VIII JORNADAS STIC CCN-CERT

La defensa del patrimonio tecnológico frente a los ciberataques

10 y 11 de diciembre de 2014

Sendas de ataque

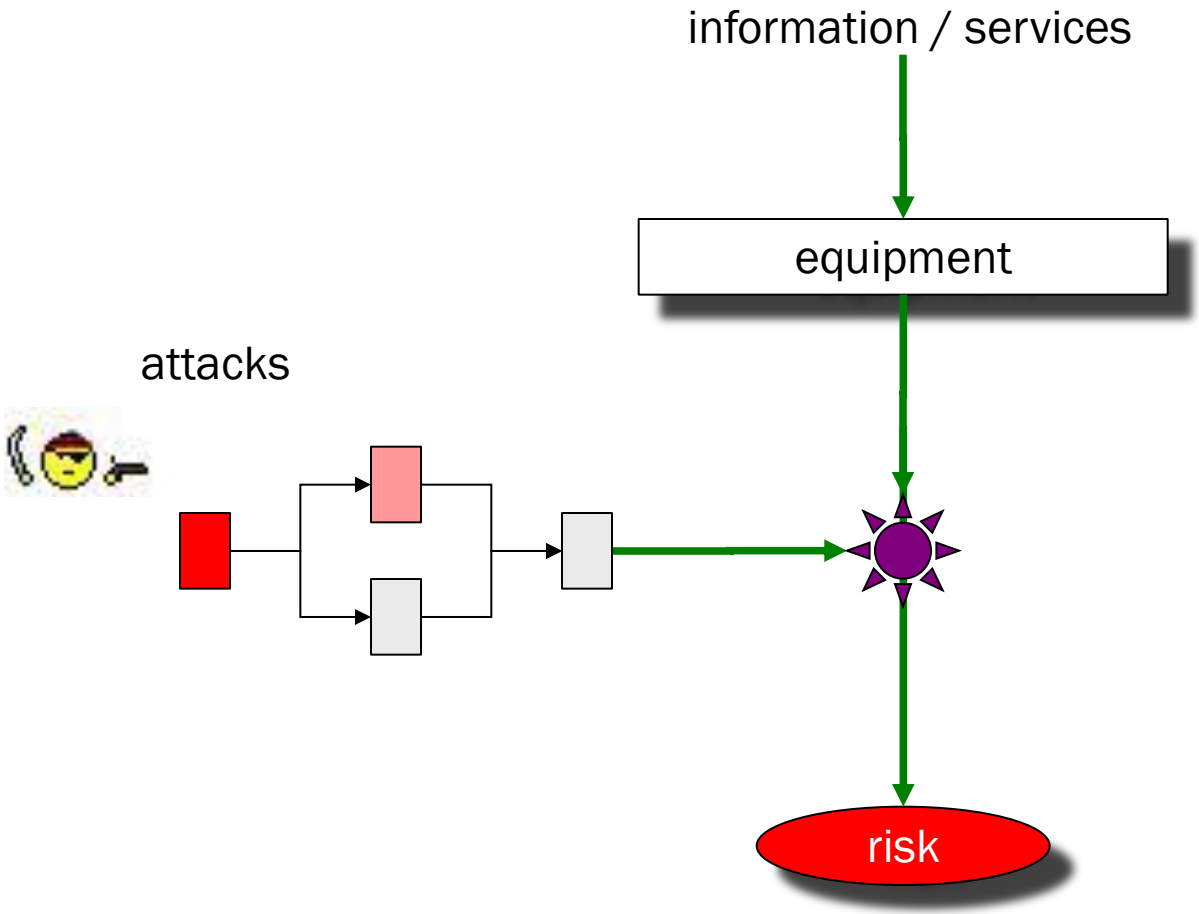
José A. Mañas

Universidad Politécnica de Madrid

jmanas@dit.upm.es

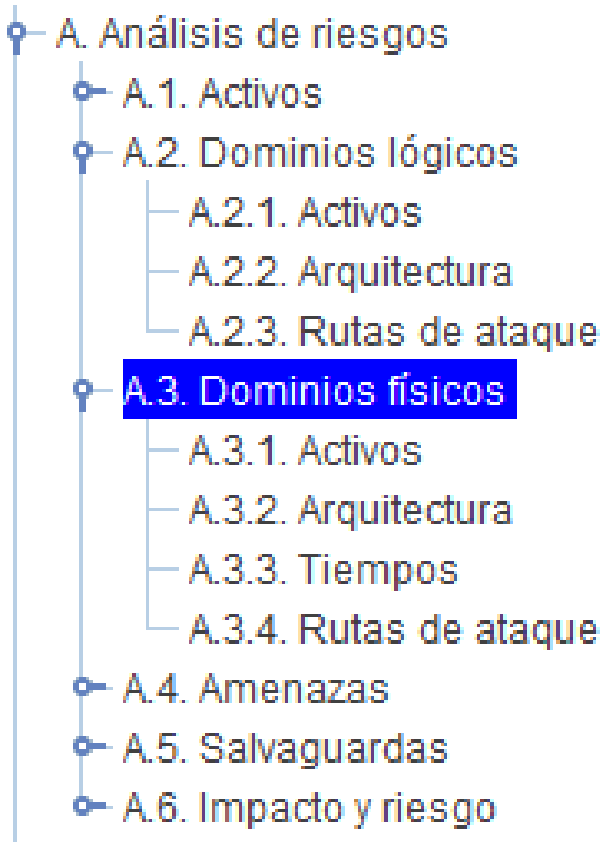
Índice

Attacks



ataques

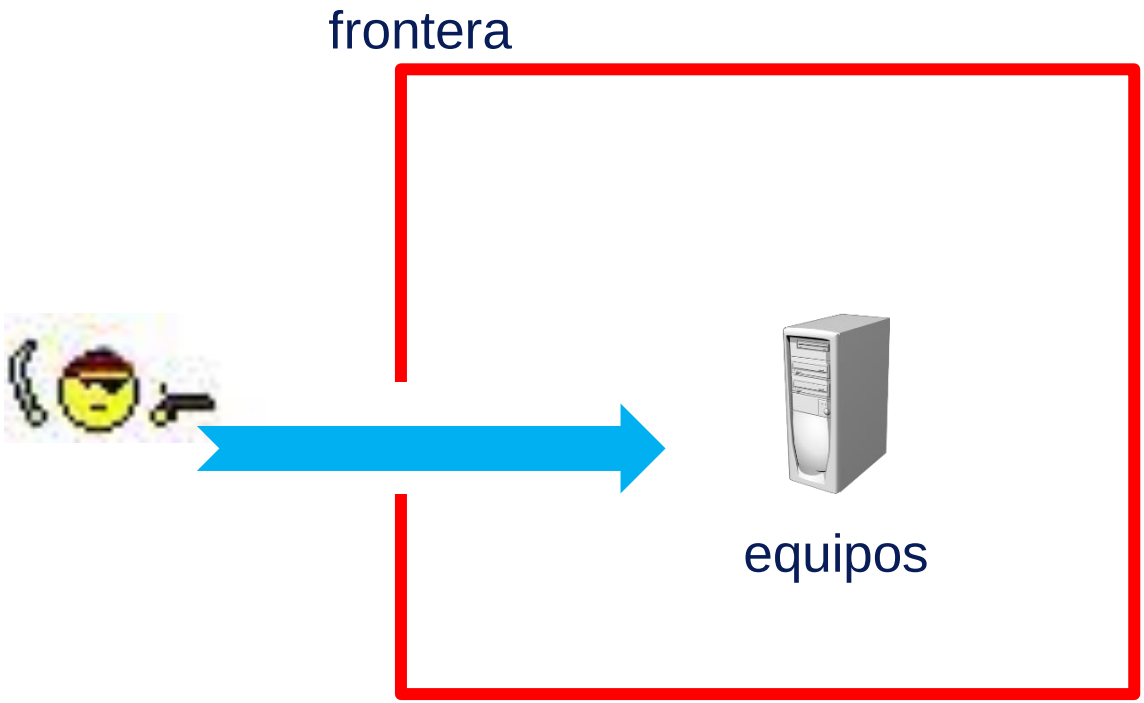
en PILAR



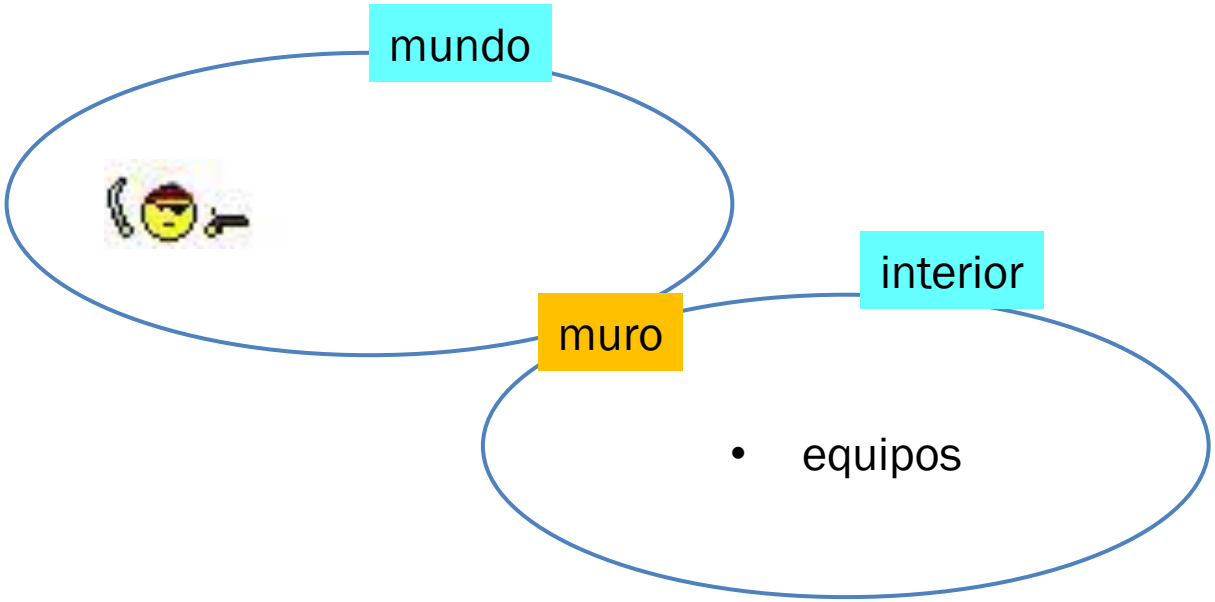
ataques

dominios físicos

- zonas físicas separadas por fronteras
- el atacante necesita atravesar el perímetro para acceder al interior

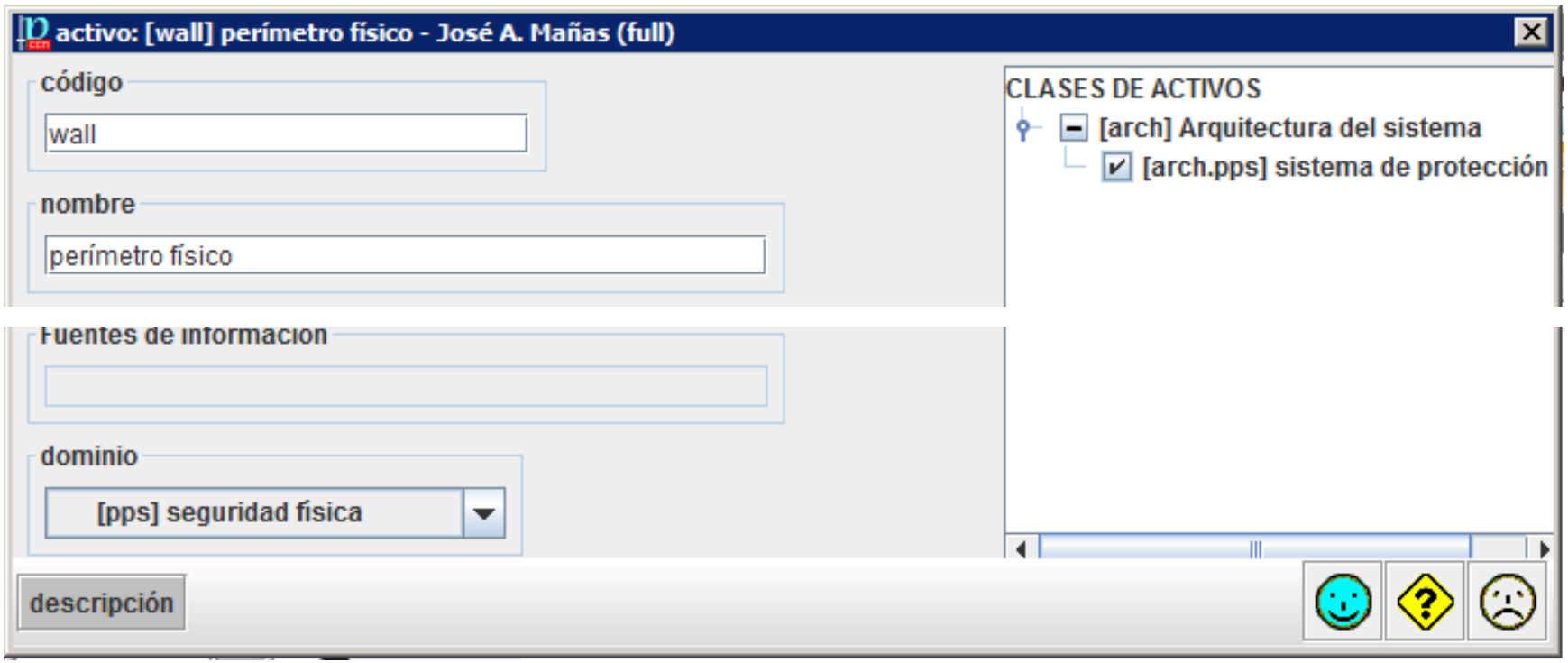


dominios físicos



ataques

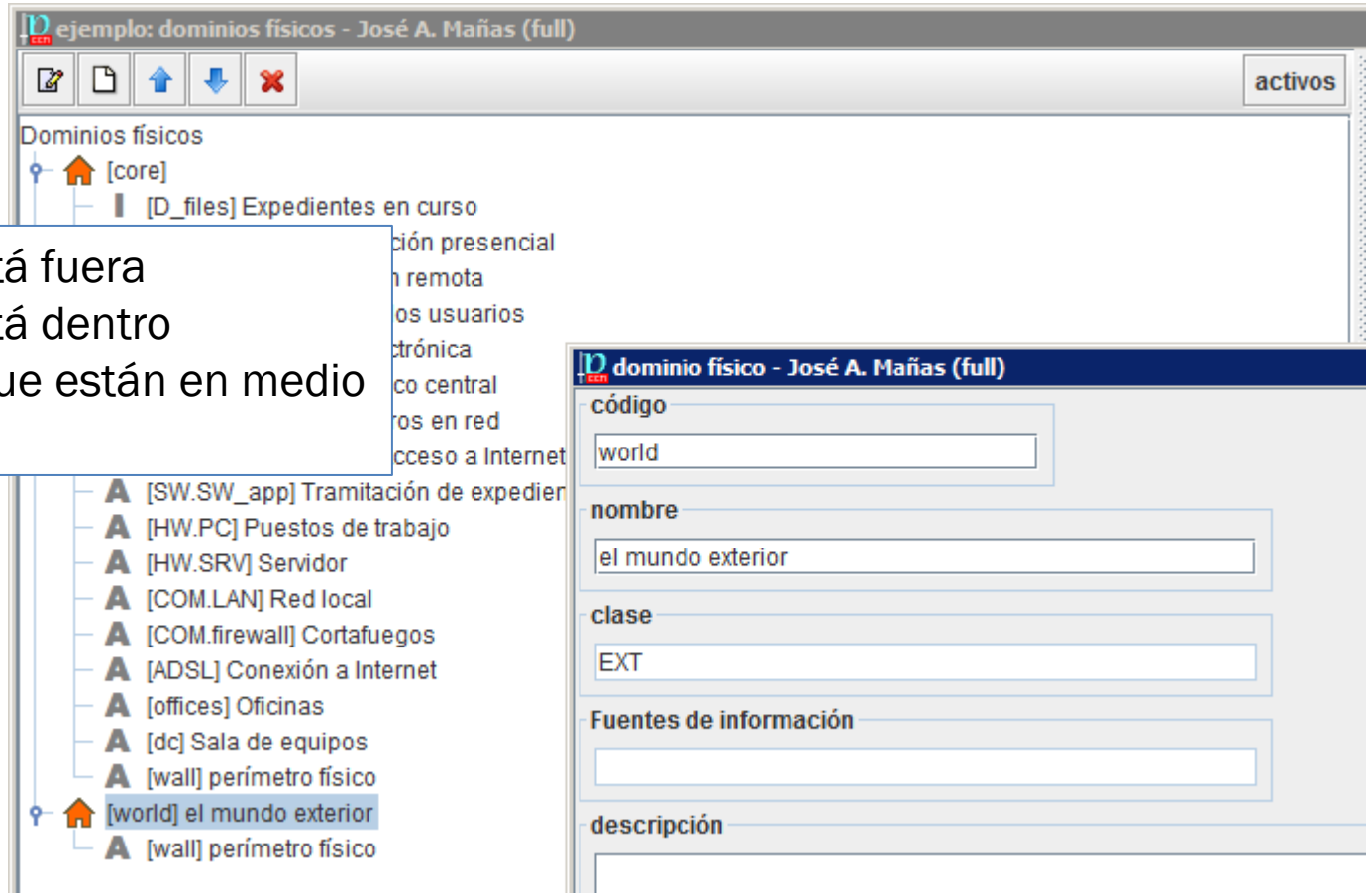
activos (lo de siempre)



ataques

dominios físicos

- este mundo se divide entre ...



- lo que está fuera
- lo que está dentro
- y cosas que están en medio

ataques

frontera

- la frontera puede estar formada por varios activos
- es necesario que haya algo de tipo PPS que es lo que detiene los ataques
- además pueden haber elementos que contribuyen a que el PPS sea eficaz
  - cámaras
  - servidores
  - personas
  - sistemas de alarma
  - ...

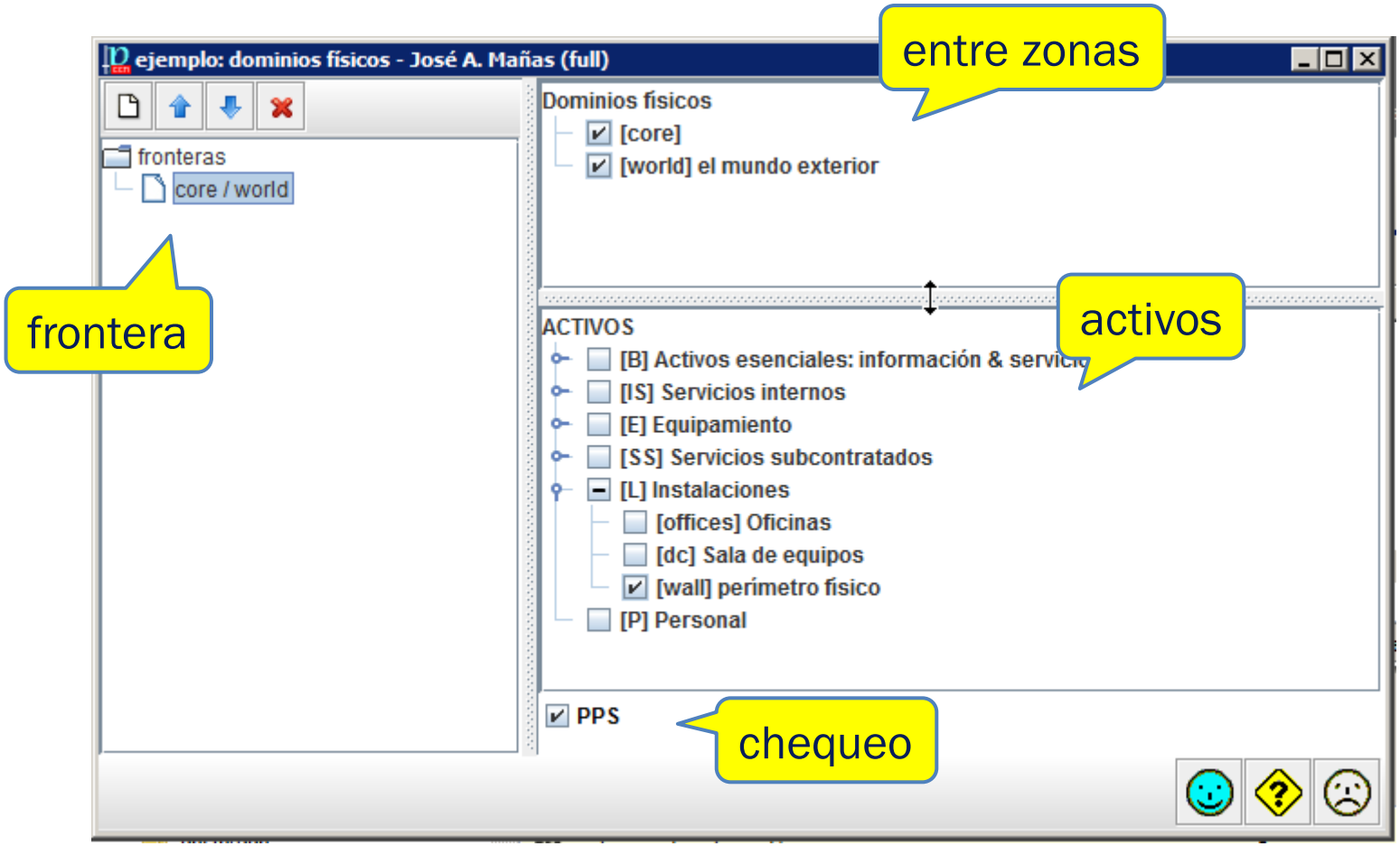
valoración de eficacia

1. se valora el elemento PPS que es la base de la eficacia
2. se corrige la eficacia protectora con la valoración de lo demás

- se usan las salvaguardas de PILAR para valorar cada activo

ataques

fronteras

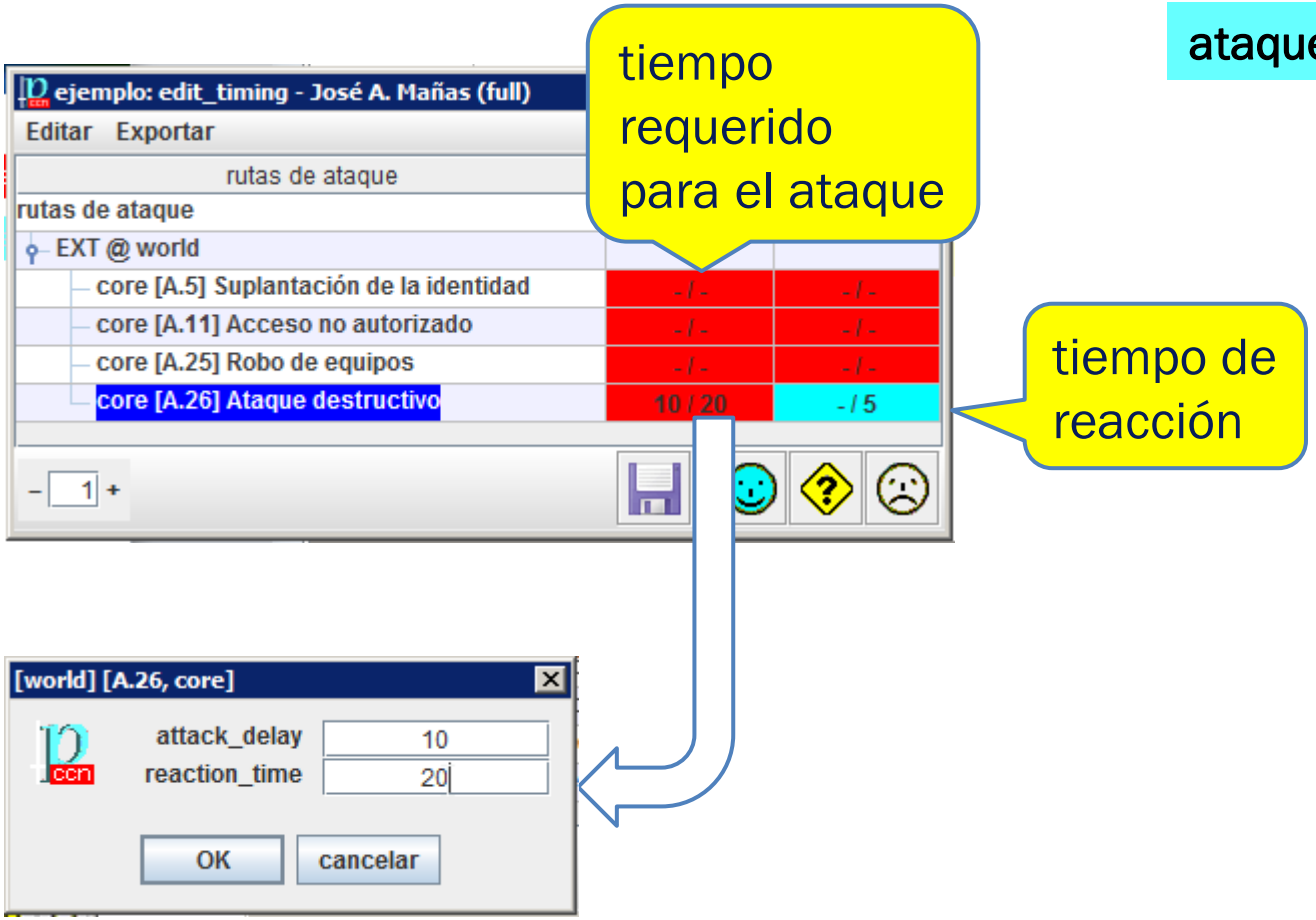


ataques

tiempos

ataque posible

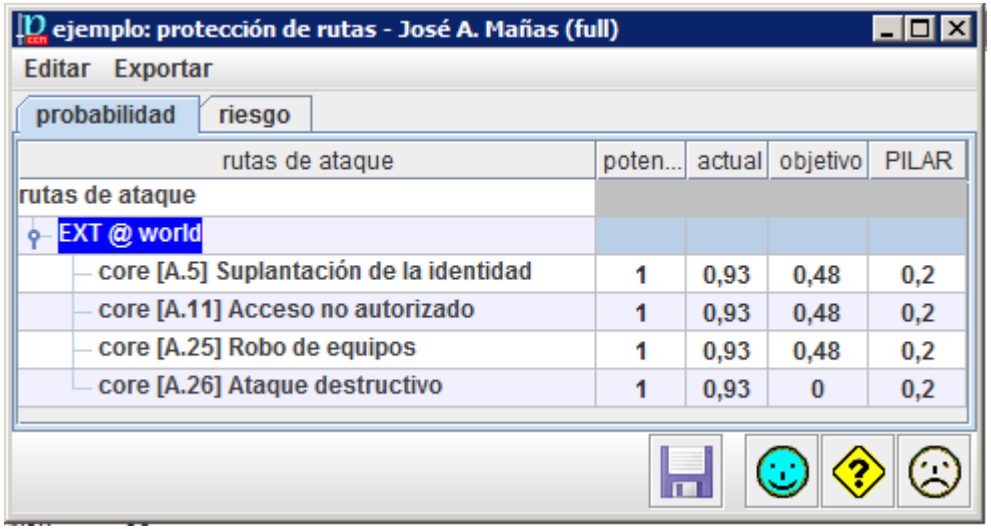
ataque conjurado



ataques

sendas de ataque

1. El atacante (EXT) está en su dominio (world)
   - podría entrar superando el perímetro
2. El atacante entra en la zona interna
   - puede atacar a los equipos



rutas de ataque	poten...	actual	objetivo	PILAR
rutas de ataque				
EXT @ world				
core [A.5] Suplantación de la identidad	1	0,93	0,48	0,2
core [A.11] Acceso no autorizado	1	0,93	0,48	0,2
core [A.25] Robo de equipos	1	0,93	0,48	0,2
core [A.26] Ataque destructivo	1	0,93	0	0,2

ataques

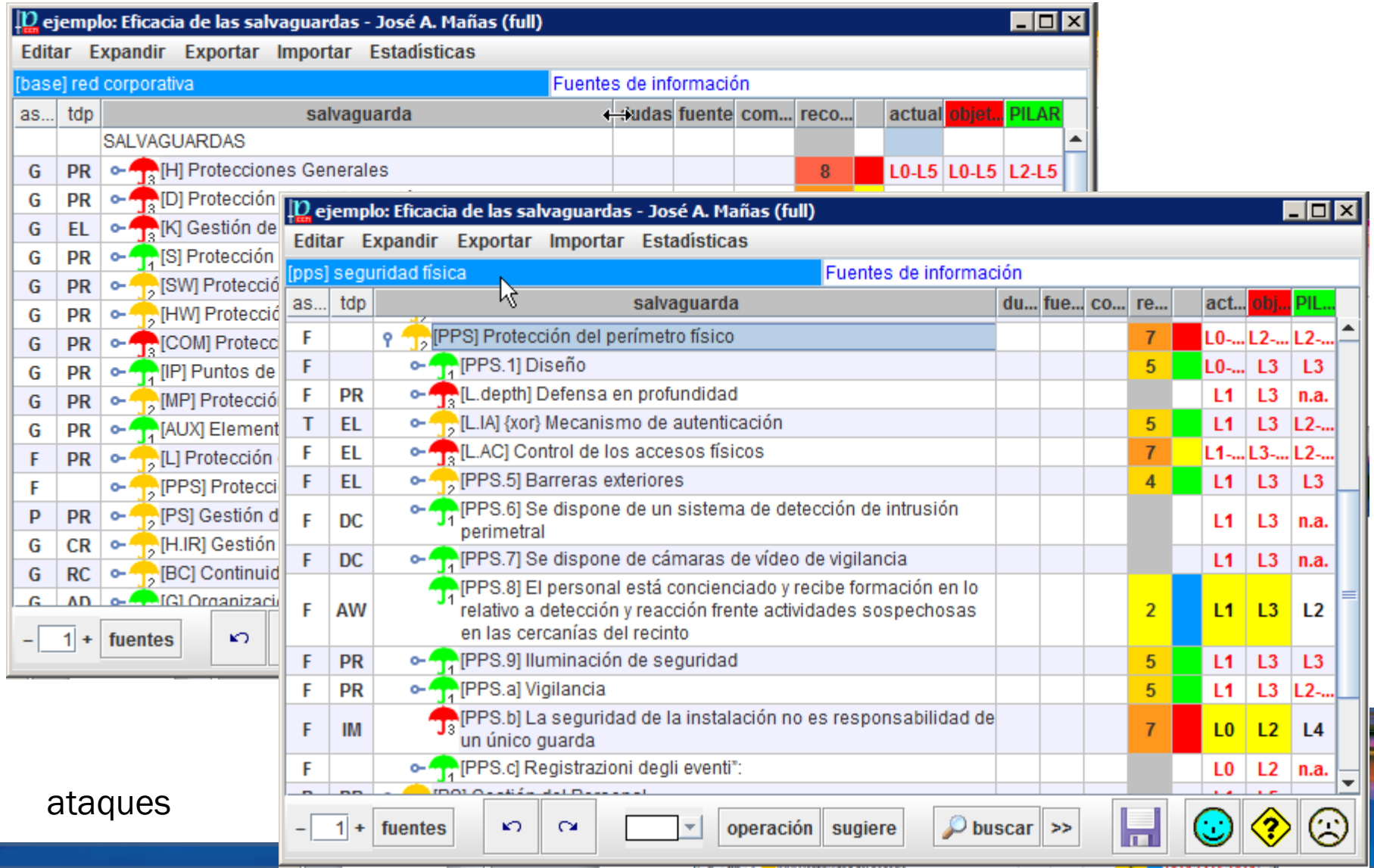
sendas de ataque

1. El atacante (EXT) está en su dominio (world)
   - podría entrar superando el perímetro
2. El atacante entra en la zona interna
   - puede atacar a los equipos

rutas de ataque	potenc...	actual	objetivo	PILAR
rutas de ataque				
EXT @ world				
core [A.5] Suplantación de la identidad	{5,0}	{3,7}	{0,96}	{5,0}
core [A.11] Acceso no autorizado	{5,0}	{3,7}	{0,96}	{5,0}
core [A.25] Robo de equipos	{4,6}	{2,6}	{0,62}	{4,6}
core [A.26] Ataque destructivo	{5,0}	{3,7}	{0}	{5,0}

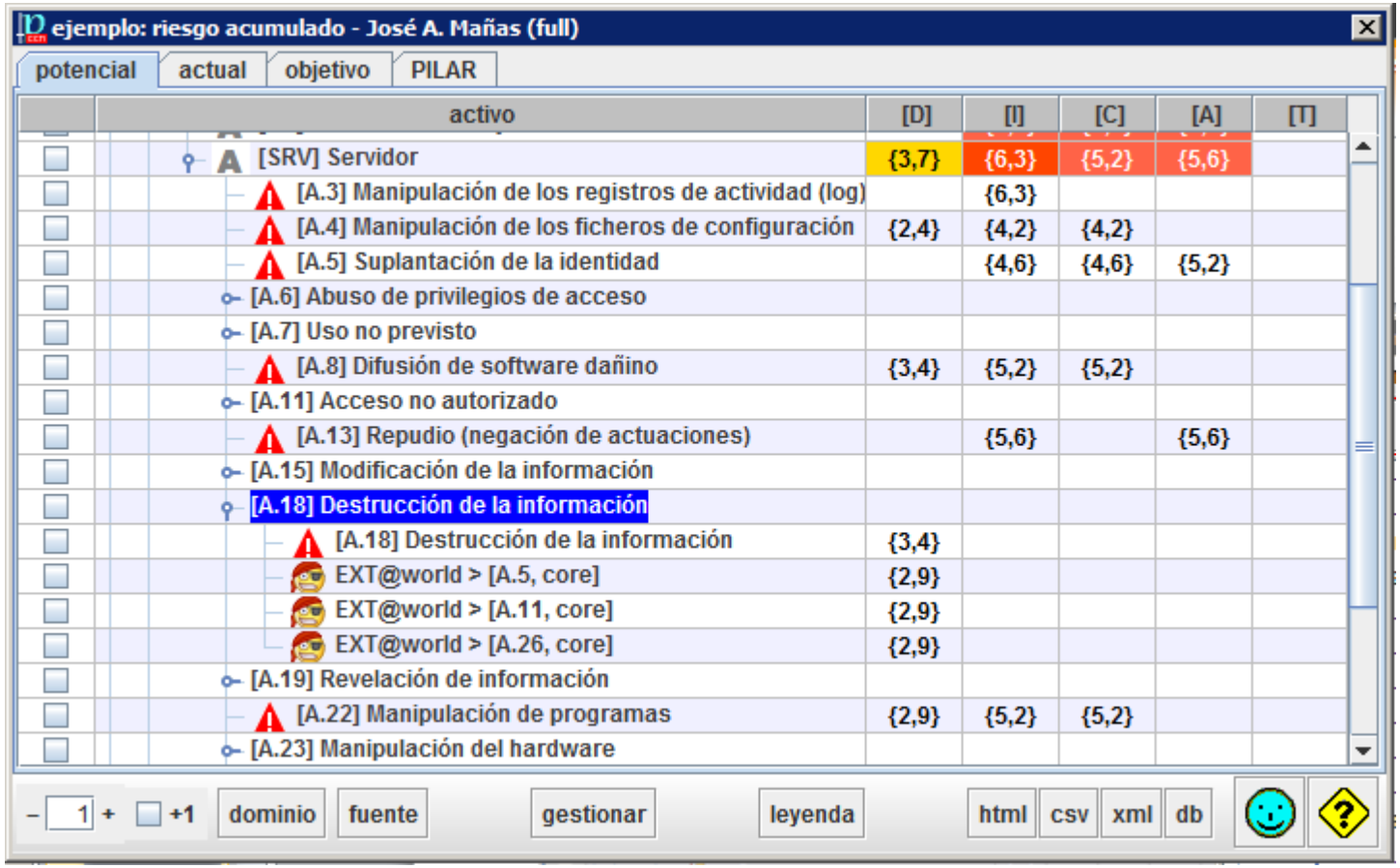
ataques

protección de los activos → protección ruta



ataques

mitigación del riesgo



ataques

mitigación del riesgo

ejemplo: riesgo acumulado - José A. Mañas (full)

potencial | actual | objetivo | PILAR | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensi...	riesgo	actual	objetivo	PILAR
[HW.SRV] Servidor	[A.3] Manipulación de los registros de activida...	[I]	{6,3}	{4,5}	{1,0}	{1,9}
[HW.SRV] Servidor	[A.15] Modificación de la información	[I]	{5,8}	{4,1}	{0,89}	{1,4}
[HW.SRV] Servidor	[A.13] Repudio (negación de actuaciones)	[I]	{5,6}	{4,1}	{0,70}	{1,1}
[HW.SRV] Servidor	[A.13] Repudio (negación de actuaciones)	[A]	{5,6}	{4,1}	{0,70}	{1,1}
[HW.SRV] Servidor	[A.22] Manipulación de programas	[C]	{5,2}	{3,8}	{0,74}	{0,95}
[HW.SRV] Servidor	[A.5] Suplantación de la identidad	[A]	{5,2}	{3,4}	{1,6}	{0,87}
[HW.SRV] Servidor	[A.22] Manipulación de programas	[I]	{5,2}	{3,5}	{0,79}	{0,96}
[HW.SRV] Servidor	[A.8] Difusión de software dañino	[I]	{5,2}	{3,6}	{0,48}	{0,88}
[HW.SRV] Servidor	[A.6] Abuso de privilegios de acceso	[I]	{5,2}	{3,2}	{0,79}	{0,99}
[HW.SRV] Servidor	[A.6] Abuso de privilegios de acceso	[C]	{5,2}	{3,5}	{0,75}	{0,97}
[HW.SRV] Servidor	[A.8] Difusión de software dañino	[C]	{5,2}	{3,7}	{0,45}	{0,87}
[HW.SRV] Servidor	EXT@world > [A.5, core] > [A.15] Modificación ...	[I]	{5,0}	{3,2}	{0,73}	{0,91}
[HW.SRV] Servidor	EXT@world > [A.11, core] > [A.15] Modificació...	[I]	{5,0}	{3,2}	{0,73}	{0,91}
[HW.SRV] Servidor	EXT@world > [A.26, core] > [A.15] Modificació...	[I]	{5,0}	{3,2}	{0,73}	{0,91}
[HW.SRV] Servidor	[A.25] Robo de equipos	[C]	{5,0}	{3,0}	{0,70}	{0,97}
[HW.SRV] Servidor	EXT@world > [A.5, core] > [A.6] Abuso de privi...	[I]	{4,8}	{2,7}	{0,69}	{0,89}
[HW.SRV] Servidor	EXT@world > [A.11, core] > [A.6] Abuso de pri...	[I]	{4,8}	{2,7}	{0,69}	{0,89}
[HW.SRV] Servidor	EXT@world > [A.26, core] > [A.6] Abuso de pri...	[I]	{4,8}	{2,7}	{0,69}	{0,89}

A | gestionar | leyenda | csv | xml | db

ataques

perfil del atacante

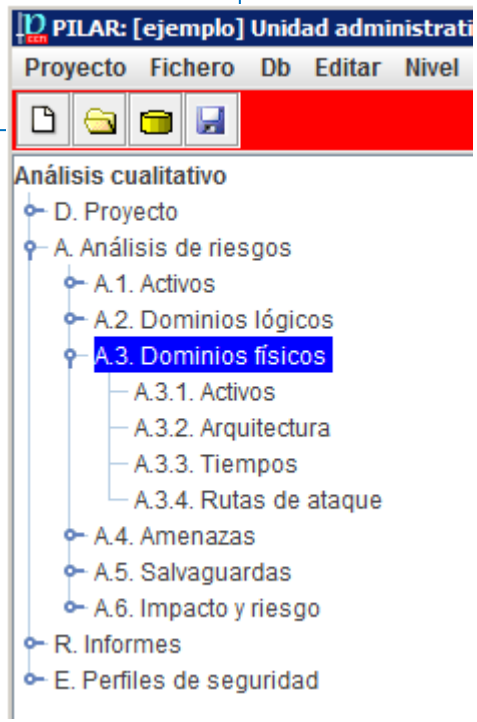
- In .CAR we may specify attacks for internal and external origins

STIC_ext_en.car - Notepad

File Edit Format View Help

tsv= 2014-08-27.tsv

physical-threats:EXT= 2014-08-27_physical.xml



ataques

perfil del atacante

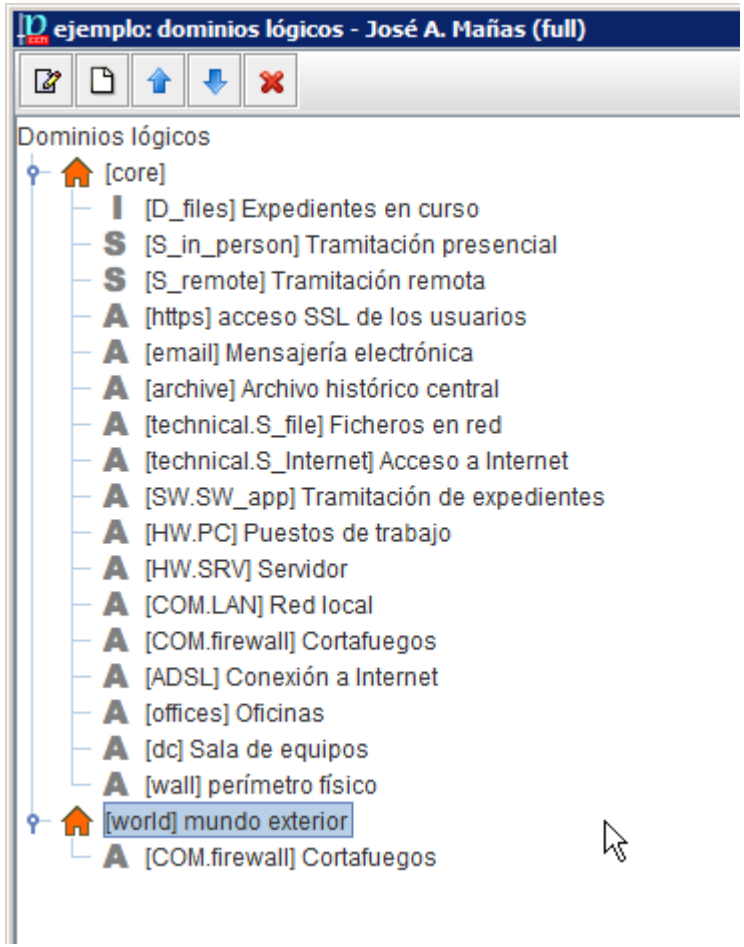
2014-08-27_physical.xml

```
<threat-standard-values>
 <pps>
  <threat Z="A.5" f="1.0" follow="A" />
  <threat Z="A.11" f="1.0" follow="A" />
  <threat Z="A.25" f="1.0" follow="A.25" />
  <threat Z="A.26" f="1.0" follow="A" />
 </pps>

 <family F="HW">
  <threat f="1.0" s="1d" Z="A.6">
   <set D="D" deg="0.1"/>
   <set D="I" deg="0.1"/>
   <set D="C" deg="0.5"/>
  </threat>
  <threat f="1.0" s="1h" Z="A.7">
   <set D="D" deg="0.1"/>
   <set D="I" deg="0.01"/>
   <set D="C" deg="0.1"/>
  </threat>
```

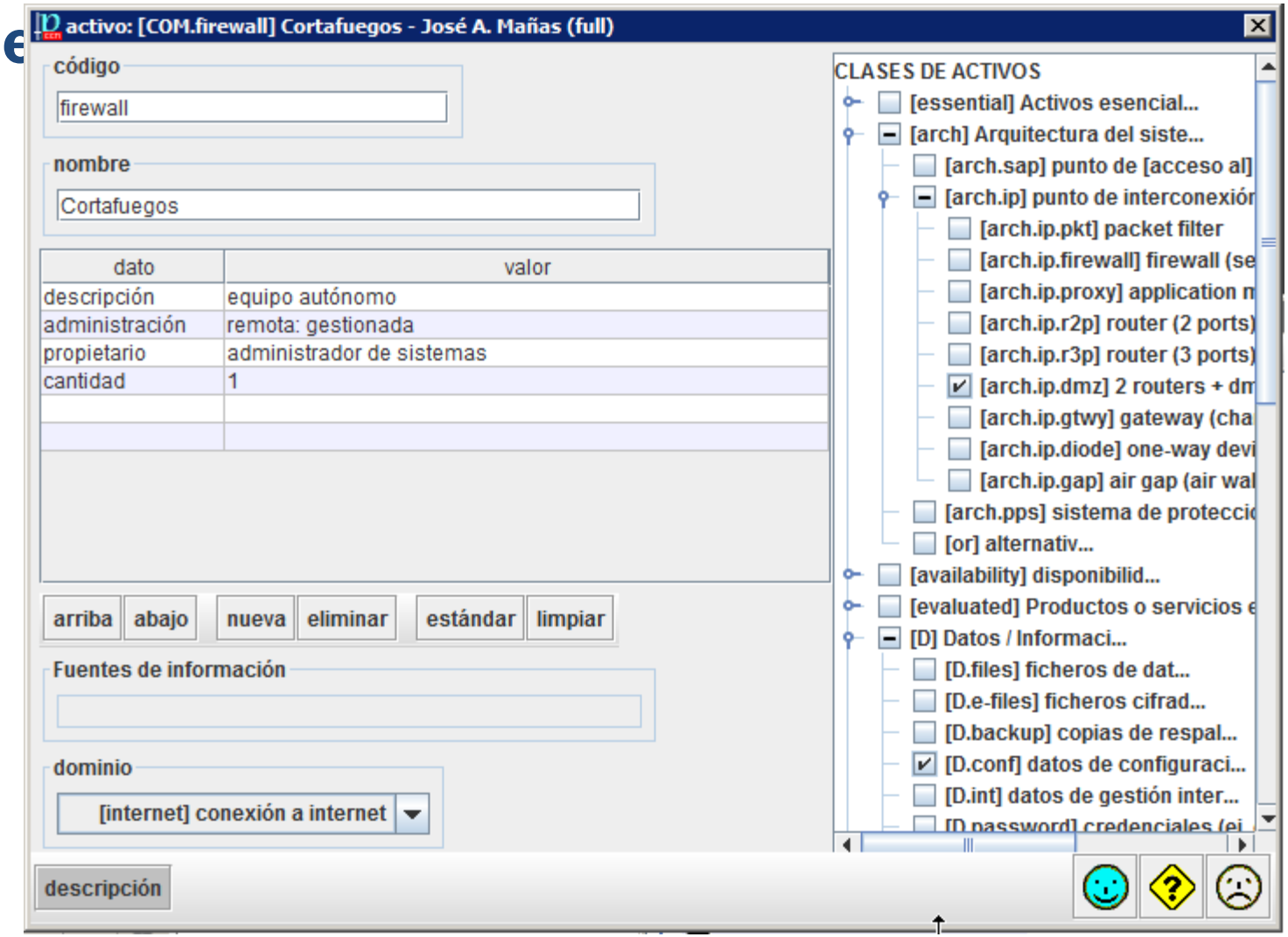
ataques

ciberseguridad – interconexiones lógicas



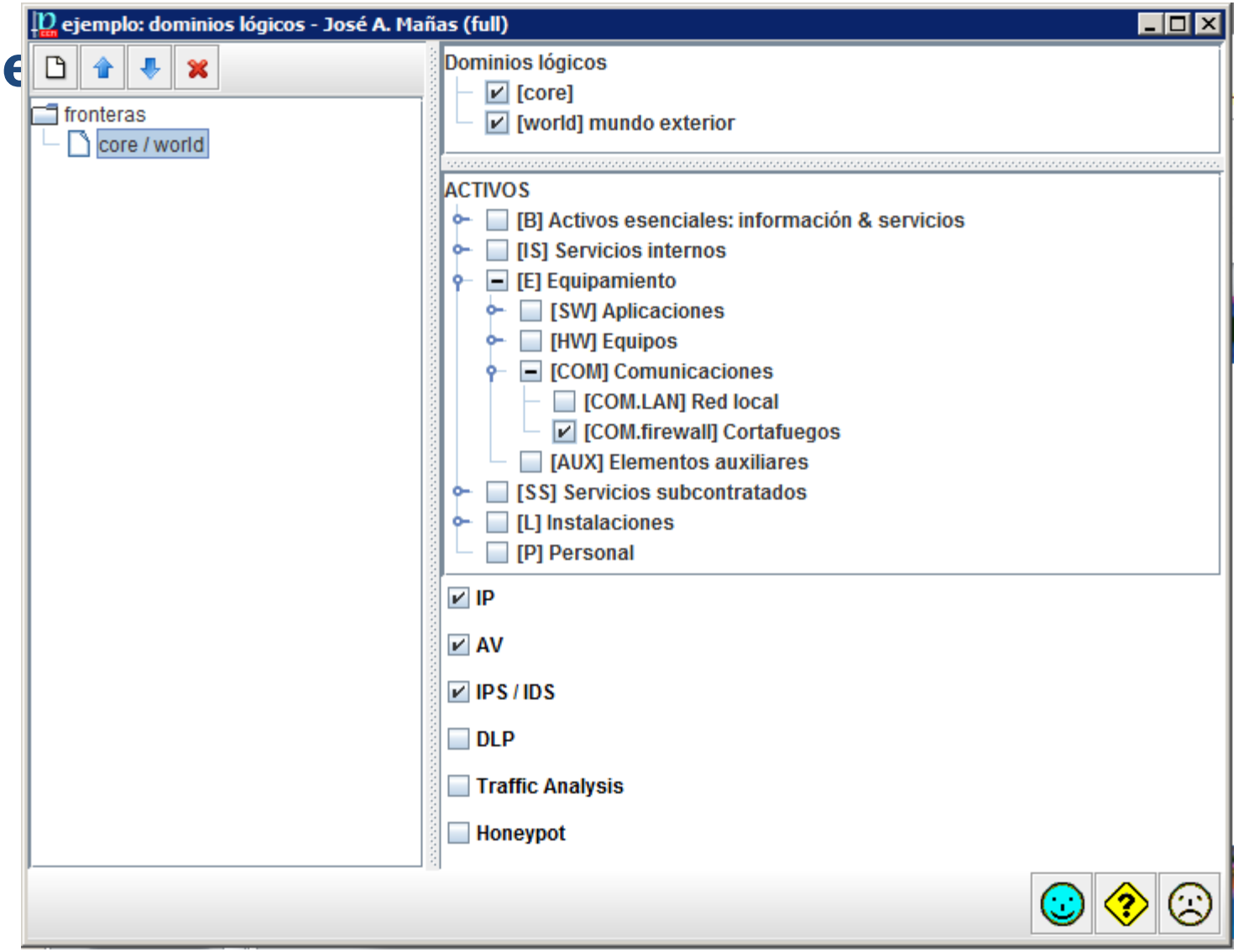
ataques

cibe



ataques

cibe



ataques

dónde estamos

- alfa
- experimentando
  - rápido para escenarios estándar
  - equilibrio entre complejidad y utilidad práctica
    (que el análisis te diga qué debes proteger y qué no puedes)
- ajustando
  - perfiles de atacantes
  - salvaguardas
  - recomendaciones
- pendiente
  - μPILAR /pps

- **E-Mails**
  - ccn-cert@cni.es
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - sondas@ccn-cert.cni.es
  - redsara@ccn-cert.cni.es
  - carmen@ccn-cert.cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es

Síguenos en Linked in