UNIDAD II. CONCEPTOS Y DEFINICIONES DEL CONTROL INTERNO INFORMATICO

1.- Conceptos y definiciones de Control Interno

Es un proceso llevado a cabo por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos relacionados con las operaciones, la información y el cumplimiento. Los controles internos son responsabilidad de todos los que trabajan en la organización, pero para que los controles sean eficaces, deben ser aplicados por la alta dirección. Los controles internos pueden ayudar a la organización a evitar riesgos y a avanzar hacia la consecución de sus objetivos y su misión. Los controles internos proporcionan una garantía razonable sobre la eficacia y la eficiencia de las operaciones, la fiabilidad de los informes financieros y el cumplimiento de las leyes y reglamentos.

Un sistema de control interno ayuda al consejo de administración y a la alta dirección de una organización a identificar, evaluar y mitigar los distintos tipos de riesgos y amenazas que pueden surgir en el cumplimiento de los objetivos empresariales. Los riesgos a los que puede estar expuesta una organización incluyen los riesgos operativos, los riesgos de cumplimiento y los riesgos financieros. Estos riesgos pueden estar relacionados con diferentes departamentos, funciones o unidades de una organización.

Conceptos básicos:

- **Entorno de control:** Es el conjunto de normas, procesos y estructuras que constituyen la base sobre la que desarrollar el control interno de la organización. Incluye la integridad y los valores éticos de la organización; los parámetros que permiten al consejo llevar a cabo sus responsabilidades de supervisión del gobierno

corporativo; la estructura organizacional y la asignación de autoridad y responsabilidad; el proceso de atraer, desarrollar y retener a profesionales competentes; y el rigor aplicado a las medidas de evaluación del desempeño, los esquemas de compensación para incentivar la responsabilidad por los resultados del desempeño.

- **Actividades de control:** Son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos con impacto potencial en los objetivos. Se ejecutan en todos los niveles de la entidad, en las diferentes etapas de los procesos de negocio y en el entorno tecnológico. Según su naturaleza, pueden ser preventivas o de detección y pueden abarcar una amplia gama de actividades manuales y automatizadas, tales como autorizaciones, verificaciones, conciliaciones y revisiones del desempeño empresarial.
- **Procesos de control:** Representan las políticas, procedimientos (manuales y automáticos) y actividades, que forman parte de un marco de control, diseñados y operados para asegurar que los riesgos estén contenidos dentro del nivel de tolerancia establecido por el proceso de evaluación de riesgos que una organización está dispuesta a aceptar.
- **Control a nivel de entidad:** Un control que opera en toda una entidad y, como tal, no está sujeto ni asociado con procesos individuales.
- **Controles a nivel de actividad:** Controles que operan para toda la actividad (área, proceso o programa). Algunos ejemplos son la revisión de los informes de los centros de costos, los recuentos de inventario y los controles suaves que influyen en el entorno de minicontrol dentro de la actividad, que puede o no ser coherente con el de la organización en su conjunto.
- **Control a nivel de proceso:** Una actividad que opera dentro de un proceso específico con el propósito de alcanzar los objetivos definidos a nivel de proceso.
- **Controles a nivel de transacción:** Controles que operan dentro del sistema de proceso de una transacción. Algunos ejemplos son las autorizaciones, la segregación de funciones e informes de excepción.
- **Control adecuado:** Es el que está presente si la dirección ha planificado y organizado (diseñado) las operaciones de manera tal que proporcionen un aseguramiento razonable de que los objetivos y metas de la organización serán alcanzados de forma eficiente y económica.
- **Control clave:** Controles que deben operar de manera efectiva para reducir a un nivel aceptable un riesgo crítico o significativo.
- **Controles compensatorios:** Una actividad que, si los controles clave no funcionan de forma totalmente eficaz, puede ayudar a reducir el riesgo relacionado. Dichos controles también pueden respaldar o duplicar múltiples controles y pueden operar a través de múltiples procesos y riesgos. Un control de compensación, por sí solo, no reducirá el riesgo a un nivel aceptable.
- **Control de detección:** Una actividad que está diseñada para descubrir eventos indeseables que ya han ocurrido. Un control de detección debe ocurrir en el

momento oportuno (antes de que el evento indeseable haya tenido un impacto negativo en la organización) para que se considere efectivo.

- **Control preventivo:** Una actividad que está diseñada para contrarrestar que eventos no deseados ocurran.
- **Control directivo:** Un control que provoca o causa la ocurrencia de un evento deseable. Algunos ejemplos son las guías, los programas de capacitación y los planes de compensación e incentivo. También se incluye en esta categoría los controles suaves como el tono en la parte superior o cumbre.
- **Controles suaves o blandos:** Elementos intangibles e inherentemente subjetivos del control interno, tales como el tono en la parte superior o cumbre, la integridad y los valores éticos, la filosofía gerencial y el estilo operativo.
- **Controles duros:** Elementos tangibles del control interno, tales como políticas y procedimientos, conciliaciones contables y firmas gerenciales.

3 objetivos del control interno empresarial:

En primer lugar, un control interno se divide en tres tipos de objetivos:

- Objetivos operacionales. Buscan la eficiencia y eficacia de las operaciones y están relacionados directamente con el rendimiento y la rentabilidad de la empresa.
- Objetivos financieros. Mantienen en orden los estados financieros para gozar de equilibrio financiero y buscan evitar pérdidas, falsificaciones o fraudes.
- Objetivos de cumplimiento. Estos objetivos están enfocados en el tema legal; es decir, al acatamientos de leyes, normas, disposiciones y regulaciones que la empresa debe cumplir.

En conjunto, cumplen las siguientes funciones:

- Asegurar la adherencia de las políticas internas establecidas.
- Promover y asegurar la eficiencia de las operaciones.
- Asegurar la confiabilidad e integridad de la información generada en la empresa.
- Proteger adecuadamente los activos y recursos de la compañía.

Una vez entendidos los objetivos del control interno, demos paso a conocer un poco más de su estructura y todos aquellos elementos y aspectos vitales que deben incorporarse para que funcione de manera correcta.

Componentes del control interno:

Entender los componentes del control interno de una empresa te permitirá diseñar, implementar y operar efectivamente los controles en los procesos de tu negocio.

- Ambiente de control interno: La estructura del control interno de una empresa comienza por el ambiente de control interno, que es la actitud de una compañía frente a los procesos de auditoría y a los controles en el interior de la empresa. Existen varios elementos que debe tener un ambiente de control interno: la filosofía de la administración frente a la gestión de riesgo, el nivel de apetito al riesgo, un directorio comprometido, la integridad y los valores éticos, una estructura organizacional sólida y una adecuada asignación de funciones. Incluso, los sistemas mejor diseñados para gestionar el riesgo pueden fallar cuando la organización no cuenta con políticas estructuradas que establezcan directrices claras.
- Evaluación de riesgo: Entre los componentes del control interno de una empresa se encuentra la evaluación de riesgo. Esta consiste en la identificación de puntos claves en los procesos de la compañía en los que es fundamental llevar a cabo un control exhaustivo. Aquí el oficial de cumplimiento debe preguntarse qué es lo que está saliendo mal para completar un análisis formal de la evaluación de riesgo, además, debe examinar en detalle las diferentes fases del negocio. Esto se puede hacer a través de diagramas de flujo y de la descripción minuciosa, uno a uno, de los procesos de la empresa.
- Información y comunicación: La información y la comunicación forman parte de las características del control interno de una empresa. Ambos conceptos aluden al proceso de recopilar y distribuir información relacionada con los mecanismos de control a través de todas las dependencias de la entidad. Este proceso se hace efectivo cuando incluye sistemas de información que transmiten a cada funcionario las nociones básicas del manejo interno de los proyectos y de los procesos. La información y comunicación comprende los manuales, el entrenamiento grupal, las campañas de divulgación y todas las maneras de difundir las actividades de control dentro de la compañía.

- Monitoreo: Otro de los componentes del control interno de una empresa es el monitoreo, que se refiere al mecanismo de auditoría por medio del cual se detectan fallas, se comprueba que los sistemas de control interno estén efectivamente diseñados y que continúen operando de manera adecuada. Un monitoreo apropiado pone a prueba las actividades y los procesos de control existentes para hacerles seguimiento a los cambios del negocio. El monitoreo implica también contar con un proceso para comunicar de manera oportuna cuáles controles no están siendo efectivos. De esta manera los miembros de la compañía pueden entender a tiempo cuándo se debe cambiar el rumbo.
- Control de las actividades: Esta característica del control interno comprende las actividades que realiza el personal de una compañía para asegurarse de que los controles están surtiendo efecto. Estas actividades están diseñadas para abordar los eventos que se encontraron al evaluar el riesgo, para luego implementar las mejoras y monitorear su funcionamiento.

2.- Control Interno Informático

Los controles internos de seguridad tienen por finalidad garantizar que todos los activos, sistemas, instalaciones, datos y archivos relacionados con el uso de la Tecnología de Información se encuentran protegidos contra accesos no autorizados, daños eventuales y uso indebido o ilegal que se encentran operables, seguros y protegidos en todo momento. La seguridad informática tiene el propósito de proteger la información de una amplia gama de amenazas para garantizar la continuidad del negocio, minimizar el costo de posibles daños para el giro del negocio y maximizar el retorno de las inversiones a la par que provee de competitividad para aprovechar oportunidades a través de un mejor posicionamiento competitivo.

El control interno informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la dirección de la organización y/o la dirección informática, así como los requerimientos legales. La función del control interno informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas. Control interno informático suele ser un órgano *staff* de la dirección del departamento de informática y está dotado de las personas y medios materiales proporcionados a los cometidos que se le encomienden.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realicen cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoria informática, así como de las auditorias externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los graso adecuados del servicio informático, lo cual no debe considerarse como que la implantación de los mecanismos de medida y responsabilidad del logro de esos niveles se ubique exclusivamente en la función de control interno, si no que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los eficazmente los fines de la organización y utiliza eficiente mente los recursos.

TIPO DE CONTROLES INTERNOS

Los controles internos se clasifican en los siguientes:

❖ Controles preventivos: Para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.

❖ Controles detectivos: Cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones.etc.

❖ Controles correctivos: Facilitan la suelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

La clasificación de los controles de acuerdo a lo que protegen es:

❖ Controles lógicos: Son aquellos basados en un software o parte de él, que nos permitirán:
  - ✓ Identificar los usuarios de ciertos datos y/o recursos: Hacer una clasificación de tipos de usuarios y sus objetivos de acceso a los sistemas.
  - ✓ Restringir el acceso a datos y recursos de los sistemas: Establecer los permisos por tipo de usuario.
  - ✓ Producir pistas para posteriores auditorias: Todos los movimientos hechos por los usuarios deben ser registrados y guardados a modo de historia de lo que ha ocurrido.

- Controles físicos: Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Según sea la herramienta utilizada:

- Controles manuales: que son ejecutados por el personal del área usuaria ó de informática, sin la utilización de herramientas computacionales
- Controles Automáticos: que son generalmente los incorporados en el software, ya se trate de software de base, software de comunicación, software de gestión de base de datos ó software de aplicación, entre otros.

Implantación de un sistema de Control interno informático

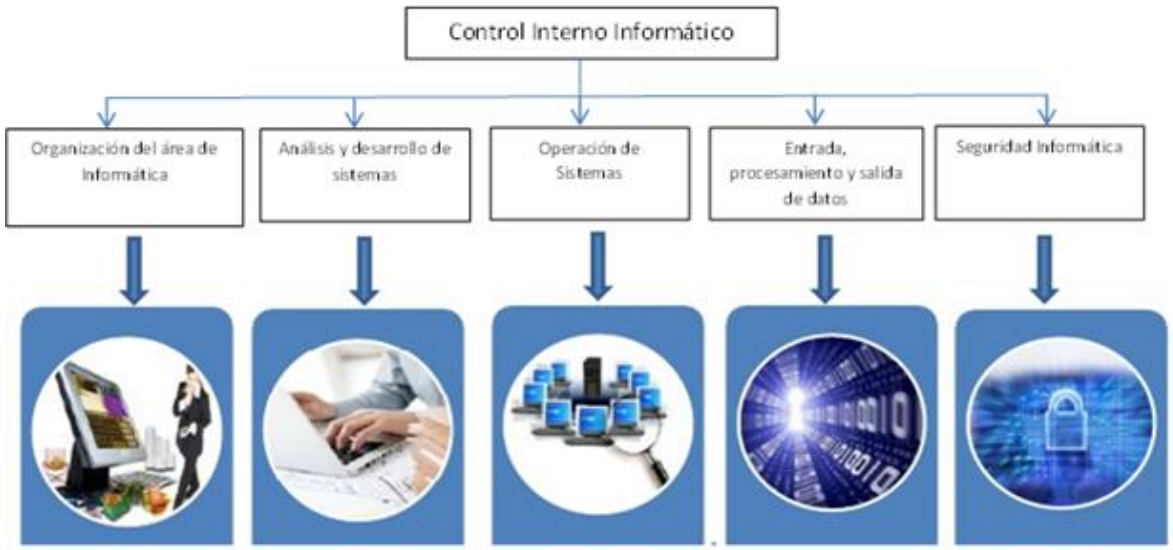
Para llegar a conocer la configuración del sistema es necesario documentar los detalles de la red, así como los distintos niveles de control y elementos relacionados:

- ✓ Entorno de red: esquema de la red, descripción de la configuración hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los ordenadores de entornos de base que soportan aplicaciones críticas y consideraciones relativas a la seguridad de la red.
- ✓ Configuración del ordenador base: Configuración del soporte físico, en torno del sistema operativo, software con particiones, entornos(pruebas y real), bibliotecas de programas y conjunto de datos.
- ✓ Entorno de aplicaciones: Procesos de transacciones, sistemas de gestión de base de datos y entornos de procesos distribuidos.
- ✓ Productos y herramientas: Software para desarrollo de programas, software de gestión de bibliotecas y para operaciones automáticas.
- ✓ Seguridad del ordenador base: Identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, etc.

Para la implantación de un sistema de controles internos informáticos habrá que definir:

- ✓ Gestión de sistema de información: políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.
- ✓ Administración de sistemas: Controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.
- ✓ Seguridad: incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.

- ✓ Gestión del cambio: separación de las pruebas y la producción a nivel del software y controles de procedimientos para la migración de programas software aprobados y probados



La función del control interno informático

El control interno informático es una función del departamento de Informática de una organización, cuyo objetivo es el de controlar que todas las actividades relacionadas con los sistemas de información automatizados se realicen observando las normas, estándares, procedimientos y disposiciones legales establecidas, interna y externamente. Entre sus tareas específicas merecen destacarse:

- Difundir y controlar el cumplimiento de las normas, estándares y procedimientos entre el personal de programación, técnicos y operadores;
- Diseñar la estructura del control interno informático en los siguientes aspectos
    - Desarrollo y mantenimiento del software de aplicación,
    - Explotación de servidores principales,
    - Software de Base,
    - Redes de Computación,
    - Seguridad Informática,
    - Licencias de software,
    - Relaciones contractuales con terceros y
    - Cultura del riesgo informático en la organización.

La relevancia de esta función se asienta sobre la planificación, control y evaluación por parte de la Dirección General de las actividades del Departamento de Informática; es inherente a dicha función disponer de:

- Plan Estratégico de Información, realizado por el Comité de Informática,
- Plan de desarrollo Informático realizado por el Departamento de Informática
- Plan General de Seguridad (física y lógica).