ANÁLISIS Y GESTIÓN DE RIESGOS
Herramienta PILAR

José Luis Quintero Villarroya
Subdirección General TIC
MINISTERIO DE DEFENSA

Patrocinadores

Caelum
SEI Partner | Carnegie Mellon

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

Colaboradores

GRUPO SMS
DiCe
UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

- **FORO: ASOCIACIÓN ESPAÑOLA DE CALIDAD**

  CSTIC 2012
- **TÍTULO: ANÁLISIS Y GESTIÓN DE RIESGOS. PILAR**
- **PONENTE:**
  - **José Luis Quintero Villarroya**
  - **SDG TIC. Ministerio de Defensa**
- **FECHA: Madrid 18 septiembre 2012**

Evolución de la Seguridad

- Primera Generación (80s)
  - *checklists* (auditoría del estado de seguridad de un S.I.)
- Segunda Generación (90s)
  - métodos específicos (análisis de riesgos, coste-beneficio)
- Tercera Generación (200x)
  - modelos de seguridad conectados a otros métodos (desarrollo …)
  - nuevas técnicas (gestión, comunicaciones, ...)
  - SGSI: sistemas de gestión de la seguridad de la información

Objetivos de la seguridad

- Mantener la **disponibilidad** de los datos almacenados, así como su disposición a ser compartidos
  - contra la interrupción del servicio
- Mantener la **integridad** de los datos ...
  - contra las manipulaciones
- Mantener la **confidencialidad** de los datos almacenados, procesados y transmitidos
  - contra las filtraciones
- Asegurar la identidad de origen y destino (**autenticidad**)
  - frente a la suplantación o engaño
- Disponer de **trazabilidad**
  - Para analizar, entender, perseguir y aprender

Seguridad de los Sistemas de Información

La capacidad de los SI de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la **disponibilidad, autenticidad, integridad y confidencialidad** de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles

Riesgo:

estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización

¿ Para que se utiliza el Análisis y Gestión de Riesgos ?

Para proveer la base que determine la necesidad de seguridad en sus sistemas TIC.

OBJETIVOS

Determinar fortaleza de la seguridad sistemas TIC
Apoyo decisión de mejoras en la seguridad

Gestión de riesgos

Análisis de riesgos

proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización

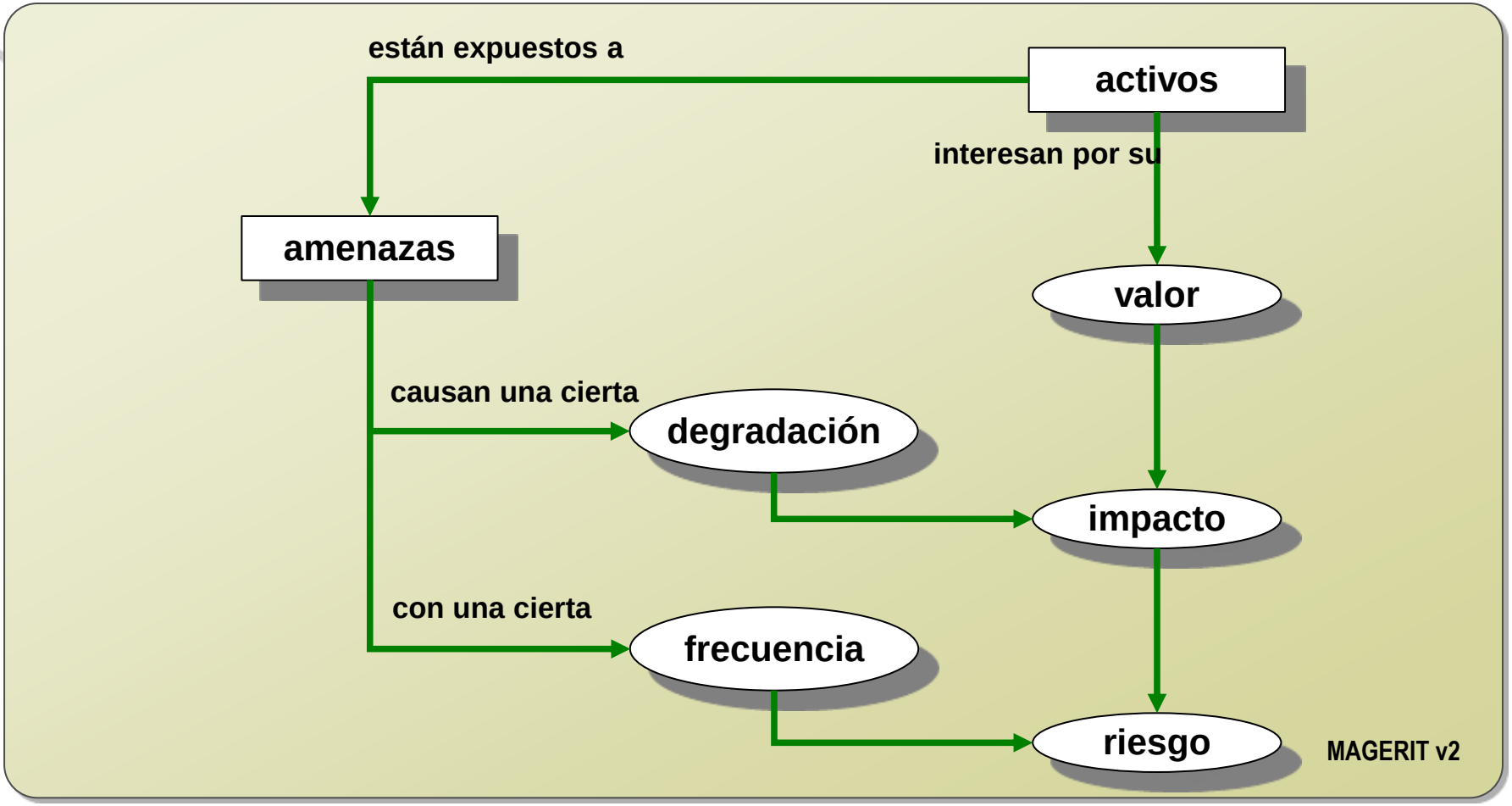
Evaluación de los riesgos

proceso en el que se coteja el riesgo estimado contra los criterios de la organización para determinar la importancia del riesgo

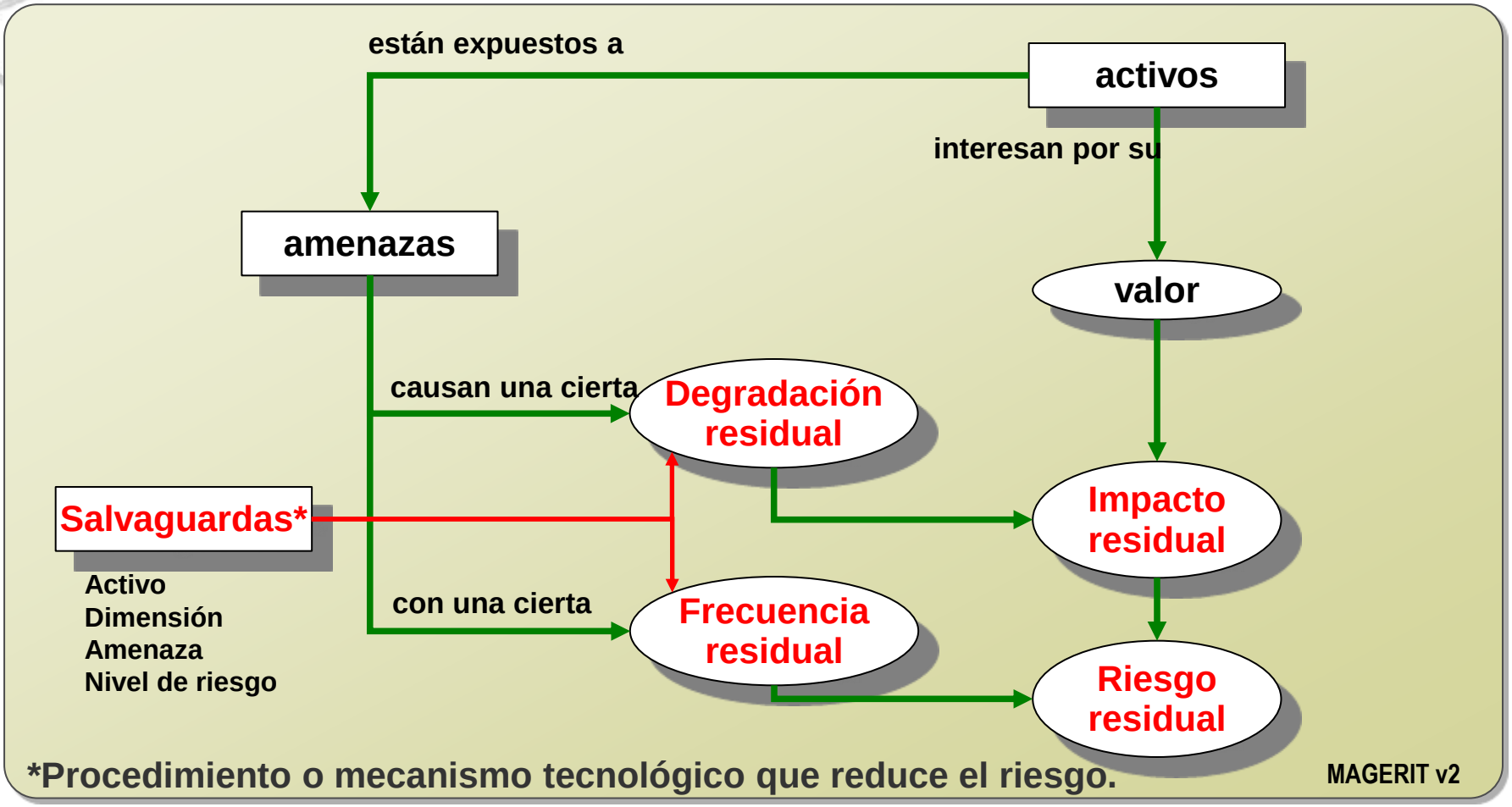
Tratamiento de riesgos

selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados

Análisis de riesgos



Gestión de riesgos



¿Qué hacer con el riesgo?

- Evitarlo
  - si se puede ... es la solución ideal
- Reducirlo | mitigarlo
  - ocurre menos
  - impacto limitado
- Transferirlo
  - se le pasa a otra organización
  - ya no es “mi problema”
- Asumirlo | aceptarlo
  - pasa a contabilizarse como gasto operacional

ANALISIS RIESGOS … CCN-STIC 101

5.1. DE DOCUMENTACIÓN DE SEGURIDAD

15. Todo Sistema que maneje información nacional clasificada deberá tener actualizada la documentación de seguridad que se relaciona en este procedimiento o en la norma correspondiente. Esta documentación será revisada y validada según lo establecido en el apartado 6 de este procedimiento.

	SECRETO / RESERVADO	CONFIDENCIAL	DIFUSION LIMITADA / SIN CLASIFICAR
Concepto de Operación.	SI	SI	SI
Análisis o valoración de riesgos.	FORMAL	NO FORMAL	NO FORMAL
Declaración de Requisitos de Seguridad (DRS).	SI	SI	OPCIONAL
Procedimientos Operativos de Seguridad (POS).	SI	SI	SI
Documento de Acreditación.	SI	SI	SI

Tabla 1. Documentación de Seguridad de los Sistemas

A. RIESGOS FORMAL. Basado en metodología aprobada que contempla una valoración CUANTITATIVA / CUALITATIVA de la amenazas / riesgos y salvaguardas.

METODOLOGIA DE ANALISIS Y GESTION DE RIESGOS DE LOS SISTEMAS DE INFORMACION DE LAS ADMINISTRACIONES PUBLICAS

V1 AÑO 1997

OBJETIVO MAGERIT:

- Estudio de los riesgos que soporta un sistema de información. Recomendar contramedidas prevenir/impedir/reducir/controlar los riesgos.
- 7 GUÍAS

Trabajo colegiado de:

- M. Administraciones Públicas (MAP) / M. De Defensa (MINISDEF) / M. Economía y Hacienda / M. Sanidad y Consumo / Banco de España / Correos y Telégrafos / Universidad CARLOS III / Informática CAM

Actualización metodología
Alineamiento MAGERIT V2 / PILAR

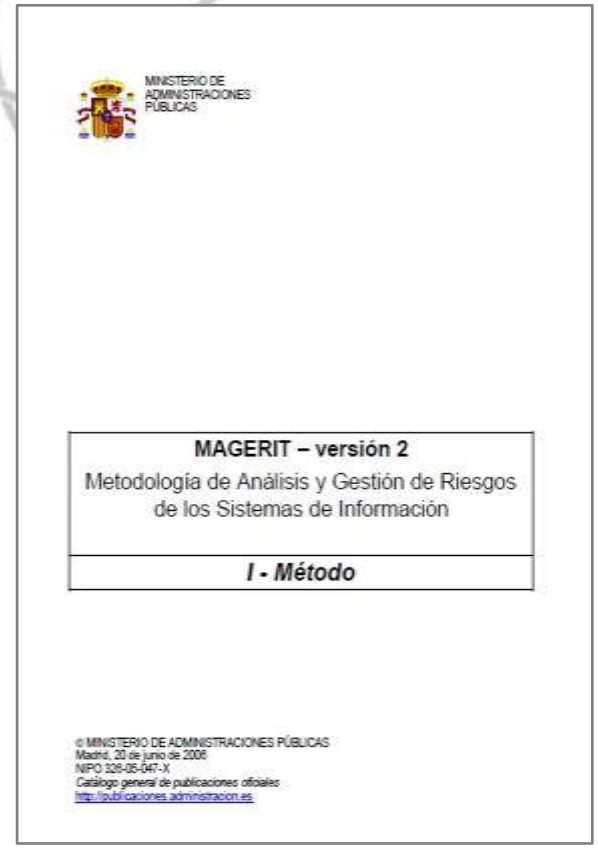
AÑO 2005

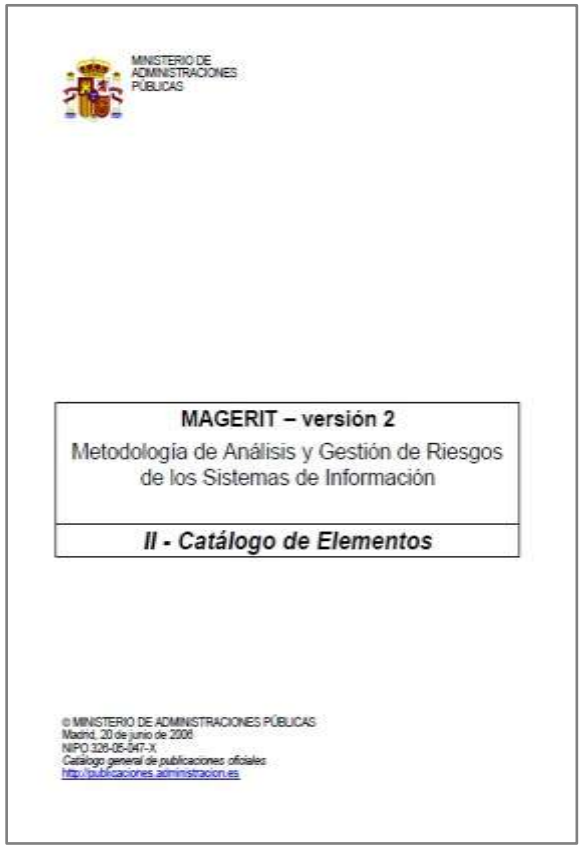
OBJETIVO MAGERIT:

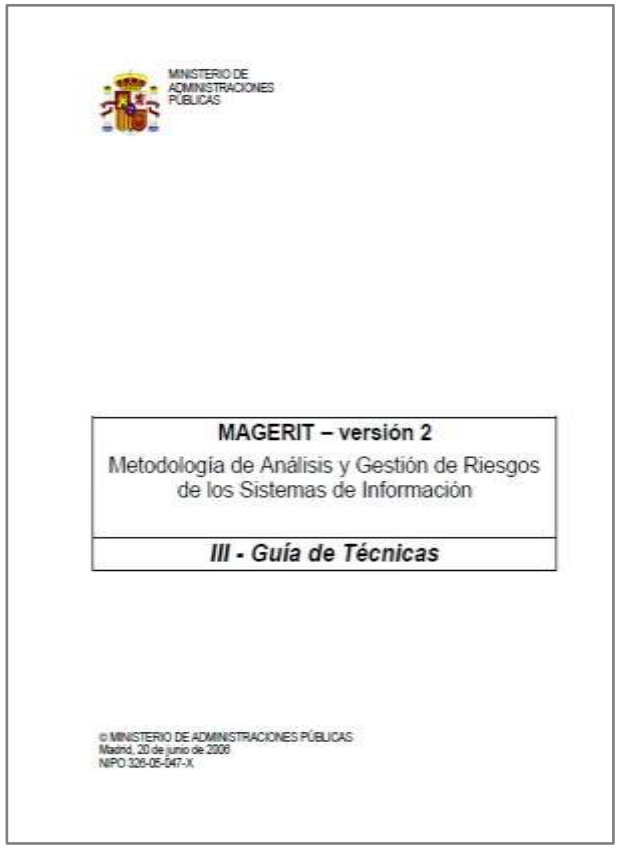
- Actualización Metodología
- Alineamiento METRICA V3
- Alineamiento otras normas internacionales
  - CC / ISO 17799
- Actualización activos / amenazas / salvaguardas
- CALCULO IMPACTO / RIESGO

Trabajo colegiado de:

- M. Administraciones Públicas (MAP) / M. De Defensa (CCN)





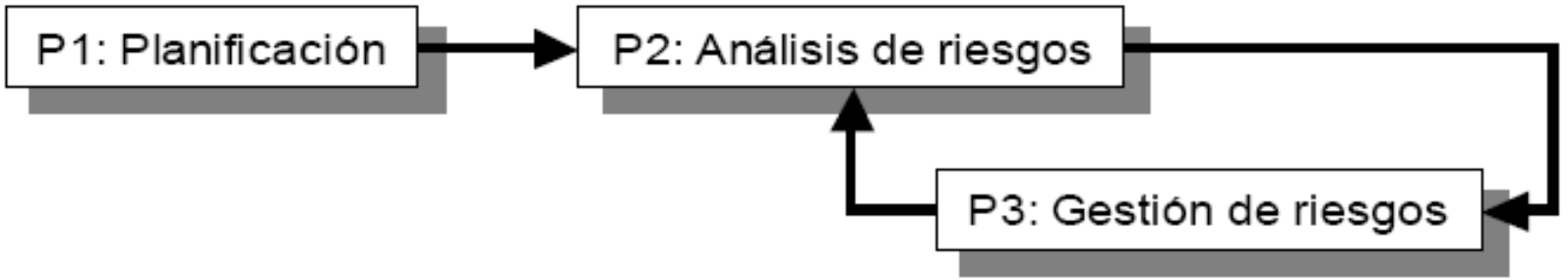


MAGERIT Versión 2 (junio de 2006)
http://administracionelectronica.gob.es

Próxima publicación V.3

DESARROLLO PROYECTO ANÁLISIS DE RIESGOS

PROCESOS-ACTIVIDADES-TAREAS



Proyecto Análisis de Riesgos

1. planificación del proyecto de análisis y gestión de riesgos

- .1 oportunidad
- .2 alcance
- .3 planificación
- .4 lanzamiento

2. análisis de riesgos

- .1 activos
- .2 amenazas
- .3 salvaguardas
- .4 estado de riesgo

3. gestión de riesgos

- .1 toma de decisiones
- .2 plan de seguridad
- .3 ejecución del plan

Proyecto Análisis de Riesgos

Proceso P1: Planificación del proyecto de análisis y gestión de riesgos

Actividad A1.1: Estudio de oportunidad
- Tarea T1.1.1: Determinar la oportunidad

Actividad A1.2: Determinación del alcance del proyecto
- Tarea T1.2.1: Objetivos y restricciones generales
- Tarea T1.2.2: Determinación del dominio y límites
- Tarea T1.2.3: Identificación del entorno
- Tarea T1.2.4: Estimación de dimensiones y coste

Actividad A1.3: Planificación del proyecto
- Tarea T1.3.1: Evaluar cargas y planificar entrevistas
- Tarea T1.3.2: Organizar a los participantes
- Tarea T1.3.3: Planificar el trabajo

Actividad A1.4: Lanzamiento del proyecto
- Tarea T1.4.1: Adaptar los cuestionarios
- Tarea T1.4.2: Criterios de evaluación
- Tarea T1.4.3: Recursos necesarios
- Tarea T1.4.4: Sensibilización

Proceso P2: Análisis de riesgos

Actividad A2.1: Caracterización de los activos
- Tarea T2.1.1: Identificación de los activos
- Tarea T2.1.2: Dependencias entre activos
- Tarea T2.1.3: Valoración de los activos

Actividad A2.2: Caracterización de las amenazas
- Tarea T2.2.1: Identificación de las amenazas
- Tarea T2.2.2: Valoración de las amenazas

Actividad A2.3: Caracterización de las salvaguardas
- Tarea T2.3.1: Identificación de las salvaguardas existentes
- Tarea T2.3.2: Valoración de las salvaguardas existentes

Actividad A2.4: Estimación del estado de riesgo
- Tarea T2.4.1: Estimación del impacto
- Tarea T2.4.2: Estimación del riesgo
- Tarea T2.4.3: Interpretación de los resultados

Proceso P3: Gestión de riesgos

Actividad A3.1: Toma de decisiones
- Tarea T3.1.1: Calificación de los riesgos

Actividad A3.2: Plan de seguridad
- Tarea T3.2.1: Programas de seguridad
- Tarea T3.2.2: Plan de ejecución

Actividad A3.3: Ejecución del plan
- Tarea T3.3.*: Ejecución de cada programa de seguridad

PILAR / EAR

PROCEDIMIENTO INFORMATICO Y LOGICO DE ANALISIS DE RIESGOS

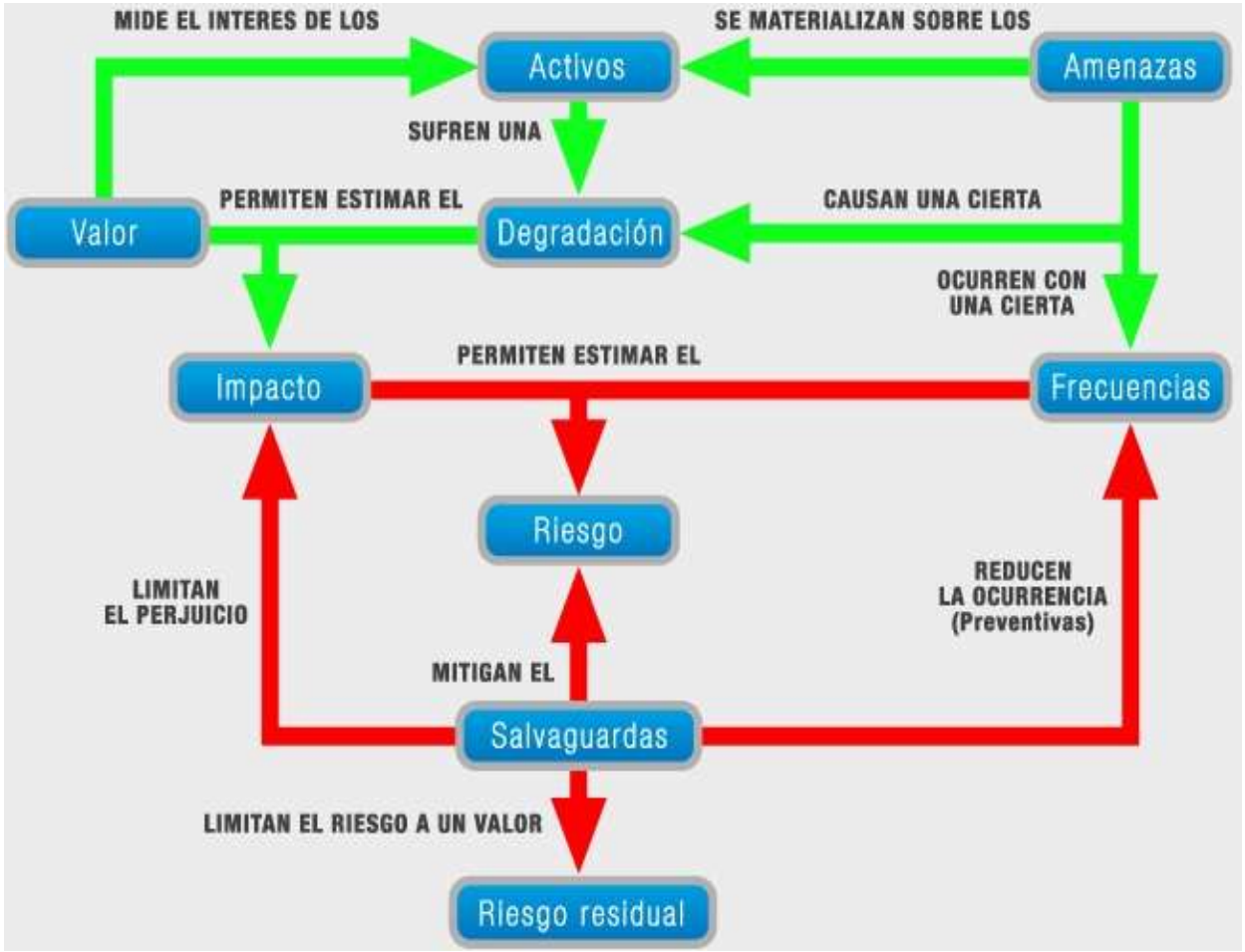
Entorno de Análisis de Riesgos

- proyecto CNI → especificación: CCN → A.L.H. J. Mañas (2003)
- comité validación: CCN + MAP + FNMT + CCAA…
  - PILAR: uso restringido a la administración pública
    EAR: herramienta comercial

OBJETIVO PILAR:

- FACILIDAD DE USO. Realización de un análisis de riesgos intuitivo en u tiempo usuarios inexpertos. *Realización SUGERENCIAS.*
- FLEXIBILIDAD. Adaptarse a las política NACIONAL / EMPRESAS / OTA
- PRIORIZACIÓN SALVAGUARDAS.

PILAR / EAR



La herramienta EAR/PILAR soporta el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit,

PILAR / EAR

- PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

  - **Esquema Nacional de Seguridad.**
  - **ISO/IEC 27002:2005.**
  - **Los Criterios de Seguridad, Normalización y Conservación (MAP)**
  - **LOPD**
  - **NIST SP 800-35**
  - **COBIT**

- El Centro Criptológico Nacional (CCN) ha patrocinado el desarrollo de la herramienta comercial, que está siendo ampliamente utilizada en la administración pública española.

- Aceptada por **OTAN** para la Acreditación de sus Sistemas **NS y NTS**

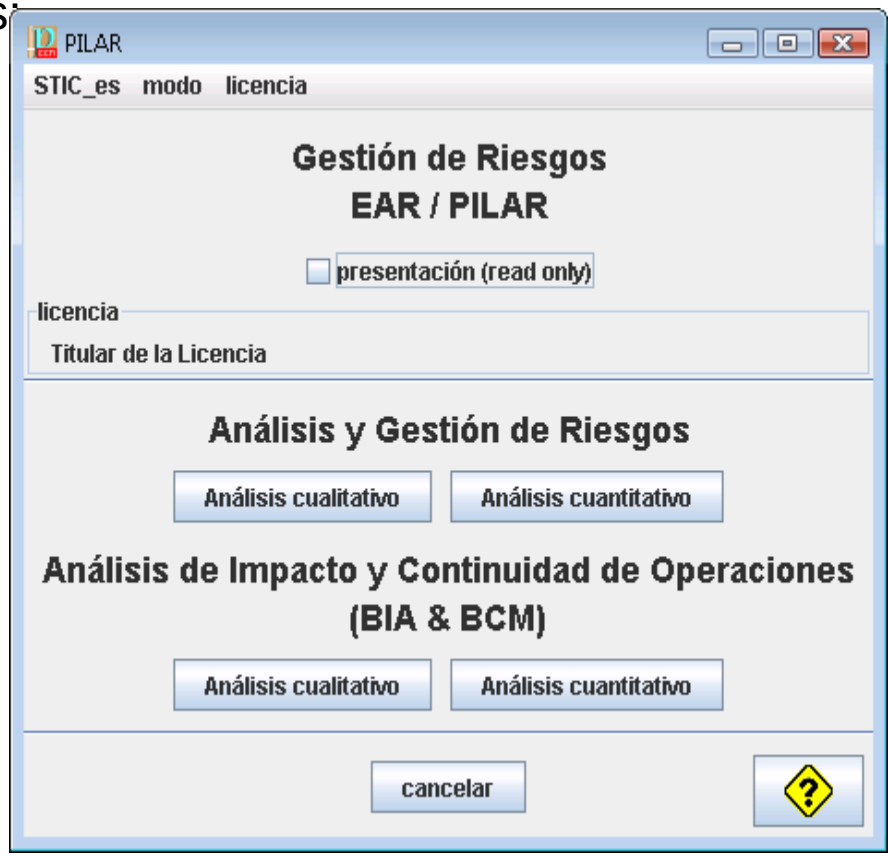
PILAR – Análisis y Gestión de Riesgos

Se analizan los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad

Para tratar el riesgo se proponen:

- salvaguardas (o contramedidas)
- normas de seguridad
- procedimientos de seguridad

analizándose el riesgo residual a lo largo de diversas etapas de tratamiento



Análisis de Impacto y Continuidad de Operaciones

Se analiza el efecto de las interrupciones de servicio teniendo en cuenta la duración de la interrupción.
Para tratar el riesgo se proponen:

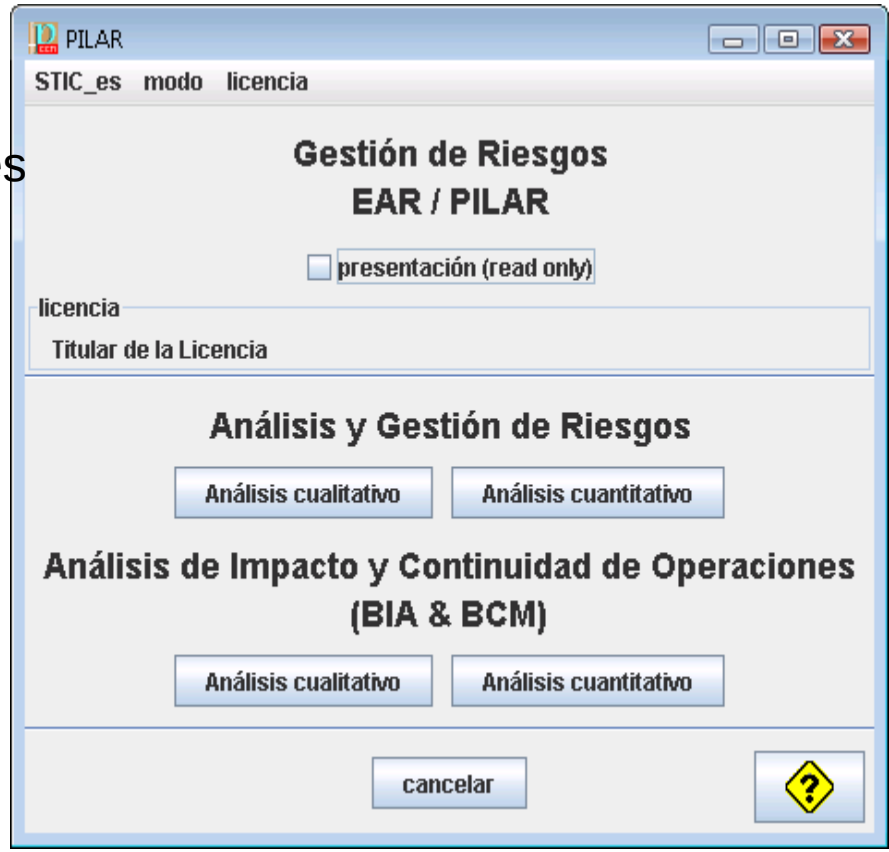
- salvaguardas (o contramedidas)
- elementos de respaldo (*back up*)
- planes de recuperación de desastres

analizándose el impacto residual a lo largo de diversas etapas de tratamiento.

La versión incorpora:

- Perfil de evaluación para el ENS.

.



RMAT (Risk Management Additional Tools)

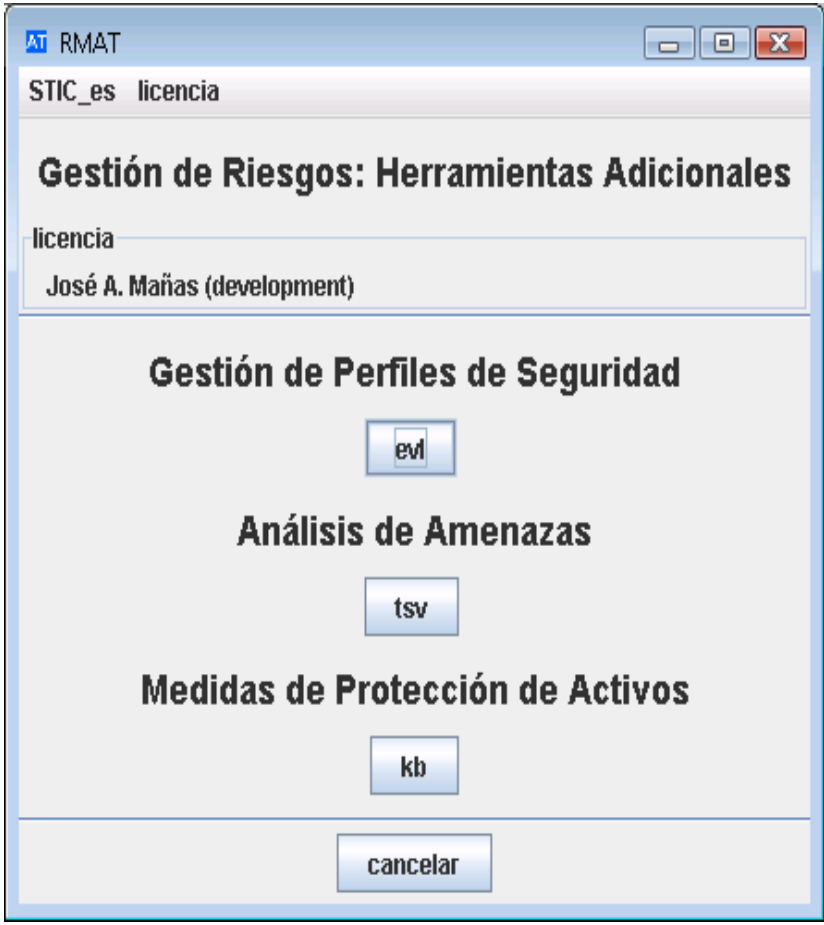
Las herramientas se pueden personalizar en varios aspectos:

EVL - Perfiles de protección.
Por ejemplo: LOPD, ENS, …

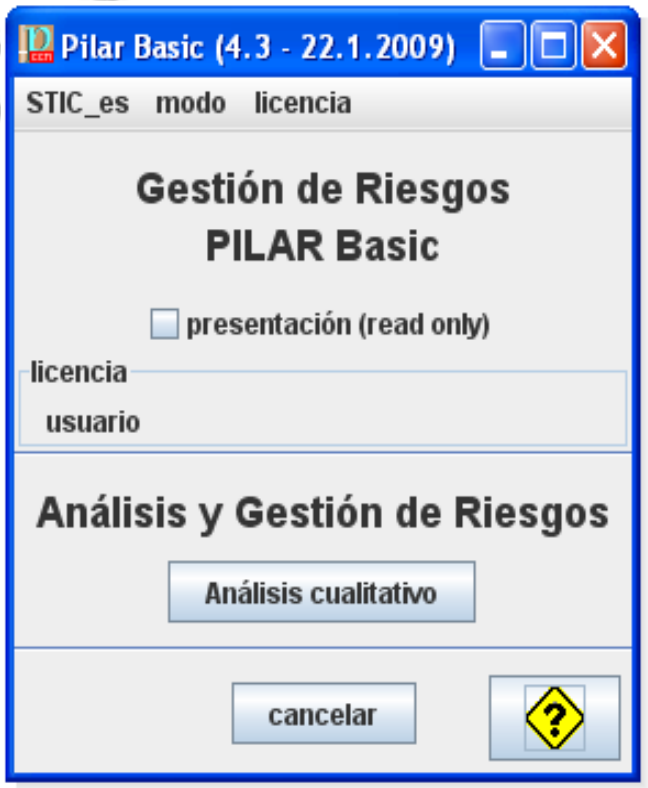
TSV - Perfiles de amenazas

KB - Protecciones adicionales Detallando protecciones adicionales sobre ciertos tipos de activos. (Wifi, FW, VoIP,…)

Estas herramientas permiten preparar y mantener personalizaciones, que se incorporan dinámicamente a la biblioteca, extendiéndola para adaptarse a un determinado contexto.
.



PILAR Basic



Análisis de riesgos para PYMES / Sistemas pequeños.

Exportable

Solo Análisis Cualitativo

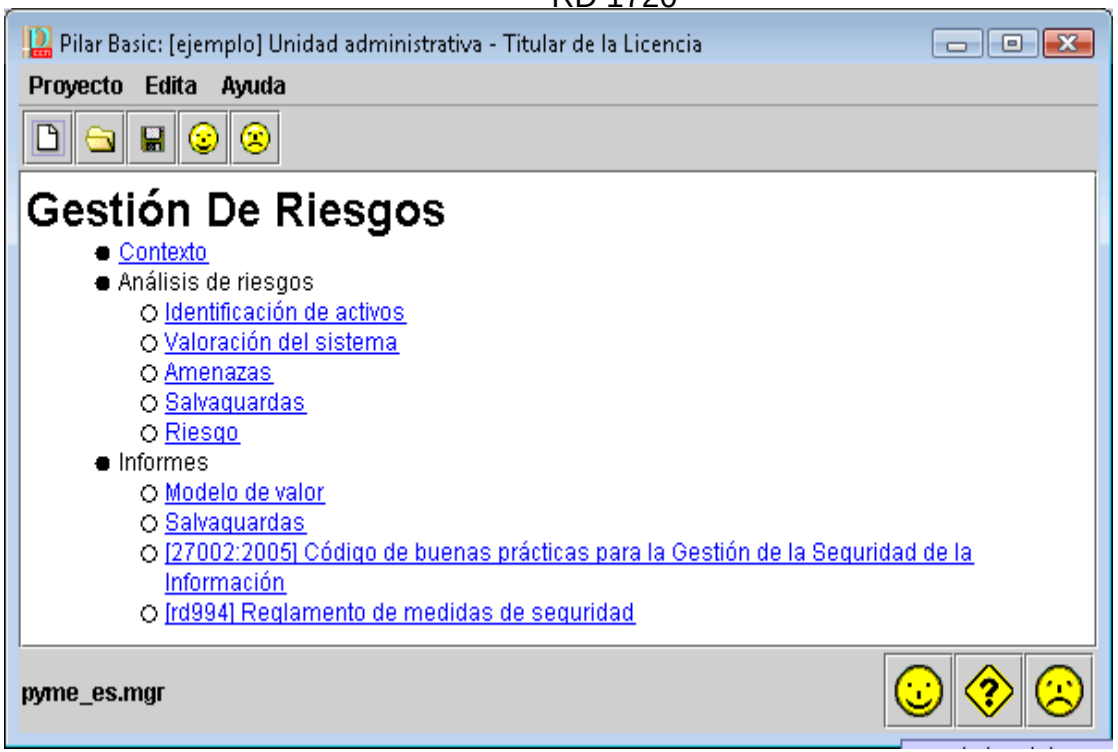
Valoración basada en dominios

Salvaguardas 2 fases

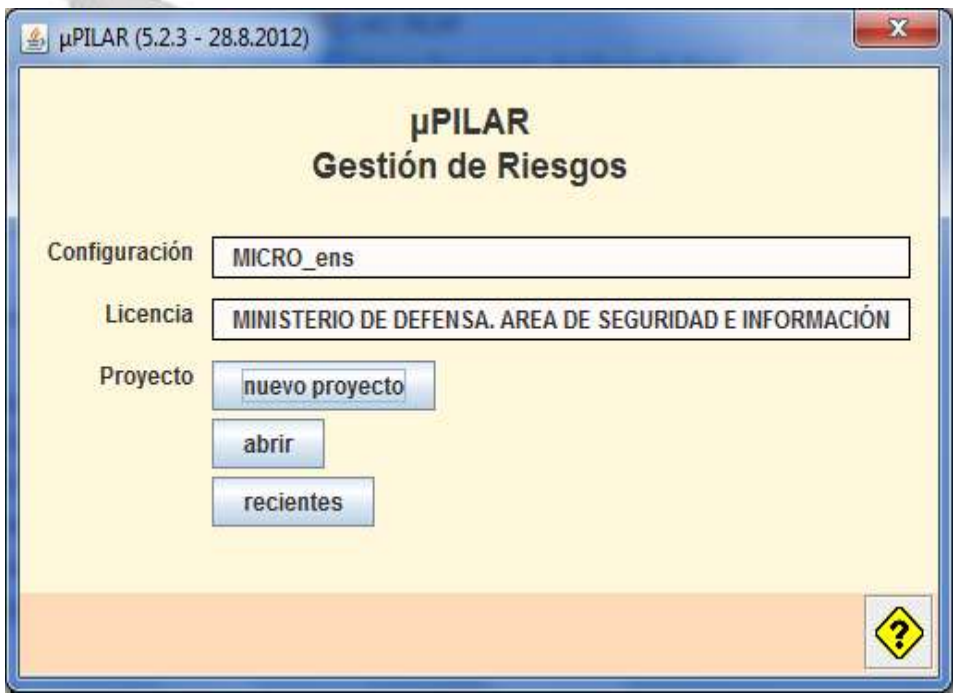
2 Criterios valoración

27002-2005

RD 1720



µPILAR



- PILAR reducida a la mínima expresión para realizar análisis de riesgos muy rápidos.

- **El resultado del análisis puede cargarse en PILAR para un estudio más detallado.**

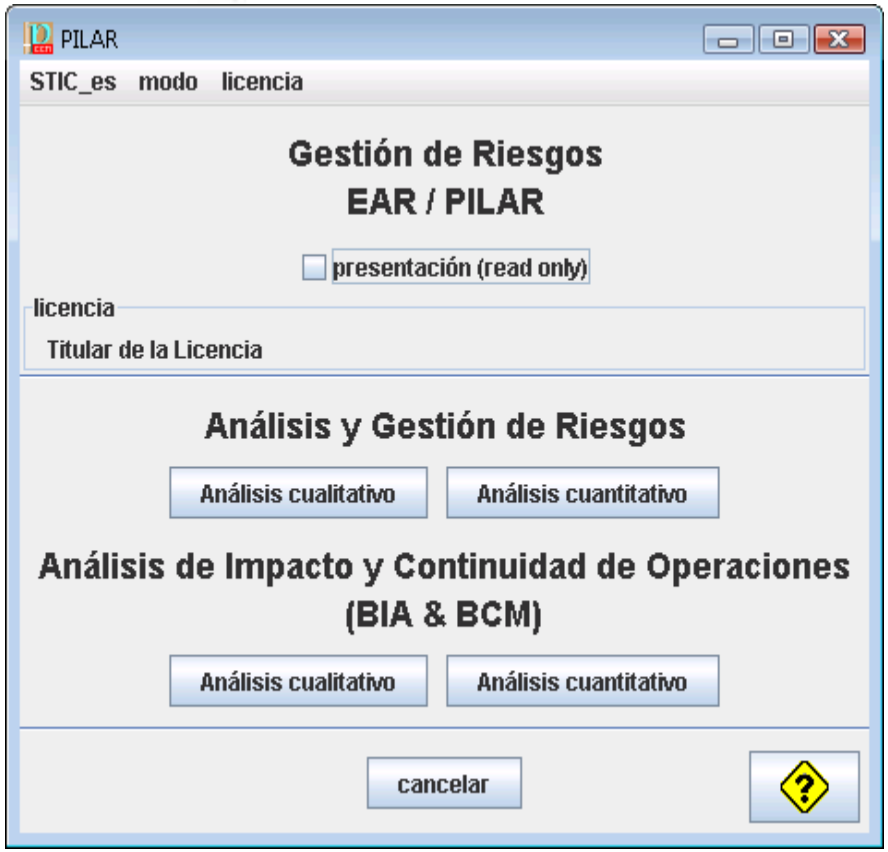
- **µPILAR se distribuye con perfiles específicos. Sólo se pueden analizar los perfiles de la distribución (27000, ENS, OTAN)**

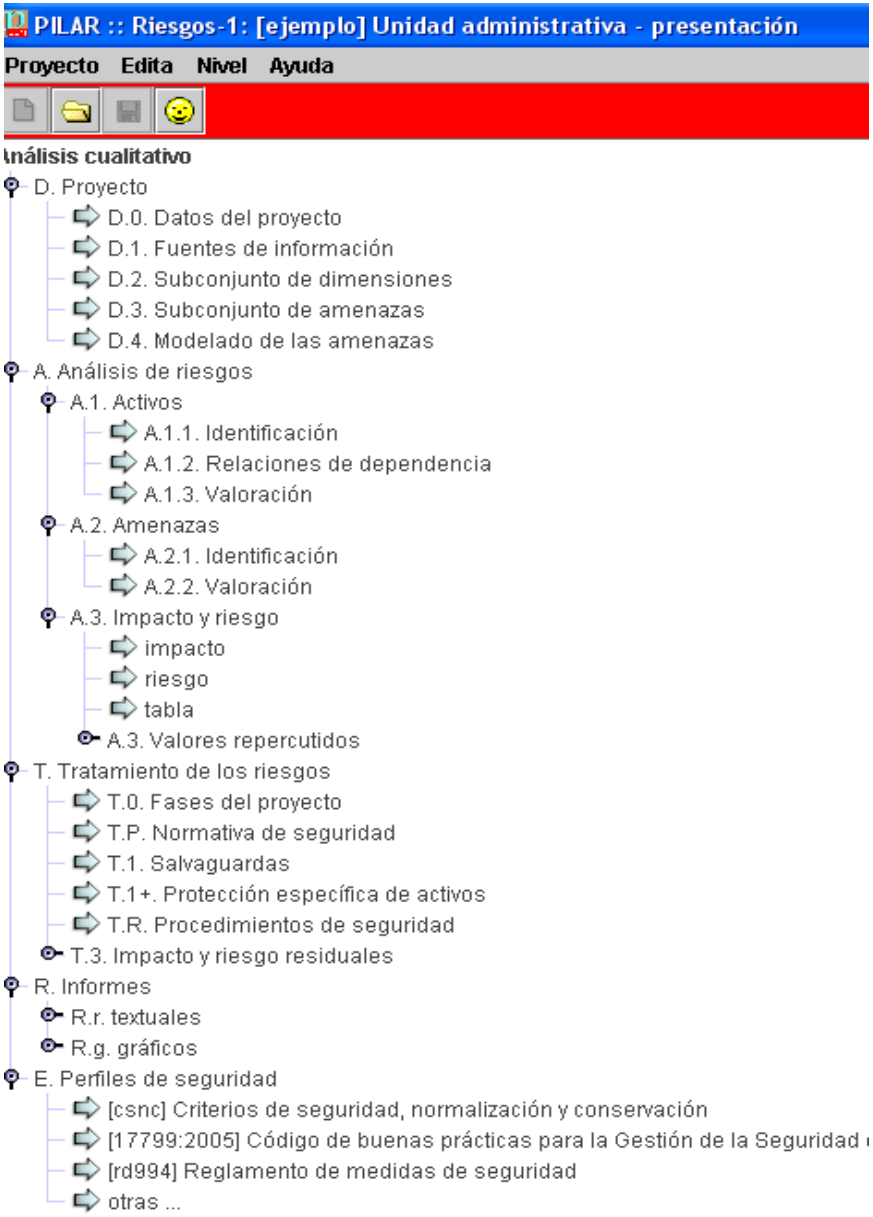
LICENCIAS

a) Si pertenece usted a una administración pública española
Esta aplicación es gratuita para administraciones públicas españolas. Para solicitar una licencia gratuita para el uso completo de la aplicación debe enviar un e-mail al ccn@cni.es

b) Si no pertenece usted a una administración pública española
Debe adquirir una licencia.

c) Licencia de evaluación
Permite generar una licencia de evaluación durante 30 días.


PILAR
STIC_es modo licencia
Gestión de Riesgos
EAR / PILAR
presentación (read only)
licencia
Titular de la Licencia
Análisis y Gestión de Riesgos
Análisis cualitativo
Análisis cuantitativo
Análisis de Impacto y Continuidad de Operaciones
(BIA & BCM)
Análisis cualitativo
Análisis cuantitativo
cancelar


PILAR :: Riesgos-1: [ejemplo] Unidad administrativa - presentación
Proyecto Edita Nivel Ayuda
Análisis cualitativo
D. Proyecto
D.0. Datos del proyecto
D.1. Fuentes de información
D.2. Subconjunto de dimensiones
D.3. Subconjunto de amenazas
D.4. Modelado de las amenazas
A. Análisis de riesgos
A.1. Activos
A.1.1. Identificación
A.1.2. Relaciones de dependencia
A.1.3. Valoración
A.2. Amenazas
A.2.1. Identificación
A.2.2. Valoración
A.3. Impacto y riesgo
impacto
riesgo
tabla
A.3. Valores repercutidos
T. Tratamiento de los riesgos
T.0. Fases del proyecto
T.P. Normativa de seguridad
T.1. Salvaguardas
T.1+. Protección específica de activos
T.R. Procedimientos de seguridad
T.3. Impacto y riesgo residuales
R. Informes
R.r. textuales
R.g. gráficos
E. Perfiles de seguridad
[csnc] Criterios de seguridad, normalización y conservación
[17799:2005] Código de buenas prácticas para la Gestión de la Seguridad
[rd994] Reglamento de medidas de seguridad
otras ...

ACTIVOS

Son los recursos del sistema de información o relacionados con éste necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

(V) Valor Coste que supone regresar a estado de seguridad (1-10)

Valor se asocia a dimensiones:

A **autenticidad**

¿Qué importancia tendría que quien accede al activo no sea realmente quien se cree?

C **confidencialidad**

¿Qué importancia tendría que el activo fuera conocido por personas no autorizadas?

D **disponibilidad**

¿Qué importancia tendría que el activo no estuviera disponible?

I **integridad**

¿Qué importancia tendría que el activo fuera modificado fuera de control?

T **trazabilidad**

¿Qué importancia tendría que no quedara constancia del uso del activo?

TIPOS

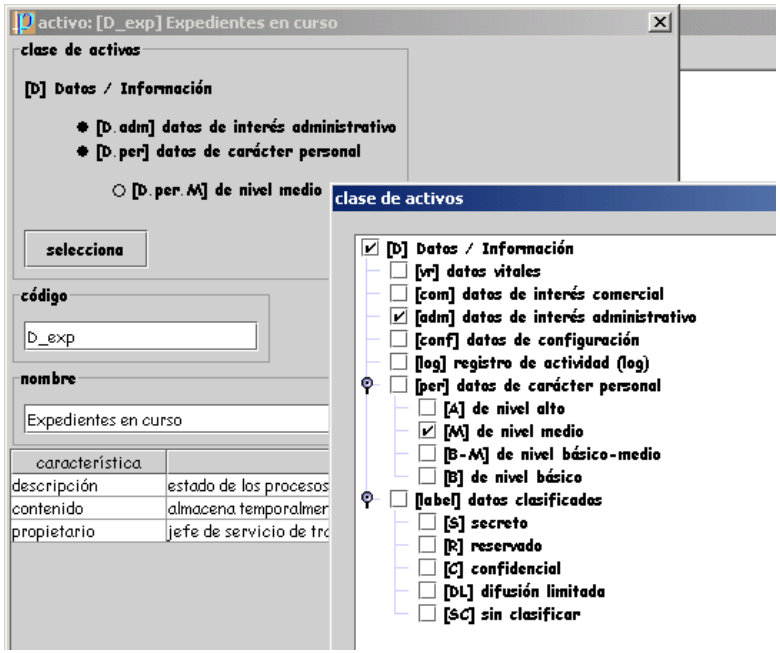
- Procesos
- Servicios
- Datos / Información

Datos / información
Servicios

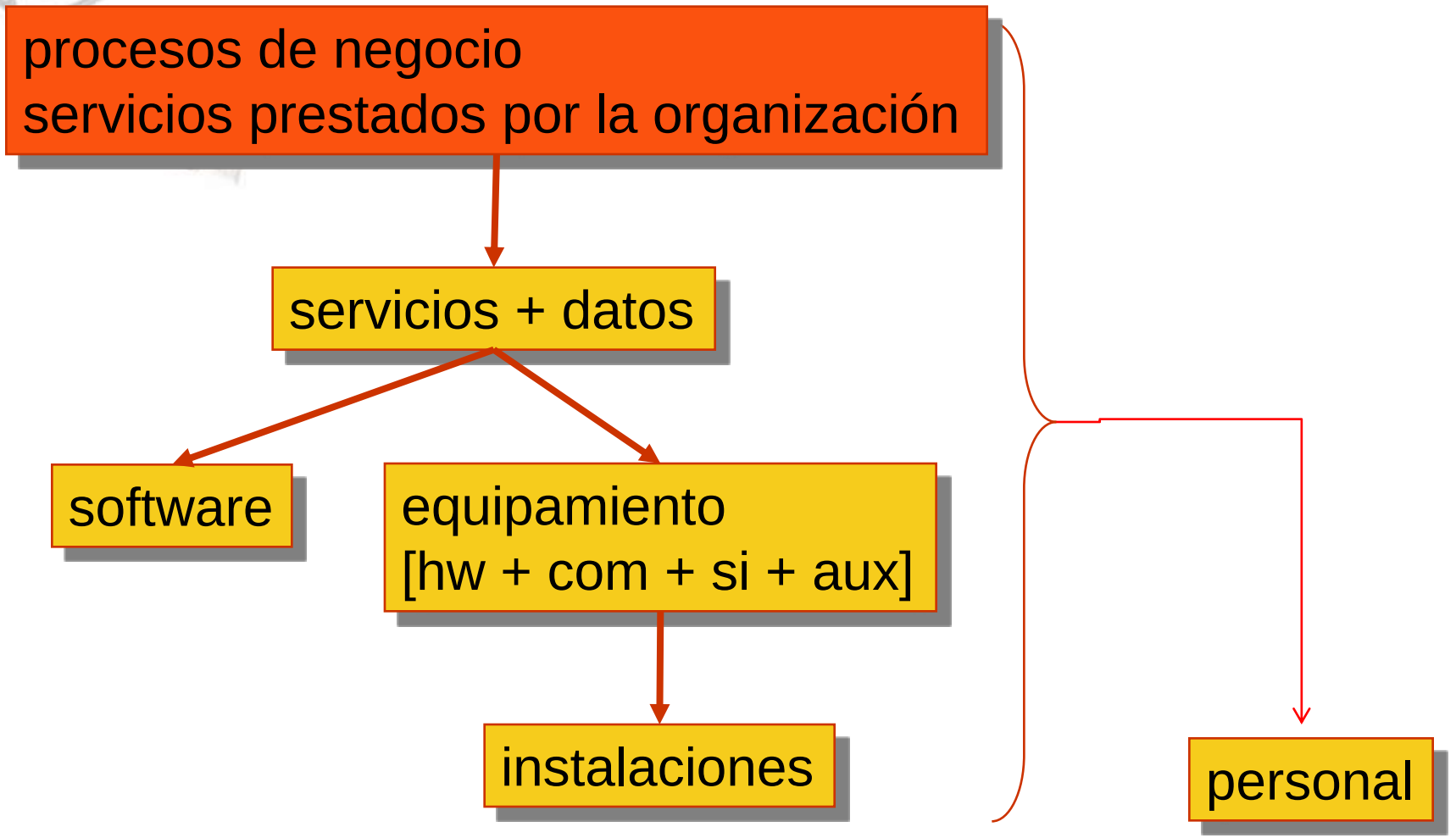
negocio

- Aplicaciones (software)
  - Sistemas Operativos
- Equipos informáticos (hardware)
- Redes de comunicaciones
- Soportes de información
- Equipamiento auxiliar
- Instalaciones (locales, etc.)
- Personal

ingeniería
aprovisionamiento



DEPENDENCIAS



DEPENDENCIAS

save | print | 100%

[SP] Servicios al público

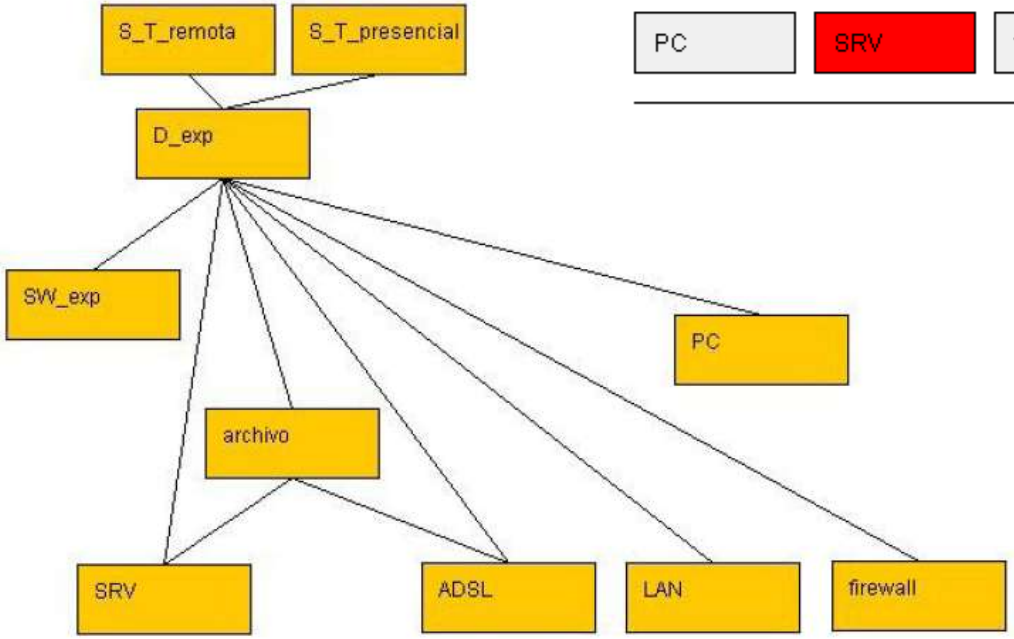
S_T_presencia | S_T_remota | D_exp | SW_exp

[SI] Servicios internos

email | archivo

[E] Equipamiento

PC | SRV | firewall | LAN | ADSL



VALORACIÓN DE ACTIVOS

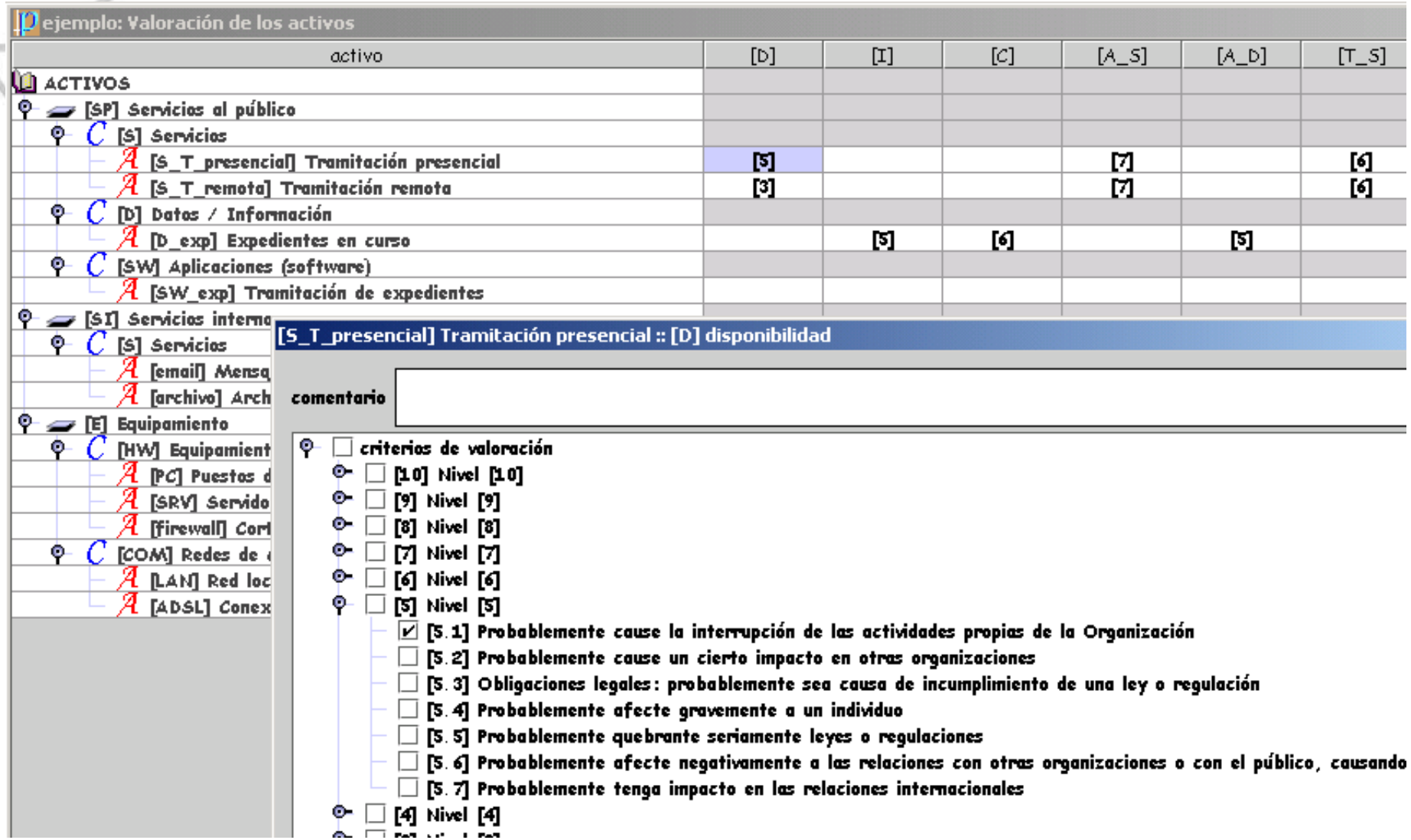
❑ VALORACIÓN DE LOS ACTIVOS

- Coste que supondría la ocurrencia de una amenaza
- **No importa lo que cuesta; importa para qué vale**

❑ QUE ACTIVOS SE VALORAN

- **Los datos (información)**
  - sin duda
- **Los servicios finales**
  - probablemente SÍ:
  - es lo que entiende la Dirección
- Los demás activos
  - probablemente NO:
  - sólo tienen valor en función de datos que manejan y los servicios que habilitan

VALORACIÓN DE ACTIVOS



AMENAZAS

Eventos que pueden desencadenar un incidente en la organización produciendo daños materiales o perdidas inmateriales en sus activos.

- No se conoce la forma ideal,
  todos los métodos son “limitados” teórica y prácticamente
- Modelos de clasificación “de éxito”
  - **por grupos de activos**
  - **por impacto**
  - **en base al agente causante (escenarios de ataque)**
  - **por la propia naturaleza de la amenaza**

	accidentales	deliberadas
Autenticidad		
Confidencialidad		
Integridad		
Disponibilidad		
otras ...		

	accidente natural o industrial	origen humano directo	origen humano indirecto
personas			
hardware			
software			

AMENAZAS

Efecto de amenaza se caracteriza:

(D) **Degradación**. Porcentaje en el que el activo se ve perjudicado.

(F) **Frecuencia de ocurrencia**. (ARO)

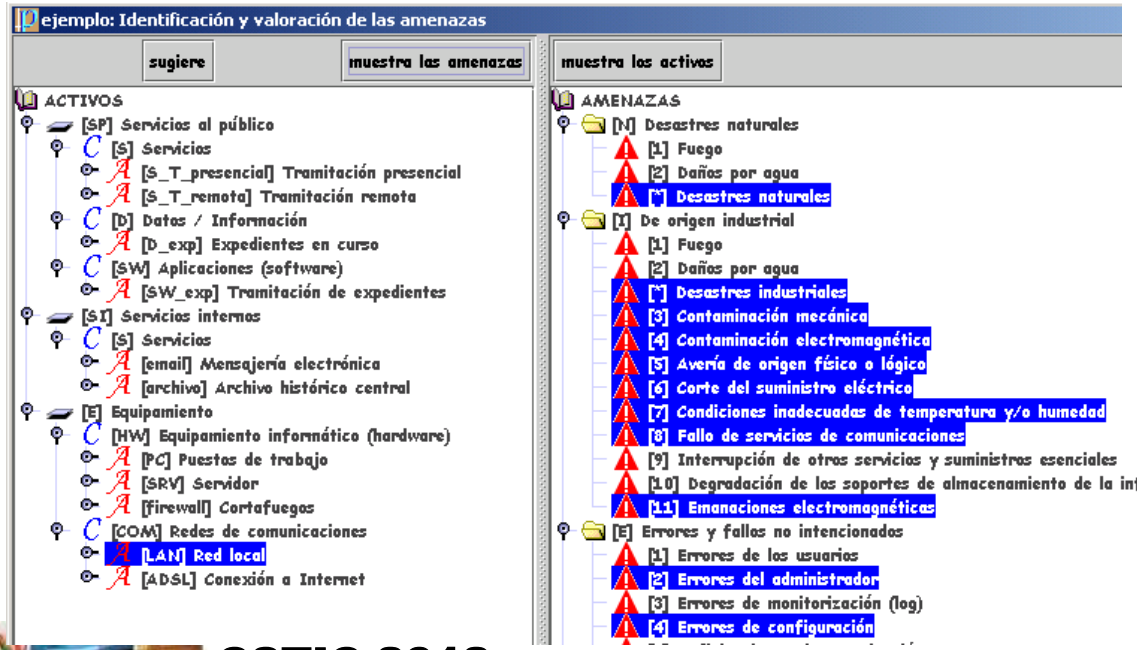
- accidentales
  - naturales
    - terremotos, inundaciones,...
  - industriales
    - electricidad, emanaciones, ...
  - humanas: errores y omisiones
- deliberadas (intencionales)
  - intercepción pasiva o activa
  - intrusión, espionaje, ...
  - robo, fraude, ...

modelo			
potencial	probabilidad	frecuencia	
XL	muy probable	100	todos los días
L	probable	10	todos los meses
M	poco probable	1	todos los años
S	improbable	0,1	cada 10 años

AMENAZAS

CLASES DE AMENAZAS Según biblioteca

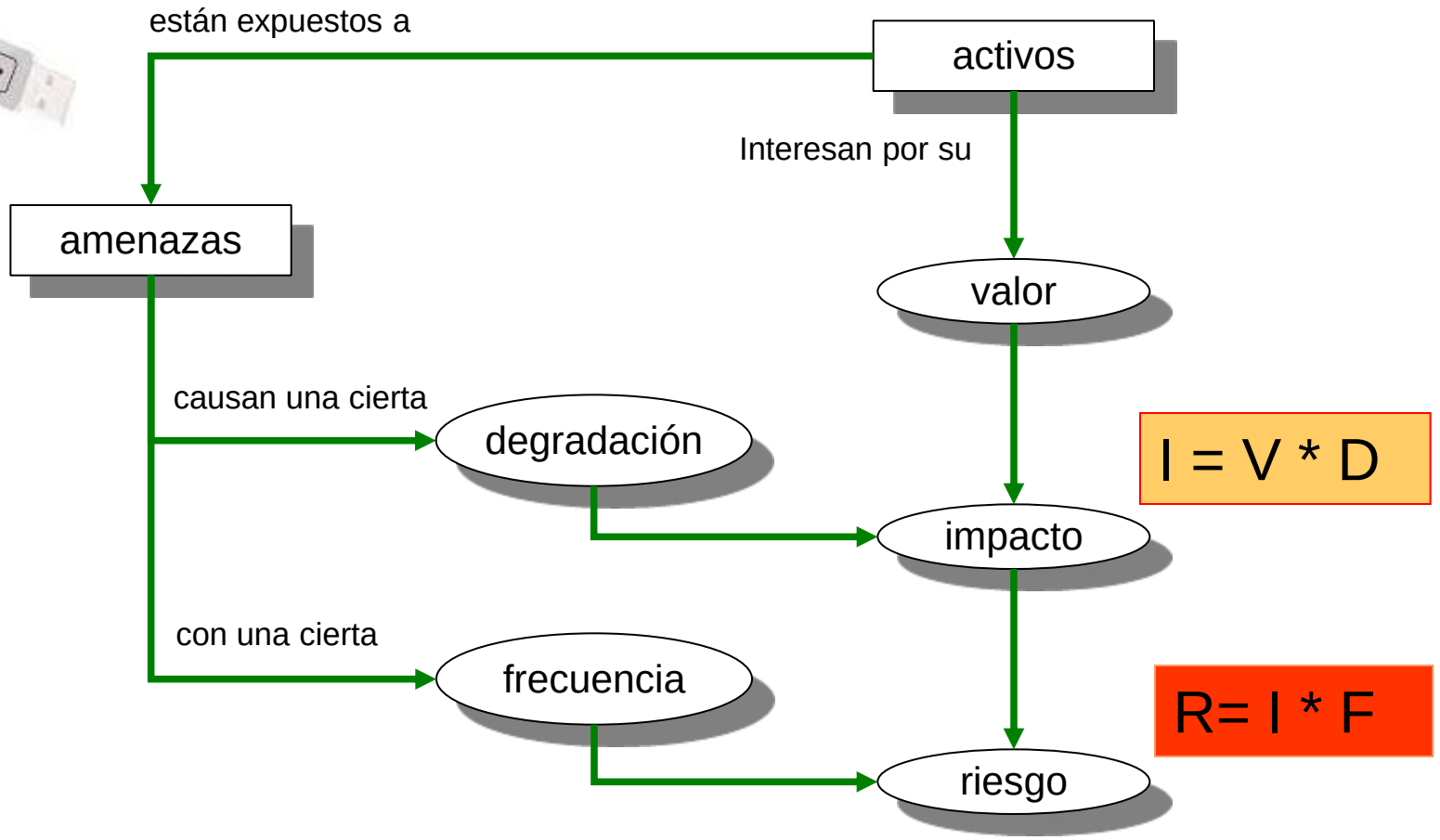
- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no ntencionados
- [A] Ataques deliberados



- [A] Ataques deliberados
  - [4] Manipulación de la configuración
  - [5] Suplantación de la identidad del usuario
  - [6] Abuso de privilegios de acceso
  - [7] Uso no previsto
  - [8] Difusión de software dañino
  - [9] [Re-]encaminamiento de mensajes
  - [10] Alteración de secuencia
  - [11] Acceso no autorizado
  - [12] Análisis de tráfico
  - [13] Repudio
  - [14] Intercepción de información (escucha)
  - [15] Modificación de información
  - [16] Introducción de falsa información
  - [17] Corrupción de la información
  - [18] Destrucción de la información
  - [19] Divulgación de información
  - [22] Manipulación de programas
  - [24] Denegación de servicio
  - [25] Robo de equipos
  - [26] Ataque destructivo
  - [27] Ocupación enemiga
  - [28] Indisponibilidad del personal
  - [29] Extorsión
  - [30] Ingeniería social

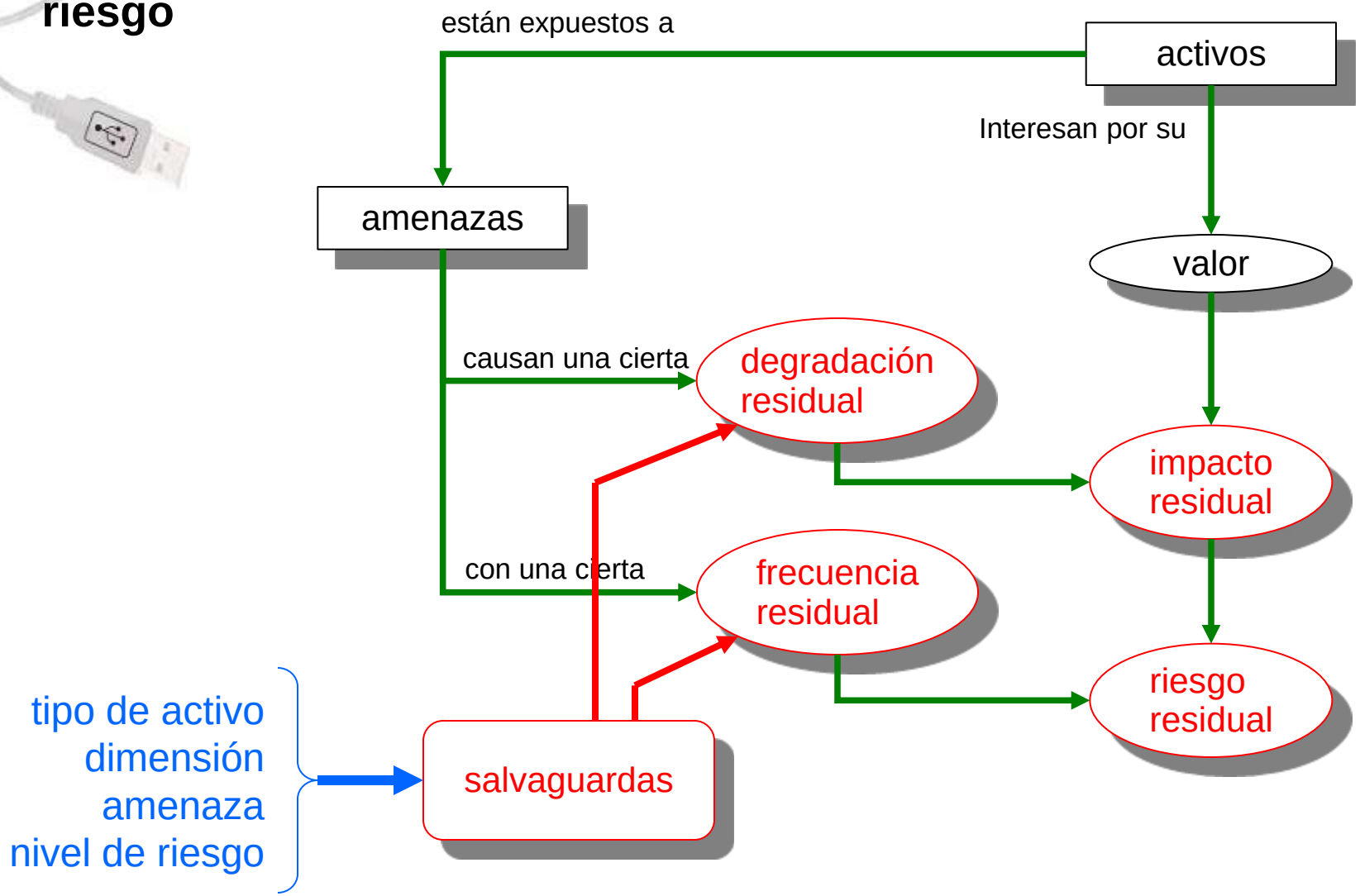
IMPACTO/RIESGO

Magerit : Análisis de Riesgo



SALVAGUARDAS

MAGERIT: Procedimiento o mecanismo tecnológico que reduce el riesgo



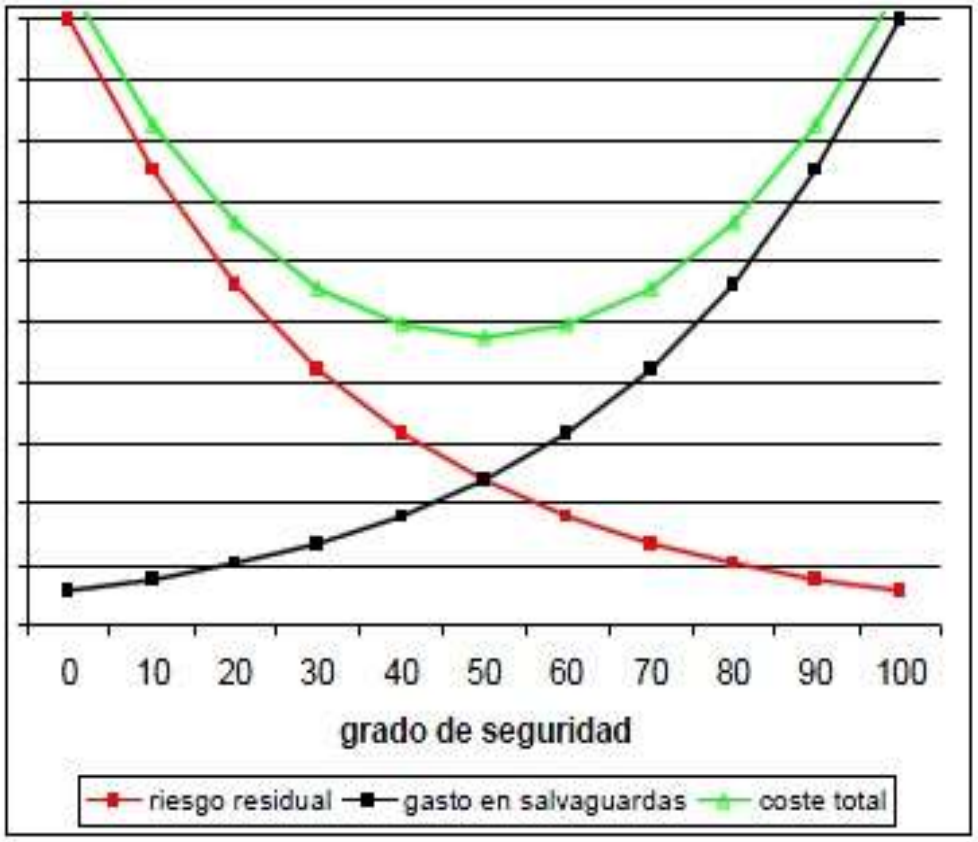
SALVAGUARDAS

- **Reducen la frecuencia de las Amenazas**
- **Limitan el daño causado**

Salvaguarda ideal:

- Teóricamente idónea
- Desplegada, Configurada y Mantenida
- Se emplea siempre
- Procedimientos claros uso normal e Incidencias
- Usuarios formados y concienciados
- Controles que avisan de fallos

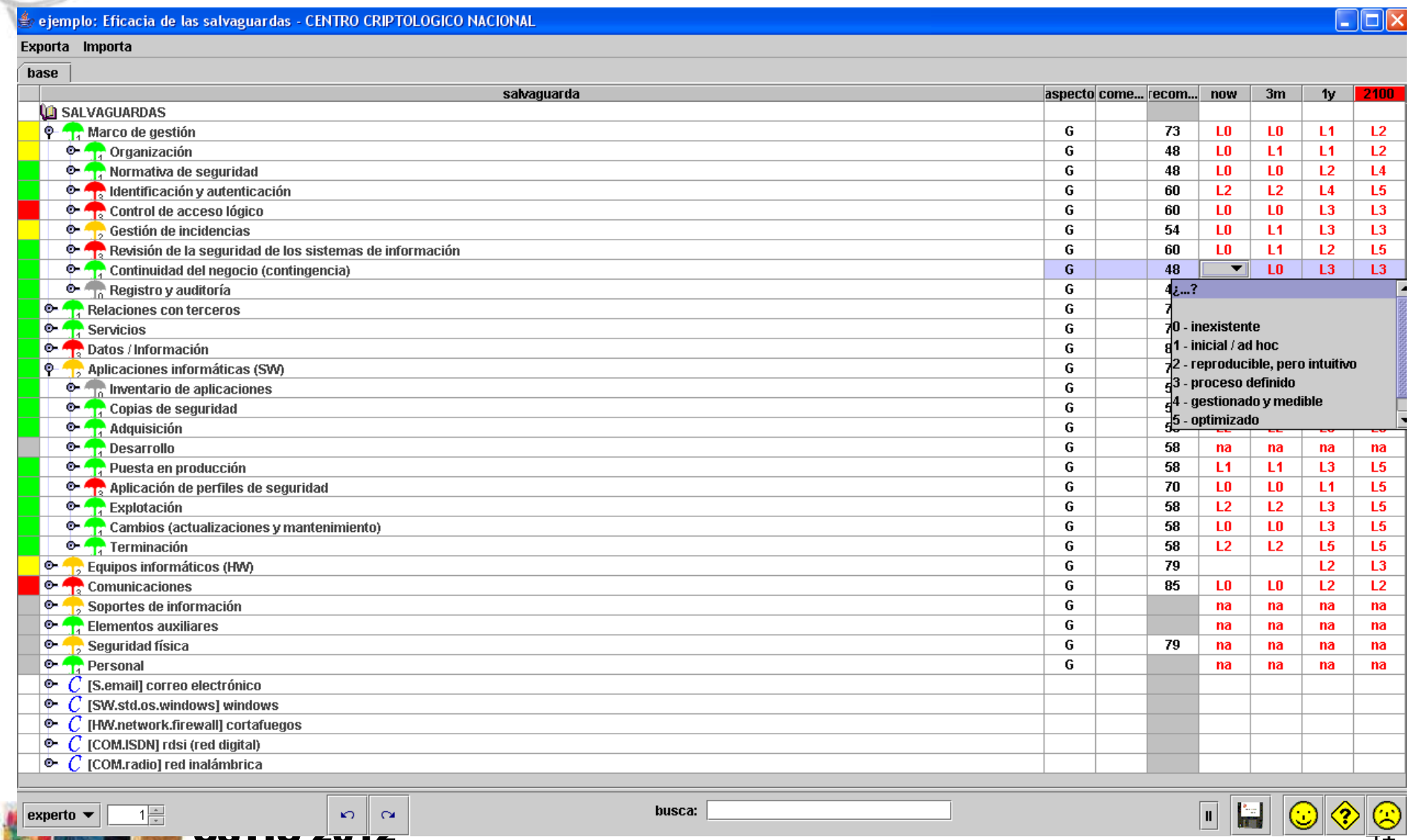
SALVAGUARDAS



No se puede invertir en salvaguardas más allá del valor de los propios activos a proteger.

SALVAGUARDAS

Salvaguardas



GESTIÓN DE RIESGOS

A.3.1 TOMA DE DECISIONES

- Carácter Urgente
  - Desarrollar plan de contingencia
  - Monitorizar y gestionar las cuentas de usuarios externos)
- Consideraciones importantes
  - Documentar procedimientos de trabajo
  - Segregar funciones de administrador
- Otros....

A.3.2 PLAN DE SEGURIDAD

- Detalle de los proyectos anteriores

A.3.3 EJECUCIÓN DEL PLAN

INFORMES

TEXTUALES

- Modelo de valor
  - Detalla activos, sus dependencias, dimensiones en las que son valiosos y su valor
- Mapa de Riesgos
  - Detalla amenazas significativas por cada activo. Frecuencia y degradación
- Evaluación de Salvaguardas
  - Detalla salvaguardas existentes. Se califican en su eficacia para reducir el riesgo.
- Estado de Riesgo
  - Para cada activo impacto/riesgo residual
- Informe de insuficiencias
  - Detalla salvaguardas necesarias pero ausentes o insuficientemente eficaces

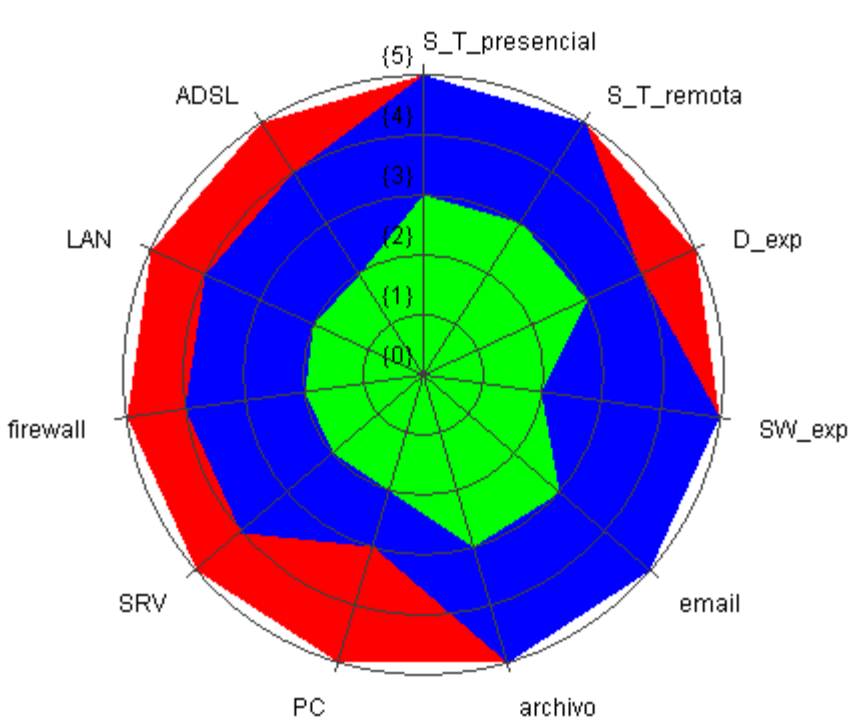
TABLAS

- Asistente para generar ficheros .csv (elaborar gráficos o completar informes)

GRAFICOS

- Impacto acumulado / Riesgo acumulado

INFORMES GRAFICOS. Riesgo Residual



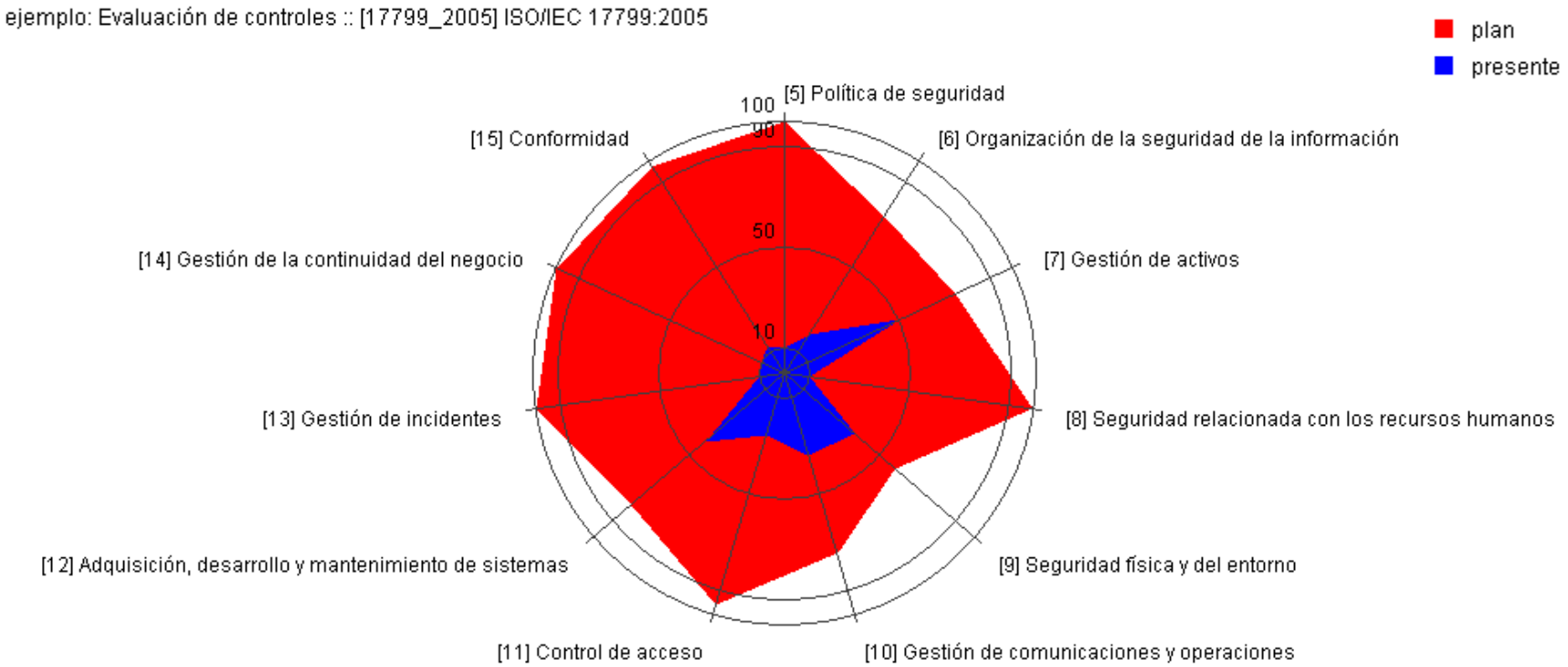
Reducción del Riesgo

Sin salvaguardas

Fase presente

Plan de Seguridad

EVALUACIONES DE SEGURIDAD … ISO 17799:2005



GRACIAS POR SU ATENCIÓN

seginfo SEGURIDAD DE LA INFORMACIÓN

TCOL JOSÉ LUIS QUINTERO VILLARROYA
Área de Seguridad de la Información
SDG de Tecnologías de la Información y Comunicaciones
Ministerio de Defensa

C/ Arturo Soria, 289. 28033 - MADRID
Tfno.: 91 395 4871 / 816 4871
Móvil : 629 807 131 / 844 6338

Correo electrónico: jquintev@et.mde.es

CSTIC 2012

Dominando los riesgos se compite mejor

18 de Septiembre de 2012 #CSTIC12

Patrocinadores

Caelum

SEI Partner | Carnegie Mellon

GOBIERNO DE ESPAÑA

MINISTERIO DE DEFENSA

Organizador

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

AEC

COMITÉ DE LOS SISTEMAS Y LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Patronos de la AEC:

Aena

aena aeropuertos

AENOR

fundación enresa

renfe

Colaboradores

grupo SMS

DiCe

UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

Cooperadores

ati

CONCITI.org