**AUDITORIA EN TECNOLOGÍAS DE INFORMACIÓN.**

TEMARIO:

**Unidad I Introduccion a la auditoria.**

* 1. Características de un auditor.
  2. Definición de auditoria y tipos de auditoria.
  3. Fases de la auditoria, preparación, planeación remisión de auditoria y elaboración del reporte.

**Unidad II Auditoria de la dirección informática.**

* 1. Examen de organigrama.
  2. Revisión de la documentación relacionada con la dirección.
  3. Entrevistas a directivos.
  4. Evaluación.

**Unidad III Auditoria de la seguridad física.**

* 1. Concepto de la seguridad física.
  2. Áreas a revisar.
  3. Evaluación de riesgos.
  4. Fuentes a utilizar.

**Unidad IV Auditoria de servicios de subcontratación.**

* 1. Subcontratación de servicios.
  2. Contratos: características y alcance.
  3. Acuerdo de nivel de servicio.
  4. Programa de auditoria al área de servicios.

**Unidad V Auditoria de base de datos.**

* 1. Concepto de auditoria de la base de datos.
  2. Diseño y carga.
  3. Explotación y mantenimiento.
  4. Explotación e implantación.
  5. Sistema gestor de base de datos.

**Unidad VI Auditoria de sistemas.**

* 1. Concepto de auditoria de sistemas.
  2. Desarrollo de sistemas.
  3. Instalación y puesta en servicio.
  4. Mantenimiento y soporte.
  5. Resolución de incidencias.
  6. Seguridad y control.

**Unidad VII Auditoria de la seguridad lógica.**

* 1. Concepto de seguridad lógica.
  2. Consecuencias y riesgos.
  3. Rutas de acceso.
  4. Claves de acceso.
  5. Software de control de acceso.
  6. Tipos de seguridad lógica.

**Unidad VIII Auditoria de las telecomunicaciones.**

* 1. Seguridad en telecomunicaciones.
  2. Vulnerabilidades amenazas y riesgos.
  3. Objetivos y criterios a evaluar.
  4. Técnicas y herramientas.

Criterios de evaluación:

1. Examen 40%
2. Exposición proyecto 30%
3. Resumen unidad 30%

Objetivo:

Identificar y aplicar una metodología de auditoria de tecnologias de la información.

Fechas:

|  |  |  |
| --- | --- | --- |
| parcial | Examen | Proyecto |
| 1 | 26 agosto | 24 agosto |
| 2 | 9 septiembre | 7 septiembre |
| 3 | 23 septiembre | 21 septiembre |
| 4 | 7 octubre | 5 octubre |
| 5 | 21 octubre | 19 octubre |
| 6 | 4 noviembre | 2 noviembre |
| 7 | 18 noviembre | 11 noviembre |
| 8 | 2 noviembre | 30 noviembre |

Primer trabajo en computadora. (Impresa) nombre de la unidad.

UNIDAD I

* 1. Características de un auditor.
  2. Definición de auditoria y tipos de auditoria.
  3. Fases de la auditoria, preparación, planeación remisión de auditoria y elaboración del reporte.

**Definición**

La auditoría es un examen minucioso para una persona capacitada a un área de reglamentos, leyes y de la empresa (especialidad).

**Características de un auditor.**

Tener certificado, conocimientos, personalidad (honesto, amable, incorruptible, responsable, presentación)

Conocimientos en área académica, complementaria y empírica.

**Tipos de auditoria**

Existen la financiera, operacional, sistemas, fiscal, administrativas, calidad.

**Fases de la auditoria.**

Planeación y programación. ¿Qué (objetivos, alcances), quién?

Ejecución de la auditoria. ¿Cómo?

Informe y plan de acción. ¿Cuándo (fechas)?

**Unidad II Auditoria de la dirección informática.**

* 1. Examen de organigrama.

Auditor con el director de la empresa

Dirección 🡪 Organigrama (representación gráfica de la estructura de la empresa).

Desempeña un papel informativo donde se encuentran los altos rangos de autoridad, la jerarquía y la relación entre ellos. El organigrama cumple los siguientes requisitos:

1. Tiene que ser fácil y sencillo de entender.
2. Debe contener únicamente los elementos indispensables.

Tipos de organigrama.

1. Vertical.- donde la autoridad baja (las jerarquías van de la parte frontal a la parte inferior).
2. Horizontal.- donde la dirección va de izquierda a derecha. (la jerarquía abarca de izquierda a derecha).
3. Mixto.- donde la relación va de izquierda a derecha y de arriba hacia abajo.
4. Circular.- la dirección gira tanto a la derecha como a la izquierda.

Datos que debe contener un organigrama.

1. Claves presupuestales, descripción del puesto, área de adscripción.

Datos que no debe contener un organigrama.

1. Nombres
2. Datos personales
3. sueldo.
   1. Revisión de la documentación relacionada con la dirección.

Objetivo de una auditoria: identificar las necesidades y requisitos legales de la organización.

1. Procesos. Ciclo del producto, metodología, soporte, recursos y controles.
2. Entender procesos. Objetivos, producto, aspectos ambientales y los riesgos
3. Gestión procesos. Planes, controles, documentos, registros, reglamentos.

Estructura

Manuales. Política, sistema, clientes

Procedimientos. Responsables del sistema

Instructivos. Personal operativo

Registros. Personal operativo, bitácoras, kardex

* 1. Entrevistas a directivos.

Descripción del registro.: aula, profesor, grupo, alumno, condición lab.

Bitácora

Nombre del puesto:

Nombre del jefe inmediato:

Puesto del jefe inmediato:

Nombre de la persona entrevistada

Fecha

Descripción del puesto

Manuales

Políticas

Procedimientos.

Cuestionario.

¿Número de equipos?

¿Cuántas maquinas funcionan?

* 1. Evaluación.

EVALUACION.

ISO

La Organización Internacional para la Estandarización (ISO) es una federación de alcance mundial integrada por cuerpos de estandarización nacionales de 153 países, uno por cada país.   
La ISO es una organización no gubernamental establecida en 1947. La misión de la ISO es promover el desarrollo de la estandarización y las actividades con ella relacionada en el mundo con la mira en facilitar el intercambio de servicios y bienes, y para promover la cooperación en la esfera de lo intelectual, científico, tecnológico y económico.   
Todos los trabajos realizados por la ISO resultan en acuerdos internacionales los cuales son publicados como Estándares Internacionales.

UNIDAD III

ISO 27000 – 2 consiste en la seguridad física

Seguridad física.

Entorno 🡪 trabajador 🡪 organización.

Instalaciones

Escaleras – anti-derrapante

**Concepto de seguridad física** Garantiza la integridad de los activos humanos, lógicos y materiales. Ayudando prevenir riesgos.

Hay tres momentos:

**Antes**

Obtener un nivel adecuado de seguridad física sobre los activos.

**Durante**

Ejecutar un plan adecuado de contingencia

**Después**

Los contratos de seguros pueden compensar en mayor o menor medida las perdidas, gastos, o responsabilidades que se puedan detectar y corregir el fallo

Contingencia algún daños o riesgos que puede ocurrir.

Factores naturales y humano, naturales no se pueden prevenir y el humano si.

AREAS A REVISAR

Edificio.

Centro de proceso de datos

Personal

Auditorias (planes de auditoria, historia de auditorías y la auditoria actual.)

EVALUACION DE RIESGOS.

Riesgo, control y pruebas

Identificación, planteamiento de solución, aplicación.

Tipo de riesgo.

Seguridad se divide en: confidencialidad, integridad y disponibilidad.

Fuentes a utilizar.

Políticas, estándares, normas, procedimientos. Elementos para auditar. Planes de seguridad, contratos, pólizas de seguros, organigrama, manuales técnicos