Dir. Generales y 12 Presidentes)

Proteger Información vs Proteger Sistemas

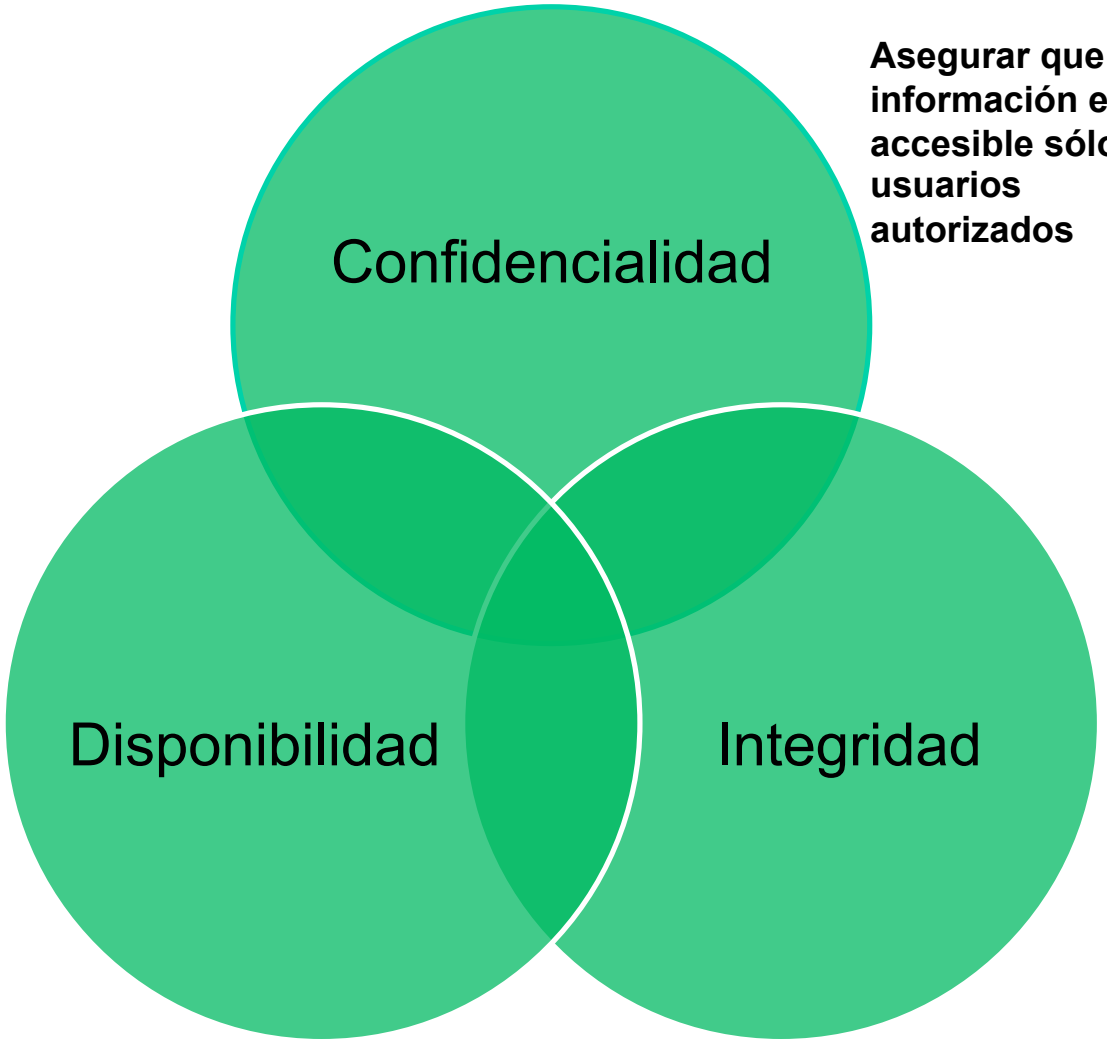
Seguir Controlando :

- ✓ las vulnerabilidades
- ✓ la seguridad perimetral
- ✓ los accesos indebidos
- ✓ intrusismo
- ✓ etc,

Y además….

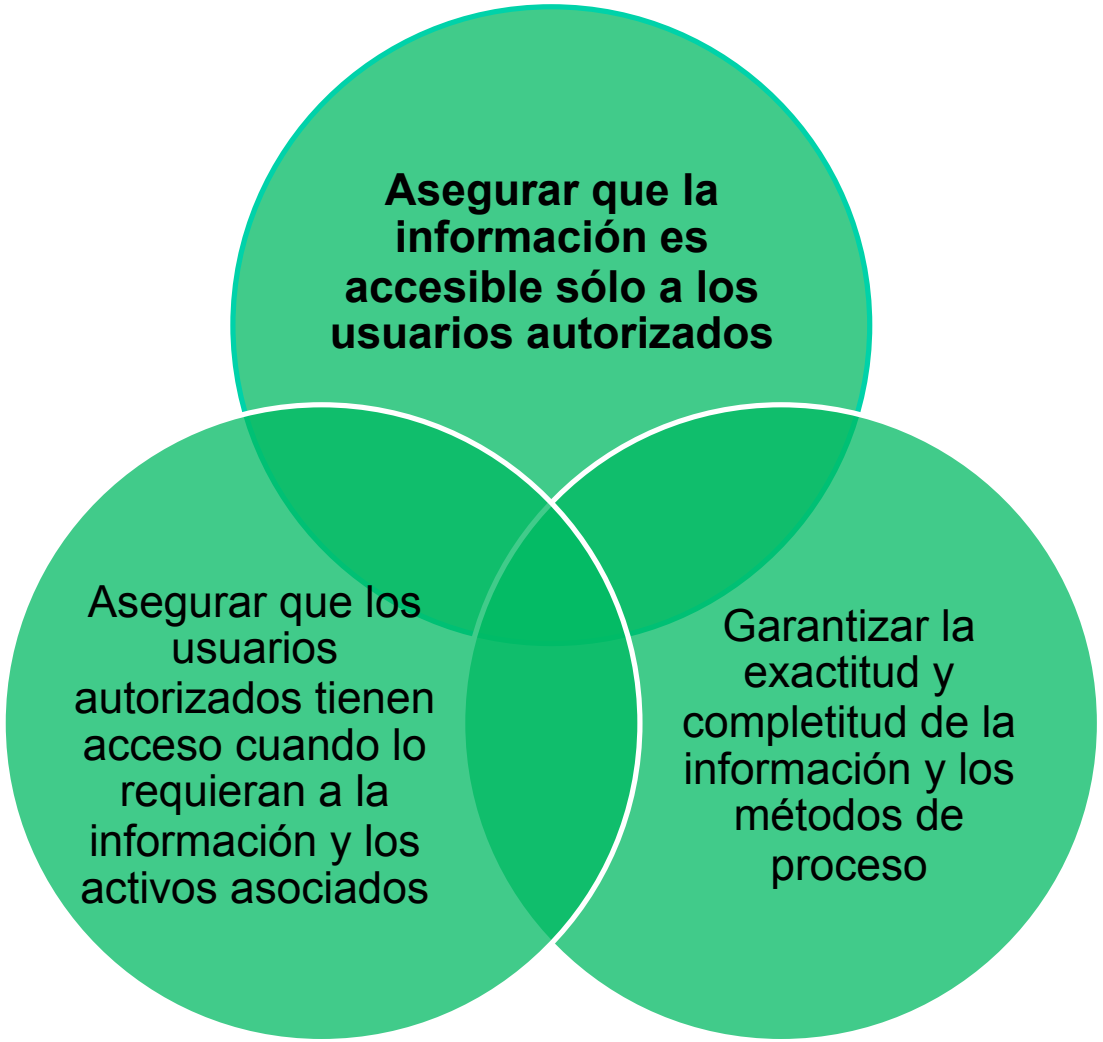
Garantizar por parte del personal que el manejo de la información de la compañía se realiza de una forma segura, independientemente del formato o soporte en el que se encuentre

Atributos de la Seguridad



Asegurar que la información es accesible sólo a usuarios autorizados

Atributos de la Seguridad



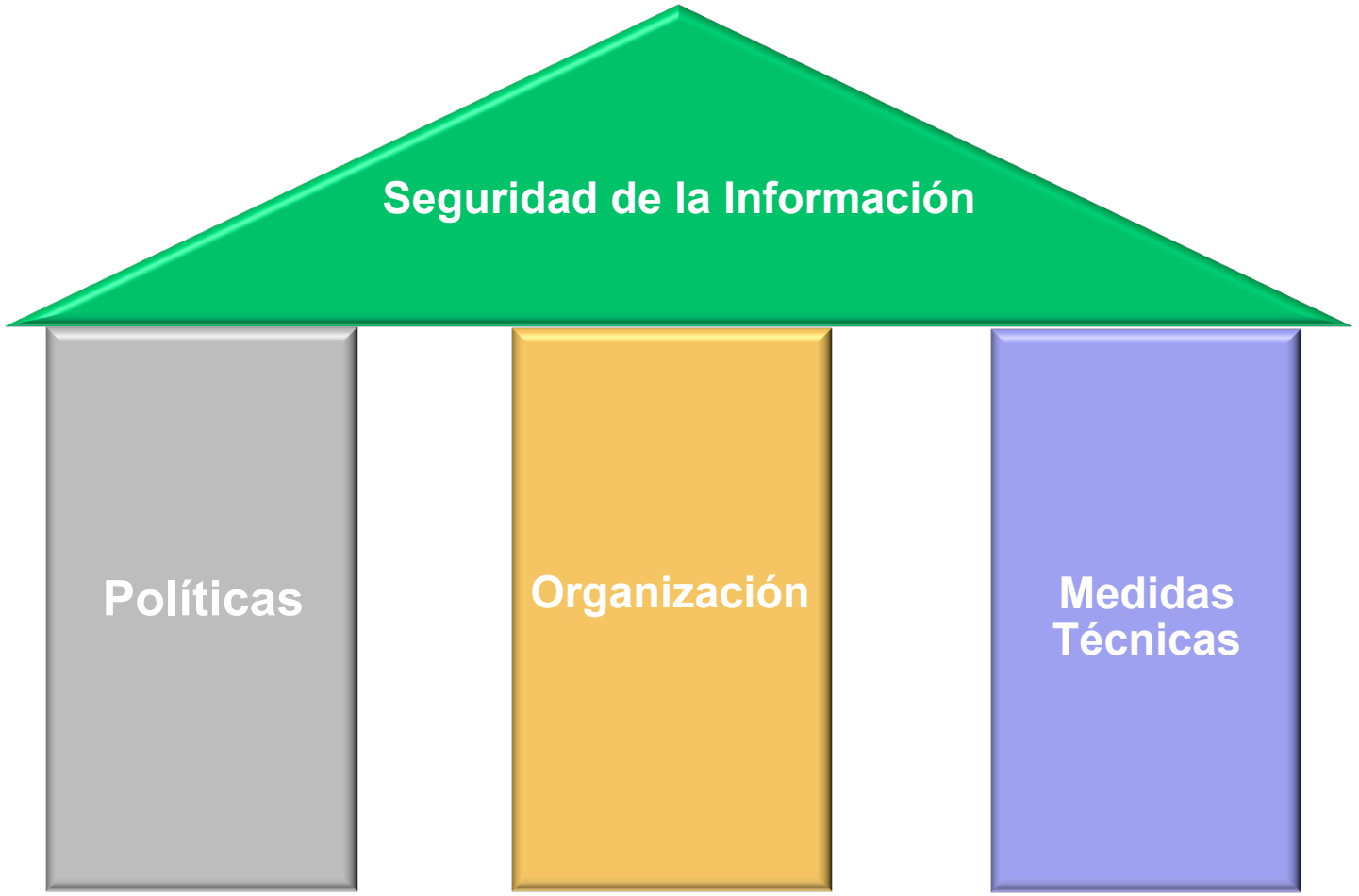
- El Problema de la seguridad
- **La norma ISO 27001 "Gestión de Seguridad de Sistemas de Información"**
- Experiencia en la FCSCL

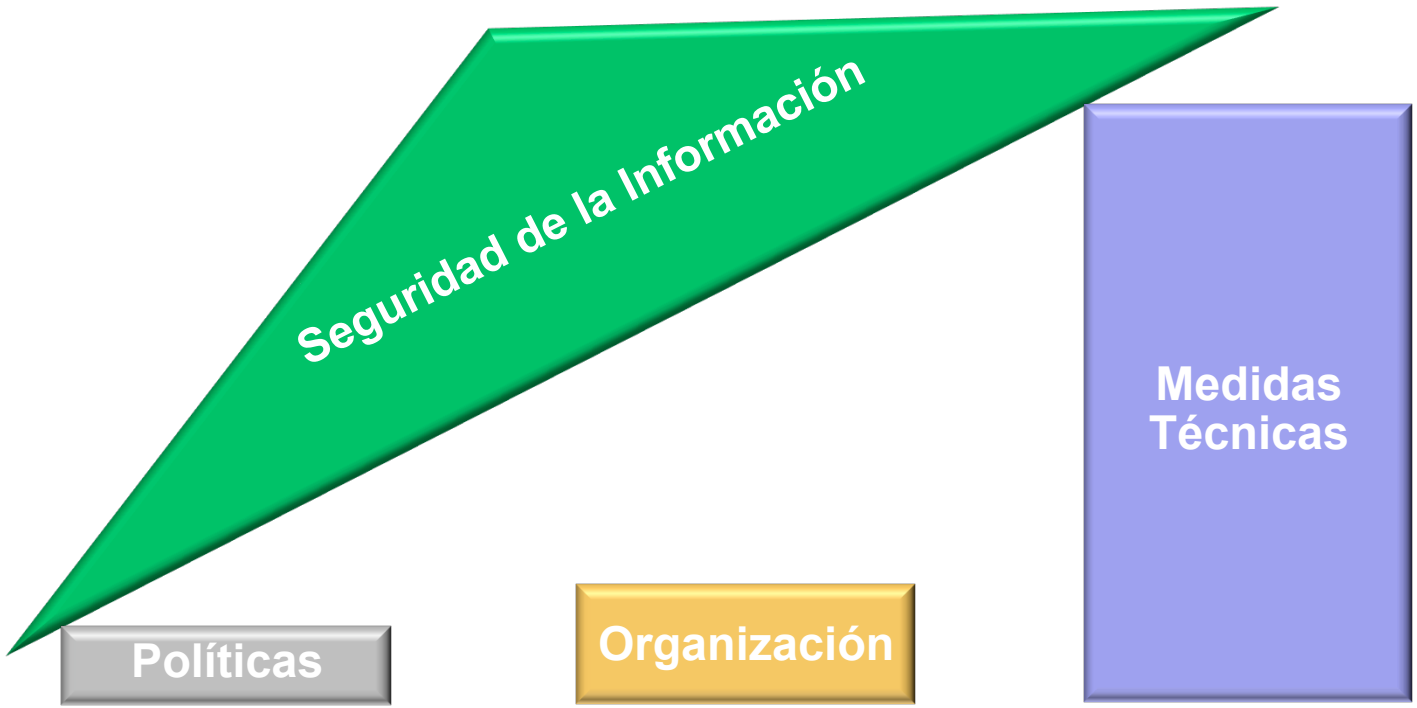
- **Parte del sistema general de gestión** que comprende la política, la estructura organizativa, los procedimientos, los procesos, y los recursos necesarios para **implantar la gestión de la seguridad de la información.**
- La **herramienta de que dispone la Dirección** para implantar las políticas y objetivos de Seguridad de la Información.
- Permite, establecer y reordenar la Seguridad de los Sistemas de Información en **concordancia con los Planes Estratégicos** de la Organización y con sus Políticas de Seguridad.

Riesgo Gestionado

- **La seguridad absoluta no existe**
- **Siempre hay que convivir con situaciones de riesgo**
- **El riesgo conocido puede ser analizado y gestionado.**

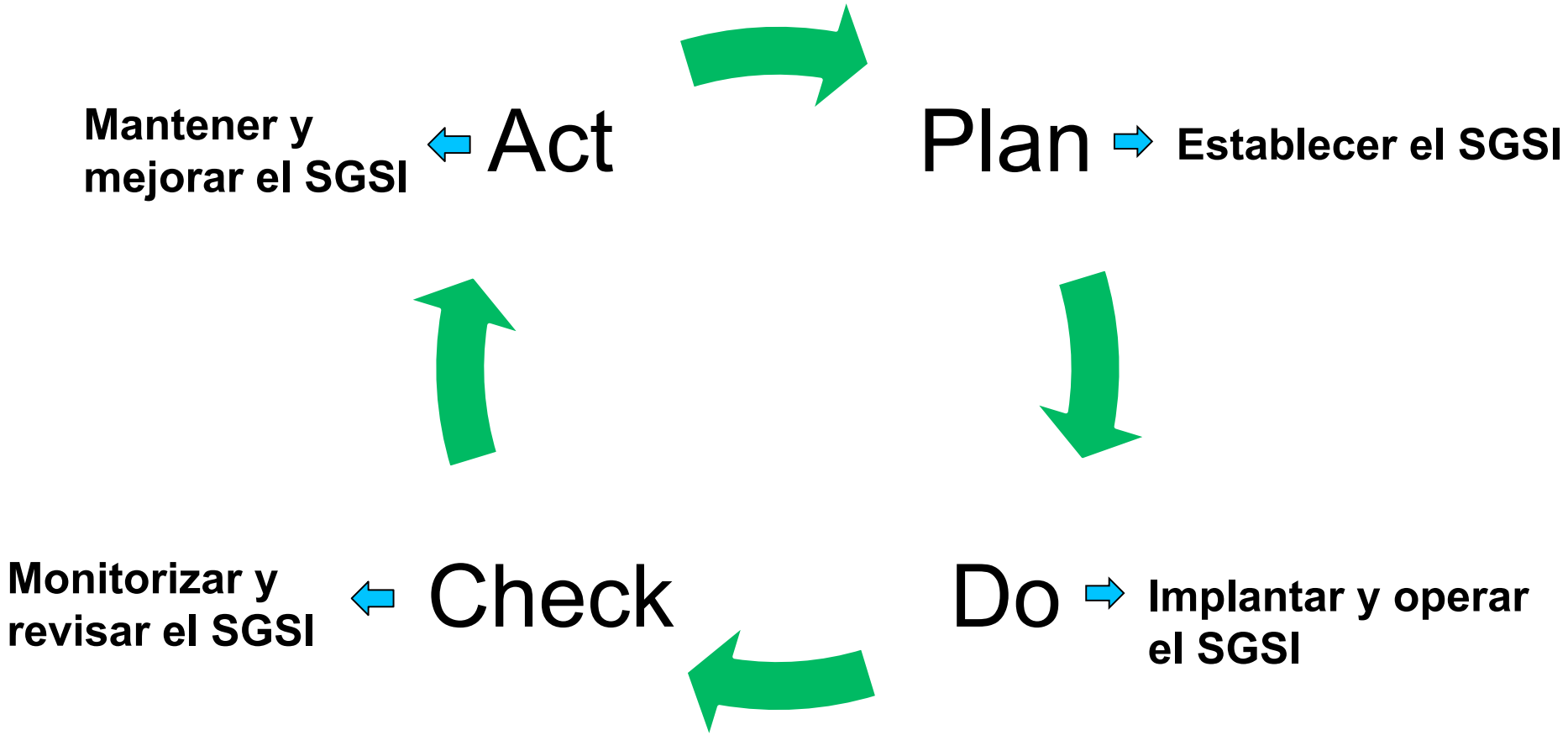
Lo que debe ser…



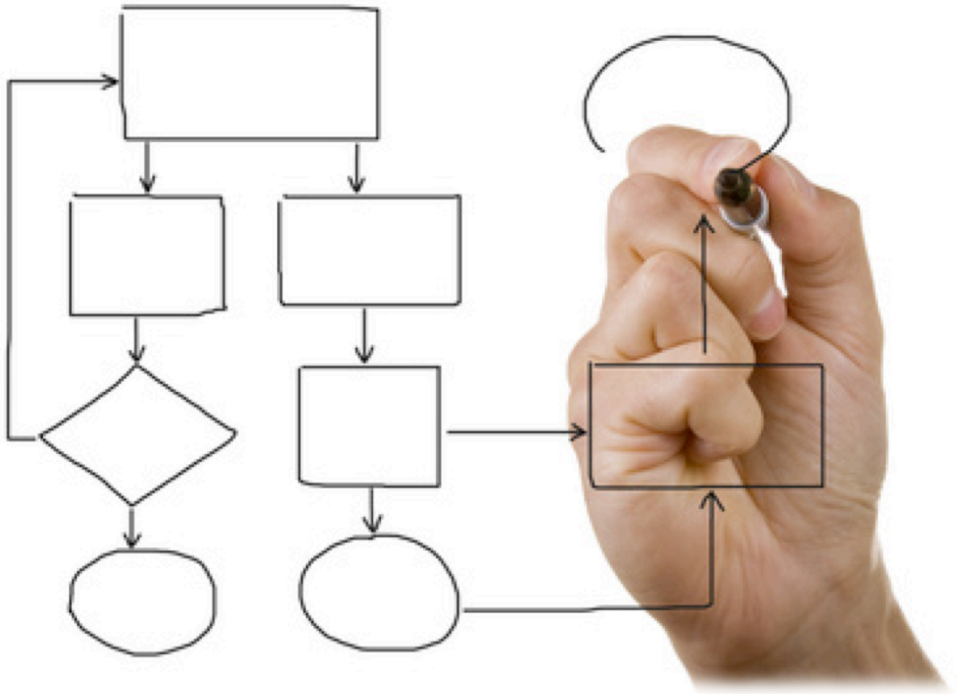


!!!Dejar en manos del equipo de TI la toma de decisiones políticas y organizativas!!!

El “poli malo” para “hacer cosas” que no podríamos justificar de otra forma



- ✓ **Definir el alcance del SGSI**
- ✓ **Definir la política del SGSI**
- ✓ **Definir los objetivos**
- ✓ **Identificar los riesgos**
- ➢ **Gestionar los riesgos**
- ➢ **Seleccionar los controles de Seguridad**



- **Definir e implantar el plan de gestión de riesgos**
- **Implantar controles seleccionados**
- **Implantar el sistema de gestión**

Monitorizar y Revisar el SGSI

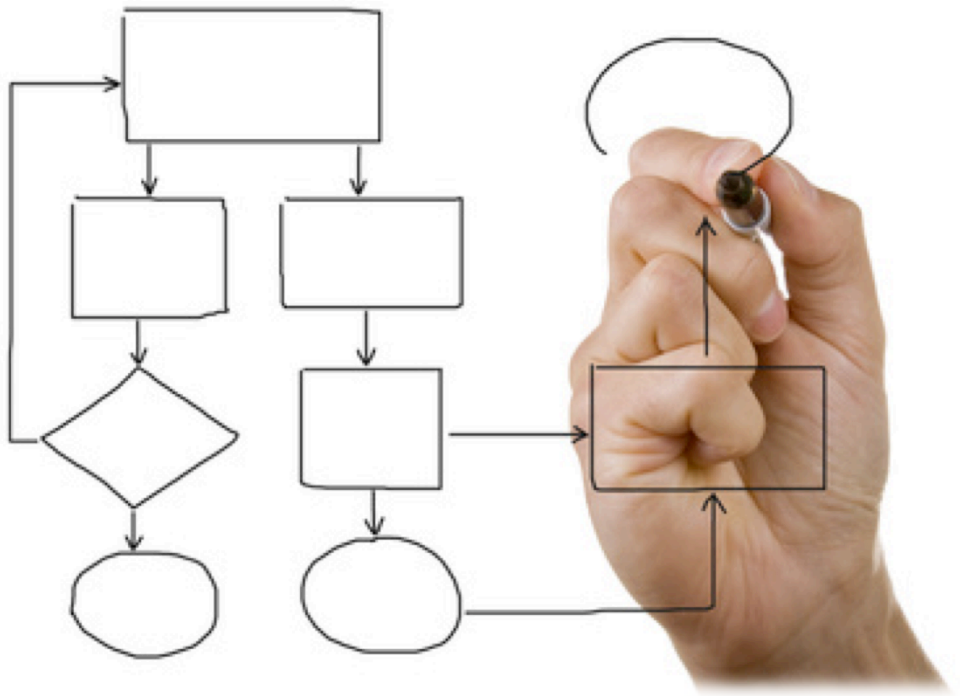
- Desarrollar procedimientos de monitorización
- Revisar regularmente el SGSI
- Revisar los niveles de Riesgo
- Auditar internamente el SGSI

- **Implantar las mejoras**
- **Adoptar acciones correctivas y preventivas**
- **Comunicar acciones y resultados**
- **Verificar que las mejoras cumplen su objetivo**

- El Problema de la seguridad
- La norma ISO 27001 “Gestión de Seguridad de Sistemas de Información”
- **Experiencia en la FCSCL**

"Prestación de Servicios de Supercomputación y Cloud Computing. Desarrollo de Proyectos de I+D+i en áreas de Supercomputación, Cloud Computing y Eficiencia Energética."

- **Definir el alcance del SGSI**
- **Definir la política del SGSI**
- **Definir los objetivos**
- **Identificar los riesgos**
- **Gestionar los riesgos**
- **Seleccionar los controles de Seguridad**



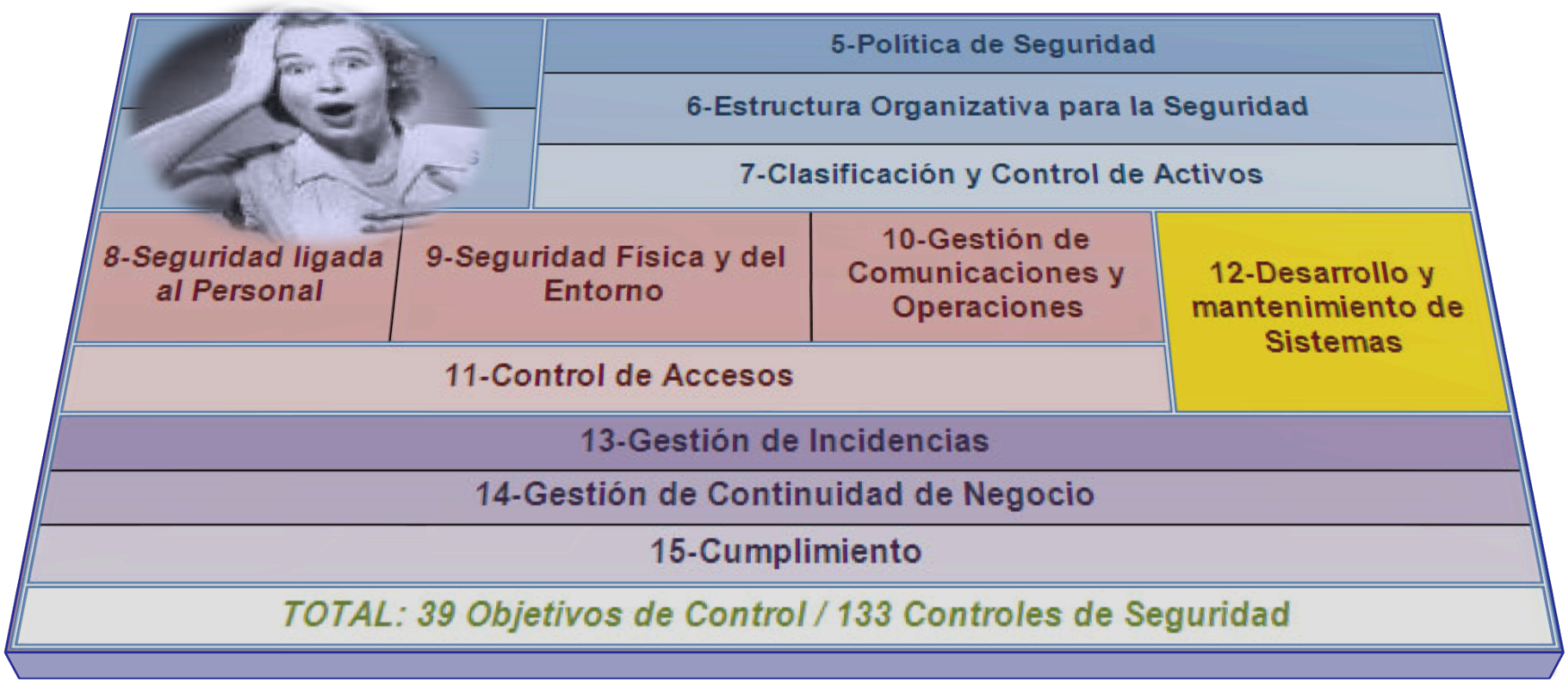
Gestión del Riesgo I

Inventario de Activos

- Abstracción
- Agrupación
- Responsabilidades

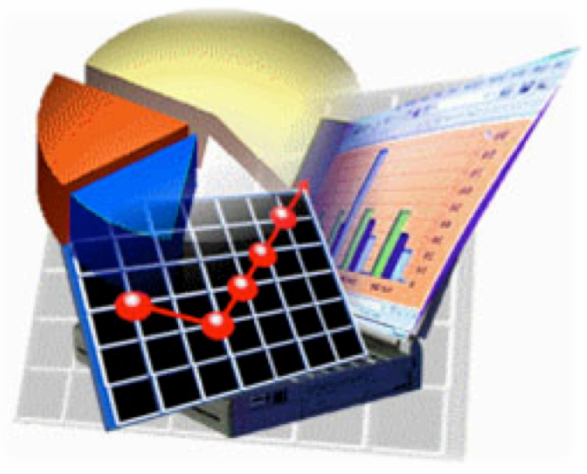
Gestión del Riesgo II

133 Controles!!



Gestión del Riesgo III

- Amenazas
- Cálculo del Riesgo
- Estado aplicabilidad controles
- Indicadores → CMI
- Gestor documental



A.x	A.x.y	Objetivos ISO 27002	Control A.x.y.z	Medida	Elemento	Estado actual	Nivel de Riesgo	Comentarios
13	13.1	Asegurar que eventos y debilidades en la seguridad de la información asociados con sistemas de información son comunicados de forma que se conceda tiempo para tomar acciones correctivas .	13.1.1	1-Una alarma anticoacción debería ser provista para los usuarios que puedan ser objeto de coacción	D15	0-No definida	4	
				2-Las incidencias de seguridad deberían informarse rápidamente y a través del canal correspondiente	D15	2-Implementada	6	
15	15.1	Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractuales, y de todo requisito de seguridad.	15.1.5	Prevención del uso indebido de los recursos de tratamiento de la informació	D17	2-Implementada	5	
			15.1.6	El uso de controles criptográficos debería acatar la legislación y regulaciones vigentes	D17	NO Implementada	5	Depende de los controles 12.3
	15.2	Asegurar la conformidad de los sistemas con las políticas y normas de seguridad.	15.2.1	Se debería hacer una comprobación para asegurar la conformidad con los estatutos pertinentes y los requerimientos de seguridad contractuales	D01	2-Implementada	6	
			15.2.2	1-Auditorias y revisiones independientes se deberían realizar regularmente	D01	1-Definida	6	Contemplado en otras directivas
	15.3	Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema.	15.3.1	1-Los requerimientos y actividades de auditoria deberían ser planeados para minimizar el riesgo de interrupción del negocio	D19	2-Implementada	6	
			15.3.2	1-El acceso a las herramientas de auditoria del sistema debería estar protegido para impedir cualquier posible abuso o puesta en peligro	D19	2-Implementada	6	

www.fcsc.es

Fundación Centro Supercompurtación de Castilla y León

Edificio CRAI-TIC
Campus de Vegazana s/n
24071 León (España)
Tlf.: (+34) 987 29 3160

FCSCL
FUNDACIÓN CENTRO DE SUPERCOMPUTACIÓN DE CASTILLA Y LEÓN