Implantación de Sistemas

Maria Ines Parnisari

17 de Diciembre de 2014

Índice

Parte 1: Implantación

Factores clave para una implantación exitosa

1) Apoyo de la gerencia
2) Apoyo de los *stakeholders*
3) Disponibilidad de recursos (dinero y recursos humanos)

Etapas de un proyecto de Sistemas

1) Captura de requisitos
2) Análisis
3) Diseño
4) Desarrollo
5) Pruebas
6) Implantación

Fases de una implantación

1. Revisión de hardware y software

Analizar si la infraestructura actual soportará el sistema nuevo. Si no la soporta, explicar qué cambios son necesarios.
Analizar si las PCs de los usuarios soportarán el nuevo sistema.

2. Método de implantación[1]

La elección del método depende de varios factores:

- Volumen de información
- Criticidad de la implementación
- Restricciones de tiempo
- Recursos humanos
- Restricciones de hardware

Tabla 1 Métodos directo, paralelo, big bang y escalonado

		Por coexistencia en el tiempo	
		Directo: el nuevo sistema no coexiste con el viejo	**Paralelo**: el nuevo sistema coexiste con el viejo durante un tiempo, pero el que está vigente es el viejo. Se comparan salidas entre ambos sistemas
Por coexistencia en el espacio	**Big Bang**: todo el nuevo sistema pasa a producción		
	Escalonado: el nuevo sistema pasa a producción por etapas (por módulos, por unidades de negocio, por unidades geográficas)		

Tabla 2 Implantación Big Bang, en paralelo y escalonado

	Revolución	⟶	*Evolución*
	Big Bang	**En paralelo**	**Escalonado**

[1] *ERP Implementation Strategies*: http://blog.softwareadvice.com/articles/manufacturing/erp-implementation-strategies-1031101/

Necesidad de control de riesgos	Bajo		Alto
Necesidad de facilitar el cambio	Bajo		Alto
Ritmo del cambio	Alto		Bajo
Adaptación del usuario	*Difícil*	⟶	*Sencilla*

Tabla 3 Implantación Big Bang

Ventajas	Desventajas
El tiempo de implantación es más corto que si fuera escalonado	Se necesitan pruebas más exhaustivas
El costo suele ser menor que si fuera escalonado	Los problemas son más pronunciados
	Existe un tiempo inicial de adaptación al nuevo sistema

Tabla 4 Implantación escalonada

Ventajas	Desventajas
Las primeras fases son difíciles, pero luego se hace más fácil	Involucra cambios durante un largo período de tiempo
No es necesario tener todo el sistema terminado para empezar la implementación	Una vuelta atrás al sistema viejo se hace más difícil con cada fase
No hay tiempo perdido de adaptación por parte de los empleados	Se necesitan interfaces temporales entre el sistema viejo y el sistema nuevo

Tabla 5 Implantación en paralelo

Ventajas	Desventajas
Término medio comparado con big bang y escalonado en cuanto a cantidad de cambios y la adaptación de los usuarios	Es el método más costoso en cuanto a recursos necesarios (hardware, personas)
La vuelta atrás es sencilla	Se pierde eficiencia organizacional porque los usuarios deben ingresar datos en dos sistemas
	Puede perderse mucho tiempo buscando bugs que resultan de la comparación de ambos sistemas, cuando tal vez no hay bug alguno
	Hay ciertos sistemas que no se pueden paralelizar. Por ejemplo, una máquina que produce cosas.

3. Puesta operativa

Es la fecha a partir de la cual el nuevo sistema entra en vigencia. A partir de ese momento las decisiones se toman usando información del nuevo sistema.

Deben estar listos:

- Migración de datos
- Capacitación
- Interfases definitivas
- Manual de Normas y Procedimientos

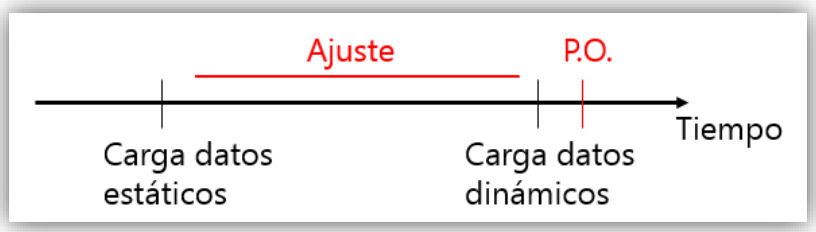
4. Migración de datos

Involucra tres partes:

1) Carga inicial
2) Conversión de datos
3) Depuración

Estáticos	Dinámicos
No varían en el tiempo	Varían en el tiempo
Ejemplo: nombres de los proveedores	Ejemplo: órdenes de compra generadas
Se deben migrar un tiempo antes de la puesta operativa, una sola vez ⟹ interfaz temporal	Se deben migrar justo antes de la puesta operativa, para reducir al mínimo la cantidad que se debe ingresar manualmente ⟹ interfaz definitiva

Figure 1 Tipos de datos



Carga inicial

Volcado de información del sistema viejo al sistema nuevo.

Se debe decidir:

⟹ Si es manual o automática
⟹ Si se cargarán los datos históricos

Conversión de datos

Convertir datos de un formato al otro. Debe haber una tabla de conversión de datos "de – para". Esta tabla indica cómo convertir cada tipo de dato desde el formato viejo al nuevo (ya que probablemente sean distintos).

Se debe decidir:

⟹ Si es manual o automática

Depuración de datos

El usuario clave es el que decide qué datos se van a depurar.

Se debe decidir:

⟹ Si es manual o automática

Se debe asegurar:

⟹ Que no se pierdan datos en la migración. *¡Realizar un backup de los datos viejos!*
⟹ Que si faltan datos, se los agregue
⟹ Que si hay datos incorrectos, se los corrija
⟹ Que no haya datos duplicados
⟹ Que los datos sea válidos en forma lógica (ejemplo: una dirección que no existe no se debería permitir)
⟹ Integridad de las referencias en las bases de datos. *Aunque el usuario quiera borrar ciertos datos, si los mismos se utilizan en otra parte del sistema, no se pueden borrar*

5. Interfases

Definen la comunicación entre sistemas.

Según si se mantienen después de la implantación	
Temporales: comunican el sistema nuevo con el viejo. Se usa para la comparación de salidas entre sistemas, y una carga inicial en el sistema nuevo. No se mantienen después de la implantación	**Definitivas:** comunican el sistema nuevo con otros sistemas. Se mantienen después de la implantación

Figure 2 Tipos de interfases

6. Perfiles / roles

Cada perfil puede ejecutar una o más funciones del sistema.

Perfiles en el equipo de implantación:

⇒ Líder
⇒ Analistas funcionales
⇒ Desarrolladores
⇒ Testers
⇒ Usuario clave

Perfiles en la organización: los define el nivel jerárquico de cada sector, pero en general son:

- Usuarios que realizan altas y bajas de datos
- Supervisor: puede manejar información confidencial
- Usuarios que realizan consultas
- Seguridad: modifican permisos, usuarios, claves, etc.

Si cambia un perfil debe actualizarse el manual de normas y procedimientos, y todo lo que se tiene como perfil tiene que aparecer en el manual de usuario. Para definir el perfil de acceso del usuario se debe tener en cuenta el Manual de Normas y Procedimientos y en caso de no existir se tendrá en cuenta la tarea que desempeña, el sector donde se desempeña y las responsabilidades que posee.

7. Plan de pruebas

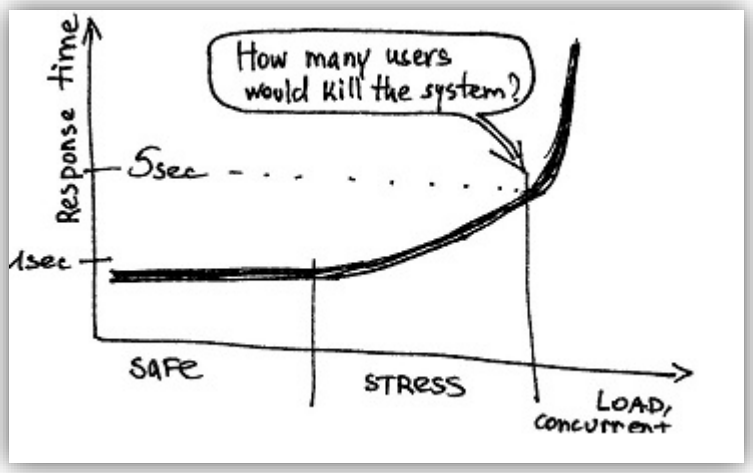


Figure 3 Tests de estrés vs. tests de volumen

¿Quién las elabora? ¿Quién las ejecuta? ¿Quién las aprueba? → El usuario clave

- **De hardware**: probar si el hardware actual soportará el nuevo sistema.
- **Unitarias**: están a cargo de los analistas. Se prueba cada módulo por separado.

- **Funcionales**: están a cargo de los analistas. Probar las diversas funciones del sistema (casos felices y casos erróneos, ver cómo se comporta el sistema). Probar la lógica de negocio.
- **De estrés**: verificar cómo es el tiempo de respuesta del sistema ante muchos usuarios. ¿Concurrencia?
- **De volumen**: verificar cómo es el tiempo de respuesta del sistema ante muchísimos usuarios. ¿Carga?
- **Integrales**: verificar todo un circuito completo. Las debe realizar el área usuaria.
- **De perfiles**: probar que un usuario con perfil X que tiene autorizado realizar Y no pueda realizar Z.
- **De interfases**: probar las interfaces entre los módulos o entre el sistema nuevo y el viejo.
- **Del plan de contingencia:** al menos una vez al año.

Definir:

- Set de datos de prueba *(siempre ficticios, excepto cuando se implanta en paralelo)*
- Salida esperada
- Persona responsable de ejecutar la prueba
- Ambiente de prueba (distinto del de producción)
- Automatización de las pruebas

8. Capacitación

- Lugar → Fuera del área de trabajo, pero en un entorno similar
- Logística → Transporte, fecha, hora, días para no reducir la capacidad productiva del negocio
- Temario →
    - Evaluación de lo aprendido
    - Clases prácticas o teóricas
    - Uso del sistema (sólo lo que ese usuario va a usar)
    - Cómo reportar errores
- Personas → Decidir si es mejor capacitar a todo el personal, o a capacitadores que capacitarán (depende de la cantidad de gente a capacitar)
- No es necesario que el manual de usuario ya esté listo para capacitar. Sí es necesario que ya estén definidos los distintos perfiles

Si el sistema a implantar es cerrado…	Si el sistema a implantar es un desarrollo propio…
Capacitación → Pruebas	Pruebas → Capacitación

9. Manual de usuario

Su objetivo es definir cómo ejecutar cada función del sistema. Existe un manual por cada perfil.

10. Manual de normas y procedimientos

Su objetivo es establecer las tareas y responsabilidades que tienen a su cargo todas las áreas de una empresa. Este manual debe estar listo antes de la puesta operativa del sistema a implantar, para poder definir los perfiles.

Proceso: conjunto de tareas.

Procedimiento: cómo llevar a cabo un conjunto de tareas.

- Responsable
- Funciones
- Tareas
- Controles

Objetivo: <circuito administrativo o acción de negocio> **Alcance:** desde/hasta **Nombre de la empresa** **Nombre del documento** **Versión**		
Responsable	**Tarea**	**Controles**
…	…	….
…	…	…
Autor / Responsable: **Fecha de vigencia:** **Aprobado por:**		

Figure 4 Plantilla de un manual de normas y procedimiento

11. Manual de autorizaciones

Indica quién hace las distintas actividades de la empresa.

Responsable	**Desde**	**Hasta**
…	…	…

Figure 5 Plantilla de un manual de autorizaciones

12. Plan de corte

Procedimiento a seguir para dar de baja el sistema viejo y poner operativo el sistema nuevo.

13. Plan de contingencia

Son los pasos a seguir en caso de una falla prolongada del sistema nuevo, para mantener la actividad del negocio. El responsable de mantenerlo es la gerencia de Sistemas.

Tareas para crear un plan de contingencia:

1) Identificar tareas críticas y sus posibles contingencias
2) Identificar el soporte de información para cada tarea crítica
3) Documentar el plan de contingencia
4) Comunicar el plan de contingencia a toda la organización
5) Simular el plan de contingencia
6) Crear manual de normas y procedimientos

14. Análisis post-implantación

Revisar:

- Si los tiempos de respuesta son mejores que los del sistema viejo
- Si cumple las expectativas y requisitos del usuario
- Si falta alguna funcionalidad
- Si se puede mejorar algo
- Si los perfiles de usuario son correctos
- Si el sistema viejo se dejó de usar por completo
- En base a los pedidos del *help desk*, si es necesaria otra capacitación

Parte 2: Auditoría

Definición

La **auditoría** es un proceso de revisión de un determinado procedimiento. Lo realiza un profesional calificado. Su objetivo es obtener una conclusión sobre el desarrollo del mismo.

Tipos de auditoría

1) **Interna**: la realiza un área de la empresa que depende, generalmente, de un nivel alto en la organización. Su objetivo es agregar valor y mejorar las operaciones de una organización.
    - *De sistemas*: revisa la configuración del sistema y los perfiles de acceso.
    - *Operativa*: verifica que las transacciones de la compañía se hagan de manera coherente. Analiza la eficiencia y eficacia de las transacciones.
    - *De calidad*: asegura que se cumplan con los estándares de calidad
    - *Administrativa*
2) **Externa**: la realiza personal independiente de la entidad auditada. La auditoría más común es la relacionada a los estados contables. Analiza si los mismos reflejan la realidad de la empresa y satisfacen las normas generalmente aceptadas.

Plan de auditoría

Debe incluir:

- Qué procesos se van a auditar
- Qué recursos se van a usar
- Objetivo de la auditoría
- Alcance de la auditoría
- Comunicación a la administración
- Programa de trabajo
    - Cómo se va a auditar
    - Metodología de trabajo
    - Objetivo de control
    - Controles a revisar
    - Cómo se prueban los controles
    - Efectividad de los controles
    - Observaciones

Salidas generadas

Informe detallado:

Situación actual	Riesgos	Probabilidad de ocurrencia	Posibles consecuencias	Recomendación sugerida
…	…	…	…	…

Informe sintético: su destinatario es la alta gerencia. Se debe utilizar un vocabulario claro, no técnico, agrupando cada riesgo por su posible consecuencia (pérdida de dinero, pérdida de clientes, etc.). Especificar:

- Objetivo
- Alcance
- Metodología del auditor
- Diagnóstico de la situación
- Principales cursos de acción

Riesgos

Un **riesgo** es la posibilidad que un evento o circunstancia, previsto o imprevisto, impidan a la organización alcanzar sus objetivos. Su criticidad depende de dos factores:

- La magnitud de impacto del evento
- La probabilidad de ocurrencia de dicho evento

Tipos de riesgos

El **riesgo de auditoría** es la posibilidad de emitir un informe de auditoría incorrecto por no haber detectado errores o irregularidades significativas que modificarían el sentido de la opinión vertida en el informe.

- riesgos relacionados con el entorno de procesamiento, que se mitigan mediante "**Controles Generales**"
- riesgos relacionados con cada aplicación, que son controlados a través de "**Controles Directos**".

El riesgo de auditoría es el conjunto de:

- **Riesgos inherentes**: tiene ver exclusivamente con la actividad económica o negocio de la empresa, independientemente de los sistemas de control interno que allí se estén aplicando. Está totalmente fuera de control por parte del auditor.
- **Riesgos de control**: es el riesgo de que los sistemas de control estén incapacitados para detectar o evitar errores en forma oportuna. Está totalmente fuera de control por parte del auditor. Para ser efectivo, un sistema de control debe ocuparse de los riesgos inherentes percibidos, incorporar una adecuada segregación de funciones incompatibles y poseer un alto grado de cumplimiento.
- **Riesgos de detección**: se trata de la no detección de la existencia de errores en el proceso de auditoría realizado.

La matriz de evaluación de riesgos se utiliza para planificar la auditoría. Se le da relevancia a cada proceso de negocio

Tabla 6 Matriz de evaluación de riesgos

		PROBABILIDAD				
		Raro	Poco probable	Posible	Muy probable	Casi seguro
CONSECUENCIAS	Despreciable	Bajo	Bajo	Bajo	Medio	Medio
	Menores	Bajo	Bajo	Medio	Medio	Medio
	Moderadas	Medio	Medio	Medio	Alto	Alto
	Mayores	Medio	Medio	Alto	Alto	Muy alto
	Catastróficas	Medio	Alto	Alto	Muy alto	Muy alto

Posibles respuestas de la gerencia frente a los riesgos:

- Eliminar el riesgo: eliminar un área de negocio o alterarla significativamente
- Reducir el riesgo: implementar controles
- Aceptar el riesgo: continuar operando
- Trasladar el riesgo: tercerizar una actividad o contratar un seguro

Controles

Un **control** es una actividad específica definida para:

- Prevenir la ocurrencia de un error (preventivo)
- Detectar y corregir un error que ya ocurrió (correctivo)

Una clasificación básica de los controles es:

- **Controles Generales**: contribuyen significativamente a la efectividad de los controles directos. Abarcan:
  - Estructura organizativa del departamento de Sistemas
  - Procedimiento de cambio a los programas
  - Acceso general a los datos o programas de aplicación
  - Continuidad de procesamiento

  Los tres riesgos que típicamente se reducen con la implantación de Controles Generales son:

  - La Estructura Organizativa y los Procedimientos Operativos pueden resultar en un entorno de procesamiento de datos no confiable.
  - Los programadores pueden efectuar modificaciones incorrectas o no autorizadas al software de aplicación.
  - Personas no autorizadas pueden obtener acceso directo a los archivos de datos o a los programas de aplicación utilizados.

Algunos controles generales:

- Segregación de funciones

- **Controles Directos**: abarcan controles gerenciales e independientes, controles de procesamiento y funciones de procesamiento computadorizadas y controles para salvaguardar activos.
- **Controles compensatorios**: son controles internos que reducen el riesgo de una debilidad de control. En empresas pequeñas, debe haber controles compensatorios, para mitigar el riesgo de no tener segregación de funciones. Por ejemplo, no se deben limitar los permisos de un administrador de BD, sino que un supervisor debe revisar sus logs de acceso.

Fraude

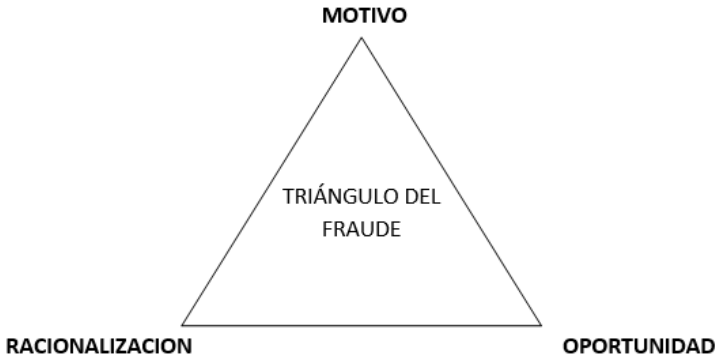


Figure 6 Triángulo del fraude

Oportunidad: está bajo control de la compañía. La misma debe asegurarse de cerrar todas las puertas de la oportunidad.

Racionalización: es el autoconvencimiento para saber aprovecharse de la oportunidad de cometer fraude.

Controles de TI

1) Acceso a programas y datos

Identificación de usuarios, usuarios especiales, configuración de contraseñas, revisión de *logs*, accesos a producción.

2) Desarrollo de aplicaciones

Asegurar que los nuevos sistemas (desarrollados o adquiridos) hayan sido autorizados, testeados, aprobados y documentados.

3) Control de cambios

Asegurar que los cambios en el ambiente de producción hayan sido autorizados, testeados, aprobados y documentados.

4) Operaciones y resguardo de datos

Resguardo de datos, contingencias, problemas en el ambiente de producción.