Auditoría Informática

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 objetivos de la auditoría informática son (ver Figura 1):

- El control de la función informática
- El análisis de la eficiencia de los Sistemas Informáticos
- La verificación del cumplimiento de la Normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.

Figura 1 Objetivos de la auditoría informática.

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

- **Eficiencia:** se refiere a operar de modo que los recursos sean utilizados de forma adecuada, en otras palabras, es lograr las metas establecidas con la menor cantidad de recursos.

- **Eficacia:** es hacer lo necesario para alcanzar o lograr los objetivos propuestos. No se trata del proceso para obtener los resultados esperados sino del cumplimiento de las metas establecidas.

- **Rentabilidad:** es la capacidad que tiene algo, ya sea un producto, empresa o persona para generar suficiente utilidad o beneficio, es decir, un negocio es rentable cuando genera más ingresos que egresos.

- **Seguridad:** se trata del conjunto de protecciones a un bien determinado con el fin de preservar la confidencialidad, disponibilidad e integridad de los bienes de la empresa u organización.

Generalmente existen diversas formas de obtener un resultado determinado, y de esto se deriva la existencia de varias metodologías para llevar a cabo una auditoría informática. En general se siguen los siguientes pasos para llevar a cabo una auditoría:

1. **Planeación.** Ésta consiste en la elaboración de los programas de trabajo que se llevarán a cabo durante la revisión a la entidad auditada.

2. **Trabajos preliminares.** Consisten básicamente, de una serie de entrevistas con el cliente, las cuales tienen como objetivo dejar en claro las características básicas del trabajo que se va a realizar, qué es lo que quiere el cliente y que hará, en términos generales, el auditor.

3. **Diagnóstico administrativo.** El diagnóstico administrativo tiene por objetivo, proporcionar una panorámica de cómo la empresa percibe y practica la administración.

4. **Investigación previa.** Aquí se dará a conocer la empresa y de ser posible se validará la problemática que fue expuesta por el cliente. Después de esta fase se estará en posibilidades de hacer una mejor estimación del tiempo y de los honorarios, si es que no se pudo hacer en la primera fase.

5. **Elaboración del programa de la AI.** Todo buen administrador debe planear sus actividades y el auditor no debe ser la excepción, el programa señala las actividades que han de realizarse, fechas de inicio y término, así como los tiempos.

6. **Obtención de la Información.** En esta fase se obtendrá toda la información pertinente sobre el caso estudiado, pudiendo recurrir a herramientas como: entrevistas, encuestas, observación, etcétera, dependiendo del tipo de información que se requiera.

7. **Análisis, clasificación y evaluación de la información.** Se llevará a cabo de la siguiente forma:

    - El análisis y clasificación de la información podrá realizarse por métodos estadísticos
    - Evaluación: es aquí en donde se pone a prueba el talento del auditor, para entender e interpretar la información y continuar con el siguiente paso.

8. **Informe, elaboración y presentación del informe final.** Deberá contener los siguientes aspectos:

    - En él se informará de manera clara y concisa, sobre los resultados de la AI. No debe olvidarse que a los ojos del cliente él paga por recibir un informe, y en él debe encontrar valiosas recomendaciones que habrán de mejorar su administración., el informe aunque es escrito, debe presentarse apoyado en una exposición verbal.

    - Implementación y seguimiento: Algunos autores consideran esta fase como opcional, que no corresponde al auditor realizarla, sino a la empresa, se considera que el auditor debe participar, para que se interpreten correctamente sus recomendaciones y no haya lugar a desvíos en las mismas.

El método de trabajo del auditor pasa por las siguientes etapas:

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.

Plan de contingencias informático

Un plan de contingencias de seguridad informática contiene los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema y por lo general, contar con reemplazos de dichos sistemas.

Las causas pueden ser variadas y pasan por un problema informático, una falla en la correcta circulación de la información o la falta de provisión de servicios básicos tales como energía eléctrica, gas, agua y telecomunicaciones.

El hecho de preparar un plan de contingencia no implica un reconocimiento de la ineficiencia en la gestión de la empresa, sino todo lo contrario, supone un importante avance a la hora de superar todas aquellas situaciones descritas con anterioridad y que pueden provocar importantes pérdidas, no sólo materiales sino aquellas derivadas de la paralización del negocio durante un período más o menos largo.

A medida que las empresas se han vuelto cada vez más dependientes de las computadoras y las redes para manejar sus actividades, la disponibilidad de los sistemas informáticos se ha vuelto crucial. Actualmente, la mayoría de las empresas necesitan un nivel alto de disponibilidad y algunas requieren incluso un nivel continuo de ésta, ya que les resultaría extremadamente difícil funcionar sin los recursos informáticos.

Los procedimientos manuales, si es que existen, sólo serían prácticos por un corto periodo. En caso de un desastre, la interrupción prolongada de los servicios de computación puede llevar a pérdidas financieras significativas, sobre todo si está implicada la responsabilidad de la gerencia de informática. Lo más grave es que se puede perder la credibilidad del público o de los clientes y, como consecuencia, la empresa puede terminar en un fracaso total.

Diseñar e implementar un plan de contingencia para recuperación de desastres no es una tarea fácil; puede implicar esfuerzos y gastos considerables, sobre todo si se está partiendo de cero. Una solución comprende las siguientes actividades:

1. Debe ser diseñada y elaborada de acuerdo con las necesidades de la empresa.

2. Puede requerir la construcción o adaptación de un sitio para los equipos computacionales.

3. Requerirá del desarrollo y prueba de muchos procedimientos nuevos, y éstos deben ser compatibles con las operaciones existentes. Se hará participar a personal de muchos departamentos diferentes, el cual debe trabajar en conjunto cuando se desarrolle e implemente la solución.

4. Implicará un compromiso entre costo, velocidad de recuperación, medida de la recuperación y alcance de los desastres cubiertos. .

Como con cualquier proyecto de diseño, un método estructurado ayuda a asegurar que se toman en cuenta todos estos factores y que se les trata adecuadamente.

A continuación se muestran las principales actividades requeridas para la planificación e implementación de una capacidad de recuperación de desastres.

1. Identificación de riesgos.
2. Evaluación de riesgos.
3. Asignación de prioridades a las aplicaciones.
4. Establecimiento de los requerimientos de recuperación.
5. Elaboración de la documentación.
6. Verificación e implementación del plan.
7. Distribución y mantenimiento del plan. (Ver figura 2)

Figura 2 Actividades principales de un plan de contingencia.

Un plan de contingencias se encuentra constituido por dos tipos de procedimientos:

a) **Preventivos:** se llevan a cabo de manera periódica y se realiza para evitar posibles vulnerabilidades no detectadas al principio del proyecto o para evitar ataques futuros.

   Se relaciona con actividades simples como actualizar antivirus, limpieza física del equipo, etcétera.

b) **Correctivos:** se llevan a cabo después de un ataque para cerrar las puertas por donde éste se realizó o también se puede realizar la corrección una vez que se han detectado fallas en la seguridad del sistema o de la organización.

Otra clasificación de plan de contingencias se lista a continuación:

a) **Planificados:** se sabe con antelación lo que debe hacerse, de modo que cuando la situación ocurre se dispone de personal, manuales y recursos para corregirla.

b) **No planificados:** el correctivo de emergencia deberá actuar lo más rápidamente posible con el objetivo de evitar costos y daños mayores.

En un plan contra desastre que permite la continuación o el reinicio de las operaciones si presentan algún problema, se observan las siguientes ventajas:

- Reduce al mínimo los daños que cualquier eventualidad pueda producir.
- Permite alcanzar una normalización de las actividades normales de la organización en un menor tiempo.
- Implica menores pérdidas tanto económicas, materiales, personales así como de imagen para la empresa.
- Estimula la creación de una cultura de seguridad informática, así como fomentar la ética entre el personal de la empresa.

Asimismo contar con un plan de contingencia presenta la siguiente desventaja para una empresa u organización:

- Implica la inversión de tiempo y dinero ya que es necesario definir los requerimientos mínimos de seguridad en cada área, dependiendo del tipo de información que se procese y de los activos que se quieren proteger. Por lo que será necesario asignar recursos para realizar dichas actividades.