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

Información

- Conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita, de su origen o de la fecha de elaboración

- La información, junto a los procesos y sistemas que hacen uso de ella, es un activo vital para el éxito y la continuidad en el mercado de cualquier organización, y debe ser protegida adecuadamente

Ciclo de vida de la información

- La información puede ser:
  - Creada
  - Guardada
  - Destruída
  - Procesada
  - Transmitida
  - Utilizada (con fines adecuados e inadecuados)
  - Corrompida
  - Robada
  - Perdida

Tipos de información

- Impresa o escrita en papel
- Guardada electrónicamente
- Transmitida por correo o medio electrónicos
- En vídeos corporativos
- Publicada en la web
- Verbal – en conversación
- ...

Seguridad de la información

- “Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad”

(ISO/IEC 27001)

Seguridad de la información

- Confidencialidad
  - La información es accesible solo a usuarios autorizados
- Integridad
  - Exactitud e integridad de la información y de los métodos de proceso
- Disponibilidad
  - Asegurar que los usuarios autorizados tengan acceso a la información y recursos asociados cuando sean requeridos

CATEGORY	DESCRIPTION	Sample Documents/Records	MARKING	PHYS & ADMIN CONTROLS	REPRODUCTION	DISTRIBUTION	DESTRUCTION/ DISPOSAL
PUBLIC or open	Information that may be broadly distributed without causing damage to the organization, its employees and stakeholders. The [PR Office/Marketing Dept/Information Security Management dept/etc.] must pre-approve the use of this classification. These documents may be disclosed or passed to persons outside the organization.	Marketing materials authorized for public release such as advertisements, brochures, published annual accounts, Internet Web pages, catalogues, external vacancy notices	None	None	Unlimited	No restrictions	Recycling/trash
INTERNAL or proprietary	Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient. Disclosure to anyone outside of [Company name] requires management authorization.	Most corporate information falls into this category. Departmental memos, information on internal bulletin boards, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories, marketing or promotional information (prior to authorized release), investment options, transaction data, productivity reports, disciplinary reports, contracts, Service Level Agreements, internal vacancy notices, intranet Web pages	"**INTERNAL USE ONLY**" Apply to bottom left corner of each page.	**Author:** responsible for proper markings. **User:** responsible for proper storage and document control.	Limited copies may be made only by employees, or by contractors and third parties who have signed an appropriate nondisclosure agreement.	**Internal**: use an internal mail envelope. **External**: use a sealed envelope. **Electronic**: use internal email system. Encryption is required for transmission to external email addresses. **FAXing**: take care over the FAX number!	**Paper documents:** shred. **Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal
CONFIDENTIAL or restricted	Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed outside of the organization without the explicit permission of a Director-level senior manager.	Passwords and PIN codes, VPN tokens, credit and debit card numbers, personal information (such as employee HR records, Social Security Numbers), most accounting data, other highly sensitive or valuable proprietary information	"**CONFIDENTIAL**" Apply to bottom left corner of each page.	**Originator:** responsible for ensuring that confidential information is distributed on a strict need-to-know basis. **Recipient:** responsible for ensuring that confidential information is encrypted and/or kept under lock & key when not in use.	Limited copies may be made only by permission of originator or his/her designates. A signed authorization slip will be presented.	**Internal:** use a sealed envelop inside an internal mail envelope. Hand deliver if possible. **External:** use a plain sealed envelope. Hand deliver or send by registered mail, courier *etc.* **Electronic:** use internal email system only. Encrypt data. **FAXing:** requires phone confirmation of receipt of a test page immediately prior to sending the FAX, and phone confirmation of full receipt.	**Paper documents:** shred using an approved cross-cut shredder. **Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.

Seguridad de la información

- El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

- En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

SGSI

- Herramienta para dotar a las organizaciones de las medidas de seguridad oportunas, proporcionando los niveles de protección de la información que en cada momento sean necesarios, de la forma más eficiente, y en un entorno de mejora continua.

- Proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial.

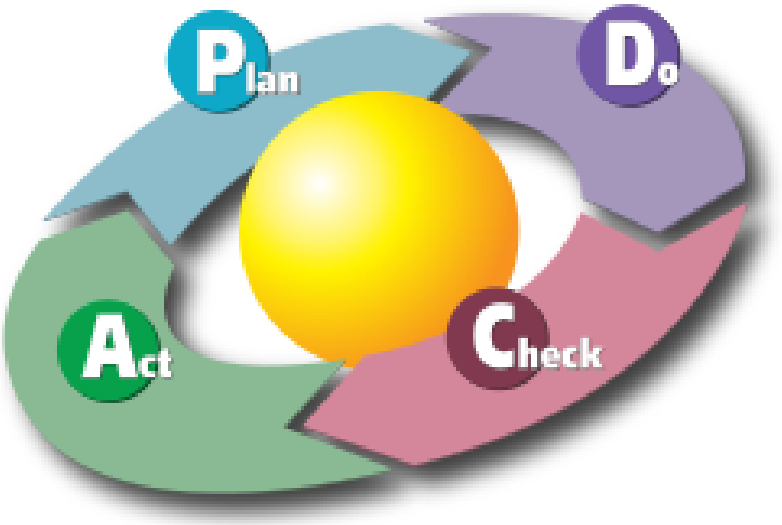
SGSI

- Ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

- Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Fases del SGSI

- *PDCA (Plan, Do, Check, Act)*
  - **Plan**: Establecer el SGSI
  - **Do**: Implementar y gestionar el SGSI
  - **Check**: Monitorizar y revisar
  - **Act**: Mantener y mejorar



Plan: Establecer el SGSI

Do: Implementar y gestionar el SGSI

- Implementar el plan de tratamiento de riesgo
- Implementar los controles
- Formación y concienciación
- Gestionar las operaciones y recursos del SGSI
- Implementar los procedimientos y controles que permitan una pronta detección de y respuesta a incidentes de seguridad.

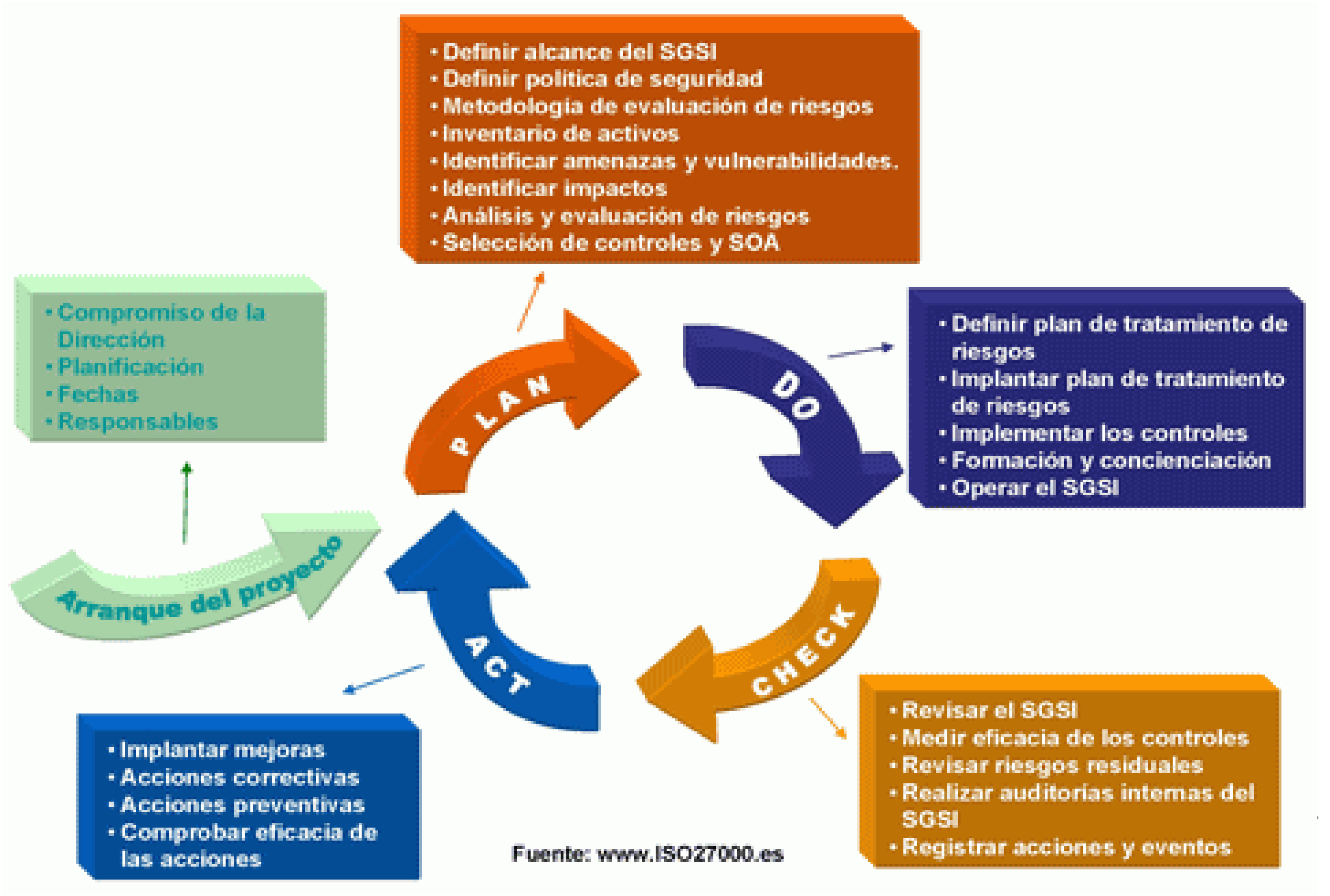
Check: Monitorizar y revisar

- Revisar el SGSI
- Medir la eficacia de los controles
- Revisar riesgos residuales
- Registrar acciones y eventos
- Realizar auditorías internas

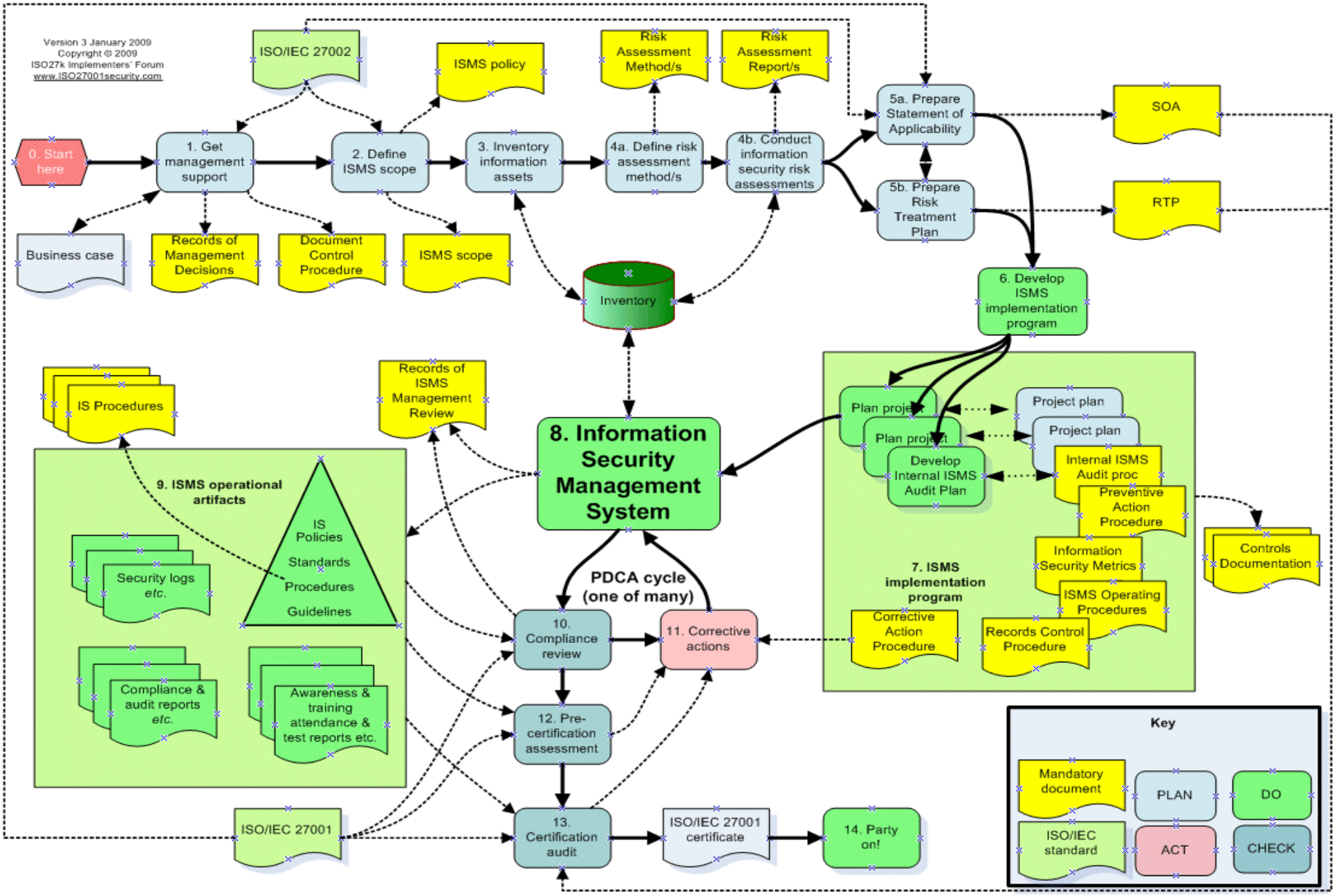
Act: Mantener y mejorar

- Implementar las mejoras identificadas.
- Tomar las acciones correctivas y preventivas apropiadas.
- Comunicar los resultados y acciones a todas las partes interesadas.
- Asegurar que las mejoras logren sus objetivos señalados.

Fases del SGSI



Implementación y certificación



Análisis y Gestión de Riesgos

Análisis de riesgos

- ¿Qué necesito proteger?
  - Recursos físicos: ordenadores, impresoras...
  - Recursos intelectuales: documentos, correo electrónico,...
  - Valoración del tiempo que se perdería ante un ataque o un fallo de los sistemas: tiempo de instalación de los programas, tiempo de recuperación de las copias de seguridad, etc.
  - Cuantificar las pérdidas que un ataque supondría desde el punto de vista de la reputación de la empresa: pérdida de confianza del cliente, imagen de la organización, que también tiene su valor.

Activos

- Activo es aquello que tiene algún valor para la organización y debe protegerse.
- Un activo de información es aquel elemento que contiene o manipula información.
- Deben definirse responsables de la seguridad de cada uno de los activos.

Activos

- ficheros y bases de datos,
- contratos y acuerdos,
- documentación del sistema,
- manuales de los usuarios,
- material de formación,
- aplicaciones,
- software del sistema,
- equipos informáticos,
- equipo de comunicaciones,
- servicios informáticos y de comunicaciones,
- utilidades generales (calefacción, energía, iluminación y aire acondicionado),
- las personas.

¿Qué es Riesgo?

- Riesgo: La posibilidad de que una amenaza explote una vulnerabilidad de un activo y cause su daño o pérdida. Un riesgo representa un problema potencial para el sistema o los usuarios.
- Amenaza: Evento (intencionado o no) que tiene el potencial de dañar a un activo.
- Vulnerabilidad: Una debilidad en el activo que puede ser explotada por una amenaza.

Amenazas

- ¿Quién podría atacar nuestro sistema?
  - Empleados de la propia empresa
  - Personal contratado temporalmente o que esté haciendo consultoría de algún tipo para la empresa
  - Competidores, personas con ideas contrarias a las de la propia empresa o personas con afán de notoriedad…
  - También debemos tener en cuenta las amenazas no intencionadas: por ejemplo, desastres naturales.

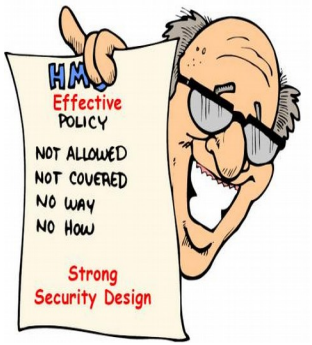
Amenazas

Usuario con grandes conocimientos

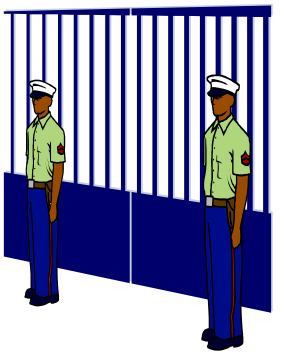
Robo o sabotaje

Virus

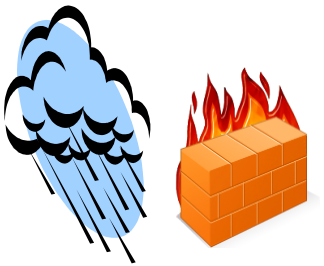
Fallo de red o de sistema



Falta de documentación

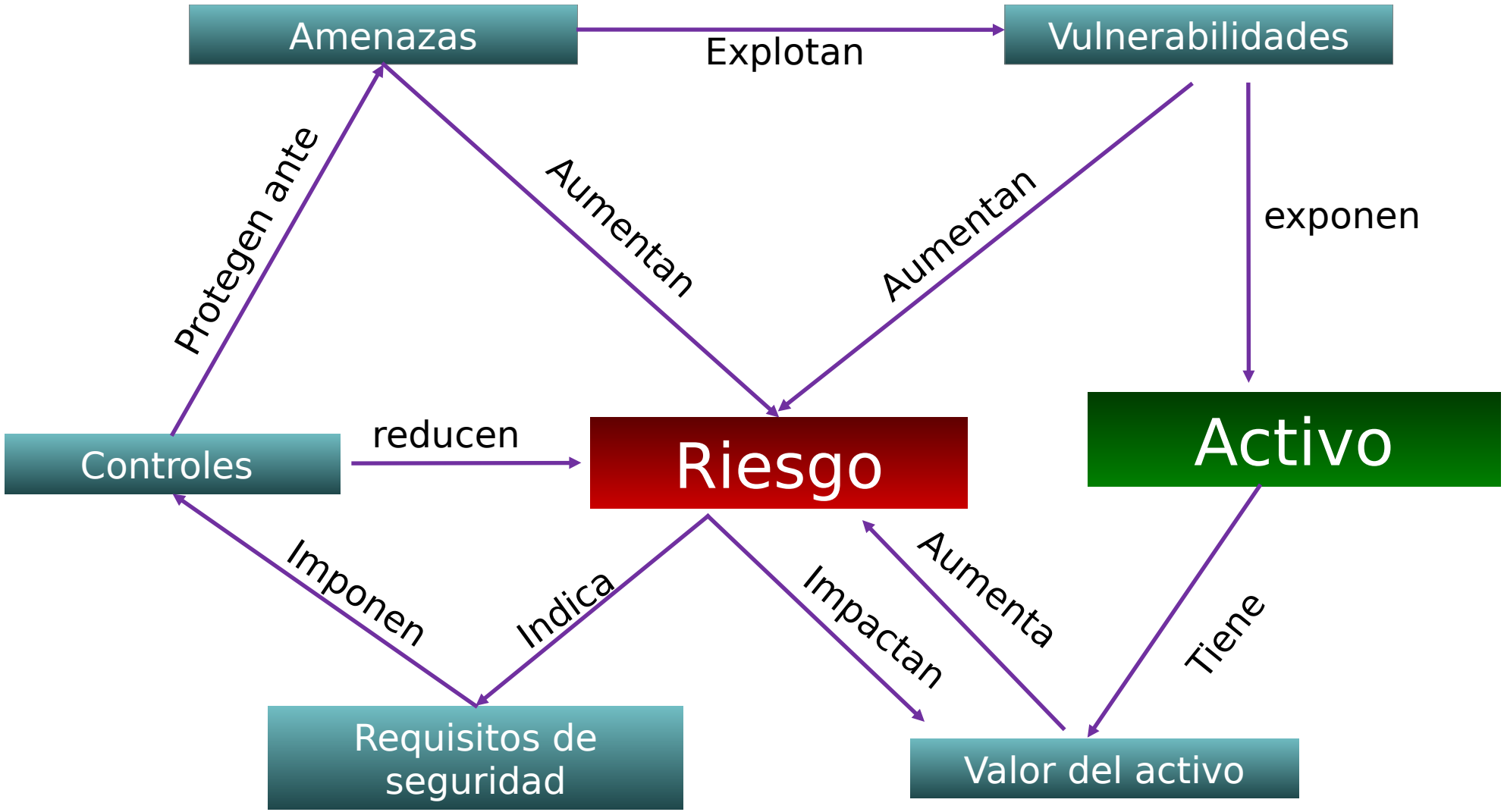


Fallo de seguridad física

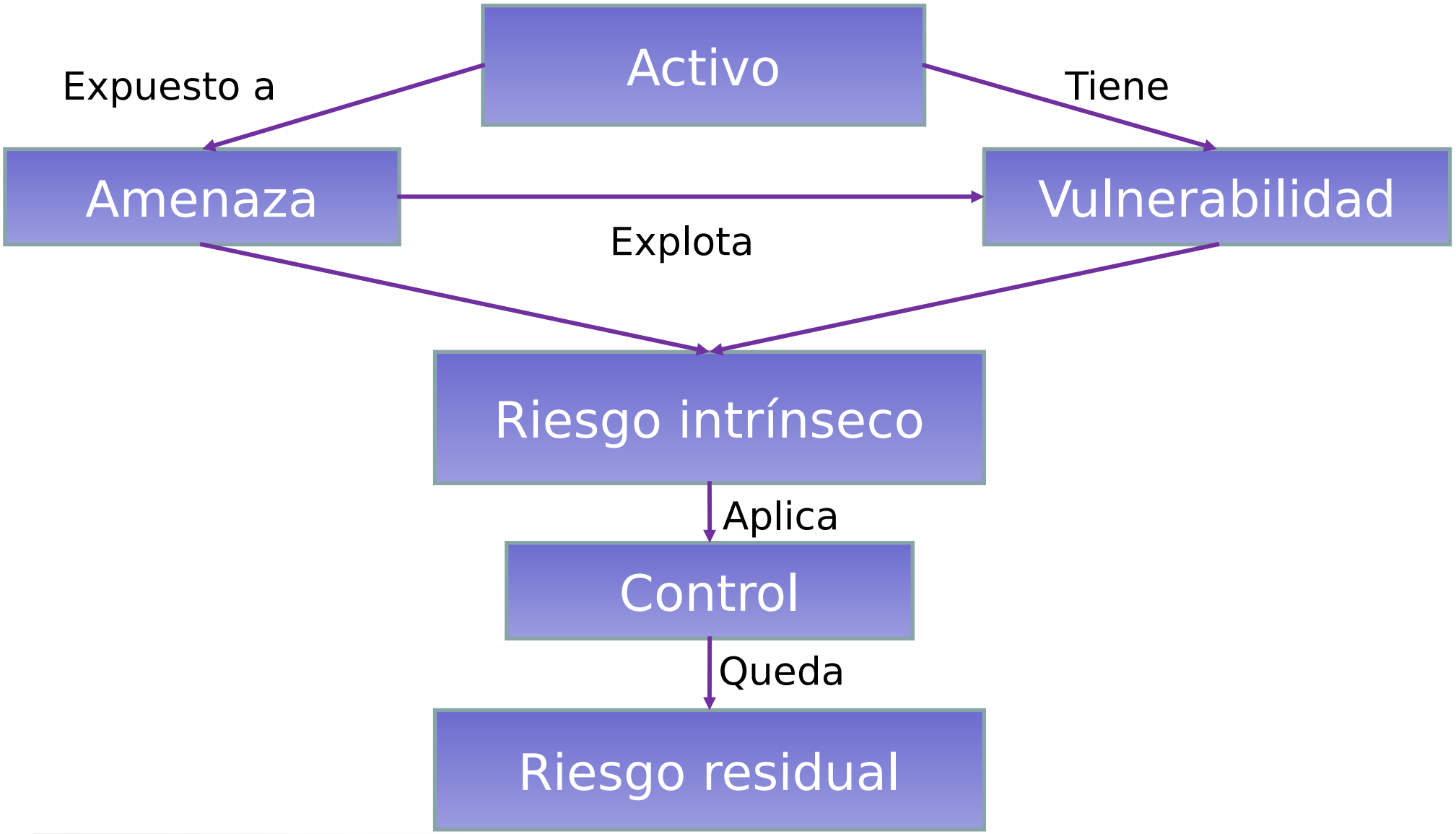


Desastres naturales e incendios

Riesgo


Amenazas
Explotan
Vulnerabilidades
Protegen ante
Aumentan
Aumentan
exponen
Controles
reducen
Riesgo
Activo
Imponen
Indica
Impactan
Aumenta
Tiene
Requisitos de seguridad
Valor del activo

Análisis de Riesgos



Análisis de Riesgos

- ¿Cuál sería el coste inmediato de un ataque?
  - Por coste inmediato se entiende lo que debería afrontar la empresa en los días siguientes al ataque para recuperar su ritmo normal de actividad.
- ¿Cuáles serían los costes de recuperación a largo plazo?
  - Por costes a largo plazo se entienden los derivados del deterioro de la imagen, de la pérdida de clientes, etc.

Análisis de Riesgos

Matriz de valoración del activo

Matriz CIA

	Confidencialidad	**Baja**			**Media**			**Alta**		
	Integridad	**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
Disponibilidad	**Baja**	3	4	5	4	5	6	5	6	7
	Media	4	5	6	5	6	7	6	7	8
	Alta	5	6	7	6	7	8	7	8	9

Análisis de Riesgos

Severidad de amenaza y vulnerabilidad: medir el impacto

Severidad Amenaza		**Baja**			**Media**			**Alta**		
Severidad Vulnerabilidad		**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
Valor del Activo	**3**	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36
	5	5	10	15	10	20	30	15	30	45
	6	6	12	18	12	24	36	18	36	54
	7	7	14	21	14	28	42	21	42	63
	8	8	16	24	16	32	48	24	48	72
	9	9	18	27	18	36	54	27	54	81

Análisis de Riesgos

- ¿Cuál es la probabilidad de un ataque?
  - Valorar los puntos débiles del sistema (vías de acceso desde el exterior, protección perimetral, método de identificación de usuarios, ...).
  - Tener en cuenta los posibles beneficios de un ataque: disponer de datos estadísticos referentes al país, al sector empresarial, etc. que nos ayuden a clarificar esas probabilidades

Análisis de Riesgos

Probabilidad de ocurrencia		
Valor	**Explicación**	**Ejemplo**
1	Nunca	No en los últimos 3 años
2	Raro	Una vez al año
3	Periódico	Una vez por trimestre
4	Regular	Una vez cada 15 días
5	Frecuente	Una vez a la semana

Impacto = (Valor tabla severidad vulnerabilidad y amenaza) x probabilidad

SEVERIDAD DE AMENAZA Y VULNERABILIDAD		IMPACTO DEL RIESGO				
	PROBABILIDAD	1	2	3	4	5
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25
	6	6	12	18	24	30
	7	7	14	21	28	35
	8	8	16	24	32	40
	9	9	18	27	36	45
	10	10	20	30	40	50
	12	12	24	36	48	60
	14	14	28	42	56	70
	16	16	32	48	64	80
	18	18	36	54	72	90
	20	20	40	60	80	100
	21	21	42	63	84	105
	24	24	48	72	96	120
	27	27	54	81	108	135
	28	28	56	84	112	140
	30	30	60	90	120	150
	32	32	64	96	128	160
	36	36	72	108	144	180
	42	42	84	126	168	210
	45	45	90	135	180	225
	48	48	96	144	192	240
	54	54	108	162	216	270
	63	63	126	189	252	315
	72	72	144	216	288	360
	81	81	162	243	324	405

Análisis de Riesgos

Resultado final: medida mucho más precisa de la probabilidad de que la empresa sufra determinados tipos de ataque, y del coste que cada uno de ellos supondría para la empresa.

Siguiente etapa: respuesta a la pregunta…

Análisis de Riesgos

- ¿Cómo puedo proteger de manera efectiva el sistema?
  - Efectiva: el coste de los sistemas de protección a instaurar debe ser inferior a las posibles pérdidas derivadas de un ataque.
  - En ciertas situaciones el experto podría valorar la posibilidad de contratar un seguro que cubriese ese tipo de incidentes, si resultase económicamente rentable.
  - También hay que tener muy en cuenta los requisitos legales a los que pueda estar sometida la empresa.

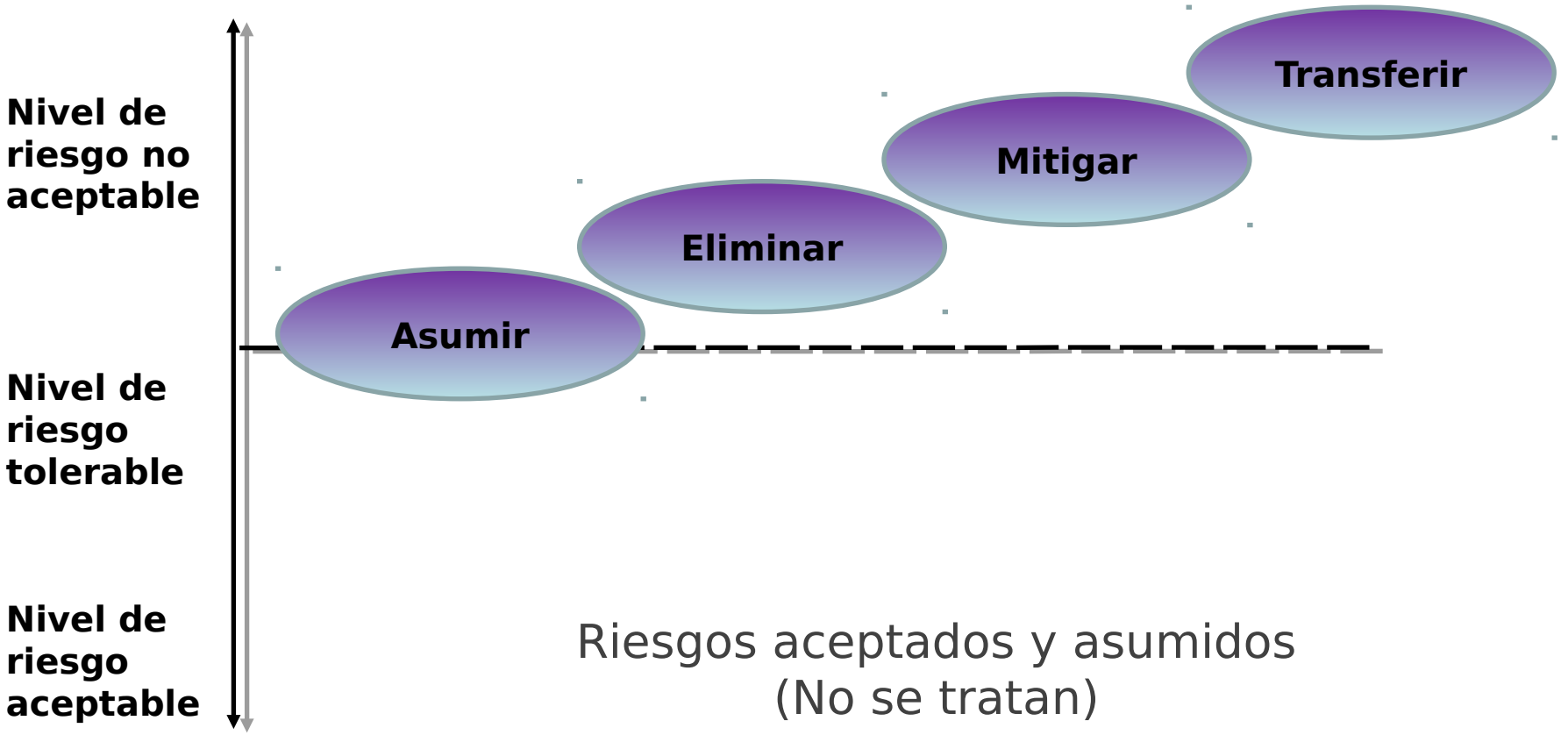
Los resultados del análisis de riesgos, así como la propuesta de arquitectura de seguridad para minimizar esos riesgos deberían estar recogidos en un **documento**.

Análisis de Riesgos

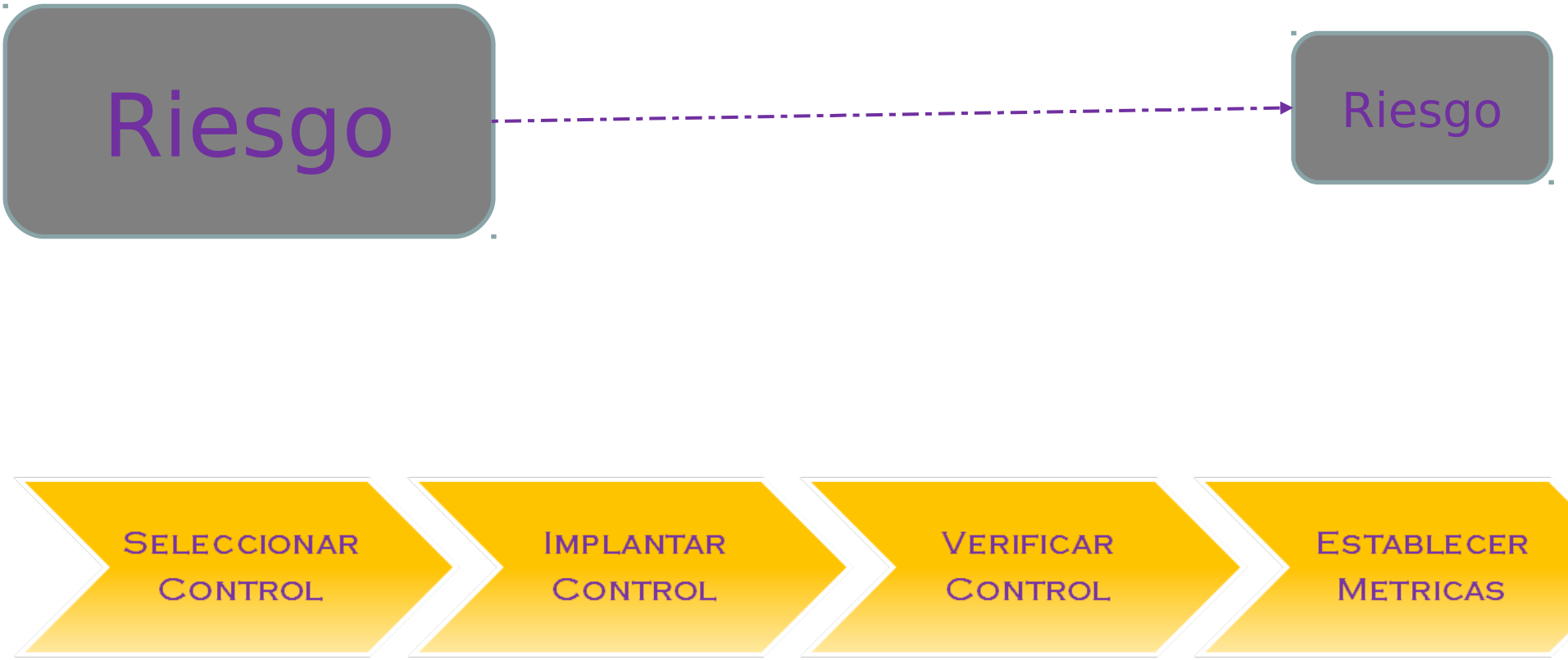
- ¿Cómo puedo proteger de manera efectiva el sistema?

Item	Amount
Risks: disclosure of company confidential data, computation based on incorrect data	
Cost to reconstruct correct data: $1,000,000 @ 10% likelihood per year	$100,000
Effectiveness of access control software: 60%	– 60,000
Cost of access control software	+25,000
Expected annual costs due to loss and controls (100,000 – 60,000 + 25,000)	$65,000
Savings (100,000 – 65,000)	$35,000

Tratamiento del Riesgo



Mitigar riesgos



Declaración de intenciones de la dirección

- Durante el análisis de riesgos realizado en (Mes) del (Año) se propusieron unos cursos de acción con el fin de implantar un nivel de seguridad aceptable. La dirección se compromete a llevar a cabo uno de los cursos de acción en un período inferior a X años.

La Dirección

Plan director de seguridad

- *Fase 1: Diagnóstico de la situación*
  - *Conocer la organización, áreas funcionales y procesos de negocio*
  - *Identificar activos, realizar entrevistas*
  - *Evaluar la seguridad de comunicaciones, sistemas, aplicaciones*
- *Fase 2: Análisis de riesgos*
  - *Análisis de las amenazas y vulnerabilidades*
  - *Identificación, cálculo y clasificación de los riesgos*
- *Fase 3: Grado de cumplimiento ISO 27001*
  - *Informe de cumplimiento de cada uno de los capítulos*
- *Fase 4: Plan de proyectos de seguridad*
  - *Agrupar las vulnerabilidades y definir proyectos a acometer*
  - *Clasificar y valorar proyectos a corto, medio y largo plazo*
- *Fase 5: Gestión de los riesgos*
  - *Disminuir con proyectos, externalizar con seguros o asumir.*

Metodologías

- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: MAGERIT Versión 3 (Portal de Administración Electrónica)

http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_metodos_instrumentos_y_normas.htm