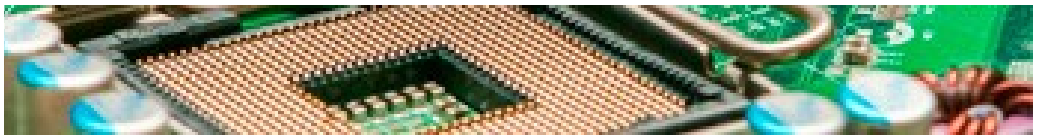
UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Máster Universitario en Ingeniería Informática

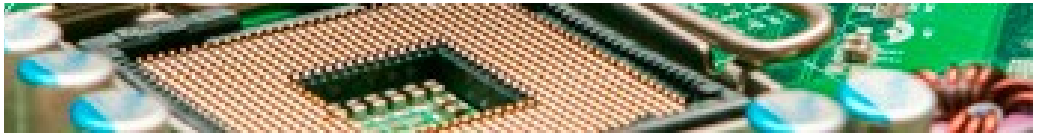
CiberSeguridad
Tema 8: Análisis de Riesgo

José Ismael Ripoll Ripoll



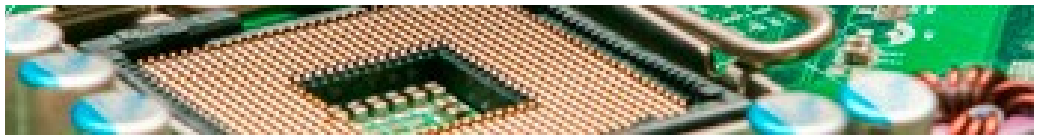
Bibliografía

- Seguiremos la guía del NIST sp800-30-r1:
  - "Guide for conducting risk assesment"
- En España tenemos el estándar MAGERIT y el programa informático de soporte Pilar.



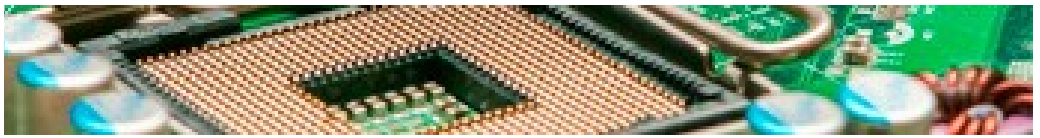
Dimensiones

- Existen 3 dimensiones de seguridad (CIA):
  - Confidencialidad (Confidentiality)
  - Integridad (Integrity)
  - Disponibilidad (Availability)
- Es España se definen dos adicionales:
  - Autenticidad:
    - Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
  - Trazabilidad
    - Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

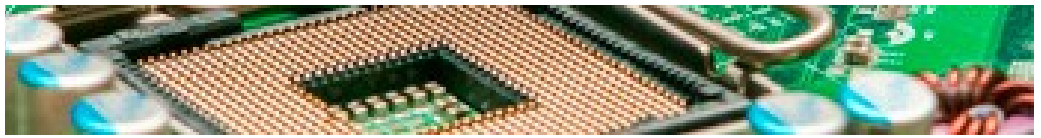


Riesgo (risk)

- Riesgo: es una medida del peligro al que está expuesto un activo a las amenazas o eventos potenciales.
- Normalmente se define como una función de:
  - los efectos adversos que pueden suceder si ciertas circunstancias o eventos suceden y
  - la probabilidad de que esos eventos sucedan.
- Los riesgos de la información son los definidos por las dimensiones de la seguridad.
  - Confidencialidad, Integridad, Disponibilidad, Autenticidad, Trazabilidad.
- Análisis de riesgos es el proceso de identificar, estimar y priorizar la información sobre los riesgos.

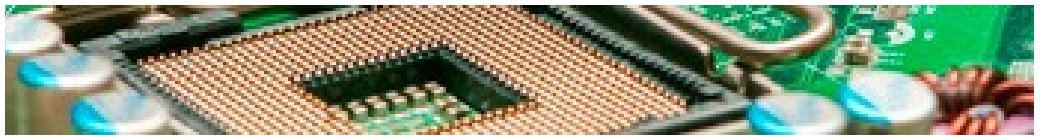


- Amenaza/Threat:
  - Eventos que pueden desencadenar un incidente, produciendo daños materiales o inmateriales en los activos.
  - A threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/ordenial of service.
  - Amenazas **naturales**: incendios, terremotos,..
  - Amenazas **humanas**: hackers, visitantes, incompetentes, errores humanos,...
  - Amenazas del **entorno**: Fallo de discos, corriente eléctrica, ...
- Pero: ¿ Se pueden conocer/valorar correctamente las amenazas ?

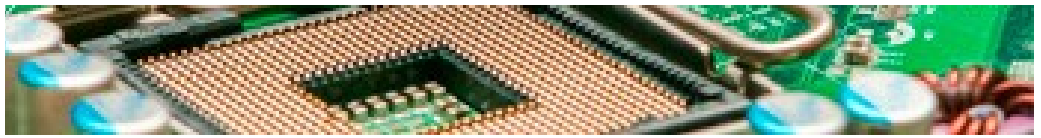


Vulnerabilidades, impacto,...

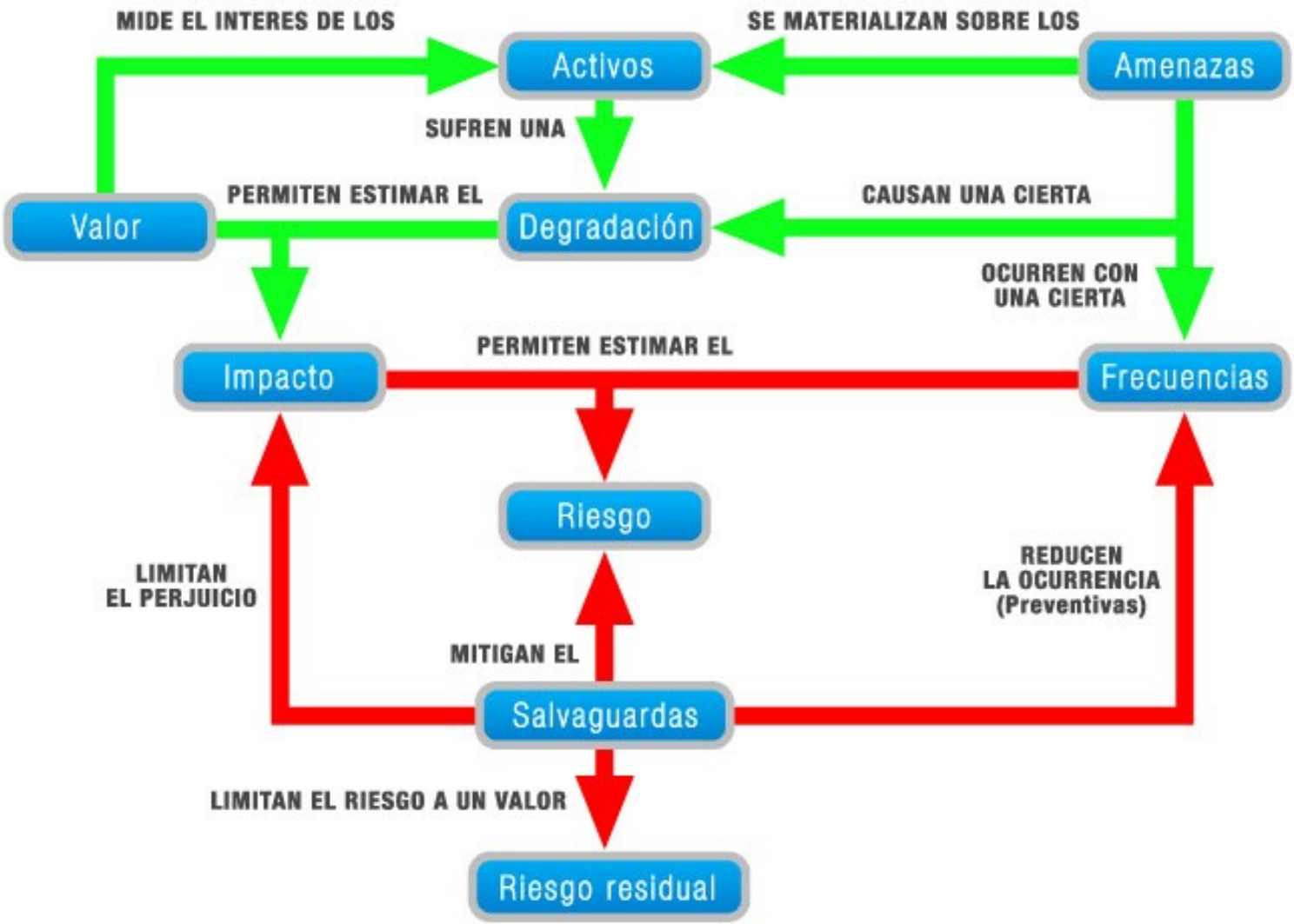
- Vulnerabilidad:
  - Debilidades que tienen los activos y pueden ser aprovechados por una amenaza.
- Impacto:
  - Consecuencia de la materialización de una amenaza sobre un activo.
- Probabilidad:
  - Frecuencia o esperanza de que se materialice una amenaza.
- Riesgo Residual:
  - Riesgo que queda tras aplicar las salvaguardas.

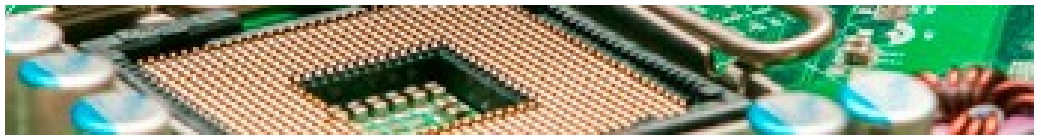


- Salvaguarda:
  - Prácticas, procedimientos o mecanismos que reducen el riesgo. Estas pueden actuar reduciendo el impacto o la probabilidad de la amenaza.
  - **Preventive**—Inhibiting a threat, such as by access controls, encryption, and authentication requirements
  - **Deterrent**—Keeping the casual threat away, such as strong passwords, twotiered authentication, and Internet use policies
  - **Detective**—Identifying and proving when a threat has occurred or is about to occur, such as audit trails, intrusion detection, and checksums
  - **Reactive**—Providing a means to respond to a threat that has occurred, such as an alarm or penetration test
  - **Recovery**—A control that helps retrieve or recreate data or applications, such as backup systems and contingency plans

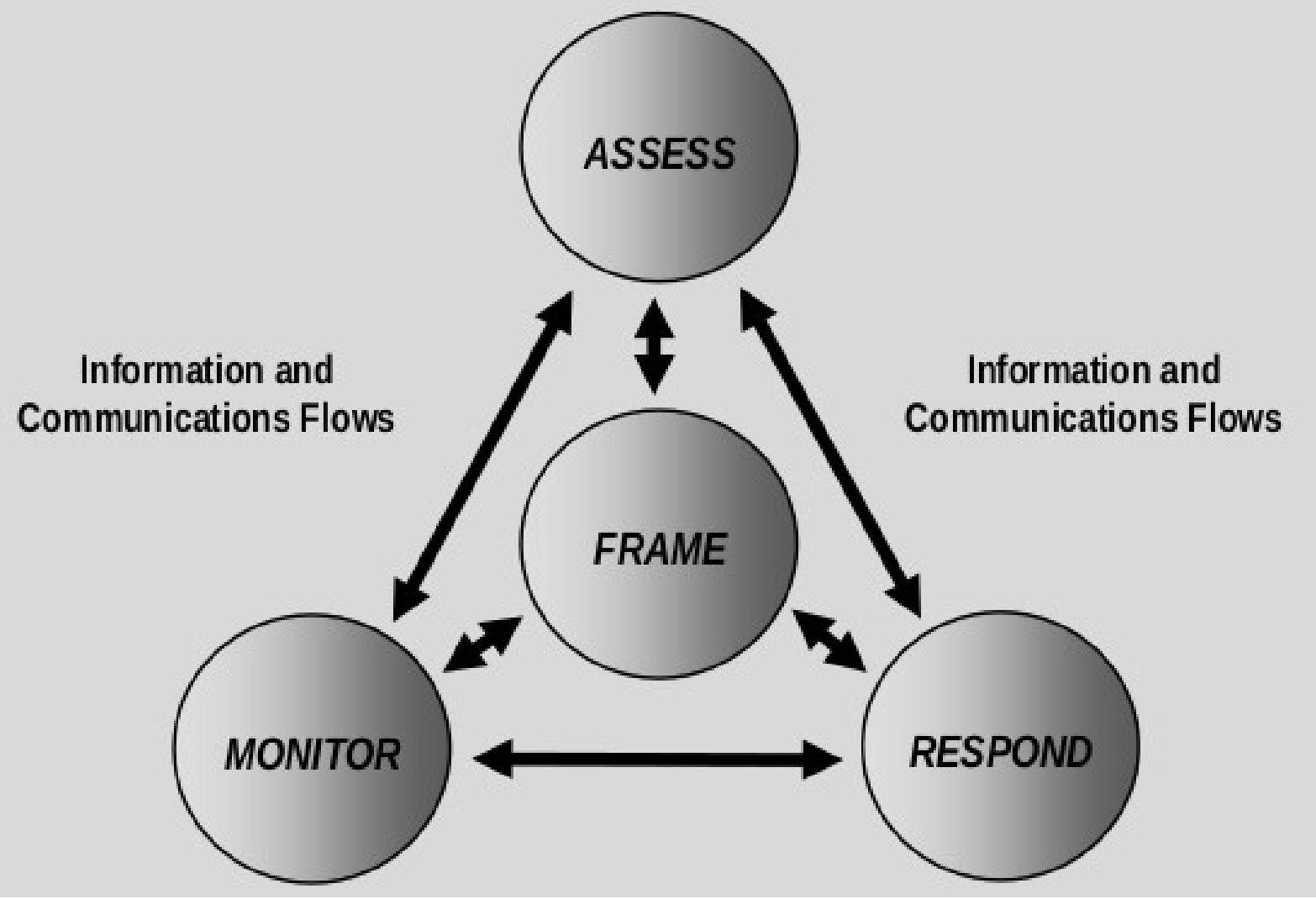


Resumen de conceptos



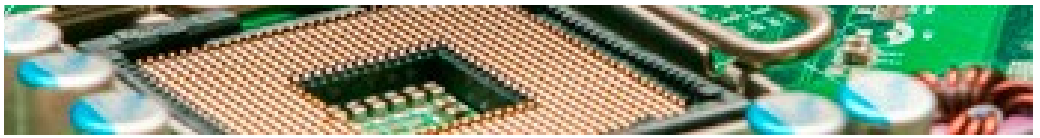


Modelo global del riesgo

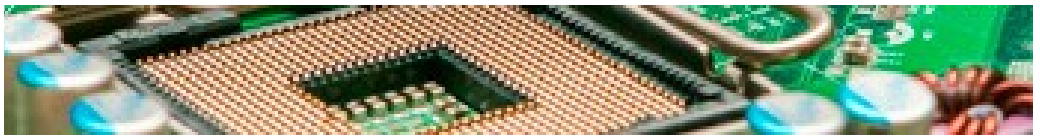


Elementos

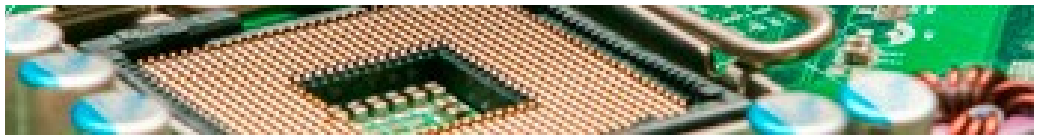
- FRAMEWORK: The first component of risk management addresses how organizations frame risk or establish a risk context—that is, describing the environment in which risk-based decisions are made.
- ASSESS: The purpose of the risk assessment component is to identify:
  - threats to organizations;
  - vulnerabilities internal and external to organizations;
  - the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities; and
  - the likelihood that harm will occur.



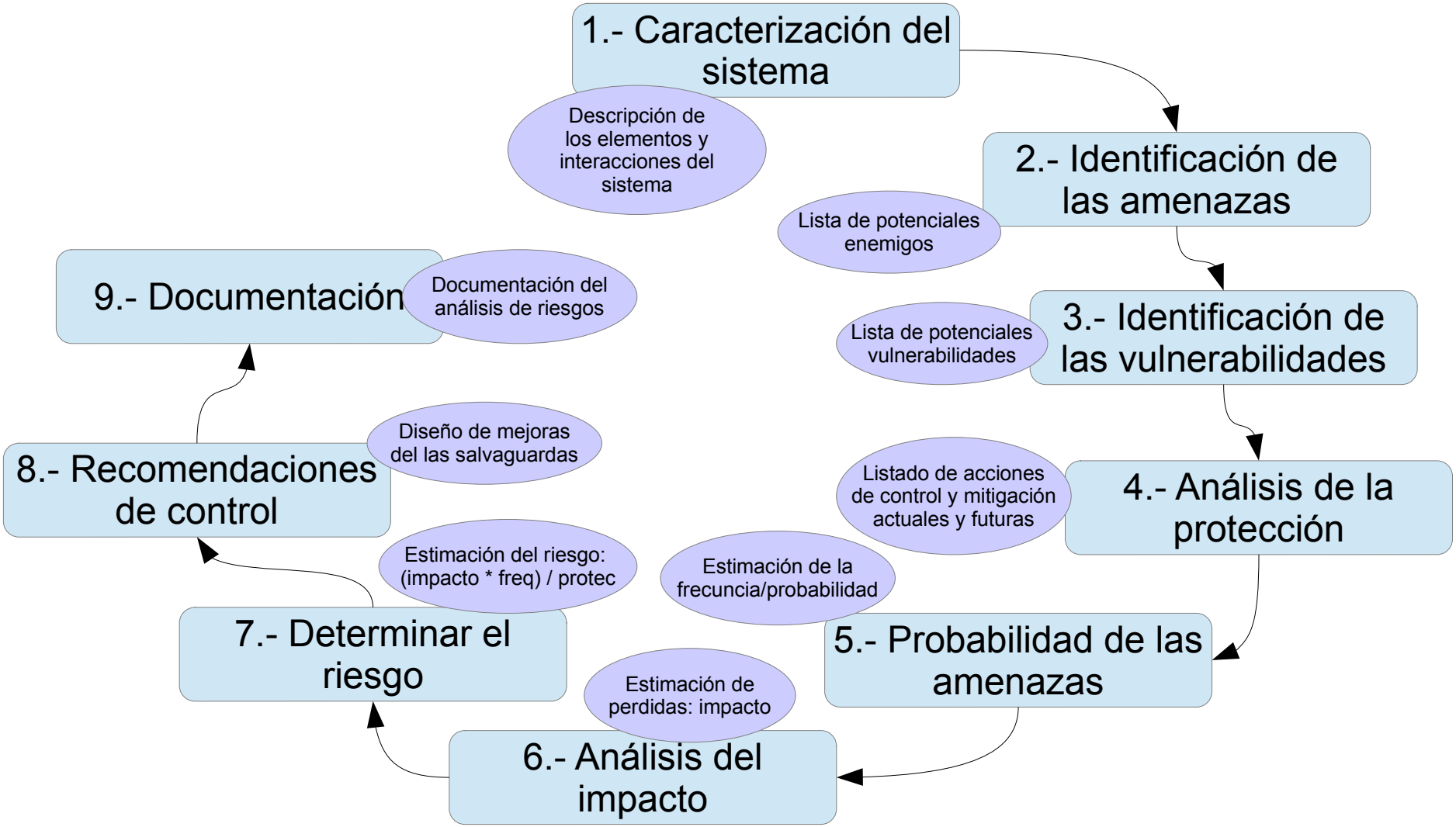
- RESPOND: how respond to risk once that risk is determined based on the results of a risk assessment. The purpose of the risk response component is to provide a consistent, organization-wide response to risk in accordance with the organizational risk frame by:
  - developing alternative courses of action for responding to risk;
  - evaluating the alternative courses of action;
  - determining appropriate courses of action consistent with organizational risk tolerance; and
  - implementing risk responses based on selected courses of action.

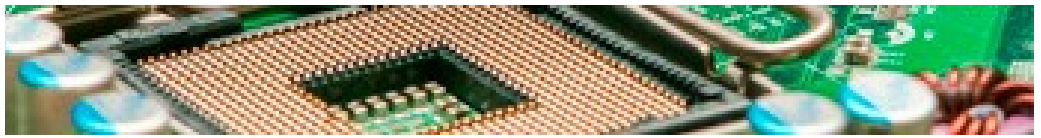


- MONITOR: The purpose of the risk monitoring component is to:
  - determine the ongoing effectiveness of risk responses (consistent with the organizational risk frame);
  - identify risk-impacting changes to organizational information systems and the environments in which the systems operate; and
  - verify that planned risk responses are implemented and information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, standards, and guidelines are satisfied.



Proceso detallado





Modelo genérico de riesgo