Ministerio de Cultura y Educación **(Programa del año 2023)**
Universidad Nacional de San Luis
Facultad de Ciencias Físico Matemáticas y Naturales
Departamento: Informatica
Area: Area IV: Pr. y Met. de Des. del Soft.

I - Oferta Académica

Materia	Carrera	Plan	Año	Período
AUDITORIA INFORMATICA	ING. INFORM.	026/12-08/15	2023	2° cuatrimestre

II - Equipo Docente

Docente	Función	Cargo	Dedicación
GARIS, ANA GABRIELA	Prof. Responsable	P.Adj Exc	40 Hs

III - Características del Curso

Credito Horario Semanal				
Teórico/Práctico	**Teóricas**	**Prácticas de Aula**	**Práct. de lab/ camp/ Resid/ PIP, etc.**	**Total**
Hs	2 Hs	2 Hs	2 Hs	6 Hs

Tipificación	Periodo
B - Teoria con prácticas de aula y laboratorio	2º Cuatrimestre

Duración			
Desde	**Hasta**	**Cantidad de Semanas**	**Cantidad de Horas**
07/08/2023	17/11/2023	15	75

IV - Fundamentación

Un ingeniero informático debe tener la capacidad de llevar a cabo el relevamiento en sistemas y procesos de control de una organización para su evaluación e informe, con el objetivo de, entre otras cosas, verificar el cumplimiento de las normativas y leyes, revisar la eficaz gestión de los recursos informáticos o prevenir el fraude informático.
La Auditoría Informática se ha consolidado como una subdisciplina fuertemente regulada y estandarizada. Esta materia pone el énfasis en transmitir conceptos y herramientas, que permitan al profesional Ingeniero en Informática, contribuir y desarrollar la "auditoría" en las empresas e instituciones de la región y del país.

V - Objetivos / Resultados de Aprendizaje

Los principales objetivos es formar profesionales de excelencia, capaces de:
- Contribuir al desarrollo de la función “auditoría” en las empresas e instituciones de la región y del país.
- Ejercitar el control de la función informática.
- Verificar el cumplimiento de las Normativas de la Autoridad de Aplicación en este ámbito.
- Ejecutar la revisión de la eficaz gestión de los recursos informáticos.
- Prevenir el fraude informático.

VI - Contenidos

Contenidos mínimos:

Concepto de Auditoría y de. Auditoría Informática. Control Interno: El "Informe COSO". Control Interno y Auditoría en el ámbito de la Tecnología Informática. Auditoria y "Gestión del Riesgo": Riesgo del "Negocio"; Riesgo de la Seguridad; Riesgo de la "Continuidad de las Operaciones". Monitoreo del riesgo. Estándares de Auditoría Informática: ISACA; IFAC. El Estándar Cobit. Aspectos legales de la Auditoría Informática. Estudios de casos: "IBM - Banco Nación"; "ENRON"; "Woldcom"; otros.

Los contenidos mínimos serán desarrollados en 5 unidades temáticas.

Unidad I
Conceptos de la Auditoría Informática: Evaluación de los Controles. Ajuste a los Procedimientos Establecidos. Aspectos Legales de la Auditoría Informática. Control y Auditoría: Responsabilidades. La Auditoría como verificación de la eficacia de los mecanismos de Control Interno. Planificación de la Auditoría. Análisis comparativo del ejercicio de la Auditoría y el Control Interno en empresas.

Unidad II
Auditoría Interna y Externa. La Auditoría Informática: Ámbito de Incumbencia. La Auditoría de Estados Contables. Auditoría Informática como soporte a la Auditoría Contable - Financiera.

Unidad III
Estándares de la auditoría Informática. El “Informe COSO”. "Information System Audit and Control Association" (ISACA): COBIT. El "Institute of Internal Auditors". Auditoría de Fraudes. El estándar de la "Association of Certified Fraud Examiners" (ACFE). El "American Institute of Certified Public Accountants (AICPA). Estudios de casos: “IBM – Banco Nación”; “ENRON”; “Worldcom”; otros. Estudio comparativo de las normas estudiadas.

Unidad IV
Amenazas, vulnerabilidades y Riesgo. Gestión del Riesgo. Riesgo de la Seguridad. Valoración del riesgo. Monitoreo del riesgo. Seguridad de la Información. Norma ISO 27001.

Unidad V
Evidencias en Auditoría. Peritaje Informático. Estudio de archivos, “audit trails”, “transaction logs”. Normas generales de Auditoría y Marco Legal vigente.

VII - Plan de Trabajos Prácticos

Metodología aplicada en el proceso de enseñanza aprendizaje:
Los trabajos prácticos vinculadas a las unidades del programa consisten en actividades de investigación, reflexión, análisis para la creación de respuestas a situaciones que pueden presentarse relacionadas a la auditoría, al tiempo que se plantean casos de estudio para abordar problemáticas vinculadas con el área de estudio.
Antes de iniciar el práctico, los estudiantes deben estudiar los conceptos teóricos propuestos por el docente. Los estudiantes deben realizar una entrega por cada trabajo práctico. Cada actividad práctica es revisada/corregida por los docentes a fin de hacer una devolución a los estudiantes sobre las repuestas elaboradas. Para cada ejercicio solicitado se realiza una corrección informada del docente hacia cada estudiante. Las dificultades generales observadas en las correcciones son sociabilizadas entre los estudiantes, a través del docente, a fin de debatir y reflexionar sobre temas comunes. Adicionalmente, ante el requerimiento de al menos un estudiante, se brindan consultas con el objetivo de aclarar dudas surgidas a lo largo del curso.

Prácticos de Aula:
Práctico 1: Introducción a la Auditoría Informática. Planificación de la auditoría. Análisis comparativo del ejercicio de la Auditoría y el Control Interno en empresas.

Práctico 2: Auditoría Interna y Externa. Auditoría Informática como soporte a la Auditoría Contable - Financiera.

Práctico 3: Estándares de la auditoría Informática. Informe COSO. COBIT. ACFE. Prevención del fraude. Estudio

comparativo de las normas estudiadas.

Práctico 4: Amenazas, vulnerabilidades y Riesgo. Gestión del Riesgo. Seguridad de la Información. Norma ISO 27001.

Práctico 5: Evidencias en Auditoría. Peritaje Informático. Estudio de archivos. Evaluación de herramientas para “audit trails” y “transaction logs”.

Laboratorio / trabajo de campo:
- Efectuar el relevamiento en sistemas y procesos de control de una organización para su evaluación e informe.
- Estudio y análisis de casos: "ENRON", "IBM – Banco Nación", entre otros.
- Estudio de evidencias con finalidad de Auditoría, utilizando herramientas de Software automatizadas.

Para cada unidad se deja disponible el material correspondiente a los contenidos de la unidad, las diapositivas de clase, videos con grabaciones de las teorías, documentos de apoyo y su correspondiente trabajo práctico en el repositorio digital.

VIII - Regimen de Aprobación

Condiciones para regularizar la materia:
Aprobar los prácticos de laboratorio/trabajo de campo y de aula con toda su documentación, entregada en tiempo y forma, y un examen integrador final.

Prácticos de aula: Entregar y aprobar el/los práctico/s. Un práctico se evalúa como aprobado o desaprobado, únicamente. Los prácticos se podrán realizar en grupos de hasta dos integrantes.

Prácticos de laboratorio/trabajo de campo: Entregar y aprobar los prácticos. Un práctico se evalúa como aprobado o desaprobado, únicamente. Los prácticos se podrán realizar en grupos de hasta cuatro integrantes.

Exámenes: Aprobar un examen final integrador o sus respectivas recuperaciones, con nota mayor o igual que seis para su regularización.

Condiciones para promocionar la materia: Regularizar la materia con las siguientes condiciones adicionales:
- Aprobar el examen integrador o sus recuperatorios con nota mayor o igual que siete.
- Tener el 80 % de asistencia a las clases.

En caso de no promocionar el estudiante deberá rendir un examen final.

No se permite rendir examen final en calidad de libre dado que se desarrollan tareas de campo que requieren del trabajo a lo largo de la cursada.

La cátedra contempla dos recuperaciones por examen.

IX - Bibliografía Básica

[1] ISACA, "COBIT an ISACA Framework". Disponible en https://www.isaca.org/resources/cobit (última visita 1/8/2023)
[2] OWASP Foundation, "Guía de Pruebas OWASP v3", 2008. Disponible en https://owasp.org/www-pdf-archive/Gu%C3%ADa_de_pruebas_de_OWASP_ver_3.0.pdf (última visita 1/8/2023)
[3] Oficina Nacional de Tecnologías de Información, Disposición 3/ 2013. "Política de Seguridad de la Información Modelo", 2013. Disponible en https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-3-2013-219163 (última visita 1/8/2023)
[4] ISO 27000 series. Portal español. Disponible en https://www.iso27000.es/sgsi.html (última visita 1/8/2023)
[5] Association of Certified Fraud Examiners, "Occupational Fraud 2022: A Report to the nations", 2022. Disponible en https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf (última visita 1/8/2023)

X - Bibliografia Complementaria

[1] ISACA,Cybersecurity Management - Transforming Cybersecurity using COBIT 5, 2013.

[2] Hall, James, "Information Technology Auditing", South-Western Cengage Learning, 2010.
[3] Tamayo Alzate, Alonso, "Auditoría de Sistemas - Una Visión Práctica", Universidad Nacional de Colombia, 2001.
[4] De León, Cesar, “Formación básica para ser perito informático de la Corte Suprema Justicia de la Nación Argentina, 2019.

XI - Resumen de Objetivos

Formar profesionales de excelencia, capaces de contribuir al desarrollo de la función “auditoría” en las empresas e instituciones de la región y del país.

XII - Resumen del Programa

Concepto de Auditoría y de Auditoría Informática. Control Interno: El “Informe COSO”. Control Interno y Auditoría en el ámbito de la Tecnología Informática. Auditoría y “Gestión del Riesgo”. Valoración del riesgo. Monitoreo del riesgo. Seguridad de la Información. Estándares de Auditoría Informática. Prevensión del fraude. El Estándar Cobit. Aspectos legales de la Auditoría Informática. Estudios de casos: “IBM – Banco Nación”; “ENRON”; “Worldcom”; otros. Evidencias en Auditoría.

XIII - Imprevistos

XIV - Otros

Contacto: Ana Garis - Email: agaris@gmail.com Oficina 1: Piso 1 – Bloque 2 Teléfono: +54 (266) 4520300 - Interno 2101