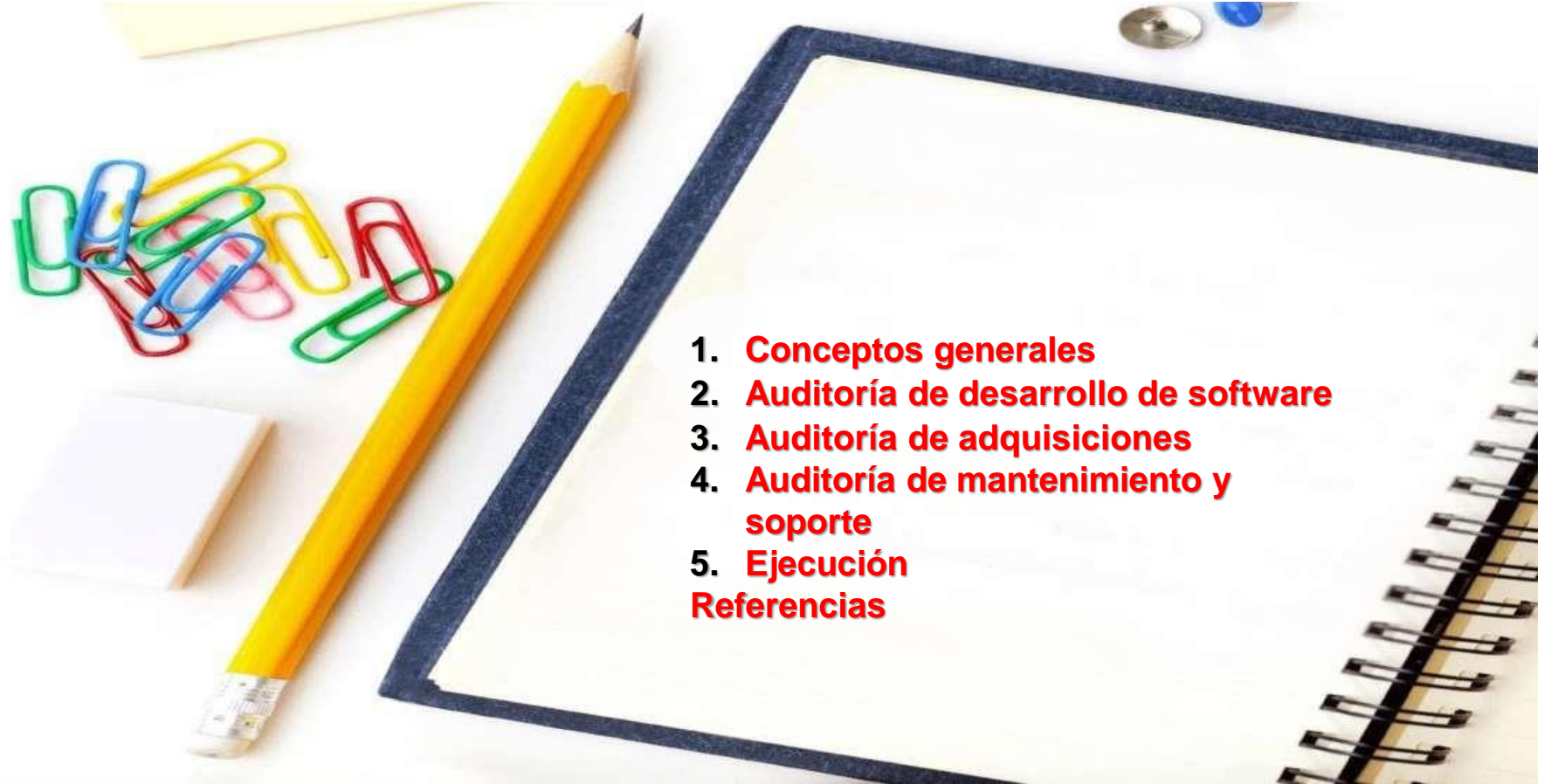


AUDITORÍA Y CONTROL DE SISTEMAS

AUDITORÍAS DEL DESARROLLO, ADQUISICIÓN, MANTENIMIENTO Y SOPORTE DE SOFTWARE

Agenda

- 
1. **Conceptos generales**
 2. **Auditoría de desarrollo de software**
 3. **Auditoría de adquisiciones**
 4. **Auditoría de mantenimiento y soporte**
 5. **Ejecución**
- Referencias**

CONCEPTOS GENERALES

Introducción



- Las organizaciones gastan importantes recursos desarrollando, adquiriendo y manteniendo aplicaciones y sistemas de información que administran procesos e información crítica.
- El desarrollo de software es el proceso de convertir las necesidades de la organización en un sistema de información **(que soporten los procesos de negocio)**

Terminología

CICLO DE VIDA DE SOFTWARE:

El periodo de tiempo que empieza desde cuando se concibe un producto de software y finaliza cuando el software ya no está disponible para su uso. El ciclo de vida del software generalmente incluye una fase conceptual, fase de requisitos, fase de diseño, fase de implementación, fase de prueba, fase de instalación y salida, fase de operación y mantenimiento y, a veces, fase de retiro. Nota: Estas fases pueden superponerse o realizarse iterativamente.

OBSOLESCENCIA,
ESCALABILIDAD, ACTUALIZACIÓN

CICLO DE DESARROLLO DEL SOFTWARE:

El periodo de tiempo que comienza con la decisión de desarrollar un producto de software y finaliza cuando se entrega el software. Este ciclo generalmente incluye una fase de requisitos, fase de diseño, fase de implementación, fase de prueba y, a veces, fase de instalación y salida

FASE/METODOLOGÍA - MODELO/
VALOR / EFECTIVIDAD

SOFTWARE:

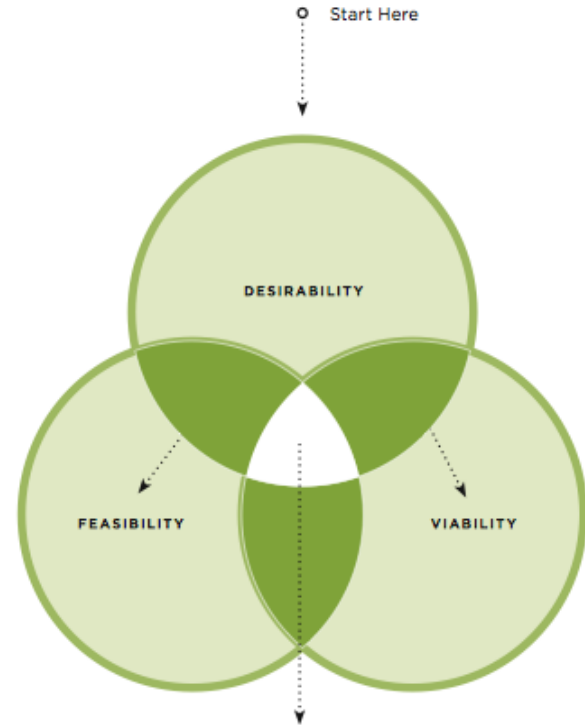
Programas de computadora, procedimientos, y posiblemente documentación asociada y datos relacionados con la operación de un sistema de computadora.

FUNCIONALIDAD, CODIFICACIÓN,
PROPIEDAD

Todas las definiciones provienen del IEEE Standard Glossary of Software Engineering Terminology.

Terminología

- El **estudio de viabilidad** debería verificar si el SI o TIC por adquirir / implementar:
 - Soporta tecnológicamente un proceso de negocio nuevo o uno ya existente.
 - Resuelva un incidente o problema existente.
 - Cubra una nueva oportunidad de negocio, que permita a la empresa obtener una ventaja competitiva dentro de su mercado.
 - Reemplace a otra aplicación dada de baja.
- También es llamado **caso de negocio o documento de visión o estudio de interés**
 - De nuevo, aplicable tanto a la opción de desarrollar (desde cero) o adquirir un SI



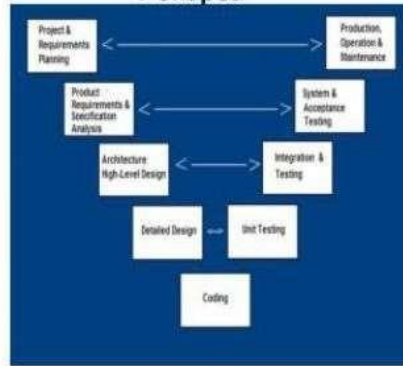
The solutions that emerge at the end of the Human-Centered Design should hit the overlap of these three lenses; they need to be **Desirable, Feasible, and Viable**.

Metodologías para el desarrollo de software

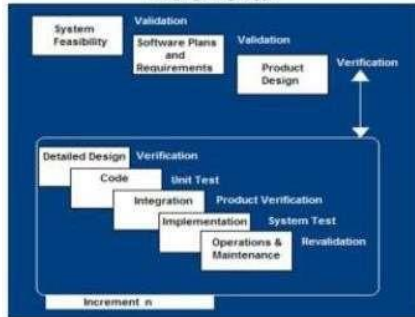
Waterfall



V-Shaped



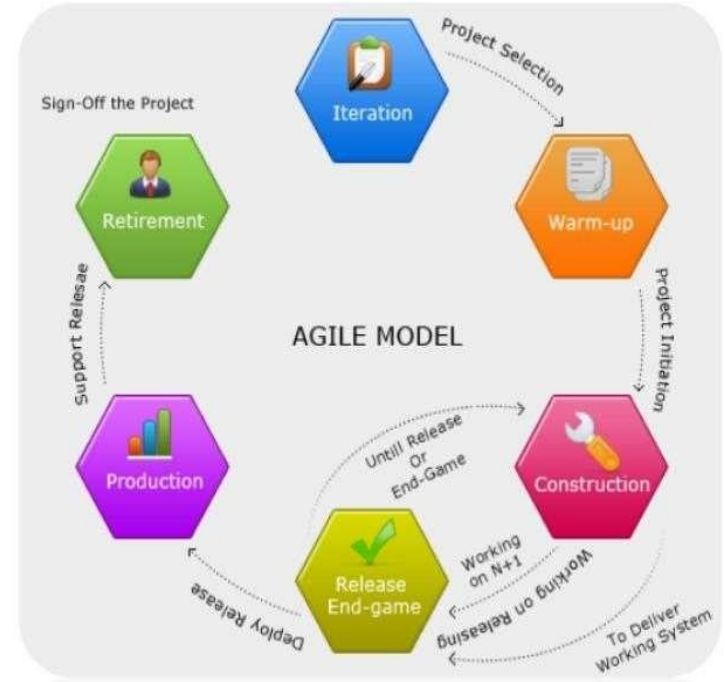
Incremental



Spiral



AGILE MODEL



1. AUDITORÍA DEL DESARROLLO DE SOFTWARE

Frentes de problema/riesgo en el diseño del Software

Proceso de Desarrollo	Sistema Desarrollado	Gestión del Proceso	Monitoreo
<ul style="list-style-type: none">• Formalización• Sostenible• Controles en el Proceso• Controles en el Producto	<ul style="list-style-type: none">• Capacidad• Sostenibilidad• Usabilidad• Confiable• Tiene Soporte	<ul style="list-style-type: none">• Planificación• Organización del Equipo de Desarrollo y del Proyecto• Experiencia• Interfases con otros procesos.	<ul style="list-style-type: none">• Indicadores• Gestión del desempeño del personal• Aseguramiento de la Calidad• Gestión de la configuración

Frentes de problema/riesgo en el diseño del Software

Requerimientos

- Estabilidad
- Completitud
- Claridad
- Validez
- Factibilidad
- Precedencia
- Escalabilidad

Diseño

- Funcionalidad
- Dificultad
- Interfases
- Desempeño
- Calidad
- Restricciones del WH

Codificación

- Claridad
- Optimización
- Documentación
- Complejidad y Costos

Integración y Pruebas

- Desarrollo
- Ambiente Productivo

Frentes de problema/riesgo en el diseño del Software

Recursos

- Cronograma
- Staff
- Presupuesto
- Entorno

Contractuales

- Tipos de Contrato
- Restricciones
- Dependencias

Relaciones con

- Cliente
- Proveedores
- Gestión Corporativa
- Políticas del Proveedor
- Exigencias Regulatorias

2. AUDITORÍA DE LA ADQUISICIÓN

Adquisición de tecnologías

Software

- **Estudios de mercado**
 - Seleccionar las versiones / actualizaciones más adecuadas para cada escenario comercial.
- **En los casos de *cambios de sistemas*:**
 - Necesidad de contar con procedimientos de control de cambios adecuadamente documentados
 - No afectar la continuidad del procesamiento

Hardware

Especificaciones	Detalle
Sobre el negocio	Descripciones sobre los aspectos legales, regulatorios y propios del adquiriente que sin ser de carácter técnico, considere necesarios de poner en conocimiento del proveedor
Sobre procesamiento de información	Interfaces con otros sistemas existentes (y futuros); requerimientos de carga de trabajo y desempeño; enfoques de procesamiento tales como en línea, en lote, en tiempo real, etc.
Sobre el hardware propiamente dicho	Descripciones sobre la velocidad de procesamiento, requerimientos de espacio en disco y memoria, cantidad de equipos, dispositivos periféricos, terminales de entrada directa, conexiones a red, etc.
Sobre el software contenido en el hardware por adquirir	Sistema operativo (versión y actualizaciones requeridas), software utilitario, biblioteca de programas, software administrador de base de datos, software de comunicaciones, control de accesos, entre otros.
Sobre los requerimientos de respaldo	Proceso de mantenimiento de los sistemas (tanto detectivo, preventivo como correctivo), capacitación al personal del adquiriente, mecanismos de copias de respaldo

Auditoría de adquisiciones



- Analizar el estudio de viabilidad para determinar **si la decisión de la adquisición fue/es correcta**, frente a las necesidades del negocio, sus objetivos y estrategias de TI.
- Revisar los términos de referencia o las solicitudes de cotización, según sea el caso, para garantizar su competencia.
- Revisar contratos con proveedores en temas de tecnología y los acuerdos de nivel de servicio y garantía que se tienen establecidos con ellos, en los contratos.

3. AUDITORÍA DE MANTENIMIENTO Y SOPORTE

Auditoría de mantenimiento y soporte

- El auditor debe garantizar que se hayan llevado a cabo **los cambios en los sistemas de información de manera lógica, adecuada y autorizada.**
- **Lo mismo para el proceso de mantenimiento de hardware.**
- Es conveniente que revise:
 - El acceso a las bibliotecas de código fuente
 - Los procesos de solicitud y aprobación de los cambios, su documentación y proceso de atención.
 - Una muestra de las solicitudes para ejecutar un seguimiento paso a paso hasta su puesta en producción.
 - Al equipo encargado de la atención de los cambios (funciones, políticas, etc.).
 - Los procedimientos de atención de los cambios de emergencia, inclusive analizando una muestra de ellos.



EJECUCIÓN DE AUDITORÍAS DE DESARROLLO, ADQUISICIÓN Y MANTENIMIENTO

Criterios

- **Responsabilidades relacionadas con desarrollo y mantenimiento**

- ☐ Comité de Proyectos
- ☐ Sponsors
- ☐ Oficina de Gestión de Proyectos
- ☐ Jefe de Proyecto
- ☐ Business Case (beneficios realistas, entendibles y medibles)

- **Prácticas de monitoreo**

- ☐ Desviaciones en la estimación de tiempos
- ☐ Hoja de ruta e hitos críticos
- ☐ Proceso formal de gestión de cambio
- ☐ Costos incurridos vs la generación de entregables

- **Aseguramiento de la calidad**

- ☐ Prácticas de aseguramiento de la calidad
- ☐ Procedimientos regulatorios
- ☐ Entradas y salidas por cada fase del proyecto.
- ☐ Monitoreo continuo de la calidad
- ☐ Política de Mejora continua

Criterios

Configuración y pruebas

- ☐ Configuración de controles de acceso y seguridad en los aplicativos asociados
- ☐ Estudios de segregación de funciones y se han configurado adecuadamente los controles asociados.
- ☐ Alertas de transacciones de excepción.
- ☐ Procedimientos de prueba y calidad
- ☐ Procedimiento de stress testing en la carga de datos

Despliegue

- ☐ Procedimiento despliegue del sistema (software + base de datos) desde un ambiente de desarrollo y pruebas hacia un ambiente de producción.
- ☐ Política de conformidad del servicio de desarrollo se ha brindado de manera correcta, dando fin al proyecto de desarrollo.

Referencias bibliográficas

- [ISACA, 2013] ISACA International. COBIT 5 - Enabling Information (p. 35). ISACA Publishing, USA (2013).
- [ISACA, 2018a] ISACA International. Certified Information Systems Auditor (CISA) Exam Preparation Guide. ISACA Publishing, USA (2018).
- [ISACA, 2018b] ISACA International. COBIT 2019. ISACA Publishing, USA (2018).
- [Piattini, Del Peso 2001] M. Piattini, E. Del Peso. Auditoría Informática, 2da Edición. AlfaOmega Ra-Ma, México (2001)
- [Ramirez, Alvarez, 2003] G. Ramirez, E. Álvarez. Auditoría a la Gestión de las Tecnologías y Sistemas de Información. Industrial Data, Vol(6)1:99-102.
- [Tupia, 2011] Manuel Tupia. Principios de auditoría de sistemas y tecnologías de información. Tupia Consultores Y Auditores S.A.C., Perú (2011)

¿Consultas?



AUDITORÍAS DEL DESARROLLO, ADQUISICIÓN, MANTENIMIENTO Y SOPORTE DE SOFTWARE