UNIDAD I. ASPECTOS GENERALES DE LA AUDITORÍA DE SISTEMAS

1.- AUDITORIA DE SISTEMAS

Los datos y la información generada en las empresas a día de hoy son infinitos. La información que se procesa y trata dentro de una empresa es incalculable. Las empresas, cada vez en mayor medida, necesitan la tecnología para trabajar, precisando complejos softwares y equipos informatizados para desarrollar su actividad de manera optimizada y eficiente. Esa presencia imperante de softwares y tecnología, provoca la necesidad de la auditoría de sistemas.

La auditoría de sistemas tiene como principal objetivo validar la integridad de la información y datos almacenados en las bases de datos de los sistemas de información y su procesamiento. Se trata de uno de los tipos de auditoría que van más allá del factor económico.

¿Qué es una auditoría de sistemas?

La auditoría de sistemas supone la revisión y evaluación de los controles y sistemas de informática, así como su utilización, eficiencia y seguridad en la empresa, la cual procesa la información. Gracias a la auditoría de sistemas como alternativa de control, seguimiento y revisión, el proceso informático y las tecnologías se emplean de manera más eficiente y segura, garantizando una adecuada toma de decisiones.

En definitiva, la auditoría de sistemas consiste en:

- La verificación de controles en el procesamiento de la información e instalación de sistemas, con el objetivo de evaluar su efectividad y presentar también alguna recomendación y consejo.
- Verificar y juzgar de manera objetiva la información.

- Examen y evaluación de los procesos en cuanto a informatización y trato de datos se refiere. Además, se evalúa la cantidad de recursos invertidos, la rentabilidad de cada proceso y su eficacia y eficiencia.

El análisis y evaluación realizados a través de la auditoría de sistemas debe ser objetivo, crítico, sistemático e imparcial. El informe de auditoría final deberá ser un claro ejemplo de la realidad de la empresa en cuanto a los procesos y la informatización se refiere, para tomar mejores decisiones y mejorar en el negocio.

Objetivos de la auditoría de sistemas

La presencia de la tecnología cada vez en más ámbitos empresariales, hace necesario un sistema de control, seguimiento y análisis, tal como la auditoría de sistemas. En primer lugar, se precisa garantizar la seguridad a la hora de tratar los datos, dotándolos de privacidad y buen uso. En segundo lugar, para hacer del sistema informático, un proceso mucho más eficiente y rentable, permitiendo detectar errores y tomando decisiones de manera inmediata.

Así, podemos decir que los objetivos de la auditoría de sistemas son:

- Mejorar la relación coste-beneficio de los sistemas de información.
- Incrementar la satisfacción y seguridad de los usuarios de dichos sistemas informatizados.
- Garantizar la confidencialidad e integridad a través de sistemas de seguridad y control profesionales.
- Minimizar la existencia de riesgos, tales como virus o hackers, por ejemplo.
- Optimizar y agilizar la toma de decisiones.
- Educar sobre el control de los sistemas de información, puesto que se trata de un sector muy cambiante y relativamente nuevo, por lo que es preciso educar a los usuarios de estos procesos informatizados.

Por tanto, la auditoría de sistemas es un modo de control y evaluación no sólo de los equipos informáticos en sí. Su ámbito de actuación gira también en torno al control de los sistemas de entrada a dichos equipos (pensemos por ejemplo en claves y códigos de acceso), archivos y seguridad de los mismos, etc.

La auditoría de sistemas es fundamental para garantizar el desempeño y seguridad de los sistemas informáticos de una empresa, que sean confiables a la hora de usarlos y garanticen la máxima privacidad posible. La auditoría informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Los aspectos relativos al control de la seguridad de la Información tienen tres líneas básicas en la auditoria del sistema de información:

- La seguridad operativa de los programas, seguridad en suministros y funciones auxiliares, seguridad contra radiaciones, atmósferas agresivas, agresiones y posibles sabotajes, seguridad físicos de las instalaciones, del personal informático, etc.
- La confidencialidad y la seguridad informática hace referencia no sólo a la protección del material, el logicial, los soportes de la información, sino también al control de acceso a la propia información.
- En relación a los aspectos jurídicos y económicos relativos a la seguridad de la información hace referencia a analizar la adecuada aplicación del sistema de información en la empresa en cuanto al derecho a la intimidad y el derecho a la información, y controlar los cada vez más frecuentes delitos informáticos que se cometen en la empresa.

Además, debe evaluar todo lo relacionado a la informática, organización de centros de información, hardware y software.

Características de la auditoria informática

La información de la empresa y para la empresa, siempre importante, se ha convertido en un activo real de la misma, como sus stocks o materias primas si las hay. Por lo que ha de realizarse inversiones informáticas, materia de la que se ocupa la auditoría de inversión informática.

Los sistemas informáticos han de protegerse de modo global y particular a ello se debe la existencia de la auditoría de seguridad informática en general, o a la auditoría de seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas.

Cuando existen cambios estructurales en la informática, se debe de reorganizar de alguna forma su función se está en el campo de la auditoría de organización informática. Estos tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial.

Cuando se realiza una auditoria del área de desarrollo de proyectos de la informática de una empresa, es porque en ese desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas.

2.- TIPOS DE AUDITORIA

Las auditorías de sistemas pueden ser aplicadas a diferentes niveles corporativos, pudiendo realizarse una auditoría de sistemas a toda la entidad, a un departamento, a un área o incluso a una actividad concreta. Por otro lado, dentro de la auditoría de sistemas, y en función de los procedimientos de auditoría aplicados y el objetivo que se quiere valorar, pueden distinguirse diferentes tipos:

- Auditoría de la gestión: se verifica el uso de los sistemas para la contratación de bienes y servicios, documentación de los programas, etc.
- Auditoría legal del Reglamento de Protección de Datos: se verifica el cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley de Protección de Datos de Carácter Personal.
- Auditoría de los datos: en la que se verifica el uso de los sistemas para la clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
- Auditoría de las bases de datos: en la que se verifica el uso de los sistemas en cuanto a los controles de acceso a las bases, de actualización, de integridad y calidad de los datos.
- Auditoría de la seguridad: referida a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y principio de no repudio.
- Auditoría de la seguridad física: referida a la ubicación de la organización, evitando ubicaciones de riesgo, y asegurando que los servidores y bases de datos se encuentran físicamente protegidos y en un entorno favorable (arcos de seguridad, CCTV, vigilantes, etc.).
- Auditoría de la seguridad lógica: referida a los métodos de autenticación de los sistemas de información.

- Auditoría de la seguridad en producción: mediante la cual se evalúan los riesgos y las respuestas frente a errores, accidentes y fraudes.

Tipos de auditorías: interna y externa. ¿En qué se diferencian?

Una auditoría puede ser tanto interna como externa y sus principales diferencias se encuentran en la naturaleza del auditor. Además, existe un tercer tipo de auditorías que son las públicas, ejecutadas por organismos.

Auditoría externa

Las auditorías externas son realizadas por auditores ajenos a la compañía. Estos pueden ser de otras empresas dentro de un grupo empresarial o bien auditores externos contratados por la misma empresa.

En una auditoría externa se realiza un análisis y control profundos para evaluar el correcto funcionamiento de la empresa, dentro de su marco normativo. Como consecuencia, el auditor externo expone una serie de mejoras y desviaciones para implementar en la organización y que cumpla con los objetivos perseguidos y en base a la legalidad.

Sin embargo, no son solo las empresas las que buscan saber la situación en la que se encuentran. Las auditorías externas también ayudan a posibles inversores, clientes o proveedores a conocer las actividades de una compañía, el control de los recursos empleados y el correcto cumplimiento legal.

Los principales objetivos que cumple una auditoría externa son:

- Identificar y denunciar posibles negligencias e incumplimientos de la empresa, dentro del marco normativo.
- Proponer mejoras que optimicen la gestión y desarrollo de las actividades empresariales.

- Proporcionan seguridad y confianza a posibles accionistas o inversores. Y atraen nuevas inversiones de capital.

Auditoría interna

El principal objetivo de la auditoría interna es mejorar el rendimiento de la compañía, realizando un análisis de todos sus componentes, departamentos y su funcionamiento.

Las auditorías internas son llevadas a cabo por recursos de la misma empresa y sus conclusiones deben ser útiles para los directivos, ejecutivos y socios del negocio, pues son quienes intervendrán en la toma de decisiones. No obstante, las auditorías internas pueden realizarse por especialistas externos si la empresa no cuenta con personal específico al que pueda encomendar esta tarea. Independientemente de quien realice la auditoría interna de la empresa, deben ceñirse a la imparcialidad y objetividad.

Este tipo de evaluaciones no son obligatorias, aunque son prácticas recomendadas pues arrojan datos significantes sobre la estructura del negocio y la situación en la que se encuentra. Además, realizar una auditoría interna es una manera de asegurarse de que la organización está cumpliendo sus funciones en cada área para conseguir los objetivos empresariales.

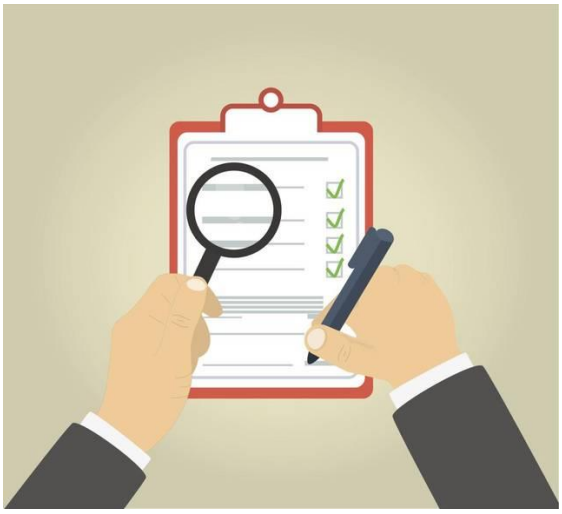
Una auditoría interna bien ejecutada ayuda a cumplir los siguientes objetivos:

- Optimizar el funcionamiento interno de la organización
- Fomentar la seguridad y productividad del negocio
- Planificar protocolos de actuación acordes a cada área o a nivel general
- Evaluar los controles operativos, contables y financieros
- Controlar el stock e inventario de la empresa
- Realizar informes que reporten irregularidades e infracciones

3.- POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS

ESTÁNDARES DE AUDITORÍA DE SISTEMAS

Definen los requerimientos obligatorios para la auditoría de sistemas y la generación de informes. Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorías de informática. Uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el «Garantizar la Seguridad de los Sistemas». Adicional a este estándar podemos encontrar el estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001.



El objetivo de los Estándares de Auditoría es informar:

Informar a los auditores de sistemas el mínimo nivel aceptado para resolver las responsabilidades profesionales precisadas en el código de ética profesional de ISACA para auditores de sistemas de información. A las gerencias y otras partes interesadas sobre las expectativas de la profesión concernientes a quienes la practican. Proveer información sobre el cómo cumplir con los estándares de la Auditoría de Sistemas.

ORGANISMOS Y ESTÁNDARES INTERNACIONALES DE LA AUDITORÍA DE SISTEMAS

- **Institute of System and Association, ISACA:** La InformationSystemAudit and Control Association -Asociación de Auditoria y Control de Sistemas de Información- ISACA, comenzó en 1967. En 1969, el grupo se formalizo, incorporándose bajo el nombre de EDP AuditorsAssociation -Asociación de Auditores de Procesamiento Electrónico de Datos. En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor del campo de gobernación y control de TI.

- **Certified Information Security Auditor, CISA:** La Asociación de Auditores y Control de Sistemas de Información (ISACA), provee una Certificación de auditores en Sistemas de Información (CISA); por medio de un examen anual que realiza el Instituto a los candidatos, el Cual cubre el conocimiento de actividades requeridas para la función de Auditoria en TI, para lo cual presenta un Manual de Información Técnica para la preparación de los Candidatos.

- **CertifiedInformation Security Manager, CISM:** También ISACA provee la Certificación para la Administración de la Seguridad de la Información del cual

intenta garantizar que existan administradores de seguridad de TI que tengan los conocimientos necesarios para reducir el riesgo y proteger a la organización.

- **Institute of InternalAuditors, IIA:** El Intitute of InternalAuditors (IIA), - organización Profesional con sede en los Estados Unidos, con más de 70.000 miembros en todo el mundo y años de existencia- anualmente organiza su Conferencia Internacional, la que habitualmente congrega a más de un millar de auditores de todos los continentes. El IIA es reconocido mundialmente como una autoridad, pues es el principal educador y líder en la certificación, la investigación y la guía tecnológica en la profesión de la auditoría interna.

- **CertifiedInternal Auditor, CIA:** El IIA cuenta con su propia Certificación de Auditores Internos CIA, la cual se da tanto a proveedores de estos servicios. Contar con profesionales certificados en auditoría interna, para la organización significa contar con un valioso recurso para la dirección y el consejo de administración, que ayuda a garantizar el avance en la dirección correcta para el logro de sus metas y objetivos.

NORMAS GENERALES DE LA AUDITORÍA DE SISTEMAS

La Asociación de Auditoría y Control de Sistemas de Información ha determinado que la naturaleza especializada de la auditoría de los sistemas de in formación y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información. La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

4.- PERFIL PROFESIONAL DEL AUDITOR DE SISTEMAS

El auditor informático es el profesional encargado de evaluar los procesos relacionados con las tecnologías de la información de la empresa, así como su infraestructura tecnológica, para asegurarse de que se ajustan a su actividad principal y ofrecer soluciones viables para los problemas detectados.

Las funciones de un auditor informático

El auditor informático, también conocido como auditor de sistemas o auditor de TI, desempeña diferentes funciones dentro de una empresa:

- Elabora el cronograma de auditorías de la empresa y a los clientes teniendo en cuenta los estándares de auditoría establecidos por la organización y la normativa vigente.
- Analiza la situación actual de los sistemas y procesos de tecnología de la información de la empresa, elaborando un informe que resuma los resultados de cada auditoría realizada.
- Controla y verifica el funcionamiento de los sistemas informáticos internos, incluyendo redes, software, programas, sistemas de comunicación y de seguridad o cualquier otro servicio que dependa de la infraestructura tecnológica.
- Detecta los riesgos que representa el entorno informático, los sistemas operativos y las redes y telecomunicaciones de la empresa para prevenir posibles ciberataques y desvíos de datos.
- Diseña soluciones para los problemas o errores hallados en la auditoría y propone nuevas estrategias para mejorar los sistemas informáticos y hacer un uso más eficiente de los mismos.

¿Cuál es el perfil de un auditor informático?

El perfil del auditor informático incluye ciertas competencias transversales que son independientes del sector donde trabaje. Un auditor informático debe tener buenas habilidades de comunicación que le permitan transmitir los resultados de su trabajo a personas que no son especialistas en su sector, así como tener un pensamiento crítico y analítico que le ayude a detectar los errores y áreas susceptibles de mejora o las tendencias y patrones que podrían representar un problema en los sistemas informáticos.

Además de esas características de un auditor informático, este profesional debe poseer una serie de competencias técnicas, con énfasis en las habilidades de seguridad. El auditor informático debe dominar las bases de la seguridad e infraestructura de TI y estar al tanto de los principales riesgos de seguridad que implica esta tecnología. También debe conocer las herramientas de visualización y análisis de datos, así como los estándares de auditoría interna (MAR, SOX, COBIT y COSO).