¿Qué es la Auditoria en Sistemas de Información?

Es el examen objetivo, crítico, sistemático, posterior y selectivo que se hace a la administración informática de una organización, con el fin de emitir una opinión acerca de:

- La eficiencia en la adquisición y utilización de los recursos informáticos.
- La confiabilidad, la integridad, la seguridad y oportunidad de información.
- La efectividad de los controles en los sistemas de información

¿Qué es la Auditoria en Sistemas de Información?

Una auditoria de SI es diferente de una auditoria de estados financieros. Mientras que una auditoria financiera su propósito es evaluar si una organización está cumpliendo con las prácticas contables habituales, los efectos de una auditoria de SI deben evaluar el diseño del sistema de control interno y la eficacia.

Esto incluye pero no se limita a la eficiencia y protocolos de seguridad, los procesos de desarrollo o de supervisión de SI.

El objetivo es evaluar la capacidad de la organización para proteger sus activos de información y debidamente prescindir de la información a personas autorizadas.

¿Qué es la Auditoria en Sistemas de Información?

La auditoria de SI se centra en determinar los riesgos que son relevantes para los activos de información, y en la evaluación de los controles a fin de reducir o mitigar estos riesgos. Mediante la implementación de controles, el efecto de los riesgos se pueden minimizar, pero no puede eliminar por completo todos los riesgos.

Definición

La auditoría de SI, auditoría informática o auditoría de sistemas es un tipo de auditoría consistente en el examen de los sistemas de información y de los centros de proceso de datos, instalaciones y unidades informáticas de las organizaciones, con objeto de facilitar la consecución de los objetivos que persiguen, tanto los del área informática como, primordialmente los del conjunto de la organización .

Verificar la calidad de los sistemas de información de la organización y proponer mejoras de los mismos, coherentes con el proyecto de calidad adoptado por la organización (cumplimiento de normas de calidad o modelo de excelencia en gestión).

Definición

La auditoría de sistemas de información persigue propiciar con sus actuaciones:

- El establecimiento y mantenimiento de sistemas de gestión de la seguridad.
- La reducción de los riesgos inherentes a la utilización de los SI.
- El incremento de la confianza de los usuarios internos y externos en los sistemas de información.

Definición

- Comprobar el cumplimiento de los requerimientos de negocio de la información, es decir las propiedades que la información debe tener para optimizar su utilización por la organización.

- Analizar la gestión de los riesgos asociados a los sistemas de información, proponiendo la adopción de medidas que mejoren el sistema de análisis y gestión de los riesgos informáticos, o que conduzcan a que los riesgos sean mitigados, eliminados, compartidos o aceptados por la organización.

- Comprobar e impulsar la seguridad de los sistemas de información.

Principales razones para auditar y controlar los SI

- ✓ Toma de decisiones incorrectas
- ✓ Reducir el costo de los errores
- ✓ Control del uso de las TIC
- ✓ Consecuencias de las pérdidas de datos
- ✓ Valor del hardware, del software y del personal
- ✓ Privacidad de los datos personales
- ✓ Fraude informático

Función

- Velar por la eficacia y eficiencia del SI, de forma que éste alcance con el menor costo posible los objetivos.

- Verificar el cumplimiento de las normas y estándares vigentes en la organización (leyes de firma electrónica, de protección de datos de carácter personal, de propiedad intelectual del software, etc.).

- Supervisar el control interno ejercido sobre los SI conducente a la protección de los activos de información de información de la organización: recursos humanos, locales e instalaciones, infraestructuras tecnológicas, sistemas y aplicaciones, información tributaria.

¿Qué es la metodología de Auditoria de SI?

- Un camino estructurado de forma lógica para asegurar el éxito de proyectos de auditoría de informática.
- Un grupo de etapas que pueden adaptarse a empresas pequeñas, medianas y grandes de cualquier giro para planear y desarrollar proyectos de auditoría en informática.

Metodología y Estándares

- Utilización de metodologías, instrumentos y procedimientos operativos propios.
- En la planificación de las auditorías informáticas Empleo de marcos referenciales para la declaración de los objetivos del control.
- En el desarrollo de las auditorías informáticas empleo de herramientas de auditoría específicas.

Metodología y Estándares

Los organismos internacionales que se ocupan del control y de la auditoría de SI son fuente de fuente de estándares:

- ISACA - Asociación de Auditoría y Control de Sistemas de Información
- ISO – Organización Internacional para la estandarización.
- NIST – Instituto Nacional de Estándares y Tecnología de los Estados Unidos.

Metodología y Estándares

En la actualidad existen tres tipos de metodologías de auditoria informática:

- ✓ R.O.A. (RISK ORIENTED APPROACH), diseñada por Arthur Andersen.
- ✓ CHECKLIST o cuestionarios.
- ✓ AUDITORIA DE PRODUCTOS (por ejemplo, Red Local Windows NT; sistemas de Gestión de base de Datos DB2; paquete de seguridad RACF, etc.).

Metodología y Estándares

En sí las tres metodologías están basadas en la minimización de los riesgos, que se conseguirá en función de que existan los controles y de que éstos funcionen. En consecuencia el auditor deberá revisar estos controles y su funcionamiento.

Las metodologías de auditoría de SI son de tipo cualitativo/subjetivo. Se puede decir que son subjetivas por excelencia. Están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen en gran profesionalidad y formación continua.

Metodología y Estándares

Solo existen dos tipos de metodologías para la auditoria de SI

- ✓ Controles Generales.- Son el producto estándar de los auditores profesionales. El objetivo aquí es dar una opinión sobre la fiabilidad de los datos del computador para la auditoría financiera, es resultado es escueto y forma parte del informe de auditoría, en donde se hacen notar las vulnerabilidades encontradas. Están desprestigiadas ya que dependen en gran medida de la experiencia de los profesionales que las usan.

Metodología y Estándares

Solo existen dos tipos de metodologías para la auditoria de SI

- ✓ Metodologías de los auditores internos.- Están formuladas por recomendaciones de plan de trabajo y de todo el proceso que se debe seguir. También se define el objetivo de la misma, que habrá que describirlo en el memorando de apertura al auditado. De la misma forma se describe en forma de cuestionarios genéricos, con una orientación de los controles a revisar. El auditor interno debe crear sus metodologías necesarias para auditar los distintos aspectos o áreas en el plan auditor