Auditoría Informática

Índice

- Concepto de auditoría
- Auditoría e Informática
- Metodología
- Áreas de la Auditoría Informática
  - Controles gerenciales
  - Controles de diseño, desarrollo y mantenimiento de sistemas
  - Control de operaciones
  - Controles de aplicación
  - Tecnología

Concepto de Auditoría

- Examen metódico de una situación relativa a un producto, proceso u organización, en materia de calidad, realizado en cooperación con los interesados para verificar la concordancia de la realidad con lo preestablecido y la adecuación al objetivo buscado

Concepto de Auditoría

- Actividad para determinar, por medio de la investigación, la adecuación de los procedimientos establecidos, instrucciones, especificaciones, codificaciones y estándares u otros requisitos, la adhesión a los mismos y la eficiencia de su implantación

Tipos de auditoría

- Auditoría financiera
- Auditoría organizativa
- Auditoría de gestión
- Auditoría informática

Auditoría Informática

- Es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control eficacia, seguridad y adecuación del servicio informático en la empresa, por lo que comprende un examen metódico, puntual y discontinuo del servicio informático, con vistas a mejorar en:
  - Rentabilidad
  - Seguridad
  - Eficacia

Requisitos auditoría informática

- Debe seguir una metodología preestablecida
- Se realizará en una fecha precisa y fija
- Será personal extraño al servicio de informática

Objetivos auditoría Interna

- Revisión y evaluación de controles contables, financieros y operativos
- Determinación de la utilidad de políticas, planes y procedimientos, así como su nivel de cumplimiento
- Custodia y contabilización de activos
- Examen de la fiabilidad de los datos
- Divulgación de políticas y procedimientos establecidos.
- Información exacta a la gerencia

Objetivos auditoría Externa

- Obtención de elementos de juicio fundamentados en la naturaleza de los hechos examinados
- Medición de la magnitud de un error ya conocido, detección de errores supuestos o confirmación de la ausencia de errores
- Propuesta de sugerencias, en tono constructivo, para ayudar a la gerencia
- Detección de los hechos importantes ocurridos tras el cierre del ejercicio
- Control de las actividades de investigación y desarrollo

Metodología

- Toma de contacto
  - Organización
  - Organigrama
  - Volumen
  - Situación en el mercado
  - Estructura del departamento
  - Relaciones funcionales y jerárquicas
  - Recursos
  - Aplicaciones en desarrollo
  - Aplicaciones en producción
  - Sistemas de explotación

Metodología (2)

- Planificación
  - Concentración de objetivos
  - Áreas que cubrirá
  - Personas de la organización que se involucrarán en el proceso de auditoría
  - Plan de trabajo
    - Tareas
    - Calendario
    - Resultados parciales
    - Presupuesto
    - Equipo auditor necesario

Metodología (3)

- Desarrollo de la auditoría
  - Entrevistas
  - Cuestionarios
  - Observación de las situaciones deficientes
  - Observación de los procedimientos
- Fase de diagnóstico
  - Meditación sin contacto con la empresa auditada
  - Factor decisivo será la experiencia del equipo auditor
  - Se deben definir los puntos débiles y fuertes, los riesgos eventuales y posibles tipos de solución y mejora

Metodología (4)

- Presentación de conclusiones
  - Se han de argumentar y documentar lo suficiente para que no puedan ser refutadas durante la discusión
  - Es especialmente delicada por el rechazo que puede provocar en la organización auditada. Se debe esmerar el tacto
  - En ocasiones serán necesarias tomar decisiones desagradables, pero es misión del auditor informar a la dirección de la forma más objetiva posible.

Metodología (5)

- Formación del plan de mejoras
  - Resumen de las deficiencias encontradas
  - Recogerá las recomendaciones encaminadas a paliar las deficiencias detectadas
  - Medidas a corto plazo: mejoras en plazo, calidad, planificación o formación
  - Medidas a medio plazo: mayor necesidad de recursos, optimización de programas o documentación y aspectos de diseño
  - Medidas a largo plazo: cambios en políticas, medios y estructuras del servicio

Área de planificación

- Toda organización se ordena mediante:
  - Plan estratégico
  - Plan táctico
  - Planes operacionales
- Objetivos de la auditoría informática
  - Qué planes del CPD están coordinados con los planes generales
  - Revisar los planes de informática
  - Contrastar su nivel de realización
  - Determinar el grado de participación y responsabilidad de directivos y usuarios en la planificación

Área de planificación

- Objetivos (cont.)
  - Participar en el proceso de planificación
  - Revisar los planes de desarrollo del software de aplicación
  - Revisar los procedimientos de planificación del software de base
  - Comprobar la ejecución del plan en cualquiera de sus niveles

Área de organización y admón

- Objetivos:
  - Revisión del organigrama del departamento y del general de la empresa
  - Comparar la estructura actual con la definida
  - Verificar los estándares de documentación
  - Determinar los procedimientos de dirección para hacer cumplir los criterios de documentación en P.D.
  - Confrontar las directrices sobre documentos con la realidad
  - Colaborar en la elaboración de nuevos documentos

Área de organización y admón

- Objetivos (cont)
  - Revisar la política personal: grado de cumplimiento de los procedimientos generales y nivel de sometimiento a la política personal
  - Evaluar la distribución de funciones
  - Examinar las políticas retributivas y los planes de formación
  - Verificar los métodos de análisis e imputación de costes
  - Confrontar presupuesto y realidad
  - Revisar todo tipo de contratos que afecten al CPD

Área de organización y admón

- Objetivos (cont)
  - Examinar los métodos de trabajo: análisis programación, pruebas,…
  - Evaluar el grado de participación de los usuarios
  - Evaluar el rendimiento de consultores externos
  - Conocer el grado de aceptación o satisfacción general con respecto al servicio informático
  - Revisar la documentación de usuario
  - Examinar los procedimientos usados para actualizar la documentación
  - Determinar el impacto de servicio de proceso de datos recibido desde fuentes externas

Área de organización y admón

- Objetivos
  - Evaluar el grado de conocimiento de los usuarios implicados sobre los sistemas automatizados

Área de sistemas

- Objetivos
  - Examinar la metodología de construcción que se esté utilizando
  - Revisar la definición de las grandes opciones que caracterizan al sistema
  - Examinar el inventario de problemas a resolver por el sistema, dictaminando sobre la prioridad y razonabilidad de éstos.
  - Verificar los medios que la organización ha dispuesto para la realización

Área de sistemas

- Objetivos
  - Comprobar el plan de realización
    - Tareas a emprender
    - Previsión de dificultades
    - Descomposición de problemas
    - Líneas de comportamiento a seguir
  - Garantizar la fiabilidad y precisión del estudio económico de costes preliminar a la realización
  - Verificar los estudios de necesidades de software y hardware asociados con el proyecto
  - Evaluar los métodos utilizados para la recogida de datos

Área de sistemas

- Objetivos
  - Colaborar en la fase de puesta en marcha del sistema
  - Comprobar los medios de seguridad con que se va a dotar al sistema en cuestión
  - Evaluar el rendimiento de un sistema ya en marcha
  - Aconsejar, si es necesario, las modificaciones oportunas para la optimización del sistema en funcionamiento.

Área de explotación

- Objetivos
  - Comprobar la existencia de normas generales escritas para el personal de explotación en lo que se refiere a sus funciones
  - Verificar la existencia de estándares de documentación en el departamento
  - Comprobar que en ningún caso los operadores acceden a documentación de programas que no sea la exclusiva para su explotación
  - Verificar que los usuarios no tienen acceso a la operación de la computadora cuando corren sus programas

Área de explotación

- Objetivos
  - Examinar que las versiones de programas y archivos activos en explotación son efectivamente las versiones que deben ser las vigentes
  - Como consecuencia de lo anterior, revisar que existen procedimientos que impidan que puedan correrse versiones de programas no activos
  - Investigar el diario de explotación y los archivos de log
  - Verificar los procedimientos según los cuales se incorporan nuevos programas a las librerías productivas

Área de explotación

- Objetivos
  - Examinar la adecuación de los locales en que se almacenan cintas y discos, así como la perfecta y visible identificación de estos medios
  - Investigar los estándares en tiempo d ejecución de la instalación, comparando éstos con las observaciones reales efectuadas.
  - Verificar los planes de mantenimiento preventivo de la instalación
  - Comprobar que existen normas escritas que regulen perfectamente todo lo relativo a copias de seguridad: manejo, autorización de obtención, destrucción, etc.

Área de explotación

- Objetivos (cont)
  - Inspeccionar el cumplimiento de sus funciones, además de la idoneidad de éstas, de la persona encargada de mantener la biblioteca de medios magnéticos
  - Comprobar que existen métodos adecuados que permitan verificar un seguimiento de los trabajos en la computadora
  - Examinar e incluso participar en la elaboración de los presupuestos del centro de explotación si éstos son independientes del resto del servicio informático

Entorno operativo hardware

- Objetivos
  - Determinar si el hardware se utiliza eficientemente
    - Revisar los informes de la dirección sobre uso del hw
    - Revisar si el equipo se utiliza par el personal autorizado
  - Examinar los estudios de adquisición, selección y evolución del hw
  - Comprobar las condiciones ambientales
  - Revisar el inventario hardware
  - Verificar los procedimientos de seguridad física
  - Examinar los controles de acceso físico

Entorno operativo hardware

- Objetivos (cont)
  - Revisar la seguridad física de los componentes de la red de teleproceso
  - Revisar los controles sobre la transmisión de los datos entre los periféricos y la computadora
  - Comprobar los procedimientos de prevención/detección/corrección frente a cualquier tipo de desastre
  - Colaborar en la confección de un plan de contingencias y desastres

Entorno operativo software

- Objetivos
  - Revisar la seguridad del software sobre archivos de datos y programas
  - Revisar las librerías utilizadas por los programadores
  - Examinar que los programas realizan lo que realmente se espera de ellos
  - Revisar el inventario de software
  - Comprobar la seguridad de datos y archivos
  - Examinar los controles sobre los datos
  - Revisar los procedimientos de entrada y salida
  - Verificar las previsiones y procedimientos de backup

Entorno operativo software

- Objetivos
  - Revisar los procedimientos de planificación, adecuación y mantenimiento del software del sistema
  - Revisar la documentación sobre sw base
  - Revisar los controles sobre programas producto
  - Examinar la utilización de estos paquetes
  - Verificar periódicamente el contenido de los archivos de usuario
  - Determinar que el proceso para usuarios está sujeto a los controles adecuados
  - Examinar los cálculos críticos

Entorno operativo software

- Objetivos
  - Supervisar el uso de las herramientas potentes al servicio de los usuarios
  - Comprobar la seguridad e integridad de las bases de datos

Medidas de seguridad a nivel básico

- Funciones y obligaciones del personal
- Registro de incidencias
- Identificación y autenticación:
  - inventario de usuarios
  - procedimiento de distribución y almacenamiento de contraseñas
- Control de acceso
  - basado en autorizaciones de usuarios, según autorización del responsable del fichero
- Gestión de soportes
  - control de almacenamiento y distribución
- Copias de respaldo y recuperación
  - copias de forma semanal
- Documento de seguridad

Medidas de seguridad a nivel medio

- Funciones y obligaciones del personal
  - **Responsable de seguridad**
- **Auditoría obligatoria de forma bi-anual**
- Registro de incidencias
  - **anotar restauraciones con pérdidas de datos**
  - **obligatoriedad de la autorización por escrito del responsable**
- Identificación y autenticación:
  - inventario de usuarios
  - procedimiento de distribución y almacenamiento de contraseñas
  - **detección de intrusiones y bloqueo de contraseñas**
- Control de acceso
  - basado en autorizaciones de usuarios, según autorización del responsable del fichero
  - **control de acceso físico**
- Gestión de soportes
  - control de almacenamiento y distribución
  - **registro de entrada y salida**
  - **inutilización de soportes obsoletos**
- Copias de respaldo y recuperación
  - copias de forma semanal
- **Pruebas con datos reales**
- Documento de seguridad

Medidas de seguridad a nivel alto

- Funciones y obligaciones del personal
  - *Responsable de seguridad*
- *Auditoría obligatoria de forma bi-anual*
- Registro de incidencias
  - *anotar restauraciones con pérdidas de datos*
  - *obligatoriedad de la autorización por escrito del responsable*
- Identificación y autenticación:
  - inventario de usuarios
  - procedimiento de distribución y almacenamiento de contraseñas
  - *detección de intrusiones y bloqueo de contraseñas*
- Control de acceso
  - basado en autorizaciones de usuarios, según autorización del responsable del fichero
  - *control de acceso físico*
  - **registro de accesos**
- Gestión de soportes
  - control de almacenamiento y distribución
  - *registro de entrada y salida*
  - *inutilización de soportes obsoletos*
  - **cifrado de soportes**
- Copias de respaldo y recuperación
  - copias de forma semanal
  - **almacenamiento en distinta ubicación**
- *Pruebas con datos reales*
- ***Cifrado de las comunicaciones***
- Documento de seguridad

Fin