PROGRAMA DE ASIGNATURA
GESTIÓN Y AUDITORIA DE SISTEMAS DE INFORMACIÓN

1.- DATOS DE LA ASIGNATURA

Asignatura	Gestión y Auditoría de Sistemas de Información				
Carrera	Contador Público y Auditor				
Código	362350				
Créditos SCT-Chile	6	**Trabajo Directo Semanal**	4 horas pedagógicas	**Trabajo Autónomo Semanal**	5.8 horas cronológicas
Nivel	8° semestre				
Pre-requisitos	Modelamiento de Procesos de Negocios				
Categoría	Obligatorio				
Área del Conocimiento según OCDE	Ciencias Sociales				
Profesor(es)	**Nombre Profesora/Profesor**		**Correo Electrónico**		

2.- CONTRIBUCIÓN AL PERFIL DE EGRESO

En lo particular, la asignatura de Gestión y Auditoria de Sistemas de Información contribuye al perfil de egreso a través del desarrollo del conocimiento teórico y práctico de la auditoría de procesos tecnológicos, con las materias propias de la planificación de la auditoria, objetos tecnológicos auditables, protección y resguardo de la información, abordando además, conceptos básicos y fundamentales relacionados con la ciberseguridad en base a estándares internacionales.

La asignatura aporta y propicia al perfil de egreso, al contemplar la:

Instauración del Gobierno corporativo de Tecnologías de la Información y su gobernanza. ISO38500 y/o COBIT5 Cobit 2019 Dominio 1

Revelación y validación de la información referida al gobierno y gestión de áreas tecnologías de la información (procesos tecnológicos), propiciando la implementación del control interno T.I. alineado con los objetivos estratégicos de la organización. ISO27000 (familia)

Normas, estándares y FrameWork base de CObit 5, Cobit 2019, familia ISO27000, ISO31000, ISO38500, principales normas NIST (National Institute of Standards and Technology) y contribuir a la Planificación de la Auditoria, diseñando programas de auditoría y redacción de Informe Técnicos de Auditoria.

3.- RESULTADOS DE APRENDIZAJE (RdeA)

Resultado de aprendizaje general	
Planificación y ejecución de auditoría de procesos tecnológicos a objetos de T.I. de mediana complejidad en base a estándares internacionales. Evaluación de riesgos asociados a procesos y objetos tecnológicos.	
Resultados de aprendizaje específicos	**Unidades temáticas**
1. Relacionar y explicar la auditoria especifica asociados a ambientes de control de Tecnologías de la Información.	Fundamentos de la Auditoria de Procesos Tecnológicos y Rol del Auditor y de la Auditoria.
2. Evaluar Control Interno de Tecnología de la Información.	Control Interno de T.I. Análisis de Riesgos Tecnológicos propiciando las contramedidas y/o optimización del control interno.
3. Planificación de la Auditoria en base a estándares ***Definición de:*** ● ***Objeto auditable*** ● ***Objetivo General de auditoria*** ● ***Objetivos Específicos*** ● ***Alcance*** ● ***Metodología*** ● ***Programa de Auditoria (Pc-Ps-Pa)*** ● ***Redacción de Pre-Informe Técnico de Auditoria*** ● ***Redacción Informe Final (Carta a la Gerencia)***	Marcos normativos y planificación de una auditoría. ISO 27000 27001 27002 ISO 38500 ISO 31000 ISO22301 ISO22313 ISO22316 ISO19011

4.- ESTRATEGIAS DE ENSEÑANZA Y DE APRENDIZAJE

En docencia directa con la identificación de riesgos tecnológicos, identificación y comprensión de procesos, actividades y tareas tecnológicos estructuradas. Estudio y análisis de situaciones de riesgos de TI a nivel nacional e internacional, conversación de control interno de TI: estándar, ideal y posible.

De forma grupal se realizarán talleres de análisis de riegos, planificación de estudios de casos reales y ficticios asociados a vulneración de la seguridad lógica y física y/o ineficiencias de tareas de TI.

Se desarrollara un proyecto semestral grupal-cooperativo relacionados con investigación de Estándares ISO, NIST, Inteligencia Artificial, ChatGPT, con avances mensuales y exposiciones de los estudiantes.

El trabajo autónomo de los estudiantes se relaciona con lecturas y análisis y desarrollo de situaciones CI de TI.

Especial valoración, como trabajo autónomo, tiene la asistencia a seminarios o charlas de profesores o personas destacadas de la profesión.

5.- EVALUACIONES

Como contexto, al inicio, es relevante compartir experiencias de situación criticas de vulnerabilidades de seguridad lógica y física; como éstas inciden e impactan en la sociedad de Inteligencias Interconectas y como proteger y custodiar los intangible digitales.

Como evaluación formativa se considera:

- Ensayos relacionados con casos atingentes a la gestión de la seguridad
- Proposición de controles específicos generales y de aplicación
- Construcción de Planificación de Trabajos de Auditoria, especialmente **PROGRAMAS De AUDITORIA** en base a Cobit, Normas ISO, CMF-RAN, NIST diñando pruebas de cumplimiento, sustantivas y analíticas.
- Redacción de Pre informes Técnicos
- Análisis y Cuantificación de Riegos Tecnológicos en base a ISO 31000, Cobit e ISO

Finalmente, como evaluación sumativa se aplica:
– Controles Individuales y grupales
– Pruebas escritas programadas de desarrollo fuera del aula,
– Exposiciones orales del trabajo final

Para las evaluaciones de los trabajos y exposiciones que impliquen la participación de pares, se utilizarán rúbricas, las que se entregarán al momento de definir la actividad.

Eventos evaluativos	Ponderación
Controles y/o trabajos (incluyen todas las evaluaciones que no corresponde a pruebas)	33%
Prueba Programada (PP) 1	33%
Prueba Programada (PP) 2	34%

Para aprobar el curso es condición que el estudiante tenga una calificación igual o superior a 4.0 en cualquiera de las dos Pruebas Programadas.

Quedará a criterio del profesor de la cátedra, optar por un examen de carácter oral, para aquellos estudiantes que hayan obtenido una de las dos PP con calificación menor a 4.0.

6.- ASPECTOS ADMINISTRATIVOS

Para el correcto desarrollo de este curso se requiere:
Considerar el Decreto Universitario 206 y modificaciones como norma de comportamiento esperado para el estudiante.

El curso requiere 75% de asistencia a clases, dejando evidencia de ello en una nómina firmada por cada estudiante, que luego se registra en la intranet.

Las inasistencias a Pruebas Programadas deben ser justificadas ante la Coordinación General de la carrera. Los estudiantes autorizados rendirán una prueba al final del semestre.

Durante la clase se deben observar las normas básicas de buenas costumbres y respeto mutuo.

Es especialmente relevante, observar y aplicar las normas y códigos de éticas de la profesión, como integridad, objetividad, escepticismo, responsabilidad, en cada actuación del curso.

El trabajo semestral de investigación se debe entregar en la fecha definida, en forma y fondo. Los integrantes de cada equipo deberán firmar un compromiso de responsabilidad, declarando haber trabajado a conciencia en el logro de los objetivos del equipo.

7.- RECURSOS DE APRENDIZAJE

Libros, publicaciones académicas, publicaciones profesionales	**Estándares** 1. Familia ISO2700 2. ISO27001 3. ISO27002 4. ISO38500 5. ISO31000 6. Cobit 5 7. Cobit 2019 8. NIST 800-xx (Identificar, proteger, detectar, detectar, responder, recuperar) 9. RAN-20-10 CMF

	Akerlof, George (1970) "*The market for "Lemons": Quality uncertainty and the market mechanism*" **Códigos de ética** 1. *Manual del Código de Ética para profesionales de la Contabilidad*, edición 2014, IESBA-IFAC[2] 2. *Código de ética,* The Institute of Internal Auditors, North America 3. *ISSAI[3] 30 - Código de Ética*, INTOSAI[4] **Cuerpos normativos** 1. ISO 27000 familia 2. ISO 38500 3. ISO 19011 4. ISO 31000 5. COBIT 5 6. COBIT 2019 7. NIST 8.
Páginas web	**www.iso27000.es** **www.isaca.org** **www.acfe.org** **www.nist.gov**
Plataformas	
Otros	1.
Otras recursos complementarios	

8.- PROGRAMACION DE ACTIVIDADES

Semana				
1	Objetivos del curso			
2	Contexto empresarial y Ciberseguridad			
3	Contexto empresarial y Ciberseguridad			
	Introducción a riesgos Tecnológicos			
4	Introducción a riesgos Tecnológicos			
5	Control Interno de TI			
6	Control Interno de TI			
7	Análisis y de Riesgos Tecnológicos de Gobernanza, Estratégicos, Tácticos, operacionales en todo ámbito de TI, planificación desarrollo y ejecución de soluciones de TI.			
8	Análisis y de Riesgos Tecnológicos de Gobernanza, Estratégicos, Tácticos, operacionales en todo ámbito de TI, planificación desarrollo y ejecución de soluciones de TI.			
9	Análisis y de Riesgos Tecnológicos de Gobernanza, Estratégicos, Tácticos, operacionales en todo ámbito de TI, planificación desarrollo y ejecución de soluciones de TI.			
10	Análisis y de Riesgos Tecnológicos de Gobernanza, Estratégicos, Tácticos, operacionales en todo ámbito de TI, planificación desarrollo y ejecución de soluciones de TI. Aplicando ISO31000 análisis de riesgos de TI en entorno reales. Entrega de informe de Análisis de Riesgos.			
11	Planificación de la Auditoria de procesos Tecnológicos practica (programas de auditoria: Objeto auditable, objetivo general,			

	objetivos específicos, alcance, metodología, pruebas de cumplimento, sustantivas y analíticas aplicadas a entornos de TI)			
12	Planificación de la Auditoria de procesos Tecnológicos practica (programas de auditoria: Objeto auditable, objetivo general, objetivos específicos, alcance, metodología, pruebas de cumplimento, sustantivas y analíticas aplicadas a entornos de TI)			
13	Planificación de la Auditoria de procesos Tecnológicos practica (programas de auditoria: Objeto auditable, objetivo general, objetivos específicos, alcance, metodología, pruebas de cumplimento, sustantivas y analíticas aplicadas a entornos de TI) – NORMAS ISO, CMF-RAN-NIST			
14	Planificación de la Auditoria de procesos Tecnológicos practica (programas de auditoria: Objeto auditable, objetivo general, objetivos específicos, alcance, metodología, pruebas de cumplimento, sustantivas y analíticas aplicadas a entornos de TI) – NORMAS ISO, CMF-RAN-NIST			
15	Planificación de la Auditoria de procesos Tecnológicos practica (programas de auditoria: Objeto auditable, objetivo general, objetivos específicos, alcance, metodología, pruebas de cumplimento, sustantivas y analíticas aplicadas a entornos de TI) – NORMAS ISO, CMF-RAN-NIST			
16	Investigación de Nuevas Normas relativas a Ciberseguridad			
17	Investigación de Nuevas Normas relativas a Ciberseguridad, exposición.			