UNIVERSITAT POLITÈCNICA DE VALÈNCIA

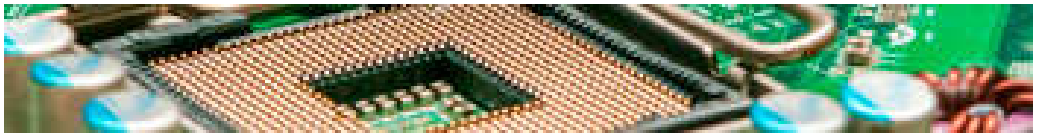
etsinf

Máster Universitario en Ingeniería Informática

Asignatura: Gestión y Gobierno de TI

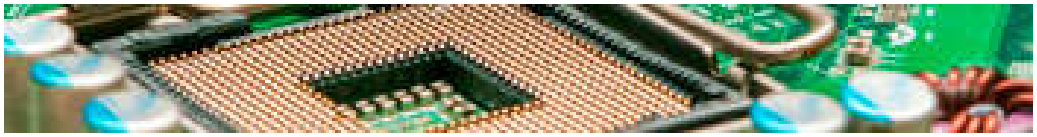
Máster Oficial Universitario en Ingeniería Informática
muiinf.webs.upv.es

MUIInf



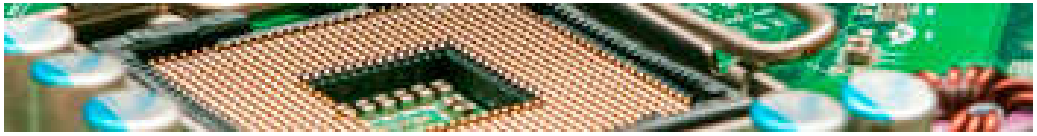
Gestión de riesgos

- **Elementos fundamentales del riesgo**
  - Activos
  - Amenazas
  - Salvaguardas
  - Probabilidad
  - Impacto
  - Riesgo



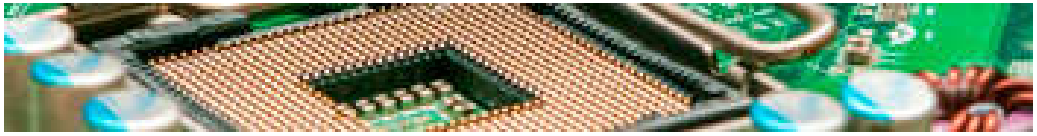
Activos

- Los activos de la **empresa**
  - Un activo es un bien que la empresa posee y que puede convertirse en dinero u otros medios líquidos equivalentes.
- Los activos de un **Sistema de Información**
  - Recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objetivos propuestos por su dirección.
  - El activo esencial es la información o dato.
- Los activos de un **proyecto**
  - Tareas
  - Recursos



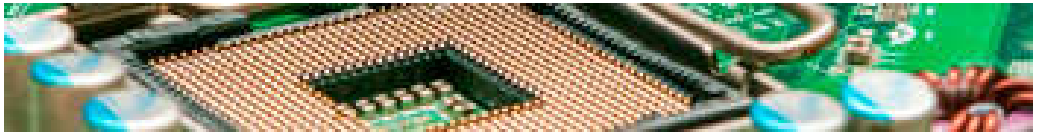
Activos

- **Activos clave en la gestión de proyectos**
  - Las organizaciones tienen un conjunto de activos clave en la gestión de proyectos que se deben cuidar y atesorar como un valor dentro de la compañía. En ocasiones las organizaciones no son conscientes de la importancia de estos activos, aunque son la base de muchas de sus ventajas competitivas.
  - Se trata de los planes, procesos, políticas, procedimientos y bases de conocimiento específicos que son utilizados a lo largo de los proyectos por parte de la organización. Incluye cualquier objeto, práctica o conocimiento, así como bases de conocimiento de la organización que pueden usarse a la hora de ejecutar o gobernar el proyecto.



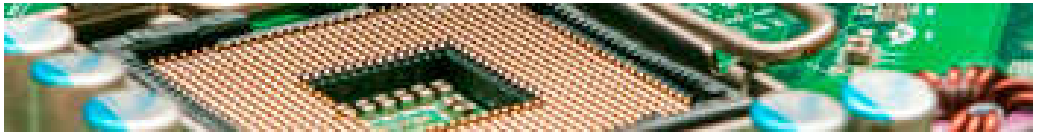
Amenazas

- La amenaza es un evento que puede desencadenar incidentes en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- La amenaza, si se materializa como agresión, modifica el estado de seguridad de los activos en cuestión.
- Lo que realmente contará es la agresión, es decir la amenaza materializada.

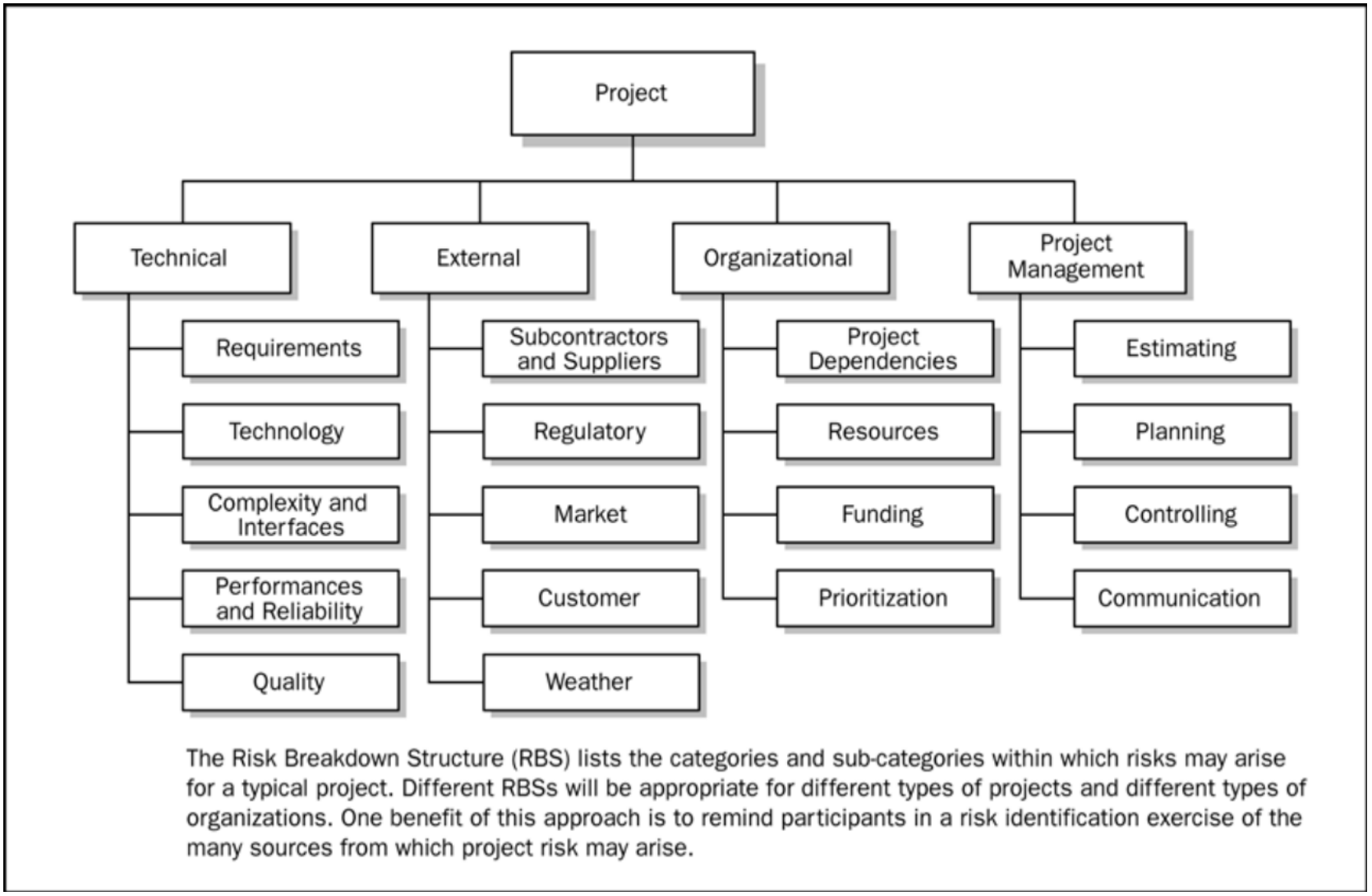


Amenazas

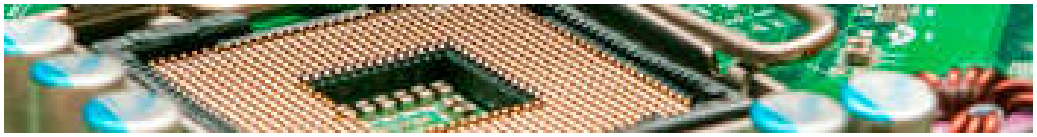
- **¿Cómo clasificar las amenazas?**
  - No se conoce la forma ideal.
    - Por grupos de activos
    - Por impacto
      - Plazo
      - Coste
      - Funcionalidad
    - En base al agente causante
      - Escenarios de ataque
      - Natural, accidental, deliberado
    - Por la propia naturaleza de la amenaza
      - Accidentes, amenazas deliberadas



Ejemplo de RBS (PMBoK)

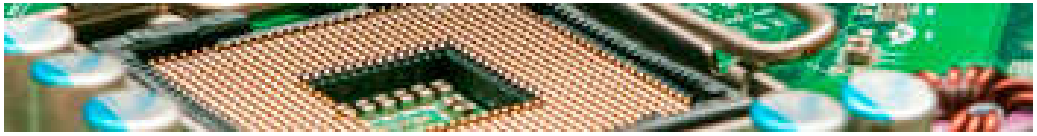


The Risk Breakdown Structure (RBS) lists the categories and sub-categories within which risks may arise for a typical project. Different RBSs will be appropriate for different types of projects and different types of organizations. One benefit of this approach is to remind participants in a risk identification exercise of the many sources from which project risk may arise.



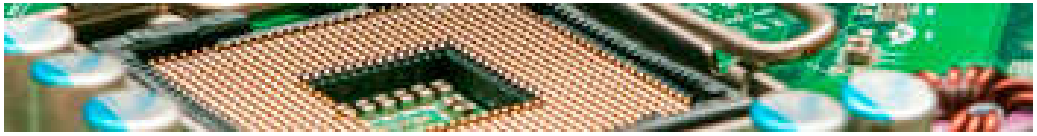
Ejemplo de RBS (Magerit)

- Grupo **A** de **Accidentes**
  - Accidente físico de origen natural o industrial
  - Accidente mecánico o electromagnético
  - Avería
  - Interrupción de servicios o de suministros esenciales
- Grupo **E** de **Errores**
  - Errores de diseño
  - Errores de utilización
  - Errores de ruta, secuencia o entrega de la información en tránsito
  - Inadecuación de la monitorización del tráfico de información



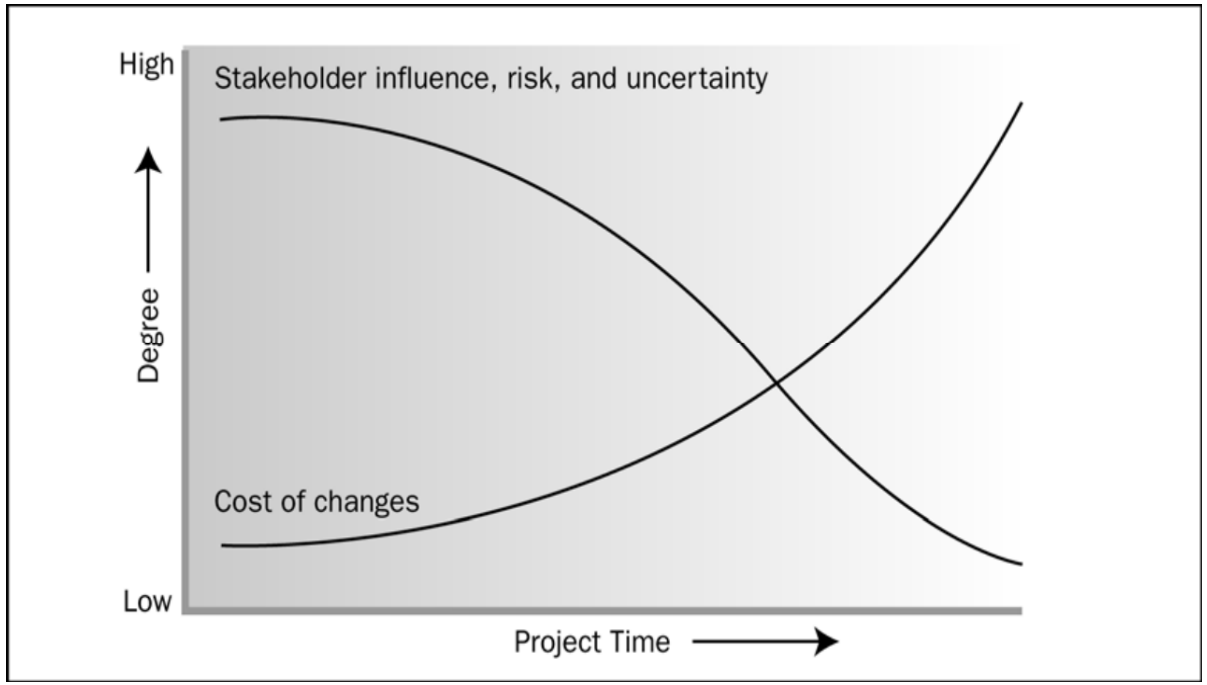
Ejemplo de RBS (Magerit)

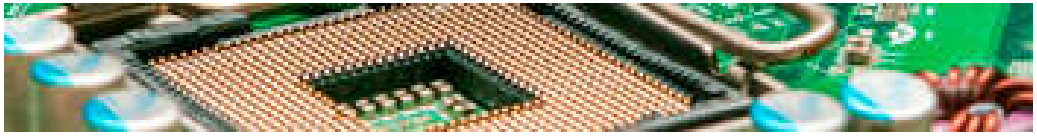
- Grupo **P** de amenazas intencionales **Presenciales**
  - Acceso físico o lógico no autorizado
  - Indisponibilidad de recursos humanos o técnicos
- Grupo **T** de **Tele-amenazas** (intencionales)
  - Acceso lógico no autorizado
  - Suplantación de la identidad del emisor
  - Repudio de la recepción de información



Evolución de las amenazas

- Durante el proyecto, los riesgos evolucionan:
  - Aparecen nuevos
  - Desaparecen algunos
  - Cambia la probabilidad o el impacto de los que permanecen
- Por ello, una buena gestión del riesgo requiere una adaptación permanente.





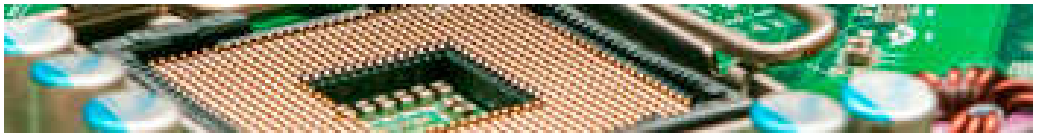
Amenazas "3 I"

Interna, intencionada, inteligente

"*Olvídese de hackers, virus, desastres naturales y todo lo demás que pueda causar daños a sus sistemas de información. Son sus empleados quienes deben preocuparle más. La gran mayoría de las brechas de seguridad informática son causadas por los propios empleados. Las formas en que los empleados son capaces de explotar o sabotear los sistemas informáticos de la organización se multiplican rápidamente: usan la información y los sistemas informáticos de las compañías para iniciar sus propios negocios, para vengarse de compañeros de trabajo, para realizar actividades ilegales o para causar cualquier otro problema. Las compañías que se conecten a Intemet se encontrarán con que sus infortunios en materia de seguridad crecerán de forma inesperada.*"

The Real Security Threat: The Enemy Within.

Michael Alexander, 1995



Aspects of risk (Prince2)

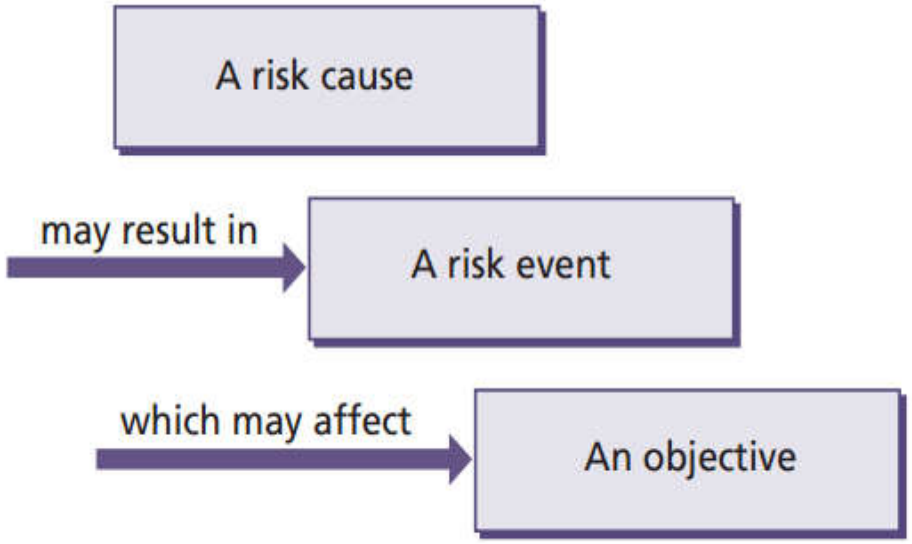
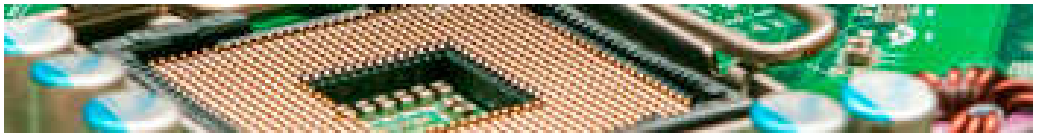
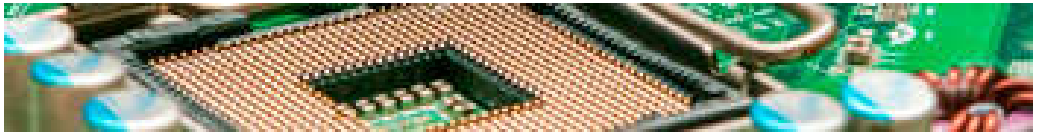


Figure 8.4 Risk cause, event and effect



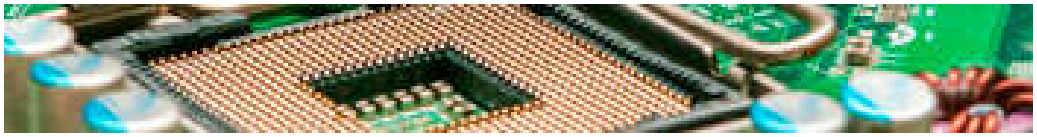
Examples of aspects of risk

- **Threat**
  - Because it has been raining heavily (risk cause), there is a threat that the river flowing through the farmer's field might overflow (risk event), which would severely damage the farmer's crop (risk effect)
- **Opportunity**
  - Because the weather has been particularly mild this winter (risk cause), there is an opportunity that fewer people will be hospitalized with influenza (risk event), which will mean that there will be less disruption to planned routine operations (risk effect).



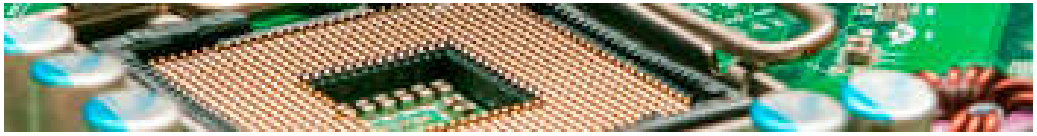
Aspectos del riesgo

Causa del riesgo	Evento del riesgo	Efecto del riesgo
Maquinaria mal colocada	Tropiezos y caídas	Lesiones corporales y fracturas
Planificación inadecuada	Sobrecarga de trabajo	Agotamiento del empleado
No uso de los equipos de protección personal	Exposición a materiales tóxicos o radioactivos	Congestión pulmonar, intoxicación, asfixia
El proveedor completa la orden de pedido antes del periodo acordado	Entrega temprana de los materiales	Adelanto de la tarea implicada
Falta de medidas de seguridad adecuadas	Robo de material	Resolicitud de aprovisionamiento de materiales
Cambio de las políticas gubernamentales de medio ambiente	Análisis del impacto medio ambiental obsoleto	Retraso en al aprobación de permisos y licencias
Quiebra del proveedor habitual	Cambio de proveedor	Aumento/Descenso del precio de los materiales
Almacenamiento inadecuado del material	Abolladuras, corrosión y daños generales en los materiales	Resolicitud de aprovisionamiento de materiales
Cambio de las políticas gubernamentales en perjuicio de los trabajadores	Huelga	Equipo de trabajo reducido
Mala gestión de las comunicaciones en el proyecto	Conflictos en el equipo de trabajo	Reasignación de recursos

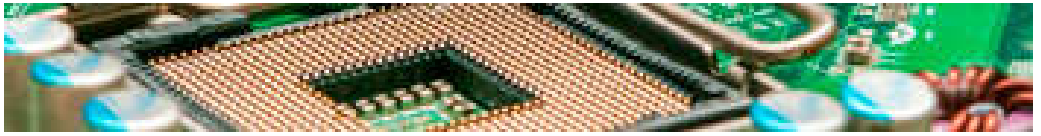


Amenazas

- **Continuidad del negocio:** Continuidad referida al negocio, a sus funciones; requiere la disponibilidad de la información y por tanto de los sistemas que la tratan y su entorno (suministros, etc.).
  - **Incidencia:** Evento que interrumpe la continuidad de los sistemas, con consecuencias limitadas para el negocio; puede reducirse por medios razonables y en general disponibles; se habla de registro de incidencias.
  - **Contingencia:** Evento que interrumpe la continuidad de los sistemas, con consecuencias catastróficas para el negocio; sólo puede reducirse por medios extraordinarios y en general muy costosos, organizativa y técnicamente; se habla de plan de contingencias.

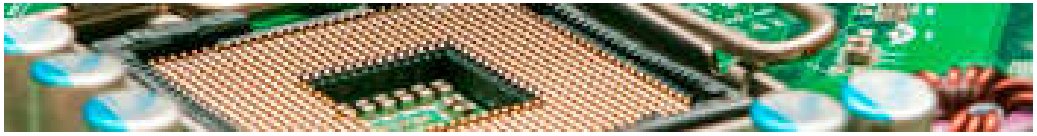


Amenaza u oportunidad



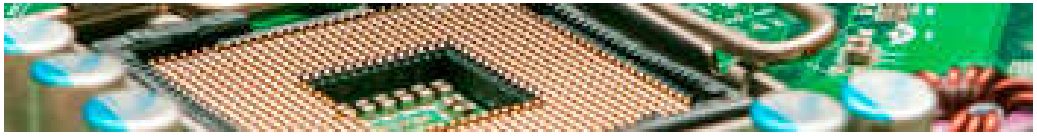
Salvaguardas

- Una salvaguarda es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado por estas.
- Actúa de dos formas posibles, en general alternativas:
  - Neutralizando o bloqueando la materialización de la Amenaza antes de ser agresión
  - Mejorando el estado de seguridad del Activo ya agredido, por reducción del Impacto.
- En proyectos se suele hablar de la **respuesta a los riesgos**.

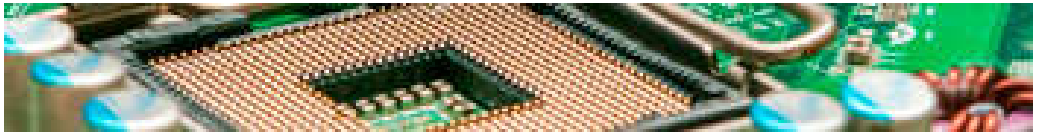


Estrategias de defensa

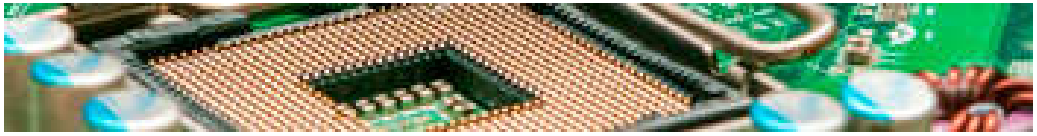
Estrategias de defensa



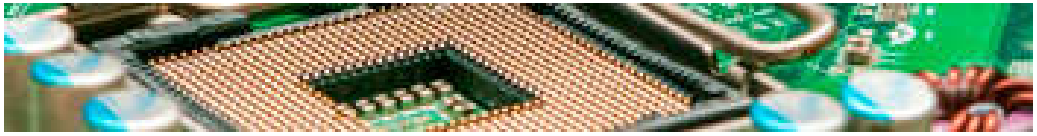
Estrategias de defensa



Estrategias de defensa

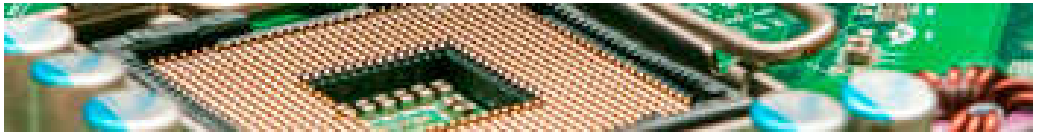


Estrategias de defensa



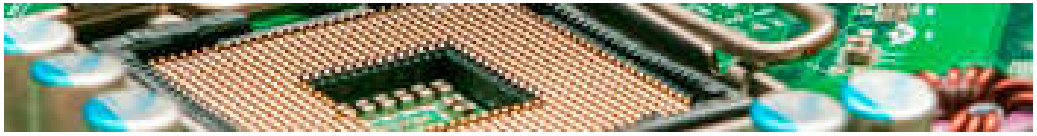
Respuestas (Prince2)

Threat responses	Opportunity responses
Avoid	Exploit
Reduce (probability and/or impact) Fallback (reduces impact only) Transfer (reduces impact only, and often only the financial impact)	Enhance
Share	
Accept	Reject



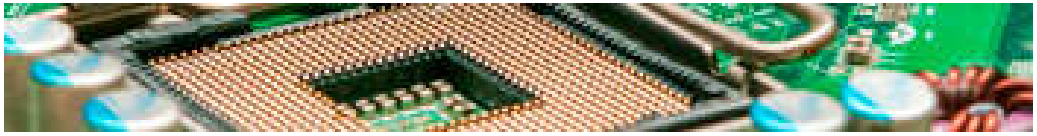
Threat responses

Avoid (threat)	Typically involves changing some aspect of the project, i.e. the scope, procurement route, supplier or sequence of activities, so that the threat either can no longer have an impact or can no longer happen.	A critical meeting could be threatened by air travel disruption so the project chooses to hold the meeting by conference call instead.
Reduce (threat)	Proactive actions taken to: ■ Reduce the probability of the event occurring, by performing some form of control ■ Reduce the impact of the event should it occur.	To reduce the likelihood of users not using a product, the number of training events is increased. To reduce the timescale impact should a prototype be damaged in transit, two prototypes are built.
Fallback (threat)	Putting in place a fallback plan for the actions that will be taken to reduce the impact of the threat should the risk occur. This is a reactive form of the 'reduce' response which has no impact on likelihood.	The company's test facility is only available for two weeks in August. To reduce the impact should the product not be available in time, there is a fallback plan to hire an alternate test facility (at a greater expense).



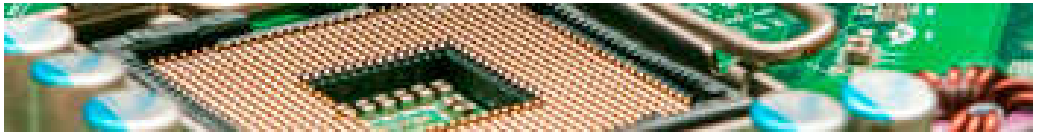
Threat responses

Transfer (threat)	A third party takes on responsibility for some of the financial impact of the threat. (For example, through insurance or by means of appropriate clauses in a contract.) This is a form of the 'reduce' response which only reduces the financial impact of the threat.	To reduce the financial impact should a prototype be damaged in transit, it is insured. To reduce the financial impact if a product is not available to launch in time for a trade show, the contract with the supplier includes liquidated damage clauses for any delays.
Accept (threat)	A conscious and deliberate decision is taken to retain the threat, having discerned that it is more economical to do so than to attempt a threat response action. The threat should continue to be monitored to ensure that it remains tolerable.	There is a threat that a competitor may launch a rival product first, thus affecting the expected market share for the product. The choice is to accelerate the project by increasing the resources, to reduce the product's scope so that it can be finished earlier, or to do nothing. Accelerating the project may lead to product quality issues; reducing the scope may make the product less appealing; so the risk is accepted and the 'do nothing' option is chosen.



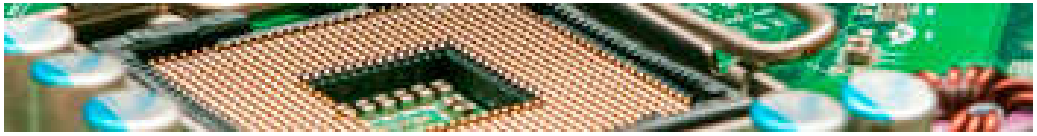
Opportunity responses

Exploit (opportunity)	Seizing an opportunity to ensure that the opportunity **will** happen and that the impact **will** be realized.	There is a risk that the project will be delayed. If it is delayed, a later version of software could be implemented instead which would reduce ongoing maintenance. The Project Board agree to change the project timescale and scope, enabling the later version of the software to be bought and implemented.
Enhance (opportunity)	Proactive actions taken to: ■ Enhance the probability of the event occurring ■ Enhance the impact of the event should it occur.	It is possible that the product completes user acceptance testing in a single test cycle, rather than the scheduled two, enabling it to be delivered early and prior to a competitor's rival product. The Project Board decide to hold a test rehearsal to increase the likelihood that the product will pass its first user acceptance tests, and prepare for the option of an earlier launch date.



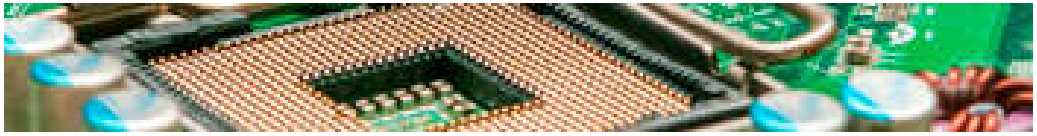
Opportunity responses

Reject (opportunity)	A conscious and deliberate decision is taken not to exploit or enhance the opportunity, having discerned that it is more economical not to attempt an opportunity response action. The opportunity should continue to be monitored.	It is possible that the product completes user acceptance testing in a single test cycle, rather than the scheduled two, enabling it to be delivered early and prior to a competitor's rival product. The Project Board decide not to take advantage of an early release and to stick with the planned launch date.



Threat / Opportunity responses

Share (threat or opportunity)	Modern procurement methods commonly entail a form of risk sharing through the application of a pain/gain formula: both parties share the gain (within pre-agreed limits) if the cost is less than the cost plan; and share the pain (again within pre-agreed limits) if the cost plan is exceeded. Several industries include risk-sharing principles within their contracts with third parties.	The cost of the project could be adversely affected due to fluctuations in the cost of oil. The customer and supplier agree to share the cost of price increases or the savings from price reductions equally from a midpoint fixed at the time of agreeing the contract.



Análisis de coste / beneficio

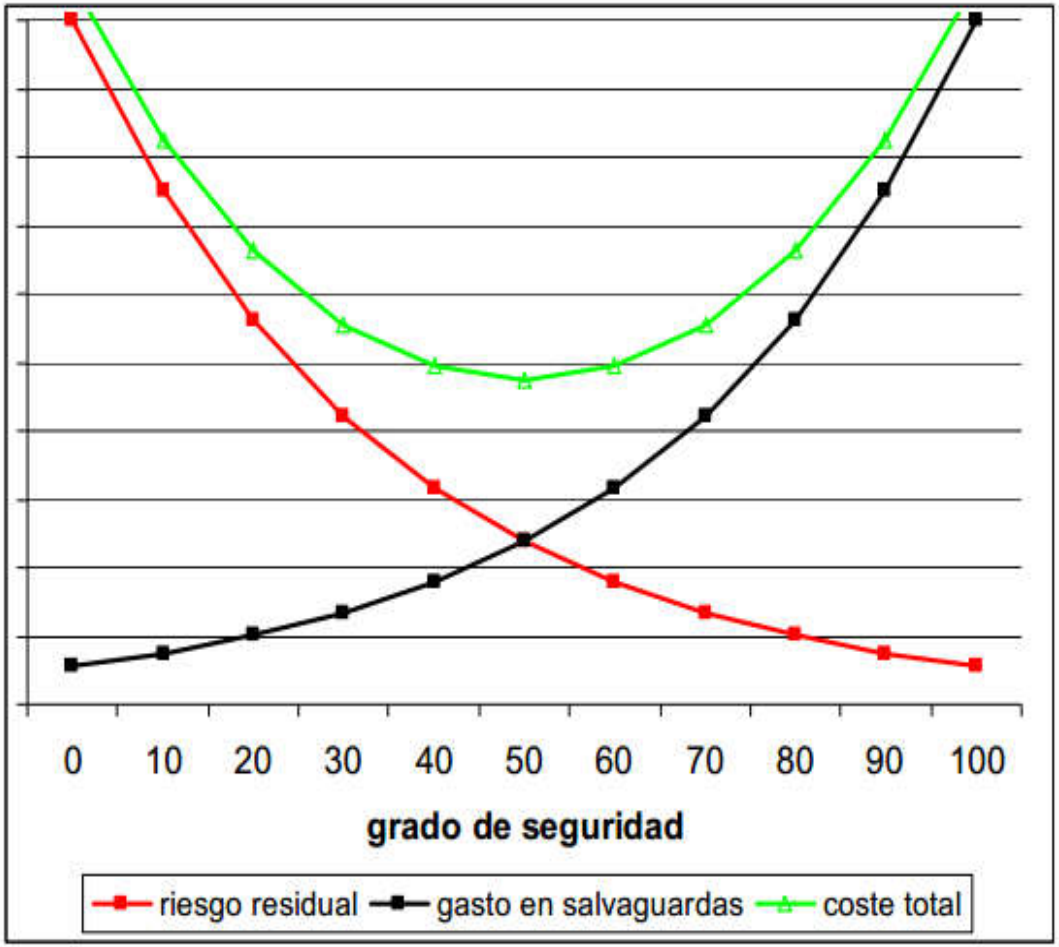
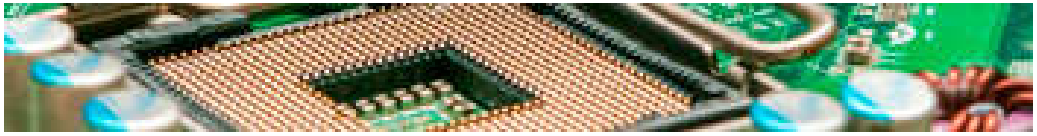
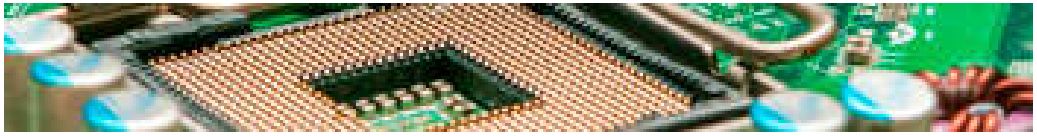


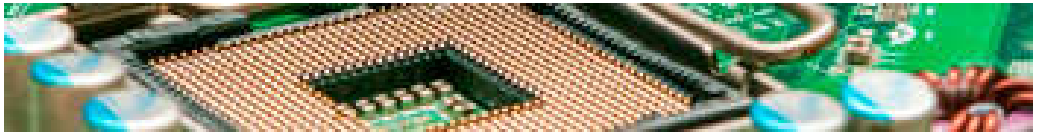
Ilustración 13. Relación entre el gasto en seguridad y el riesgo residual



Sobre protección

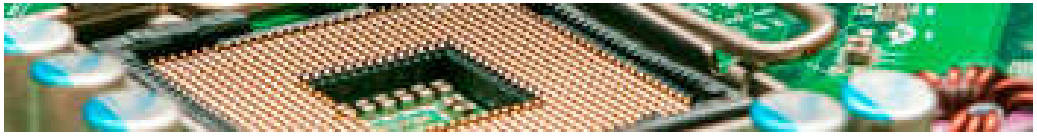


Falsa sensación de seguridad



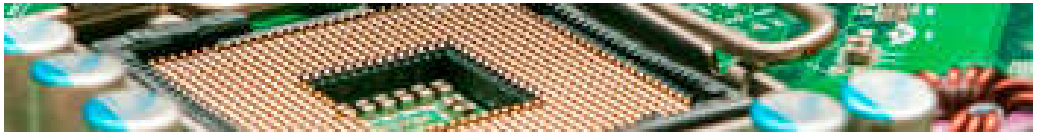
Probabilidad

- **Definición**
  - **Potencialidad de ocurrencia de la materialización de una amenaza sobre un activo:**
    - **Frecuencia** para los casos de **calculabilidad definida**
    - **Posibilidad** para los casos de **calculabilidad difusa**
  - La vulnerabilidad es una propiedad de relación entre activo y amenaza.



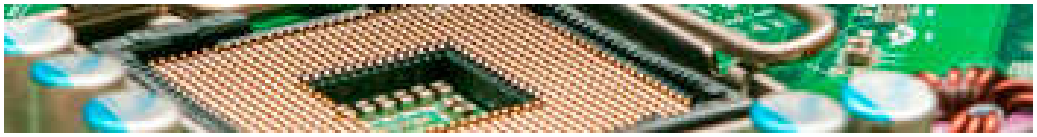
- **Métrica**
  - La métrica de la vulnerabilidad consiste en considerar la distancia entre la amenaza (potencial) y su materialización como agresión (real) sobre el activo.
  - La vulnerabilidad se mide como frecuencia o **Tasa Anual de Ocurrencia ARO.**

Periodo medio entre ocurrencias	Escala subjetiva	Escalas objetivas	
		Por día	Por año
Inferior a 1 semana	Frecuencia muy alta	0.2	50
Inferior a 2 meses	Frecuencia alta	0.02	5
Inferior a 1 año	Frecuencia media	0.002	1
Inferior a 6 años	Frecuencia baja	0.0002	0.0
Superior a 6 años	Frecuencia muy baja	0	0.002



Impacto

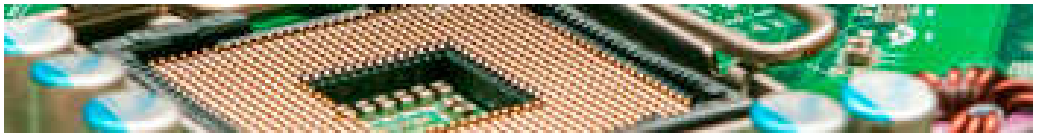
- **Definición**
  - **Consecuencia sobre el activo de la materialización de una amenaza**
  - El impacto es la diferencia en las estimaciones del estado de seguridad del activo obtenidas antes y después de la agresión o materialización de la amenaza sobre este.



Impacto

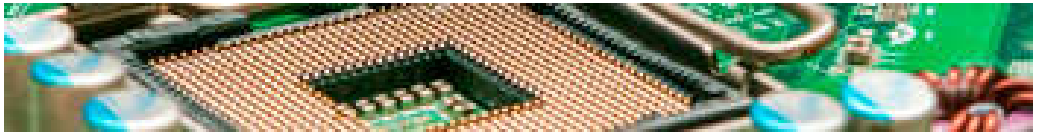
- **Métrica**
  - La cuantificación de los impactos es no sólo uno de los procesos más difíciles del análisis de riesgos, sino que es el más influyente en el cálculo del propio riesgo.
  - El impacto se mide como **Tasa (Rate) Anual de Impacto ARI.**

Rango de valores en euros	**Impacto**
Inferior a 1.000	Muy bajo
Inferior a 10.000	Bajo
Inferior a 100.000	Medio
Inferior a 1.000.000	Alto
Superior a 1.000.000	Muy alto



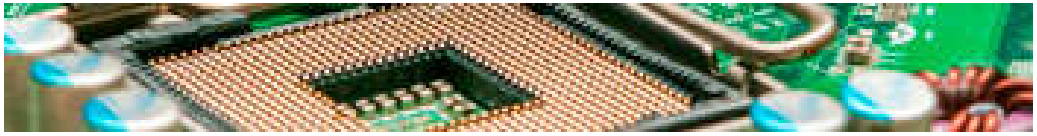
Riesgo

- **Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización**
- Resultado del análisis de riesgos para obtener un valor calculado de riesgo que permita tomar decisiones, por comparación explícita del riesgo calculado con un nivel prefijado de riesgo o umbral de riesgo



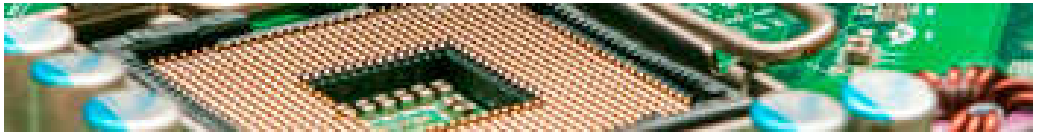
Distintos tipos de riesgos

- Riesgo intrínseco
  - Es el riesgo calculado antes de aplicar salvaguardas: situación hipotética
  - Riesgo potencial, usado como valor de referencia
- Riesgo efectivo
  - Es el riesgo calculado después de aplicar **salvaguardas existentes**: situación real
  - Riesgo real
  - Riesgos efectivo <= Riesgo intrínseco
- Riesgo residual
  - El que resulta tras la aplicación de **salvaguardas propuestas** dispuestas en un escenario de simulación o en el mundo real.

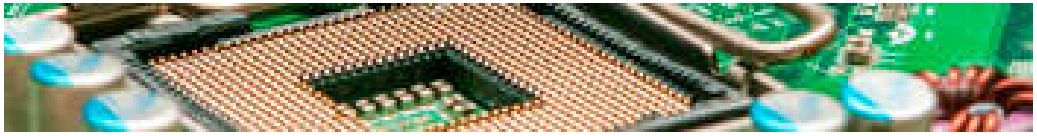


Umbral de riesgo

- Riesgo asumido, aceptado, tolerado
- Se define como el valor establecido como base para decidir por comparación si el riesgo calculado es asumible, aceptable o tolerable.
  - Un riesgo efectivo superior al umbral implica una decisión de reducción de riesgo.
  - Un riesgo efectivo inferior al umbral queda como riesgo residual que se considera asumible o aceptable.



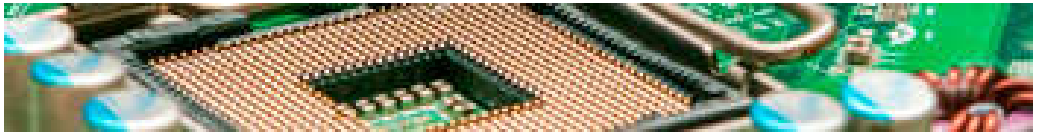
Risk tolerance



Short Risk Questionnaire

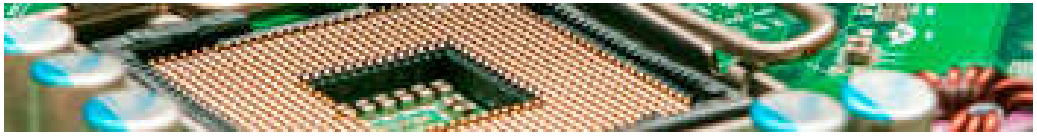
PROJECT NAME — **SHORT RISK QUESTIONNAIRE**

Product / System Risk						
1. Overall System / Service / Product		Simple		Average		Complex
2. Logical Data Model		"		"		"
3. Interface to other systems / services / products		"		"		"
4. Function and processes		"		"		"
5. New business procedures / alterations		None		Some		Extensive
6. Stability of requirements		Stable		Average		Unstable
7. Performance requirements		Low		Medium		High
8. Technology requirements		Simple		Average		Complex
9. Level of innovation		None		Some		Extensive
Team Risk						
10. Intrinsic team skills (general skills)		High		Average		Low
11. Relevant skill level (with application / product)		Extensive		Some		None
12. Project manager experience		Extensive		Some		None
13. Project staffing level		1 to 4		5 to 10		Over 10
14. Use of contractors / part-time team members		None		Some		Extensive
15. Project development length		1 to 3 mth		4 to 6 mth		Over 6 mth
16. Schedule / deadline		Flexible		Firm		Fixed
17. Priority of project for team		High		Medium		Low
18. Team experience with hardware / technology		Extensive		Average		Some
19. Project team physical / support environment		Excellent		Average		Poor
Environment / Targt Risk						
20. Level of client / user support		High		Medium		Low
21. Client experience with product / system		Extensive		Some		None
22. Client / Project Sponsor support		High		Medium		Low / None
23. Impact on client / user operations (new technology, policy)		Low		Medium		High
24. Client / business expert participation		Full-time		Part-time		Ad-hoc
25. Critical stakeholders		1 to 3		4 to 10		More than 10
OVERALL PROJECT RISK	☐	**LOW**	☐	**MEDIUM**	☐	**HIGH**



Matriz del riesgo cualitativa

Matriz del RIESGO		VULNERABILIDAD			
		muy baja	baja	media	fuerte
IMPACTO	Crítico	Alto	Crítico	Crítico	Crítico
	Grave	Medio	Alto	Alto	Crítico
	Medio	Bajo	Bajo	Medio	Medio
	Bajo	Bajo	Bajo	Bajo	Bajo



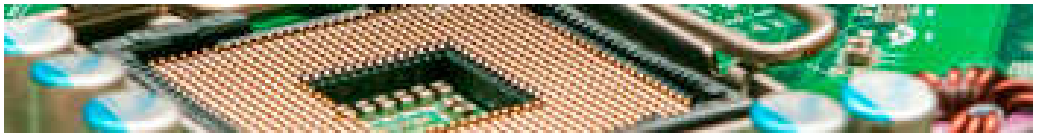
Matriz del riesgo cuantitativa

Probability and Impact Matrix

Probability	Threats					Opportunities				
0.90	0.05	0.09	0.18	0.36	0.72	0.72	0.36	0.18	0.09	0.05
0.70	0.04	0.07	0.14	0.28	0.56	0.56	0.28	0.14	0.07	0.04
0.50	0.03	0.05	0.10	0.20	0.40	0.40	0.20	0.10	0.05	0.03
0.30	0.02	0.03	0.06	0.12	0.24	0.24	0.12	0.06	0.03	0.02
0.10	0.01	0.01	0.02	0.04	0.08	0.08	0.04	0.02	0.01	0.01
	0.05	0.10	0.20	0.40	0.80	0.80	0.40	0.20	0.10	0.05

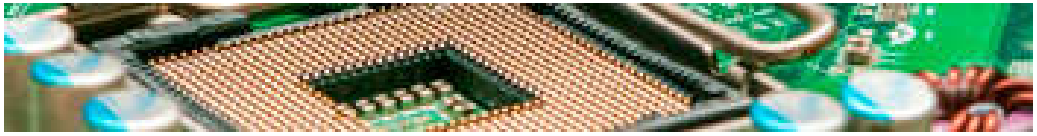
Impact (relative scale) on an objective (e.g., cost, time, scope or quality)

Each risk is rated on its probability of occurring and impact on an objective if it does occur. The organization's thresholds for low, moderate or high risks are shown in the matrix and determine whether the risk is scored as high, moderate or low for that objective.

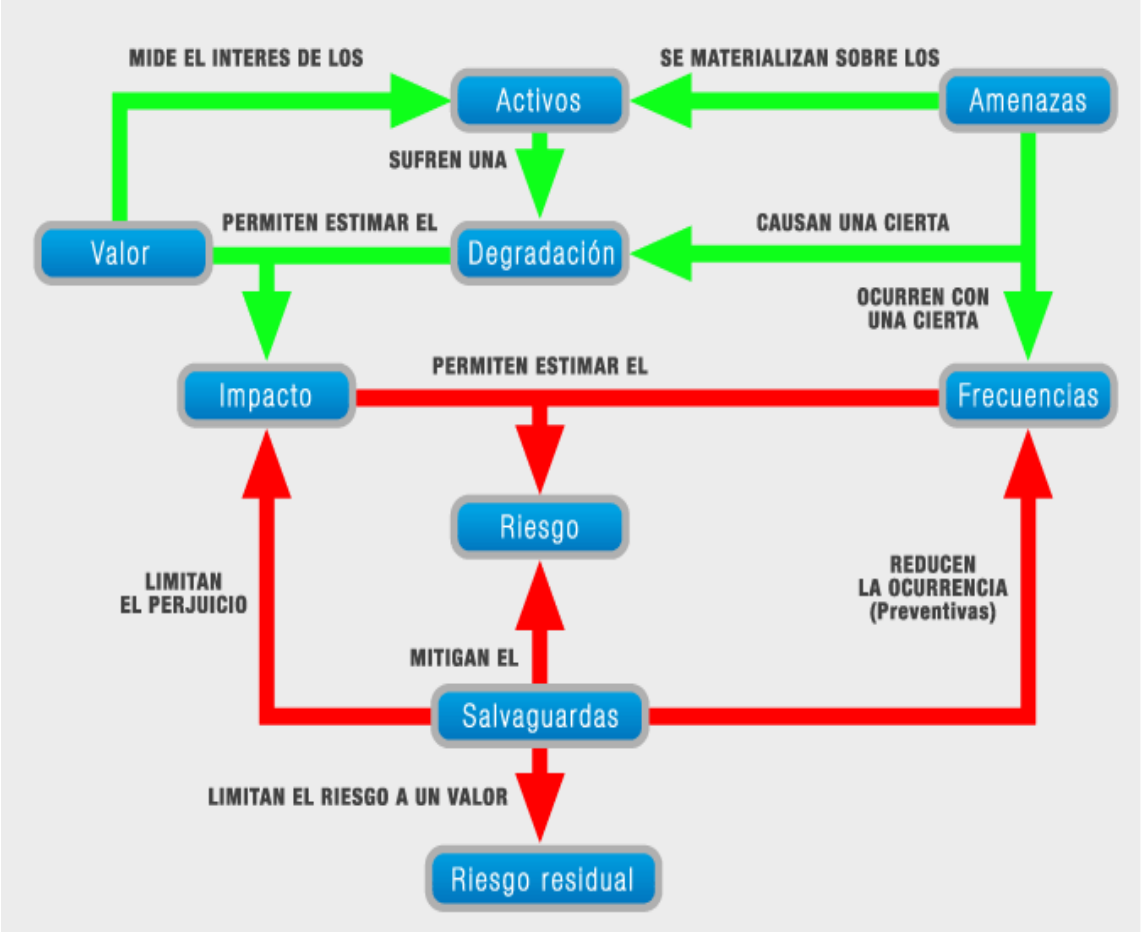


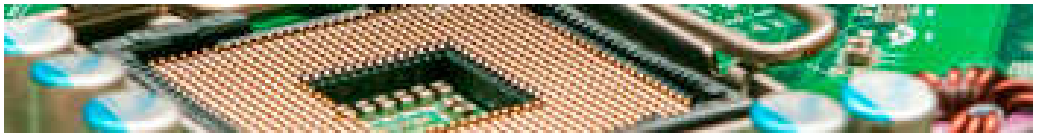
Risk template

Project:				Date Completed:			
Project Sponsor:				Project Manager:			
Risk	**Likelihood**	**Impact**	**Risk Rating**	**Impact**	**Mitigation Strategies**	**Assigned To**	**Status**
	Rare	Insignificant	**Low**				
	Unlikely	Minor	**Low**				
	Possible	Moderate	**Medium**				
	Likely	Major	**Critical**				
	Almost Certain	Catastrophic	**Certain & Critical**				
	Rare	Catastrophic	**Low**				
	Unlikely	Major	**Medium**				
	Possible	Moderate	**Medium**				
	Likely	Minor	**Medium**				
	Almost Certain	Insignificant	**Low**				
			0				

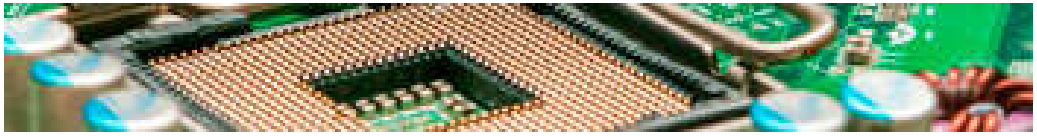


- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información





Risk versus danger



UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Máster Universitario en Ingeniería Informática

Asignatura: Gestión y Gobierno de TI

Máster Oficial Universitario en Ingeniería Informática
muiinf.webs.upv.es

MUIInf