Seguridad y Auditoría Informática

La Informática como Herramienta del Auditor

Objetivos

- Entender qué es Auditoría a través de los elementos que componen su concepto
- Diferenciar Consultoría de Auditoría
- Identificar las funciones del Control Interno y Auditoría Informática
    - Sus similitudes y diferencias

Concepto de Auditoría

Contenido	Una **opinión**
Condición	**Profesional**
Justificación	Sustentada en determinados **procedimientos**
Objeto	Información obtenida desde un cierto soporte
Finalidad	Determinar **fiabilidad**
Momento	A **posteriori**

Clases de Auditoría

Clase	Contenido	Objeto	Finalidad
Financiera	**Opinión**	Cuentas Anuales	Presentar realidad
Informática	**Opinión**	Sistemas de aplicación, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente y según normas establecidas
Gestión	**Opinión**	Dirección	Eficacia, eficiencia, rendimiento económico
Cumplimiento	**Opinión**	Normas establecidas	Las operaciones están alineadas a estas normas

Procedimientos

- Permiten fundamentar y justificar la opinión profesional
- Cada clase o tipo de auditoría tiene sus propios procedimientos y éstos definen el alcance de la auditoría
- Buscan garantizar que:
  - El trabajo se planificará y se supervisará adecuadamente
  - Se estudiará y evaluará el sistema de control interno
  - Se obtendrá evidencia suficiente y adecuada

Procedimientos - Riesgos

- Con los métodos tradicionales no fue posible verificar la totalidad de operaciones existiendo riesgo de que algunas irregularidades hayan escapado de la atención
- El auditor debe mantener este riesgo dentro de límites tolerables
- Este riesgo tiene dos componentes:
  - Errores de importancia producidos durante el proceso
  - Falta de detección de irregularidades en el examen del auditor
- Para mitigar este riesgo, el auditor debe confiar en:
  - El control interno de la entidad auditada
  - Sus pruebas de detalle y procedimientos

Variación del Objeto de Auditoría - CAATs

Ventajas Procedimientos **Automatizados** vs **Manuales**:

- Bajo Costo de Puesta en Marcha
- Bajo Costo de Operación
- Aumento del Rendimiento Continuo
- Excelente Consistencia

Ventajas de Procedimientos **Manuales** vs **Automatizados**:

- Mejor capacidad de reacción ante lo inesperado
- Incorporación del sentido común
- Mejor lenguaje para comunicar

Concepto de Consultoría

Contenido	Dar **asesoramiento** o **consejo**
Condición	De caracter **especializado**
Justificación	En base a un **examen** o **análisis**
Objeto	La **actividad** o **cuestión** sometida a consideración
Finalidad	Establecer **la manera de llevarla a cabo** adecuadamente
Momento	A **priori**

Control Interno y Auditoría Informática

Control Interno (1/4)

Para reforzar el Control Interno, las organizaciones deben recurrir a iniciativas como:

- Reingeniería de procesos
- Gestión de la calidad total
- Redimensionamiento del tamaño (downsizing, upsizing)
- Tercerización (outsourcing)
- Descentralización

Control Interno (2/4)

Control Interno Informático se ocupa de:

- Que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales
- Asesorar sobre el conocimiento de las normas
- Colaborar con los esfuerzos de Auditoría Informática y otras Auditorías Externas
- Definir, establecer y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático

Control Interno (3/4)

- Realiza en los diferentes sistemas (centrales, departamentales, redes locales, PC’s, etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes actividades operativas sobre:
  - El cumplimiento de procedimiento, normas y controles dictados, especialmente sobre el control de cambios y versiones del software
  - Controles sobre la producción diaria
  - Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del software y del servicio informático
  - Controles en las redes de comunicaciones
  - Controles sobre el software de base
  - Controles en los sistemas microinformáticos

Control Interno (4/4)

- La seguridad informática
  - Usuarios, responsables y perfiles de uso de archivos y bases de datos
  - Normas de seguridad
  - Control de información clasificada
- Licencias y relaciones contractuales con terceros
- Asesorar y transmitir cultura sobre el riesgo informático

Auditoría Informática (1/2)

- Es el proceso de recoger, agrupar y evaluar **evidencias** para determinar si un sistema informatizado protege los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos
- La auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría
- El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos
- El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implementados y sobre la fiabilidad de la información suministrada

Auditoría Informática (2/2)

- Se pueden establecer tres grupos de funciones a realizar por un auditor informático:
  - Participar en las revisiones durante y después del diseño, realización, implementación y uso de aplicaciones informáticas, así como en las fases análogas de realización de cambios importantes
  - Revisar y juzgar los controles implementados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes
  - Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información

Control Interno y Auditoría Informática: Campos Análogos

	Control Interno Informático	Auditoría Informática
Similitudes	• Personal Interno • Conocimientos Especializados en Tecnología de la Información • Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección General para los sistemas de información	
Diferencias	• Análisis de los controles en el día a día • Informa a la Dirección del Departamento de Informática • Sólo personal interno • El alcance de sus funciones es únicamente sobre el Departamento de Informática	• Análisis de un momento informático determinado • Informa a la Dirección General de la Organización • Personal interno y/o externo • Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización

Control Interno Informático

Cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos

Sistema de Control Interno Informático (1/6)

- Los objetivos de los controles informáticos se han clasificado en las siguientes categorías:
  - Controles preventivos
  - Controles detectivos
  - Controles correctivos

Sistema de Control Interno Informático (2/6)

- Para llegar a conocer la configuración del sistema es necesario documentar los detalles de la red, así como los distintos niveles de control y elementos relacionados:
  - Entorno de Red
  - Configuración de los Equipos
  - Entorno de Aplicaciones
  - Productos y Herramientas
  - Seguridad de los Equipos

Sistema de Control Interno Informático (3/6)

- Para establecer un sistema de controles internos informáticos habrá que definir:
  - Gestión de sistemas de información
  - Administración de sistemas
  - Seguridad
  - Gestión del cambio

Sistema de Control Interno Informático (4/6)

- Cada función de la organización juega un papel importante en las fases de establecimiento de una política y cultura sobre la seguridad:
  - Dirección de Negocio o Dirección de Sistemas de Información (S.I.)
  - Dirección de Informática

Sistema de Control Interno Informático (5/6)

Reforzando sobre Control Interno Informático

- Debe definir los diferentes controles periódicos a realizar en cada una de las funciones informáticas, conforme a los objetivos de negocio y dentro del marco legal aplicable
- Realizará periódicamente la revisión de los controles establecidos informando de las desviaciones a la Dirección de Informática y sugiriendo cuantos cambios serán convenientes en los controles, así como transmitirá constantemente a toda la organización de informática la cultura y políticas del riesgo informático

Sistema de Control Interno Informático (6/6)

Auditor Interno/externo informático

- Debe revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa, de acuerdo al nivel de riesgo, conforme a los objetivos definidos por la Dirección del Negocio y la Dirección de Informática
- Informará a la alta dirección de los hechos observados y al detectarse deficiencias o ausencias de controles recomendará acciones que minimicen los riesgos que pueden originarse

Controles Internos para Sistemas de Información

1. Controles generales organizativos
2. Controles de desarrollo, adquisición y mantenimiento de sistemas de información
3. Controles de uso de sistemas de información
4. Controles en aplicaciones
5. Controles específicos de ciertas tecnologías

Síntesis

- Auditoría
- Consultoría
- Control Interno
- Auditoría Informática

¿Preguntas?

¡Muchas Gracias!