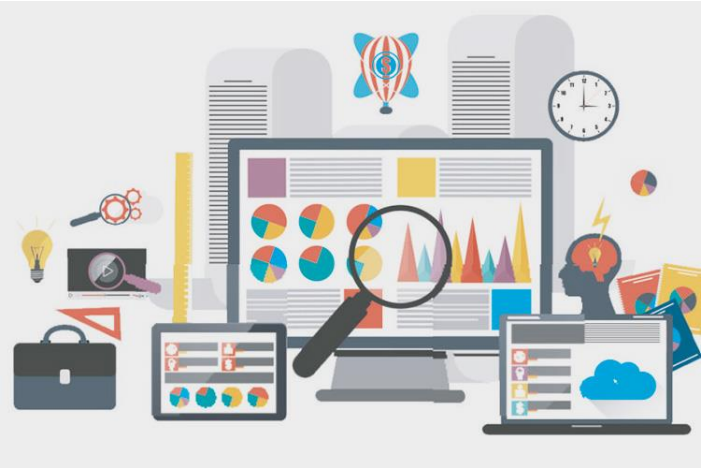
UNIDAD III.- TECNICAS DE AUDITORÍA DE SISTEMAS

Se define a las técnicas de auditoría como “los métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que fundamente sus opiniones y conclusiones, su empleo se basa en su criterio o juicio, según las circunstancias”. Al aplicar su conocimiento y experiencia el auditor, podrá conocer los datos de la empresa u organización a ser auditada, que pudieran necesitar una mayor atención.



Las técnicas y los procedimientos están estrechamente relacionados, si las técnicas no son elegidas adecuadamente, la auditoría no alcanzará las normas aceptadas de ejecución, por lo cual las técnicas, así como los procedimientos de auditoría tienen una gran importancia para el auditor. Según el IMCP en su libro *Normas y procedimientos de auditoría* las técnicas se clasifican generalmente con base en la acción que se va a efectuar, estas acciones pueden ser oculares, verbales, por escrito, por revisión del contenido de documentos y por examen físico. Siguiendo esta clasificación las técnicas de auditoría se agrupan específicamente de la siguiente manera:

- Estudio General
- Análisis
- Inspección
- Confirmación
- Investigación
- Declaración
- Certificación
- Observación
- Cálculo

Las técnicas son los procedimientos que se usan en el desarrollo de un proyecto de auditoría informática. Estas son algunas de las técnicas más comunes y aceptadas:

- Análisis y diseño estructurado
- Gráficas de Pert
- Gráficas de Gantt
- Documentación
- Programación estructurada
- Modulación de datos y procesos
- Entrevistas

1.- Auditoria de Datos:

La auditoría de datos es un proceso crucial que las organizaciones emprenden para valorar y evaluar sus prácticas de gestión de datos. Implica una revisión sistemática de los métodos de recopilación, almacenamiento, uso y protección de datos para garantizar el cumplimiento de las regulaciones y mejores prácticas. Realizar una auditoría de datos es esencial para mantener la privacidad, la seguridad y la integridad de los datos. Desde una perspectiva legal, las auditorías de datos ayudan a las organizaciones a cumplir con las leyes de protección de datos, como el Reglamento General de Protección de Datos (GDPR) y la Ley de privacidad del Consumidor de california (CCPA). Estas regulaciones exigen que las empresas sean transparentes sobre sus prácticas de datos, obtengan consentimiento para la recopilación de datos e implementen medidas de seguridad adecuadas. Al realizar una auditoría de datos, las organizaciones pueden identificar cualquier brecha en el cumplimiento y tomar las acciones necesarias para rectificarla.

Desde un punto de vista empresarial, las auditorías de datos proporcionan información valiosa sobre la calidad y precisión de los datos. Al revisar las fuentes de datos, las organizaciones pueden identificar información redundante u obsoleta, asegurando que solo se utilicen datos relevantes y confiables para los procesos de toma de decisiones. Esto ayuda a mejorar la eficiencia operativa y reduce el riesgo de tomar decisiones basadas en datos inexactos o incompletos. Ahora, profundicemos en una exploración en profundidad de los aspectos clave de la auditoría de datos:

- Recopilación de datos: este paso implica evaluar cómo se recopilan los datos, incluidas las fuentes, los métodos y los propósitos de la recopilación de datos. Las organizaciones deben asegurarse de contar con mecanismos de consentimiento adecuados y de que los datos se recopilen únicamente para fines legítimos.
- Almacenamiento de datos: evaluar las prácticas de almacenamiento de datos es crucial para garantizar la seguridad y el cumplimiento de los datos. Esto incluye evaluar la infraestructura de almacenamiento, las políticas de retención de datos, los métodos de

cifrado y los controles de acceso. Las organizaciones deben implementar medidas de seguridad sólidas para proteger los datos contra accesos no autorizados o violaciones.

- Uso de datos: comprender cómo se utilizan los datos dentro de una organización es esencial para mantener la privacidad y el cumplimiento. Esto implica revisar las actividades de procesamiento de datos, las prácticas de intercambio de datos y los mecanismos de transferencia de datos. Las organizaciones deben contar con políticas y procedimientos claros para regular el uso de datos y garantizar que los datos se utilicen únicamente para fines autorizados.
- Protección de Datos: Evaluar las medidas de protección de datos es vital para salvaguardar la información sensible. Esto incluye revisar los procesos de copia de seguridad y recuperación de datos, planes de recuperación ante desastres y protocolos de respuesta a violaciones de datos. Las organizaciones deben contar con mecanismos sólidos de protección de datos para mitigar el riesgo de pérdida de datos o divulgación no autorizada.
- Políticas de privacidad de datos: las organizaciones deben tener políticas de privacidad de datos bien definidas que describan cómo se maneja la información personal. Estas políticas deben ser de fácil acceso para las personas y proporcionar información clara sobre las prácticas de recopilación, uso y divulgación de datos. Es necesario revisar y actualizar periódicamente las políticas de privacidad para alinearse con las regulaciones y mejores prácticas cambiantes.

Auditoria Almacenamiento y recuperación de Datos

Una auditoría de almacenamiento de datos es un examen minucioso de las instalaciones de almacenamiento de datos en busca de posibles riesgos de seguridad. Los auditores también verifican las aptitudes de los empleados y el inventario almacenado. Las auditorías de almacenamiento de datos pueden incluir:

- Comprobación de la integridad de los datos
- Comprobación de si el almacenamiento y las copias de seguridad están suficientemente protegidos

- Auditoría de los intentos de los usuarios de acceder a objetos del sistema de archivos en un dispositivo de almacenamiento extraíble

Auditoria Base de Datos

Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:

- Quién accede a los datos.
- Cuando se accedió a los datos.
- Desde qué tipo de dispositivo/aplicación.
- Desde que ubicación en la Red.
- Cuál fue la sentencia SQL ejecutada.
- Cuál fue el efecto del acceso a la base de datos.

Objetivos Generales de la Auditoría de BD

Disponer de mecanismos que permitan tener trazas de auditoría completas y automáticas relacionadas con el acceso a las bases de datos incluyendo la capacidad de generar alertas con el objetivo de:

- ✓ Mitigar los riesgos asociados con el manejo inadecuado de los datos.
- ✓ Apoyar el cumplimiento regulatorio.
- ✓ Satisfacer los requerimientos de los auditores.
- ✓ Evitar acciones criminales.
- ✓ Evitar multas por incumplimiento.

La importancia de la auditoría del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoría de las aplicaciones que utiliza esta tecnología. La Auditoría de BD es importante porque:

- Toda la información financiera de la organización reside en bases de datos y deben existir controles relacionados con el acceso a las mismas.

- Se debe poder demostrar la integridad de la información almacenada en las bases de datos.
- Las organizaciones deben mitigar los riesgos asociados a la pérdida de datos y a la fuga de información.
- La información confidencial de los clientes, son responsabilidad de las organizaciones.
- Los datos convertidos en información a través de bases de datos y procesos de negocios representan el negocio.
- Las organizaciones deben tomar medidas mucho más allá de asegurar sus datos.

Deben monitorearse perfectamente a fin de conocer quién o qué les hizo exactamente qué, cuándo y cómo.

Auditoría sistemas distribuidos

Un sistema distribuido es un entorno informático en que conviven múltiples dispositivos, coordinando sus esfuerzos para completar una tarea de forma mucho más eficiente que si se realizara con solo un dispositivo. Esto ofrece muchas ventajas en comparación con los entornos informáticos tradicionales, tales como mayor escalabilidad, mejoras en la fiabilidad y menos riesgos al evitar un único punto vulnerable a fallas o ataques cibernéticos. Las auditorías de estos sistemas sirven para verificar el nivel de riesgo y exposición y si posee o no la protección y seguridad adecuada que debería ir ligada a este tipo de sistemas. La auditoría debe asegurar que exista un monitoreo de las actividades y el rendimiento de los nodos y los usuarios, a través de procesos de recopilación, análisis y generación de informes de datos y métricas sobre el estado, el comportamiento y la seguridad del sistema. Puede utilizar varias herramientas y marcos para la supervisión y la auditoría, también debe verificar la existencia de políticas y procedimientos de registro, alerta y respuesta a incidentes.

Auditoría a ambientes de microcomputadores

Es la auditoría técnica y especializada que se enfoca únicamente a la evaluación del funcionamiento y uso correctos del equipo de cómputo, su hardware, software y periféricos asociados. Esta auditoría también se realiza a la composición y arquitectura de las partes físicas y demás componentes del hardware, incluyendo equipos asociados, instalaciones y comunicaciones internas o externas, así como el diseño, desarrollo y uso del software de operación, de apoyo y aplicación". Lo que se busca con este tipo de auditorías es evaluar exclusivamente el equipamiento del sistema computacional, a fin de verificar su funcionamiento adecuado; esto se realiza con los propios sistemas computacionales o con las técnicas, métodos, procedimientos y herramientas diseñadas especialmente para practicar estas auditorías. El aspecto clave de estas evaluaciones es revisar los equipos, tanto desde el punto de vista físico (hardware), como desde el punto de vista lógico (software), al igual que todos los elementos que contribuyen a su funcionamiento, incluyendo las actividades de su personal y usuarios, la información, telecomunicaciones y demás componentes del sistema. En este tipo de evaluación el auditor de sistemas debe conocer las principales características, componentes y funcionamiento de la parte física de los sistemas, a fin de poder evaluar su aplicación, uso y aprovechamiento adecuados en la función informática de la organización.

Auditoría de la Seguridad de los sistemas computacionales

La revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema computacional, de sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, de las bases de datos, redes, sistemas, instalaciones y usuarios del mismo. Es también la revisión de los planes contra contingencias y mediadas de protección para la información, los usuarios y los propios sistemas computacionales, y en sí es la evaluación de todos aquellos aspectos que contribuyen a la protección y salvaguarda del buen funcionamiento del área de sistematización, sistemas de redes o computadoras personales, incluyendo la prevención y erradicación de los virus informáticos. Precisamente, con la auditoría de sistemas computacionales se puede evaluar la repercusión de la seguridad, protección y salvaguarda de los sistemas de la empresa, analizando sus impactos en los siguientes aspectos:

- En los sistemas computacionales y dispositivos periféricos.
- En la información institucional y bases de datos.
- En el personal informático y los usuarios del sistema.
- En la protección y conservación de locales, instalaciones, mobiliario y equipos.

- En los accesos a las áreas de sistemas, así como a sus sistemas computacionales, información y software.
- En la piratería informática.
- En los virus informáticos.

Éstos son algunos de los muchos aspectos de la seguridad de los sistemas computacionales de las empresas que se deben evaluar, aunque esto se puede aplicar también para las populares computadoras de las casas, escuelas y pequeñas empresas. A continuación analizaremos los principales aspectos que se deben contemplar en la auditoría de la seguridad de los sistemas computacionales, mismos que presentaremos de manera general, ya que su real aplicación se debe hacer de acuerdo con las características y necesidades de la administración de la seguridad, protección y salvaguarda de los bienes informáticos o del sistema computacional del área de cómputo de cada empresa:

- ✓ Auditoría de la seguridad en las condiciones e instalaciones físicas del área de sistemas.
- ✓ Protección contra los riesgos y contingencias de origen natural relacionadas con el medio ambiente de trabajo.
- ✓ Protección contra riesgos y contingencias relacionados con el medio ambiente de trabajo en las áreas de sistemas de la empresa.
- ✓ Protección contra riesgos y contingencias causados por factores meteorológicos, atmosféricos y desastres naturales incontrolables.
- ✓ Protección contra riesgos y contingencias derivados del suministro de la energía eléctrica.
- ✓ Protección y seguridad de los espacios físicos de las instalaciones de cómputo.
- ✓ El análisis a los planes de contingencias informáticas.
- ✓ Auditoría de la seguridad y protección en el diseño de las instalaciones del área de sistemas de la empresa o empresas de cómputo.
- ✓ Auditoría de la seguridad del hardware. Auditoría de la seguridad del softwar.
- ✓ Auditoría de la seguridad en los sistemas computacionales.
- ✓ Protección contra los actos ilegales en contra de los sistemas, activos informáticos e información.
- ✓ Protección contra el mal uso de la información.
- ✓ Protección contra la piratería y robo de información.
- ✓ Protección para el almacenamiento de la información.
- ✓ Protección contra virus informático.

2.- Técnicas Administrativas

Ser un administrador efectivo requiere experiencia en tu industria y con diferentes técnicas de administración. Las técnicas de administración no son trucos a corto plazo usados para

motivar empleados, sino que son métodos efectivos de administración que ayudan a desarrollar un lugar de trabajo productivo. No existe una sola técnica de administración que funcione en todas las situaciones, por lo que es importante familiarizarse con más de una.

Las Técnicas de Auditoría de Sistemas para probar controles de Aplicaciones en Producción

Las técnicas de auditoría de sistemas para probar controles de aplicaciones en producción, se orientan básicamente a verificar cálculos en aplicaciones complejas, comprobar la exactitud del procesamiento en forma global y específica y verificar el cumplimiento de los controles preestablecidos, de acuerdo con el manual correspondiente.

Las cuales son:

- Método de datos de pruebas: Consiste en la elaboración de un conjunto de registros que sean representativos de una o varias transacciones que son realizadas por la aplicación que va a ser examinada, y que luego serán ingresadas en dicha aplicación para la verificación del procesamiento exitoso de los datos. Este método es fácil utilizar y de entender, proporciona una prueba bastante especifica de las características individuales de los controles y da una evidencia objetiva para soportar el informe de auditoría, sin embargo consume una considerable cantidad de tiempo y requiere un alto esfuerzo manual.
- Evaluación del sistema de caso base (ESCB): Es conceptualmente similar al método datos de prueba, pero es más completa y requiere un alto grado de cooperación entre usuarios, auditores y personal de sistemas para su ejecución. La técnica ESCB se utiliza especialmente para validar los sistemas antes de entrar a producción, se utiliza normalmente por los auditores para examinar aplicaciones en producción. Esta técnica agiliza las pruebas por modificaciones y distribuye de una mejor forma la responsabilidad del sistema, pero requiere mayor tiempo de preparación y no orienta a la detección de fraudes.
- Operación Paralela: consiste en verificar la exactitud de la información sobre los resultados que produce un sistema nuevo que sustituye a uno ya auditado, el procedimiento se hace sobre los mismos datos reales con los procedimientos actuales y con los procedimientos nuevos para luego comparar los resultados y detectar inconsistencia.

Técnicas para seleccionar y monitorear transacciones

Estas técnicas son las que definen la forma, manera, cantidad y calidad de capturar una muestra del sistema de información para ser evaluadas. Generalmente el auditor utiliza pruebas de rangos, técnicas de muestreo y condiciones de error. Esto lo hace en base a criterio y experiencia profesional. Dentro de las técnicas más importante tenemos:

- Selección de transacciones de entrada: esta técnica se ejecuta mediante un software de auditoría, que es independiente al sistema de producción. Consiste en seleccionar y separar datos de entrada que son parte de las aplicaciones. Y se las hace en base al criterio profesional y experimentado del auditor. Estas transacciones separadas son sometidas a un riguroso examen establecido por una adecuada planificación del auditor. Cabe mencionar que esta técnica es muy segura ya que no existe el riesgo de la alteración de los datos del sistema de información.
- Archivo de revisión de auditoría como control del sistema (SCARF): esta técnica consiste en incorporar aplicaciones de auditoría en el sistema de producción para que ejecute distintos tipos de supervisiones y monitoreo de transacciones de forma permanente. La aplicación de este software se conoce como subrutina. Una vez que esta subrutina cargue las transacciones se procederá a la selección mediante muestreo previamente definidos por el auditor.
- Archivo de revisión de auditoría por muestreo (SARF): esta técnica (SARF) es muy similar a la anterior (SCARF). Lo único que cambia es la selección de las transacciones mediante al software ya que no son en forma automática y no son predefinidas, sino que la selección de la muestra se realiza al azar. Su objetivo es capturar archivos representativos para proceder a evaluarlos, esta técnica es muy utilizada por los auditores externos ya que permite analizar las transacciones y seleccionar los archivos en forma aleatoria o apoyándose con el muestreo estadístico. Para realizar este tipo de muestra se requiere de un analista de sistema o programador para que separen los módulos a decisión del auditor.
- Registros extendidos: esta técnica consiste en la aplicación de pequeñas rutinas que permiten recoger todos los datos que han afectado una transacción. Estas rutinas son conocidas como pistas de auditorías completas que son instaladas por el personal del sistema y programación al momento de preparar el sistema en producción, estos tipos de registros permiten tener un historial de todas las actividades, secuencias y/o fallos de sistema.

Técnicas para el examen de archivos

Permiten al auditor establecer el alcance de la revisión, definir las tareas de interés y la metodología a seguir para la ejecución del examen. Dentro de las técnicas más importantes para el examen de archivo, tenemos las siguientes.

- ✓ Programas generalizados de auditoria: esta técnica para evaluar archivos es muy general, se basa en procesos y procedimientos estándar para evaluar e investigar las deficiencias y falencias.
- ✓ Programa de utilería o de servicios: consiste en un software que mucha de las instalaciones de procesamiento electrónico de datos PED lo poseen como parte de sus herramientas para clasificar, seleccionar, insertar, copiar, fusionar, imprimir, buscar, intercalar. En la actualidad la mayoría de los auditores utilizan herramientas o utilitarios como parte de su apoyo informático que cumplen y realizan funciones iguales en las PED pero así mismo a este tipo de utilitarios o herramientas hay que ponerle mucho control debido a que muchos de estos utilitarios pueden hacer gran cantidad de modificaciones y no dejar rastro, pero así mismo existen otros programas que no alteran los datos de prueba.
- ✓ Programa de auditoría a la medida: son rutinas diseñadas para evaluar los procesos sistematizados de la empresa. Se dividen en dos tipos, la primera es diseñada por el departamento de programación o sistema de la empresa para monitorear o diseñar medidas de control y el segundo es realizado por el mismo auditor. Este programa es diseñado a la necesidad de la empresa y disponibilidad del auditor.
- ✓ Vaciado de archivos: esta técnica permite al auditor examinar el contenido de los archivos mediante una copia o vaciado de los datos a un medio de almacenamiento secundario, este vaciado se lo puede realizar en cualquier medio de almacenamiento computarizado. Generalmente el auditor realiza transacciones

para hacerle el respectivo seguimiento para luego verificar la secuencia y resultado lógico en los archivos maestros.

Técnicas para examinar programas de aplicación

Los programas de aplicación son aquellos que siendo estandarizados y/o a la medida tiene como objetivo resolver los problemas mediante el uso del computador.
En cuanto a la aplicación de esta técnica se debe poseer un alto grado de conocimiento técnico, pues está orientada a la evaluación del funcionamiento interno de las aplicaciones en producción y la manera que estas procesan su información. Esta comprende:

✓ Snapshot (Imagen Instantánea): es la técnica que permite una copia o fotografía de la memoria del computador que contiene todos los elementos de un proceso de decisión en el momento de su ejecución. EL SNAPSHOT es un programa utilitario que opera en sistema de producciones en los sistemas interactivos y de proceso Bacht. Esta técnica describe los problemas de programas de las computadoras, además proporciona un método para examinar la memoria de la computadora durante el procesamiento.

✓ Mapping (Mapeo): es una técnica ejecutada por una herramienta de medición de software que analiza un programa de computador, durante su ejecución para determinar si son utilizadas todas las instrucciones del programa.

✓ Racing (Rastreo): esta técnica se muestra en un lenguaje de programación y permite realizar un seguimiento ya que identifica y muestra en forma secuencial las instrucciones que han sido ejecutadas, como resultado nos arroja un listado de todas las tracciones efectuadas que servirá como evidencia de todas las acciones y transacciones realizadas para el auditor.

✓ Flujogramas de control (control flowcharting): este tipo de técnica permite evaluar de forma integral al sistema a su vez permite relacionar e interpretar los controles lógicos con los controles manuales y realizar un seguimiento para verificar la operación de los mismos controles.

✓ Comparaciones de código: sirve para comparar dos tipos de versiones de un mismo programa, también para revisar la copia del sistema que va a ser entregado al auditor para que lo evalué o para revisar las secuencias de las actualizaciones de un sistema; esto permite verificar los procedimientos de mantenimientos y cambios de los programas. Esta técnica no proporciona evidencia de la confiabilidad de los archivos de datos ni sobre la eficiencia y eficacia de los programas. La ejecución de este programa se lo puede realizar en código fuente y código objeto.

✓ Control de Bytes: es uno de los más seguros y adoptados por los auditores debido a que se somete al conteo de números de Bytes para detectar por medio de este, variaciones

o alteraciones del sistema no autorizadas. Este control ofrece un alto grado de confidencialidad en materia de integridad e inviolabilidad.

✓ Análisis de la lógica de los Programas: esta expresa que si los controles de los programas están funcionando de forma eficiente y efectiva y que los procesos de los datos se encuentran de acuerdo a las políticas establecidas basta con la revisión profunda de la lógica del sistema mediante varios de los manuales y documentos del sistema tales como: una narración descriptiva y detallada del programa, el diagrama de la lógica de los programas detallados y los listados de los programas.