tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

111

MANTENIMIENTO DE LA CONTINUIDAD DEL SERVICIO USANDO LA HERRAMIENTA PILAR DE SOPORTE A LA GESTIÓN DE RIESGOS

José A. Mañas
Centro Criptológico Nacional
Centro Nacional de Inteligencia

José A. Mañas

Palabras clave

Continuidad del servicio, plan de contingencia, análisis de impacto, análisis de riesgos, gestión de riesgos, recuperación de desastres.

Resumen de su Comunicación

La herramienta PILAR se diseñó para la gestión de los riesgos a que están sometidos los sistemas de información, analizando los componentes del sistema, sus relaciones internas, las amenazas a las que están expuestos y las salvaguardas desplegadas. Todo ello permite derivar consecuencias y necesidades de actuación para racionalizar el estado de riesgo residual. Estas mismas técnicas se aplican a una dimensión muy concreta de la seguridad que es la disponibilidad, valorándose los activos por el daño que supondría una indisponibilidad de un cierto tiempo. PILAR nos aportará datos sobre la criticidad de los componentes del sistema, permitiéndonos incorporar equipos de respaldo e incluso diseñar un plan de recuperación.

José A. Mañas

MANTENIMIENTO DE LA CONTINUIDAD DEL SERVICIO USANDO LA HERRAMIENTA PILAR DE SOPORTE A LA GESTIÓN DE RIESGOS

1. Introducción

Las organizaciones instalan y operan sistemas de información con el objetivo de prestar una serie de servicios que se consideran importantes para alcanzar sus objetivos o misión. Estos servicios se pueden ver afectados por situaciones de emergencia o de desastre que impiden su normal desempeño. Ante estas situaciones hay que reaccionar prontamente de tal forma que los servicios se sigan prestando en condiciones aceptables.

A los sistemas de información les pueden pasar cosas que interrumpan temporal o definitivamente su capacidad de prestar servicio. El rango de cosas es amplio, desde pequeños incidentes hasta grandes desastres. Ante unos u otros necesitamos planes de continuidad que garanticen que la organización sigue prestando sus servicios. La continuidad puede alcanzarse por medio de equipos alternativos o, en caso de desastre, puede requerir la reconstrucción del sistema en otro lugar. Se denomina desastre a una "desgracia grande", término que, en sistemas de información, usaremos para referirnos a la pérdida de equipos e instalaciones.

Sea la desgracia grande (desastre) o pequeña (incidente), siempre necesitamos un plan de emergencia que nos permita reaccionar con presteza. Durante las emergencias no vale improvisar pues ello equivaldría a no poder garantizar un tiempo de respuesta. Aunque no es el lugar para dudar de la buena voluntad de las personas, de lo que se trata es de organizar esa buena disposición en un plan que se ejecuta cuando es necesario.

Los planes de emergencia incluyen múltiples aspectos, desde salvar las vidas de los ocupantes, pasando por recuperar la información y terminando por habilitar medios alternativos de trabajo. Aquí nos centraremos en los activos de los sistemas de información que deben ser conocidos y analizados para poder desarrollar planes con fundamento y garantía de que alcanzarán los objetivos propuestos por la dirección de la organización.

2. PILAR

PILAR (Procedimiento Informático y Lógico para el Análisis de Riesgos) es una herramienta desarrollada bajo prescripciones del Centro Nacional de Inteligencia (CNI) para el análisis de los sistemas de información, análisis encaminado a determinar los riesgos potenciales que penden sobre los sistemas, identificar contra medidas proporcionadas a aquellos riesgos, y resumir el riesgo residual que aún soporta la organización (debido a que las salvaguardas son inadecuadas o insuficientes). En particular, se soporta la metodología MAGERIT desarrollada por el Ministerio para las Administraciones Públicas.

Es universalmente reconocido que un análisis de riesgos es tarea previa necesaria para acometer planes de continuidad, en la medida en que refleja qué elementos constituyen el sistema de información, qué servicios prestan, cómo se interrelacionan y cómo de protegidos se hayan.

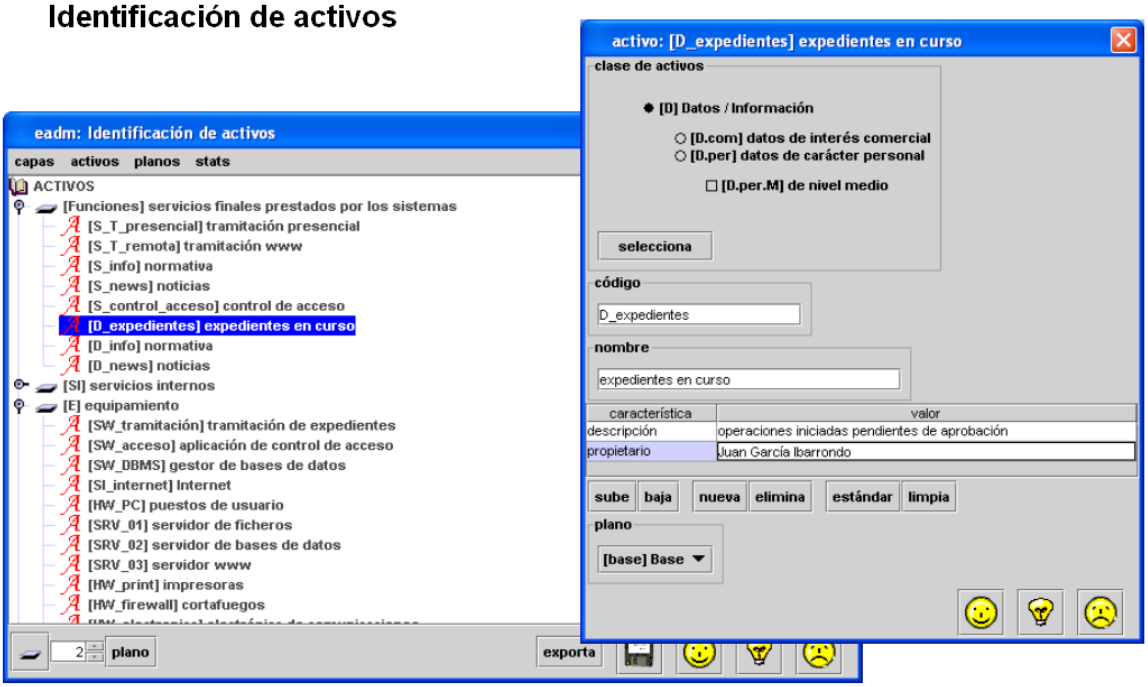
Activos

Lo primero que necesitamos es determinar qué recursos (informática y comunicaciones) constituyen el sistema de información o están directamente relacionados con él, siendo imprescindibles para alcanzar los

objetivos propuestos. Equipos informáticos, redes de comunicaciones y equipamiento auxiliar son, sin duda, parte constituyente del sistema. A ello deberíamos añadir las instalaciones que los acogen y el personal que los utiliza o los administra.

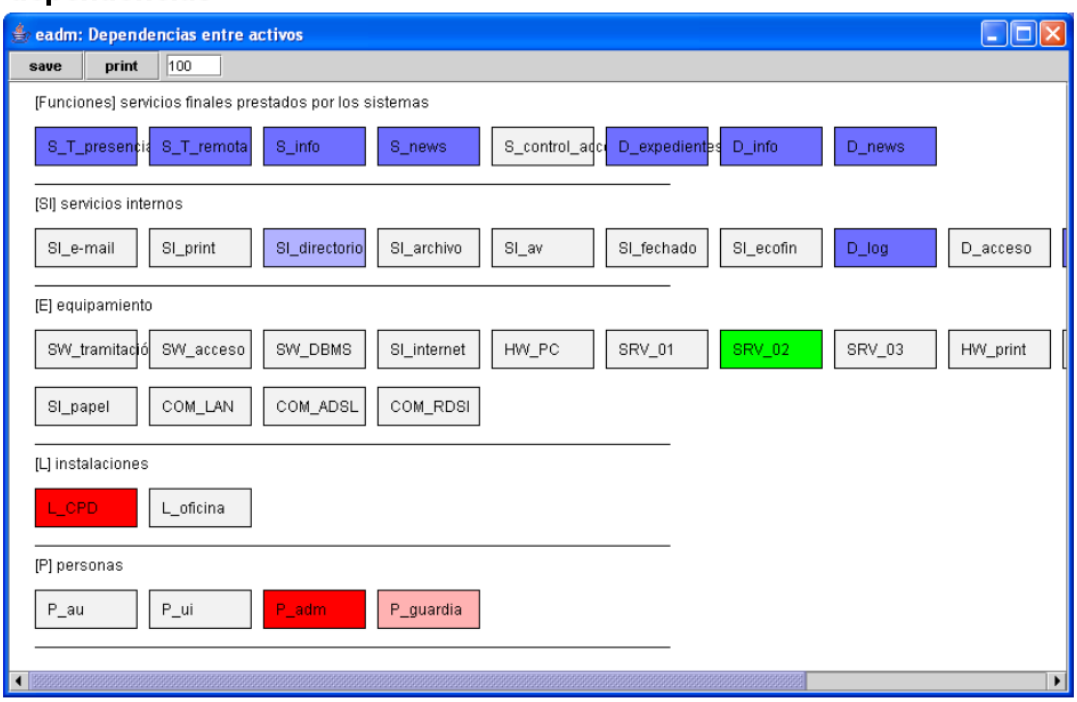
A dichos activos de carácter tangible hay que añadir algunos aspectos intangibles que constituyen su razón de ser: la información que manejan y los servicios que ofrecen. Visto por pasiva, no tendría sentido que un sistema de información ni manejara información valiosa, ni proporcionara servicios útiles. En cualquier caso, a lo que nos ocupa, no habría ninguna necesidad de que sobreviviera tras un incidente o un desastre.

Identificación de activos



Los activos se relacionan entre sí, de forma que la información se deposita en los equipos informáticos y transita por la redes de comunicaciones. Los servicios sólo se pueden prestar si se dispone de los equipos y de las líneas de conexión. A su vez, equipos y redes dependen de las instalaciones físicas que los acogen y todo depende del personal que administra equipos e instalaciones.

Inter dependencias



Las interdependencias entre activos van a ser un elemento crítico para determinar las consecuencias sobre los servicios finales de la detención o destrucción de partes del equipamiento. Si la disponibilidad de un servicio es importante, todos los activos que lo soportan son igual de importantes y deberán ser objeto de medidas adecuadas que los hagan prescindibles (por ejemplo mediante equipamiento alternativo) o rápidamente recuperables. Estas imputaciones incluyen instalaciones y personal necesario.

Las interdependencias son también un elemento crítico para diseñar un plan de recuperación de desastres pues el responsable del plan puede diseñar una recuperación progresiva (o escalonada) en la que los primeros activos a recuperar están enfocados a rehabilitar los servicios más críticos pero, habitualmente, "de paso" habilitan otros servicios. Este comentario no hace sino constatar que habitualmente el equipamiento es compartido por múltiples servicios.

Por último, las interdependencias nos informas de otros requisitos tales como garantías de confidencialidad, integridad y autenticidad que, sin ser parte de la continuidad del servicio sin son parte crítica de las condiciones en que dicha continuidad debe proporcionarse; es decir, de las salvaguardas (técnicas y procedimentales) que se le van a exigir al equipamiento alternativo.

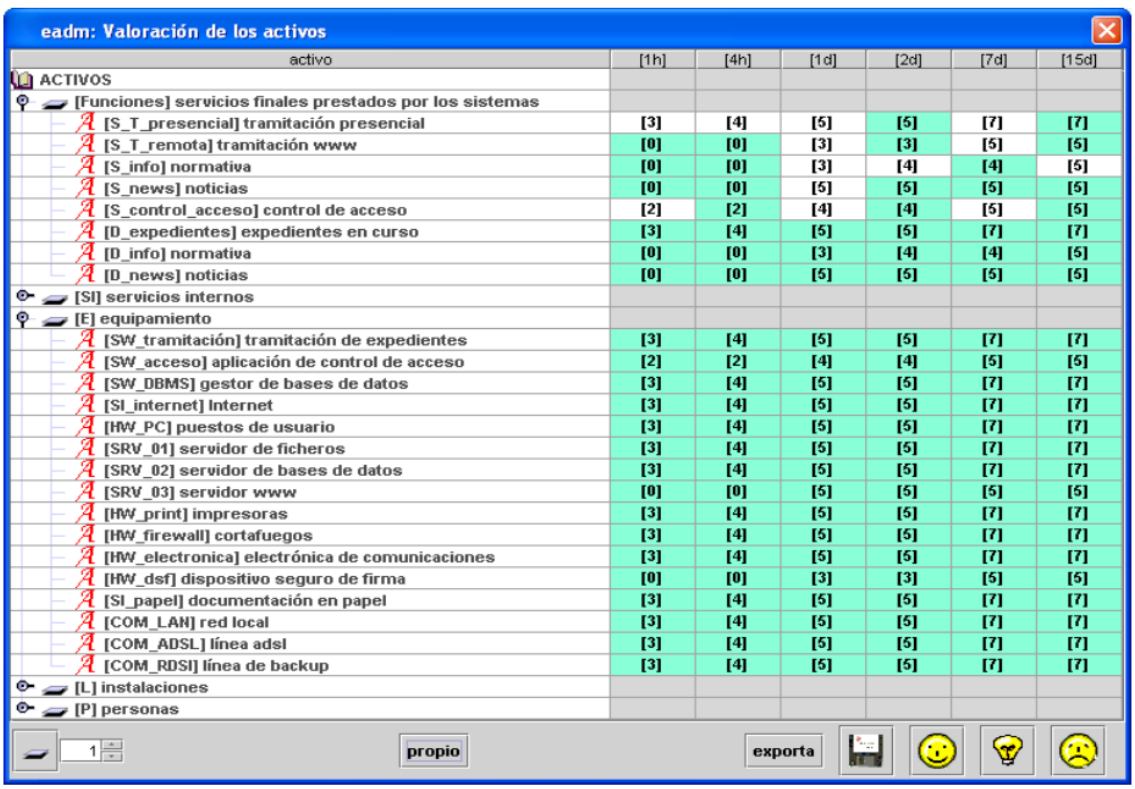
3. Valoración de los activos

Los sistemas de información son subsidiarios del servicio que prestan y los datos que custodian. Su valor fundamental es el que soportan. Un PC puede ser muy barato en términos de adquisición; pero convertirse en muy valioso si soporta una función crítica. En los análisis de riesgos clásicos se estudia el valor de la confidencialidad, integridad, autenticidad, etc., entendiendo por tales el daño o impacto que causaría la pérdida de dichas calidades.

En términos de continuidad es importante introducir el factor tiempo, pues no es lo mismo que el sistema de control de una central nuclear se detenga durante 1 minuto, que un minuto de detención de una página web de la administración electrónica. Es habitual que los sistemas de control industrial den un alto valor a

tiempos cortos de interrupción, mientras que los servicios administrativos internos sean más tolerantes. En un punto intermedio se encuentran los servicios prestados al público.

Valoración acumulada



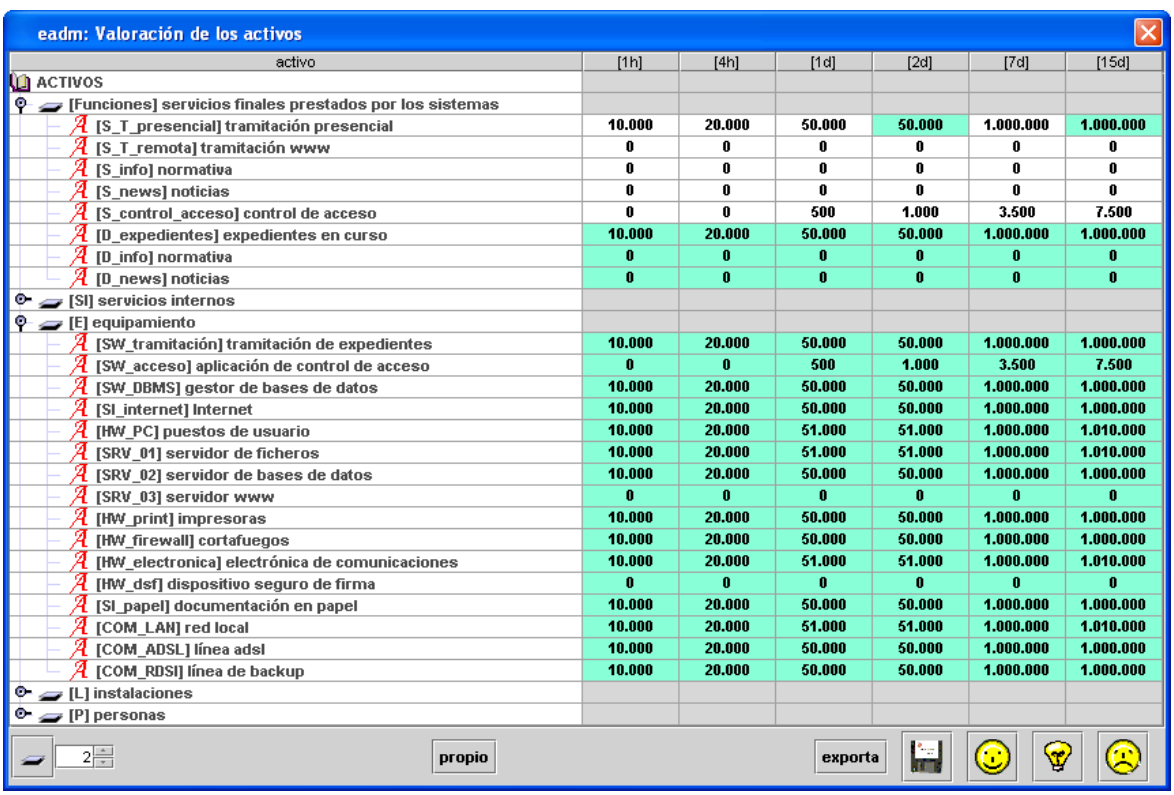
activo	[1h]	[4h]	[1d]	[2d]	[7d]	[15d]
ACTIVOS						
[Funciones] servicios finales prestados por los sistemas						
[S_T_presencial] tramitación presencial	[3]	[4]	[5]	[5]	[7]	[7]
[S_T_remota] tramitación www	[0]	[0]	[3]	[3]	[5]	[5]
[S_info] normativa	[0]	[0]	[3]	[4]	[4]	[5]
[S_news] noticias	[0]	[0]	[5]	[5]	[5]	[5]
[S_control_acceso] control de acceso	[2]	[2]	[4]	[4]	[5]	[5]
[D_expedientes] expedientes en curso	[3]	[4]	[5]	[5]	[7]	[7]
[D_info] normativa	[0]	[0]	[3]	[4]	[4]	[5]
[D_news] noticias	[0]	[0]	[5]	[5]	[5]	[5]
[SI] servicios internos						
[E] equipamiento						
[SW_tramitación] tramitación de expedientes	[3]	[4]	[5]	[5]	[7]	[7]
[SW_acceso] aplicación de control de acceso	[2]	[2]	[4]	[4]	[5]	[5]
[SW_DBMS] gestor de bases de datos	[3]	[4]	[5]	[5]	[7]	[7]
[SI_internet] Internet	[3]	[4]	[5]	[5]	[7]	[7]
[HW_PC] puestos de usuario	[3]	[4]	[5]	[5]	[7]	[7]
[SRV_01] servidor de ficheros	[3]	[4]	[5]	[5]	[7]	[7]
[SRV_02] servidor de bases de datos	[3]	[4]	[5]	[5]	[7]	[7]
[SRV_03] servidor www	[0]	[0]	[5]	[5]	[5]	[5]
[HW_print] impresoras	[3]	[4]	[5]	[5]	[7]	[7]
[HW_firewall] cortafuegos	[3]	[4]	[5]	[5]	[7]	[7]
[HW_electronica] electrónica de comunicaciones	[3]	[4]	[5]	[5]	[7]	[7]
[HW_dsf] dispositivo seguro de firma	[0]	[0]	[3]	[3]	[5]	[5]
[SI_papel] documentación en papel	[3]	[4]	[5]	[5]	[7]	[7]
[COM_LAN] red local	[3]	[4]	[5]	[5]	[7]	[7]
[COM_ADSL] línea adsl	[3]	[4]	[5]	[5]	[7]	[7]
[COM_RDSI] línea de backup	[3]	[4]	[5]	[5]	[7]	[7]
[L] instalaciones						
[P] personas						

En PILAR podemos valorar en términos cualitativos o cuantitativos. Las valoraciones cualitativas se instrumentan por medio de una escala entre 0 (sin valor digno de consideración) y 10 (consecuencias gravísimas), donde un punto intermedio 5 establece la frontera entre lo que son consecuencias que no trascienden a otras organizaciones, y consecuencias que causan daños a terceras partes. Como criterios de valoración se tienen en cuenta aspectos de servicios a ciudadanos, a otras organizaciones, responsabilidades legales o administrativas, problemas de orden público, para la salud de las personas, etc.

Como se ve en la figura adjunta, el coste de una interrupción depende del tiempo que dure ésta. En ejemplo, el servicio de atención presencial empieza a hacerse notar al cabo de 1 hora de detención (nivel 3), trascendiendo al exterior al cabo de 1 día (nivel 5) y causando perjuicios importantes a otras organizaciones al cabo de 7 días de interrupción (nivel 7). Siempre hay un incremento de consecuencias cuando se incrementa el periodo de interrupción. Otros servicios como el de tramitación remota se han evaluado con unas consecuencias más laxas. Las casillas en blanco indican valores estimados por la dirección, que podemos interpretar como especificaciones para el sistema de información. Las casillas en color capturan aquellos valores y los imputan a los activos cuya concurrencia es necesaria para alcanzar los objetivos. Un activo puede soportar varios servicios, siendo su criticidad la del servicio más crítico que soporta (los demás se benefician por añadidura).

Además de las consecuencias intangibles también se puede con frecuencia estimar costes económicos asociados a la interrupción. Un sistema parado es habitualmente una máquina de perder dinero: los empleados se quedan parados, no son productivos, aunque hay que pagarles el sueldo igualmente. Además, cuando el sistema se recupere tendrán que reintroducir los datos procesados manualmente durante la interrupción, esfuerzo que puede traducirse en una productividad mermada o en horas extras; todo ello

cuesta dinero. También pueden darse otras consecuencias económicas, dependiendo fuertemente del tipo de servicio que se presta: penalizaciones por incumplimiento de garantías de servicio o retrasos en las entregas, gastos derivados de responsabilidad civil subsidiaria, multas por violación de obligaciones legales, costes financieros por requerir dinero para hacer frente a las obligaciones de la organización con medios nuevos, etc.



eadm: Valoración de los activos

activo	[1h]	[4h]	[1d]	[2d]	[7d]	[15d]
ACTIVOS						
[Funciones] servicios finales prestados por los sistemas						
[S_T_presencial] tramitación presencial	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[S_T_remota] tramitación www	0	0	0	0	0	0
[S_info] normativa	0	0	0	0	0	0
[S_news] noticias	0	0	0	0	0	0
[S_control_acceso] control de acceso	0	0	500	1.000	3.500	7.500
[D_expedientes] expedientes en curso	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[D_info] normativa	0	0	0	0	0	0
[D_news] noticias	0	0	0	0	0	0
[SI] servicios internos						
[E] equipamiento						
[SW_tramitación] tramitación de expedientes	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[SW_acceso] aplicación de control de acceso	0	0	500	1.000	3.500	7.500
[SW_DBMS] gestor de bases de datos	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[SI_internet] Internet	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[HW_PC] puestos de usuario	10.000	20.000	51.000	51.000	1.000.000	1.010.000
[SRV_01] servidor de ficheros	10.000	20.000	51.000	51.000	1.000.000	1.010.000
[SRV_02] servidor de bases de datos	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[SRV_03] servidor www	0	0	0	0	0	0
[HW_print] impresoras	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[HW_firewall] cortafuegos	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[HW_electronica] electrónica de comunicaciones	10.000	20.000	51.000	51.000	1.000.000	1.010.000
[HW_dsf] dispositivo seguro de firma	0	0	0	0	0	0
[SI_papel] documentación en papel	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[COM_LAN] red local	10.000	20.000	51.000	51.000	1.000.000	1.010.000
[COM_ADSL] línea adsl	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[COM_RDSI] línea de backup	10.000	20.000	50.000	50.000	1.000.000	1.000.000
[L] instalaciones						
[P] personas						

2 propio exporta

En la figura puede apreciarse una valoración económica del servicio de tramitación presencial en la que aparece un fuerte incremento al séptimo día, intentando simular una hipotética sanción administrativa. También aparece un coste lineal en el servicio de control de acceso, que intenta simular la necesidad de contratar a una persona para cubrir la carencia de los sistemas de control.

Para estimar el coste económico de una interrupción hay que tener en cuenta la merma de beneficios y el incremento de costes derivados de la interrupción. La diferencia entre los valores normales (sin interrupción) y los valores en caso de interrupción es la medida del daño causado por la interrupción.

En el caso cuantitativo, lo activos que son necesarios para prestar varios servicios suman los costes derivados de su interrupción pues ahora causan un daño múltiple, acumulativo.

4. Amenazas

Identificados los activos corresponde analizar a qué amenazas están expuestos, amenazas que pudieran provocar su detención temporal o su destrucción permanente. Típicamente se consideran accidentes o desastres naturales o industriales (desde averías que requieren una reparación, hasta incendios que requieran otro equipo). También hay que considerar errores humanos (tales como errores en la planificación de capacidades o en la configuración de los sistemas) y ataques (tales como los de denegación de servicio). Este conjunto de amenazas hay que cotejarlo con el tipo de activos que tengamos y estimar cuán vulnera-

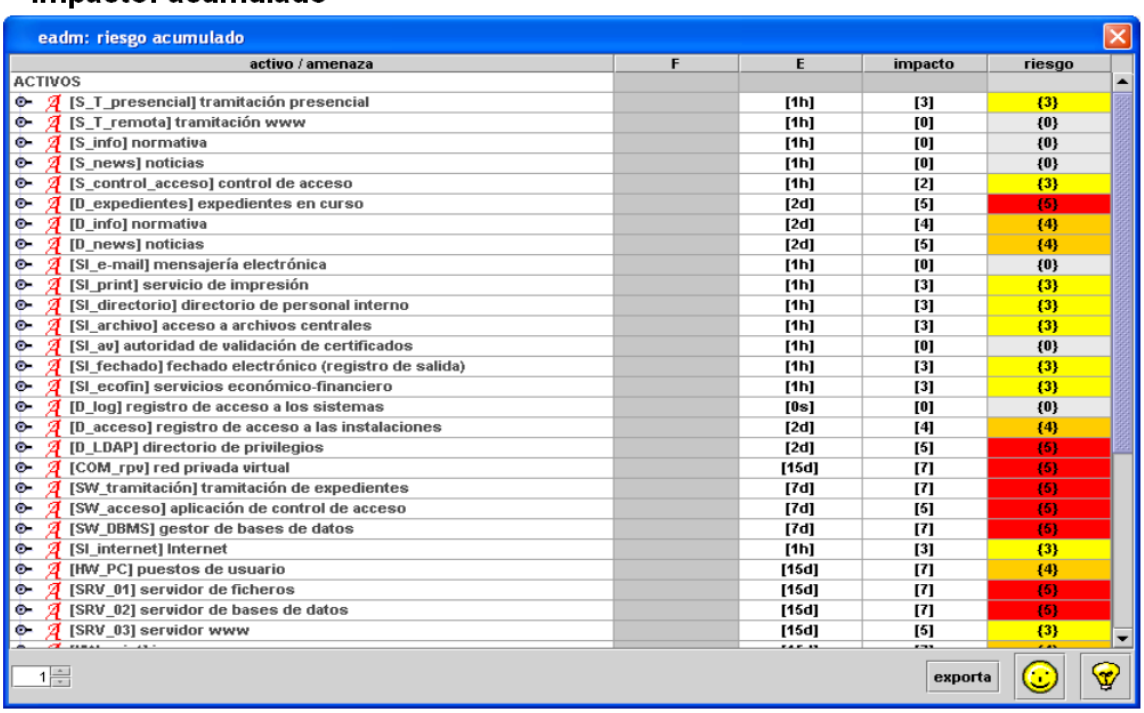
bles son y cómo de contundentes serían las consecuencias de la materialización de la amenaza.

De todo ello se podrá derivar un mapa de riesgos que informa de qué puede pasar a qué, qué posibilidades hay de que pase y cuáles serían las consecuencias.

5. Estado de riesgo potencial

Todo lo anterior nos proporciona una estimación del estado de riesgo que nos indica los activos críticos (en términos intangibles) y de consecuencias económicas más graves (en términos económicos).

Impacto: acumulado



activo / amenaza	F	E	impacto	riesgo
ACTIVOS				
[S_T_presencial] tramitación presencial		[1h]	[3]	{3}
[S_T_remota] tramitación www		[1h]	[0]	{0}
[S_info] normativa		[1h]	[0]	{0}
[S_news] noticias		[1h]	[0]	{0}
[S_control_acceso] control de acceso		[1h]	[2]	{3}
[D_expedientes] expedientes en curso		[2d]	[5]	{5}
[D_info] normativa		[2d]	[4]	{4}
[D_news] noticias		[2d]	[5]	{4}
[SI_e-mail] mensajería electrónica		[1h]	[0]	{0}
[SI_print] servicio de impresión		[1h]	[3]	{3}
[SI_directorio] directorio de personal interno		[1h]	[3]	{3}
[SI_archivo] acceso a archivos centrales		[1h]	[3]	{3}
[SI_av] autoridad de validación de certificados		[1h]	[0]	{0}
[SI_fechado] fechado electrónico (registro de salida)		[1h]	[3]	{3}
[SI_ecofin] servicios económico-financiero		[1h]	[3]	{3}
[D_log] registro de acceso a los sistemas		[0s]	[0]	{0}
[D_acceso] registro de acceso a las instalaciones		[2d]	[4]	{4}
[D_LDAP] directorio de privilegios		[2d]	[5]	{5}
[COM_rpv] red privada virtual		[15d]	[7]	{5}
[SW_tramitación] tramitación de expedientes		[7d]	[7]	{5}
[SW_acceso] aplicación de control de acceso		[7d]	[5]	{5}
[SW_DBMS] gestor de bases de datos		[7d]	[7]	{5}
[SI_internet] Internet		[1h]	[3]	{3}
[HW_PC] puestos de usuario		[15d]	[7]	{4}
[SRV_01] servidor de ficheros		[15d]	[7]	{5}
[SRV_02] servidor de bases de datos		[15d]	[7]	{5}
[SRV_03] servidor www		[15d]	[5]	{3}

6. Elementos de respaldo

Conociendo los requisitos de disponibilidad sobre los activos es posible tomar decisiones para limitar el daño; es decir, decisiones que pongan un límite a la posible interrupción. Esto suele costar un dinero (en adquisiciones, mantenimiento, personas dedicadas a mantener el sistema de respaldo en perfectas condiciones de ser usado, etc.) pero es efectivo para limitar el daño. En términos económicos es obvio que no deberíamos gastar en equipamiento de respaldo más dinero del que costaría la inhabilitación para el servicio del equipo respaldado. En términos intangibles, la decisión no es económica sino gerencial y debe tomarse en cuanta valorando si la inversión es prudente para las consecuencias estimadas.

Los elementos de respaldo son diferentes según el tipo de activo, pues en general son de la misma naturaleza. La prontitud con la que un respaldo entra en servicio depende de si es propio, contratado o acordado, teniendo en consideración las distancias físicas y la disponibilidad del personal que lleva a cambio la sustitución. En el caso ideal los equipos están permanentemente disponibles y la sustitución es automática.

7. Salvaguardas

Además de disponer de los medios hay que tener en cuenta

- todos los aspectos de gestión pertinentes:
    - planes procedimentados que permitan actuar según lo previsto
    - acuerdos de prestación de servicios alternativos
    - planificación de capacidades
- los mecanismos de detección de incidencias
- los sistemas automáticos de activación de elementos de respaldo

8. Estado de riesgo residual

Con todo ello podremos disponer de un estado de riesgo residual que nos indica la situación efectiva de riesgo. El impacto no podrá ser menor que el correspondiente al tiempo de entrada en funcionamiento del equipamiento alternativo; pero si no funcionan adecuadamente las salvaguardas, este tipo puede ser "meramente teórico", convirtiéndose en la práctica en un daño muy superior.

El estado de riesgo matiza cual es el activo dañado. Por ejemplo, si disponemos de un cluster como soporte informático, la detención de un procesador se subsana en un tiempo mínimo; pero no tiene ningún efecto si todos los elementos del cluster se encuentra en el mismo CPD y este arde. Igualmente, disponer de un centro alternativo en 24horas puede ser inútil si los equipos destruidos no pueden reponerse hasta pasados 7 días.

El estado de riesgo residual identifica dónde puede pasar qué, permitiendo bien asumir el riesgo, bien traspasarlo (por ejemplo mediante un seguro), bien lanzar un programa de mejoras encaminado a reducir el riesgo residual a mejores cotas.

9. Plan de recuperación de desastres

En caso de desastre, o incidente mayor que destruye el equipamiento o lo deja inservible a todos los efectos prácticos, se requiere un plan de recuperación en algún centro alternativo. El plan de recuperación, en lo que afecta al sistema de información, no es sino un plan de reconstrucción que

1. comienza disponiendo de un centro alternativo,

2. continua instalando infraestructura básica,

3. instala y configura equipos y comunicaciones

4. instala y configura aplicaciones

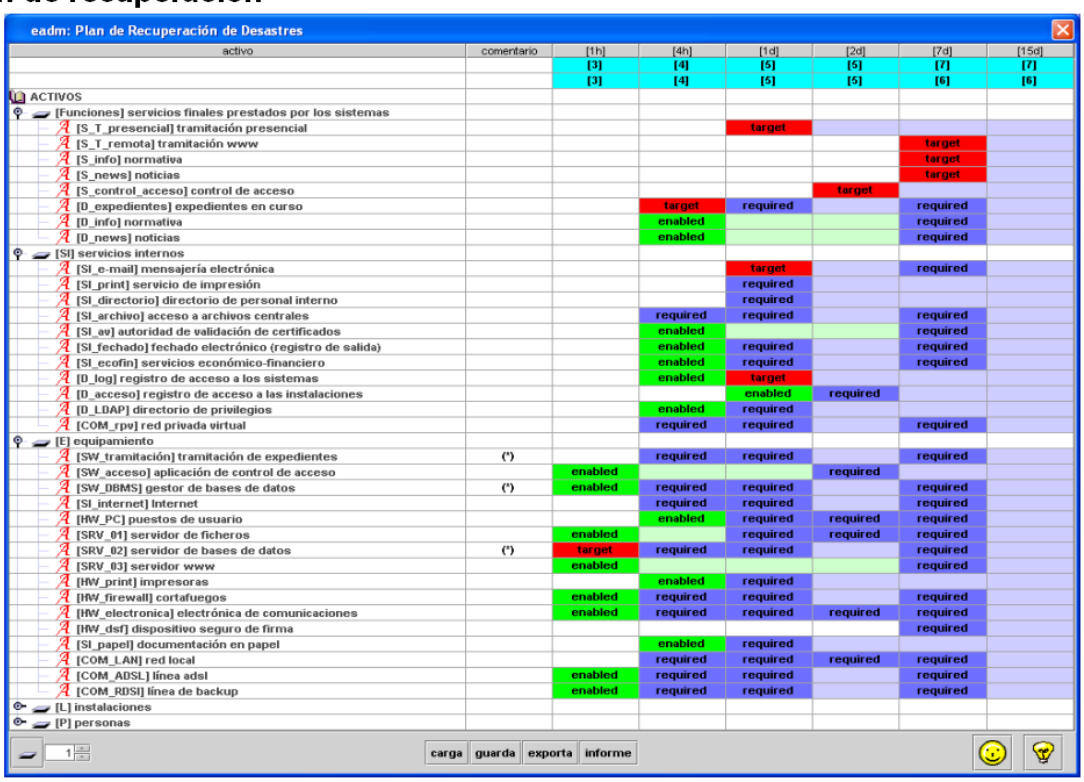
5.recupera datos (configuración, cuentas e información)

6. y, por último, reanuda el servicio en las nuevas instalaciones

Son muchas actividades que requieren un plan meticuloso que involucra a muchas partes. Las diferentes tareas se pueden anticipar en el tiempo a la ocurrencia del desastre, o iniciarse cuando ocurre. La diferencia es tiempo y, a través del análisis de impactos, daños materiales e inmateriales. En los casos más críticos se opta por centros espejo en los que todos los equipos están permanentemente dispuestos y los datos se mantienen continuamente al día. Esto es caro por lo que a menudo se opta por soluciones manuales, desde

centros calientes (preparados y equipados, listos para pasar directamente al punto 5) hasta centros fríos (preparados para empezar directamente con el punto 3).

Plan de recuperación



activo	comentario	[1h]	[4h]	[1d]	[2d]	[7d]	[15d]
		[3]	[4]	[5]	[5]	[7]	[7]
		[3]	[4]	[5]	[5]	[6]	[6]
ACTIVOS							
[Funciones] servicios finales prestados por los sistemas							
[S_T_presencial] tramitación presencial				target			
[S_T_remota] tramitación www						target	
[S_info] normativa						target	
[S_news] noticias						target	
[S_control_acceso] control de acceso					target		
[D_expedientes] expedientes en curso			target	required		required	
[D_info] normativa			enabled			required	
[D_news] noticias			enabled			required	
[SI] servicios internos							
[SI_e-mail] mensajería electrónica				target		required	
[SI_print] servicio de impresión				required			
[SI_directorio] directorio de personal interno				required			
[SI_archivo] acceso a archivos centrales			required	required		required	
[SI_av] autoridad de validación de certificados			enabled			required	
[SI_fechado] fechado electrónico (registro de salida)			enabled	required		required	
[SI_ecofin] servicios económico-financiero			enabled	required		required	
[D_log] registro de acceso a los sistemas			enabled	target			
[D_acceso] registro de acceso a las instalaciones				enabled	required		
[D_LDAP] directorio de privilegios			enabled	required			
[COM_rpv] red privada virtual			required	required		required	
[E] equipamiento							
[SW_tramitación] tramitación de expedientes	(*)		required	required		required	
[SW_acceso] aplicación de control de acceso		enabled			required		
[SW_DBMS] gestor de bases de datos	(*)	enabled	required	required		required	
[SI_internet] Internet			required	required		required	
[HW_PC] puestos de usuario			enabled	required	required	required	
[SRV_01] servidor de ficheros		enabled		required	required	required	
[SRV_02] servidor de bases de datos	(*)	target	required	required		required	
[SRV_03] servidor www		enabled				required	
[HW_print] impresoras			enabled	required			
[HW_firewall] cortafuegos		enabled	required	required		required	
[HW_electronica] electrónica de comunicaciones		enabled	required	required	required	required	
[HW_dsf] dispositivo seguro de firma						required	
[SI_papel] documentación en papel			enabled	required			
[COM_LAN] red local			required	required	required	required	
[COM_ADSL] línea adsl		enabled	required	required		required	
[COM_RDSI] línea de backup		enabled	required	required		required	
[L] instalaciones							
[P] personas							

La herramienta PILAR nos ayudará en la planificación de cómo recuperarnos de un desastre (1) permitiendo marcarnos objetivos de recuperación (por ejemplo, servicios críticos), (2) indicándonos los elementos que son necesarios para alcanzar el objetivo propuesto y (3) mostrando los activos que quedan habilitados para proceder al siguiente objetivo de recuperación.

El plan de recuperación se materializa en una serie de tareas que llevan su tiempo. Por tanto, al tiempo que se tarde en tomar la decisión de activar el plan de recuperación hay que sumarle el tiempo que requiera llevar las tareas prescritas a buen término y re-habilitar los servicios. La suma de estos tiempos nos indica dónde frenamos el impacto. Si la dirección no lo admite, habrá que activarse antes u optimizar las tareas necesarias (por ejemplo, ejecutándolas antes de que se de la situación de emergencia).

10. Conclusiones

A lo largo de las páginas anteriores se ha cubierto someramente la problemática de cómo mantener los servicios operativos y los datos disponibles, centrándonos en los aspectos más técnicos, sin por ello despreciar los muy laboriosos aspectos de gestión asociados.

Se ha mostrado como la herramienta PILAR, inicialmente diseñada para el análisis y gestión de riesgos, puede aplicarse para

1. modelar el coste (monetario e intangible) de una interrupción del servicio,

2. identificar elementos críticos del sistema de información,
3. determinar qué equipo de respaldo es adecuado ,
4. evaluar las salvaguardas que complementan el equipamiento de respaldo,
5. estimar el riesgo residual remanente tras el despliegue del equipamiento de respaldo tomando en consideración las salvaguardas desplegadas y su eficacia y
6. diseñar un plan de recuperación en caso de desastre.