ANÁLISIS DE SISTEMAS III

CARRERA:

- **ANÁLISIS DE SISTEMAS**

SEMESTRE:

- **QUINTO**

ÍNDICE

Introducción a la Asignatura

Mis queridos estudiantes, a lo largo de toda nuestra dinámica educativa, puedo decirles, que Análisis de Sistemas III, para la institución en esencia es: Auditoria de Sistemas; la misma se centra en determinar los riesgos que son relevantes para los activos de información, y la evaluación de los controles informáticos, a fin de reducir o mitigar posibles fallas o riesgos que pudieran desencadenar aspectos negativos en el diario gestionar de la organización.

Es decir:

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, siendo su objetivo final el de asegurar la protección de la información como también lograr que los equipos funcionen de forma eficiente.

ADRIANA E. GONZALEZ R.

- Magister en Gerencia Estratégica -

Una publicación de

Instituto Universitario de Tecnología para la Informática

Programa

OBJETIVO GENERAL:

Capacitar al alumno en el conocimiento de los procedimientos y normativas para llevar a cabo auditorias en los centros de información.

CONTENIDO:

1. AUDITORIA, ACCIONES CORRECTIVAS Y PREVENTIVAS
Conceptos y Tipos; Importancia; Lineamientos

2. IMPORTANCIA DEL TRABAJO EN EQUIPO
Filosofía e Importancia en el control de los procesos de gestión.

3. PLANIFICACIÓN DE LAS AUDITORIAS
Objetivos y Tipos; Aplicación y Desarrollo

4. ANÁLISIS Y TOMA DE DECISIONES
Conceptos Lineamientos
Esquematización e Importancia en los sistemas de auditorías

5. AUDITORIA Y EVALUACIÓN DE LOS CENTROS DE COMPUTACIÓN
Importancia de los centros de computación Desarrollo de listas de verificación; Check-List; Reporte de no conformidad

6. CONTROLES APLICADOS EN LA AUDITORÍA EN INFORMÁTICA
Conceptos Tipos, Funciones Importancia

7.- PIRATERÍA DE SOFTWARE
Conceptos, Tipos, Entes que participan Leyes y Sanciones

8.- INTRODUCCIÓN A LA AUDITORIA DE SISTEMAS BASADO EN LA NORMA ISO900
Conceptos; Uso de la aplicación de cada requisito.

LA AUDITORIA DE SISTEMAS

Unidad I

Origen:

Etimológicamente (estudio del origen de las palabras individuales) viene del verbo latino audire, que significa 'oír', que a su vez tiene su origen en los primeros auditores que ejercían su función juzgando la verdad o falsedad de lo que les era sometido a su verificación, principalmente mirando. Sin embargo, también se dice que viene del verbo en inglés to audit, que significa 'revisar' o 'intervenir'.

Concepto:

Una auditoría es una revisión SISTEMÁTICA de los procedimientos o de una situación que se llevan en una empresa a nivel contable o laboral entre otros, para comprobar o evaluar que se reúne una serie de requisitos, normas o políticas establecidos. Puede ser interna o externa, en función de si la realiza la propia empresa, o una entidad externa a la misma.

Tipos:

Los tipos de auditoría son las categorías en las que se pueden clasificar las auditorías. Estas son las técnicas de evaluación mediante las cuales se busca conocer las características de una organización empresarial. Es decir, los tipos de auditoría son las diferentes clases de análisis que se pueden elaborar respecto a una empresa.

Como realizar una Auditoria Informática:

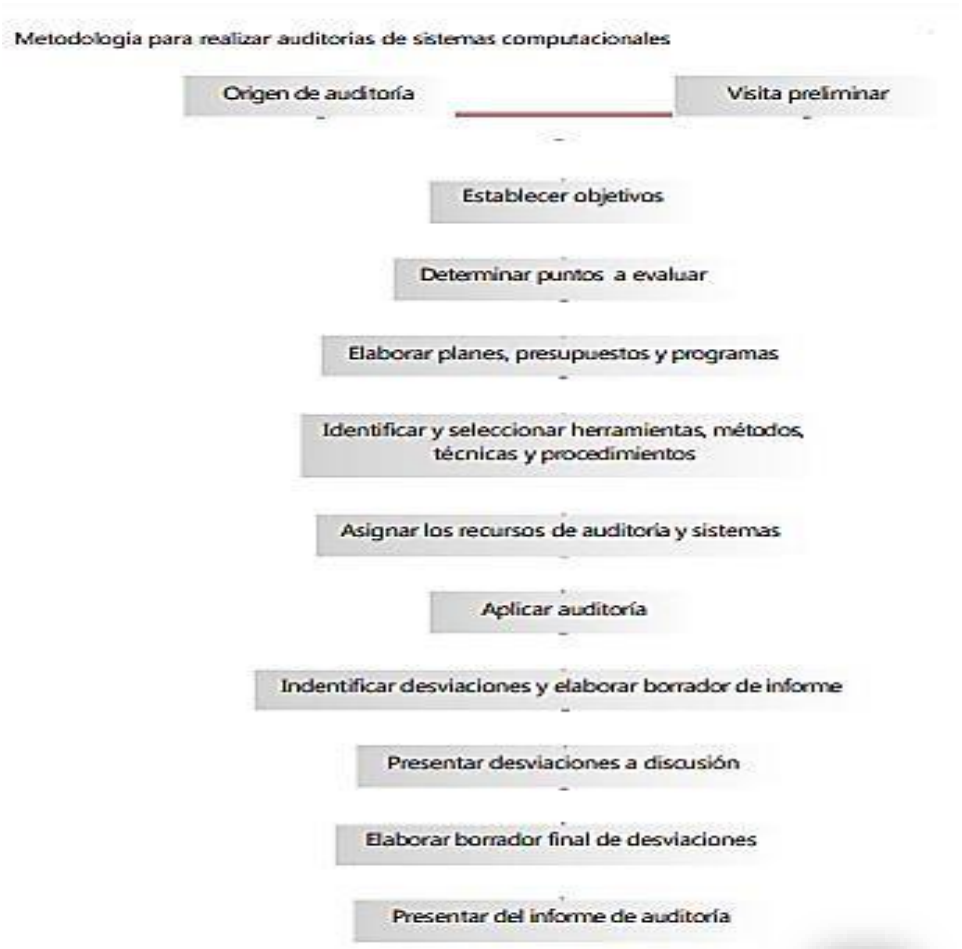
Objetivos de la auditoría informática:

- 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.

Las auditorías pueden clasificarse en base a distintos criterios: Según quién es el encargado de elaborar la auditoría.

Beneficios de la Auditoria Informática:

- Mejora la imagen pública.
- Confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad (reprocesos, rechazos, reclamos, entre otros).
- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.



Esta metodología tiene tres etapas fundamentales:

1ª ETAPA: PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS COMPUTACIONALES
2ª ETAPA: EJECUCIÓN DE LA AUDITORÍA DE SISTEMAS COMPUTACIONALES
3ª ETAPA: DICTAMEN DE LA AUDITORÍA DE SISTEMAS COMPUTACIONALES

Metodologías, pruebas y herramientas para la auditoría informática:

Existen diferentes metodologías que ayudan en el proceso de revisión de riesgos informáticos. Dos de las más utilizadas son Octave y Magerit.

ACTIVIDAD EVALUATIVA DE LA UNIDAD Nro.1:

1.- De donde surgió la palabra Auditoria?

2.- Cuales serían los tipos de Auditoria según su categoría?

3.- Que objetivo cumple una Auditoria Informática?

4.- Mencione algunas herramientas, metodología y/o pruebas que se pudiera realizar en una Auditoria Informática.

5.- Que beneficios pudiera aportar la A.I. a la organización?

TRABAJO EN EQUIPO

Unidad II

Importancia:

En la diversidad de temas, la variedad de objetivos en la tipología de las organizaciones y su necesidad de evaluarlas integralmente, requieren la conformación de equipos de auditoría con profesionales experimentados, idóneos y competentes, especialistas en temas de carácter técnico, financiero/contable, administrativo, jurídico y sistemas entre otros, que contribuyan en buscar la armonía de la Auditoría de manera planificada a través de un grupo interdisciplinario calificado, especializado y organizado en procura de obtener resultados objetivos, coherentes, concisos y soportados.

Tener un equipo de auditoría es crucial por varias razones:

- ✓ **Diversidad de Conocimientos:** Un equipo de auditoría está compuesto por profesionales con diferentes especialidades (financieras, contables, administrativas, jurídicas, etc.), lo que permite una evaluación integral y detallada de la entidad auditada.
- ✓ **Mejora de la Fiabilidad:** La interacción entre los auditores y los auditados, así como entre los propios miembros del equipo, mejora la fiabilidad y razonabilidad de los resultados de la auditoría.
- ✓ **Identificación de Riesgos:** Un equipo bien coordinado puede identificar y abordar riesgos emergentes de manera más efectiva.

Quienes deben conformar un equipo de auditoría de sistemas:

- ➢ **Líder del Equipo Auditor:** Responsable de planificar, organizar y dirigir la auditoría.
- ➢ **Auditores Principales:** Encargados de llevar a cabo la auditoría.

- **Auditores de Soporte:** Apoyan al equipo principal.
- **Secretario de Auditoría:** Encargado de la documentación y registro.
- **Expertos Técnicos:** Especialistas en temas técnicos, financieros, administrativos, jurídicos y sistemas

El equipo de trabajo deberá alinearse a estos requerimientos concretos:

- ✓ Organizacionales y
- ✓ Propio de la Auditoria

Importancia del trabajo en equipo en las organizaciones:

El trabajo en equipo facilita el cumplimiento de objetivos, incrementa la motivación y la creatividad, y favorece las habilidades sociales de cada uno. El trabajo en equipo es una capacidad altamente valorada en el mercado laboral, y es una de las características más demandadas por las empresas.

El trabajo en equipo promueve la comunicación efectiva y la coordinación entre los miembros de la organización. Esto es esencial para compartir información sobre posibles riesgos, identificar problemas de manera temprana y tomar decisiones informadas para mejorar los procesos de control interno.

¿Por qué es importante el trabajo en equipo en auditoría:?

Trabajo en equipo. Como auditor de una empresa, la colaboración en equipo es una necesidad constante. Reconocer la importancia del trabajo en equipo es crucial, ya que las personas a menudo se encuentran desempeñando roles tanto de miembros del equipo como de líderes . Equiparnos con las habilidades para funcionar de manera cohesiva es inmensamente beneficioso.

ACTIVIDAD EVALUATIVA DE LA UNIDAD Nro.2:

1.- Cual sería según su criterio, la importancia del trabajo en equipo en una organización ?

2.- Como debería ser conformado el equipo de auditoria?

3.- Según su criterio, porque se debe conformar un equipo multidisciplinario al realizar una A.I.?

4.- Mencione algunos beneficios o ventajas que brindaría a la auditoria la conformación del equipo multidisciplinario.

PLANIFICACIÓN DE LAS AUDITORIAS

Unidad III

Porque la Planificación?:

Las fallas en los Sistemas de Información han causado grandes trastornos en la organización y provocado conflictos entre individuos, secciones y/o departamentos. Cuando un sistema de información computarizado presenta inconsistencias, o no tiene buena acogida por parte de los usuarios, provoca que se vuelva difícil desarrollar nuevos sistemas en el futuro, ocasionando para la empresa u organización, la pérdida de los beneficios que un sistema de información bien estructurado, diseñado y operado trae consigo.

La planeación de la Auditoría de Sistemas debe atenderse como la proyección del trabajo de auditoría, definiendo su norte e indicando las pautas a seguir para lograr su desarrollo, por lo tanto se debe responder a los siguientes interrogantes: Qué se debe hacer?, Qué aspectos se van a auditar?. Cuándo se debe hacer?. Cómo se va a realizar ?. Qué recursos demandara ?, De qué recursos se dispone?, cuestionamientos que de ser respondidos adecuada y oportunamente, conducen a la optimización de recursos, evitando la improvisación y desfases en la estimación.

Entendiendo bien la unidad 1, donde La auditoría informática o auditoría de los sistemas de información, es un proceso de análisis a los sistemas de información de una organización, con el objetivo de evaluar su estado y el nivel de seguridad existente, sabiendo que y según de Pablos et al.,2006; es la revisión, verificación y evaluación con un conjunto de métodos, técnicas y herramientas de los sistemas de información de una organización, de forma continua y a petición de su Dirección, con el fin de mejorar su rentabilidad, seguridad y eficacia

Igualmente una auditoria en sistemas de información recoge, agrupa y evalúa evidencias, para determinar si un sistema de información cumple con los requisitos de salvaguardar los activos de la organización, mantener la integridad de los datos y lograr eficazmente los fines de la organización.

LINEAMIENTOS Y HERRAMIENTAS:

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática que promueven la creación y desarrollo de buenas prácticas como lo son: COBIT, COSO e ITIL

El Plan de Auditoria informática determina la gran importancia que tienen las administraciones de Sistemas de Información y equipos de cómputo para verificar los riesgos informáticos en los procesos administrativos, llevando a cabo procedimientos basados en controles de seguridad.

La planeación de la Auditoria Informática deberá incluir (4):

- Preparativos logísticos (viajes, instalaciones, etc.).
- Asuntos relacionados con la confidencialidad.
- Cualesquiera acciones de seguimiento de la auditoria.
- Solicitar documentos sobre los equipos, número de ellos, localización y características.

Una auditoria informática se realiza siguiendo diferentes fases o etapas, que son necesarias para determinar objetivos y así obtener un resultado satisfactorio, como, por ejemplo:

- ✓ Estudio de la situación actual. ...
- ✓ Análisis profundo. ...
- ✓ Proponer soluciones. ...
- ✓ Implementación. ...
- ✓ Evaluación de resultados.

La auditoría informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido o matiz "político" ajeno a la propia estrategia y política general de la empresa. La función auditora puede actuar de oficio, por iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente.

Fases de la auditoria informática:

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) es una organización global sin fines de lucro que desarrolla y recomienda de manera independiente prácticas estándar de la industria para la auditoría de sistemas de información. *Las normas de ISACA recomiendan tres fases* para un proceso de revisión de auditoría: **planificación, trabajo de campo y presentación de informes .**

Sin embargo una publicación realizada por EUROINNOVA quien es un instituto de educción en línea describe 7 fases

Según Tamayo Alsate y Néstor Dario Duque indican que no existen parámetros precisos que nos guíen en el desarrollo de un proyecto de auditoría de sistemas; en realidad cada proyecto debe administrarse con una estrategia diferente según sea su dimensión, alcance y nivel de riesgo, y es la falta de planeación la causa principal de los fracasos, retrasos, incumplimientos, incrementos de costos y la poca calidad en las auditorias desarrolladas; para evitar estos problemas se requiere de una planeación cuidadosa y para lograrlo es fundamental que el auditor conozca la empresa del cliente que va a auditar y entre más familiarizado esté con ella mejor aún.

Es así como el SAS N ®22 Au 311 indica " La planeación adecuada incluye que el auditor adquiera la comprensión de la naturaleza operativa del negocio, su organización, la ubicación de sus instalaciones, los productos vendidos o servicios prestados, su estructura financiera, las operaciones relacionadas con otros, los métodos de remuneración y muchos otros asuntos."

Para una efectiva planeación, es necesario obtener la información correspondiente en forma selectiva a través de entrevista personal, observación, encuesta y muestreo, entre otras.

¿Qué es programa de auditoría?

Un programa de auditoría es un sistema de objetivos, alcance, calendario y actividades de auditoría que llevarán a cabo los auditores. Un programa de auditoría, también conocido como plan de auditoría, funciona como una guía para llevar a cabo diversos tipos de auditorías en una empresa.

Según Tamayo Alsate y Néstor Dario recomienda el siguiente programa en la planeación de una auditoria que básicamente debe contener los siguientes pasos:

1. **Objeto de la auditoría:** Se debe determinar con suma claridad que tipo de auditoría se va a realizar, por ejemplo, auditoría para aplicaciones en funcionamiento, auditoría para aplicaciones en desarrollo, auditoría al centro de informática, etc.

2. **Soporte legal:** Es necesario conocer la normatividad tanto interna como externa, así como los procedimientos y reglamentos que afectan a la empresa, para lograr un conocimiento más amplio de ella y de esta forma poder proyectar el plan más eficientemente.

3. **Alcance:** 'El auditor es quien determina el alcance de la auditoría que va a realizar, de acuerdo a las condiciones que se presentan en el momento y a las normas, regulaciones, extensión y complejidad que la cobija.

4. Metodología, a aplicar: Dependiendo si se trata de aplicaciones en funcionamiento o aplicaciones en desarrollo, se deben definir los pasos a seguir para llevar a cabo la auditoría, como son: diseño de cuestionarios de control, diseño de papeles de trabajo, definición de procedimientos de auditoría y preparación de informes.

5. Tiempo estimado: Se debe hacer un estimativo del tiempo requerido para auditar cada aplicación considerando la complejidad, tamaño de la aplicación, experiencia del equipo auditor y recursos disponibles, por lo tanto, es conveniente que se asigne el tiempo en horas que demandará cada actividad para su ejecución.

6. Conformación del equipo asesor: El director del proyecto de auditoría conformará un equipo de trabajo de acuerdo a su criterio y necesidades, de tal manera que cubra tanto los aspectos administrativos como técnicos de la auditoría a realizarse. El equipo debe ser capaz de aplicar el enfoque sistémico y debe estar integrado por profesionales de diferentes áreas del conocimiento como administradores de empresas, contadores, economistas, ingenieros industriales, administradores de sistemas, ingenieros de sistemas, analistas, diseñadores y programadores, entre otros, capaces de reunir habilidades y destrezas, y crear un sentido unificador de sus relaciones.

7. Lugar donde se desarrollará la auditoría: Se debe definir el sitio donde Se realizará la auditoría, como domicilio contractual para todos los efectos y acciones a realizar; así mismo, es indispensable definir la fecha tentativa de inicio de labores.

8. Recursos logísticos y técnicos necesarios para su desarrollo: Se Deben definir los horarios de trabajo, equipos de trabajo, equipos y elementos de oficina necesarios, recursos informáticos tanto de software como de hardware, definición de accesos, perfiles de usuario, asignación de cuentas, archivos y bibliotecas de producción, etc.

Diagrama de flujo de documentos y su importancia

El diagrama de flujo ayuda al auditor a visualizar los distintos pasos del programa e identificar posibles debilidades o áreas de riesgo que se deben abordar . El diagrama de flujo también puede ayudar al auditor a identificar errores o ineficiencias en el programa y hacer recomendaciones para realizar mejoras.

ACTIVIDAD EVALUATIVA DE LA UNIDAD Nro.3:

1. Que entiende usted por planificación de Auditoria informática?

2. Cuáles serían los lineamientos en una Auditoria informática?

3. Según lo estudiado, cuáles serían las fases de la auditoria informática?

4. Cual considera usted, la causa principal de los fracasos en la auditoria informática?

5. Que es un programa de auditoria?

ANÁLISIS Y TOMA DE DECISIONES:

Unidad IV

Concepto e importancia en las organizaciones:

Según (Chacin, s.f.) la toma de decisiones afirma que es el proceso de identificar y solucionar un problema encontrado, con la finalidad de fijar el rumbo de una empresa hacia los objetivos empresariales, y mantener una visión clara para su posicionamiento en el mercado.

En la actualidad, con la rapidez de avances tecnológicos, el crecimiento de la economía y el volumen de datos producidos, las instituciones deben tener la capacidad de manipular la información de forma segura con el fin de impulsar su desarrollo y continuidad; utilizando como herramienta principal los sistemas de información, que no son otra cosa que una agrupación de componentes dirigidos al procesamiento y gestión de datos e información de diferente formato, producidos para cubrir un objetivo. Estos componentes pueden ser: individuos, actividades, datos y recursos materiales (GestioPolis, 2018).

La Informática hoy, está subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma.

En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el «management» o gestión de la empresa.

La informática está inmersa en la gestión integral de la organización. A finales del siglo XX, los sistemas de TI (tecnologías de la información) se constituyeron como las herramientas más poderosas para cualquier organización, puesto que apoyan la toma de decisiones, generando un alto grado de dependencia, así como una elevada inversión en ellas. Debido a la importancia que tienen en el funcionamiento de una organización, existe la auditoría informática.

Al igual que cualquier área de la organización, los sistemas de TI deben estar sometidos a controles de calidad y auditoría informática porque las computadoras y los centros de procesamiento de datos son blancos apetecibles para el espionaje, la delincuencia y el terrorismo.

Asimismo, un sistema de TI mal diseñado puede convertirse en una herramienta muy peligrosa para la gestión, coordinación y toma de decisiones de la organización.

La toma de decisiones ayuda a la empresa a identificar sus oportunidades, a evaluar los riesgos y a elaborar planes para lograr sus objetivos. Además, la toma de decisiones permite asignar recursos (que son siempre limitados) de manera efectiva, ya sean financieros, materiales o humanos.

Ventajas de la toma de decisiones con IA:

Permite procesar grandes cantidades de datos: La IA permite analizar todos los datos que genera la empresa. Y gracias a ello se pueden extraer patrones y relaciones entre ellos. Lo que permite llegar a conclusiones y tomar decisiones estratégicas mejor fundamentadas.

Los sistemas de IA pueden analizar datos históricos en tiempo real para identificar posibles amenazas y oportunidades, permitiendo a las empresas anticipar y mitigar riesgos, así como aprovechar al máximo las oportunidades emergentes.

La IA tiene un enorme potencial para transformar la toma de decisiones en diversas industrias. La tecnología puede automatizar los procesos de toma de decisiones, analizar grandes conjuntos de datos y proporcionar información que los humanos tal vez no puedan ver

Desventajas en el empleo de la IA?

- Desplazamiento de empleos. ...
- Sesgo algorítmico. ...
- Falta de empatía. ...

- Menor privacidad. ...
- Dependencia tecnológica. ...
- Desafíos éticos. ...
- Posibilidad de ataques cibernéticos. ...
- Menor resolución de problemas inesperados.

El nuevo panorama plantea retos diversos que no habría que pasar por alto. Es el caso de la seguridad de los datos que manejan los programas de IA. Lo mismo sucede cuando se piensa sobre la posibilidad de controlar al 100 % una tecnología en constante crecimiento. No hace demasiado tiempo se supo que Facebook tuvo un problema con su sistema de inteligencia artificial, ya que había creado un lenguaje propio que ni sus creadores conocían.

Así, al analizar el desarrollo de la inteligencia artificial, sus ventajas y las desventajas que puede llegar a tener, es clave para saber hacia dónde tenemos que ir en el desarrollo tecnológico.

ACTIVIDAD EVALUATIVA DE LA UNIDAD Nro.4:

1.- Que rol tiene la toma de decisiones en una organización?

2.- Qué papel juega los avances tecnológicos en la toma de decisiones e una organización?

3.- Considera usted que tener I.A. en las organizaciones privadas podría ser una ventaja competitiva?

4.- Que opinión daría usted en dejar en manos de la, I.A. la toma de decisiones en ambientes cerrados (organizaciones), abiertos (gestión pública de gobiernos).

AUDITORIA Y CONTROL DE LOS CENTROS DE COMPUTACION:

Unidad V

Conceptos:

La Auditoría Informática es el proceso mediante el cual se comprueba el manejo de los recursos computacionales dentro de la empresa, del mismo modo, analiza los términos legales de los sistemas ofimáticos (Molina, 2020).

La Especialización en Auditoría y Control estudia los procesos de control en las organizaciones y los mecanismos para garantizar la seguridad y confianza de los usuarios internos y externos en la información.

Entonces la auditoría y control de los centros de computación es aquella que se realiza con el apoyo de los equipos de cómputo y sus programas, para evaluar cualquier tipo de actividades y operaciones, no necesariamente computarizada pero si susceptible de ser automatizada; dicha auditoria se realiza también a las actividades del propio centro de sistemas y a sus componentes.

Características:

La principal característica de este tipo de auditoria es que, sea en un caso o en otro, o en ambos, se aprovecha la computadora y sus programas para la evaluación de las actividades que se revisaran, de acuerdo con las necesidades concretas del auditor, utilizando en cada caso las herramientas especiales del sistema y las tradicionales de la propia auditoria en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma.

En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el «management» o gestión de la empresa.

Esta auditoria se caracteriza porque al realizarla se cuenta con el apoyo de los equipos de cómputo y de sus programas de revisión específica para evaluar la propia área de sistemas, utilizando los servicios informáticos como si fueran elementos de soporte para auditar cualquier otra área de la empresa.

En esta auditoria se utilizan los sistemas computacionales de acuerdo con las necesidades específicas de las áreas a revisar, aprovechando las técnicas tradicionales de auditoria de computación que ofrecen los sistemas, mismas que se adaptan a las técnicas tradicionales de auditoria para realizar con ambos una revisión, evaluación y dictamen de las áreas de sistemas que serán auditadas.

Beneficios en la aplicación de la Auditoria en los centros de cómputo:

- Efectuar procedimientos de evaluación de riesgo.

- Efectuar procedimientos analíticos:

  - ✓ Probar la eficacia operativa de los controles;
  - ✓ Pueden ser útiles para identificar relaciones o transacciones de ingresos inusuales o imprevistos.
  - ✓ Identificar las partidas poco usuales en una población que satisfagan los criterios establecidos previamente

Un departamento de Informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados digitalmente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc. La explotación informática o centro de cómputo, se puede considerar como una fábrica con ciertas peculiaridades que la distinguen de las reales. Para realizar la Explotación Informática se dispone de una materia prima, los Datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del Proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son

sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

SECCIONES QUE COMPONEN A CENTRO DE CÓMPUTO:

Auditar el centro de cómputo consiste en auditar las secciones que la componen y sus interrelaciones. El centro de cómputo o Explotación Informática se divide en tres grandes áreas: Planificación, Producción y Soporte Técnico, en la que cada cual tiene varios grupos:

Control de Entrada de Datos:

Se analizará la captura de la información en soporte compatible con los Sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a Norma.

Planificación y Recepción de Aplicaciones:

Se auditarán las normas de entrega de Aplicaciones por parte de Desarrollo, verificando su cumplimiento y su calidad de interlocutor único. Deberán realizarse muestreos selectivos de la Documentación de las Aplicaciones explotadas. Se inquirirá sobre la anticipación de contactos con Desarrollo para la planificación a medio y largo plazo.

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Muy escuetamente, una Aplicación recorre las siguientes fases:

- Prerequisitos del Usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (Preprogramación y Programación)
- Pruebas

- Entrega a Explotación y alta para el Proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Una auditoría de Aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

1. Revisión de las metodologías utilizadas: Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
2. Control Interno de las Aplicaciones: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo:

   - ✓ Estudio de Vialidad de la Aplicación. [importante para Aplicaciones largas, complejas y caras]
   - ✓ Definición Lógica de la Aplicación. [se analizará que se han observado los postulados lógicos de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto]
   - ✓ Desarrollo Técnico de la Aplicación. [Se verificará que éste es ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles]
   - ✓ Diseño de Programas. [deberán poseer la máxima sencillez, modularidad y economía de recursos]
   - ✓ Métodos de Pruebas. [Se realizarán de acuerdo a las Normas de la Instalación. Se utilizarán juegos de ensayo de datos, sin que sea permisible el uso de datos reales]
   - ✓ Documentación. [cumplirá la Normativa establecida en la Instalación, tanto la de Desarrollo como la de entrega de Aplicaciones a Explotación]
   - ✓ Equipo de Programación. [Deben fijarse las tareas de análisis puro, de programación y las intermedias. En Aplicaciones complejas se

producirían variaciones en la composición del grupo, pero estos deberán estar previstos]

3. Satisfacción de usuarios: Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

4. Control de Procesos y Ejecuciones de Programas Críticos: El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de Desarrollo de Aplicaciones. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran podríase provocar, desde errores de bulto que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las Librerías de programas; aquellos programas fuente que hayan sido dados por bueno por Desarrollo, son entregados a Explotación con el fin de que éste:

    4.1. Copie el programa fuente en la Librería de Fuentes de Explotación, a la que nadie más tiene acceso.
    4.2. Compile y monte ese programa, depositándolo en la Librería de Módulos de Explotación, a la que nadie más tiene acceso.
    4.3. Copie los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente por el punto 1.

Centro de Control y Seguimiento de Trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación Informática ejecuta procesos por cadenas o lotes sucesivos (Batch*), o en tiempo real (Tiempo Real*). Mientras que las

Aplicaciones de Teleproceso están permanentemente activas y la función de Explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de Explotación. En muchos Centros de Proceso de Datos, éste órgano recibe el nombre de Centro de Control de Batch. Este grupo determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

***Batch y Tiempo Real:**

Las Aplicaciones que son Batch son Aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que lo que hace es relacionar toda la información, calcular cosas y obtener como salida, por ejemplo, reportes. O sea, recolecta información durante el día, pero todavía no procesa nada. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente.

Las Aplicaciones que son Tiempo Real u Online, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son Sistemas que tienen que responder en Tiempo Real.

Operación. Salas de Ordenadores:

Se intentarán analizar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo. Se verificará la existencia de un responsable de Sala en cada turno de trabajo.

Se analizará el grado de automatización de comandos, se verificara la existencia y grado de uso de los Manuales de Operación. Se analizará no solo la existencia de planes de formación, sino el cumplimiento de los mismos y el tiempo transcurrido para cada Operador desde el último Curso recibido. Se estudiarán los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del Sistema hasta el montaje real. Se verificarán las líneas de

papel impresas diarias y por horas, así como la manipulación de papel que comportan.

Centro de Control de Red y Centro de Diagnosis (Help Desk):

El Centro de Control de Red suele ubicarse en el área de producción de Explotación. Sus funciones se refieren exclusivamente al ámbito de las Comunicaciones, estando muy relacionado con la organización de Software de Comunicaciones de Técnicas de Sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todos las líneas asociadas al Sistema.

La importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

El Auditor de Sistemas deberá observar si los sistemas que se utilicen para la transferencia de datos cumplen con los requisitos mínimos de controles internos y todo lo que se refiera a la seguridad física, lógica y operación de los equipos, así como que existan circuitos alternativos frente a posibles interrupciones del servicio. Se deberán verificar los mecanismos de protección de datos que se usan en la transmisión por la red de telecomunicaciones, si existen técnicas adecuadas de encriptación por "hardware" y/o "software

El Centro de Diagnosis (Help Desk) es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de Software como de Hardware. El Centro de Diagnosis está especialmente indicado para informáticos grandes y con usuarios dispersos en un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la Informática de la empresa. Debe ser auditada desde esta perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispone. No basta con comprobar la eficiencia técnica del Centro, es necesario analizarlo simultáneamente en el ámbito de Usuario.

ACTIVIDAD EVALUATIVA DE LA UNIDAD Nro.5:

1. Que busca la Auditoría y Control en los centros de cómputos de las organizaciones.

2. Qué ventajas o beneficios ofrece la aplicación de la Auditoria con la computadora.

3. Cuál sería la principal característica de esta auditoría.

4. En cuantos se divide el centro de cómputo o Explotación Informática.

5. Como podría auditarse el Centro de Control de Red.

CONTROLES APLICADOS EN AUDITORIA DE SISTEMAS:

Unidad VI

Concepto:

Un Control es un conjunto de métodos coordinados y medidas adoptadas dentro de una organización con el fin de:

1.-Salvaguardar activos.
2.-Asegurar la confiabilidad y corrección de los datos contables y extracontables.
3.-Promover la eficacia y eficiencia de las operaciones.
4.-Promover la adhesión a las políticas vigentes.

Entendiendo que los mecanismos de control en el área de Informática son: directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia

Actividades de control en auditoría?

Son aquellas acciones establecidas, a través de políticas y procedimientos, por los responsables de las unidades administrativas para alcanzar los objetivos institucionales y responder a sus riesgos asociados, incluidos los de corrupción y los de sistemas de información.

¿Entonces que podría ser el control auditoría de sistemas?

Se podría decir que es un examen sistemático de todos recursos que involucran el sistema en su totalidad para determinar si se requiere de

inversión en los recursos que componen el sistema para garantizar que los objetivos se cumplan.

Objetivo fundamental del control en la auditoría informática:

Son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos.

No es admisible detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo.

La auditoría debe iniciar su actividad cuando los Sistemas están operativos, es el principal objetivo el de mantener tal situación. Tal objetivo debe conseguirse tanto a nivel global como parcial.

La operatividad de los Sistemas ha de constituir entonces, **la principal preocupación del auditor informático** y para conseguirla hay que acudir a la realización de:

1) Controles Técnicos Generales de operatividad:
Son los que se realizan para verificar la compatibilidad de funcionamiento simultáneo del Sistema Operativo y el Software de base, con todos los subsistemas existentes, así como la compatibilidad del Hardware y de Software instalados.

2) Controles Técnicos Específicos de Operatividad:
Son igualmente necesarios pero menos acusado, para lograr la Operatividad de los Sistemas. Un ejemplo de lo que se puede encontrar mal, son parámetros de asignación automática de espacio en disco (todas las aplicaciones que se desarrollan son super-parametrizadas en asignación de espacio en disco). También, los periodos de retención de ficheros comunes a varias Aplicaciones pueden estar definidos con distintos plazos en cada una de ellas, de modo que la pérdida de

información es un hecho que podrá producirse con facilidad, quedando inoperativa la explotación de alguna de las Aplicaciones mencionadas.

Una vez conseguida la Operatividad de los Sistemas, el **segundo objetivo de la auditoría es la verificación de la observancia de las normas** teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

1. Las Normas Generales de la Instalación Informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta Normativa General Informática no está en contradicción con alguna Norma General no informática de la empresa.

2. Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de Explotación. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.

3. Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales. Así, Explotación no debería explotar una Aplicación sin haber exigido a Desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los Procedimientos Específicos no se opongan a los Procedimientos Generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los Procedimientos Generales de la propia empresa, a los que la Informática debe estar sometida.

CRITERIOS BASICOS DE EVALUACIÓN

El auditor debe identificar en que lugar dentro de la estructura organizacional está ubicada el área de Sistemas de Información la que deberá depender funcionalmente de un nivel tal que permita garantizar su independencia tanto de las áreas usuarias como de Administración. Concretamente se debe verificar que ningún área de usuarios tenga autoridad para modificar los datos sin pasar por los responsables de sistemas.
Debe observar si existe un plan de Sistemas formal contenga un cronograma de las actividades del área, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un período mínimo de 1 año, que permita una supervisión continua y directa de las tareas que realizan los distintos sectores.

Se debe constatar que el área presenta una clara delimitación de las tareas entre desarrollo (si lo hubiera) y mantenimiento de sistemas, Administración de Bases de Datos, operaciones, carga de datos, soporte técnico y supervisión, de manera que se garantice una adecuada segregación de funciones y fomente un control por oposición de intereses.

Asimismo debe verificar si existen políticas generales para el área con una clara definición de las misiones y funciones de todos los puestos de trabajo (responsabilidad, dependencia, funciones que supervisa. etc.), estándares y procedimientos escritos que sean la base de la planificación, el control y la evaluación gerencial.

ACTIVIDAD EVALUATIVA DE LA UNIDAD Nro.6:

1.- A que llamamos conjunto de métodos coordinados y medidas adoptadas dentro de una organización para entre ellas Promover la eficacia y eficiencia de las operaciones?
2.- Qué son las actividades de control en auditoría?
3.- Que entiende usted por el control auditoría de sistemas?
4.- Cuál sería el objetivo fundamental del control en la auditoría informática?
5.- Según sus observaciones cual sería el segundo objetivo de la Auditoria Informática?

PIRATERIA DEL SOFTWARE:

Unidad VII

¿ QUE ES ?

La piratería digital consiste en la copia o distribución ilegal a través de Internet de material sujeto a derechos de autor, lo que tiene efectos perniciosos para las industrias de la creación, como el cine, la televisión, la edición, la música y el juego.

Los tipos principales de piratería:

Según ITD Consulting en Venezuela existen 8 tipos principales de software pirata.

Cómo hacer una auditoría de software pirata dentro de la organización:

Según el portal de Emiliano Pardo Saguier, Cualquier organización que no sepa monitorear el software pirata sufrirá costos impensados. De ahí que es fundamental detectarlo en tu auditoría de software pirata.

La Piratería de Software involucra a varios actores y/o entes en los que destacan: usuarios finales, distribuidores ilegales, desarrolladores de software piratas, grupos organizados, plataformas en líneas., entre otros.

¿Cómo afecta la piratería informática a las organizaciones?
En primer lugar, les hace perder dinero. Según SoftwareKey, un sitio web de prevención de la piratería:

"La piratería de software está muy extendida. La Software Alliance informa de que la piratería de software alcanza el 37% de todo el uso de software.

Los proveedores de software y las empresas pierden casi 46.000 millones de dólares al año por la piratería."
Pero esos son sólo los costos anuales que sufren los vendedores y desarrolladores, como tu, ya que cada copia pirata que hay es un cliente perdido. Sin embargo, más allá de lo obvio, el software pirata dentro de tu organización puede costarte aún más.

Una cosa es perder un cliente, pero otra muy distinta es ser penalizado si una auditoría de software pirata lo detecta en tu organización. Según la Universidad de Stanford:

"La Ley de Derechos de Autor de los Estados Unidos considera a los culpables de la reproducción ilegal de software sujetos a daños civiles de hasta 100.000 dólares por título infringido, y a sanciones penales, incluyendo multas de hasta 250.000 dólares por título infringido y prisión de hasta cinco años."

Estamos hablando de un cuarto de millón por título y de posibles penas de cárcel. A veces, este tiempo de prisión ni siquiera involucra a los responsables directos, sino a los que están más arriba, como los directivos.

Y la cosa no termina ahí, ya que el software pirata también puede aumentar la probabilidad de que se produzcan ciberataques o que se introduzcan diversas formas de malware en tu sistema. Es posible que pienses: "Oye, no es para tanto", pero los costos anuales de los ataques de malware ascienden a 359.000 millones de dólares.

Así que, para evitar todo esto, es necesario adoptar un enfoque proactivo. El software de monitoreo te ayudará a garantizar que todos los rincones de tu organización cumplan con las prácticas legales de software, lo que implica que vas a prevenir pérdidas millonarias y a evitarte a ti y a tus empleados complicaciones innecesarias.

Ahora que tenemos el "por qué" y el "qué", echemos un vistazo al "cómo" se usa dicha herramienta para hacer la auditoría de software pirata

En el ámbito internacional, aunque los programas de computación no fueron explícitamente protegidos por el Convenio de Berna; posiblemente por ello, han sido posteriormente objeto de atención por parte de múltiples convenios internacionales en materia de derechos de autor5, entre ellos y que es norma venezolana, el artículo 4 de la Decisión 351 del Acuerdo de Cartagena que les reconoce protección expresa.

El artículo 3 de la Decisión 351 del Acuerdo de Cartagena, define al programa de computación como la "expresión de un conjunto de instrucciones mediante palabras, códigos, planes o en cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador –un aparato electrónico o similar capaz de elaborar informaciones–, ejecute determinada tarea u obtenga determinado resultado. El programa de ordenador comprende también la documentación técnica y los manuales de uso".

En Venezuela, el artículo 17 de la Ley sobre Derecho de Autor establece que debe entenderse por "programa de computación a la expresión en cualquier modo, lenguaje, notación o código, de un conjunto de instrucciones cuyo propósito es que un computador lleve a cabo una tarea o una función determinada, cualquiera que sea su forma de expresarse o en el soporte material en que se haya realizado la fijación".

Uso de software ilegal y sus consecuencias:

Cualquiera que copie o utilice ilegalmente un programa de computador, podrá ser demandado civil o penalmente. El titular de los derechos de autor podrá solicitar medidas cautelares consistentes en impedir el uso de los programas de computador y exigir la destrucción de todas las copias piratas; el secuestro preventivo de las copias no autorizadas así como de los equipos de cómputo con que fueron realizadas.

La Ley Contra Delitos Informáticos fue publicada en Gaceta Oficial Nº 37.313 el 30 de octubre del 2001. El objetivo de esta ley es ser utilizada como herramienta o instrumento legal para proteger a todas las personas que empleen la utilización de la tecnología de información.

Estas consecuencias legales varían según el país. Por ejemplo en Venezuela existe una legislación al respecto titulada Ley de Delitos Informáticos.

Existe articulo interesante publicado por David Andreani que habla sobre la piratería del software y el marco legal en Venezuela.: https://es.scribd.com/document/578457986/Pirateria-de-Software-en-Venezuela

Debate (país España-2019) sobre el uso intelectual en las redes entre La responsable de cultura de la Cadena SER, Pepa Blanes, y el de Economía, Javier Ruiz explican en La Ventana cómo ha cambiado el consumo de películas o series en internet ---

La criminalidad informática incluye una amplia variedad de delitos informáticos. El fenómeno se puede analizar en dos grupos:

- Informática como medio del delito: Dentro de este grupo se encuentra la falsificación de documentos electrónicos, cajeros automáticos y tarjetas de crédito, robo de identidad, phreaking, fraudes electrónicos y pornografía infantil.

- Informática como objeto del delito: Esta categoría incluye por ejemplo el sabotaje informático, la piratería informática, el hackeo, el crackeo y el DDNS (Denegación de servicio de nombres de dominio).

La piratería informática consiste en la violación ilegal del derecho de autor. Según la definición que en su artículo 51 brinda el ADPIC (Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual) son aquellas "mercaderías que lesionan el derecho de autor". La piratería es una de las modalidades de reproducción técnica (la otra es la reproducción burda del original cuya apariencia dista mucho de la auténtica), que implica la elaboración de una copia semejante al original, con la intención de hacerla pasar por tal.

Modalidades que se incluyen como piratería informática:

Existen dos, a saber:

1. El hurto de tiempo de máquina: consiste en el empleo del computador sin autorización, y se pretende aludir a situaciones en que un tercero utiliza indebidamente recursos de la empresa en que trabaja o un sujeto autorizados se vale de tales prestaciones informáticas en un horario no permitido, utilizándolas para su provecho sin contar con permiso para ese uso fuera de hora.12

2. La apropiación o hurto de hardware y datos: en este caso el sujeto accede a un computador ajeno o a la sesión de otro usuario, retirando archivos informáticos, mediante la ejecución de los comandos copiar o cortar, para luego guardar ese contenido en un soporte propio.

ACTIVIDAD EVALUATIVA DE LA UNIDAD Nro.7:

1.- Que es La piratería digital?

2.- Como se detecta un software pirata en una organización.

3.- Cuáles serían las consecuencias legales del uso de un software ilegal en Venezuela?

4.- Que incluye la criminalidad informática?

5.- Cuales son las modalidades de Piratería Informática?

NORMAS I.S.O.

Unidad VIII

Que son y para qué sirven:

La información es el activo más preciado de cualquier organización en la actualidad. Las empresas almacenan datos confidenciales sobre su negocio. Toda esta información se guarda en equipos informático y puede ser vulnerable si no se protege de forma adecuada.

Para evitar filtraciones o robos, se debe contar con las herramientas necesarias para protegerla correctamente. El Sistema de Gestión en Seguridad de la información se ha creado para que cualquier organización pueda preservar la integridad sus equipos informáticos. Para asegurar la correcta aplicación de este sistema es recomendable obtener la certificación ISO con una auditoría informática. Es la prueba frente a clientes y proveedores de que la corporación se preocupa por la confidencialidad y privacidad.

¿Cuál es el ISO que certifica a la auditoría de sistema?
ISO 19011 - Auditoria de Sistemas de Gestión - Normes ISO.

La norma ISO 19011:2018 es un documento de orientación para las organizaciones que están estableciendo programas de auditoría y realizando auditorías para los sistemas de gestión existentes. Abarca todo el ciclo de vida de los sistemas de auditoría, desde el proyecto hasta la evaluación.

La Organización internacional de Estandarización (ISO) ha elaborado normas para asegurarse de la seguridad informática de las organizaciones. Estas están agrupadas en la familia de normativas ISO 27000.

Las normas ISO son una serie de regulaciones y estándares internacionales aplicables a una amplia gama de sectores y organizaciones. En el contexto de la seguridad informática, estas normas son vitales para asegurar la protección de los sistemas informáticos y la privacidad de los datos.

En una artículo publicado en la página web: https://www.ealde.es/iso-auditoria-informatica/ , por Alejandro Riveros detalla sobre Qué es y para qué sirve una auditoría informática y la importancia para la organización el conseguir la Certificación ISO.

¿Cuáles son las normas ISO en informática?

Las normas ISO más relevantes para la ciberseguridad son la ISO 27001 y la ISO 27002. La primera establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), mientras que la segunda ofrece directrices para el establecimiento de medidas de seguridad efectivas.

1.- ¿Qué es la norma ISO 27007?

ISO/IEC 27007 proporciona orientación para los organismos de certificación acreditados, auditores internos, auditores externos/terceros y otros que auditan los SGSI contra ISO/IEC 27001 (es decir, auditan el sistema de gestión para verificar su conformidad con la norma).

Está diseñada para ayudar a los auditores a evaluar si el SGSI cumple con los requisitos establecidos en la norma ISO 27001 y si se están implementando adecuadamente los controles de seguridad de la información.

La norma ISO 27007 se basa en gran medida en ISO 19011, el estándar para auditar sistemas de gestión, que ofrece orientación específica para el Sistema de Gestión de Seguridad de la Información.

2. ¿Para qué sirve la norma ISO 27007?

La norma ISO 27007 es útil para:

- ✓ Evaluar la eficacia de un SGSI.
- ✓ Identificar las áreas de mejora del SGSI.
- ✓ Demostrar la conformidad con la norma ISO 27001.

- ✓ Mejorar la confianza en los en los sistemas de seguridad de la información.

3. Secciones relevantes

Estas secciones establecen los principios, requisitos y directrices para la gestión y realización de una auditoría de un SGSI basando en la norma ISO 27001.

3.1. Introducción (alcance, propósito, referencias normativas)
3.2. Términos y definiciones
3.3. Principios de auditoría
3.4. Gestión de un programa de auditoría (directrices que incluyen planificación, la programación y la asignación de recursos para auditoría)
3.5. Realización de la auditoría (preparación para la auditoría, recolección de evidencia y la realización de pruebas de auditoría)
3.6. Competencia y evaluación de auditores (proporciona requisitos de competencia y directrices sobre la evaluación de los auditores)
3.7. Informe de auditoría (hallazgos, las no conformidades y las recomendaciones para la mejora del SGSI).

3.8. Seguimiento de la auditoría (verificación de la implementación de las recomendaciones y realización de auditorías de seguimiento.

El estándar cubre todos los aspectos específicos del Sistema de Gestión de Seguridad de la Información de la auditoría de cumplimiento:

- Administración del programa de auditoría del Sistema de Gestión de Seguridad de la Información para determinar que se debe auditar, cuando y como, además de asignar los auditores apropiados, administrar todos los riesgos, mantener registros de auditoría, mejorar de forma continua el proceso, etc.
- Realización de una auditoría, con los que se debe realizar una planificación, establecer una conducta, llevar a cabo las actividades clave de auditoría, incluyendo el trabajo de campo, realizar el análisis, los informes y el seguimiento.
- Gestión de auditores del Sistema de Gestión de Seguridad de la Información, como puede ser competencias, habilidades, atributos y evaluación.

4. ¿Dónde se aplica?

La norma ISO 27007 se puede aplicar a cualquier tipo de organización, ya sea del sector público o privado, pequeñas o grandes, y en cualquier sector o industria.

Puede ser aplicada por auditores internos y externos que estén encargados de realizar auditorías de un SGSI basado en la norma ISO 27001.

Es de gran utilidad para los consultores que asesoran a las organizaciones sobre cómo implementar y mantener un SGSI y para los responsables de la seguridad de la información en las organizaciones que buscan mejorar su sistema de seguridad de la información y demostrar su conformidad con la norma ISO 27001

Existen otras normas también relevantes explicadas en portal de Dolbuck, empresa de ciberseguridad, donde lo explica de forma muy resumida por qué son importantes el conocimiento y uso de las NORMAS ISO.

.

¿Cómo la Inteligencia Artificial (IA) Potencia la ciberseguridad?

ACTIVIDAD EVALUATIVA DE LA UNIDAD Nro.8:

1.- Que entiende usted por ISO?

2.- ¿Cuál es el ISO que certifica a la auditoría de sistema?

3.- ¿Cuáles son las normas ISO en informática?

4.- ¿Qué es la norma ISO 27007?

5.- Según lo aprendido, ¿Cómo la Inteligencia Artificial (IA) Potencia la ciberseguridad?

Recursos Interactivos

AUDITORÍA A LOS SISTEMAS COMO HERRAMIENTA PARA EXAMINAR LOS PROCESOS EN LAS EMPRESAS
https://portal.amelica.org/ameli/jatsRepo/221/2211077005/index.html

VENTAJAS DE REALIZAR UNA AUDITORÍA DE SISTEMAS DE INFORMACIÓN
https://youtu.be/WH8FiuUMCBo?t=21/

QUE ES LA AUDITORIA INFORMATICA POR LA ASOCIACIÓN ESPAÑOLA DE CONTABILIDAD Y ADMINISTRACIÓN DE EMPRESAS SERVICIO INFOAECA
http://aeca.es/old/buscador/infoaeca/articulosespecializados/pdf/auditoria/pdfauditoria/22.pdf

TIPOS DE AUDITORIA
https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica#Tipos_de_auditor%C3%ADa

METODOLOGIAS DE ANALISIS DE RIESGOS: «MAGERIT Y OCTAVE»
https://seguridadenlasredes.wordpress.com/2010/08/12/metodologias-de-analisis-de-riesgos-magerit-y-octave/

METODOLOGÍAS PARA LA AUDITORÍA INFORMÁTICA
https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica#Principales_pruebas_y_herramientas_para_efectuar_una_auditor%C3%ADa_inform%C3%A1tica

PLANEACION DE LA AUDITORIA INFORMATICA
http://www.ucla.edu.ve/dac/departamentos/informaticaii/ejemplo_plan_auditoria_informatica.pdf

COBIT, ITIL e ISO
https://youtu.be/ZteJcV1ajKk?t=6

SISTEMAS DE INFORMACIÓN COMO SOPORTE A LA TOMA DE DECISIONES | | UPV
https://youtu.be/9YD8IZ-Ii-g?t=19

TECNOLOGIA Y TOMA DE DECISIONES
https://youtu.be/T55NGXSzIdk?t=41

CONTROL INTERNO INFORMATICO

https://noris14.wordpress.com/2011/06/10/control-interno-informatico/

HISTORIA DE LA PIRATERIA
https://youtu.be/zZIxgjFxPDE?t=9

LA PIRATERIA A DEBATE
https://youtu.be/L3TUvgACQ3E?t=7

TIPOS DE DELITOS INFORMÁTICOS EN VENEZUELA
https://blog.juridicosvenezuela.com/tipos-de-delitos-informaticos-en-venezuela/

¿QUÉ SON LAS NORMAS ISO Y POR QUÉ SON IMPORTANTES PARA LA CIBERSEGURIDAD?
https://dolbuck.net/proteccion-datos/que-son-las-normas-iso/#:~:text=Las%20normas%20ISO%20m%C3%A1s%20relevantes,de%20medidas%20de%20seguridad%20efectivas.

¿Cómo la Inteligencia Artificial (IA) potencia la ciberseguridad?
https://canvia.com/inteligencia-artificial-ciberseguridad/https:/canvia.com/inteligencia-artificial-ciberseguridad/