Universidad Autónoma del Estado de México
Centro Universitario Valle de Teotihuacán

Programa Educativo de la Licenciatura en Informática Administrativa

Manual de Prácticas de Auditoria Informática

Elaboró: L.I.A. Cecilia Bibiana Ramírez Waldo
Dr. En T.I.E. Oscar Hernández Gómez
M. en Ing. José Francisco Martínez Lendech

Fecha: 24 01 23

Fecha de aprobación	H. Consejo Académico	H. Consejo de Gobierno

INDICE

PRESENTACIÓN

Con el presente manual el estudiante proveerá de escenarios educativos para la integración, aplicación y desarrollo de los conocimientos, habilidades y actitudes que le permitan el desempeño de funciones, tareas y resultados ligados a las dimensiones y ámbitos de intervención profesional o campos emergentes de la misma. Con la finalidad de proponer proyectos de dirección, gestión, asesoramiento, evaluación y control de organizaciones privadas o públicas, lucrativas o no lucrativas; en cualquiera de sus áreas: comercialización e investigación de mercados, producción u operaciones y recursos humanos.

La Auditoria Informática representa el mecanismo que tiene cualquier especialista de la Gestión de Tecnologías de Información para verificar y dar seguimiento al buen desempeño de la función de la Administración de TIC, mediante la generación de auditorías enfocadas tanto a la gestión de TIC´s, seguridad de la información, desempeño de la infraestructura de TIC´s, así como el control de la planeación estratégica informática.

La unidad de aprendizaje tiene un desarrollo descrito por un proceso mediante el cual se preparará al estudiante para desarrollar auditorias informáticas eficientes, determinando los objetivos de la auditoria y en consecuencia la planificación, la ejecución y reporte de esta, coadyuvando así al cumplimiento del perfil de egreso del Licenciado en Informática Administrativa. Donde se facilitan los medios para la resolución de casos, la ejercitación de entrevistas, revisión documental, el ejercicio de la observación, y la generación de simulaciones para la mejor comprensión de una auditoria informática. El alumno deberá ser receptivo para identificar las capacidades posee y cuales tiene que desarrollar para realizar auditorías informáticas de manera eficiente.

Por tanto, siempre ha existido una preocupación por parte de las organizaciones por optimizar todos los recursos con que cuenta la empresa, sin embargo, por lo que respecta a la tecnología o los equipos de cómputo, generalizándolos en el hardware, software, redes, bases de datos, telecomunicaciones, por mencionar algunos sectores de la informática, la cual representa una herramienta estratégica que representa rentabilidad y ventaja competitiva frente a sus similares en el mercado, el este sector el ámbito de los sistemas de información y tecnología en un alto porcentaje de las empresas con el manejo de control, considerando tanto datos como los elementos que almacena, procesa y distribuye.

Si bien, la auditoría informática se define como la orientación evaluada en los sistemas administrativos, es decir la estructura de la organización, el proceso administrativo, la operación y el ambiente de control establecido. Determinar: pérdidas y diferencias, mejores métodos, formas de control, eficiencia operativa y una mejor utilización de los recursos físicos y humanos.

En suma, en una auditoría informática en el área administrativa, se determina que es aquel examen completo que se realiza en una empresa u organización, la misma que debe cumplir con sus diferentes fases como son la planeación, organización, ejecución y el control administrativo, de esta manera se realiza con éxito el propósito de ver el desempeño de cada nivel e identificar la debilidad que se llegue a presentar, para generar una acción en la toma de decisiones.

La auditoría informática es realizada por una serie de procesos los cuales son efectuados por profesionales principalmente los que estén preparados y sean responsables, para almacenar, adjuntar y evaluar toda evidencia que sea establecida sin la necesidad de tener un sistema de información, el cual resguarde todas las actividades y su información de la empresa, solo así se podrá verificar que la integridad de los datos de la organización sean eficaces y se utilicen los

recursos de manera correcta, cumpliendo con las leyes y regulaciones (Imbaquingo, et al., 2020)

PRACTICA No. 1

Conceptos de auditoria

DURACIÓN:
2 horas

INTRODUCCIÓN:
Es la evaluación y verificación de las políticas, controles, procedimientos y la seguridad en general, correspondiente al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección), a fin de que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Según José A. Echenique, la auditoría en informática “es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistemas o procedimiento especifico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles archivos, seguridad y obtención de información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización especifica que hará posible el uso de los equipos de cómputo”.

Según Mario Piattini Velthuis, la auditoría informática es “el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

OBJETIVO(S):

Comprender los elementos básicos necesarios de la auditoria mediante la identificación de conceptos, metodologías, normas y buenas prácticas informáticas para la realización de una auditoria informática.

REQUISITOS:

- Contar con Manual de Prácticas de laboratorio impreso
- Presentar el material necesario para realizar la práctica

MATERIAL Y EQUIPO PARA UTILIZAR:

- Equipo de cómputo

DESARROLLO:

La importancia de una auditoría informática dentro del proceso productivo de una empresa debe evolucionar consciente y reflexivamente a la par que se van obteniendo beneficios inducidos y subyacentes de un sistema informático sólido integrado a la perfección con todas las estructuras legales, jurídicas, económicas, sociales e incluso culturales en la que se desarrolla la organización.

Un proceso de auditoría correcto traerá importantes beneficios para cualquier negocio. Desafortunadamente, para algunas personas, parece que una auditoría sólo acarrea una gran cantidad de trastornos al final, pero en realidad una auditoría no sólo es importante para el funcionamiento interno de la empresa, sino también para la solidificación de la misma y para el sostenimiento progresivo de sus órganos reguladores totalmente alineados con la política de la corporación, sino además organizaciones benéficas que puedan depender de ella, para su junta de accionistas e incluso para potenciales fondos de inversión de los que pueda formar parte la empresa auditada. Precisamente por esto es por lo que los procesos de auditoría representan para las grandes y medianas empresas un requisito legal que justifica cualquier esfuerzo, principalmente, porque el único y verdadero beneficiado del mismo, es la propia empresa y todo el mundo que participa de una manera directa o indirecta de su actividad económica, que a la postre determina su valor real frente a la sociedad y el resto de organizaciones sociales y económicas del país.

Por lo tanto, una auditoría informática ayuda a aumentar la confianza de los clientes, lo que facilita la inversión en la actividad económica y aumenta la credibilidad y el potencial de financiación en el mercado. Del mismo modo, un proceso de auditoría sólido proporciona un nivel independiente de control sobre los sistemas y la gestión de registros para garantizar que se mitiguen los riesgos futuros de sorpresas desagradables, como la pérdida de datos, la seguridad de los

datos, equipos y los ataques al software propio. En consecuencia, la conceptualización adecuada de la auditoria es el parteaguas para una correcta comprensión y aplicación de las percepciones como auditor.

Ejemplo:

1. Analiza la conceptualización básica de auditoria informática.

Evaluación

Consiste en analizar mediante pruebas la calidad y cumplimiento de funciones, actividades y procedimientos que se realizan en una organización o área. Las evaluaciones se utilizan para valorar registros, planes, presupuestos, programas, controles y otros aspectos que afectan la administración y control de una organización o las áreas que la integran. La evaluación se aplica para investigar algún hecho, comprobar alguna cosa, verificar la forma de realizar un proceso, evaluar la aplicación de técnicas, métodos o procedimientos de trabajo, verificar el resultado de una transacción, comprobar la operación correcta de un sistema software entre otros muchos aspectos.

Inspección

La inspección permite evaluar la eficiencia y eficacia del sistema, en cuanto a operación y procesamiento de datos para reducir los riesgos y unificar el trabajo hasta finalizarlo. La inspección se realiza a cualquiera de las actividades, operaciones y componentes que rodean los sistemas.

Confirmación

El aspecto más importante en la auditoria es la confirmación de los hechos y la certificación de los datos que se obtienen en la revisión, ya que el resultado final de la auditoria es la emisión de un dictamen donde el auditor expone sus

opiniones, este informe es aceptado siempre y cuando los datos sean veraces y confiables. No se puede dar un dictamen en base a suposiciones o emitir juicios que no sean comprobables.

Comparación

Otra de las técnicas utilizadas en la auditoria es la comparación de los datos obtenidos en un área o en toda la organización y cotejando esa información con los datos similares o iguales de otra organización con características semejantes. En auditoria a los sistemas software se realiza la comparación de los resultados obtenidos con el sistema y los resultados con el procesamiento manual, el objetivo de dicha comparación es comprobar si los resultados son iguales, o determinar las posibles desviaciones, y errores entre ellos.

Revisión Documental

Otra de las herramientas utilizadas en la auditoria es la revisión de documentos que soportan los registros de operaciones y actividades de una organización. Aquí se analiza el registro de actividades y operaciones plasmadas en documentos y archivos formales, con el fin de que el auditor sepa cómo fueron registrados las operaciones, resultados y otros aspectos inherentes al desarrollo de las funciones y actividades normales de la organización. En esta evaluación se revisan manuales, instructivos, procedimientos, funciones y actividades. El registro de resultados, estadísticas, la interpretación de acuerdos, memorandos, normas, políticas y todos los aspectos formales que se asientan por escrito para el cumplimiento de las funciones y actividades en la administración de las organizaciones.

Matriz de Evaluación

Es uno de los documentos de mayor utilidad para recopilar información relacionada con la actividad, operación o función que se realiza en el área informática, así como también se puede observar anticipadamente su cumplimiento. La escala de valoración puede ir desde la mínima con puntaje 1 (baja, deficiente) hasta la valoración máxima de 5(superior, muy bueno, excelente). Cada una de estas valoraciones deberá tener asociado la descripción del criterio por el cual se da ese valor. Esta matriz permite realizar la valoración del cumplimiento de una función específica de la administración del centro de cómputo, en la verificación de actividades de cualquier función del área de informática, del sistema software, del desarrollo de proyectos software, del servicio a los usuarios del sistema o cualquier otra actividad del área de informática en la organización.

Matriz FODA

Este es un método de análisis y diagnóstico usado para la evaluación de un centro de cómputo, que permite la evaluación del desempeño de los sistemas software, aquí se evalúan los factores internos y externos, para que el auditor puede evaluar el cumplimiento de la misión y objetivo general del área de informática de la organización.

En adición, las mejores prácticas en auditoria recomiendan Cobit como la herramienta estándar para tecnologías de información más utilizada en la ejecución de auditorías; a continuación, se explica detalladamente algunos conceptos manejados por ésta y los dominios, procesos y actividades que lo conforman:

Efectividad. Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

Eficiencia. Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.
Confidencialidad. Se refiere a la protección de información sensible contra divulgación no autorizada.

Integridad. Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

Disponibilidad. Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Cumplimiento. Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.

Confiabilidad de la información. Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Datos. Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
Aplicaciones. Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

Tecnología. La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
Instalaciones. Recursos para alojar y dar soporte a los sistemas de información.

Personal. Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Niveles de Cobit: La estructura del estándar Cobit se divide en dominios que son agrupaciones de procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible.

2. Elabora las tablas de distribución de dominios, procesos y objetivos de control de la metodología COBIT.

DOMINIOS	PROCESOS	OBJETIVOS DE CONTROL
PLANIFICAR Y ORGANIZAR	PO1 Definir un Plan Estratégico de TI	PO1.1 Administración del Valor de TI
		PO1.2 Alineación de TI con el Negocio
		PO1.3 Evaluación del Desempeño y la Capacidad Actual
		PO1.4 Plan Estratégico de TI
		PO1.5 Planes Tácticos de TI
		PO1.6 Administración del Portafolio de TI
	PO2 Definir la Arquitectura de la Información	PO2.1 Modelo de Arquitectura de Información Empresarial
		PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos
		PO2.3 Esquema de Clasificación de Datos
		PO2.4 Administración de Integridad
	PO3 Determinar la Dirección Tecnológica	PO3.1 Planeación de la Dirección Tecnológica
		PO3.2 Plan de Infraestructura Tecnológica
		PO3.3 Monitoreo de Tendencias y Regulaciones Futuras
		PO3.4 Estándares Tecnológicos
		PO3.5 Consejo de Arquitectura de TI
	PO4 Definir los Procesos, Organización y Relaciones de TI	PO4.1 Marco de Trabajo de Procesos de TI
		PO4.2 Comité Estratégico de TI
		PO4.3 Comité Directivo de TI
		PO4.4 Ubicación Organizacional de la Función de TI
		PO4.5 Estructura Organizacional
		PO4.6 Establecimiento de Roles y Responsabilidades
		PO4.7 Responsabilidad de Aseguramiento de Calidad TI

PLANIFICAR Y ORGANIZAR		PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento
		PO4.9 Propiedad de Datos y de Sistema
		PO4.10 Supervisión
		PO4.11 Segregación de Funciones
		PO4.12 Personal de TI
		PO4.13 Personal Clave de TI
		PO4.14 Políticas y Procedimientos para Personal Contratado
		PO4.15 Relaciones
	PO5 Administrar la Inversión en TI	PO5.1 Marco de Trabajo para la Administración Financiera
		PO5.2 Prioridades Dentro del Presupuesto de TI
		PO5.3 Proceso Presupuestal
		PO5.4 Administración de Costos de TI
		PO5.5 Administración de Beneficios
	PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	PO6.1 Ambiente de Políticas y de Control
		PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI
		PO6.3 Administración de Políticas para TI
		PO6.4 Implantación de Políticas de TI
		PO6.5 Comunicación de los Objetivos y la Dirección de TI
	PO7 Administrar Recursos Humanos de TI	PO7.1 Reclutamiento y Retención del Personal
		PO7.2 Competencias del Personal
		PO7.3 Asignación de Roles
		PO7.4 Entrenamiento del Personal de TI
		PO7.5 Dependencia Sobre los Individuos
		PO7.6 Procedimientos de Investigación del Persona
		PO7.7 Evaluación del Desempeño del Empleado
		PO7.8 Cambios y Terminación de Trabajo
	PO8 Administrar la Calidad	PO8.1 Sistema de Administración de Calidad
		PO8.2 Estándares y Prácticas de Calidad
		PO8.3 Estándares de Desarrollo y de Adquisición
		PO8.4 Enfoque en el Cliente de TI
		PO8.5 Mejora Continua
		PO8.6 Medición, Monitoreo y Revisión de la Calidad
	PO9 Evaluar y Administrar los Riesgos de TI	PO9.1 Marco de Trabajo de Administración de Riesgos
		PO9.2 Establecimiento del Contexto del Riesgo
		PO9.3 Identificación de Eventos
		PO9.4 Evaluación de Riesgos de TI
		PO9.5 Respuesta a los Riesgos
		PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos
		PO10.1 Marco de Trabajo para la Administración de Programas

	PO10 Administrar Proyectos	PO10.2 Marco de Traba
		PO10.3 Enfoque de Administración de Proyectos
		PO10.4 Compromiso de los Interesados
		PO10.5 Declaración de Alcance del Proyecto
		PO10.6 Inicio de las Fases del Proyecto
		PO10.7 Plan Integrado del Proyecto
		PO10.8 Recursos del Proyecto
		PO10.9 Administración de Riesgos del Proyecto
		PO10.10 Plan de Calidad del Proyecto
		PO10.11 Control de Cambios del Proyecto
		PO10.13 Medición del Desempeño, Reporte y Monitoreo del Proyecto
		PO10.14 Cierre del Proyecto
ADQUIRIR E IMPLEMENTAR	AI1 Identificar soluciones automatizadas	AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio
		AI1.2 Reporte de Análisis de Riesgos
		AI1.3 Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos
		AI1.4 Requerimientos, Decisión de Factibilidad y Aprobación
	AI2 Adquirir y Mantener Software Aplicativo	AI2.1 Diseño de Alto Nivel
		AI2.2 Diseño Detallado
		AI2.3 Control y Posibilidad de Auditar las Aplicaciones
		AI2.4 Seguridad y Disponibilidad de las Aplicaciones
		AI2.5 Configuración e Implementación de Software Aplicativo Adquirido
		AI2.6 Actualizaciones Importantes en Sistemas Existentes
		AI2.7 Desarrollo de Software Aplicativo
		AI2.8 Aseguramiento de la Calidad del Software
		AI2.9 Administración de los Requerimientos de Aplicaciones
		AI2.10 Mantenimiento de Software Aplicativo
	AI3 Adquirir y Mantener Infraestructura Tecnológica	AI3.1 Plan de Adquisición de Infraestructura Tecnológica
		AI3.2 Protección y Disponibilidad del Recurso de Infraestructura
		AI3.3 Mantenimiento de la infraestructura
		AI3.4 Ambiente de Prueba de Factibilidad
	AI4 Facilitar la Operación y el Uso	AI4.1 Plan para Soluciones de Operación
		AI4.2 Transferencia de Conocimiento a la Gerencia del Negocio
		AI4.3 Transferencia de Conocimiento a Usuarios Finales
		AI4.4 Transferencia de Conocimiento al Personal de Operaciones y Soporte
	AI5 Adquirir Recursos de TI	AI5.1 Control de Adquisición
		AI5.2 Administración de Contratos con Proveedores
		AI5.3 Selección de Proveedores
		AI5.4 Adquisición de Recursos TI

	AI6 Administrar Cambios	AI6.1 Estándares y Procedimientos para Cambios
		AI6.2 Evaluación de Impacto, Priorización y Autorización
		AI6.3 Cambios de Emergencia
		AI6.4 Seguimiento y Reporte del Estatus de Cambio
		AI6.5 Cierre y Documentación del Cambio
	AI7 Instalar y Acreditar Soluciones y Cambios	AI7.1 Entrenamiento
		AI7.2 Plan de Prueba
		AI7.3 Plan de Implementación
		AI7.4 Ambiente de Prueba
		AI7.5 Conversión de Sistemas y Datos
		AI7.6 Pruebas de Cambios
		AI7.7 Prueba de Aceptación Final
		AI7.8 Promoción a Producción
		AI7.9 Revisión Posterior a la Implantación
ENTREGAR Y DAR SOPORTE	DS1 Definir y administrar los niveles de servicio	DS1.1 Marco de Trabajo de la Administración de los Niveles de Servicio
		DS1.2 Definición de Servicios
		DS1.3 Acuerdos de Niveles de Servicio
		DS1.4 Acuerdos de Niveles de Operación
		DS1.5 Monitoreo y Reporte del Cumplimiento de los Niveles de Servicio
		DS1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos
	DS2 Administrar los Servicios de Terceros	DS2.1 Identificación de Todas las Relaciones con Proveedores
		DS2.2 Gestión de Relaciones con Proveedores
		DS2.3 Administración de Riesgos del Proveedor
		DS2.4 Monitoreo del Desempeño del Proveedor
	DS3 Administrar el Desempeño y la Capacidad	DS3.1 Planeación del Desempeño y la Capacidad
		DS3.2 Capacidad y Desempeño Actual
		DS3.3 Capacidad y Desempeño Futuros
		DS3.4 Disponibilidad de Recursos de TI
		DS3.5 Monitoreo y Reporte
	DS4 Garantizar la Continuidad del Servicio	DS4.1 Marco de Trabajo de Continuidad de TI
		DS4.2 Planes de Continuidad de TI
		DS4.3 Recursos Críticos de TI
		DS4.4 Mantenimiento del Plan de Continuidad de TI
		DS4.5 Pruebas del Plan de Continuidad de TI
		DS4.6 Entrenamiento del Plan de Continuidad de TI
		DS4.7 Distribución del Plan de Continuidad de TI
		DS4.8 Recuperación y Reanudación de los Servicios de TI
		DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
		DS4.10 Revisión Post Reanudación

ENTREGAR Y DAR SOPORTE	DS5 Garantizar la Seguridad de los Sistemas	DS5.1 Administración de la Seguridad de TI
		DS5.2 Plan de Seguridad de TI
		DS5.3 Administración de Identidad
		DS5.4 Administración de Cuentas del Usuario
		DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
		DS5.6 Definición de Incidente de Seguridad
		DS5.7 Protección de la Tecnología de Seguridad
		DS5.8 Administración de Llaves Criptográficas
		DS5.9 Prevención, Detección y Corrección de Software Malicioso
		DS5.10 Seguridad de la Red
		DS5.11 Intercambio de Datos Sensitivos
	DS6 Identificar y Asignar Costos	DS6.1 Definición de Servicios
		DS6.2 Contabilización de TI
		DS6.3 Modelación de Costos y Cargos
		DS6.4 Mantenimiento del Modelo de Costos
	DS7 Educar y Entrenar a los Usuarios	DS7.1 Identificación de Necesidades de Entrenamiento y Educación
		DS7.2 Impartición de Entrenamiento y Educación
		DS7.3 Evaluación del Entrenamiento Recibido
	DS8 Administrar la Mesa de Servicio y los Incidentes	DS8.1 Mesa de Servicios
		DS8.2 Registro de Consultas de Clientes
		DS8.3 Escalamiento de Incidentes
		DS8.4 Cierre de Incidentes
		DS8.5 Análisis de Tendencias
	DS9 Administrar la Configuración	DS9.1 Repositorio y Línea Base de Configuración
		DS9.2 Identificación y Mantenimiento de Elementos de Configuración
		DS9.3 Revisión de Integridad de la Configuración
	DS10 Administración de Problemas	DS10.1 Identificación y Clasificación de Problemas
		DS10.2 Rastreo y Resolución de Problemas
		DS10.3 Cierre de Problemas
		DS10.4 Integración de las Administraciones de Cambios, Configuración y Problemas
	DS11 Administración de Datos	DS11.1 Requerimientos del Negocio para Administración de Datos
		DS11.2 Acuerdos de Almacenamiento y Conservación
		DS11.3 Sistema de Administración de Librerías de medios
		DS11.4 Eliminación
		DS11.5 Respaldo y Restauración
		DS11.6 Requerimientos de Seguridad para la Administración de Datos
	DS12 Administración del Ambiente Físico	DS12.1 Selección y Diseño del Centro de Datos
		DS12.2 Medidas de Seguridad Física
		DS12.3 Acceso Físico

		DS12.4 Protección Contra Factores Ambientales
		DS12.5 Administración de Instalaciones Físicas
	DS13 Administración de Operaciones	DS13.1 Procedimientos e Instrucciones de Operación
		DS13.2 Programación de Tareas
		DS13.3 Monitoreo de la Infraestructura de TI
		DS13.4 Documentos Sensitivos y Dispositivos de Salida
		DS13.5 Mantenimiento Preventivo del Hardware
MONITOREAR Y EVALUAR	ME1 Monitorear y Evaluar el Desempeño de TI	ME1.1 Enfoque del Monitoreo
		ME1.2 Definición y Recolección de Datos de Monitoreo
		ME1.3 Método de Monitoreo
		ME1.4 Evaluación del Desempeño
		ME1.5 Reportes al Consejo Directivo y a Ejecutivos
		ME1.6 Acciones Correctivas
	ME2 Monitorear y Evaluar el Control Interno	ME2.1 Monitoreo del Marco de Trabajo de Control Interno
		ME2.2 Revisiones de Auditoría
		ME2.3 Excepciones de Control
		ME2.4 Control de Auto Evaluación
		ME2.5 Aseguramiento del Control Interno
		ME2.6 Control Interno para Terceros
		ME2.7 Acciones Correctivas
MONITOREAR Y EVALUAR	ME3 Garantizar el Cumplimiento con Requerimientos Externos	ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales
		ME3.2 Optimizar la Respuesta a Requerimientos Externos
		ME3.3 Evaluación del Cumplimiento con Requerimientos Externos
		ME3.4 Aseguramiento Positivo del Cumplimiento
		ME3.5 Reportes Integrados
	E4.1 Establecimiento de un Marco de Gobierno de TI	E4.1 Establecimiento de un Marco de Gobierno de TI
		ME4.2 Alineamiento Estratégico
		ME4.3 Entrega de Valor
		ME4.4 Administración de Recursos
		ME4.5 Administración de Riesgos
		ME4.6 Medición del Desempeño
		ME4.7 Aseguramiento Independiente

CONCLUSIONES:

Analizar las herramientas y procedimientos en las diferentes áreas del entorno informático, para verificar que los sistemas y procesos informáticos se realicen acorde a las funciones para los que han sido programados y sus activos digitales

se encuentren debidamente protegidos, frente a cualquier tipo de contingencia que se presente en las organizaciones comprendiendo los elementos básicos de la auditoria informática, para una buena aplicabilidad.

CUESTIONARIO:

¿Qué es auditoria?

¿Qué es auditoria informática?

¿Qué es la metodología COBIT?

PRACTICA No. 2

Gestión de un programa de auditoria

DURACIÓN:
2 horas

INTRODUCCIÓN:

El primer paso para realizar una auditoría de sistemas es la planeación de cómo se va a ejecutar la auditoria, donde se debe identificar de forma clara las razones por las que se va a realizar la auditoria, la determinación del objetivo de la misma, el diseño de métodos, técnicas y procedimientos necesarios para llevarla a cabo y para la solicitud de documentos que servirán de apoyo para la ejecución, terminando con la elaboración de la documentación de los planes, programas y presupuestos para llevarla a cabo.

Identificar el origen de la auditoria: Este es el primer paso para iniciar la planeación de la auditoria, en esta se debe determinar por qué surge la necesidad o inquietud de realizar una auditoría. Las preguntas que se deben contestar ¿de dónde?, ¿por qué?, ¿quién? o ¿para qué? Se quiere hacer la evaluación de algún aspecto de los sistemas de la empresa.

Visita Preliminar al Área informática: Este es el segundo paso en la planeación de la auditoria y consiste en realizar una visita preliminar al área de informática que será auditada, luego de conocer el origen de la petición de realizar la auditoria y antes de iniciarla formalmente; el propósito es el de tener un primer contacto con el personal asignado a dicha área, conocer la distribución de los sistemas y donde se localizan los servidores y equipos terminales en el centro de cómputo, sus

características, las medidas de seguridad y otros aspectos sobre que problemáticas que se presentan en el área auditada.

Aquí se deben tener en cuenta aspectos tales como:

- La visita inicial para el arranque de la auditoria cuya finalidad es saber:

¿Cómo se encuentran distribuidos los equipos en el área?,

¿Cuántos, cuáles, cómo y de que tipo son los servidores y terminales que existen en el área?,

¿Qué características generales de los sistemas que serán auditados?,

¿Qué tipo de instalaciones y conexiones físicas existen en el área?,

¿Cuál es la reacción del personal frente al auditor?,

¿Cuáles son las medidas de seguridad física existentes en el área?, y

¿Qué limitaciones se observan para realizar la auditoria?

Con esta información el auditor podrá diseñar las medidas necesarias para una adecuada planeación de la auditoria y establecer algunas acciones concretas que le ayuden al desarrollo de la evaluación.

OBJETIVO(S):

Realizar un programa de auditoría en una organización específica, mediante su implementación, seguimiento, revisión y mejora continua para gestionarlo.

REQUISITOS:

- Contar con Manual de Prácticas de laboratorio impreso
- Presentar el material necesario para realizar la práctica

MATERIAL Y EQUIPO PARA UTILIZAR:

- Equipo de cómputo

DESARROLLO:

1. **Establecer los Objetivos de la Auditoria:** Los objetivos de la planeación de la auditoria son:

El objetivo general que es el fin global de lo que se pretende alcanzar con el desarrollo de la auditoría informática y de sistemas, en el se plantean todos los aspectos que se pretende evaluar.

Los objetivos específicos que son los fines individuales que se pretenden para el logro del objetivo general, donde se señala específicamente los sistemas, componentes o elementos concretos que deben ser evaluados.

Determinar los Puntos que serán evaluados: Una vez determinados los objetivos de la auditoria se debe relacionar los aspectos que serán evaluados, y para esto se debe considerar aspectos específicos del área informática y de los sistemas computacionales tales como: la gestión administrativa del área informática y el centro de cómputo, el cumplimiento de las funciones del personal informático y usuarios de los sistemas, los sistemas en desarrollo, la operación de los sistemas en producción, los programas de capacitación para el personal del área y usuarios de los sistemas, protección de las bases de datos, datos confidenciales y accesos a las mismas, protección de las copias de seguridad y la restauración de la información, entre otros aspectos.

Elaborar Planes, programas y Presupuestos para Realizar la auditoria: Para realizar la planeación formal de la auditoria informática y de sistemas, en la cual se concretan los planes, programas y presupuestos para llevarla a cabo se debe elaborar los documentos formales para el desarrollo de la auditoria, donde se delimiten las etapas, eventos y actividades y los tiempos de ejecución para el

cumplimiento del objetivo, anexando el presupuesto con los costos de los recursos que se utilizarán para llevarla a cabo.

Algunos de los aspectos a tener en cuenta serán: Las actividades que se van a realizar, los responsables de realizarlas, los recursos materiales y los tiempos; El flujo de eventos que sirven de guía; la estimación de los recursos humanos, materiales e informáticos que serán utilizados; los tiempos estimados para las actividades y para la auditoria; los auditores responsables y participantes de las actividades; Otras especificaciones del programa de auditoría.

Identificar y seleccionar los Métodos, herramientas, Instrumentos y Procedimientos necesarios para la Auditoria: En este se determina la documentación y medios necesarios para llevar a cabo la revisión y evaluación en la empresa, seleccionando o diseñando los métodos, procedimientos, herramientas, e instrumentos necesarios de acuerdo a los planes, presupuestos y programas establecidos anteriormente para la auditoria. Para ello se debe considerar los siguientes puntos: establecer la guía de ponderación de cada uno de los puntos que se debe evaluar; Elaborar una guía de la auditoria; elaborar el documento formal de la guía de auditoría; determinar las herramientas, métodos y procedimientos para la auditoria de sistemas; Diseñar los sistemas, programas y métodos de pruebas para la auditoria.

Asignar los Recursos y Sistemas computacionales para la auditoria: Finalmente se debe asignar los recursos que serán utilizados para realizar la auditoria. Con la asignación de estos recursos humanos, informáticos, tecnológicos y de cualquier otro tipo se llevará a cabo la auditoria.

Etapa de Ejecución de la Auditoria

La siguiente etapa después de la planeación de la auditoria es la ejecución de esta, y está determinada por las características propias, los puntos elegidos y los requerimientos estimados en la planeación.

Etapa de Dictamen de la Auditoria

La tercera etapa Lugo de la planeación y ejecución es emitir el dictamen, que es el resultado final de la auditoria, donde se presentan los siguientes puntos: la elaboración del informe de las situaciones que se han detectado, la elaboración del dictamen final y la presentación del informe de auditoría.

Analizar la información y elaborar un informe de las situaciones detectadas: Junto con la detección de las oportunidades de mejoramiento se debe realizar el análisis de los papeles de trabajo y la elaboración del borrador de las oportunidades detectadas, para ser discutidas con los auditados, después se hacen las modificaciones necesarias y posteriormente el informe final de las situaciones detectadas.

Elaborar el Dictamen Final: El auditor debe terminar la elaboración del informe final de auditoría y complementarlo con el dictamen final, para después presentarlo a los directivos del área auditada para que conozcan la situación actual del área, antes de presentarlo al representante o gerente de la empresa.

Una vez comentadas las desviaciones con los auditados, se elabora el informe final, lo cual es garantía de que los auditados ya aceptaron las desviaciones encontradas y que luego se llevan a documentos formales.

Elaborar el Dictamen Formal: El último paso de esta metodología es presentar formalmente el informe y el dictamen de la auditoria al más alto de los directivos

de la empresa donde se informa de los resultados de la auditoria. Tanto el informe como el dictamen deben presentarse en forma resumida, correcta y profesional.

La presentación de esta se hace en una reunión directiva y por eso es indispensable usar un lenguaje claro tanto en el informe como en la exposición de este. El informe debe contener los siguientes puntos: la carta de presentación, el dictamen de la auditoria, el informe de situaciones relevantes y los anexos y cuadros estadísticos.

Al elaborar el dictamen formal se hace tomando en cuenta el informe comentado a los directivos, junto al formato de hallazgos o desviaciones y los papeles de trabajo de cada uno de los auditores. La integración del dictamen y el informe final de auditoría deben ser elaborados con la máxima perfección, tratando de evitar errores. También deben contener de manera clara y concreta, las desviaciones detectadas en la evaluación.

Tabla 1: Etapas proceso de autoría de sistemas

FASE	ACTIVIDADES
Conocimiento del sistema o área auditada	1. Identificar el origen de la auditoria. 2. Realizar visitas para conocer procesos, activos informáticos, procesos y organización del área auditada. 3. Determinar las vulnerabilidades, y amenazas informáticas a que está expuesta la organización. 4. Determinar el objetivo de la auditoría de acuerdo a las vulnerabilidades, y amenazas informáticas encontradas.
Planeación de la Auditoria de Sistemas	1. Elaborar el plan de auditoría 2. Seleccionar los estándares a utilizar de acuerdo al objetivo (CobIT, MAGERIT, ISO/IEC 27001, ISO/IEC 27002, otro) 3. De acuerdo al estándar elegido, seleccionar los ítems que serán evaluados que estén en relación directa con el objetivo y alcances definidos en el plan. 4. Seleccionar el equipo de trabajo y asignar tareas específicas 5. Determinar las actividades que se llevarán a cabo y los tiempos en que serán llevadas a cabo en cada ítem evaluado. (Programa de auditoría) 6. Diseñar instrumentos para recolección de información (formatos de entrevistas, formatos de listas de chequeo, formatos de cuestionarios) 7. Diseñar el plan de pruebas (formato pruebas)
Ejecución de la Auditoria de Sistemas	1. Aplicar los instrumentos de recolección de información diseñados 2. Ejecutar las pruebas del plan de pruebas 3. Levantar la información de activos informáticos de la organización auditada 4. Determinar las vulnerabilidades y amenazas informáticas aplicando una metodología (MAGERIT) 5. Realizar la valoración de las amenazas y vulnerabilidades encontradas y probadas 6. Realizar el proceso de evaluación de riesgos 7. Determinar el tratamiento de los riesgos
Resultados de la Auditoria de Sistemas	1. Determinar las soluciones para los hallazgos encontrados (controles) 2. Elaborar el Dictamen para cada uno de los procesos evaluados. 3. Elaborar el informe final de auditoría para su presentación y sustentación 4. Integrar y organizar los papeles de trabajo de la auditoria 5. Diseñar las políticas y procedimientos integrando los controles definidos

2. Iniciar con los inventarios de software y hardware, ejemplo:

Tabla 2. Inventario de Software

Inventario de Software		
Área	**Software**	**Licencia**
Servidor	Sistema Operativo Linux	Si
	EFIMAX (Software de Administración Contable)	Si
	Base de Datos EFIMAX	Si
Contabilidad	Sistema Operativo Windows XP Professional	No
	Microsoft Office 2003	Si
	EFIMAX	Si
	Antivirus Kaspersky Total Security	Si
	Anexos Transaccional SRI	Si
	Comprimidor Winzip 8.1	Si
	Nero Burning 6	Si
	Microsoft Internet Explorer	Si
Jefe de Contabilidad	Sistema Operativo Windows 8	No
	Microsoft Office 2007	Si
	EFIMAX (Software de Administración Contable)	Si
	Microsoft Internet Explorer	Si
Contadora	Sistema Operativo Windows 8	No
	Microsoft Office 2007	Si
	EFIMAX (Software de Administración Contable)	Si
	Microsoft Internet Explorer	Si
	Comprimidor Winzip 8.1	Si
	Nero Burning 6	Si
Presupuesto	Sistema Operativo Windows 8	No
	Microsoft Office 2007	Si
	EFIMAX (Software de Administración Contable)	Si
	Microsoft Internet Explorer	Si
	Comprimidor Winzip 8.1	Si
	Nero Burning 6	Si
Dirección Financiera	Sistema Operativo Windows 7	No
	Microsoft Office 2007	No
	EFIMAX (Software de Administración Contable)	Si
	Microsoft Internet Explorer	Si
	Comprimidor Winzip	Si

Tabla 3. Inventario de Hardware

1.7 Área	1.8 Equipo
Jefe de Contabilidad	CPU: Intel Pentium IV 5.2 GHz 256 MB de RAM, 80 GB (Disco Duro Samsung) Monitor Samsung SVGA 15" Teclado Genius PS/2 Mouse Genius PS/2 MODEM 56.6 Kbps Tarjeta de Red 30/100 Mbps Impresa LX – 300 Matricial
Contadora	CPU: Intel Pentium IV 5.2 GHz 256 MB de RAM, 80 GB (Disco Duro Samsung) Monitor Samsung SVGA 15" Teclado Genius PS/2 Mouse Genius PS/2 MODEM 56.6 Kbps Tarjeta de Red 50/100 Mbps Impresora HP – 650C inyección a tinta
Presupuestario	CPU: Intel Pentium IV 6.2 450 MB de RAM, 80 GB (Disco Duro Samsung) Monitor Samsung SVGA 15" Teclado Genius PS/2 Mouse Genius PS/2 MODEM 56.6 Kbps Tarjeta de Red 50/100 Mbps Impresora Samsung ML 8500 Láser
Asistente Contabilidad	CPU: Intel Pentium III 1.00 GHz 256 MB de RAM, 50 GB (Disco Duro Samsung) Monitor LG SVGA 14" Teclado Genius PS/2 Mouse Genius PS/2 MODEM 56.6 Kbps Tarjeta de Red 30/100 Mbps Impresora multifunción Lexmark XL - 2500
Tesorería	CPU: Intel Pentium IV 28 GHz 256 MB de RAM, 80 GB (Disco Duro Samsung) Monitor Samsung SVGA 15" Teclado Genius PS/2 Mouse Genius PS/2 MODEM 56.6 Kbps Tarjeta de Red 20/100 Mbps Impresora Multifunción Lexmark XL - 2500

CONCLUSIONES:

En el análisis del inventario de software y hardware se puede determinar las características similares de los quipos que han sido adquiridos en conjunto, para poder recuperar o dar de baja los obsoletos o brindar soporte necesario.

CUESTIONARIO:

¿Cuáles son las actividades de la fase del conocimiento del sistema o área auditada?

¿Cuáles son las actividades de la fase de planeación de auditoría de sistemas?

¿Cuáles son las actividades de la fase de ejecución de auditoría de sistemas?

¿Cuáles son las actividades de la fase de resultados de auditoría de sistemas?

PRACTICA No. 3

Realización de plan de auditoria

DURACIÓN:
6 horas

INTRODUCCIÓN:

Plan de Auditoria

Antecedentes: En las Aulas de informática de una Institución educativa se realiza anualmente un plan de seguimiento a todos los procesos técnicos y académicos de la institución, esto debido a que las instituciones requieren la acreditación de calidad en el manejo de sus procesos y para ello se hace necesario realizar auditorías internas permanentes y de tipo externo periódicamente para lograrlo.

Uno de los recursos tecnológicos disponibles en las instituciones educativas es el de la red de datos que opera en las diferentes sedes y que generalmente se encuentra certificada bajo las normas de la IEEE\EIA\TIA, las cuales se deben cumplir estrictamente.

Objetivos

- **Objetivo general:** Realizar la revisión y verificación del cumplimiento de normas mediante una auditoría a la infraestructura física de la red de datos en una de las instituciones educativas.

- **Objetivos específicos:**

Planificar la auditoría que permita identificar las condiciones actuales de la red de datos de la institución educativa.

- Aplicar los procesos de auditoría teniendo en cuenta el modelo estándar de auditoría COBIT como herramienta de apoyo en el proceso inspección de la red de datos de la institución educativa.

- Identificar las soluciones para la construcción de los planes de mejoramiento a la red de la institución educativa de acuerdo con los resultados obtenidos en la etapa de aplicación del modelo de auditoría.

Alcance y delimitación: La presente auditoria pretende identificar las condiciones actuales del hardware, la red de datos y eléctrica de la institución educativa, con el fin de verificar el cumplimiento de normas y la prestación del servicio de internet para optimizar el uso de los recursos existentes para mejorar el servicio a los usuarios.

Los puntos para evaluar serán los siguientes:
De las instalaciones físicas se evaluará:

- Instalaciones eléctricas
- Instalación cableado de la red de datos
- Sistemas de protección eléctricos
- Seguridad de acceso físico a las instalaciones

De equipos o hardware se evaluará:

- Inventarios de hardware de redes y equipos
- Mantenimiento preventivo y correctivo de equipos y rede
- Hojas de vida de los equipos de cómputo y redes
- Los programas de mantenimiento de los equipos de cómputo y redes
- Revisión de informes de mantenimiento
- Personal encargado de mantenimiento
- Obsolescencia de la tecnología

Metodología: Para el cumplimiento de los objetivos planteados en la auditoría, se realizarán las siguientes actividades:

1. Investigación preliminar: visitas a la institución para determinar el estado actual de la organización, entrevistas con administradores y usuarios de las redes para determinar posibles fallas, entrevistas con administrador y usuarios para determinar la opinión frente al hardware existente y obsolecencia de equipos.

2. Recolectar información: Diseño de formatos de entrevistas, diseño de formatos para listas de chequeo, diseño de formatos para cuestionarios, diseño del plan de pruebas, selección del estándar a aplicar, elaboración del programa de auditoría, distribución de actividades para los integrantes del grupo de trabajo.

3. Aplicación de instrumentos: Aplicar entrevistas al administrador y usuarios, aplicar listas de chequeo para verificar controles, aplicar cuestionarios para descubrir nuevos riesgos y conformar los que han sido detectados anteriormente.

4. Ejecución de las pruebas: ejecutar las pruebas para determinar la obsolecencia del hardware, ejecutar pruebas sobre la red, ejecutar pruebas para comprobar la correspondencia de los inventarios con la realidad.

5. Realizar el proceso de análisis y evaluación de riesgos: elaborar el cuadro de vulnerabilidades y amenazas a que se ven enfrentados, determinar los riesgos a que se ven expuestos, hacer la evaluación de riesgos, elaborar el mapa o matriz de riesgos.

6. Tratamiento de riesgos: determinar el tratamiento de los riesgos de acuerdo a la matriz de riesgos, proponer controles de acuerdo a la norma de buenas prácticas aplicadas, definir las posibles soluciones.

7. Dictamen de la auditoría: Determinar el grado de madurez de la empresa en el manejo de cada uno de los procesos evaluados, medir el grado de madurez de acuerdo con los hallazgos detectados en cada proceso.

8. Informe final de auditoría: elaboración del borrador del informe técnico de auditoría para confrontarlo con los auditados, elaboración del informe técnico final, elaboración del informe ejecutivo, organización de papeles de trabajo para su entrega.

Recursos:

- **Humanos:** La auditoría se llevará a cabo por el grupo de auditores especializados en redes de datos con la asesoría metodológica de un Ingeniero Auditor.
- **Físicos:** Instalaciones de la institución educativa, aulas de informática y dispositivos de red.
- **Tecnológicos:** equipos de cómputo, software instalado para la red, cámara digital, Intranet institución.

Cronograma de actividades del plan de auditoria

Actividad		Mes 1				Mes 2				Mes 3			
		1	2	3	4	1	2	3	4	1	2	3	4
Planificar la auditoría	Estudio Preliminar	■	■										
	Determinación de Áreas Críticas de Auditoria		■										
Aplicar el modelo de auditoria	Elaboración de Programa de Auditoria			■	■	■							
	Evaluación de Riesgos					■	■						
	Ejecución de Pruebas y Obtención de Evidencias							■	■	■			
Construir los planes de mejoramiento	Elaboración de Informe										■	■	
	Sustentación de Informe												■

OBJETIVO(S):

Crear el cronograma de actividades de su plan de auditoría e implementar los formatos de definición de fuentes de conocimiento.

REQUISITOS:

- Contar con Manual de Prácticas de laboratorio impreso
- Presentar el material necesario para realizar la práctica

MATERIAL Y EQUIPO PARA UTILIZAR:

- Equipo de cómputo

DESARROLLO:

Para la planeación del proceso de auditoría es necesario el diseño de los formatos para el proceso de recolección de información y la presentación de los resultados de la auditoría, estos documentos denominados papeles de trabajo finalmente son organizados por cada proceso evaluado y al final se presenta el dictamen y el informe final de resultados.

A continuación, se presentará algunos de los formatos que se usan en el proceso de auditoría, para que los apliques a tu empresa auditada:

CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO	REF	

ENTIDAD AUDITADA		PAGINA		
		1	DE	1
PROCESO AUDITADO				
RESPONSABLE				
MATERIAL DE SOPORTE	COBIT			
DOMINIO				
PROCESO				

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANALISIS	DE EJECUCION

AUDITOR RESPONSABLE:

En este formato se observa los siguientes campos que deben ser diligenciados por el auditor para cada uno de los procesos evaluados.

REF: Se refiere al ID del elemento.

ENTIDAD AUDITADA: En este espacio se indicará el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

PROCESO AUDITADO: En este espacio se indicará el nombre del proceso objeto de la auditoria, para el caso será Contratación TI.

RESPONSABLE: En este espacio se indicarán los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: En este espacio se indicará el nombre del material que soporta el proceso, para el caso será COBIT.

DOMINIO: Espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

PROCESO: Espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

FUENTES DE CONOCIMIENTO: Espacio donde se indicará la fuente de donde proviene la información (documento, plano, manual, entrevista con la persona, otra fuente).

REPOSITORIO DE PRUEBAS APLICABLES: Pruebas que serán aplicadas en cada uno de los procesos de acuerdo con los objetivos de control que pretendan evaluarse.

PRUEBAS DE ANÁLISIS: Las pruebas de análisis hacen referencia a las pruebas que pueden aplicarse en el proceso mediante comparación (benchmarking) o por revisión y análisis documental.

PRUEBAS DE EJECUCIÓN: Las pruebas de ejecución hacen referencia a las pruebas que se pueden hacer en caliente sobre los sistemas o software que se pretende auditar. Estas pruebas generalmente se hacen sobre los sistemas en producción en las auditorías de seguridad (redes, base de datos, seguridad lógica, sistemas operativos), auditorías a la funcionalidad del software y las entradas y salidas del sistema.

 **CONCLUSIONES:**

Para poder conocer la información de fuentes de conocimiento se requiere de los campos anteriormente estudiados para ser diligenciados por el auditor para cada uno de los procesos.

 **CUESTIONARIO:**

¿Qué es una entidad auditada?

¿Qué es el proceso auditado?

¿Por qué es importante la firma del auditor?

PRACTICA No. 5

Realización de lista de chequeo

DURACIÓN:
6 horas

INTRODUCCIÓN:
Las listas de chequeo tienen como objetivo fundamental la verificación de la existencia de controles en cada uno de los procesos evaluados, para la construcción de las preguntas de la lista de chequeo es necesario conocer los objetivos de control en cada proceso, en esos objetivos de control están descritos los controles en cada proceso de acuerdo al estándar aplicado en la auditoría.

Las listas de chequeo en general se usarán también para verificar el cumplimiento de una norma estándar que se debe evaluar en la auditoría, por ejemplo, el cumplimiento de normas RETIE de instalaciones eléctricas o el cumplimiento de normas de cableado estructurado TIA/EIA, o cualquier otro estándar.

Para el caso del estándar CobIT 4.1, la estructura de la norma se divide en 4 dominios, 32 procesos y 334 objetivos de control, donde cada dominio se divide en procesos y en cada proceso existen varios objetivos de control. En cada objetivo de control están descritos los controles generales que debería existir, por lo tanto, las preguntas de la lista de chequeo deben ser solamente de existencia de esos controles en el proceso evaluado.

OBJETIVO(S):
Crear un modelo de formato para las listas de chequeo para los procesos del estándar CobIT.

REQUISITOS:

- Contar con Manual de Prácticas de laboratorio impreso
- Presentar el material necesario para realizar la práctica

MATERIAL Y EQUIPO PARA UTILIZAR:

- Equipo de cómputo

DESARROLLO:

La lista de chequeo, se usan para la verificación de la existencia de controles en el proceso o procesos auditados, en la lista de chequeo se puede usar escalas diferentes por ejemplo respuestas cerradas de SI/NO, o respuestas de cumplimiento por ejemplo CUMPLE TOTALMENTE (CT)/CUMPLE PARCIALMENTE (CP)/NO CUMPLE (NC), O como en este ejemplo donde se marca las preguntas donde existe control y se deja en blanco los controles que no se cumplen.

Las preguntas de las listas de chequeo se deben hacer teniendo en cuenta los objetivos de control, que serán los controles que deben existir en el proceso y se elabora preguntas sobre la existencia de dicho control, el auditor encargado de evaluar el proceso será quien aplique la lista de verificación de controles o lista de chequeo y de acuerdo con la respuesta se determina los hallazgos sobre la no existencia de controles en el proceso.

Diseño de las listas de chequeo

Para el diseño de las listas de chequeo hay que tener en cuenta el están aplicado y la estructura de este. Por ejemplo, en el siguiente caso se muestra las listas de chequeo para el estándar CobIT cuya estructura se divide en Dominios, procesos

y objetivos de control, donde en cada objetivo de control se definen los controles que debería existir para cumplir la norma.

Hay que tener en cuenta que las preguntas de la lista de chequeo son elaboradas teniendo en cuenta los controles que deberían existir de acuerdo a la norma, por cada control debe haber una o dos preguntas asociadas que indiquen si los controles existen o no en la empresa evaluada.

A continuación, se presentará algunos de los formatos que se usan para las listas de chequeo, para que los apliques a tu empresa auditada, hay que recordar que se aplica una por dominio de la metodología Cobit:

LISTA CHEQUEO			
DOMINIO	Planear y Organizar (PO)	**PROCESO**	PO9 Evaluar y administrar los riesgos de TI
OBJETIVO DE CONTROL	PO9.1 Marco de trabajo de administración de riesgos:		

Nº	**ASPECTO EVALUADO**	**CONFORME**		**OBSERVACIÓN**
		SI	**NO**	
1	¿Existe un marco de referencia para la evaluación sistemática de los riesgos a los que está expuesta la infraestructura tecnológica de la institución?		x	
OBJETIVO DE CONTROL	PO9.2 Establecimiento del Contexto del Riesgo:			
2	¿Se realiza la evaluación de los riesgos que pueden afectar la infraestructura tecnológica mediante la utilización de una metodología?		x	
OBJETIVO DE CONTROL	PO9.3 Identificación de eventos:			
3	¿Se realiza actualización de los diferentes tipos de riesgos que pueden afectar la infraestructura tecnológica?		x	
OBJETIVO DE CONTROL	PO9.4 Evaluación de los riesgos de TI:			
4	¿Se utilizan métodos cualitativos o cuantitativos para medir la probabilidad e impacto de los riesgos que pueden afectar la infraestructura tecnológica?	x		
OBJETIVO DE CONTROL	PO9.5 Respuesta a los riesgos:			
5	¿Existe un plan de acción para mitigar los riesgos de la infraestructura tecnológica de forma segura?		x	
OBJETIVO DE CONTROL	PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos:			
6	¿Se monitorea el plan de acción en contra de los riesgos de la infraestructura tecnológica?		x	

En el siguiente ejemplo se muestra las listas de chequeo aplicada para la verificación de normas para áreas de cómputo, que pueden servir como referencia para centros educativos o salas de cómputo:

Lista de chequeo Aulas de informática Institución Educativa		**R/PT**		
Cuestionario de Control		**LC1**		
Dominio	Adquisición e Implementación			
Proceso	AI3: Adquirir y mantener la arquitectura tecnológica			
Objetivo de Control	Evaluación de Nuevo Hardware			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se cuenta con un inventario de todos los equipos que integran el centro de cómputo?				
¿Con cuanta frecuencia se revisa el inventario?				
¿Se posee de bitácoras de fallas detectadas en los equipos?				
Características de la bitácora (señale las opciones).				
• ¿La bitácora es llenada por personal especializado? • ¿Señala fecha de detección de la falla? • ¿Señala fecha de corrección de la falla y revisión de que el equipo funcione correctamente? • ¿Se poseen registros individuales de los equipos? • ¿La bitácora hace referencia a hojas de servicio, en donde se detalla la falla, y las causas que la originaron, así como las refacciones utilizadas?				
¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?				
¿Se cuenta con servicio de mantenimiento para todos los equipos?				
¿Con cuanta frecuencia se realiza mantenimiento a los equipos?				
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?				
¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos a adquirir y así elegir el mejor?				
Documentos probatorios presentados:				

Lista de chequeo Aulas de informática Institución Educativa		**R/PT**		
Cuestionario de Control		**LC2**		
Dominio	Adquisición e Implementación			
Proceso	AI3: Adquirir y mantener la arquitectura tecnológica			
Objetivo de Control	Mantenimiento Preventivo para Hardware			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?				
¿Se cuenta con servicio de mantenimiento para todos los equipos?				
¿Con cuanta frecuencia se realiza mantenimiento a los equipos?				
¿Se cuenta con procedimientos definidos para la adquisición de nuevos equipos?				
¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos a adquirir y así elegir el mejor?				
Documentos probatorios presentados:				

Cuestionario de Control		**LC6**		
Dominio	Entrega de Servicios y Soportes			
Proceso	Protección contra Factores Ambientales			
Objetivo de Control	Seguridad Física			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Se tienen lugares de acceso restringido?				
¿Se poseen mecanismos de seguridad para el acceso a estos lugares?				
¿A este mecanismo de seguridad se le han detectado debilidades?				
¿Tiene medidas implementadas ante la falla del sistema de seguridad?				
¿Con cuanta frecuencia se actualizan las claves o credenciales de acceso?				
¿Se tiene un registro de las personas que ingresan a las instalaciones?				
Documentos probatorios presentados:				

Lista de chequeo		**LC3**		
Dominio	Entrega de Servicios y Soportes			
Proceso	DS12: Administración de Instalaciones.			
Objetivo de Control	Escolta de Visitantes			
Cuestionario				
Pregunta		**SI**	**NO**	**N/A**
¿Las instalaciones (aulas, cubículos y oficinas) fueron diseñadas o adaptadas específicamente para funcionar como un centro de cómputo?				
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?				
¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?				
¿Existen lugares de acceso restringido?				
¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?				
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?				
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?				
¿Se tienen medios adecuados para extinción de fuego en el centro de cómputo?				
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?				
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?				
¿Se tiene un lugar asignado para papelería y utensilios de trabajo?				
¿Son funcionales los muebles instalados dentro del centro de cómputo: cintoteca, Discoteca, archiveros, mesas de trabajo, etc?				
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?				
¿Se cuenta con suficientes carteles en lugares visibles que recuerdan estas prohibiciones?				
¿Con cuanta frecuencia se limpian las instalaciones?				
¿Con cuanta frecuencia se limpian los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)?				
Documentos probatorios presentados:				

CONCLUSIONES:

Verificar de controles o lista de chequeo y de acuerdo con la respuesta se determina los hallazgos sobre la no existencia de controles en el proceso.

CUESTIONARIO:

¿Qué importancia tiene la lista de chequeo?

¿Con base a que se realizan las listas de chequeo?

¿Qué se puede obtener con la información de las listas de chequeo?

PRACTICA No. 6

Análisis y evaluación de riesgos

DURACIÓN:
6 horas

INTRODUCCIÓN:

El proceso de gestión de riesgos involucra tres subprocesos fundamentales: El primero que consiste en el análisis de los riesgos donde se identifica y detalla las causas que originan los riesgos, quienes se ven involucrados y como se presentan. El segundo en la evaluación de riesgos en cuanto a probabilidad e impacto, donde se definen las escalas de medición de los riesgos para medir la probabilidad de ocurrencia de riesgos en un periodo de tiempo y el impacto que esos riesgos pueden ocasionar deteriorando parcial o completamente los activos impactados o los servicios que se prestan a través de los sistemas que los soportan. Y la tercera que es la gestión de los riesgos donde una vez que se identifican las causas del riesgo, se propone los controles para mitigar esos riesgos.

En este ejemplo se indicará como llevar a cabo el proceso de análisis y evaluación de riesgos indicando las posibles opciones para el tratamiento de los riesgos de acuerdo con un ejemplo genérico que ustedes deben aplicar a cada uno de los procesos evaluados.

Inicialmente se tienen como insumos para este proceso, el cuadro de los riesgos consolidado y los riesgos que han sido identificados con la aplicación de los instrumentos de recolección de la información que se extraen del cuestionario.

RIESGOS INICIALES:

De los riesgos iniciales, cada estudiante de acuerdo al proceso que está evaluando, debe mirar que riesgos son los que están relacionados directamente con el proceso evaluado y deben listarse como riesgos.

1. Incumplimiento en el cronograma de copias de seguridad de equipos de cómputo de usuarios y servidores
2. Funcionamiento inadecuado de las aplicaciones de software institucionales
3. Indisponibilidad del servidor o equipos de computo
4. Funcionamiento inadecuado del almacenamiento
5. Fallas en las telecomunicaciones y/o fluido eléctrico

RIESGOS CON LA APLICACIÓN DE INSTRUMENTOS

Posteriormente, al aplicar los instrumentos como entrevistas se descubrieron nuevos riesgos, al aplicar la lista de chequeo se descubre que faltan algunos controles en el proceso evaluado de acuerdo a la norma, y en el cuestionario están prácticamente, todos los riesgos detectados en el proceso evaluado y se hace una lista de ellos.

6. Desactualización Software
7. Perdida de información por virus informáticos
8. Incumplimiento en el reporte re la información
9. Uso indebido de la información
10. Inadecuada utilización del portal Web institucional
11. Desconocimiento de los avances del Plan Estratégico
12. Accesos no autorizados a las instalaciones del área tecnológica

OBJETIVO(S):

Crear un análisis de los riesgos donde se identifica y detalla las causas que originan los riesgos, quienes se ven involucrados y como se presentan.

REQUISITOS:

- Contar con Manual de Prácticas de laboratorio impreso
- Presentar el material necesario para realizar la práctica

MATERIAL Y EQUIPO PARA UTILIZAR:

- Equipo de cómputo

DESARROLLO:

De acuerdo con las normas aplicadas se construye las escalas de medición del impacto y la probabilidad de ocurrencia de los riesgos, hay que tener en cuenta que puede haber una valoración cuantitativa y cualitativa y que deben describirse los valores correspondientes tal y como aparece en las siguientes matrices:

MATRIZ PARA MEDICIÓN DE PROBABILIDAD E IMPACTO DE RIESGOS

IMPACTO		
NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

PROBABILIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir sólo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Se ha presentado al menos 1 vez en los últimos 5 años
3	Posible	El evento puede ocurrir en algún momento	Se ha presentado al menos de 1 vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Se ha presentado al menos 1 vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Se ha presentado más de 1 vez al año

Con las escalas de medición se construye la matriz de riesgos general que se aplica para cualquiera de los procesos, teniendo en cuenta los riesgos encontrados.

EVALUACIÓN Y MEDIDAS DE RESPUESTA					
PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

IMPACTO
Insignificante = 1
Menor = 2
Moderado = 3
Mayor = 4
Catastrófico = 5

PROBABILIDAD
Raro = 1
Improbable = 2
Posible = 3
Probable = 4
Casi Seguro = 5

Posteriormente con la información anterior, puede quedar así tu información:

RESULTADO MATRIZ DE RIESGOS

EVALUACIÓN Y MEDIDAS DE RESPUESTA					
PROBABILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)					
Improbable (2)		R7	R4, R10		
Posible (3)			R6, R11	R2, R9	R1, R5, R8
Probable (4)				R3	
Casi Seguro (5)					

CONCLUSIONES:

Una vez se tiene la matriz de riesgos aplicada a cada uno de los procesos se indica las acciones que pueden realizarse para el tratamiento de los riesgos de acuerdo con la siguiente tabla donde se indica por cada color, el tratamiento que se puede aplicar en cada caso.

B	Zona de riesgo Baja: Asumir el riesgo
M	Zona de riesgo Moderada: Asumir el riesgo, reducir el riesgo
A	Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir
E	Zona de riesgo Extremo: Reducir el riesgo, evitar, compartir o transferir

CUESTIONARIO:

¿Para que se utiliza una matriz de probabilidad e impactos de riesgos?

¿Cuál es la finalidad de las escalas de medición se construye la matriz de riesgos?

REFERENCIAS

Básico

ISO. (2018). ISO 19011:2018. Organización Internacional de Estándares. Suiza.

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De La Torre, J., & Jesús, J. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura. Revista Ibérica de Sistemas e Tecnologias de Informatica, (E32), 427-440

Ortega, C. (2014). Auditoría en informática asistida por tecnología con dictamen y sugerencias. Facultad de Contaduría, Campus IV-Tapachula: Universidad Autónoma de Chiapas. México.

Piattini, V. (2001). AUDITORIA INFORMÁTICA: UN ENFOQUE PRÁCTICO. Alfaomega. México.

Solís, G. (2002). Reingeniería de la auditoría informática. Trillas. México.

Complementario:

Bernal, R. (1996). Auditoría de los sistemas de información. Universidad Politécnica de Valencia, Servicio de Publicaciones. España.

Gómez, Á. (2012). Auditoría de seguridad informática / Álvaro Gómez Vieites. Editorial Starbook. España.

Gómez, A. (2013). Auditoría de seguridad informática / Álvaro Gómez Vieites. Ediciones de la U. Colombia.

Merino, C. (2014). Auditoría de sistemas de gestión de seguridad de la información (SGSI). Fundación Confemetal. España.

ANEXOS SI SON NECESARIOS