PRESENTACIÓN INFOSECURITY 2015

BDO: ASEGURAMIENTO DE PROCESOS INFORMÁTICOS (API)

Ing. Pablo A. SILBERFICH

Nuestro equipo está integrado por profesionales especializados en TI al servicio del negocio, con certificaciones CISA, CISM, CISSP, CEH, entre otros.

PRODUCTO / SERVICIO: AUDITORÍA Y CONSULTORÍA INFORMÁTICA

NUESTROS SERVICIOS

Auditoría

(Interna, Externa y Certificaciones – Homologaciones, Computación Forense)

Consultoría

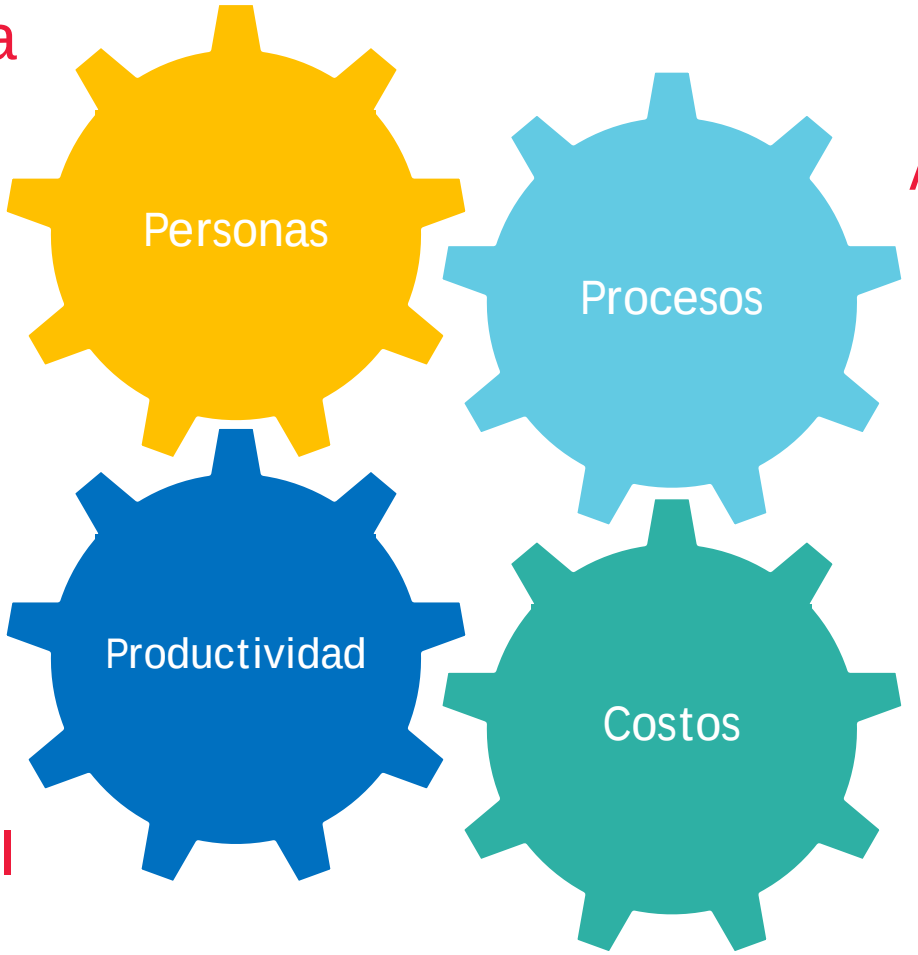
(Tecnología Informática, Sistemas, Aplicaciones, Comunicaciones y Seguridad de la Información)

Tercerización

(Servicios de «collocation» de RRHH y/o soporte)

BENEFICIOS CONCRETOS PARA NUESTROS CLIENTES

Seguridad de la Información



Administración de TI

Calidad de Servicio de TI

Enfoque de Negocio

AUDITORÍA DE SISTEMAS

Auditorías de sistemas y aplicativos bajo marcos de referencia y estándares internacionales (COBIT, GTAGs) y nacionales (BCRA 4609, 5374) y otros.

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

BDO

EJEMPLOS DE NUESTROS SERVICIOS - AUDITORIA

Servicio Auditoría Interna de Sistemas

Prevenir….
Evitar Multas / Sanciones / Fraudes

Servicio API

¿CÓMO PODEMOS AYUDARLO? (cont.)

CONSULTORÍA EN SISTEMAS Y CONTROL DE PROYECTOS

Asesoramiento y consultoría en áreas de TI.
Planificación estratégica de TI.
Análisis y gestión de riesgos de TI basado en Magerit 2.
Consultoría en estándares nacionales e internacionales como ITIL, ISO 20.000, COBIT, BCRA 4609, BCRA 5374.
Análisis de factibilidad de proyectos de sistemas.
Consultoría en controles de aplicaciones y procesos de áreas de TI.
Gerenciamiento y control de proyectos informáticos.
Desarrollo de RFP's y selección de sistemas.
Proyectos de Business Intelligence, Data Warehouse, Datamart y Data Mining.
Seguridad en E-Commerce.

Comunicación "A" 4609 del BCRA para entidades Financieras

- Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.

ISO/IEC 27001, 27005

- Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI)

Basilea II

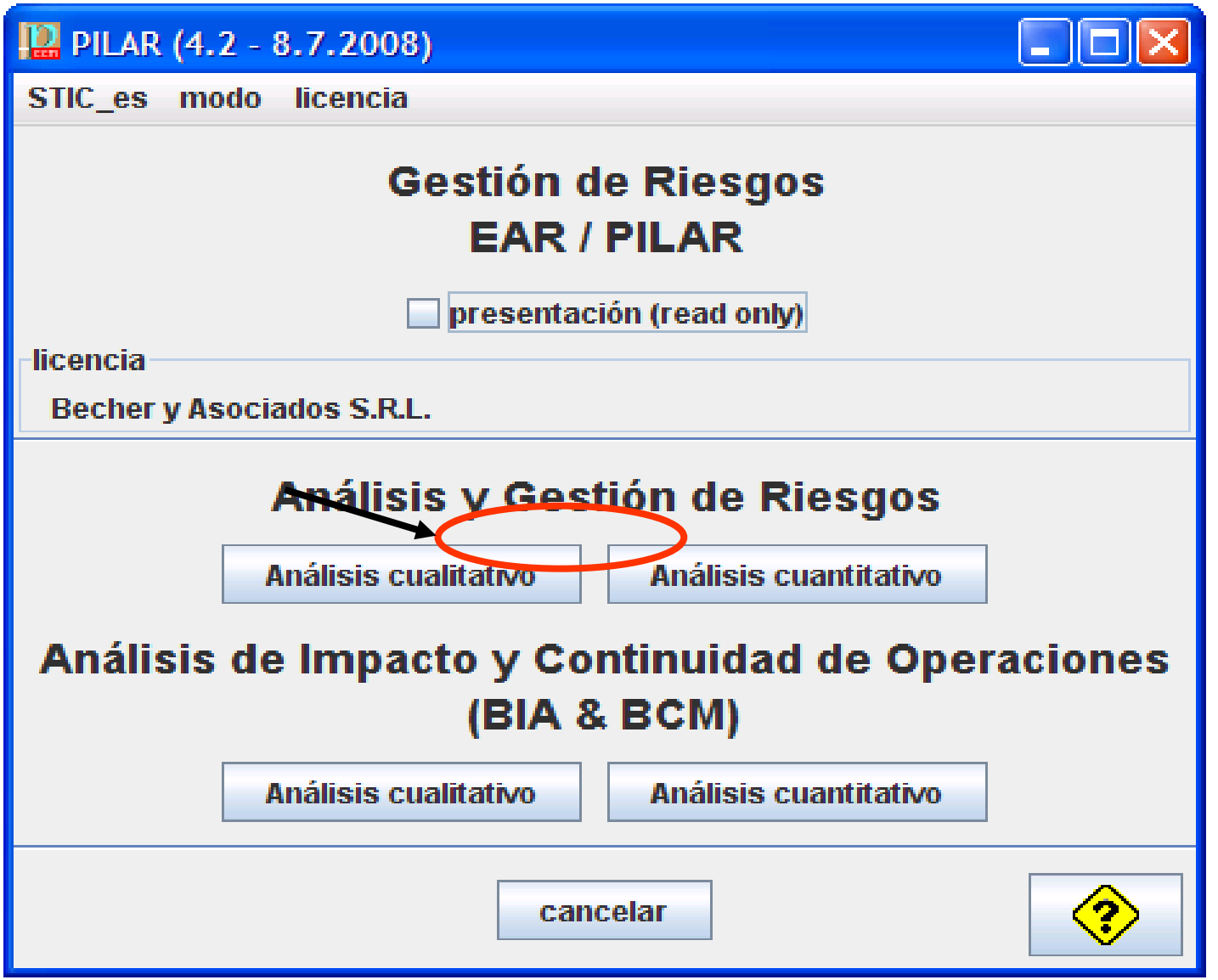
- Estandar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

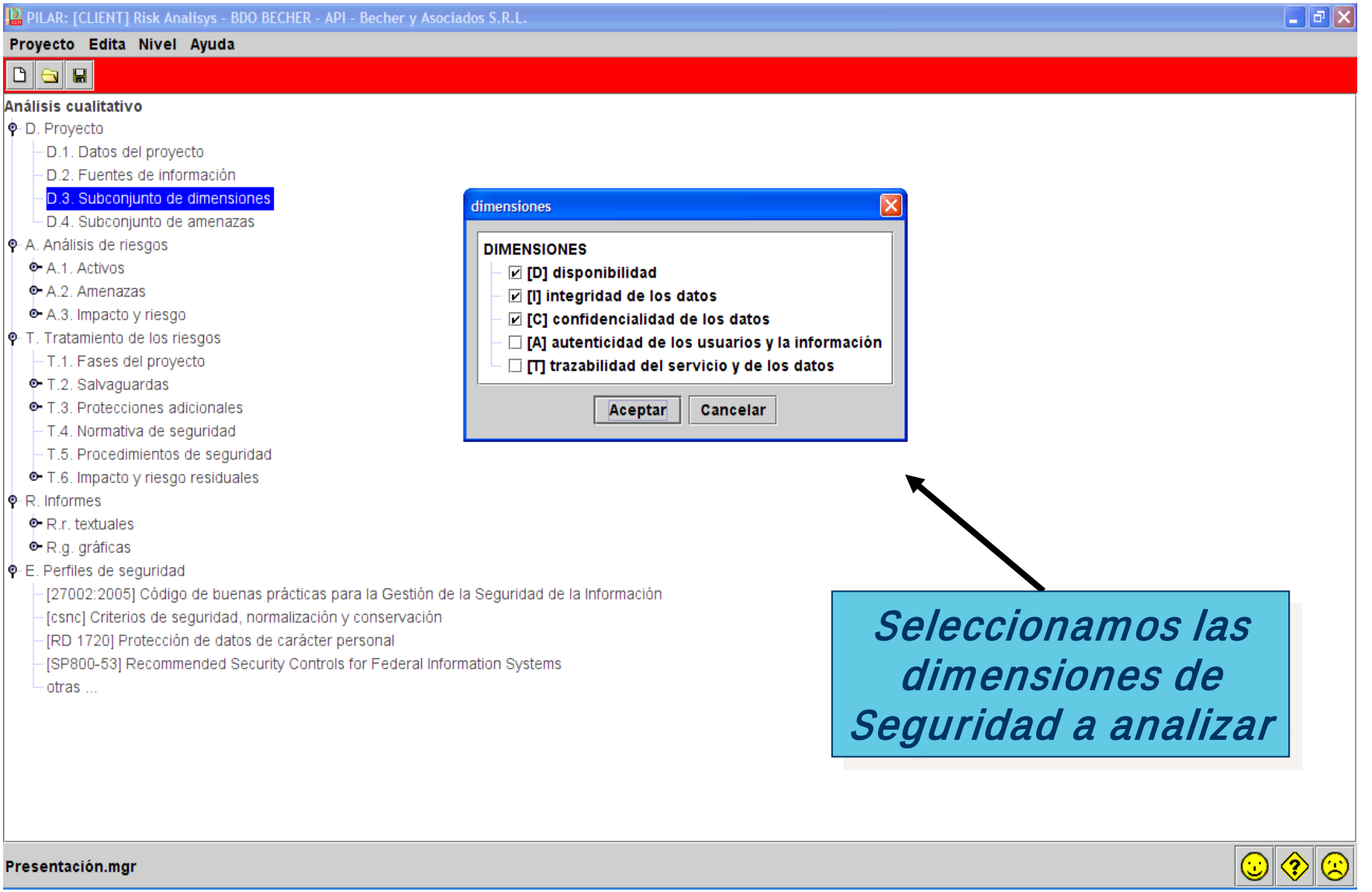
Ley Sarbanes Oxley (SOX)

- Impulsada por el gobierno norteamericano como respuesta a los mega fraudes corporativos que impulsaron Enron, Tyco International, WorldCom y Peregrine Systems. Es un conjunto de medidas tendientes a asegurar la efectividad de los controles internos sobre reportes financieros.

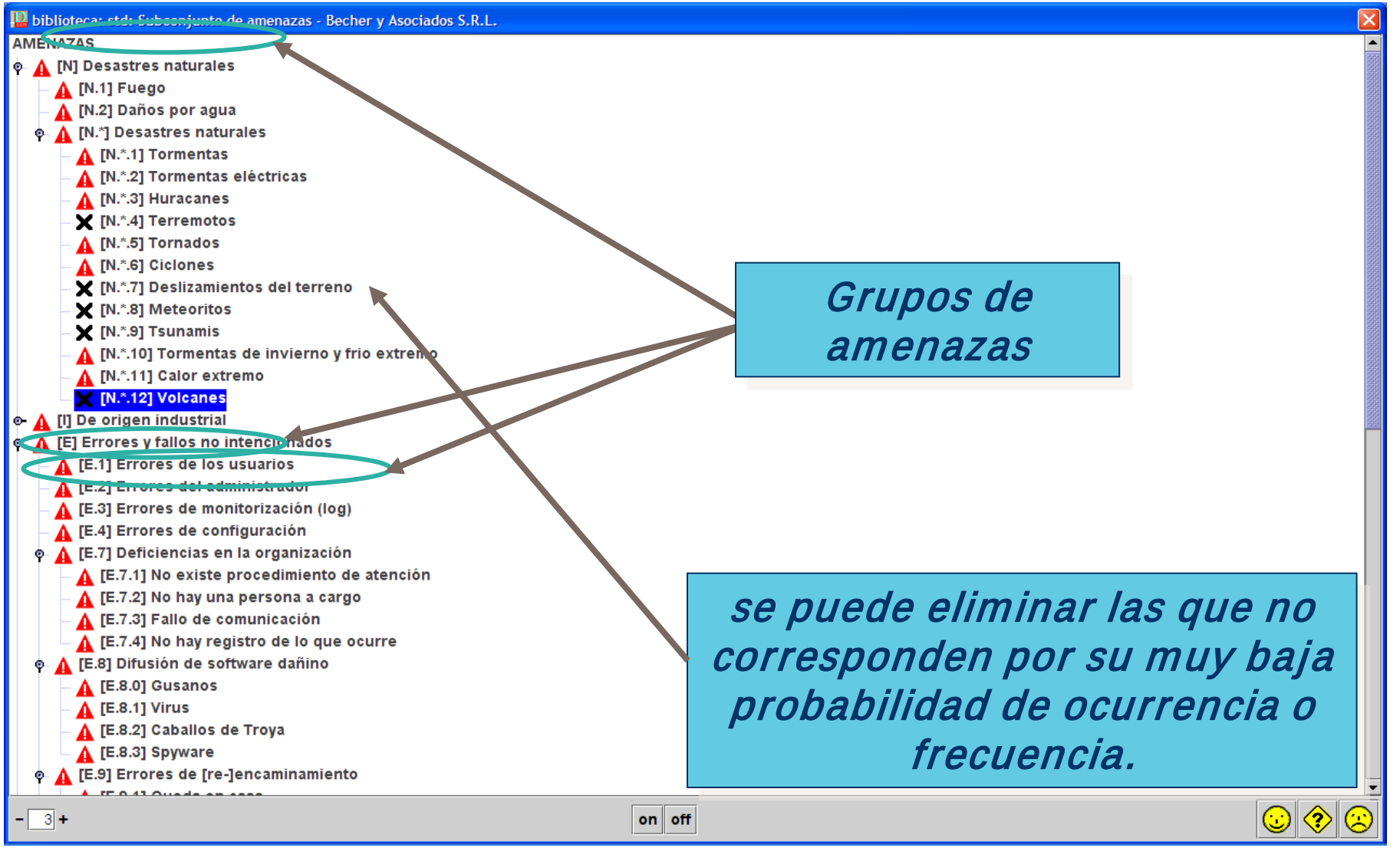
ISO/IEC 27005

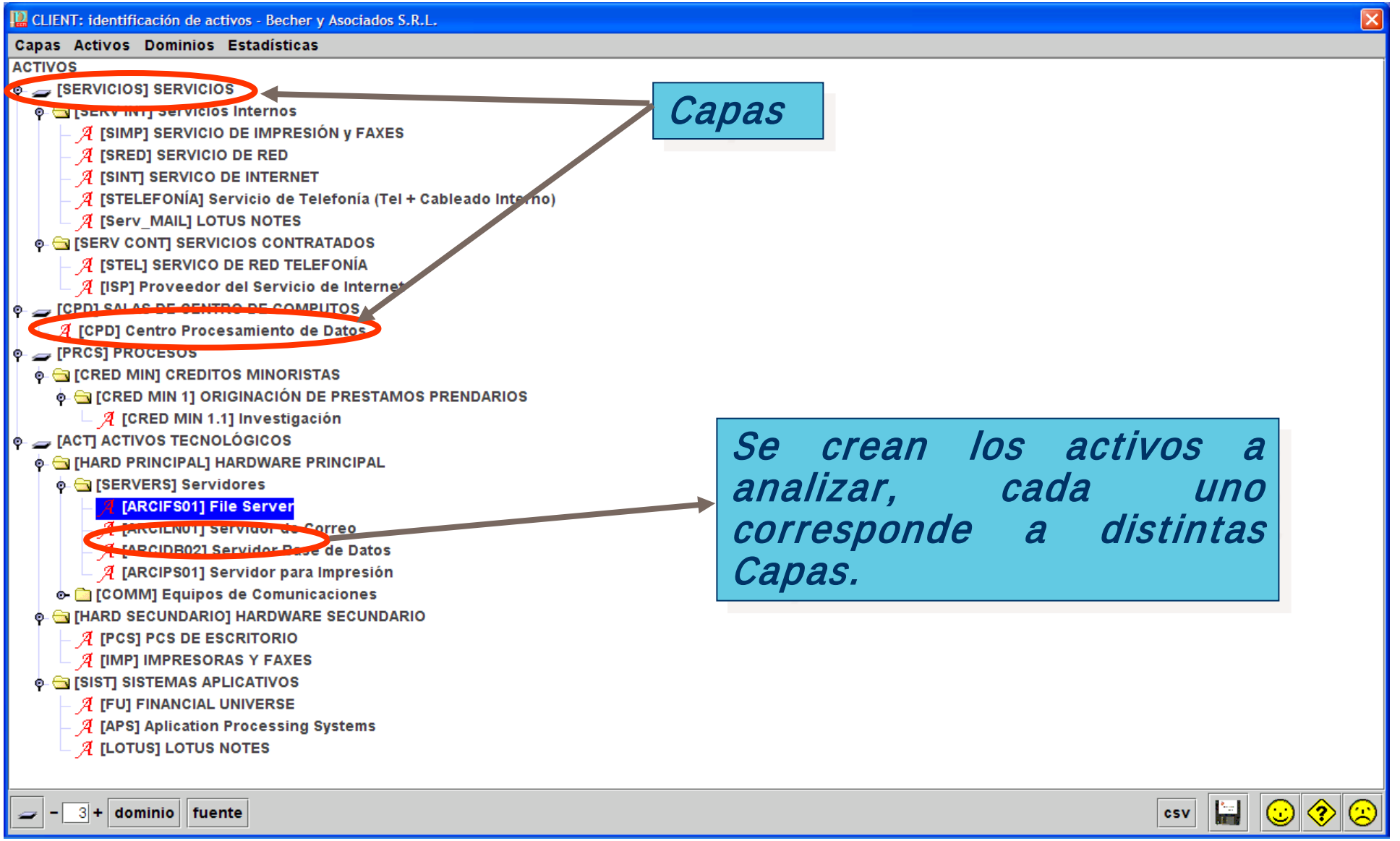
1. Establecer el contexto.
2. Evaluación del riesgo.
    a. Identificación del riesgo
    b. Estimación del riesgo
    c. Valoración del riesgo
3. Tratamiento del riesgo.
4. Aceptación del riesgo.
5. Comunicación del riesgo.
6. Seguimiento del riesgo.


PILAR (4.2 - 8.7.2008)
STIC_es modo licencia
Gestión de Riesgos
EAR / PILAR
presentación (read only)
licencia
Becher y Asociados S.R.L.
Análisis y Gestión de Riesgos
Análisis cualitativo
Análisis cuantitativo
Análisis de Impacto y Continuidad de Operaciones
(BIA & BCM)
Análisis cualitativo
Análisis cuantitativo
cancelar

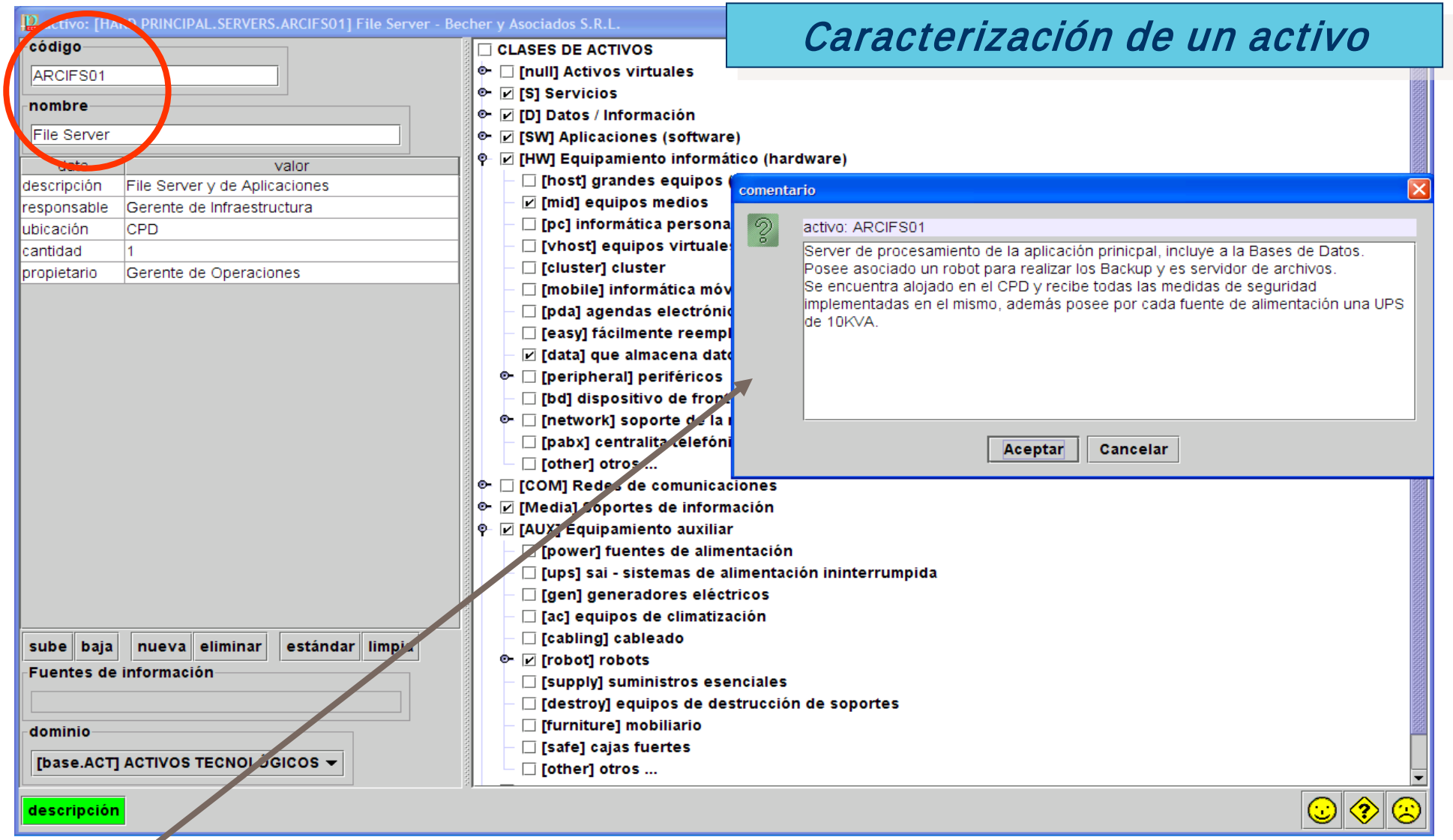


Seleccionamos las dimensiones de Seguridad a analizar

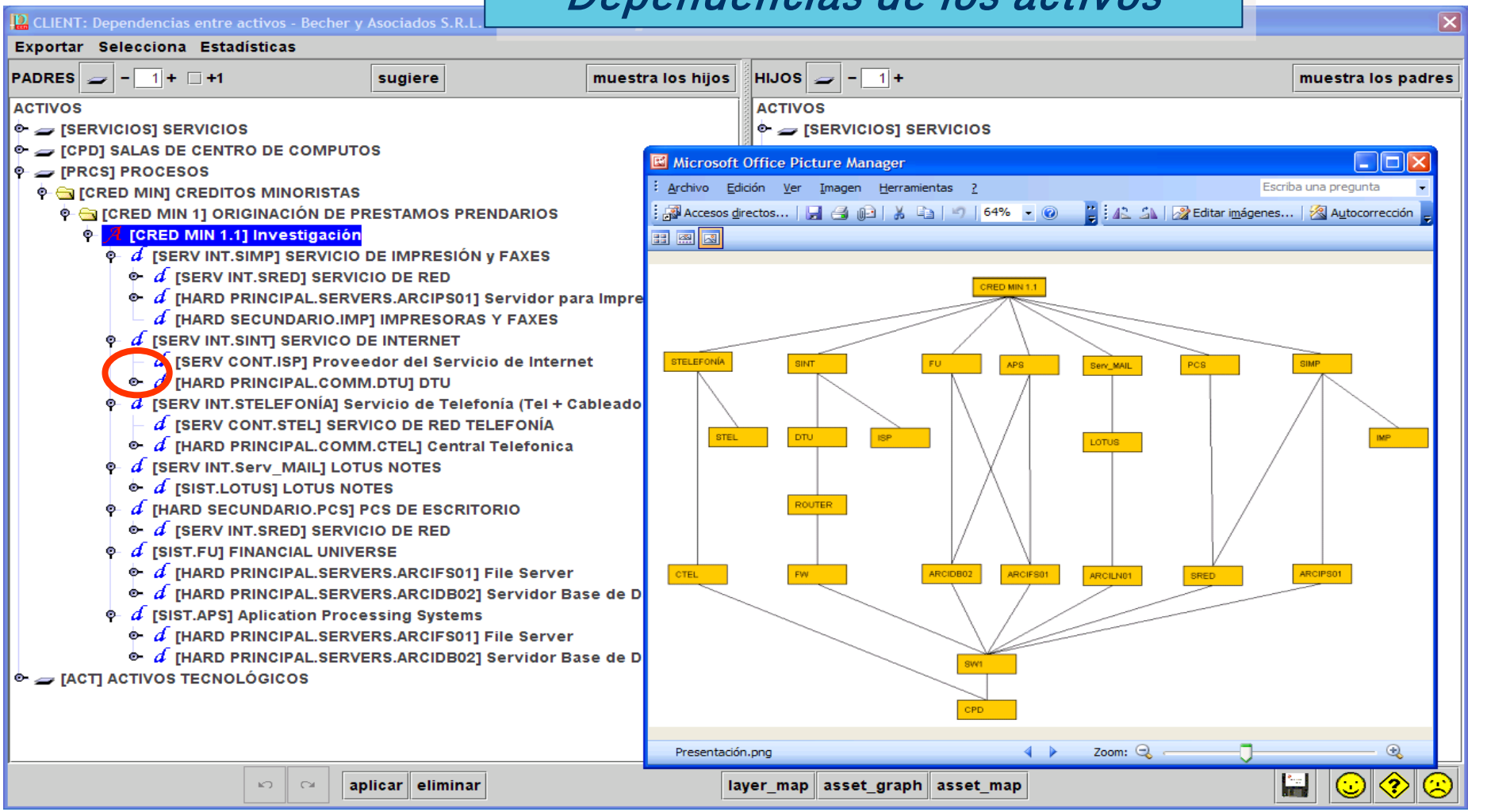

biblioteca: std: Subconjunto de amenazas - Becher y Asociados S.R.L.
AMENAZAS
[N] Desastres naturales
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[N.*.1] Tormentas
[N.*.2] Tormentas eléctricas
[N.*.3] Huracanes
[N.*.4] Terremotos
[N.*.5] Tornados
[N.*.6] Ciclones
[N.*.7] Deslizamientos del terreno
[N.*.8] Meteoritos
[N.*.9] Tsunamis
[N.*.10] Tormentas de invierno y frio extremo
[N.*.11] Calor extremo
[N.*.12] Volcanes
[I] De origen industrial
[E] Errores y fallos no intencionados
[E.1] Errores de los usuarios
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.7.1] No existe procedimiento de atención
[E.7.2] No hay una persona a cargo
[E.7.3] Fallo de comunicación
[E.7.4] No hay registro de lo que ocurre
[E.8] Difusión de software dañino
[E.8.0] Gusanos
[E.8.1] Virus
[E.8.2] Caballos de Troya
[E.8.3] Spyware
[E.9] Errores de [re-]encaminamiento
Grupos de amenazas
se puede eliminar las que no corresponden por su muy baja probabilidad de ocurrencia o frecuencia.
on
off

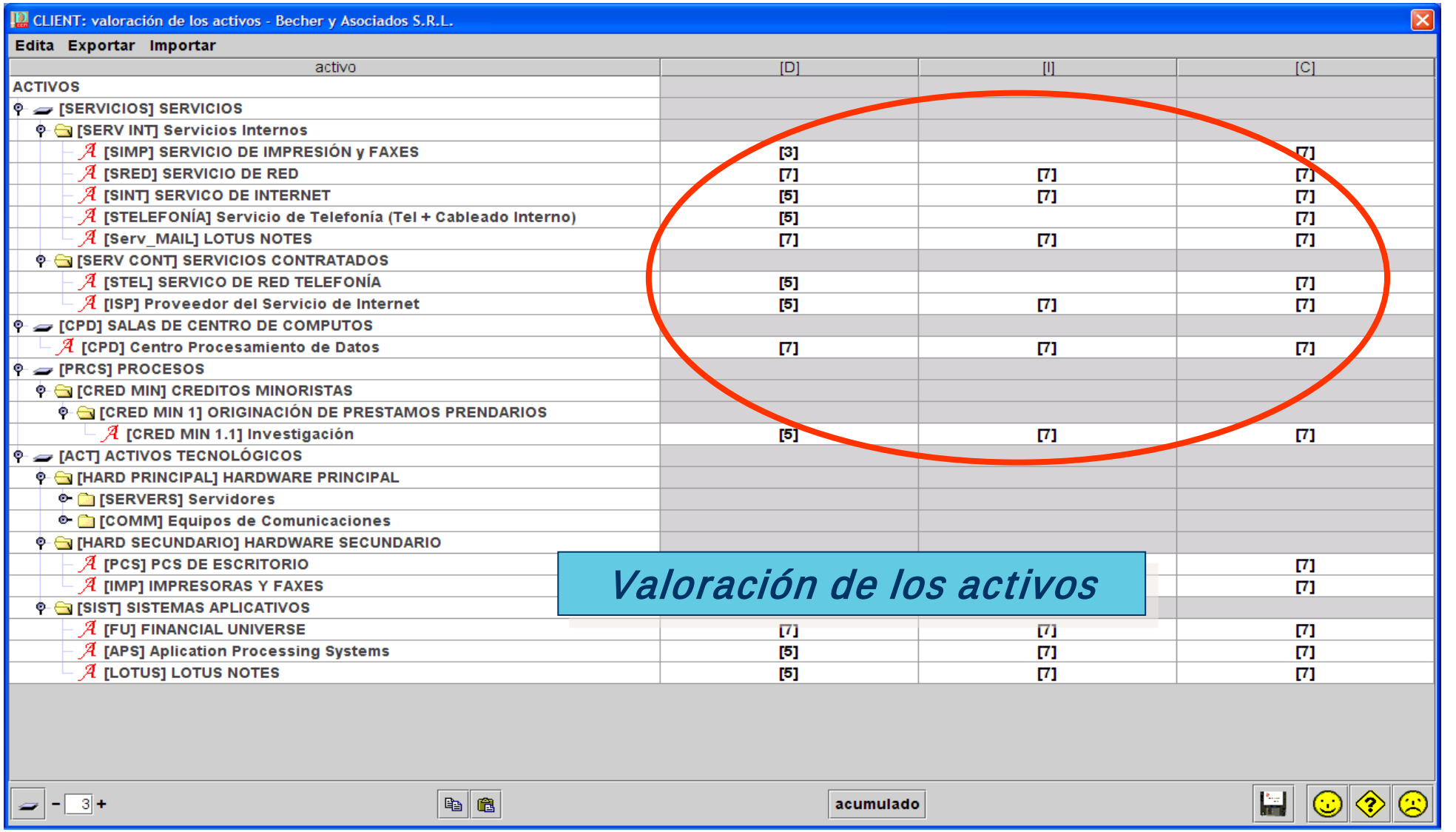

CLIENT: identificación de activos - Becher y Asociados S.R.L.
Capas Activos Dominios Estadísticas
ACTIVOS
[SERVICIOS] SERVICIOS
[SERV INT] Servicios Internos
[SIMP] SERVICIO DE IMPRESIÓN y FAXES
[SRED] SERVICIO DE RED
[SINT] SERVICO DE INTERNET
[STELEFONÍA] Servicio de Telefonía (Tel + Cableado Interno)
[Serv_MAIL] LOTUS NOTES
[SERV CONT] SERVICIOS CONTRATADOS
[STEL] SERVICO DE RED TELEFONÍA
[ISP] Proveedor del Servicio de Internet
[CPD] SALAS DE CENTRO DE COMPUTOS
[CPD] Centro Procesamiento de Datos
[PRCS] PROCESOS
[CRED MIN] CREDITOS MINORISTAS
[CRED MIN 1] ORIGINACIÓN DE PRESTAMOS PRENDARIOS
[CRED MIN 1.1] Investigación
[ACT] ACTIVOS TECNOLÓGICOS
[HARD PRINCIPAL] HARDWARE PRINCIPAL
[SERVERS] Servidores
[ARCIFS01] File Server
[ARCIEN01] Servidor de Correo
[ARCIDB02] Servidor Base de Datos
[ARCIPS01] Servidor para Impresión
[COMM] Equipos de Comunicaciones
[HARD SECUNDARIO] HARDWARE SECUNDARIO
[PCS] PCS DE ESCRITORIO
[IMP] IMPRESORAS Y FAXES
[SIST] SISTEMAS APLICATIVOS
[FU] FINANCIAL UNIVERSE
[APS] Aplication Processing Systems
[LOTUS] LOTUS NOTES
3
dominio
fuente
csv
Capas
Se crean los activos a analizar, cada uno corresponde a distintas Capas.

Caracterización de un activo

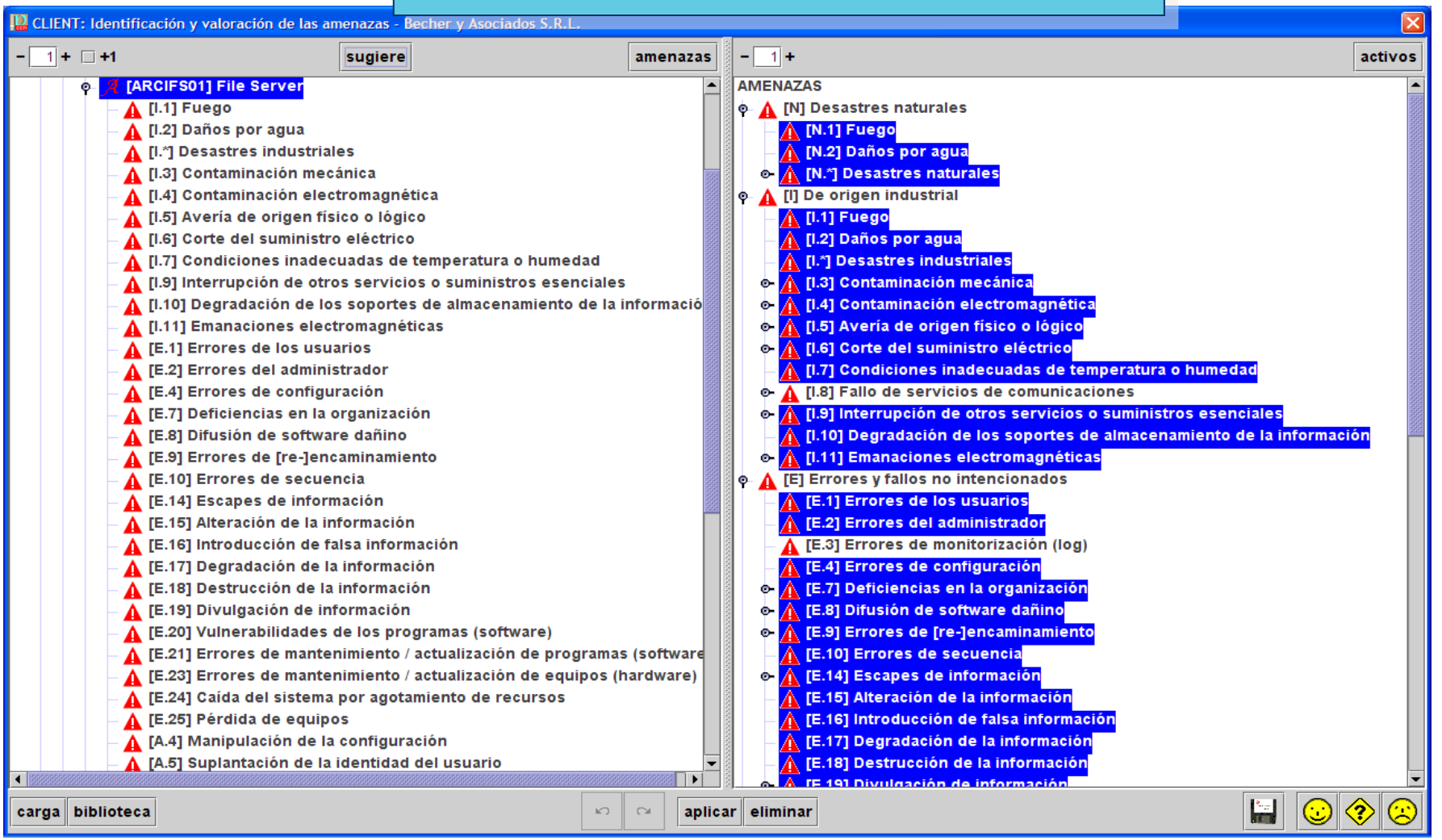


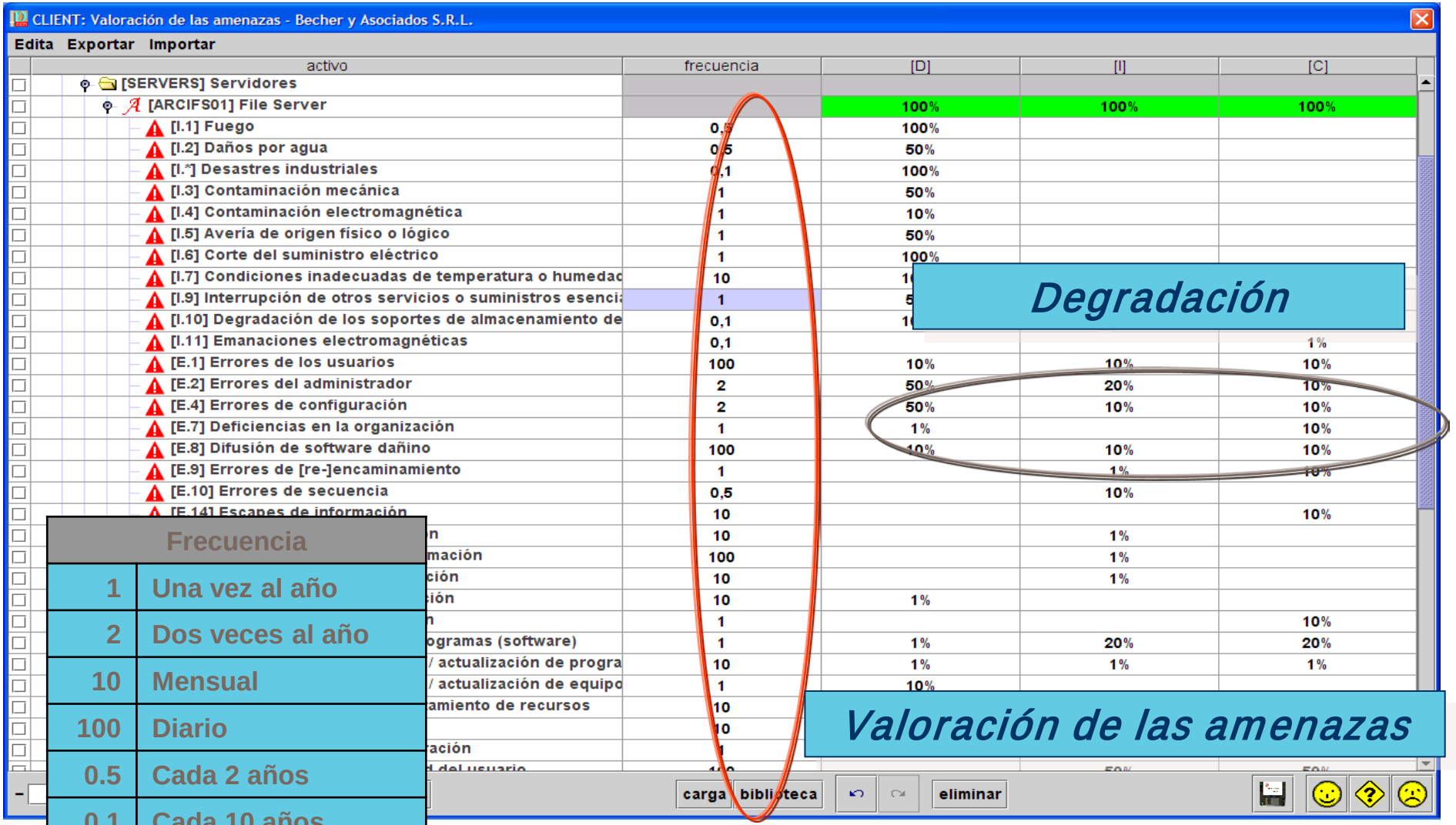
Dependencias de los activos

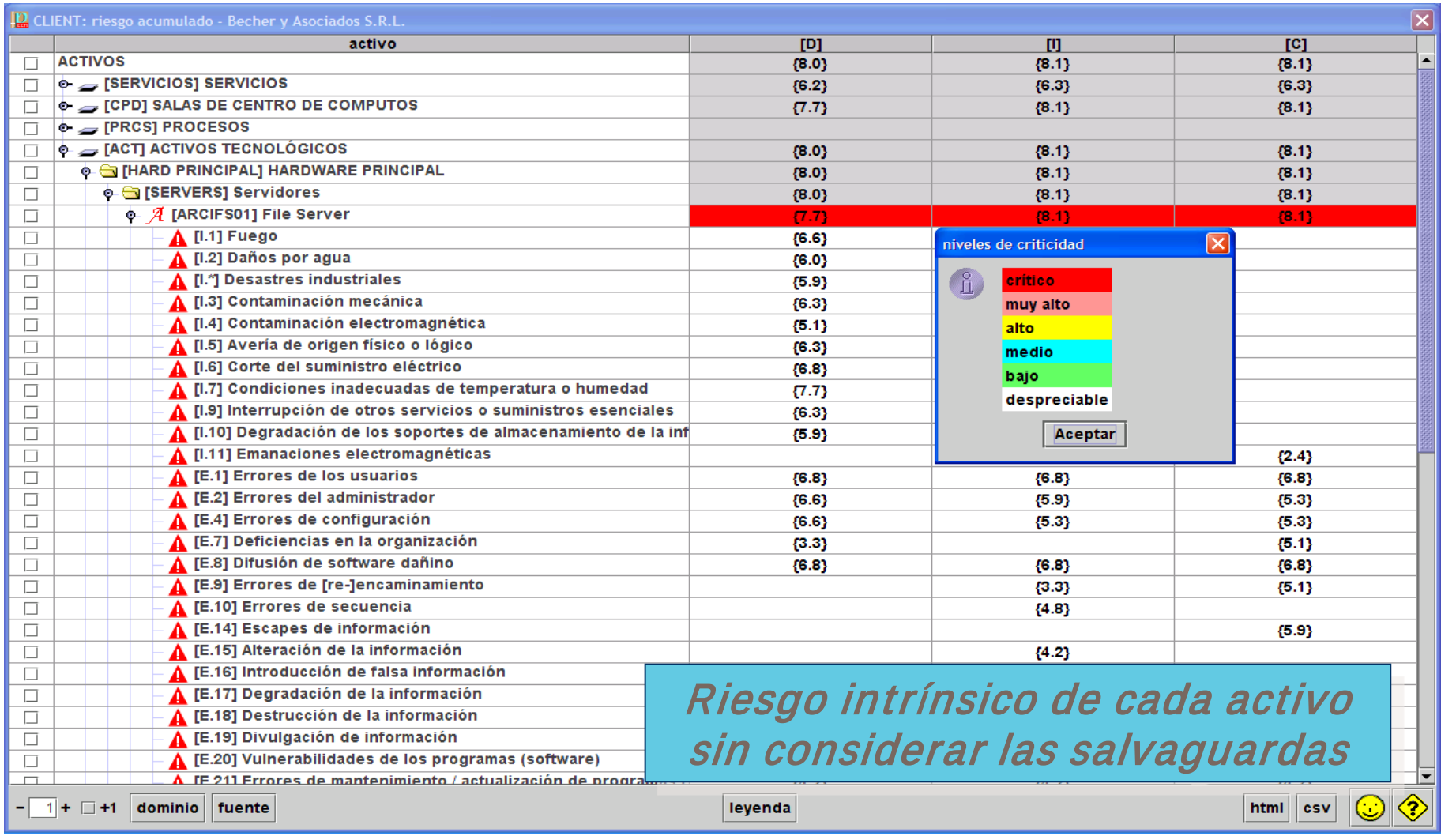



CLIENT: valoración de los activos - Becher y Asociados S.R.L.
Edita Exportar Importar
activo [D] [I] [C]
ACTIVOS
[SERVICIOS] SERVICIOS
[SERV INT] Servicios Internos
[SIMP] SERVICIO DE IMPRESIÓN y FAXES [3] [7]
[SRED] SERVICIO DE RED [7] [7] [7]
[SINT] SERVICO DE INTERNET [5] [7] [7]
[STELEFONÍA] Servicio de Telefonía (Tel + Cableado Interno) [5] [7]
[Serv_MAIL] LOTUS NOTES [7] [7] [7]
[SERV CONT] SERVICIOS CONTRATADOS
[STEL] SERVICO DE RED TELEFONÍA [5] [7]
[ISP] Proveedor del Servicio de Internet [5] [7] [7]
[CPD] SALAS DE CENTRO DE COMPUTOS
[CPD] Centro Procesamiento de Datos [7] [7] [7]
[PRCS] PROCESOS
[CRED MIN] CREDITOS MINORISTAS
[CRED MIN 1] ORIGINACIÓN DE PRESTAMOS PRENDARIOS
[CRED MIN 1.1] Investigación [5] [7] [7]
[ACT] ACTIVOS TECNOLÓGICOS
[HARD PRINCIPAL] HARDWARE PRINCIPAL
[SERVERS] Servidores
[COMM] Equipos de Comunicaciones
[HARD SECUNDARIO] HARDWARE SECUNDARIO
[PCS] PCS DE ESCRITORIO [7]
[IMP] IMPRESORAS Y FAXES [7]
[SIST] SISTEMAS APLICATIVOS
[FU] FINANCIAL UNIVERSE [7] [7] [7]
[APS] Aplication Processing Systems [5] [7] [7]
[LOTUS] LOTUS NOTES [5] [7] [7]
Valoración de los activos
acumulado

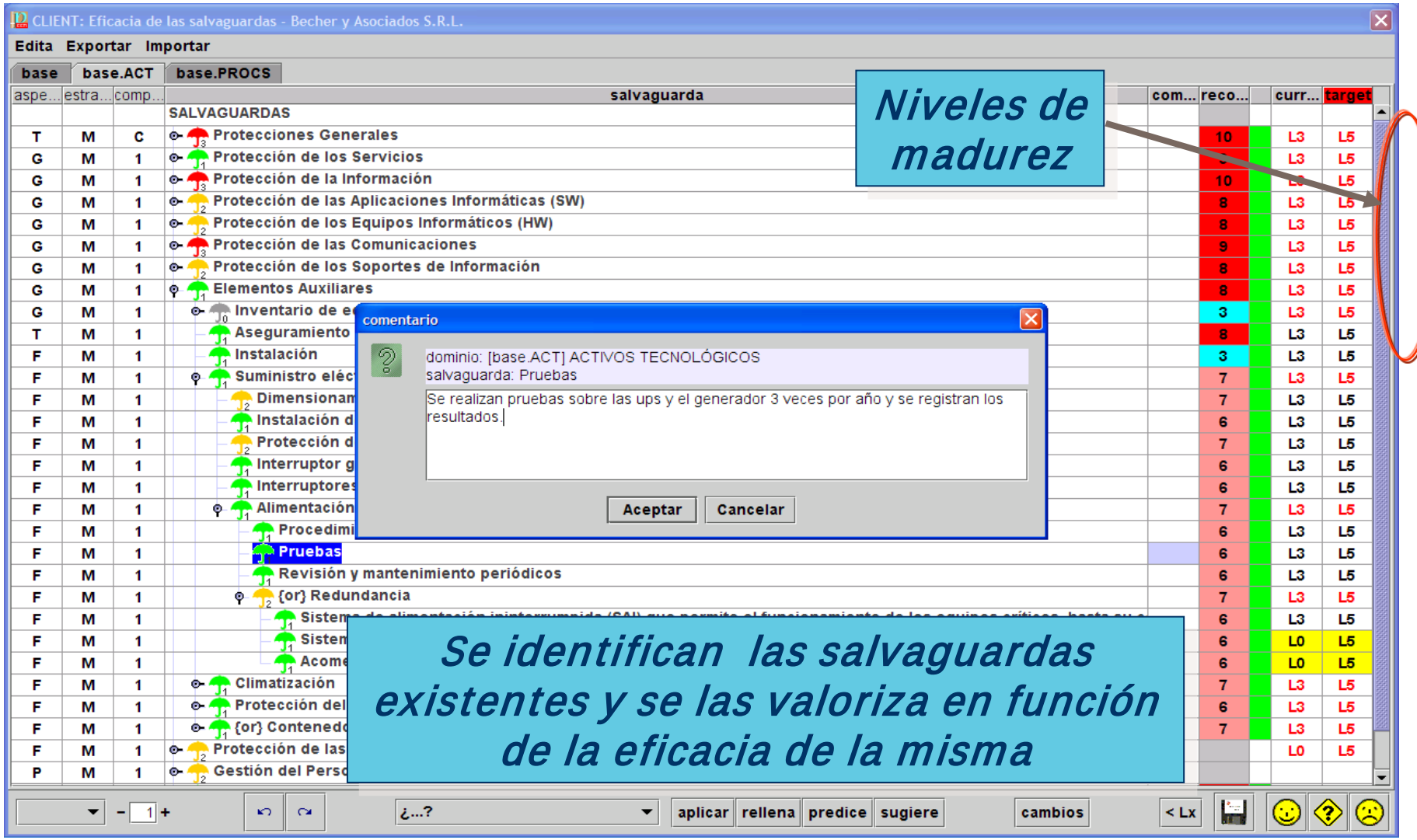
Identificación de las amenazas

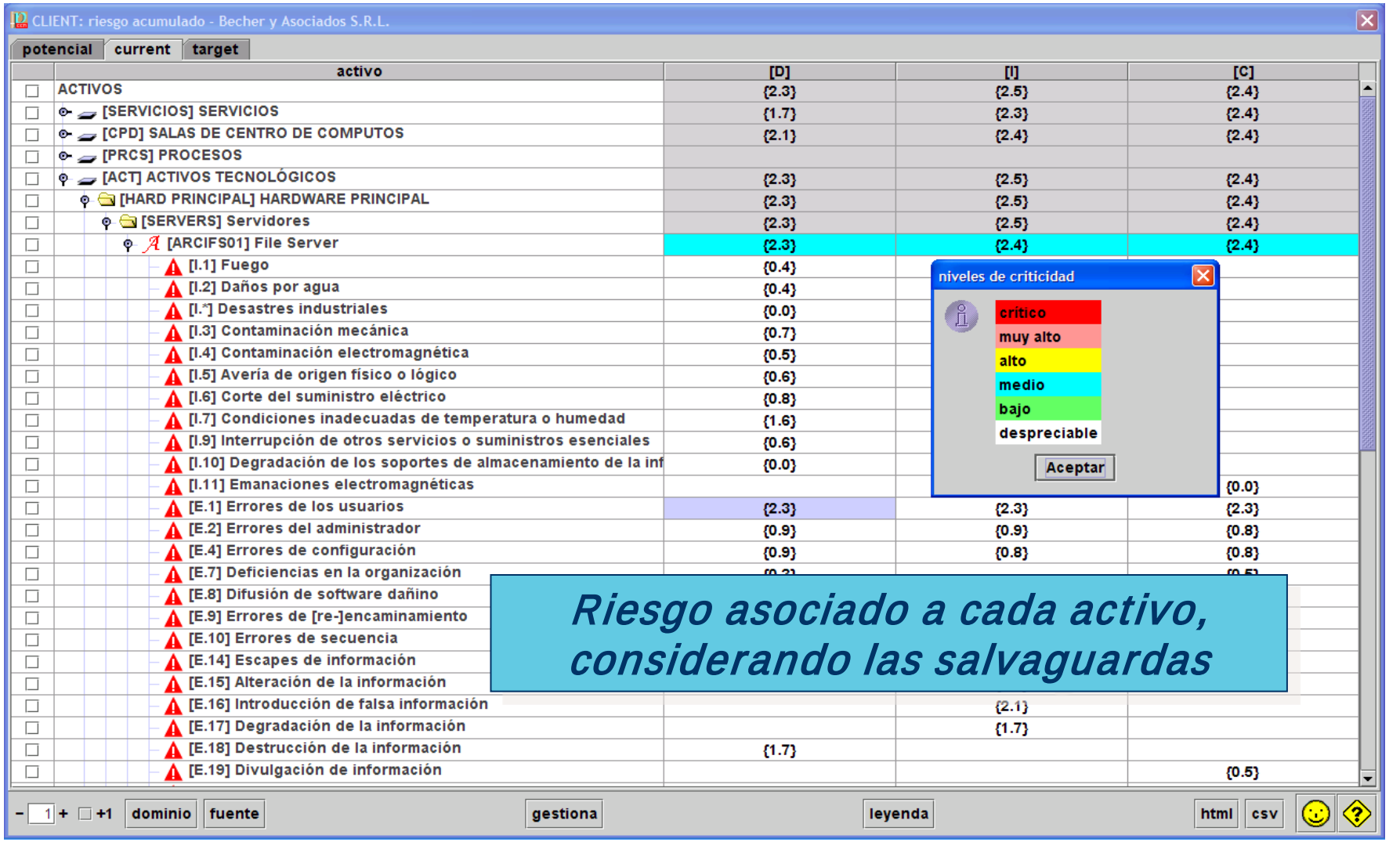



CLIENT: Valoración de las amenazas - Becher y Asociados S.R.L.
Edita Exportar Importar
activo
frecuencia
[D]
[I]
[C]
[SERVERS] Servidores
[ARCIFS01] File Server
100%
100%
100%
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.9] Interrupción de otros servicios o suministros esenci
[I.10] Degradación de los soportes de almacenamiento de
[I.11] Emanaciones electromagnéticas
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Escapes de información
ogramas (software)
/ actualización de progra
/ actualización de equipo
amiento de recursos
ración
carga
biblioteca
eliminar
Degradación
Valoración de las amenazas
Frecuencia
1 Una vez al año
2 Dos veces al año
10 Mensual
100 Diario
0.5 Cada 2 años
0.1 Cada 10 años



Riesgo intrínsico de cada activo sin considerar las salvaguardas


CLIENT: Eficacia de las salvaguardas - Becher y Asociados S.R.L.
Edita Exportar Importar
base base.ACT base.PROCS
aspe... estra... comp... salvaguarda com... reco... curr... target
SALVAGUARDAS
Protecciones Generales
Protección de los Servicios
Protección de la Información
Protección de las Aplicaciones Informáticas (SW)
Protección de los Equipos Informáticos (HW)
Protección de las Comunicaciones
Protección de los Soportes de Información
Elementos Auxiliares
Inventario de e
Aseguramiento
Instalación
Suministro eléc
Dimensionam
Instalación d
Protección d
Interruptor g
Interruptores
Alimentación
Procedimi
Pruebas
Revisión y mantenimiento periódicos
{or} Redundancia
Sisten
Sisten
Acome
Climatización
Protección del
{or} Contenedo
Protección de las
Gestión del Perso
comentario
dominio: [base.ACT] ACTIVOS TECNOLÓGICOS
salvaguarda: Pruebas
Se realizan pruebas sobre las ups y el generador 3 veces por año y se registran los resultados.
Aceptar
Cancelar
¿...?
aplicar
rellena
predice
sugiere
cambios
< Lx
Niveles de madurez
Se identifican las salvaguardas existentes y se las valoriza en función de la eficacia de la misma



Riesgo asociado a cada activo, considerando las salvaguardas

CLIENT: riesgo repercutido - Becher y Asociados S.R.L.

potencial | current | target

activo	[D]	[I]	[C]
ACTIVOS	{2.3}	{2.5}	{2.4}
[SIMP] SERVICIO DE IMPRESIÓN y FAXES	{1.9}		{2.4}
[SRED] SERVICIO DE RED	{1.8}	{2.3}	{2.4}
[SINT] SERVICO DE INTERNET	{1.6}	{2.3}	{2.4}
[STELEFONÍA] Servicio de Telefonía (Tel + Cableado Interno)	{1.6}		{2.4}
[Serv_MAIL] LOTUS NOTES	{2.1}	{2.3}	{2.3}
[STEL] SERVICO DE RED TELEFONÍA	{1.3}		{2.4}
[ISP] Proveedor del Servicio de Internet	{1.3}	{2.3}	{2.4}
[CPD] Centro Procesamiento de Datos	{1.8}	{2.2}	{2.2}
[CRED MIN 1.1] Investigación	{2.0}	{2.3}	{2.4}
[ARCIFS01] File Server	{2.3}	{2.4}	{2.4}
[...] ...			
[CPD] Centro Procesamiento de Datos	{2.1}	{2.4}	{2.4}
[N.1] Fuego	{0.9}		
[N.2] Daños por agua	{0.7}		
[N.*] Desastres naturales	{0.4}		
[I.1] Fuego	{0.9}		
[I.2] Daños por agua	{0.7}		
[I.*] Desastres industriales	{0.7}		
[I.3] Contaminación mecánica	{0.4}		
[I.5] Avería de origen físico o lógico	{0.7}		
[I.6] Corte del suministro eléctrico	{2.1}		
[I.7] Condiciones inadecuadas de temperatura o humedad	{1.6}		
[A.7] Uso no previsto			{2.4}
[A.11] Acceso no autorizado	{1.2}	{1.1}	{1.3}
[A.25] Robo de equipos	{0.5}		{0.6}
[A.26] Ataque destructivo	{0.7}		
[A.27] Ocupación enemiga	{0.7}	{0.6}	{0.6}
[HARD PRINCIPAL.COMM.SW1] Swicth 1	{1.8}	{1.1}	{1.2}
[ARCILN01] Servidor de Correo	{2.1}	{2.4}	{2.4}
[ARCIDB02] Servidor Base de Datos	{2.3}	{2.5}	{2.4}
[ARCIPS01] Servidor para Impresión	{1.9}		{2.1}

niveles de criticidad

- crítico
- muy alto
- alto
- medio
- bajo
- despreciable

Aceptar

leyenda | html | csv

Riesgo Repercutido

EJEMPLOS DE NUESTROS SERVICIOS – CONSULTORÍA

Servicio Seguridad en E-Commerce

Llegada a nuevos clientes y consecuente mejora en la facturación.

Servicio API

EJEMPLOS DE NUESTROS SERVICIOS – CONSULTORÍA

SEGURIDAD DE LA INFORMACIÓN

Podemos brindarle soluciones a su medida, ya que contamos con una amplia experiencia en el área de seguridad de la información, dando servicios de consultoría en las normas de la serie ISO 27000, Ley de Protección de Datos Personales, test de intrusión, Asesoramiento a Gerencias de Seguridad de la Información (PESI), planes de concientización (Awareness), Computación forense, BCP (Business Continuity Plan) y DRP (Disaster Recovery Plan) y otros servicios especializados del área.

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI)

Es un instrumento en donde se refleja secuencialmente y priorizados las políticas, inversiones, recursos y necesidades del negocio relacionadas con la Seguridad de la Información.

Cómo armar e Implementar un PESI?

1. Identificar tareas actuales aplicados a S.I.
2. Identificar tiempos asociados a las tareas (1).
3. Identificar tiempos disponibles del personal de S.I.
4. Identificar la capacidad del personal de S.I.

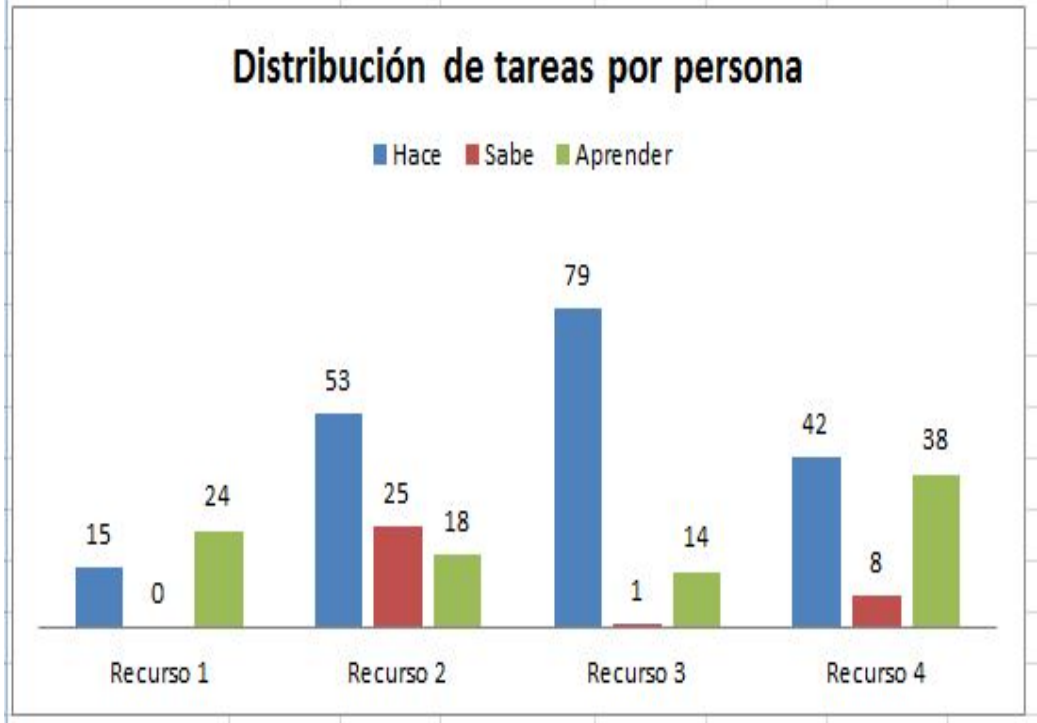
Cómo armar e Implementar un PESI?

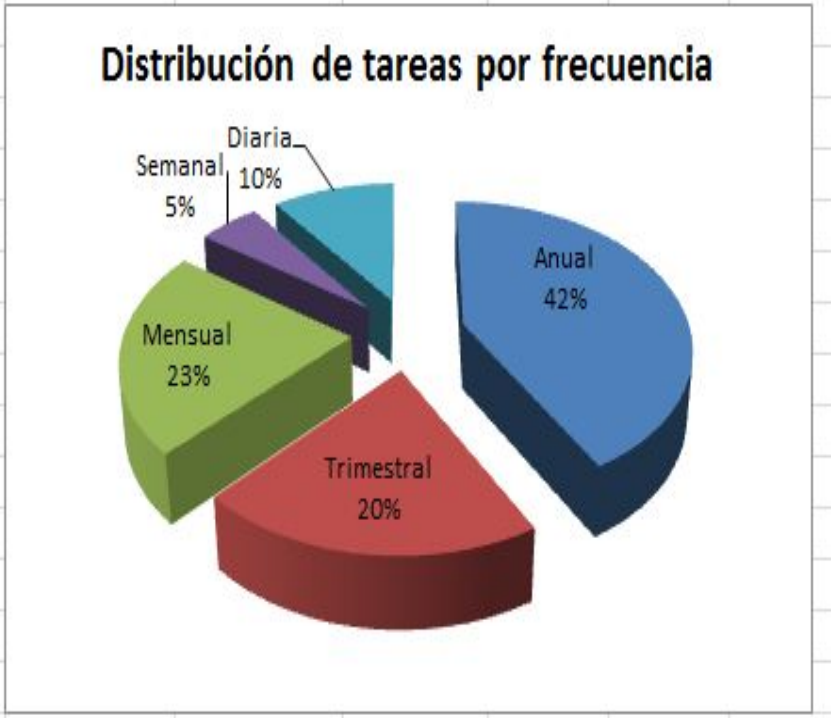
#	Aplic.	Grupo	Tarea	Tecnica / Funcional
1	No	Acceso al CPD	Actualización logs en Tablero de Control	Técnica
2	No	Acceso al CPD	Administración de usuarios (ABM)	Técnica
3	No	Acceso al CPD	Configuración del Equipo	Técnica
12	No	Active Directory	Definición de políticas (GPO)	Funcional
13	No	Active Directory	Delegación de Funciones	Técnica
17	No	Administración de claves	Administración de claves de usuarios especiales y de	Funcional
20	No	Análisis de vulnerabilidades	Análisis periódicos de vulnerabilidades en servidores	Técnica
21	No	Análisis de vulnerabilidades	Control sobre administradores locales de las maquinas	Funcional
36	Si	Windows	Administración de usuarios (ABM)	Técnica
37	Si	Windows	Blanqueo de contraseñas	Técnica
38	Si	Windows	Desbloqueo de usuarios	Técnica
40	Si	Windows	Administración de usuarios (ABM)	Técnica
41	Si	Windows	Blanqueo de contraseñas	Técnica
42	Si	Windows	Desbloqueo de usuarios	Técnica
43	No	Auditoria	Atención a Auditores externos e internos (temas Seguridad)	Funcional
44	No	Auditoria	Recolección de información y coordinación de reuniones para responder los informes	Funcional
45	No	Auditoria	Respuesta a Informes de Auditoria	Funcional

Cómo armar e Implementar un PESI?

Recurso	Hace	Sabe	Aprender	Total
Recurso 1	15	0	24	39
Recurso 2	53	25	18	96
Recurso 3	79	1	14	94
Recurso 4	42	8	38	88

Frecuencia	Cantidad
Anual	41
Trimestral	20
Mensual	22
Semanal	5
Diaria	10





¿Cómo armar e Implementar un PESI? (cont.)

Segunda Etapa: Identificar Objetivos

1. Identificar tareas requeridas por normativa determinada.
2. Identificar tareas resultado de procesos controles y/o auditorias previ
3. Identificar tareas objeto de procesos ajenos a Seguridad de la Información.
4. Identificar los niveles de implementación requeridos por el negocio para cada tarea.
5. Proyectar/Identificar necesidades POST implementación de una tarea.

Segunda Etapa: Identificar Objetivos

#	Tareas del Administrador de Seguridad	Año Actual	Prioridad	Año Objetivo (Por ej. 2013)
T	Análisis de Riesgo de TI			
2	Generación de Marco Normativo relacionado al Análisis de Riesgo de TI	L1		L3
3	Planificación para la ejecución del Análisis de Riesgo de TI	L1		L2
4	Implementación del Análisis de Riesgo de TI	L1		L3
5	Comunicación de resultados a las autoridades pertinentes	L1		L2
6	Generación de Plan de Acción en Base a resultados del Análisis de Riesgo de TI y concenso con autoridades pertinentes	L1		L2
T	Desarrollo, mantenimiento e implementación del Marco Normativo de Seguridad de la Información			
8	Generación y publicación de Política de Seguridad (Firmada por la Dirección)	L4		L4
9	Generación y publicación de Normas y procedimientos relacionados a la seguridad de la información	L3		L4
10	Generación y publicación de Procedimientos Operativos (Backup, operación de aplicativos, etc)	L2		L3
11	Generación y publicación de Manual de Misiones y Funciones del Área de Seguridad Informática	L3		L4
12	Generación y publicación de Responsabilidades en Materia de Seguridad de la Información	L3		L4
13	Definición de responsable de establecer contacto con autoridades pertinentes (bomberos, policias, emergencias médicas)	N/A		N/A
14	Revisión de Marco Normativo	L1		L3
T	Foro de Seguridad de la Información			
16	Creación del Foro de Seguridad de la Información	L0		L0
17	Coordinación de reuniones del Foro de Seguridad de la Información	L0		L0

BDO

Cómo armar e Implementar un PESI? (cont.)

Tercera Etapa: Armado del PESI

1. Identificar los tiempos requeridos por cada tarea.
2. Identificar responsables de llevarla a cabo / su implementación.
3. Identificar los costos/recursos asoci
4. Generar el Plan de Implementación requerimientos externos.

Cómo armar e Implementar un PESI? (cont.)

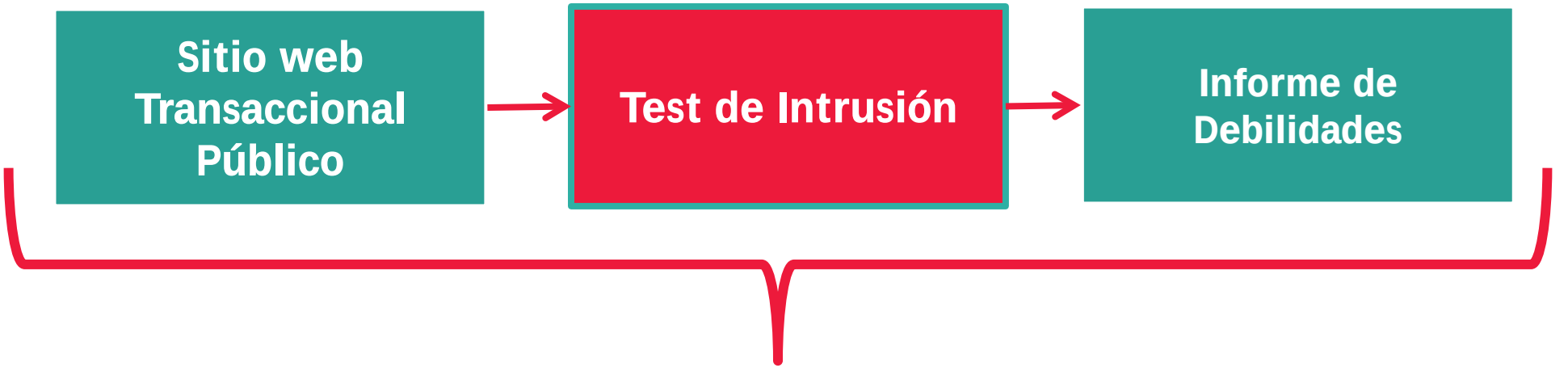
Cuarta Etapa: Implementación Exitosa

1. Sponsoreo de la Alta Dirección
2. Monitoreo de los avances.
3. Gestión de los retrasos/desvíos.
4. Adecuaciones oportunas.

¡¡ SEGUIMIENTO CONTINUO !!

EJEMPLOS DE NUESTROS SERVICIOS – CONSULTORÍA

Servicio Test de Intrusión



Seguridad en las operaciones de clientes (impacto en la imagen)/empleados.

Servicio API

¿CÓMO PODEMOS AYUDARLO? (cont.)

NORMAS Y REGULACIONES LOCALES E INTERNACIONALES

Diagnóstico, asesoramiento y consultoría para el cumplimiento de diferentes regulaciones y normativas, incluyendo entre las principales: Secc. 404 de la Ley Sarbanes-Oxley, PCI-DSS, SSAE 16 (reemplaza SAS 70),ISAE 3402, ISO 20000, ISO 27000 y otras.

BDO

EJEMPLOS DE NUESTROS SERVICIOS – CONSULTORÍA

Servicio PCI-DSS

Ahorro Económico (menos Postnets y procesos administrativos eficaces)

Servicio API

PCI - DSS

PREPARADOS PARA EL CAMBIO

El nuevo estándar de la Industria de Tarjetas de Pago se encuentra vigente desde enero de 2014 y será exigible desde enero de 2015.
En BDO pensamos como asistir a nuestros clientes en los nuevos desafíos, por ello desarrollamos metodologías y buenas prácticas para acompañarlos en el cambio.

INFRAESTRUCTURA Y TECNOLOGÍA

Consultoría para áreas de tecnología abarcando implementación, soporte, migración y mantenimiento de sistemas operativos y redes, soluciones seguras de mensajería y correo electrónico, implementación de productos de seguridad informática (herramientas para administración de logs, IDS/IPS), reingeniería de comunicaciones, virtualización de servidores, cloud computing.

SEGURIDAD EN ERP

Diagnóstico y consultoría para evaluar aspectos clave que hacen a la seguridad del sistema, destacando segregación funcional y controles por oposición, roles y funciones, logs de auditoría, accesos de personal del área de TI a funciones de negocio y políticas de seguridad en el aplicativo, bases de datos y sistema operativo.

EJEMPLOS DE NUESTROS SERVICIOS – TERCERIZACIÓN

Servicio Soporte en Infraestructura

Menos interrupciones del negocio por indisponibilidad de sistemas.

Servicio API

NUESTROS ANTECEDENTES

Las principales compañías financieras y bancos de la República Argentina han contratado nuestros servicios, al igual que empresas especializadas en mercados verticales tales como petróleo, telecomunicaciones, datacenters, laboratorios, salud.

YPF

BANCO PIANO
Nuestra virtud es saber interpretarlo

Santander Río

IRSA

AP

CRESUD

Banco Provincia

TELECOM

C.S.F.

QBE SEGUROS
LA BUENOS AIRES

Telefónica

HOSPITAL UNIVERSITARIO AUSTRAL

DIRECTV

BDO

NUESTROS ANTECEDENTES

Argentina
Bolivia
Brazil
Chile
Colombia
Costa Rica
Ecuador
El Salvador
Guatemala
Mexico
Panama
Paraguay
Peru
Uruguay
Venezuela

Somos Centro de Excelencia de LATAM.

¡MUCHAS GRACIAS!

Ing. Pablo Silberfich
Socio
Aseguramiento de Procesos Informáticos

Maipú 942 1° piso
Rondeau 1664, PB
Buenos Aires, Argentina
Tel.: 54 11 4106 7000
Fax: 54 11 4106 7255

www.bdoargentina.com