Seguridad y Auditoría Informática

Auditoría de la Dirección de Informática y Área de Desarrollo

Auditoría de la Dirección de Informática

Proceso de Dirección Informática

Es necesaria la evaluación independiente de la función que gestiona las tecnologías de la información.

Las actividades básicas del proceso de dirección son:

- Planificar
- Organizar
- Dirigir
- Controlar

Planificar

Tiene como objetivo prever la utilización de tecnologías de información.

El plan principal se denomina **Plan Estratégico de Sistemas de Información**.

- Debe estar alineado con los objetivos de la empresa.
- **No** es responsabilidad exclusiva de la Dirección de Informática, aunque ésta debe impulsar una planificación adecuada y a tiempo.
- El entorno de la empresa define el plazo del plan. Por lo general, es de **3 a 5 años**.

Planificar – Otros Planes Relacionados

Plan Operativo Anual

- Sistemas de información a desarrollar
- Cambios tecnológicos previstos
- Recursos y plazos necesarios

Plan de Dirección Tecnológica

Plan de Arquitectura de la Información

Plan de Recuperación ante Desastres

Organizar y Dirigir

Se organiza para estructurar los recursos, flujos de información y controles para alcanzar los objetivos propuestos en la planificación.

Se establece el **Comité de Informática**, impulsado por la Dirección de Informática, como lugar de encuentro entre los informáticos y los usuarios.

- Presidido por el director con mayor experiencia dentro de la empresa
- Las grandes áreas usuarias deberían estar representadas al nivel de sus directores
- El director de Auditoría Interna debería ser miembro del Comité

Organizar y Dirigir – Funciones del Comité de Informática

- **Aprobación** del Plan Estratégico de Sistemas de Información
- Aprobación de las grandes inversiones en tecnología de la información
- Fijación de prioridades entre los grandes proyectos informáticos
- Vehículo de discusión entre la Informática y sus usuarios
- Vigila y realiza el seguimiento de la actividad del Departamento de Informática

Posición del Departamento de Informática en la Empresa

Lo suficientemente alto en la jerarquía y contar con masa crítica suficiente.

Suele depender de la Dirección General. En grandes organizaciones, el Director de Informática es miembro del Comité de Dirección.

El auditor evalúa la equidad de trato a los diferentes departamentos de la empresa.

Descripción de Funciones y Responsabilidades del Departamento de Informática

Segregación de Funciones: funciones descritas y sus responsabilidades claramente delimitadas y documentadas. Evita que un individuo pueda trastornar un proceso crítico.

Aseguramiento de la Calidad: función organizativa de Aseguramiento de la Calidad independiente. Responde directamente a la Dirección de Informática.

Estándares de Funcionamiento y Procedimientos. Descripción de los Puestos de Trabajo.

Deben existir estándares de funcionamiento y procedimientos que gobiernen la actividad del Departamento de Informática y sus relaciones con los departamentos usuarios.

Deben estar documentados, actualizados y ser comunicados adecuadamente a todos los departamentos afectados.

Deben existir descripciones documentadas de los puestos de trabajo dentro de Informática.

Gestión Económica

Presupuestación: El Departamento de Informática debe tener un presupuesto económico, normalmente en base anual.

Adquisición de bienes y servicios: Los procedimientos que el Departamento de Informática siga para adquirir los bienes y servicios deben estar documentados y alineados con los procedimientos de compras del resto de la empresa.

Medida y reparto de costos: La Dirección de Informática debe en todo momento gestionar los costos asociados con la utilización de los recursos informáticos: humanos y tecnológicos.

Controlar

Control y Seguimiento: La Dirección tiene la obligación de controlar y efectuar un seguimiento permanente de las distintas actividades del Departamento.

Cumplimiento de la normativa legal: La Dirección de Informática debe controlar que la realización de sus actividades se lleva a cabo dentro del respeto a la normativa legal aplicable.

Auditoría del Área de Desarrollo

Funciones del Área de Desarrollo

- 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. relacionados con el desarrollo y adopción de los mismos.
- Establecimiento de un plan de formación para el personal asignado al área.
- Establecimiento de normas y controles para todas las actividades que se realizan en el área y comprobación de su cumplimiento.

Planteamiento y Metodología

Se abordará la auditoría del área en dos grandes apartados:

- Auditoría de la organización y gestión del área de desarrollo.
- Auditoría de proyectos de desarrollo de sistemas de información.

Se aplicará la metodología propuesta por ISACA basada en la evaluación de riesgos.

A través de las pruebas, se determinará cuáles son los riesgos no cubiertos, en qué medida lo son y qué consecuencias se pueden derivar de esa situación.

Auditoría de la Organización y Gestión del Área de Desarrollo

Objetivos de Control (1/2):

1. El área de desarrollo debe tener funciones asignadas dentro del departamento y una organización que le permita el cumplimiento de las mismas.

2. El personal del área de desarrollo debe contar con la formación adecuada y estar motivado para la realización de su trabajo.

3. Si existe un plan de sistemas, los proyectos que se lleven a cabo se basarán en dicho plan y lo mantendrán actualizado.

4. La propuesta y aprobación de nuevos proyectos debe realizarse siguiendo reglas preestablecidas.

Auditoría de la Organización y Gestión del Área de Desarrollo

Objetivos de Control (2/2):

5. La asignación de recursos a los proyectos debe basarse en reglas preestablecidas.

6. El desarrollo de sistemas de información debe hacerse aplicando principios de ingeniería del software ampliamente aceptados.

7. Las relaciones con el exterior del departamento tienen que producirse de acuerdo a un procedimiento.

8. La organización del área debe estar siempre adaptada a las necesidades de cada momento.

Auditoría de Proyectos de Desarrollo de S.I. (Fases)

La auditoría de un proyecto de desarrollo se puede hacer en dos momentos distintos: a medida que avanza el proyecto y una vez concluido.

Las fases a auditar serán:

- Aprobación, Planificación y Gestión del Proyecto
- Auditoría de la Fase de Análisis
- Auditoría de la Fase de Diseño
- Auditoría de la Fase de Construcción
- Auditoría de la Fase de Implementación

Aprobación, Planificación y Gestión del Proyecto

Objetivos de Control:

1. El proyecto de desarrollo deberá estar aprobado, definido y planificado formalmente.

2. El proyecto se debe gestionar de forma que se consigan los mejores resultados posibles teniendo en cuenta las restricciones de tiempo y recursos.

Auditoría de la Fase de Análisis

La fase de análisis pretende obtener un conjunto de especificaciones formales que describan las necesidades de información que deben ser cubiertas por el nuevo sistema de forma independiente del entorno técnico. Esta fase se divide en dos módulos.

- **Análisis de Requisitos del Sistema (ARS)**: En este módulo se identificarán los requisitos del nuevo sistema, tanto los funcionales como los no funcionales, se determinarán las posibles soluciones y se elegirá la más adecuada.

- **Especificación Funcional del Sistema (EFS)**: Se elaborará una especificación funcional detallada del sistema que sea coherente con lo que se espera de él.

Análisis de Requisitos del Sistema (ARS)

Objetivos de Control:

1. Los usuarios y responsables de las unidades a las que afecta el nuevo sistema establecerán de forma clara los requisitos del mismo.

2. En el proyecto de desarrollo se utilizará la alternativa más favorable para conseguir que el sistema cumpla los requisitos establecidos.

Especificación Funcional del Sistema (EFS)

Objetivos de Control:

1. El nuevo sistema debe especificarse de forma completa desde el punto de vista funcional, contando esta especificación con la aprobación de los usuarios.

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. Hay un único módulo.

- **Diseño Técnico del Sistema (DTS)**

Diseño Técnico del Sistema (DTS)

Objetivos de Control:

1. Se debe definir una arquitectura física para el sistema coherente con la especificación funcional que se tenga y con el entorno tecnológico elegido.

Auditoría de la Fase de Construcción

En esta fase se desarrollarán 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. Tiene dos módulos:

- **Desarrollo de Componentes del Sistema (DCS)**
- **Desarrollo de Procedimientos de Usuario (DPU)**

Desarrollo de Componentes del Sistema (DCS)

Objetivos de Control:

1. Los componentes o módulos deben desarrollarse usando técnicas de programación correctas.

Desarrollo de Procedimientos de Usuario (DPU)

Objetivos de Control:

1. Al término del proyecto, los futuros usuarios deben estar capacitados y disponer de todos los medios para hacer uso del sistema.

Auditoría de la Fase de Implementación

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

- **Pruebas, Implementación y Aceptación del Sistema (PIA)**

Pruebas, Implementación y Aceptación del Sistema (PIA)

Objetivos de Control:

1. El sistema debe ser aceptado formalmente por los usuarios antes de ser puesto en funcionamiento.

2. El sistema se pondrá en funcionamiento formalmente y pasará a estar en mantenimiento sólo cuando haya sido aceptado y esté preparado todo el entorno en el que se ejecutará.

¿Preguntas?

¡Muchas Gracias!