I. IDENTIFICACIÓN

1.	Asignatura	: Electiva 6 - Auditoría y Tecnología de la Información
2.	Semestre	: Décimo
3.	Horas semanales	: 7 horas
	3.1. Clases teóricas	: 4 horas
	3.2. Clases prácticas	: 3 horas
4.	Total real de horas disponibles	: 112 horas
	4.1. Clases teóricas	: 64 horas
	4.2. Clases prácticas	: 48 horas

II. JUSTIFICACIÓN

La penetración de la tecnología en las empresas y la dependencia que esta crea, hace que el control sobre estos activos cobre mayor relevancia y requiera una adecuada capacitación para cubrir con suficiencia las múltiples especialidades que la tecnología de la información y las comunicaciones despliega en la infraestructura de las empresas.
El profesional informático debe conocer el rol del auditor a fin de entender el objetivo de las políticas de tecnología definidas en las empresas y aportar un valor agregado a sus labores aplicando técnicas de autoevaluación de riesgos, con lo que se constituye en un elemento proactivo en el control interno de la empresa.
El auditor interno informático, además de conocer características específicas a verificar en las revisiones de Sistemas Operativos, Sistemas de Aplicación, Redes, infraestructuras físicas, etc., debe conocer los nuevos enfoques adoptados por los marcos de trabajo actuales a fin de optimizar los resultados y generar valor agregado a su labor.
En ese sentido, se pretende que el profesional cuente con una visión general de los frameworks más importantes en la asignatura, a fin de adecuar sus actividades al marco que más se adecue a la empresa en la que desempeñe sus actividades de control interno.

III. OBJETIVOS GENERALES

1. Analizar el propósito del departamento de auditoría interna informática.
2. Adquirir el concepto de independencia y evitar su mala utilización.
3. Estimular al auditor a agregar valor con su trabajo, más allá de las auditorías formales, vía consultas e involucramientos tempranos.
4. Identificar e interpretar los conceptos de la evaluación de sistemas informáticos.
5. Enunciar y describir las técnicas y herramientas que se utilizan en la evaluación de rendimiento de un sistema informático.
6. Interpretar y aplicar los pasos para el estudio estructurado del rendimiento de un sistema informático.
7. Elaborar guías prácticas sobre cómo realizar la función de auditoría informática de modo que sea considerada un elemento esencial y respetado en el ambiente de tecnología de la compañía.
8. Apreciar los consejos prácticos y detallados de, no solo que hacer, sino también por qué y cómo hacerlo.
9. Identificar los frameworks como el COBIT, ITIL, ISO27001, así como regulaciones locales en la asignatura e internacionales como Sarbanes – Oxley, HIPAA y PCI.

IV. OBJETIVOS ESPECÍFICOS

A. Conocimientos

1. Describir los escenarios tecnológicos actuales donde se ejecutan las aplicaciones informáticas, las herramientas y los recursos utilizados.
2. Clasificar y diferenciar las diversas plataformas orientadas a la ejecución de aplicaciones actuales que forman parte de la sociedad del conocimiento.
3. Formular las llamadas a sistemas y órdenes específicas conducentes a la verificación de los parámetros del sistema en estudio que pueden ser sistemas hardware o sistemas software).
4. Interpretar las técnicas básicas de modelado y análisis de rendimiento para poder realizar las evaluaciones de los sistemas.

B. Habilidades

1. Interpretar la estructura de todos los niveles de los componentes de un sistema informático (hardware y software) donde se ejecutan las aplicaciones.
2. Emplear las herramientas más adecuadas para evaluar el rendimiento y las vulnerabilidades.
3. Determinar y emplear las fases y métricas apropiadas para cada caso.
4. Interpretar y aplicar las diferentes técnicas y métricas para cada situación de evaluación, infiriendo otras no observadas.
5. Aplicar frameworks adecuados al objetivo de la revisión a realizar.

C. Competencias

1. Capacidad de aplicar los conocimientos en la práctica.
2. Disposición para el trabajo en equipo.
3. Capacidad de abstracción, análisis y síntesis y presentaciones orales.

4. Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.
5. Capacidad para identificar, plantear y resolver problemas
6. Capacidad de comunicación oral y escrita.

V. PRE - REQUISITO

1. Aprobar el 80% de los Créditos
2. Realizar las 300 horas de Pasantía

VI. CONTENIDO

6.1. Unidades programáticas

1. Auditoría Informática - Introducción
2. El proceso de auditoría
3. Auditoría de controles a nivel corporativo
4. Auditoría de Centros de Procesamiento de Datos y Recuperación de desastres.
5. Auditoría de Ruteadores, Switches y Firewalls.
6. Auditoría de Sistemas Operativos Windows.
7. Auditoría de Sistemas Operativos Unix y Linux.
8. Auditoría de Servidores Web y Aplicaciones Web.
9. Auditoría de Bases de Datos.
10. Auditoría de Almacenamiento de datos
11. Auditoría de Entornos virtuales
12. Auditoría de WLANs y dispositivos móviles.
13. Auditoría de Aplicaciones.
14. Auditoría de computación en la nube y operaciones tercerizadas.
15. Frameworks y estándares.
16. Administración del Riesgo

6.2. Desarrollo de las unidades programáticas

1. Auditoría Informática – Introducción

    1.1. Construcción de una Efectiva Función de Auditoría Interna de TICs.
    1.2. Independencia, el gran mito
    1.3. Consultoría e involucramiento temprano
    1.4. Cuatro métodos de consultoría e involucramiento temprano
    1.5. Involucramiento temprano
    1.6. Auditorías informales
    1.7. Compartir conocimientos
    1.8. Auto evaluación
    1.9. Construcción del relacionamiento: Sociedad vs Supervisión
    1.10. Aprender a construir asociaciones
    1.11. El rol del equipo de auditoría de TICs
    1.12. Auditor de aplicaciones
    1.13. Especialistas en extracción y análisis de datos
    1.14. Auditores de TICs
    1.15. Formación y mantenimiento de un equipo de auditoría efectivo.
    1.16. Auditores de TICs de carrera.
    1.17. Profesionales de TICs
    1.18. Auditores de TICs de carrera vs Profesionales de TICs: reflexiones finales
    1.19. Mantenimiento de la Experiencia
    1.20. Fuentes de aprendizaje
    1.21. Relacionamiento con Auditores externos.

2. El proceso de auditoría

    2.1. Controles Internos
    2.2. Tipos de controles internos
    2.3. Ejemplos de controles internos
    2.4. Determinación de qué auditar
    2.5. Creación del universo a auditar
    2.6. Ranking del universo a auditar
    2.7. Determinación de qué auditar: reflexiones finales.
    2.8. Las etapas de una auditoría
    2.9. Planificación
    2.10. Trabajo de campo y documentación
    2.11. Descubrimiento de debilidades y validación.
    2.12. Desarrollo de la solución
    2.13. Redacción del borrador de informe y remisión del informe.
    2.14. Seguimiento de observaciones.
    2.15. Estándares.

3. Auditoría de controles a nivel corporativo.

    3.1. Auditoría de controles a nivel de Entidad
    3.2. Antecedentes

3.3. Pasos para auditar Controles a nivel de Entidad
3.4. Base de conocimiento
3.5. Checklist principal.

4. Auditoría de Centros de Procesamiento de Datos y Recuperación de desastres.

4.1. Aspectos esenciales para la auditoría de Datacenters.
4.2. Controles de seguridad física y ambiental
4.3. Plan de recuperación de sistemas
4.4. Copias de respaldo y restauración
4.5. Plan de recuperación de desastres
4.6. Base de conocimiento
4.7. Checklist principal.
4.8. Auditoría de Datacenters

5. Auditoría de Ruteadores, Switches y Firewalls.

5.1. Aspectos esenciales para la auditoría de redes
5.2. Protocolos
5.3. Modelo OSI
5.4. Ruteadores y Switches
5.5. Firewalls
5.6. Auditoría de Switches, Ruteadores y Firewalls.
5.7. Pasos generales para auditar equipos de red.
5.8. Controles adicionales de Switches: Capa 2
5.9. Controles adicionales de Ruteadores: Capa 3
5.10. Controles adicionales de Firewalls
5.11. Herramientas y tecnología
5.12. Base de conocimiento
5.13. Checklist principal.
5.14. Pasos generales para auditar equipos de redes.
5.15. Auditoría de dispositivos de capa 2: Controles adicionales para Switches
5.16. Auditoría de dispositivos de capa 3: Controles adicionales para Ruteadores.
5.17. Auditoría de Firewalls: Controles adicionales.

6. Auditoría de Sistemas Operativos Windows.

6.1. Aspectos esenciales de auditoría de ambientes Windows
6.2. Ayudas para modo comando
6.3. Herramientas esenciales para modo comando
6.4. Comandos comunes
6.5. Herramientas para administración de Servidores
6.6. Realización de la auditoría
6.7. Pasos para auditar entornos Windows
6.8. Setup y controles generales
6.9. Repaso de servicios, aplicaciones instaladas y tareas programadas.
6.10. Administración de cuentas y control de passwords.
6.11. Revisión de derechos de usuarios y opciones de seguridad.
6.12. Seguridad de red y controles.
6.13. Escaneo de vulnerabilidad de redes y prevención de intrusión
6.14. Como realizar una auditoría simplificada de clientes Windows.
6.15. Herramientas y tecnología
6.16. Base de conocimiento
6.17. Checklist principal.
6.18. Auditoría de Servidores Windows
6.19. Auditoría de Clientes Windows.

7. Auditoría de Sistemas Operativos Unix y Linux.

7.1. Aspectos esenciales de auditoría de Unix y Linux
7.2. Conceptos clave
7.3. Diseño de la estructura de archivos y navegación
7.4. Permisos de la estructura de archivos.
7.5. Usuarios y autenticación
7.6. Servicios de red
7.7. Pasos para auditar Unix y Linux
7.8. Administración de cuentas y control de passwords.
7.9. Seguridad de archivos y controles
7.10. Seguridad de red y controles
7.11. Pistas de auditoría
7.12. Monitoreo de seguridad y controles generales.
7.13. Herramientas y tecnología
7.14. Nessus
7.15. NMAP
7.16. Chkrootkit
7.17. Crack and Hohn the Ripper
7.18. Tiger y TARA
7.19. Shell/Awk/etc
7.20. Base de conocimiento
7.21. Checklist principal.
7.22. Auditoría del administrador de cuentas y control de passwords

7.23. Auditoría de seguridad de red y controles
7.24. Auditoría de pistas de auditoría.
7.25. Auditoría de monitoreo de seguridad y controles generales.

8. Auditoría de Servidores Web y Aplicaciones Web.

8.1. Aspectos esenciales de auditoría Web
8.2. Una auditoría con múltiples componentes
8.3. Parte 1: Pasos de prueba para auditar Sistemas Operativos (host)
8.4. Parte 2: Pasos de prueba para auditar Servidores Web.
8.5. Parte 3: Pasos de prueba para auditar Aplicaciones Web.
8.6. Pasos adicionales para auditar aplicaciones web.
8.7. Herramientas y Tecnología
8.8. Base de conocimiento
8.9. Checklist principal.
8.10. Auditoría de Servidores Web
8.11. Auditoría de Aplicaciones Web

9. Auditoría de Bases de Datos.

9.1. Aspectos esenciales para auditar Bases de Datos
9.2. Marcas comunes de Bases de Datos
9.3. Componentes de las Bases de Datos
9.4. Pasos para auditar Bases de Datos
9.5. Configuración y controles generales
9.6. Seguridad del Sistema Operativo
9.7. Administración de cuentas y permisos de acceso.
9.8. Encripción de datos
9.9. Monitoreo y Administración
9.10. Herramientas y tecnología
9.11. Herramientas de auditoría
9.12. Herramientas de monitoreo
9.13. Base de conocimiento
9.14. Checklist principal.
9.15. Auditoría de Bases de Datos

10. Auditoría de Almacenamiento de datos

10.1. Aspectos esenciales a auditar en medios de almacenamiento
10.2. Componentes clave de medios de almacenamiento
10.3. Conceptos clave de medios de almacenamiento.
10.4. Pasos para auditar medios de almacenamiento.
10.5. Configuración y controles generales
10.6. Administración de cuentas
10.7. Administración de medios de almacenamiento
10.8. Controles de seguridad adicionales
10.9. Base de conocimiento
10.10. Checklist principal.

11. Auditoría de Entornos virtuales

11.1. Antecedentes
11.2. Proyectos comerciales y Libres
11.3. Aspectos esenciales de auditoría de entornos virtuales
11.4. Pasos para auditar entornos virtuales.
11.5. Configuración y controles generales
11.6. Altas y Bajas de cuentas y recursos. Buscar sinónimos de los términos.

12. Auditoría de WLANs y dispositivos móviles.

12.1. Antecedentes
12.2. Antecedentes de WLANs
12.3. Antecedentes de dispositivos móviles con servicios de datos habilitados
12.4. Aspectos esenciales de auditoría en WLAN y dispositivos móviles.
12.5. Pasos para auditar redes inalámbricas.
12.6. Parte 1: Auditoría técnica de WLANs
12.7. Parte 2: Auditoría operacional de WLANs.
12.8. Pasos para auditar dispositivos móviles
12.9. Parte 1: Auditoría técnica de dispositivos móviles.
12.10. Parte 2: Auditoría operacional de dispositivos móviles.
12.11. Consideraciones adicionales.
12.12. Herramientas y tecnología
12.13. Base de conocimiento
12.14. Checklist principal.
12.15. Auditoría de redes LANs
12.16. Auditoría de dispositivos móviles

13. Auditoría de Aplicaciones.

13.1. Antecedentes
13.2. Aspectos esenciales de auditoría de aplicaciones
13.3. Marcos de trabajo generalizado

13.4. Mejores prácticas
13.5. Pasos para auditar aplicaciones
13.6. Controles de entrada de datos
13.7. Controles de Interfaces de aplicaciones.
13.8. Tablas de auditoría
13.9. Controles de acceso
13.10. Controles de modificación de aplicaciones
13.11. Copias de respaldo y restauración.
13.12. Retención de datos y clasificación e involucramiento del usuario
13.13. Controles de Sistemas Operativos, Bases de Datos y otros activos de infraestructura.
13.14. Checklist principal.
13.15. Mejores prácticas para evaluar aplicaciones
13.16. Auditoría de aplicaciones

14. Auditoría de computación en la nube y operaciones tercerizadas.

14.1. Antecedentes
14.2. Tercerización de Sistemas e Infraestructura de TICs.
14.3. Tercerización de Servicios de TICs.
14.4. Otras consideraciones para tercerizar Servicios de TICs.
14.5. Reportes SAS70
14.6. Pasos para auditar computación en la nube y operaciones tercerizadas.
14.7. Pasos preliminares y visión de conjunto
14.8. Selección del Vendedor y Contratos
14.9. Seguridad de Datos
14.10. Operaciones
14.11. Consideraciones legales y cumplimiento normativo
14.12. Base de conocimiento
14.13. Checklist principal.
14.14. Auditoría de computación en la nube y operaciones tercerizadas.

15. Frameworks y estándares.

15.1. Introducción a los controles internos de TICs, Frameworks y estándares
15.2. COSO
15.3. Definición COSO del Control Interno
15.4. Conceptos clave del Control Interno
15.5. Framework integrado del Control Interno
15.6. Framework integrado de la administración de riesgo corporativo
15.7. COBIT
15.8. Conceptos de COBIT
15.9. Gobernanza de TICs
15.10. Modelo de madurez del gobierno de TICs.
15.11. La conexión COSO-COBIT
15.12. COBIT 5.0
15.13. ITIL
15.14. Conceptos ITIL
15.15. ISO 27001
15.16. Conceptos ISO 27001
15.17. Metodología de evaluación NSA INFOSEC
15.18. Conceptos sobre la evaluación NSA INFOSEC
15.19. Fase de pre evaluación
15.20. Fase de actividades on-site
15.21. Fase de post evaluación
15.22. Tendencias de frameworks y estándares.

16. Administración del Riesgo

16.1. Beneficios de la administración de riesgos
16.2. Administración de riesgos desde la perspectiva ejecutiva
16.3. Enfrentando los riesgos
16.4. Análisis de riesgos cualitativos vs cuantitativos
16.5. Análisis de riesgos cuantitativos
16.6. Elementos del riesgo
16.7. Aplicación práctica
16.8. Análisis cuantitativo del riesgo en la práctica
16.9. Causas comunes de imprecisiones.
16.10. Análisis de riesgos cualitativos
16.11. Ciclo de vida de la administración de riesgos de TICs.
16.12. Fase 1: Identificar activos de información
16.13. Fase 2: Cuantificar y calificar amenazas.
16.14. Fase 3: Evaluar las vulnerabilidades.
16.15. Fase 4: Remediar los gaps de control.
16.16. Fase 5: Administrar los riesgos residuales.
16.17. Sumario de fórmulas.

VII. ESTRATEGIAS METODOLÓGICAS

1. La asignatura está concebida sobre las prácticas de laboratorio que los estudiantes irán desarrollando durante las clases, apoyados sobre la base teórica.
2. Las clases teóricas se desarrollan en clases magistrales y trabajos grupales, dirigidos por el docente. Además los estudiantes participarán activamente de las clases al realizar lecturas previas de un tema determinado, indicadas a través del sitio virtual de la Facultad.
3. Los estudiantes realizarán los trabajos de laboratorios en grupos o individuales y serán supervisados por los docentes.
4. Presentación y defensa de memorias de prácticas de laboratorio y de artículos científicos relacionados con el área en cuestión.
5. En la plataforma virtual de la Facultad se realizarán: foros de discusión, tareas individuales y grupales, video con tutoriales, talleres, entregas de memorias, etc.
6. Posterior al primer examen parcial se tendrán 10 horas de prácticas de laboratorio en las que se aplicarán herramientas de monitoreo, análisis de tráfico de red, análisis de vulnerabilidades; en las que se pondrán en práctica los conceptos desarrollados en las diferentes plataformas tecnológicas abarcadas por el presente programa de estudios.
7. Las mismas se realizarán en los laboratorios de la Facultad y se utilizarán, principalmente, herramientas libres o en modalidad de evaluación.

VIII. MEDIOS AUXILIARES

1. Pizarras acrílicas.
2. Marcadores.
3. Borrador de pizarra acrílica.
4. Computadoras.
5. Proyectores multimedia.
6. Parlantes para multimedia.
7. Plataforma virtual "EDUCA".
8. Sala de laboratorio equipada para las prácticas.
   - 8.1. Computadoras en red.
   - 8.2. Sistemas operativos Linux, Windows.
   - 8.3. Acceso a internet.

IX. EVALUACIÓN

Para evaluar la asignatura se tienen en cuenta lo siguiente:

1. Examen final de teoría con un % asignado.
2. Evaluación continúa de teoría, obtenida con la media de los controles realizados durante el curso.
3. Nota de laboratorio donde se ponga de manifiesto la experiencia adquirida en las sesiones de laboratorio, que consta de la media ponderada de las notas de todas las prácticas, con un peso dependiendo de las prácticas, según se indique en clases, donde se evalúa lo siguiente:
   a. Presentación
   b. Comprensión de las herramientas utilizadas.
   c. Logro del objetivo propuesto en las prácticas.

1. Las calificaciones se basan en el reglamento de la Universidad.
2. Es imprescindible la entrega de todas las prácticas para poder calcular la nota de prácticas.

X. BIBLIOGRAFÍA

A. Básica

- Davis, Chris. IT Auditing – Using Controls to protect information assets. – Chris Davis, Mike Schiller, Kevin Wheeler.

B. Complementaria

- Piattini, M. del Peso, E. y otros; Auditoría Informática: Un enfoque práctico. 2ª Edición. Editorial Ra-ma 2000.
- Nava, F. Apuntes de Auditoría Informática. Servicio de Publicaciones de la URJC
- Derrien, Yann. Técnicas de la auditoría informática / YannDerrien -- México: Alfaomega, Marcombo,
- 1995. -- 229 p. ISBN: 970-15- 0030-X
- Echenique García, José Antonio. Auditoría en informática / José Antonio Echenique García -- México: McGraw-Hill, 2000. -- 200 p.ISBN: 968-422- 288-2
- Echenique García, José Antonio. Auditoría en informática / José Antonio Echenique García -- 2a. ed. -- México: McGraw-Hill, 2003. -- 300 p. ISBN: 970-10- 3356-6
- Frielink, A. B.. Auditing automatic data processing: a survey of papers on the subject / A. B. Frielink -- Amsterdam: Elsevier Scientific Publishing Company, 1960. -- 70 p.