TECNOLOGICO DE ESTUDIOS SUPERIORES DE COACALCO

INGENIERIA EN SISTEMAS COMPUTACIONALES

AUDITORIA INFORMATICA DE DESARROLLO DE PROYECTOS Y APLICACIONES

AUDITORÍA INFORMÁTICA

FRANCO CABRERA LUIS MAURICIO

ING. DOMINGUEZ CISNEROS DANIEL

Auditoría Informática

La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes. La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia. Los objetivos de la auditoria Informática son:

O El control de la función informática

O El análisis de la eficiencia de los Sistemas Informáticos

O La verificación del cumplimiento de la Normativa en este ámbito

O La revisión de la eficaz gestión de los recursos informáticos

La auditoría informática sirve para mejorar ciertas características en la empresa como:

O Desempeño

O Fiabilidad

O Eficacia

O Rentabilidad

O Seguridad

O Privacidad

Generalmente se puede desarrollar en alguna o combinación de las siguientes áreas:

O Gobierno corporativo

O Administración del Ciclo de vida de los sistemas

O Servicio de Entrega y Soporte

O Protección y Seguridad

O Planes de continuidad y Recuperación de desastres

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoria informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO e ITIL. Actualmente la certificación de ISACA para ser CISA Certified Information Systems Auditor es una de las más reconocidas y avaladas por los estándares internacionales ya que el proceso de selección consta de un examen inicial bastante extenso y la necesidad de mantenerse actualizado acumulando horas (puntos) para no perder la certificación.

Tipos de Auditoria Informática

Dentro de la auditoria informática destacan los siguientes tipos (entre otros):

Auditoria de la gestión: La contratación de bienes y servicios, documentación de los programas, etc.

Auditoria legal del Reglamento de Protección de Datos: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

Auditoria de los datos: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.

Auditoria de las bases de datos: Controles de acceso, de actualización, de integridad y calidad de los datos.

Auditoria de la seguridad: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

Auditoria de la gestión: La contratación de bienes y servicios, documentación de los programas, etc.

Auditoria de la seguridad física: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc) y protecciones del entorno.

Auditoria de la seguridad lógica: Comprende los métodos de autenticación de los sistemas de información.

Auditoria de las comunicaciones: SFrente a errores, accidentes y fraudes.

Auditoria de la seguridad en producción: Se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.

Principales pruebas y herramientas para efectuar una auditoria informática

En la realización de una auditoria informática el auditor puede realizar las siguientes pruebas:

Pruebas sustantivas: Verifican el grado de confiabilidad del SI del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.

Pruebas de cumplimiento: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Las principales herramientas de las que dispone un auditor informático son:

O Observación

O Realización de cuestionarios

O Entrevistas a auditados y no auditados

O Muestreo estadístico (Trazas y/o huellas)

O Flujogramas

O Listas de chequeo (checklist)

O Mapas conceptuales

O Inventario

Fases Auditoria Informática

Fase I: Conocimientos del Sistema

O Aspectos Legales y Políticas Internas

O Características del Sistema Operativo

O Características de la aplicación de computadora

Fase II: Análisis de transacciones y recursos

O Definición de transacciones

O Análisis de las transacciones

O Análisis de los recursos

O Relación entre transacciones y recursos

Fase II: Fase III: Análisis de riesgos y amenazas

O Identificación de riesgos

O Identificación de amenazas

O Relación entre recursos/amenazas/riesgos

Fase IV: Análisis de controles

O Codificación de controles

O Relación entre controles

O Análisis de cobertura de los controles requerid

Fase IV: Análisis de controles

O Objetivos de la evaluación

O Plan de pruebas de los controles

O Pruebas de controles

O Análisis de resultados de las pruebas

Fase VI: El informe de auditoria

O Informe detallado de recomendaciones

O Informe resumen para la alta gerencia

Fase VII: Seguimiento de las Recomendaciones

O Informes de seguimiento

O Evaluación de los controles implantados