# Universidad Ricardo Palma

## FACULTAD DE INGENIERÍA

### ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA INFORMATICA

# SÍLABO 2023-II

## 1. DATOS ADMINISTRATIVOS

| | | |
|---|---|---|
| **ASIGNATURA** | **:** | Auditoria de Sistemas |
| **COIGO** | **:** | IF 1004 |
| **NATURALEZA.** | **:** | Teoría – Practica – Laboratorios |
| **CONDICION** | **:** | Obligatorio |
| **REQUISITOS** | : | II 0904 Taller de Aseguramiento de Calidad |
| **SEMESTRE** | **:** | 10 |
| **CREDITOS** | **:** | 4 |
| **HORAS POR SEMANA** | **:** | **5** (Teoría =3 Laboratorios= 2) |
| **SEMESTRE** | **:** | 10 |
| **PROFESOR** | **:** | Yolanda Yopla Mercado |
| **PROFESOR E-MAIL** | **:** | Yolanda.yopla@urp.edu.pe |

## 2. SUMILLA DEL CURSO

El curso se divide en dos partes, donde en la primera se prepara al estudiante en dar los conocimientos de auditoria, técnicas, métodos entre otros para integrar equipos de auditoria y poder realizar labores de auditoria de sistemas principalmente, desde la planificación de auditoria hasta la formulación y presentación del informe de auditoria. En la segunda parte se prepara al estudiante en todos los fundamentos para que este en la capacidad de implementar sistemas de gestión de la seguridad de la información alineado a las normas ISO referente a seguridad de la información y buenas practicas.

## 3. COMPETENCIAS GENERICAS A LAS QUE CONTRIBUYE LA ASIGNATURA

- Solución de Problemas
- Aplicación de las Ciencias
- Comportamiento ético

## 4. COMPETENCIAS ESPECIFICAS A LAS QUE CONTRIBUYE LA ASIGNATURA

4.1. Planificación.- Para una labor de auditoria y/o seguridad se debe realizar un adecuado levantamiento de información de acuerdo a los objetivos trazados que permita realizar labores e planificación, tanto de auditoria como de seguridad de la información..

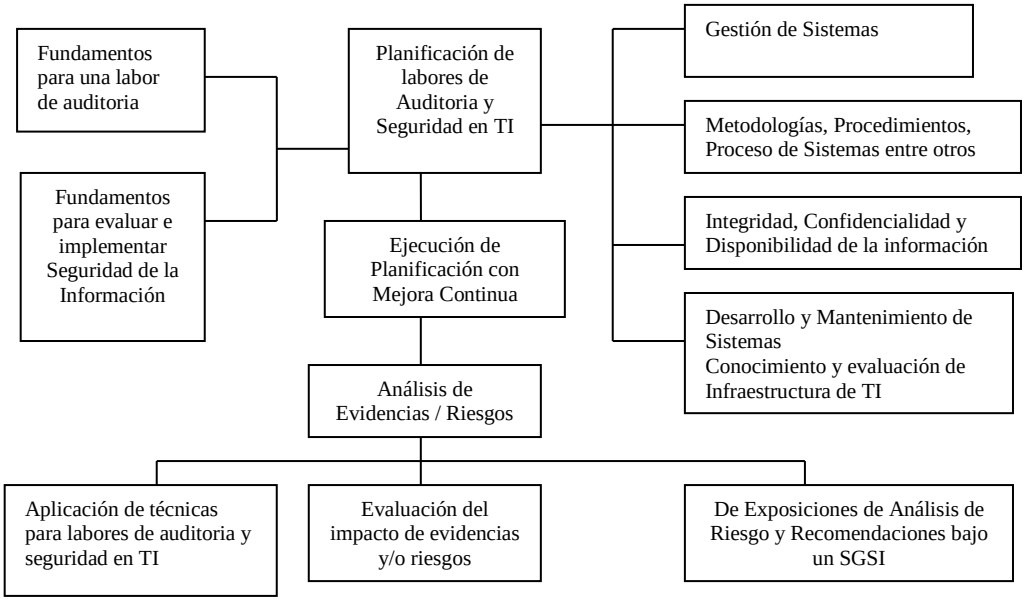
4.2. Análisis.- Permite aplicar todos los conocimientos que a la fecha el alumno tiene, para una adecuada labor de auditoria de sistemas o labores de seguridad de la información.

4.3. Aplica los criterios del Control Interno a todo proceso / actividad en su carrera profesional. Así como la aplicación de las buenas practicas de ITIL, Cobit.

4.4. Administra los principales riesgos a la integridad, confidencialidad y disponibilidad de la información de la empresa, sobre la base del análisis de riesgos.

4.5. Presenta alternativas basada en casos de cómo diseñar e implementa mecanismos de protección contra las principales técnicas de delitos informáticos

## 5. RED DE APRENDIZAJE:




## 6. PROGRAMACIÓN SEMANAL DE LOS CONTENIDOS

### UNIDAD TEMÁTICA N° 1: CONCEPTOS BASICOS Y DEFINICIONES PREVIAS

**Logro de la Unidad:** Reformar los conocimientos de los alumnos en los conocimientos necesarios que se debe tener para el desarrollo de una labor de auditoria y seguridad en tecnologías de información.
**Nº de horas: 05**

| SEMANA | CONTENIDOS | ACTIVIDADES DE APRENDIZAJE |
|---|---|---|
| 1 | Introducción al curso<br>Conceptos básicos para el desarrollo del curso<br>Derecho informático | Introducción al curso /Objetivo del curso / Marco conceptual / Metodología para la labor de auditoria de sistemas / Tipos y niveles según sistemas de información / Metodología de desarrollo de sistemas de información / La organización y el área de informática / Certificaciones y especializaciones en el Área de TI / Derecho Informático / Pirámide del Kelsen / Entidades emisoras de normas sobre Tecnología de Información |

### UNIDAD TEMÁTICA N° 2: DEFINICIONES DE AUDITORIA GUBERNAMENTAL y AUDITORIA DE SISTEMAS. HERRAMIENTAS PARA LABORES DE AUDITORIA

**Logro de la Unidad:** Dar los conceptos de auditoria y porque se realiza labores de auditoria, así como el perfil y rol del auditor de sistemas, así como el conocimiento de herramientas automatizadas para labores de auditoria de sistemas.
**Nº de horas: 05**

| SEMANA | CONTENIDOS | ACTIVIDADES DE APRENDIZAJE |
|---|---|---|
| 2 | Auditoria Gubernamental<br>Definición de Auditoria de Sistemas<br>Técnicas de Auditoria Asistido por Computadora – TAAC y Técnicas en General | Porque se realiza una labor de auditoria gubernamental / Conocer la estructura del Sistema Nacional de Control del Perú / Tipos de Auditoria Gubernamental / Definición Características / Riesgos / Tipos y clasificación / Justificación / Objetivos /Perfil / Rol / TAAC |

### UNIDAD TEMÁTICA N° 3: FUNDAMENTOS PARA UNA PLANIFICACION DE AUDITORIA DE SISTEMAS

**Logro de la Unidad:** Que los alumnos conozcan una metodología para una labor integral de auditoria, asimismo, que conozcan sobre certificaciones para labores de auditoria de sistemas, así como conocimiento de buenas practicas a través de la aplicación de COBIT.
**Nº de horas: 10**

| SEMANA | CONTENIDOS | ACTIVIDADES DE APRENDIZAJE |
|---|---|---|
| 3 | Isaca y Cobit<br>Sistema de Control Interno | Organizaciones de Auditoria de Sistemas /Que es ISACA ? / Certificaciones de ISACA /Que es Cobit? / Metodología COBIT /Gobierno IT / Sistema de Control Interno |
| 4 | Cuestionario de Control Interno<br>Metodología para una labor de auditoria de sistemas<br>Formulación de un plan de auditoria<br>Casos propuesto y resueltos | Definición de Cuestionario / Características / Supuestos en un cuestionarios / preguntas claves en la formulación de un cuestionario / Tipos de preguntas de aplicación en cuestionarios /Ejemplos / Metodología para labor de auditoria |

**UNIDAD TEMÁTICA N° 4: PLANIFICACION Y EJECUCION DE UNA LABOR DE AUDITORIA DE SISTEMAS**
**Logro de la Unidad:** Dar los conceptos básicos para que puedan realizar labores de planificación de labores de auditoria enfocada al desarrollo de un objetivo definido, que les permita encontrar evidencias y/o riesgos para realizar de ser el caso la formulación de observaciones, conclusiones y/o recomendaciones.
**Nº de horas: 10**

| SEMANA | CONTENIDOS | ACTIVIDADES DE APRENDIZAJE |
|---|---|---|
| 5 | Formulación de un programa de auditoria<br>Formulación de hallazgos de auditoria<br>Formulación de observaciones, conclusiones y recomendaciones<br>Casos propuesto y resueltos | Estructura de un programa de auditoria / normas a aplicar según el caso / formulación de programas de auditoria / atributos del hallazgos / ejemplos y casos resueltos y propuestos |
| 6 | Práctica Calificada | |

**UNIDAD TEMÁTICA N° 5: INFORMES DE AUDITORIA**
**Logro de la Unidad**: Que los alumnos sepan formular informes de auditoria, así como saber documentar toda la evidencia que respalde el informe de auditoria a través de los papeles de trabajo.
**Nº de horas: 05**

| SEMANA | CONTENIDOS | ACTIVIDADES DE APRENDIZAJE |
|---|---|---|
| 7 | Formulación de un informe de auditoria<br>Papeles de trabajo de una labor de auditoria<br>Casos propuesto y resueltos<br>Exposición de Trabajo de Auditoría | Estructura de informes de auditoria, informes técnicos que sustenta y respalda los informes de auditoria / ejemplos de informes/ desarrollo de informes a través de las observaciones |
| 8 | **SEMANA DE EXÁMENES PARCIALES** | |

**UNIDAD TEMÁTICA N° 6: LA SEGURIDAD DE LA INFORMACION Y EVALUACIÓN DE RIESGOS EN TI**
**Logro de la Unidad:** Dar los conocer la importancia de la seguridad de la información que se viene dando hoy en día en las organizaciones y las acciones que vienen tomando, sobre un análisis de riesgo.
**Nº de horas: 10**

| SEMANA | CONTENIDOS | ACTIVIDADES DE APRENDIZAJE |
|---|---|---|
| 9 | La seguridad de la información, principios básicos<br>Gestión de Riesgos y Matriz de Riesgos | La importancia de la seguridad de la información / principios de confidencialidad, integridad y disponibilidad, enfoque de análisis de riegos y gestión de riesgos / alternativas de solución / video |

| | | |
|---|---|---|
| 10 | Certificaciones CISO y Fundamentos para implementar un modelo de Sistema de Gestión de la Seguridad de la Información – SGSI<br>Basado en la normas ISO de la serie 27001 | La importancia del oficial de seguridad de la información -CSO/ certificaciones para CSO / Definiciones de Procedimientos / Proceso / Acciones para implementar un modelo de SGSI |

**UNIDAD TEMÁTICA N° 7: IMPLEMENTACION DE UN MODELO DE SGSI – PARTE I**

**Logro de la Unidad:** Desarrollo de actividades y/o acciones que permita al negocio implementar como buenas prácticas: Política de Seguridad, Organización de la Seguridad de la Información, Gestión de Activos, Seguridad de los Recursos Humanos, Seguridad Física y Ambiental, Gestión de las Comunicaciones, Operaciones y Control de Accesos en aras de incrementar la seguridad y disminuir los riesgos de la información del negocio.

**Nº de horas: 15**

| SEMANA | CONTENIDOS | ACTIVIDADES DE APRENDIZAJE |
|---|---|---|
| 11 | Dominio 01: Política de Seguridad<br>Dominio 02: Organización de Seguridad/Organización de la Seguridad de la Información<br>Dominio 03: Administración de Activos/Gestión de Activos<br><br>Casos propuesto y resueltos | Política de seguridad de la información / Documento de política de seguridad de la información /. Organización de la Seguridad de la Información / Responsabilidad de los Activos / Clasificación de la Información |
| 12 | Dominio 04: Seguridad de los Recursos Humanos<br>Dominio 05: Seguridad Física y Ambiental<br>Dominio 06: Gestión de las Comunicaciones y Operaciones<br><br>Casos propuesto y resueltos | Seguridad en la definición del trabajo y los recursos / Seguridad en el desempeño de las funciones del empleo / Finalización o cambio del puesto de trabajo / Áreas seguras / Seguridad de los equipos. |
| 13 | Dominio 07: Sistema de Control de Accesos/Control de Accesos. Dominio 08: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información<br>Dominio 09: Administración/Gestión de Incidentes de Seguridad<br><br>Casos propuesto y resueltos | Procedimientos y responsabilidades de operación / Supervisión de los servicios contratados a terceros. / Protección contra software malicioso y código móvil. / Ejemplos y trabajos en grupo |

**UNIDAD TEMÁTICA N° 8: IMPLEMENTACION DE UN MODELO DE SGSI – PARTE II**

**Logro de la Unidad:** Desarrollo de actividades y/o acciones que permita al negocio implementar como buenas prácticas: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, Gestión de Incidentes de Seguridad de la Información, Plan de Continuidad del Negocio y Cumplimiento en aras de incrementar la seguridad y disminuir los riesgos de la información del negocio..

**Nº de horas: 10**

| SEMANA | CONTENIDOS | ACTIVIDADES DE APRENDIZAJE |
|---|---|---|
| 14 | Práctica Calificada | |
| 15 | Dominio 10: Plan de Continuidad del Negocio/Gestión de la Continuidad Comercial<br>Dominio 11: Cumplimiento<br><br>Exposición de trabajo Final de Seguridad | Aspectos de la gestión de continuidad del negocio / Conformidad con los requisitos legales |
| 16 | **SEMANA DE EXÁMENES FINALES** | |
| 17 | **SEMANA DE EXÁMENES SUSTITUTORIOS** | |

## 7. LABORATORIOS Y EXPERIENCIAS PRÁCTICAS

Laboratorio 1: Formulación de la Planificación de Auditoria en base a un objetivo determinado

Laboratorio 2: Formulación de Hallazgos de Auditoria
Trabajo 1 : Presentación de un Informe de Auditoria
Laboratorio 3: Funciones del Área de Seguridad de la Información, Análisis de Riesgos
Laboratorio 4: Desarrollo de Acciones, Procedimientos y/o Procesos para implementar dominios del SGSI
Trabajo 2 : Presentación del Plan de Gestión de Seguridad de la Información

## 8. TÉCNICAS DIDÁCTICAS

El curso se desarrolla en sesiones de teoría, práctica y laboratorio de cómputo. En las sesiones de teoría, el docente presenta los conceptos, fundamentos y aplicaciones. En las sesiones prácticas, se resuelven diversos ejercicios, casos y problemas donde se analiza su solución y son resueltos.

En las sesiones de laboratorio se desarrolla casos de aplicación real para una labor de auditoria desde la planificación hasta la presentación del informe de auditoria, asimismo la presentación en forma progresiva de una implementación de un modelo de sistema de gestión de la seguridad de la información basado en las normas ISO de seguridad de la información. Los laboratorios son evaluados y los alumnos debe presentar y exponer un trabajo o proyecto integrador. En todas las sesiones se promueve la participación activa del alumno. Aprendizaje basado en proyectos y Aprendizaje colaborativo.

## 9. EVALUACIÓN

### 9.1. Criterios:

- La asistencia a clases es del 70 % como mínimo.
- Conocimientos
- Desarrollar los casos y laboratorios dejados en forma grupal
- Orden y claridad de ideas en las exposiciones, debates y diálogos.
- Presentación de trabajos en forma ordenada y concordante

### 9.2. Fórmula:

El Promedio Final PF se calcula tal como se muestra a continuación:

**PF = [EA + EB + ((LB1 + LB2 + TF1 + LB3 + LB4 + TF2)/6) + (PC1 + PC2)/2] / 4**

EA: Examen Parcial EB: Examen Final
PC: Prácticas Calificadas LB: Laboratorios Calificados
TF: Trabajo Final

## 10. RECURSOS

- Equipos: computadora, laptop, Tablet, celular
- Materiales: apuntes de clase del Docente, separatas de problemas, lecturas, videos.
- Plataformas: Kahoot

## 11. REFERENCIAS BIBLIOGRAFICAS

a. AUDITORÍA INFORMÁTICA
Un Enfoque Práctico, 2ª Ed. Ampliada y Revisada
PIATTINI, Mario y Del PESO, Emilio (coordinadores)
Editorial Alfaomega-Rama, 2005

b. TÉCNICAS DE LA AUDITORÍA INFORMÁTICA
DERRIEN, Yann
Editorial Alfaomega-Rama, 2005

c. Auditoria Informática.
José Antonio Echenique.
Ed. Mc-Graw Hill.

**Referencias en la Web**

http://www.isaca.org
http://www.theiia.org
http://www.sans.org
http://www.acl.com
http://www.auditnet.org
http://www.astalavista.net