



# Universidad Mariano Gálvez de Guatemala

Facultad de Ingeniería en Sistemas de Información y Ciencias de la Computación

## SEGURIDAD Y AUDITORIA DE SISTEMAS – 050

Ciclo 10 Semestre 2

Catedrático:

Horario:

Créditos: 5

### I. Justificación:

Brindar a los estudiantes de Ingeniería en Sistemas de Información y Ciencias de la Computación los fundamentos técnicos y prácticos de telecomunicaciones, los cuales son fundamentales para el desenvolvimiento en sus respectivas carreras.

### II. Objetivos del curso y resultados:

#### *Objetivo General*

Ser capaz de ejecutar la auditoría de sistemas y administrar de manera eficiente el riesgo tecnológico en aquellas instituciones públicas o privadas que utilizan el procesamiento electrónico de datos para la obtención de información económica, contable y de toma de decisiones

#### *Objetivos Específicos*

Que el estudiante:

- Se refuercen los conocimientos sobre los sistemas de información, automatizados en cuanto a planeación, análisis, diseño e implantación y producción.
- Proporcionar recomendaciones prácticas y posibles, a los riesgos identificados dentro de las áreas de la institución.
- Aplicar los procedimientos básicos y primordiales para el aseguramiento de los sistemas de información.
- Elegir técnicas, herramientas, métodos de análisis, a utilizar para el aseguramiento de los sistemas de información.

#### *Resultados esperados del curso*

Al final de este curso, los estudiantes podrán:

1. Proporcionar al estudiante los conocimientos esenciales que le sirven para administrar de forma eficiente el riesgo tecnológico, en aquellas empresas que utilizan el procesamiento electrónico de datos para procesar la información económica, contable y de toma de decisiones.
2. Evaluar el control interno relativo a la organización de sistemas informáticos y aplicaciones sistematizadas de una empresa. Con base en su examen se deberán proporcionar recomendaciones orientadas a fortalecer las debilidades reveladas.

3. Proporcionar al estudiante los conocimientos esenciales que le sirven para ejecutar la auditoría de informática, en aquellas empresas que utilizan el procesamiento electrónico de datos para procesar la información económica, contable y de toma de decisiones.
4. Realizar diagnósticos, desarrollar proyectos de implementación de políticas, normativas y mejores prácticas que estén correctamente alineadas a las estrategias de negocio y a la situación real de las empresas.

### **III. Prerequisito**

175 Créditos

### **IV. Formato y Procedimientos:**

Este curso está estructurado de la siguiente forma: principalmente se darán clases magistrales con el apoyo de presentaciones en PP que ayudarán a fijar por medio de la memoria visual los conceptos vistos en clase. Se reforzará lo aprendido en clase con laboratorios en grupo sobre el tema principal de la clase, y por último se les pedirá que elaboren un trabajo final que formará parte de la nota final.

Lo que se espera de los estudiantes en cuanto a comportamiento y estudio es respeto hacia su catedrático como hacia sus compañeros, se les solicitará apagar o poner en modo vibrador su aparato celular con el fin de no interrumpir la clase. En cuanto al estudio se les solicitará su mayor compromiso y dedicación para con el curso, pues el mismo será parte imprescindible en su vida laboral y profesional. Su asistencia y participación serán tomadas en cuenta siempre para su evaluación durante el curso, por lo que deben completar el porcentaje mínimo de asistencia.

**V. Requerimientos del Curso:** Todas las tareas y asignaciones que incluya el curso se darán a conocer con el suficiente tiempo de antelación para su debida elaboración y entrega. Las tareas y proyectos serán entregados en la fecha y por el medio establecidos.

**1. Política de asistencia y participación en clase:**

Se requiere el 80% de asistencia a clases y participación constante dentro de las clases para enriquecer la discusión de temas y experiencias.

### **VI. Ponderación del Curso: Notas o punteos para las diferentes actividades del curso:**

- Evaluación Parcial 1: 10 puntos
- Evaluación Parcial 2: 20 puntos
- Laboratorios, tares y trabajos de investigación: 20 puntos
- Evaluación Final: 50 puntos

### **VII. Integridad Académica**

Se espera que cada estudiante en éste curso, cumpla y esté al tanto de la Ley de Derecho de Autor y Derechos Conexos de Guatemala (Dto. 33-98 del Congreso de la República de Guatemala), demuestre honestidad y ética. Cualquier trabajo presentado por un estudiante en éste curso para obtener créditos académicos será de la autoría del estudiante. En caso de ser trabajos en grupo, debe ser propio de los estudiantes integrantes del grupo. En los casos en que se deban hacer

referencias a artículos o citas de otros autores, deberán ser reconocidos e indicados correctamente en los trabajos, siguiendo los estándares de la APA (American Psychological Association).

En caso de producirse una copia, tanto el estudiante que copia el trabajo de otro estudiante y el estudiante que dio el material que se va a copiar, recibirán automáticamente un cero en la nota del trabajo correspondiente.

Durante las evaluaciones, cada estudiante debe hacer su propio trabajo. Hablar o discutir, no está permitido la durante las evaluaciones, ni tampoco puede comparar documentos, copiar de los demás, o colaborar de una u otra manera. Cualquier comportamiento de este tipo durante las evaluaciones resultará en la anulación de la prueba, y puede conducir a un fallo del curso y las medidas disciplinarias por parte de la universidad.

### VIII. Programación tentativa del curso

| Semana | Fechas | Indicadores de logro   | Temas/Contenidos  | Actividades               | Bibliografía | Recursos a utilizar  |
|--------|--------|--|---|---------------------------|--------------|--|
| 1      |        | El estudiante será capaz de comprender y explicar los fundamentos de la seguridad informática  | <ul style="list-style-type: none"> <li>• <b>Conceptos básicos de Seguridad Informática</b></li> <li>• <b>Finalidades de la Seguridad Informática</b></li> <li>• <b>Fundamentos de la Seguridad Informática</b></li> <li>• <b>Objetivos generales y específicos de la Seguridad Informática</b></li> <li>• <b>Metodologías para el desarrollo e implementación de la Seguridad Informática</b></li> <li>• <b>Etapas de madurez de la Seguridad Informática y laboratorios</b></li> </ul> | Clase magistral dinámica. | 1            | Presentación en PowerPoint®  |
| 2      |        | El estudiante será capaz de diferenciar y aplicar los diferentes procesos de la seguridad informática en los distintos campos de acción, así como entender la relación con otras ciencias de la administración | <ul style="list-style-type: none"> <li>• <b>Procesos de Seguridad Informática</b></li> <li>• <b>Campos de acción de la Seguridad Informática</b></li> <li>• <b>Relación de la Seguridad Informática con otras ciencias de la Administración.</b></li> <li>• <b>Riesgo Operativo y Riesgo Financiero. Riesgo Tecnológico</b></li> <li>• <b>Laboratorios</b></li> </ul>   | Clase magistral dinámica  | 1            | Presentación en PowerPoint   |
| 3      |        | El estudiante será capaz de comprender y conocer las leyes y reglamentos concernientes a la seguridad informática en Guatemala, así como las estrategias de implementación de un gobierno de TI                | <ul style="list-style-type: none"> <li>• <b>Principales estrategias del Cyber-crimen. Análisis retrospectivo, actualizado y a futuro.</b></li> <li>• <b>Leyes y reglamentos de la República de Guatemala, relacionados con Seguridad Informática</b></li> <li>• <b>Gobierno de TI. Estrategias de implementación</b></li> <li>• <b>Laboratorios</b></li> </ul>  | Clase magistral           | 1            | Presentación en PowerPoint<br>Quiz de preguntas<br>Laboratorio No. 3 en clase elaboración de un Gantt con actividades ficticias dadas por el profesor. |

|   |  |  |   |                 |                   |   |
|---|--|--|---|-----------------|-------------------|---|
| 4 |  | El estudiante deberá ser capaz de aplicar las mejores prácticas para la seguridad informática, tener el conocimiento básico del uso de algunas de las herramientas para la administración de la seguridad informática. | <ul style="list-style-type: none"> <li>• <b>Definición de Cyber-crimen</b></li> <li>• <b>Metodologías, políticas y normativas generalmente aceptadas. ISO, ITIL, COBIT, PCI.</b></li> <li>• <b>Organizaciones internacionales que combaten el Cyber-crimen. IOCE. CERT.</b></li> <li>• <b>Mejores prácticas para Seguridad Informática</b></li> <li>• <b>Hacking ético</b></li> <li>• <b>Herramientas administrativas para proyectos de Seguridad Informática</b></li> <li>• <b>Laboratorios</b></li> </ul> | Clase Magistral | 1                 | Presentación en PowerPoint                  |
| 5 |  | El estudiante debe ser capaz de manejar los diferentes controles de seguridad en distinto ambientes  | <ul style="list-style-type: none"> <li>• <b>Ámbitos de control físico y lógico. Controles de Seguridad Informática</b></li> <li>• <b>Controles de seguridad física</b></li> <li>• <b>Controles de seguridad lógica</b></li> <li>• <b>Aseguramiento del Data Center (Centro de Datos)</b></li> </ul>   |                 | 1, notas de clase | Laboratorio Preguntas                       |
| 6 |  | PRIMERA EVALUACIÓN PARCIAL   | 18 hrs. Salón de clase  | NINGUNA         | NINGUNA           | Examen escrito resuelto de forma individual |
| 7 |  | El estudiante deberá comprender y explicar los conceptos que se refieren al aseguramiento de la calidad, virtualización de servidores y proceso de seguridad   | <ul style="list-style-type: none"> <li>• <b>Aseguramiento de la calidad los servicios que brinda TI. Productos de hardware y software. Control de Cambios. Control de Accesos</b></li> <li>• <b>Virtualización de servidores. Globalización de servicios. Ambientes homogéneos. Procesos de Hardening y Patching. Continuidad</b></li> </ul>  | Clase Magistral | 1                 | Presentación en PowerPoint                  |
| 8 |  | El estudiante será capaz de explicar y comprender las diferentes estrategias tecnológicas que requieren seguridad informática  | <ul style="list-style-type: none"> <li>• <b>Estrategias tecnológicas. e-commerce, e-banking. Firma digital. IT Mobile. Otros</b></li> <li>• <b>Laboratorios</b></li> <li>• <b>Toma de decisiones críticas en proyectos de Seguridad Informática</b></li> </ul>  | Clase Magistral | 1                 | Presentación en PowerPoint                  |
| 9 |  | El estudiante podrá comprender y explicar los diferentes aspectos administrativos relacionados con la seguridad de sistemas, así como los conceptos básicos del BCP y DRP  | <ul style="list-style-type: none"> <li>• <b>Manejo de presupuestos en proyectos de Seguridad Informática</b></li> <li>• <b>Dificultades de la Seguridad Informática. Análisis retrospectivo, actualizado y a futuro.</b></li> <li>• <b>Reseña sobre Business Continuity Planning, Disaster Recovery Planning y su relación con la Seguridad Informática</b></li> </ul>  | Clase magistral | 1,2               | Presentación en PowerPoint                  |

|    |                    |   |  |                                    |                       |   |
|----|--------------------|---|--|------------------------------------|-----------------------|---|
| 10 |                    | El estudiante deberá obtener conocimiento básico de las diferentes especializaciones en cuanto a seguridad informática y sus aplicaciones | <ul style="list-style-type: none"> <li>• Retos y proyecciones de TI, del Cyber-crimen y de la Seguridad Informática.</li> <li>• Acompañamiento del marco normativo legal</li> <li>• Especializaciones en Seguridad Informática: CISM, CISA, CISSP, CCNA, ITIL</li> <li>• Laboratorios</li> </ul> |                                    | 1,2 y notas de clase  |   |
| 11 |                    | El estudiante deberá comprender y explicar los conceptos básicos de la auditoría de sistemas  | <ul style="list-style-type: none"> <li>• Conceptos básicos de la auditoría de sistemas</li> <li>• Riesgos, controles y evaluación</li> <li>• Organización y planeación de la auditoría informática</li> </ul>  |                                    | 1,2                   | Presentación en PowerPoint                |
| 12 | AB17 - AB21 (2017) | SEMANA SANTA  |  |                                    |                       |   |
| 13 |                    | SEGUNDA EVALUACIÓN PARCIAL  | 18 HRS Salón de clase  | Examen escrito de forma individual | NINGUNA               | Resolución de examen de forma individual. |
| 14 |                    | El estudiante deberá obtener los conocimientos necesarios para poder implementar una auditoría de sistemas                                | <ul style="list-style-type: none"> <li>• Metodología para el desarrollo e implantación de la auditoría informática</li> <li>• Etapas de la auditoría informática</li> </ul>  | Clase magistral                    | 1,2                   | Presentación en PowerPoint                |
| 15 |                    | El estudiante deberá conocer los diferentes tipos de auditorías de sistemas que pueden presentarse en la vida profesional                 | <ul style="list-style-type: none"> <li>• Auditorías sobre cada área de la empresa</li> <li>• Auditorías sobre bases de datos</li> <li>• Auditorías sobre Sistemas Aplicativos</li> </ul>   | Clase magistral                    | 1,2                   | Presentación en PowerPoint                |
| 16 |                    | El estudiante deberá conocer los diferentes tipos de auditorías de sistemas que pueden presentarse en la vida profesional                 | <ul style="list-style-type: none"> <li>• Auditorías de seguridad de las redes</li> <li>• Auditorías de los departamentos de informática</li> </ul>   |                                    | 1,2, y notas de clase |   |
| 17 |                    | El estudiante deberá comprender las diferentes técnicas y herramientas para la ejecución de una auditoría de sistemas                     | <ul style="list-style-type: none"> <li>• Técnicas, herramientas y controles de la auditoría informática</li> <li>• Auditorías integrales y por procesos</li> <li>• Auditoría informática e Internet</li> </ul>   | Clase magistral                    | 1,2                   | Presentación en PowerPoint                |

|    |  |  |  |                           |         |  |
|----|--|--|--|---------------------------|---------|--|
| 18 |  | El estudiante conocerá y será capaz de entender la estructura y tipos de informes de auditoria | <ul style="list-style-type: none"> <li>• <b>Tipos de Informe (Final y Parcial)</b></li> <li>• <b>Informe sobre las diferentes áreas evaluadas</b></li> <li>• <b>Contenido Mínimo del informe</b></li> <li>• <b>Estructura del Informe</b></li> <li>• <b>Tipos de Informe (técnico Administrativo)</b></li> </ul> | Clase magistral           | 1,2     | Presentación en PowerPoint                                       |
| 19 |  | El estudiante conocerá y será capaz de entender la estructura y tipos de informes de auditoria | <ul style="list-style-type: none"> <li>• <b>Cedulas de trabajo</b></li> <li>• <b>Tipos de Formulario para entrevistas</b></li> <li>• <b>Definición de formulario por área</b></li> <li>• <b>Interpretación del Formulario</b></li> <li>• <b>El formulario como ayuda en el informe</b></li> </ul>                | Clase magistral           | 1,2     | Presentación en PowerPoint                                       |
| 20 |  | EXAMEN FINAL   | <b>18 HRS Salón de clase</b>   | Examen escrito individual | Ninguna | El examen será resuelto de forma individual por cada estudiante. |

## IX. Bibliografía del Curso

1. Hernández, E. H. (2000). Auditoria en informática: un enfoque metodológico y práctico (2da. Ed.). México: CECSA.