AUDITORÍA INFORMÁTICA

Tipos de Auditorías

- ✓ Auditoría de Base de Datos
- ✓ Auditoría de Desarrollo
- ✓ Auditoría de Redes

Auditoría de Base de Datos

Esta se encarga de monitorear, medir, asegurar y registrar los accesos a toda la información almacenada en las bases de datos.

Participantes en esta auditoría

- ✓ Tecnología de información
- ✓ Auditores de sistemas
- ✓ Riesgo corporativo
- ✓ Cumplimiento corporativo
- ✓ Seguridad corporativa

Auditoría de Base de Datos

Objetivos principales

Esta auditoría se encarga de manera fundamental en la seguridad de las bases de datos. Entre sus objetivos se encuentran:

- ✓ Evitar el acceso externo
- ✓ Imposibilitar el acceso interno a usuarios no autorizados
- ✓ Autorizar el acceso solo a los usuarios autorizados

Auditoría de Base de Datos

Con esta auditoria se busca:

- ✓ Monitorear y mantener un registro del uso de los datos por los usuarios autorizados y no autorizados.
- ✓ Conservar trazas de uso y del acceso a las bases de datos.
- ✓ Permitir investigaciones
- ✓ Alertas en tiempo real

Auditoría de Base de Datos

Instrumentos de evaluación

Investigación Preliminar.

- ✓ Observar el inventario de recursos (Hardware, software) y la información requerida para apoyar el examen que el equipo de Auditoría va realizar. El resultado de todo esto se organiza en un archivo especial denominado archivo permanentemente o expediente continuo de Auditoría.
- ✓ Saber todo acerca del negocio y de los sistemas implementados, datos de la empresa, objetivo social, políticas e normas implementadas. Sin olvidar toda la información que corresponda al sistema de Bases de datos.

Auditoría de Base de Datos

Instrumentos de evaluación

Definir los grupos de riegos.

- ✓ Todos los escenarios de riesgo del sistema de bases de datos.
- ✓ Agrupación.

Evaluar el estado de control existente.

- ✓ Problemas por seguridad en instalaciones y el acceso físico
- ✓ Riesgo relacionado a los accesos lógicos y privacidad de las bases de datos
- ✓ Relación entre sistema operativo y DBMS
- ✓ Riesgo relacionado a las aplicaciones y utilitarios utilizados en la empresa

Auditoría de Base de Datos

Donde se debe aplicar esta auditoria ?

En toda empresa que conste con un Sistema de Base de Datos con información sumamente importante para su desarrollo y datos confidenciales de usuarios externos. Ejemplos: Bancos, Supermercados, Colegios y Universidades.

Auditoría de Desarrollo

Aplicando la división funcional al departamento de informática de cualquier entidad, una de las áreas que tradicionalmente aparece es la de desarrollo.

El desarrollo incluye todo el ciclo de vida del software excepto la explotación, el mantenimiento y el fuera de servicio de las aplicaciones cuando ésta tenga lugar.

Auditoría de Desarrollo

Importancia de la auditoría de desarrollo

- ✓ Los avances en tecnologías de las computadoras han hecho que actualmente el desafío más importante y el principal reto sea la calidad del software
- ✓ El gasto destinado a software es cada vez superior al que se dedica al hardware
- ✓ El software como producto es muy difícil de validar. Un mayor control en el proceso de desarrollo incrementa la calidad del mismo y disminuye los costos de mantenimiento.
- ✓ El índice de fracasos en proyectos de desarrollo es demasiado alto, lo cual denota la inexistencia o mal funcionamiento de los controles en este proceso.
- ✓ Las aplicaciones informáticas, que son el producto principal obtenido al final del desarrollo, pasan a ser la herramienta de trabajo principal de las áreas informatizadas, convirtiéndose en un factor esencial para la gestión y la toma de decisiones.

Auditoría de Desarrollo

Planteamiento y metodología

Para tratar la auditoría de desarrollo es necesario, en primer lugar, definir las funciones o tareas, las funciones que tradicionalmente se asignan al área son:

- ✓ Planificación del área y participación en la elaboración del plan estratégico de informática
- ✓ Desarrollo de nuevos sistemas
- ✓ Estudio de nuevos lenguajes, técnicas, metodologías, estándares, herramientas, etc.
- ✓ Establecimiento de un plan de formación para el personal adscrito al área
- ✓ Establecimiento de normas y controles para todas las actividades que se realizan en el área y comprobación de su observancia.

Auditoría de Desarrollo

Planteamiento y metodología

Una metodología aplicable es la propuesta por la ISACA (Asociación de Auditoría y Control de Sistemas de Información), que está basada en la evaluación de riesgos partiendo de los riesgos potenciales a los que está sometida una actividad (en este caso el desarrollo de un sistema de información), se determinan una serie de objetivos de control que minimicen esos riesgos.

Auditoría de Desarrollo

Etapas

Aprobación, planificación y gestión del proyecto.

El proyecto de desarrollo debe estar aprobado, definido y planificado formalmente.
Se debe comprobar que:

- ✓ Existe una orden de aprobación del proyecto firmada por un órgano competente.
- ✓ En el documento de aprobación están definidos de forma clara y precisa los objetivos del mismo y las restricciones.
- ✓ Se han identificado las unidades de la organización a las que afecta

Auditoría de Desarrollo

Etapas

Auditoría de la fase de análisis

En este módulo se identificarán los requerimientos del nuevo sistema. Se incluirán tanto los requerimientos funcionales como los no funcionales, distinguiendo para cada uno de ellos su importancia y prioridad.

Los usuarios y responsables de las unidades a las que afecte el nuevo sistema establecerán de forma clara los requerimientos del mismo.

Auditoría de la fase de diseño

En la fase de diseño se elaborará el conjunto de especificaciones físicas del nuevo sistema que servirán de base para la construcción del mismo.

A partir de las especificaciones funcionales, y teniendo en cuenta el entorno tecnológico, se diseñará la arquitectura del sistema y el esquema externo de datos.

Auditoría de Desarrollo

Etapas

Auditoría de la fase de construcción

En esta fase se programarán y probarán los distintos componentes y se pondrán en marcha todos los procedimientos necesarios para que los usuarios puedan trabajar con el nuevo sistema. Estará basado en las especificaciones físicas obtenidas en la fase de diseño.

En este módulo se realizarán los distintos componentes, se probarán tanto individualmente como de forma integrada, y se desarrollarán los procedimientos de operación.

Auditoría de la fase de implantación

En esta fase se realizará la aceptación del sistema por parte de los usuarios, además de las actividades necesarias para la puesta en marcha.

Se verificará en este módulo que el sistema cumple con los requerimientos establecidos en la fase de análisis. Una vez probado y aceptado se pondrá en explotación.

Auditoría de Redes

Mecanismos que prueban una red informática, evaluando la seguridad y su desempeño, para lograr mayor eficiencia y aseguramiento de la información

Metodología

- ✓ Estructura física(hardware, topología)
- ✓ Estructura lógica(software, aplicaciones)

Auditoría de Redes

Etapas

- ✓ Análisis de vulnerabilidades: Punto más crítico de toda la auditoría
- ✓ Estrategia de saneamiento: Identificar los agujeros en la red y proceder repáralos, actualizando el software afectado, reconfigurándolo de mejor manera o reemplazándolo por otro similar
- ✓ Plan de contención: Elaborar Plan B, que prevea un incidente después de tomadas las medidas de seguridad.
- ✓ Seguimiento Continuo del desempeño del sistema: La seguridad no es un producto, es un proceso.

Auditoría de Redes

Tipos

Auditoría de comunicaciones

- ✓ La gestión de redes: los equipos y su conectividad
- ✓ La monitorización de las comunicaciones
- ✓ La revisión de costes y la asignación formal de proveedores
- ✓ Creación y aplicabilidad de estándares

Auditoría de Redes

Tipos

Auditoría de Red Física

- ✓ Áreas de equipo de comunicación con control de acceso
- ✓ Protección y mantenimiento adecuado de cables y líneas de comunicación para evitar accesos físicos
- ✓ Utilización de equipos de prueba de comunicaciones para monitorizar la red y el tráfico de esta
- ✓ Recuperación del sistema
- ✓ Control de las líneas telefónicas
- ✓ Equipo de comunicación en lugares cerrados y de acceso limitado
- ✓ Seguridad física del equipo adecuada

Auditoría de Redes

Tipos

Auditoría de Red Lógica

- ✓ En líneas telefónicas: No debe darse el numero como público y tenerlas configuradas con retro-llamada, código de conexión o interruptores
- ✓ Contraseñas de acceso
- ✓ Una transmisión debe ser recibida solo por el destinatario
- ✓ Registrar actividades de los usuario en la red

¿Que busca la auditoria Aplicaciones ?

- Posibilidades de fallo:
  - Software
  - Hardware
  - Redes y telecomunicaciones
  - Software múltiple
  - Computador central
  - Dispositivos periféricos
  - Transmisión de datos
  - Servidores – Módems – líneas de comunicación
- Confidencialidad e integridad
  - Gran uso de internet en las aplicaciones

Auditoria de Aplicaciones

¿A que se aplica ?

- En Aplicaciones en funcionamiento en cuanto al grado de cumplimiento de los objetivos para los que fueron creadas

Objetivos de las aplicaciones

- Registro de las operaciones
- Procesos de cálculo y edición
- Almacenamiento de la información
- Dar respuesta a consultas de usuarios
- Generar informes de interés para la organización

Metodología para aplicarla

- Entrevistas
- Encuestas
- Observación del trabajo realizado por los usuarios con la aplicación
- Pruebas
  - De conformidad
  - De validación
- Uso del computador
  - GAS (web: herramientas de auditoría)
  - SQL / QBE

Observación del trabajo realizado por los usuarios

- Es conveniente observar como algún usuario hace uso de aquellas transacciones mas significativas por su volumen o riesgo.
- Este método es muy útil para el auditor, ya que deja ver que aunque una aplicación funcione bien; puede que no tenga el nivel óptimo de efectividad esperado.
- Es indispensable aprovechar estas observaciones para solicitar simulaciones de situaciones previsibles de error para comprobar si la respuesta del sistema es la esperada

Pruebas de conformidad

- Son actuaciones orientadas específicamente a comprobar que determinados procedimientos, normas o controles internos, particularmente los que merecen confianza de estar adecuadamente establecidos, se cumplen o funcionan de acuerdo con lo previsto y esperado.

- La evidencia de incumplimiento puede ser puesta de manifiesto a través de informes de excepción.

- Los testimonios de incumplimiento no implica evidencia pero, si parten de varias personas, es probable que la organización asuma como validos dichos testimonios

Pruebas substantivas o de validación

- Este tipo de pruebas están destinadas a detectar la presencia o ausencia de errores o irregularidades en procesos, actividades, transacciones o controles internos integrados en ellos
- Los siguientes son algunos de los tipos de errores que pueden ser considerados para este tipo de pruebas:

  - Transacciones omitidas
  - Duplicadas
  - Inexistentes indebidamente incluidas
  - Registradas sin contar con las autorizaciones establecidas
  - Incorrectamente clasificadas o contabilizadas en cuentas diferentes a las procedentes
  - Transacciones con información errónea, desde su origen o por alteración posterior

Uso del computador

- El uso del computador constituye una de las herramientas mas valiosas en la realización de la auditoria de una aplicación informática.
  - Computadores personales
  - Computador o computadores sobre los que se explota la aplicación objeto de auditoria
- Existen en el mercado infinidad de productos de software concebidos para facilitar la tarea del auditor.
- Se puede utilizar herramientas que no son necesariamente diseñadas para esta función pero de las cuales se pueden obtener resultados similares y que pueden estar disponibles en la organización como por ejemplo: Lenguaje SQL

Etapas de la auditoria de una aplicación informática

- Recogida de información y documentación sobre la aplicación
- Determinación de los objetivos y alcance de la auditoria
- Planificación de la auditoria
- Trabajo de campo, informe e implantación de mejoras
- Conclusiones

Auditoria de mantenimiento

- Su objetivo principal:
  - Darle seguimiento a los procesos que se realizan para el mantenimiento de sistemas informáticos, con esto se pretende que se establezcan estándares para el mantenimiento de los sistema y se cumplan al pie de la letra.

Indicadores utilizados para la auditoria de mantenimiento

- Tiempo Promedio Entre Fallas
- Tiempo Promedio Para Reparación
- Tiempo Promedio Para Falla
- Disponibilidad de equipos
- Tiempo Promedio de mantenimiento
- Progreso en los esfuerzos reducción costos
- Costo relativo con personal propio

Herramientas comunes

- Entrevistas
- Encuestas
- Observación del trabajo de los recursos informáticos que se están evaluando.
- Pruebas de efectividad de los recursos.

Pilares para determinar la madurez del mantenimiento

- Actitud de la gestión administrativa
- Estado organizacional
- Porcentaje de perdida de los recursos
- Solución de problemas
- Calificación y mantenimiento
- Sistema de informaciones
- Posición de la compañía

Grado de madurez del mantenimiento

- Nivel 1: Inconsciente
- Nivel 2: Despertando
- Nivel 3: Desarrollando
- Nivel 4: Capacitado
- Nivel 5: Consciente

Ejemplo de medición del grado de madurez

- Actitud de la gestión administrativa

- Nivel 1 Inconsciente: No comprende lo que es mantenimiento preventivo.
- Nivel 2 Despertando: Reconoce que el mantenimiento puede ser mejorado, sin embargo se siente incapacitado para implementar.
- Nivel 3 Desarrollando: Desarrolla mayor interés y seguridad.
- Nivel 4 Capacitando: Actitud participativa; reconoce que la gestión de mantenimiento es mandataria.
- Nivel 5 Consciente: Incluye el mantenimiento como una parte del sistema global de la compañía.