AUDITORIA DE SISTEMAS

OBJETIVO: Conocer el marco conceptual de la auditoría informática

Ing. Pablo Almeida Haro Msc. PhD (C)

CONCEPTO

- Es un examen crítico con carácter objetivo para evaluar la eficiencia y eficacia en el uso de los recursos informáticos y la gestión informática de un período determinado en cumplimiento de los objetivos empresariales

CARACTERISTICAS

- Objetiva: Orientada hacia los objetivos de la organización
- Sistemática: Planeada y cumple un proceso
- Profesional: Elaborado por personal capacitado en forma ética
- Concluyente: El resultado es un informe con resultados, observaciones, conclusiones y recomendaciones
- Descubre: Evidencias, riesgos, vulnerabilidad, Impacto

IMPORTANCIA

- Verifica el cumplimiento de los objetivos estratégicos
- Disminuye el incremento de delitos informáticos
- Evita problemas con la administración tributaria, seguridad social, etc
- Evita desastres informáticos
- Controla el presupuesto informático

- Informa a la alta gerencia del estado de TI
- Mejora la atención al usuario
- Recomienda la generación de documentación del área de TI
- Evalúa el outsourcing

OBJETIVOS

- Evaluar el costo beneficio de las TIC implementadas
- Evaluar la satisfacción de los usuarios
- Verificar:
  - Integridad de información
  - Confidencialidad
  - Confiabilidad
- Establecer esfuerzos y actividades del área de TI para lograr los objetivos
- Verificar riesgos:
  - Información
  - Hardware
  - Comunicaciones
- Evaluar decisiones de inversión y gastos

METODOLOGIAS Y NORMAS

- COBIT (Isaca)
- ITIL
- COSO
- AICPA (SAS)
- IFAC (NIA)
- SAC
- MARGERIT
- EDP
- ISO
- CMMI
- PMBOK
- ISTQB

OECD Organization for Economic Cooperation and Development

GAPP Generaly Accepted Principles and Practices. National Institute of Standards and Technology (NIST)

BS 7799 British Standard Institute

SAC Security Auditability and Control. The Inst. of Internal Audit.

COSO Internal Control Integrated Framework. Committee of Sponsoring Organizations

SSE CMM Systems Security Engineering Capability Maturity Model National Security Agency (NSA) Defense- Canada.

CoCo Criteria of Control Board of The Canadian Institute of Chartered Accountants.

ITCG Information Technology Control Guidelines. Canadian Institute of Chartered Accountants (CICA)

GASSP Generaly Accepted System Security Principles. International Information Security Foundation (IISF)

Cobit Control Objectives for Information and Related Technologies

FISCAM Federal Information Systems Controls Audit Manual. GAO

SysTrust AICPA/CICA SysTrust Principles and Criteria for System Reliability

SSAG System Self-Assessment Guide for Information Technology Systems. NIST

TIPOS DE AUDITORIA

- **Auditoría forense:**
- En aquellos casos que existan sospechas de fraude o actuaciones ilegales, pueden realizarse investigaciones para obtener evidencia
- Se utilizan herramientas informáticas para recuperar datos de forma legal de equipos informáticos
- Este tipo de actuaciones se realiza, generalmente, por la policía, fiscalía o a instancia judicial.

- Auditoría de gestión:
  - **E**xamen de un sistema informático para evaluar si los objetivos previstos al implementar el sistema han sido alcanzados efectivamente, con criterios de economía y eficiencia.
- Auditorías sobre adquisición de equipos y sistemas:
  - Orientada a la compra de hardware, software, comunicaciones

- **Auditoría de seguridad informática:**
  - **A**uditoría de controles de seguridad en sistemas informáticos para evaluar la extensión en la que se mantiene la confidencialidad, integridad y disponibilidad de los datos
  - Considerando el perfil de riesgo de la entidad y de sus sistemas TI.
  - Descubre vulnerabilidades

- Auditoría de aplicaciones informáticas
  - El objetivo es evaluar el grado de confianza que puede depositarse en las transacciones procesadas y en los informes generados por el sistema.

FASES DE AUDITORIA

1. Evaluar el riesgo de manifestaciones erróneas significativas
2. Diseñar y ejecutar los procedimientos de auditoría precisos en respuesta a los riesgos evaluados y reducir el riesgo a un nivel aceptablemente bajo
3. Emitir un adecuado informe escrito basado en la evidencia de auditoría obtenida y en las incidencias de auditoría detectadas.

ETAPAS PRINCIPALES DE AUDITORIA

- **Exploración:**
  - Se realiza el estudio o examen previo al inicio de la Auditoria
  - Se busca conocer en detalle las características de la entidad a auditar.
  - Permite hacer la selección y las adecuaciones a la metodología y programas a utilizar
  - Determina la importancia de las materias que se habrán de examinar.
- **Planeamiento:**
  - Define la estrategia que se debe seguir
  - Define el tiempo a emplear en la ejecución de cada comprobación o verificación
  - El resultado es el plan global o general de la Auditoría.

- Contenidos del plan:
  - Definición de los temas y las tareas a ejecutar.
  - Nombre del o los especialistas que intervendrán en cada una de ellas.
  - Fecha prevista de inicio y terminación de cada tarea. Se considera desde la exploración hasta la conclusión del trabajo.
  - Igualmente se confecciona el plan de trabajo individual de cada especialista, considerando como mínimo:
    - Nombre del especialista.
    - Definición de los temas y cada una de las tareas a ejecutar.
    - Fecha de inicio y terminación de cada tarea.

- **Supervisión:**
  - El propósito es asegurar el cumplimiento de los objetivos de la Auditoría y la calidad razonable del trabajo
  - Debe garantizar el cumplimiento de las Normas de Auditoría
  - Que el informe final refleje correctamente los resultados de las comprobaciones, verificaciones e investigaciones realizadas.
- **Ejecución:**
  - El propósito de esta etapa es recopilar las pruebas que sustenten las opiniones del auditor en cuanto al trabajo realizado
  - Es el trabajo de campo, esta depende grandemente del grado de profundidad con que se hayan realizado las dos etapas anteriores
  - Se elaboran los Papeles de Trabajo y las hojas de nota, instrumentos que respaldan excepcionalmente la opinión del auditor

- **Informe:**
  - En esta etapa el Auditor se dedica a formalizar en un documento los resultados
  - La elaboración del informe final de Auditoría es una de las fases más importante y compleja de la Auditoría
- El informe de Auditoría debe cumplir con los principios siguientes:
  - Que se emita por el jefe de grupo de los auditores actuantes.
  - Por escrito.
  - Oportuno.
  - Que sea completo, exacto, objetivo y convincente, así como claro, conciso y fácil de entender.
  - Que todo lo que se consigna esté reflejado en los papeles de trabajo y que responden a hallazgos relevantes con evidencias suficientes
  - Que refleje una actitud independiente.
  - Que muestre la calificación según la evaluación de los resultados de la Auditoría.
  - Distribución rápida y adecuada.

- **Seguimiento:**
  - En esta etapa se siguen los resultados de una Auditoría
  - Pasado un tiempo aproximado de seis meses o un año se vuelve a realizar otra Auditoría de tipo recurrente para comprobar el verdadero cumplimiento de las deficiencias detectadas en la Auditoria.

Técnicas y Herramientas de trabajo

- Análisis de la información recabada del auditado.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.
- Muestreos.
- Cuestionarios.
- Cuestionario Checklist.
- Simuladores (Generadores de datos).
- Paquetes de auditoría (Generadores de Programas).

RIESGOS

- Cada ambiente de trabajo de IT es diferente
- El conjunto de riesgos es diferente en cada empresa
- No se pueden generalizar los riesgos para todas las empresas
- Existen muchas variables para el riesgo:
  - Grado de centralización
  - Número de servidores
  - Tipo de infraestructura
  - Grado de customización

  - Estructura organizacional del departamento de IT
  - Versiones de sistemas operativos y software en general
  - Si existe o no outsourcing
  - Políticas corporativas
  - Arquitectura de las aplicaciones
- Por lo tanto el plan de auditoría será desarrollado en función de cada realidad

- Evolución del riesgo
  - No es estático
  - Crece como la información de los sistemas
  - Se deberá replantear el plan cada cierto tiempo
- Tipos de riesgos relacionados:
  - Disponibilidad
  - Seguridad
  - Integridad
  - Confidencialidad
  - Efectividad
  - Eficiencia