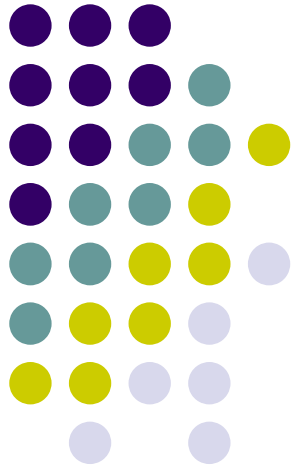
Auditoria en Ciberseguridad Informática

Jacob Lyng
Australia - CdMx

Publicaciones La Tecla AC



Publicaciones la Tecla

Introducción

- La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Auditoría

- La palabra auditoría viene del latín **auditorius** y de esta proviene auditor, que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo

Tipos de Auditorias

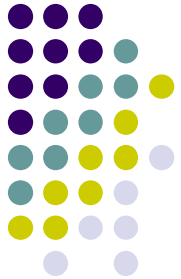
Áreas Específicas

- Explotación
- Desarrollo
- Sistemas
- Comunicaciones
- Seguridad

Áreas Generales

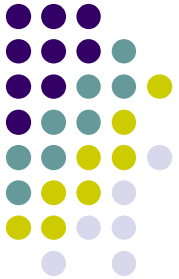
- Interna
- Dirección
- Usuario
- Seguridad

Metodología de auditoría informática



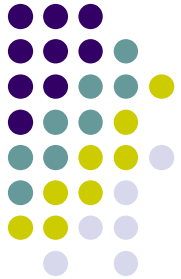
- Alcance y objetivos
- Estudio inicial del entorno auditable
- Determinación de los recursos
- Elaborar plan y programa de trabajo
- Actividades de auditoría
- Informe final
- Carta de presentación del informe

Objetivo General de Auditoría de sistemas



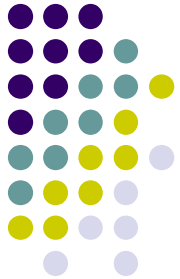
- Operatividad 100%

Herramientas para Auditoría informática



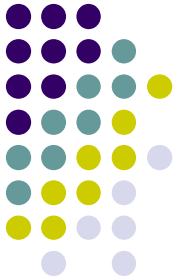
- Cuestionarios
- Entrevistas
- Check list (de rango y binario)
- Trazas
- Software de interrogación

Consideraciones para el éxito del análisis crítico



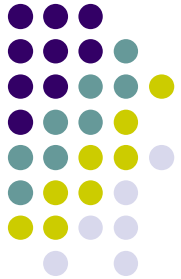
- Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)
- Investigar las causas, no los efectos.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

Estándares de Seguridad de la información



- **ISO/IEC 27000-series**
- **COBIT**
- **ITIL**

ISO/IEC 27000-series



- La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).
- La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

COBIT

- Objetivos de Control para la información y Tecnologías relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology)
- Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoria y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

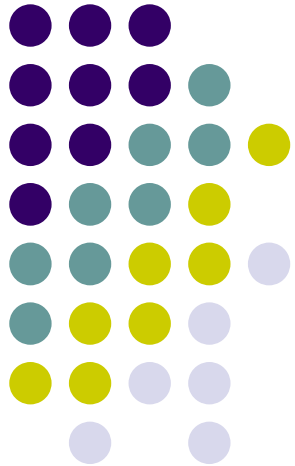
ITIL

- La Information Technology Infrastructure Library ("Biblioteca de Infraestructura de Tecnologías de Información"), frecuentemente abreviada ITIL.
- Es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI

Auditoria en Ciberseguridad Informática

Jacob Lyng
Australia - CdMx

Publicaciones La Tecla AC



Publicaciones la Tecla