# Metodologías para el diseño de sistemas de información

PID_00250488

Joan Antoni Pastor Collado
Eduard Elias Vila

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

# Índice

# Introducción

Dada la relevancia que tiene el sistema de información, tanto en la gestión diaria de la organización como en la toma de decisiones por parte de su equipo directivo, es fundamental que reúna dos condiciones indispensables: que sea correcto y que esté correcto.

- *que sea correcto*: es decir, que la información que contiene realmente represente de forma correcta la realidad, sin distorsiones. Solo eso permitirá, a los gestores del día a día, ejecutar las acciones correctas, que respondan de forma correcta a los problemas reales a los que se enfrente la organización y, al equipo directivo, tomar las decisiones correctas para el futuro de la organización.

- *que esté correcto*: es decir, que cada vez que se produzcan actos relevantes para la organización, desde las pequeñas gestiones del día a día hasta grandes cambios en el entorno, se vean correctamente reflejadas en el SI para seguir representando la realidad.

La primera característica se refiere más a la estructura del SI, a asegurar que prevea los mecanismos de recogida, incorporación, mantenimiento y explotación de la información realmente relevante y toda la información relevante para la organización.

**Ejemplos de SI incompletos o redundantes**

En el pasado, la informática entró en la mayoría de las empresas por el departamento de contabilidad. Imaginemos, por ejemplo, una empresa puramente comercial que almacenara y comercializara productos sin manipularlos. Supongamos que esta empresa informatizara la emisión, recepción, cobro y pago de todas sus facturas, pero no registrara la entrada y salida de productos de su almacén, ni los que aparecieran en sus facturas recibidas y emitidas, y mantuviera esta información en albaranes de almacén, o sea, en papel.

Su SI informático no representaría de forma correcta la realidad de esa empresa, ni permitiría tomar decisiones muy importantes, como el mantenimiento de existencias en su almacén. Solo se podría considerar que esa empresa tiene un SI correcto si se considerara en su conjunto, como SI parcialmente informatizado, contando tanto las facturas gestionadas informáticamente como los albaranes gestionados en papel.

En el otro extremo, el SI de una empresa con un gestor obsesivo que forzara a sus empleados a registrar a qué dedican cada minuto de su tiempo, incluyendo las pausas necesarias para ir al lavabo o para fumar o incluso cuando se distrajeran por cualquier motivo, muy probablemente, acabaría lleno de un montón de información totalmente irrelevante, que no sería útil para tomar ninguna decisión relevante.

El correcto diseño de un SI requiere una labor previa de identificar qué información es realmente importante para la organización. Bajando al detalle, qué datos son necesarios y qué relaciones se dan entre ellos para conocer el estado real de la organización y de su entorno, para poder gestionarla y guiarla acertadamente hacia la consecución de sus objetivos.

La segunda característica, que el SI esté correcto, se refiere más a los procedimientos establecidos en el seno de la organización para mantener la vigencia de los datos contenidos en el SI, para que siga reflejando la realidad de la organización y de su entorno, sin perder datos relevantes o introducir distorsiones (datos incorrectos o ficticios) en el SI. Un análisis bien dirigido de estos procedimientos mejorará la eficacia y la eficiencia de la organización.

# Objetivos

En los materiales incluidos en este módulo, el estudiante encontrará las herramientas básicas para lograr los siguientes objetivos:

1. Conocer las etapas del proceso de análisis para identificar lo que una organización determinada necesita de su SI.

2. Comprender los objetivos y los pasos que conducen a un buen diseño y planificación de un SI.

3. Saber identificar con claridad las responsabilidades de cada parte implicada en la construcción de un SI.

4. Conocer las dos estrategias más extendidas para conseguir la preservación de la privacidad: **la privacidad por el diseño** (en inglés *privacy by design*, PbD), como estrategia *a priori*, y **la evaluación del impacto de la privacidad** (en inglés *privacy impact assessment*, PIA), cuando el SI ya está operativo.

5. Ligado al PIA, comprender cómo se lleva a cabo y qué supone la **gestión de riesgos**.

# 1. Fundamentos de diseño de SI

El diseño de todo SI empieza por una fase de análisis.

**Análisis** es el proceso de clasificación e interpretación de los hechos que afectan a la organización, el diagnóstico de problemas y el empleo de la información disponible para recomendar mejoras de todo orden (procedimientos, etc.).

**Diseño** es la plasmación de las conclusiones del análisis en la especificación de las características que debe tener el nuevo sistema.

En el caso concreto del SI de una organización, esos dos procesos, análisis y diseño, se refieren a examinar la situación de la organización en relación con su SI, con el propósito de mejorar tanto la eficiencia como la eficacia de esta.

Muchos autores han estudiado las actividades que se llevan a cabo durante el análisis y se suelen distinguir las siguientes cinco etapas:

**1)** Reconocimiento del problema: identificar dónde están las ineficiencias o ineficacias de la organización que se pueden mejorar y en qué está fallando el SI actual para que se produzcan.

**2)** Evaluación y síntesis: recoger datos sobre el problema, valorarlos y considerar alternativas, valorarlas (desde el punto de vista técnico, económico, legal, etc.) y elegir la o las alternativas más plausibles, para acabar eligiendo la más conveniente.

**3)** Modelado: definición y delimitación de la solución elegida.

**4)** Especificación: redacción, lo más exhaustiva que sea posible y razonable, de todas las características que debe reunir la solución.

**5)** Revisión: revisión exhaustiva de la corrección de todos los supuestos y decisiones por parte de todas las partes que se vayan a ver afectadas por los cambios que se introducirán.

El objetivo final del análisis debería prever reflejar todo este proceso:

**a)** Identificación del problema y objetivos de la solución: sería el resultado de la primera etapa.

**b)** Estudio de viabilidad: resultado de la segunda etapa. Debería incluir:

- Viabilidad económica: tomando en cuenta tanto los costes de planificación, desarrollo, implantación y mantenimiento como la comparación de estos con los ingresos o beneficios que vaya a suponer la modificación del SI.

- Viabilidad técnica: consideración de todos los condicionantes técnicos, teniendo en cuenta tanto los medios disponibles como las posibilidades que ofrece la tecnología del momento.

- Viabilidad legal: también hay que tener en cuenta las repercusiones legales que pueda tener el uso y tratamiento de la información que vaya a contener el SI. Por ejemplo, el uso de datos de carácter personal o la gestión de secretos industriales, etc.

**c)** Especificación: resultado de las etapas de modelado y especificación.

**d)** Resultados de la revisión: se debería hacer constar la revisión y aprobación por parte de todas las partes que se van a ver afectadas.

Vistos estos rudimentos sobre el proceso de análisis y diseño de un SI (o de rediseño de uno ya existente), vamos a considerar un par de metodologías que hacen hincapié en una cuestión fundamental: la privacidad.

## 2. Privacidad por el diseño (*privacy by design*, PbD)

La privacidad por el diseño (en inglés, *privacy by design*, PbD) es una iniciativa sobre el diseño de sistemas de información que apareció por primera vez en un artículo publicado en 1995 por el Comisionado para la Información y la Privacidad de Ontario (Canadá), la Autoridad de Protección de Datos de Holanda y la Organización Holandesa para la Investigación Científica Aplicada.

Se trata de un claro ejemplo de lo que se conoce como diseño sensible a valores, que persigue, en este caso, el más escrupuloso respeto por la privacidad de los datos personales de todos los ciudadanos a escala global. Se basa en la observancia de los siguientes siete principios fundacionales:

Los siete principios fundacionales del PbD

**1)** Proactivo, no reactivo; preventivo, no correctivo

**2)** Privacidad como configuración por defecto

**3)** Privacidad incorporada en el diseño

**4)** Funcionalidad completa – de suma positiva, no de suma cero

**5)** Seguridad de extremo a extremo – protección de todo el ciclo de vida

**6)** Visibilidad y transparencia – mantenerlo abierto

**7)** Respeto por la privacidad del usuario – mantenerlo centrado en el usuario

Vamos a ver qué significan estos principios enunciados de forma tan lapidaria:

**1) Proactivo, no reactivo; preventivo, no correctivo** (en inglés, *proactive not reactive; preventative not remedial*)

La idea es conseguir que se diseñe todo el SI procurando anticipar y prevenir cualquier posibilidad de actos que invadan o puedan invadir la privacidad. No esperar a que se materialicen riesgos de privacidad y ofrecer remedios, sino prevenir que eso ocurra. O sea PdD está antes de los hechos, no después.

**2) Privacidad como configuración por defecto** (en inglés, *privacy as the default setting*)

Con este principio se persigue que, en cualquier situación en la que el usuario pueda elegir entre opciones que signifiquen distintos niveles de privacidad, el sistema venga siempre preconfigurado con la más restrictiva por defecto. De este modo, el usuario no tiene que hacer nada para preservar su privacidad.

En un escrito publicado por Ann Cavoukian, comisionada para la Información y la Privacidad de Ontario, esta especifica un poco más en este apartado y llega a concretar unos principios que guardan similitudes con los que establece la legislación europea en materia de protección de datos:

- **Finalidad específica**: el fin con el que se recogen datos del usuario tiene que estar claro y debe entenderse en sentido limitativo.

- **Limitación en la recogida**: la recogida de información personal debe ser justa, limitada a lo estrictamente necesario para la finalidad indicada y acorde con la legalidad.

- **Minimización de datos**: los datos personales deben reducirse al mínimo imprescindible.

- **Limitación en el uso, conservación y revelación**: estas tres operaciones se deben limitar a lo estrictamente necesario para la finalidad indicada.

**3) Privacidad incorporada en el diseño** (en inglés, *privacy embedded into design*)

Se pretende que la privacidad no sea un añadido posterior que se aplica sobre el producto ya terminado, sino algo incorporado en el mismo núcleo del diseño, sin disminuir la funcionalidad. Ello implica que la privacidad debe ser embebida en la tecnología, operación y arquitectura del SI de una manera global, integradora y creativa: *global*, ya que hay que considerar la privacidad en los contextos más amplios posibles; *integradora*, ya que todas las partes interesadas deben ser consideradas, y *creativa*, ya que incorporar privacidad algunas veces significa reinventar las opciones existentes, porque estas son inaceptables.

**4) Funcionalidad completa – de suma positiva, no de suma cero** (en inglés, *full functionality – positive-sum, not zero-sum*)

El enunciado de este principio considera falsas dicotomías como la que se suele pretender entre privacidad y seguridad. Se pretende evitar cualquier tipo de mercadeo compensatorio, y se busca obtener ambas cosas: privacidad ***y*** seguridad, no ***o***.

**5) Seguridad de extremo a extremo – protección de todo el ciclo de vida** (en inglés, *end-to-end security – full lifecycle protection*)

La seguridad de cada dato se debe mantener durante todo su ciclo de vida: desde su recogida hasta su destrucción, pasando por todas las operaciones en las que pueda intervenir. Este principio de seguridad tiene relevancia capital, ya que, en su esencia, sin una fuerte seguridad, no puede haber ninguna privacidad.

**6) Visibilidad y transparencia – mantenerlo abierto** (en inglés, *visibility and transparency – keep it open*)

Todas las partes implicadas deben operar de acuerdo con sus promesas y objetivos declarados y deben estar sujetas a verificación independiente, es decir, auditoría por terceros. Todos los componentes y operaciones deben quedar visibles y transparentes, tanto para los usuarios como para los proveedores. Confianza sí, ¡pero con verificación!

**7) Respeto por la privacidad del usuario – mantenerlo centrado en el usuario** (en inglés, *respect for user privacy – keep it user-centric*)

Según este último principio, el foco, durante todo el diseño, se debe mantener en el interés del usuario individual, y ofrecer medidas como estándares elevados de privacidad, avisos apropiados y preferir las opciones amigables con el usuario (*user-friendly*).

Esta filosofía de diseño, más que una metodología, ha sido adoptada por varios organismos internacionales, entre los que, en algún grado, se cuenta incluso la Unión Europea.

Sin embargo, también tiene detractores. Se le achaca el hecho de reducirse a puros principios muy vagos y, por lo tanto, asemejarse mucho más a un código de buenas prácticas o de autorregulación que a una norma.

Recordemos que la legislación europea aún vigente (la directiva 95/46/CE) es del 24 de octubre del mismo año 1995 y, curiosamente, España, habitualmente más reactiva que proactiva, había legislado sobre la materia en el año 1992 (Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal). Es decir, no fue una iniciativa innovadora ni tan siquiera una verdadera regulación, pero sí hay que admitirle que ayudó a hacer internacional una cuestión que amenazaba con quedarse solo en el ámbito europeo, y de hecho la importancia de los principios de PbD han quedado reflejados en los artículos 22 y 23 del Reglamento Europeo de Protección de Datos publicado en mayo de 2016 y que los países europeos deberán adoptar inexcusablemente a partir de mayo de 2018 (con lo que se deroga a partir de esta fecha la 95/46/CE). Sin embargo, y a pesar de ello, en muchos países, PbD sigue siendo la única referencia en materia de privacidad.

## 3. Evaluación del impacto de la privacidad (*privacy impact assessment*, PIA)

Con esta denominación inglesa se conoce lo que, de acuerdo con las prácticas de nuestro país, podríamos llamar una auditoría de privacidad. Responde a un movimiento que se orienta, principalmente, a los grandes tenedores de datos personales, los estados y las grandes corporaciones, y lo que pretende es que se detecte cualquier posible riesgo en la gestión de estos datos.

Cuando una organización se plantea una evaluación (o auditoría, como hemos dicho) de este tipo, persigue tres objetivos:

- Asegurar el cumplimiento de todos los requisitos exigibles (legales o de cualquier otro tipo) en materia de privacidad.

- Identificar cualquier posible riesgo y sus posibles efectos en caso de producirse.

- Plantear medidas de protección o alternativas que reduzcan esos riesgos potenciales.

Los dos últimos responden a lo que se conoce como gestión de riesgos.

Genéricamente, la gestión de riesgos es un proceso que empieza por evaluar cada riesgo como una amenaza (algo que puede suceder y que podría causar daños a la organización) que tiene una determinada probabilidad de producirse y que tendría unas consecuencias que, normalmente, se valoran económicamente, como un perjuicio o daño.

Así, se construye una tabla con las siguientes columnas:

Amenaza Probabilidad Perjuicio Valoración

Donde la valoración se calcula, simplemente, como el producto de la probabilidad (expresada en *tanto por 1*) por el perjuicio. La tabla se ordena por esta columna, de mayor a menor. El total de esta columna es, teóricamente, el riesgo potencial total al que está expuesta la organización.

A partir de esta tabla y priorizando los riesgos más graves, es decir, los que quedan en la parte superior de la tabla, se estudian medidas que reduzcan o bien la probabilidad o bien los posibles perjuicios (o, si es posible, ambos, claro).

Se considera que una medida vale la pena si el coste de llevarla a cabo es inferior a la reducción de valoración del riesgo que consigue (o riesgos; una misma medida puede mejorar varios riesgos). En caso contrario, puede salir más a cuenta, simplemente, tomar un seguro que cubra esa eventualidad o, si la valoración es realmente muy baja, ese riesgo puede ser asumido por la organización.

**Nota**

Cuantificar los perjuicios no es fácil, especialmente cuando se llega a intangibles como la reputación, la credibilidad o la confianza.

Entre los beneficios de llevar a cabo una auditoría de privacidad, se cuenta el hecho de actuar *a priori* en lugar de cuando ya se ha producido un problema de privacidad, lo cual evita los costes o la mala imagen de tener que resolver un problema de este tipo, permite demostrar que la organización ha intentado evitarlo y orienta las decisiones en esta materia.

Los más partidarios incluso la presentan como una forma de ganar credibilidad y buena reputación, tanto ante el público en general como ante los propios empleados, proveedores y clientes. La tentación, para directivos sin escrúpulos, está en centrarse solo en este aspecto y realizar una evaluación PIA poniendo más énfasis en que se sepa que se está haciendo que en los resultados. Es cuando se dice que se pasa de la ética a la «cosm-ética».

Hay que recordar que, precisamente, si se hace una evaluación de esta naturaleza y luego sucede algo que debería haber sido detectado y prevenido, la responsabilidad será del evaluador, concretamente, de quien firme el informe

final que no recomendara nada al respecto. Si hubiera recomendaciones y no hubieran sido tomadas en consideración, entonces la responsabilidad sería del que hubiera tomado esa decisión.

Una práctica habitual en muchos tipos de auditoría, no solo este, es que el evaluador utilice baterías de preguntas o formularios «estándares» establecidos por organizaciones de reconocido prestigio y que haga constar que se le ordena que use esos cuestionarios y nada más. Es una forma de limitar sus responsabilidades. Si sucede algo que no estuviera previsto en el cuestionario, «la culpa» sería de quien hubiera tomado la decisión de usar esos cuestionarios o, incluso, subsidiariamente, de la organización que los hubiera publicado.

La ejecución de una auditoría tipo PIA se concreta en cuatro etapas:

**1) Objetivos**: en este paso se define el alcance del proceso de evaluación de riesgos de privacidad. En algunos casos, por ejemplo cuando la organización no ha hecho este proceso nunca antes y no puede valorar el alcance que debe plantearse, se puede hacer un piloto preliminar, por ejemplo en un departamento o bien centrándose en algún aspecto concreto.

**2) Análisis** de flujos de datos: en este paso se analizan los distintos grupos de datos personales que pasan por la organización en algún momento y todo el flujo de cómo circulan por ella. Esta información se puede plasmar en un diagrama de flujos de datos.

**3) Análisis de la privacidad**: en esta fase se pasan cuestionarios a todo el personal involucrado en la gestión de los flujos anteriores e, incluso, si hace falta se complementan con entrevistas o reuniones de grupo, para discutir los aspectos más controvertidos o dudosos que hayan aparecido en los cuestionarios.

**4) Informe final**: en el informe resultante, que puede llevar como anexos todos los documentos anteriores, es donde se lleva a cabo el análisis y gestión de riesgos, a partir de todas las amenazas que se hayan detectado en la fase 3.

Es decir, un procedimiento muy similar a auditorías sobre cuestiones en las que la intervención humana tenga un impacto relevante.

# 4. Responsabilidades alrededor de un SI

Como se ha visto en este módulo, así como en los precedentes, la planificación y desarrollo de un SI de una cierta dimensión, incluso solo su mantenimiento diario, es una obra muy «coral», en la que intervienen muchas personas, departamentos y niveles de responsabilidad en la organización muy diferentes. Es habitual que, por lo menos en la planificación y desarrollo de un SI nuevo o en una revisión a fondo, se contrate una empresa de servicios informáticos experta en este ámbito. O sea, que incluso interviene personal externo.

Este es el caldo de cultivo ideal para que, en caso de que suceda algo no previsto y tenga consecuencias negativas, todas las partes implicadas empiecen a achacar responsabilidades a las demás y se acabe convirtiendo en un desagradable espectáculo de cruce de acusaciones, donde nadie entone ningún *mea culpa*, sino más bien «yo no he sido». Esto puede envenenarse especialmente cuando, como hemos comentado que es habitual, hay implicada una empresa especializada contratada, aparte de la propia organización.

Conviene, pues, delimitar de forma lo más clara posible a quién corresponde la responsabilidad de cada paso. Vamos a ver, en el caso del análisis y diseño, el reparto de responsabilidades en las fases que hemos visto en el primer apartado de este módulo. En cada caso, cuando se hable de consultores externos, de una hipotética empresa contratada para proveerlos, si no la hubiera, se deberá entender que el texto se refiere al personal informático de la propia organización, que ejerce esa función.

## 4.1. Análisis y diseño de un nuevo SI (o de la revisión del existente)

- **Reconocimiento del problema**: Es evidente que, aunque un buen consultor con experiencia en casos similares pueda ayudar y mucho, quien conoce su actividad o su negocio es la organización que contrata el desarrollo del nuevo SI. Normalmente, cuando la dirección de una organización decide emprender el desarrollo de un nuevo SI ya es porque ha identificado la existencia de algún problema en el que está usando. La consultoría externa puede ayudar aportando buenas prácticas al proceso, pero la iniciativa, el liderazgo y la toma de todas las medidas necesarias para atraer a toda la organización a colaborar en esta primera tarea corresponde a la dirección de la organización.

- **Evaluación y síntesis**: El proceso de recogida exhaustiva de toda la información necesaria para considerar todas las posibilidades y priorizarlas o descartarlas corresponde a la consultoría. Pero, mayoritariamente, la información se recoge por medio de entrevistas al personal más relevante

para el caso. Si no se han establecido, por parte de la dirección, las medidas oportunas para facilitar la colaboración de este personal, esto puede llevar el proyecto al fracaso.

- **Modelado y especificación**: Con toda claridad, estas dos etapas son responsabilidad prácticamente exclusiva de la consultoría, que deberá definir el problema, a partir de toda la información recogida, y redactar la especificación, es decir, la descripción, lo más clara y detallada posible, del sistema que se va a crear. Haciendo un símil, por otro lado muy habitual, con el sector de la construcción, las especificaciones son los planos del nuevo edificio. Y, lógicamente, son responsabilidad del «arquitecto», o sea, de la consultoría.

- **Revisión**: Este es el punto donde se producen más malentendidos entre las partes. La revisión de las especificaciones hechas por los consultores solo la puede hacer la dirección y el personal de la organización. Es muy frecuente que, cuando una organización encarga el desarrollo de su SI a una consultora externa, no entienda que la especificación no es «un documento técnico» del que solo la consultora se tenga que ocupar. Es la sucinta descripción de lo que se va a construir. Solo la dirección y el personal relevante de la organización pueden saber si realmente responde a sus necesidades o no. Muchos proyectos fracasan por desacuerdos entre la organización y la consultoría en fases de construcción del SI mucho más adelantadas, por cuestiones que estaban en la especificación y que no fueron revisadas en su momento por la organización. La especificación debería tratarse como un contrato, se debería firmar y, como se hace con todo aquello que se firma, debería ser concienzudamente revisado y verificado.

### 4.2. Construcción del SI

Tras estas etapas, que eran las de análisis y diseño, viene la construcción del SI propiamente dicho. Eso será responsabilidad exclusiva del equipo técnico. Únicamente, cada vez que este personal haga entrega de algún hito del proyecto (módulos individualizados, prototipos, etc.) será responsabilidad de la organización probarlos como es debido. La falta de prueba facilita la no detección de problemas que acabarán apareciendo más tarde, en ocasiones mucho más tarde, y eso conllevará problemas.

Es importante destacar que, cuanto más se tarde en detectar la más mínima disparidad de criterios sobre lo que se debe construir, más difícil será reconducir la situación. Volviendo al símil de la construcción, si las partes no han dejado claro si el edificio que se va a construir es de tres o de cinco plantas, si se dan cuenta antes de empezar los cimientos, se podrá construir directamen-

te con la altura correcta. Si no se dan cuenta hasta que los albañiles ya van por la segunda planta, es probable que haya que rehacer cimientos, reforzar columnas y estructuras de los primeros pisos para soportar más peso, etc.

También en la construcción de un SI, modificaciones del proyecto fruto de una negociación para resolver conflictos de interpretación cuando el proyecto ya había completado varias etapas obligarán, no solo a replantear el trabajo que quede, sino, y ahí está la dificultad, a revisar todo el trabajo ya hecho.

La detección tardía hace que reconducir el proyecto a lo que debería ser resulte más compleja y laboriosa. Evidentemente, volviendo al símil, es más fácil construir directamente un edificio de cinco plantas que empezarlo de tres y, cuando ya se llevan dos construidas, tener que reforzar todas las estructuras para acabarlo de cinco.

Evitar que esta situación se dé o detectarla cuanto antes es una responsabilidad compartida que, por su experiencia, debería ser explicitada y recordada por la consultoría. La fluidez del diálogo entre las partes es fundamental para la buena marcha del proyecto.

### 4.3. Alternativa: paquete estándar

Las fases indicadas para el análisis y diseño del sistema serían las mismas en el caso de elegir un paquete estándar, en lugar de hacer un desarrollo a medida. La única diferencia estaría en el documento de especificaciones, que, en lugar de contener la descripción de todo un nuevo sistema, se podría limitar a indicar todas las configuraciones y adaptaciones que requeriría el estándar para adaptarse a las necesidades detectadas en las fases anteriores.

Atención con pensar que por el hecho de elegir un estándar el proceso va a ser más fácil. Esos estándares vienen preconfigurados para una organización, habitualmente una empresa «genérica». Pero, naturalmente, las «empresas genéricas» no existen. Todas son concretas y requieren una adaptación que, en ocasiones, puede ser muy laboriosa. Es paradigmático el caso de los grandes ERP (*enterprise ressource planning system*). Estas herramientas son de dimensiones muy considerables, igual que su complejidad. Su adaptación es un completo proyecto que puede llegar a tomar más de un año y, si no se lleva el proyecto con sumo cuidado, tiene muchas probabilidades de acabar mal.

Hablando de responsabilidades, los proyectos de implantación de ERP que acaban mal suelen convertirse en un enfrentamiento judicial en el que cada parte atribuye toda la responsabilidad del fracaso del proyecto a la otra. Los ERP estándares más extendidos pertenecen a grandes compañías multinacionales que los distribuyen mediante empresas locales colaboradoras (*partners*). En ese caso el reparto de «culpas» se distribuye entre la multinacional, la colaboradora y el cliente. Las propias multinacionales suelen ofrecen modelos de contrato en los que se procura explicitar todas las etapas del proyecto y las responsabi-

lidades de cada parte en cada una. A pesar de ello, cuando el proyecto se tuerce, todos aplican la célebre máxima de Aristóteles: «la victoria tiene muchas madres, la derrota es huérfana».

### 4.4. Implantación y migración de datos

Otro fallo, lamentablemente muy habitual, es olvidar que, evidentemente, al final del proceso de diseño y construcción, hay que instalar el nuevo sistema en las máquinas donde deberá funcionar (formalmente, esto se llama **implantar**), trasladar toda la información del sistema antiguo al nuevo, lo que implica la extracción de los datos, la depuración (no es extraño que en los sistemas antiguos los datos sean erróneos o estén duplicados), su posible transformación (algunas codificaciones en los sistemas antiguos son obsoletas en los nuevos), carga en el nuevo y validación de que los datos cargados son correctos (formalmente, **migración de datos**), y formar al personal de la organización para que sepa desenvolverse con el nuevo sistema con la misma soltura con que lo hacía con el antiguo.

La responsabilidad de estos últimos pasos para el uso normal del nuevo SI no está clara, especialmente si la organización dispone de personal informático propio. Se debería especificar en el contrato y, de no haber sido específicamente contratado, se entenderá que la organización se ocupará de estas tareas con su propio personal. Cuando ninguna de las partes ha pensado en incluir eso en la contratación entre ellas, esto suele ser una desagradable sorpresa para la organización contratante y un motivo de agrias controversias.

### 4.5. Mantenimiento y día a día

Al hablar de mantenimiento de un SI, y especialmente de un SI informático, hay que distinguir varios tipos de mantenimiento. Ya desde la década de los setenta se empezó a distinguir, por lo menos, las siguientes cuatro categorías. Se refieren al mantenimiento de aplicaciones informáticas, pero es perfectamente extrapolable a SI informatizados (e incluso SI en general):

Los cuatro tipos básicos de mantenimiento

**Mantenimiento adaptativo**: introducir en el sistema modificaciones para hacer frente a cambios en el entorno (legislativos, de sistemas operativos o versiones de herramientas necesarias para el sistema, de preferencias o necesidades por parte de clientes relevantes, etc.).

**Mantenimiento perfectivo**: introducir mejoras en el comportamiento del sistema, por nuevos requerimientos o la observación de cálculos o previsiones, por parte de la organización contratante, que no resultaron suficientemente acertados.

**Mantenimiento correctivo**: diagnosticar y corregir aquellos errores que vayan apareciendo con el uso de la aplicación.

**Mantenimiento preventivo**: realizar modificaciones para aumentar la capacidad de mantenimiento del sistema, para facilitar los demás tipos de mantenimiento.

**El mantenimiento correctivo**

El mantenimiento correctivo debe considerarse incluido, aunque el contrato no lo indique explícitamente. La corrección de los errores más graves, comunicados en tiempo y forma, es una obligación para el desarrollador del programa o del SI.

Si bien, al hablar de mantenimiento de un SI, se suele pensar más en el mantenimiento correctivo, especialmente al principio, después de la creación del sistema, la experiencia demuestra que los dos primeros tipos, el adaptativo y el perfectivo, se suelen llevar alrededor del 75 % del esfuerzo y, en consecuencia, de los costes.

En cuanto a responsabilidades, que es lo que aquí nos ocupa, habría que concluir que, salvo acuerdo contractual entre las partes:

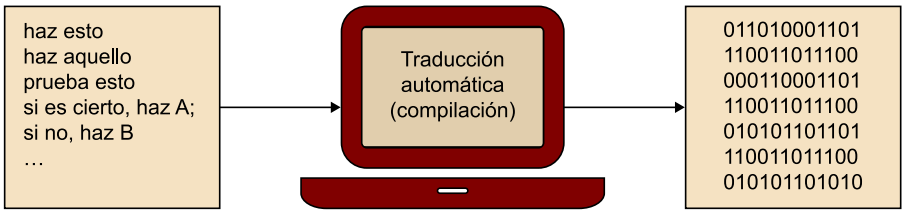
- El mantenimiento correctivo, en cuanto se refiere a la corrección de errores que suponen que el SI no se comporta tal como había sido especificado y, por lo tanto, comprometido, se debe considerar incluido. Es habitual que las empresas de servicios informáticos se cubran incluyendo en el contrato una limitación temporal de la obligación de este tipo de mantenimiento. Eso obliga a la organización contratante a probar su nuevo SI, tan exhaustivamente como pueda, en ese periodo. De todas formas, en caso de error grave, que dificulte el uso del sistema por parte de la organización, hay sentencias que han obligado a llevar a cabo este mantenimiento años después de acabado el contrato. Entra perfectamente en el concepto jurídico de *vicio oculto*.

- Los otros tres mantenimientos, especialmente el perfectivo y el adaptativo, que responden a nuevas necesidades de la organización, sobrevenidas tras la finalización y prueba del nuevo SI, no se consideran responsabilidad de la empresa de servicios informáticos contratada si no se indica lo contrario en el contrato. El preventivo, en la mayoría de las ocasiones, ni

se contempla. Se suele asumir que la organización lo contratará aparte en el futuro.

En este último punto interviene una cuestión poco conocida por el personal no técnico y que reviste bastante importancia: la titularidad del código desarrollado y los derechos sobre este. Previo a distinguir las distintas posibilidades en este aspecto, cuestión ya tratada sucintamente en otros módulos, hay que introducir un poco de vocabulario técnico:

Figura 1




Los programadores (humanos) escriben los programas en lenguajes de programación, formados por palabras inteligibles para humanos

**Programa fuente**

El programa final se traduce al lenguaje del ordenador, prácticamente ininteligible para los humanos

**Programa ejecutable o código máquina**

Para que el programa funcione sobre un ordenador, basta con disponer del código máquina o programa ejecutable. Para poder introducir cualquier modificación en el programa, sea por cualquiera de los tipos de mantenimiento antes expuestos, hace falta el código fuente, que es el único con el que pueden trabajar los programadores.

Dicho esto, ahora podemos distinguir, por lo menos, entre:

- ***Software* propietario**: la titularidad del programa queda en manos de la empresa que lo confecciona. A la organización cliente solo se le entrega el código máquina. Si este cliente quiere hacer alguna modificación en el programa tendrá que recurrir a la empresa desarrolladora para que lo haga. Es un cliente cautivo, no se puede plantear ninguna alternativa.

- ***Software* libre**: la titularidad de todo el programa se hace pública mediante una licencia de *software* libre. El cliente recibe el programa ejecutable y, normalmente, también el programa fuente. En caso contrario, el programa fuente está disponible por medio de internet. En cualquier caso, si la organización cliente quiere introducir modificaciones, puede contratar a la misma empresa o, si no está satisfecha, puede acudir a otra para que continúe el proyecto sobre el mismo código.

**La licencia GNU**

La licencia GNU es la licencia de *software* libre más conocida y la más extendida, aunque hay otras.

- ***Software* propio**: la titularidad del programa queda en manos de la organización que lo desarrolla, o encarga a terceros, para su propio uso. La organización dispone del código fuente, el programa ejecutable y toda la do-

cumentación relacionada con su elaboración. La organización propietaria es libre de introducir las modificaciones que precise y, si ha lugar, encargarlas a quien mejor le convenga. Sin embargo, este tipo de *software* ha sido fuente de amplios debates y litigios sobre quién es el propietario real de este *software*: la empresa que lo encarga (y paga) o quien físicamente lo desarrolla, discusión ligada y finalmente sancionada por la legislación sobre propiedad intelectual vigente en cada país.

Como vemos, el tipo de licencia del programa instalado condiciona las posibilidades de mantenimiento futuro, especialmente el adaptativo y el perfectivo, que se pueden deber a necesidades surgidas mucho tiempo después de finalizado el proyecto.

# Glosario

**Amenaza** *f* Hecho que puede suceder y que podría causar daños y perjuicios a la organización en cuestión. En gestión de riesgos, se suele denominar así la primera componente de un riesgo. La segunda es su probabilidad y la tercera la valoración de sus consecuencias.

**Análisis** *m* (de un SI) Proceso de clasificación e interpretación de los hechos que afectan a la organización, el diagnóstico de problemas y el empleo de la información disponible para recomendar mejoras de todo orden (procedimientos, optimizaciones, etc.).

**Auditoría** *f* Proceso lo más establecido y sistematizado posible para determinar la situación de una determinada organización frente a un determinado criterio. Por ejemplo, en informática se hacen auditorías de seguridad, para saber cómo está la organización en esta materia, o en economía se hacen auditorías contables, para verificar que la contabilidad registrada por la organización refleja realmente su situación financiera. Un PIA se podría considerar una auditoría de privacidad.

**Diseño** *m* (de un SI) Plasmación de las conclusiones del proceso de análisis en la especificación de las características que debe reunir el nuevo SI.

**Evaluación del impacto de la privacidad** *f* (en inglés, *Privacy Impact Assessment*, PIA) Metodología de evaluación y gestión de los riesgos que pueda suponer una incorrecta gestión de la privacidad de los datos de una organización.

**Finalidad** *f* (de una cesión de datos) Razón por la que una persona o entidad entrega datos sobre sí mismo/a a otra. Por ejemplo, para la obtención de un servicio.

**Flujo de datos** *m* Recorrido que atraviesan los datos en una organización, desde que se obtienen, se procesan y se guardan, hasta que se utilizan y se destruyen.

**Gestión de riesgos** *f* Conjunto de procedimientos y estrategias usadas en ingeniería y en otros ámbitos, con el fin de minimizar el impacto negativo de circunstancias difíciles de prever y que podrían causar daños y perjuicios a la organización afectada.

**Mantenimiento** *m* Último paso en el proceso de construcción de un SI, consistente en llevar a cabo las operaciones necesarias para que siga siendo útil a la organización. Se suelen distinguir cuatro tipos de mantenimiento: adaptativo, perfectivo, correctivo y preventivo. Ved el texto para ver sus definiciones.

**Migración de datos** *f* Uno de los últimos pasos en el proceso de construcción de un SI nuevo, consistente en el trasvase de toda la información del sistema antiguo al nuevo.

**Privacidad** *f* Característica de un SI que evita que los datos que un usuario no quiere que sean revelados para otro fin que aquel para el que los entrega, efectivamente no acaben destinados a ningún otro fin.

**Privacidad por el diseño** *f* (en inglés, *Privacy by Design*, PbD) Estrategia o reunión de principios a tener en cuenta durante el análisis y diseño de un SI con el fin de asegurar que respete la privacidad de los datos de todas las personas que guarden alguna relación con él.

***Privacy by Design*** *f* Ved *privacidad por el diseño*.

***Privacy Impact Assessment*** *f* Ved *evaluación del impacto de la privacidad*.

**Redundancia** *f* Propiedad que se dice que se da en un conjunto de datos cuando una misma información aparece reflejada de varias maneras en el mismo. Cuando existen dos formas distintas de obtener la misma información a partir del mismo conjunto de datos.

**Responsabilidad** *f* (de un acto o de sus consecuencias) Concepto jurídico que se refiere a quién debe responder por los daños o perjuicios causados por un hecho determinado, en caso de que se produzca.

***Software* libre** *m* Tipo de *software* en el que quienes lo construyen (normalmente de forma cooperativa) ceden todos los derechos al público en general. En particular, cualquier usuario, por sí mismo o vía la contratación de una empresa de servicios informáticos, puede introducir modificaciones en el programa, puesto que el código fuente siempre está disponible.

***Software* propietario** *m* Tipo de *software* que se caracteriza por el hecho de que quien lo ha construido (normalmente una empresa) mantiene todos los derechos sobre el *software* y solo le cede algunos derechos, en ocasiones bastante limitados, al usuario. En particular, el

usuario no puede introducir ninguna modificación en el código, puesto que, normalmente, no dispone del código fuente, necesario para ello.

***Software* propio** *m* Tipo de *software* desarrollado por la propia organización.

# Bibliografía

**AUTELSI(Asociación española de Usuarios de Telecomunicaciones y de la Sociedad de la Información)** (2014, diciembre). «Estudio sobre el principio "Privacy by Design"».

**Cavoukian, A.** *Privacy by Design. The 7 Foundational Principles*.

**ICO(Information Comissioner's Office)** (2017, enero). «The Guide to Data Protection».

<https://ico.org.uk/for-organisations/guide-to-data-protection/>.

**McNurlin, B. C.; Sprague, R. H.; Bui, T.** (2009). *Information systems management in practice*. Prentice Hall / Pearson Education.

**Kendall, K.; Kendall, J. P.** (2011). *Systems Analysis and Design* (8.ª ed.). Prentice Hall / Pearson Education.

**Piattini Velthuis, M. G.; Hervada Vidal, F.** (2007). *Gobierno de las tecnologías y los sistemas de información*. Madrid: Ra-Ma.