ANÁLISIS Y GESTIÓN DE RIESGOS EN LA UPCT CON PILAR

Esteban Sánchez Sánchez
Universidad Politécnica de Cartagena
esteban.sanchez@si.upct.es

ANÁLISIS Y GESTIÓN DE RIESGOS CON PILAR

Universidad Politécnica de Cartagena

- **1. Creación del proyecto con Pilar**
- **2. Análisis de riesgos**
  - **2.1 Refresco de conceptos básicos**
  - **2.2 Activos**
    - 2.2.1 Identificación
    - 2.2.2 Clases
    - 2.2.3 Dependencias
    - 2.2.4 Valoración
  - **2.3 Amenazas**
    - 2.3.1 Vulnerabilidad
    - 2.3.2 Identificación
    - 2.3.3 Valoración
  - **2.4 Impacto y Riesgo acumulado**

Universidad Politécnica de Cartagena

- **3. Tratamiento y gestión de riesgos**
  - **3.1 Refresco de conceptos básicos**
  - **3.2 Salvaguardas**
    - 3.2.1 Identificación
    - 3.2.2 Valoración
  - **3.3 Impacto y Riesgo residuales**
- **4. Informes**

1. CREACIÓN DEL PROYECTO CON PILAR

Universidad Politécnica de Cartagena

- ¿Por donde empiezo?

- Información de partida en esta fase:

- Información y servicios que queremos proteger

- Identificación de los 4 sistemas que llevan esta información y servicios

- Incluir resto de activos (aplicaciones, hardware,etc..)

- Recopilar la información de activos y establecer las relaciones entre ellos de acuerdo a los 4 sistemas identificados

- Primera aproximación al modelo de relación entre activos que se acabará reflejando en Pilar

- Licencia de Pilar

- Mucha voluntad

- Traducir los sistemas y el modelo de relaciones entre los activos de los sistemas al mundo de Pilar

1. CREACIÓN DEL PROYECTO CON PILAR

Universidad Politécnica de Cartagena

¿Tengo licenciada pilar y ahora que?

¿Cómo traslado los 4 sistemas a Pilar?

Se barajaron 3 opciones:

- **Opción 1**→ Un sólo proyecto y un mismo dominio de seguridad

- **Opción 2**→ Un solo proyecto y varios dominios de seguridad

- **Opción 3**→ Un proyecto y un dominio de seguridad por cada sistema

¿Cuál es la mejor opción?

1. CREACIÓN DEL PROYECTO CON PILAR

Universidad Politécnica de Cartagena

Opción 1 → Un sólo proyecto y un mismo dominio de seguridad

Ventajas:

- Todo en un único proyecto

- No es necesario replicar activos

Desventajas:

- Modelado complejo

- Pérdida de visión de los sistemas por separado

1. CREACIÓN DEL PROYECTO CON PILAR

Universidad Politécnica de Cartagena

Opción 2 → Un solo proyecto y varios dominios de seguridad

Ventajas:

- Todo en un único proyecto

- Visión de los sistemas por separado (uno por dominio)

Desventajas:

- Necesidad de replicar activos entre dominios

- Pilar no termina de funcionar bien con varios dominios

1. CREACIÓN DEL PROYECTO CON PILAR

Universidad Politécnica de Cartagena

Opción 3 → Un proyecto y un dominio de seguridad por cada sistema

Ventajas:

- Visión de los sistemas por separado (uno por dominio)

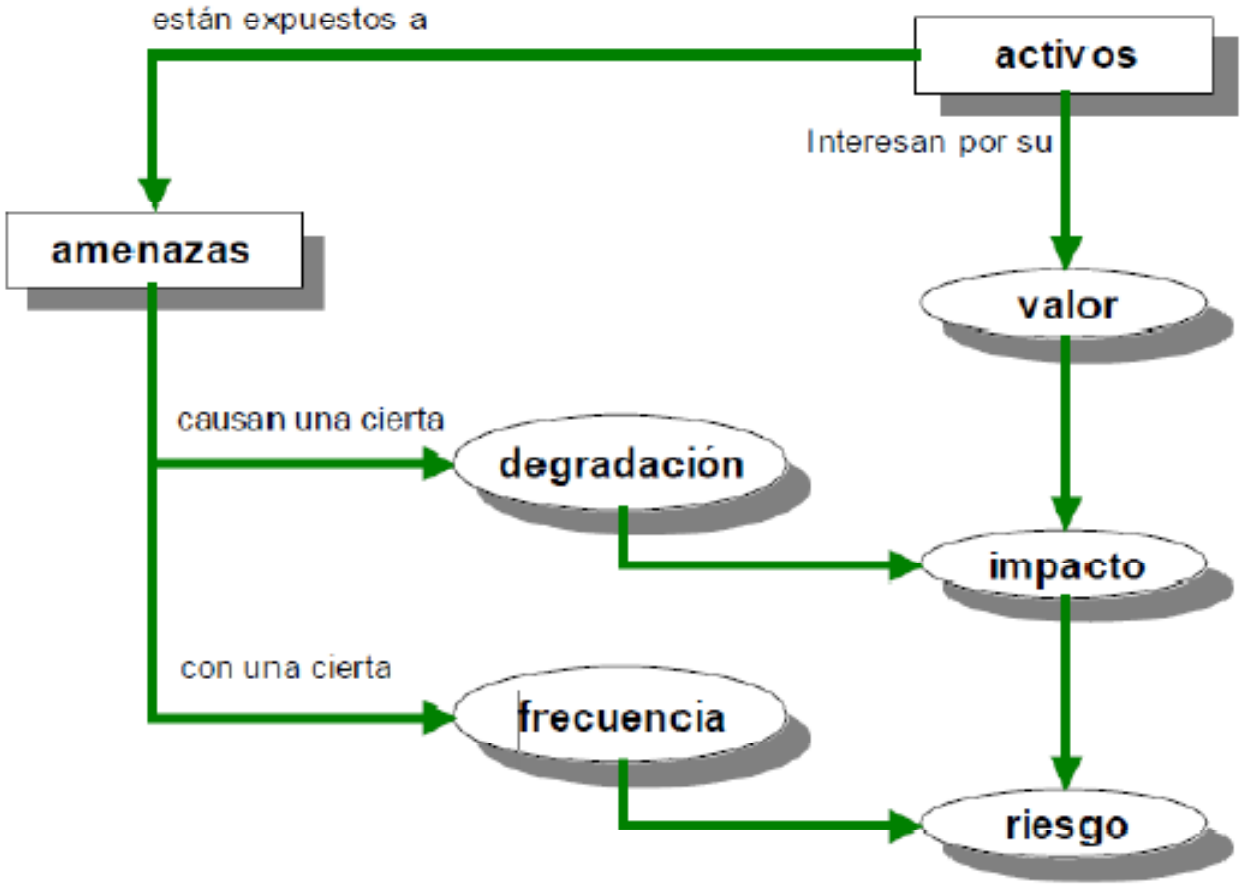
- Seguridad de que Pilar funcionará correctamente

Desventajas:

- Necesidad de replicar activos entre proyectos

2. ANÁLISIS DE RIESGOS

2.1 CONCEPTOS BÁSICOS



Universidad Politécnica de Cartagena

2.1 CONCEPTOS BÁSICOS

Activo:

- **Valor propio:** el del elemento en sí mismo.
- **Valor acumulado:** el proporcional a los elementos que tiene encima
- **Valor nuclear:** El que tiene el elemento de más alto nivel (generalmente la información)

Universidad Politécnica de Cartagena

2.1 CONCEPTOS BÁSICOS

Amenazas:

- Eventos que pueden desencadenar un incidente en la organización produciendo daños materiales o pérdidas inmateriales

- Tipos de amenazas:

  - Naturales
  - Industriales
  - Errores no intencionados
  - Ataques intencionados

Universidad Politécnica de Cartagena

2.1 CONCEPTOS BÁSICOS

- Las amenazas varían de un activo a otro.
- Amenaza por cada activo y dimensión
- No todas las dimensiones afectadas por todas las amenazas

Universidad Politécnica de Cartagena

2.1 CONCEPTOS BÁSICOS

Impacto:

- Medida del daño sobre un activo derivado de la materialización de una amenaza
- Impacto por cada amenaza, activo y dimensión
- 2 tipos de impacto: acumulado y repercutido

Universidad Politécnica de Cartagena

2.1 CONCEPTOS BÁSICOS

Impacto Acumulado:

- Valor acumulado*degradación
- Se calcula sobre un activo teniendo en cuenta:
  - Su valor acumulado (el propio más el acumulado por los activos que dependen de él)
  - Las amenazas a las que está expuesto

Universidad Politécnica de Cartagena

2.1 CONCEPTOS BÁSICOS

Impacto Repercutido:

- Valor propio*degradación
- Se calcula sobre un activo teniendo en cuenta:
  - Su valor propio
  - Las amenazas a las que están expuesto los activos de los que depende

Universidad Politécnica de Cartagena

2.1 CONCEPTOS BÁSICOS

Riesgo:

- Medida del daño probable de un sistema. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización

- Riesgo por activo amenaza y dimensión

- 2 tipos de riesgo: acumulado y repercutido

Universidad Politécnica de Cartagena

2.1 CONCEPTOS BÁSICOS

Riesgo Acumulado:

- Impacto acumulado * frecuencia amenaza
- Se calcula sobre un activo teniendo en cuenta:
  - El impacto acumulado sobre un activo
  - La frecuencia de la amenaza

Universidad Politécnica de Cartagena

2.1 CONCEPTOS BÁSICOS

Riesgo Repercutido:

- Impacto repercutido * frecuencia amenaza
- Se calcula sobre un activo teniendo en cuenta:
  - El impacto repercutido sobre un activo
  - La frecuencia de la amenaza

2. ANÁLISIS DE RIESGOS

Universidad Politécnica de Cartagena

2.2 ACTIVOS - 2.2.1 Identificación de activos

Modelo Sugerido:

- Información
- Servicios
- Aplicaciones
- Equipo informático
- Soporte de información
- Equipamiento auxiliar
- Redes de comunicaciones
- Ubicaciones
- Personas

Modelo UPCT:

- Información
- Servicios
- Aplicaciones
- Servicios TI
- Hosts
- Hardware
- Redes y Comunicaciones
- Ubicaciones
- Personas

2. ANÁLISIS DE RIESGOS

Universidad Politécnica de Cartagena

2.2 ACTIVOS - 2.2.2 Clases de activos

¿Para que sirve tener el activo clasificado?

- Tenerlo clasificado e identificado en el modelo

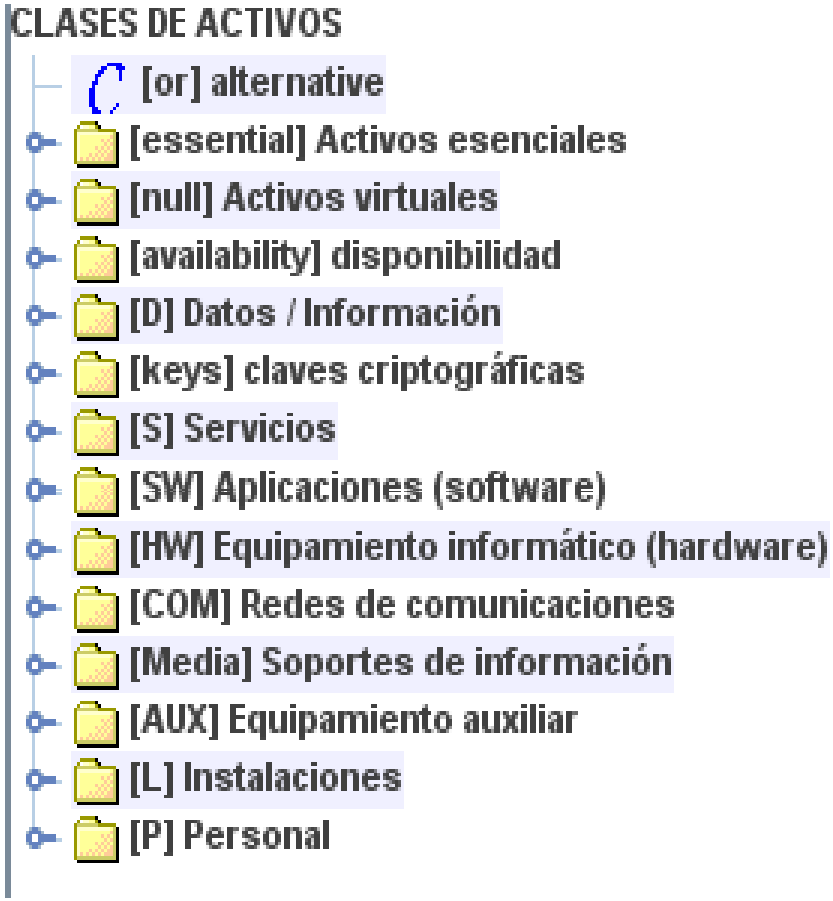
- Agruparlo junto con otros activos de la misma clase facilitando el modelado

¿Sirve para algo más?

- Una amenaza puede afectar a todos los activos a sólo a algunos en base a su clase

- La correspondencia activo -amenaza ya la sabe Pilar (Que lista!!). Por tanto clasificarlos permite a Pilar seleccionar por nosotros las amenazas en la fase de identificación de amenazas

- Conclusión: una buena clasificación, no ir a la ligera. Aprovechar las subcategorias que ofrece Pilar



Universidad Politécnica de Cartagena

2.2 ACTIVOS - 2.2.3 Dependencias entre activos

¿Para que sirven las dependencias?

- Construimos un modelo del sistema en base a las relaciones entre sus activos.

- No es un modelo detallado:

    - La herramienta de Pilar no permite modelado complejo

    - La forma de relacionar una activo con otros activos viene determinada por el tipo de activo

    - Tipos de activos diferentes tienen distintos tipos de relaciones (no simpre es “contenido en” o “depende de”)

    - Independientemente de los tipos de relaciones ,nuestro objetivo final es hacer un modelo lo más posible y que cumpla con los requisitos para el análisis de riesgo

¿Cómo debe ser un modelo que sirva para el análisis de riesgos?

- El valor acumulado se debe repartir de forma adecuado entre todos los activos.
- Activos de capas inferiores acumulan valor de activos de capas superiores

2. ANÁLISIS DE RIESGOS

Universidad Politécnica de Cartagena

2.2 ACTIVOS - 2.2.4 Valoración de activos

¿Para que sirve la valoración?

- Nos dará una visión de la importancia de nuestro activo en términos de seguridad en base a la valoración de las 5 dimensiones de la seguridad (IDCAT).

- Se empleará el valor acumulado. Así un activo por sí mismo puede valer menos que la suma de los activos que tiene por encima.

¿Qué escala de valoración se empleo?

- Cualitativa:
  - 0 → Sin valorar
  - 1 → Bajo
  - 4 → Medio
  - 5 → Alto

- Se eligió de manera que encajase con los valores que se les dio a la información y a los servicios en la fase previa a Pilar

- La información y los servicios es lo más importante en cuanto a valor nuclear desde el punto de vista del ENS. Su valor se arrastra al resto seleccionando valor acumulado.

2. ANÁLISIS DE RIESGOS

Universidad Politécnica de Cartagena

2.3 AMENAZAS - 2.3.1 Dominios de Vulnerabilidad

¿Qué es la vulnerabilidad?

- Probabilidad de que se produzca y degradación que genera

¿Qué nos permite Pilar?

- Seleccionar una serie de condiciones iniciales para el entorno que dan idea de su vulnerabilidad

¿Cómo nos ayudará esto?

- En base a lo seleccionado podemos pedir a Pilar que nos “sugiera” unos valores de frecuencia y degradación adecuados al entorno seleccionado.

Universidad Politécnica de Cartagena

2.3 AMENAZAS - 2.3.2 Identificación

Recordar a la hora de identificarlas que:

- Una amenaza puede afectar a uno o varios activos

- Se puede consultar el “ameno” manual con todas las amenazas una por una e ir seleccionado.

¿Cómo se seleccionaron?

- Dejar a Pilar que nos sugiera. Recordar que lo hace en base a como clasificamos los activos (2.1.2 clases de activos)

- En base al manual de información de Pilar eliminar las que no convencen o introducir otras nuevas

Universidad Politécnica de Cartagena

2.3 AMENAZAS - 2.3.3 Valoración

Recordar a la hora de valorar que:

- Una amenaza puede afectar a una o varias dimensiones de un activo

- Podemos volver a consultar el “ameno” manual con todas las amenazas una por una e ir viendo a que dimensiones afecta.

¿Cómo se valoraron?

1.- Dejar a Pilar que nos sugiera. Recordar que lo hace en base a como describimos nuestro escenario en términos de vulnerabilidad (2.2.1 dominio de vulnerabilidad)

2.- Partiendo de las valoraciones de Pilar, adaptarlas a nuestra escala

2. ANÁLISIS DE RIESGOS

2.3 AMENAZAS - 2.3.3 Valoración

Frecuencia:

100 → muy frecuente–a diario

10 → frecuente–menualmente

1 → normal–una vez al año

1/10 → poco frecuente – cada varios años

1/100 → muy infrecuente–cada varias décadas

Degradación:

5% → Degradación Baja

30% → Degradación Media

50% → Degradación Alta

80% → Degradación Muy Alta

100% → Completa

2.3 AMENAZAS - 2.3.3 Valoración

Problemas más importantes que surgen al valorar :

- Hay que valorar como si no hubiese salvaguardas (algo bastante complicado).

- Falta una base de datos que recoja de forma detallada todo el histórico de incidentes

-Además se puede pensar que hay amenazas que no se han producido nunca cuando en verdad lo que ha pasado es que:

- Las han parado las salvaguardas que tenemos

- No se han podido detectar que ocurran con los medios de los que se dispone

Universidad Politécnica de Cartagena

2.3 AMENAZAS - 2.3.3 Valoración

Método a seguir al valorar :

- Reuniones de donde sacar experiencia previa

- Cuando no se tiene experiencia previa de que haya sucedido , para el caso de la frecuencia la seleccionamos de acuerdo con lo probable que es que se produzca ese incidente aunque no haya pasado nunca.

- Cuando valoramos la degradación lo hacemos sin tener en cuenta ningún tipo de salvaguarda, por lo que cosas que ya han pasado provocarán una mayor degradación puesto que no está la salvaguarda que protegió en su momento

2. ANÁLISIS DE RIESGOS

2.4 IMPACTO Y RIESGO ACUMULADO

UPCT_ENS_AE: riesgo acumulado - UNIVERSIDAD POLITÉCNICA DE CARTAGENA

activo	amenaza	dimensión	V	VA	D	I	F	riesgo
[NETSEC.NETSEC_ASA] Cisco ASA 5500	[A.5] Suplantación de la identidad del ...	[A]		[4]	100%	[4]	10	{4,2}
[H_HPUX] Host Cluster HPUX	[A.22] Manipulación de programas	[C]		[4]	100%	[4]	10	{4,2}
[ALM.HW_CABINA] Cabina de Almacen...	[A.4] Manipulación de los ficheros de ...	[C]		[4]	100%	[4]	10	{4,2}
[H_REGISTRO] Host REGISTRO.UPCT.ES	[A.22] Manipulación de programas	[C]		[4]	100%	[4]	10	{4,2}
[ALM.HW_CABINA] Cabina de Almacen...	[A.4] Manipulación de los ficheros de ...	[I]		[4]	100%	[4]	10	{4,2}
[H_HPUX] Host Cluster HPUX	[A.22] Manipulación de programas	[I]		[4]	100%	[4]	10	{4,2}
[H_CETUS] Host CETUS.SI.UPCT.ES	[A.4] Manipulación de los ficheros de ...	[A]		[4]	100%	[4]	10	{4,2}
[I_FACTURA] Información de Factura El...	[A.5] Suplantación de la identidad del ...	[A]	[4]	[4]	100%	[4]	10	{4,2}
[ALM.HW_NETF2] Red de Almacenamie...	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}
[H_REGISTRO] Host REGISTRO.UPCT.ES	[A.22] Manipulación de programas	[I]		[4]	100%	[4]	10	{4,2}
[ALM.HW_NETALM] Red de Almacena...	[A.5] Suplantación de la identidad del ...	[A]		[4]	100%	[4]	10	{4,2}
[ALM.HW_NETF1] Red de Almacenamie...	[A.5] Suplantación de la identidad del ...	[A]		[4]	100%	[4]	10	{4,2}
[S_TRAMITACION] Servicio de Tramita...	[A.5] Suplantación de la identidad del ...	[A]	[4]	[4]	100%	[4]	10	{4,2}
[SERV.HW_BLADE01_SI] Servidor BLAD...	[A.4] Manipulación de los ficheros de ...	[D]		[4]	100%	[4]	10	{4,2}
[ALM.HW_CABINA] Cabina de Almacen...	[A.22] Manipulación de programas	[I]		[4]	100%	[4]	10	{4,2}
[ALM.HW_NETALM] Red de Almacena...	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}
[NETHW.NETHW_ASR1000] Router Cisc...	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}
[ALM.HW_NETF1] Red de Almacenamie...	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}
[SERV.HW_BLADE03_SI] Servidor BLAD...	[A.4] Manipulación de los ficheros de ...	[D]		[4]	100%	[4]	10	{4,2}
[H_ARA] Host ARA.SI.UPCT.ES	[A.4] Manipulación de los ficheros de ...	[A]		[4]	100%	[4]	10	{4,2}
[NETHW.HW_HPPC5412_2] Switch-Rout...	[A.5] Suplantación de la identidad del ...	[A]		[4]	100%	[4]	10	{4,2}
[SERV.HW_BLADE04_SI] Servidor BLAD...	[A.4] Manipulación de los ficheros de ...	[D]		[4]	100%	[4]	10	{4,2}
[SERV.HW_VMWARE] Cluster WMWare	[A.4] Manipulación de los ficheros de ...	[D]		[4]	100%	[4]	10	{4,2}
[I_FACTURA] Información de Factura El...	[A.15] Modificación de la información	[I]	[4]	[4]	100%	[4]	10	{4,2}
[NETHW.HW_HPPC5412] Switch-Router ...	[A.5] Suplantación de la identidad del ...	[A]		[4]	100%	[4]	10	{4,2}
[H_CETUS] Host CETUS.SI.UPCT.ES	[A.4] Manipulación de los ficheros de ...	[D]		[4]	100%	[4]	10	{4,2}
[NETHW.NETHW_ASR1000] Router Cisc...	[A.5] Suplantación de la identidad del ...	[A]		[4]	100%	[4]	10	{4,2}
[ALM.HW_CABINA] Cabina de Almacen...	[A.15] Modificación de la información	[I]		[4]	100%	[4]	10	{4,2}
[I_TRAMITACION] Información de Tra...	[A.19] Divulgación de información	[C]	[4]	[4]	100%	[4]	10	{4,2}
[H_WEB09] Host WEB09.UPCT.ES	[A.5] Suplantación de la identidad del ...	[I]		[4]	100%	[4]	10	{4,2}
[SERV.HW_BLADE05_SI] Servidor BLAD...	[A.4] Manipulación de los ficheros de ...	[D]		[4]	100%	[4]	10	{4,2}
[H_ALFRESCO] Host Alfresco	[A.5] Suplantación de la identidad del ...	[A]		[4]	100%	[4]	10	{4,2}
[H_SEDE] Host SEDE.UPCT.ES	[A.5] Suplantación de la identidad del ...	[A]		[4]	100%	[4]	10	{4,2}
[H_WEB09] Host WEB09.UPCT.ES	[A.5] Suplantación de la identidad del ...	[C]		[4]	100%	[4]	10	{4,2}
[I_TRAMITACION] Información de Tra...	[A.5] Suplantación de la identidad del ...	[A]	[4]	[4]	100%	[4]	10	{4,2}
[H_ARA] Host ARA.SI.UPCT.ES	[A.4] Manipulación de los ficheros de ...	[D]		[4]	100%	[4]	10	{4,2}
[S_PORTAFIRMAS] Servicio Portafirmas	[A.5] Suplantación de la identidad del ...	[A]	[4]	[4]	100%	[4]	10	{4,2}
[NETTOP.NETTOP_DMZ] LAN - Zona DMZ	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}
[IT_SGBD] Servicio de Bases de Datos	[A.5] Suplantación de la identidad del ...	[A]		[4]	100%	[4]	10	{4,2}
[H_INDUS] Host INDUS	[A.3] Manipulación de los registros de...	[T]		[4]	100%	[4]	10	{4,2}

A | leyenda | csv | xml | db

Universidad Politécnica de Cartagena

3.1 CONCEPTOS BÁSICOS

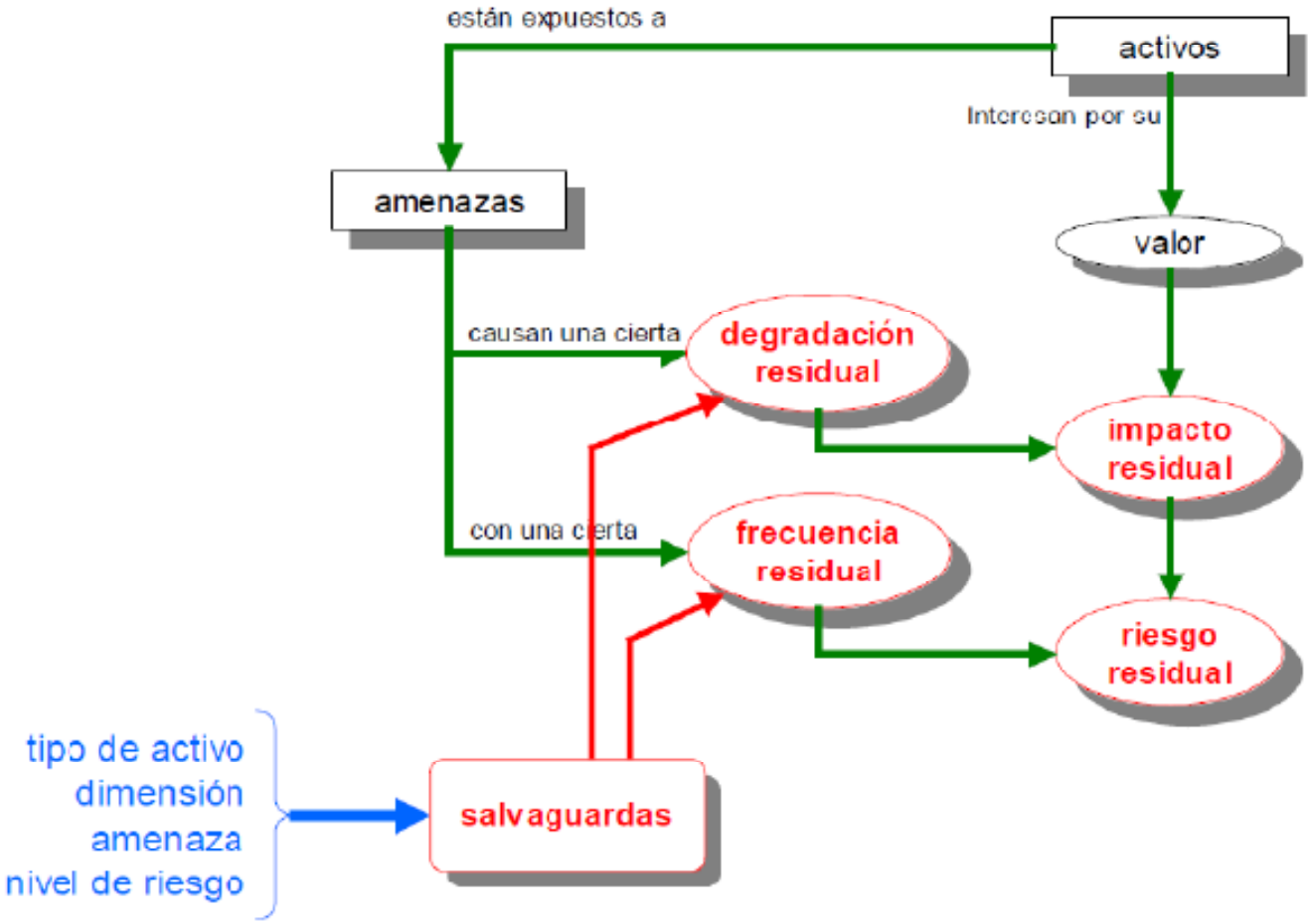
Salvaguardas:

- Se aplican para mitigar o reducir el riesgo hasta unos niveles asumibles por la organización
- Salvaguardas se eligen de forma global
- La salvaguarda debe/puede producir reducción en la degradación de la amenaza para cada dimensión
- La salvaguarda debe/puede producir una reducción en la frecuencia para cada dimensión

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universidad Politécnica de Cartagena

3.1 CONCEPTOS BÁSICOS



3. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.1 Identificación

- Las salvaguardas se aplican a nivel global para todo el sistema reduciendo y evitando el riesgo (gestionando el riesgo)

- Pilar contempla salvaguardas y grupos de salvaguardas

- Estas salvaguardas y grupos se pueden clasificar en función de diferentes criterios:

1 .- Aspecto que se protegerá

G: Aspecto de gestión.
T: Aspecto técnico → medidas más concretas que la de gestión
P: Aspecto de Personal.
F: Aspecto de Seguridad física (instalaciones)

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.1 Identificación

2.- Estrategia que adopta la salvaguarda ante el incidente:

CR: Correctivas (gestión de incidentes)
IM: Minimizar impacto (desconexión de equipos)
RC: Recuperación del incidente (copias de seguridad)
DT: Detección (detectores de incendios)
MN: Monitorización (registros de actividad)
EL: Eliminación (Eliminar cuentas de usuarios que ya no emplean)
PR: Preventiva (autorización previa de usuarios)
DR: Disuasoria (vallas, guardias de seguridad)
AD: Administrativas (inventario de activos)
AW: Concienciación (cursos de concienciación)
std: basadas en normas
proc: basadas en procedimientos
cert: basadas en productos certificados (Firewalls)

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.1 Identificación

3 .- Clase de activo que protegerá (Grupo principal/raíz)

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

3.2 SALVAGUARDAS – 3.2.1 Identificación

4.- Importancia de la salvaguarda:

5.- Forma en la que se aplica:

{and}: Deberían aplicarse todas las salvaguardas.

{or}: Debería aplicarse al menos una de las salvaguardas

{xor}: Debería aplicarse sólo una de las salvaguardas (la que mejor aplique → la más recomendada).

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

3.2 SALVAGUARDAS – 3.2.1 Identificación

6.- Recomendación de su implantación:

1 (blanco) → no recomendable por que no aplica

2,3 (azul) → recomendable

4,5 (amarillo) → bastante recomendable

6,7 (rojo palido) → muy recomendable

8,9 (rojo) → necesaria

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.1 Identificación

- Consideración sobre su aplicación:

[Vacío]: Aplica la salvaguarda o no, según tenga configurado en las “Opciones”.

n.a.: No aplica la salvaguarda y, por lo tanto, no se mostrará a la hora de evaluar las salvaguardas. Si se la pongo a un grupo afecta a todo lo que hay por debajo

…: Indica que se trata de un grupo de salvaguardas que contiene a alguna salvaguarda en “n.a.”.

- Consideración sobre su estado:

On: Quiero usarla para el análisis

Off: Aunque aplique a mi sistema, en este análisis no la quiero considerar

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.1 Identificación

Consideraciones sobre su selección:

- Cantidad muy elevada de salvaguardas
- Me interesan sobre todo las que se aplican al ENS

¿Hay alguna forma de hacer una preselección?

- Usar perfil de seguridad del ENS → Subconjunto de salvaguardas que se ofrecen en Pilar y que son de aplicación al ENS

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.1 Identificación

Dentro del perfil ENS, Pilar distingue entre:

- **Controles:** se corresponden con los apartados principales que aparecen en la normativa del ENS. Sirven par agrupar preguntas y salvaguardas

- **Preguntas:** se corresponden con los comentarios y subapartados que aparecen en la norma del ENS. Sirven para evaluar el nivel de cumplimiento de la norma pero no tienen influencia sobre los valores del riesgo

- **Salvaguardas:** se corresponden con las que aparecen en el apartado T.2.1 y que Pilar ha seleccionado para dar cumplimiento a los controles y preguntas de la norma. Si tiene una influencia sobre los valores del riesgo.

Para tener un análisis completo Pilar recomienda evaluar todas las salvaguardas y no sólo las que aparecen con la norma

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.1 Identificación

- Consideración sobre aplicación de controles y preguntas:

M: Es obligatorio a cumplir según la norma.

[Vacío]: Es un control que no hay que cumplir según el nivel de la dimensión o se trata de un grupo de controles donde hay uno que no tiene que cumplirla.

Ejemplo: [mp.if.9] Instalaciones alternativas

Gris: No tiene que cumplir según la norma porque no se han incluído categorías de activos que contempla esa norma

Ejemplos: [mp.eq.3] Equipos portátiles
[mp.info.1] Datos de carácter personal

n.a.: Es obligatorio según la norma pero en nuestro caso se dan condiciones por las que no se va a cumplir → no influye sobre la gestión del riego

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.2 Valoración

Valor seleccionable (niveles de madurez) (niveles de estado)	Valor mostrado	Significado
[Vacío]		Se intentará usar el valor de un dominio padre o de una fase previa (en función de lo que haya seleccionado en las "Opciones"). Si no hay valor en ningún dominio padre, ni en ninguna fase previa, se entiende que falta el dato y no se calcula nada (tendría el mismo efecto que ponerlo a L0 o "n.a.", en función de lo que haya seleccionado en "Opciones"). Es el valor por defecto de valoración.
L0 - Inexistente L0 - Inexistente	L0	*Procedimiento:* No se realiza. *Elemento:* No se tiene. *Documento:* No se tiene.

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.2 Valoración

L1 - Inicial / ad hoc L1 - Iniciado	L1	*Procedimiento:* Se está empezando a hacer, o sólo lo hacen algunas personas. *Elemento:* Se tiene, pero no se usa apenas. *Documento:* Se está preparando su elaboración.
L2 - Reproducible, pero intuitivo L2 - Parcialmente realizado	L2	*Procedimiento:* Todos lo hacen igual, pero no está documentado. *Elemento:* Se tiene, pero se está terminando de afinar. *Documento:* Se está elaborando.
L3 - Proceso definido L3 - En funcionamiento	L3	*Procedimiento:* Todos lo hacen igual y está documentado. *Elemento:* Se tiene y funciona correctamente. *Documento:* Se tiene.

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.2 Valoración

L4 - Gestionado y medible L4 - Monitorizado	L4	*Procedimiento:* Se obtienen indicadores. *Elemento:* Se obtienen indicadores. *Documento:* Se obtienen indicadores.
L5 - Optimizado L5 - Mejora continua	L5	*Procedimiento:* Se revisa el mismo y los indicadores, se proponen mejoras y se aplican. *Elemento:* Se revisa el mismo y los indicadores, se proponen mejoras y se aplican. *Documento:* Se revisa el mismo y los indicadores, se proponen mejoras y se aplican.
No es aplicable	n.a.	La salvaguarda no tiene sentido en el dominio. Se debe introducir un comentario que

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

Universidad Politécnica de Cartagena

3.2 SALVAGUARDAS – 3.2.2 Valoración

Nivel	Efectividad
L0	0%
L1	10%
L2	50%
L3	90%
L4	95%
L5	100%

3. TRATAMIENTO Y GESTIÓN DE RIESGOS

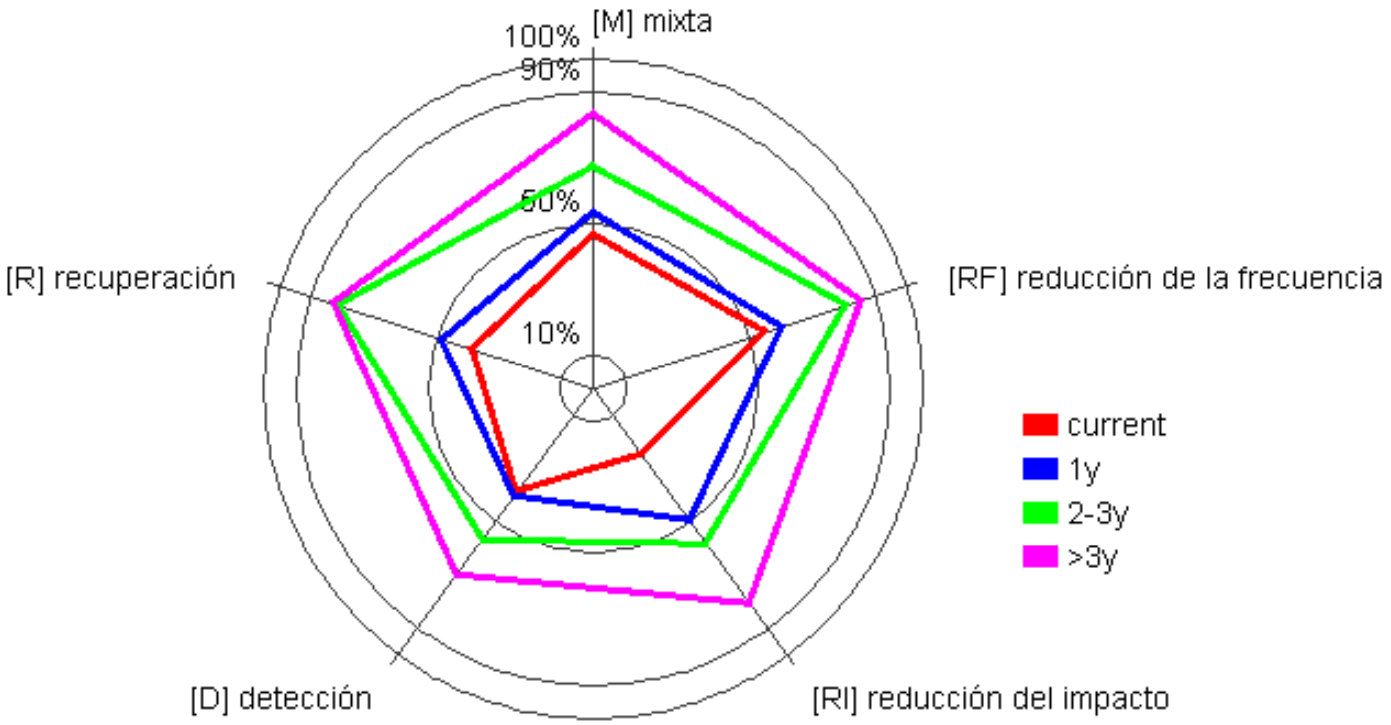
Universidad Politécnica de Cartagena

3.3 IMPACTO Y RIESGO RESIDUALES

potencial | current | 1y | 2-3y | >3y | resumen (impacto) | resumen (riesgo)

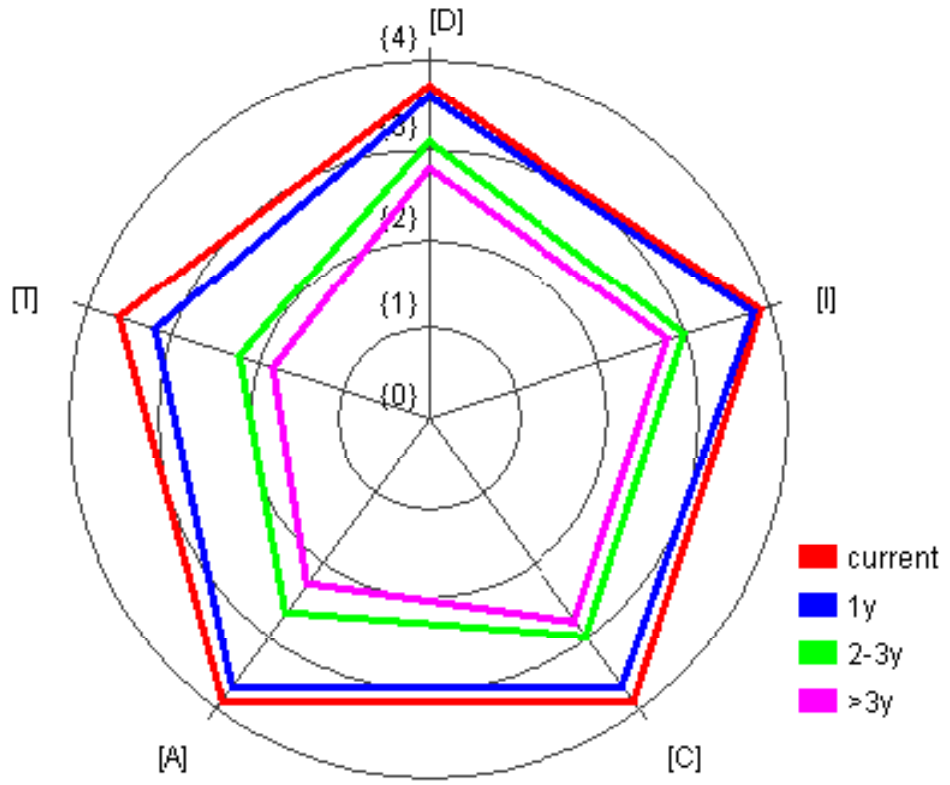
activo	amenaza	dimensión	V	VA	D	I	F	riesgo
A_PORTAFIRMAS] Aplicación Portafirmas	[A.5] Suplantación de la identidad del usu...	[A]		[4]	100%	[4]	10	{4,2}
H_CETUS] Host CETUS.SI.UPCT.ES	[A.4] Manipulación de los ficheros de conf...	[A]		[4]	100%	[4]	10	{4,2}
ALM.HW_NETF2] Red de Almacenamient...	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}
SERV.HW_BLADE01_SI] Servidor BLADE0...	[A.4] Manipulación de los ficheros de conf...	[D]		[4]	100%	[4]	10	{4,2}
A_SIGEM] Aplicación SIGEM	[A.5] Suplantación de la identidad del usu...	[A]		[4]	100%	[4]	10	{4,2}
H_ARA] Host ARA.SI.UPCT.ES	[A.4] Manipulación de los ficheros de conf...	[D]		[4]	100%	[4]	10	{4,2}
NETTOP.NETTOP_DMZ] LAN - Zona DMZ	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}
IT_SGBD] Servicio de Bases de Datos	[A.5] Suplantación de la identidad del usu...	[A]		[4]	100%	[4]	10	{4,2}
I_FACTURA] Información de Factura Elect...	[A.5] Suplantación de la identidad del usu...	[A]	[4]	[4]	100%	[4]	10	{4,2}
NETHW.NETHW_7200] Router Cisco 7200	[A.5] Suplantación de la identidad del usu...	[A]		[4]	100%	[4]	10	{4,2}
NETHW.HW_HPPC5412] Switch-Router H...	[A.5] Suplantación de la identidad del usu...	[A]		[4]	100%	[4]	10	{4,2}
ALM.HW_CABINA] Cabina de Almacenam...	[A.15] Modificación de la información	[I]		[4]	100%	[4]	10	{4,2}
SERV.HW_BLADE05_SI] Servidor BLADE0...	[A.4] Manipulación de los ficheros de conf...	[D]		[4]	100%	[4]	10	{4,2}
H_HPUX] Host Cluster HPUX	[A.22] Manipulación de programas	[D]		[4]	100%	[4]	10	{4,2}
H_ALFRESCO] Host Alfresco	[A.22] Manipulación de programas	[C]		[4]	100%	[4]	10	{4,2}
SERV.HW_BLADE07_SI] Servidor BLADE0...	[A.4] Manipulación de los ficheros de conf...	[D]		[4]	100%	[4]	10	{4,2}
I_TRAMITACION] Información de Tramita...	[A.15] Modificación de la información	[I]	[4]	[4]	100%	[4]	10	{4,2}
H_INDUS] Host INDUS	[A.3] Manipulación de los registros de acti...	[T]		[4]	100%	[4]	10	{4,2}
I_FACTURA] Información de Factura Elect...	[A.15] Modificación de la información	[I]	[4]	[4]	100%	[4]	10	{4,2}
ALM.HW_CABINA] Cabina de Almacenam...	[A.4] Manipulación de los ficheros de conf...	[D]		[4]	100%	[4]	10	{4,2}
H_SEDE] Host SEDE.UPCT.ES	[A.22] Manipulación de programas	[I]		[4]	100%	[4]	10	{4,2}
A_FACTURAE] Aplicación FACTURAE	[A.5] Suplantación de la identidad del usu...	[A]		[4]	100%	[4]	10	{4,2}
H_REGISTRO] Host REGISTRO.UPCT.ES	[A.22] Manipulación de programas	[I]		[4]	100%	[4]	10	{4,2}
H_REGISTRO] Host REGISTRO.UPCT.ES	[A.5] Suplantación de la identidad del usu...	[A]		[4]	100%	[4]	10	{4,2}
ALM.HW_NETF1] Red de Almacenamient...	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}
SERV.HW_BLADE02_SI] Servidor BLADE0...	[A.4] Manipulación de los ficheros de conf...	[D]		[4]	100%	[4]	10	{4,2}
H_ARA] Host ARA.SI.UPCT.ES	[A.5] Suplantación de la identidad del usu...	[A]		[4]	100%	[4]	10	{4,2}
H_ALFRESCO] Host Alfresco	[A.22] Manipulación de programas	[I]		[4]	100%	[4]	10	{4,2}
NETHW.NETHW_7200] Router Cisco 7200	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}
I_TRAMITACION] Información de Tramita...	[A.5] Suplantación de la identidad del usu...	[A]	[4]	[4]	100%	[4]	10	{4,2}
H_REGISTRO] Host REGISTRO.UPCT.ES	[A.22] Manipulación de programas	[C]		[4]	100%	[4]	10	{4,2}
NETHW.HW_HPPC5412_2] Switch-Router...	[A.5] Suplantación de la identidad del usu...	[A]		[4]	100%	[4]	10	{4,2}
NETSEC.NETSEC_ASA] Cisco ASA 5500	[A.24] Denegación de servicio	[D]		[4]	100%	[4]	10	{4,2}

4. INFORMES



Evolución de salvaguardas. UPCT

4. INFORMES



Evolución del riesgo acumulado. Sistema Administración Electrónica. UPCT

5. OPCIONES

Universidad Politécnica de Cartagena