Programa de Asignatura

Carrera:

Contador Público

Plan de Estudio (aprobado por ordenanza):

Ord 05/2018-CD y Ord 66/2018-CS

Espacio Curricular:

4724 - Seguridad De Sistemas De Información / Electiva

Aprobado por resolución número:

Res. 62/2025- CD

Programa Vigente para ciclo académico:

2025

Profesor Titular (o a cargo de cátedra):

DICHIARA, Andrea Amalia

Profesores Adjuntos:

DICHIARA, Andrea Amalia

Jefes de Trabajos Prácticos:

CERDA CHARADIA, Ramón Horacio
GIUNTA FORNASIN, Elizabeth
MAJOWKA, Pablo David

Características

Área	Periodo	Formato espacio curricular	Créditos
Economía, Administración, Sistemas y Gestión		Teórico-Aplicado	6

Requerimiento de tiempo del estudiante:

Horas clases teoría	Horas clases práctica	Subtotal horas clases	Horas de estudio	Horas de trabajo autónomo	Evaluaciones	Total horas asignatura
30	30	60	50	60	10	180

Espacios curriculares correlativos

Sistemas Y Tecnologías de Información ,

Contenidos

Fundamentos:

La Seguridad de la Información constituye un elemento fundamental dentro de la estrategia empresarial de cualquier organización. En el marco del gobierno de tecnologías de la información, desempeña un papel crucial al respaldar a las organizaciones en la revisión y evaluación de políticas, procedimientos y controles. Este enfoque permite optimizar el uso de la información de manera segura y efectiva, asegurando así el cumplimiento de los objetivos del negocio.
En este contexto, es imperativo que los estudiantes adquieran los conocimientos necesarios para utilizar metodologías de análisis de riesgos. Esto les permitirá identificar vulnerabilidades asociadas con la seguridad de la información y comprender la importancia de establecer políticas, planes, programas y medidas de control. Estas iniciativas fortalecen la gestión organizacional y protegen los recursos tecnológicos al analizar, evaluar y proponer mejoras en los sistemas de control interno.
Además, este aprendizaje capacita a los estudiantes para reconocer herramientas y productos tecnológicos que refuercen los controles y mitiguen riesgos. De esta manera, se mejora significativamente la seguridad de los sistemas de información, asegurando la integridad y confidencialidad de los datos críticos de la organización.

Contenidos Mínimos:

Auditoría de sistemas computadorizados: Seguridad de los activos informáticos. Seguridad de las aplicaciones. Análisis de riesgos CIS (Aplicaciones - Centro de cómputos). Auditoría de sistemas en desarrollo y de sistemas en funcionamiento. Delito informático. Aplicación en sistemas complejos.

Competencias Generales:

Utilizar tecnologías de información y comunicación genéricas y especializadas en su campo como soporte de su ejercicio profesional
Plantearse preguntas para la investigación, el pensamiento lógico y analítico, el razonamiento y el análisis crítico
Asignar prioridades y trabajar en entornos de alta exigencia con la finalidad de brindar respuestas oportunas y de calidad
Capacidad crítica y autocrítica
Capacidad para encontrar nuevas ideas y soluciones
Capacidad para trabajar con iniciativa y espíritu emprendedor
Compromiso ético en el trabajo y motivación por la calidad del trabajo
Capacidad para trabajar con otros en equipo con el objetivo de resolver problemas
Flexibilidad para trabajar en entornos de diversidad
Capacidad para manejar efectivamente la comunicación en su actuación profesional: habilidad para la presentación oral y escrita de trabajos, ideas e informes
Desarrollar una visión global de las organizaciones, con espíritu abierto, flexible en entornos de diversidad e innovador.
Trabajar con iniciativa y espíritu emprendedor en equipos interdisciplinarios y con capacidad de liderazgo con actuación multidisciplinaria, visión sistémica y sustentable, motivando a los miembros del equipo hacia el logro de objetivos comunes.

Competencias Específicas:

Capacidad de diseñar, implementar, evaluar y controlar sistemas de gestión y auditoría operativa
Capacidad para describir, analizar, sintetizar, representar, diseñar, auditar y rediseñar procesos de negocios y los sistemas de información asociados

Capacidad de aplicar las herramientas de tecnología de la información y del procesamiento de datos para la resolución de situaciones profesionales
Capacidad para interpretar, evaluar y proyectar los hechos económicos que afecten a las organizaciones y las unidades productivas

Programa de Estudio (detalle unidades de aprendizaje):

UNIDAD 1: MARCO CONCEPTUAL DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN:
Introducción a la seguridad de la información. Concepto de Seguridad. Diferencia entre Seguridad en los sistemas de información y Seguridad Informática. Definición de una política de seguridad informática: Organización y divisiones de responsabilidades. Seguridad Física. Seguridad Lógica. Introducción a las Gtag: Definición y tipos de Guías.

UNIDAD 2: PROCESO DE CONTROL PARA LA PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN
Seguridad y Control. Controles de los Sistemas de Información. Controles Generales. Controles de las aplicaciones. Objetivos de Seguridad de la Información. Estándares de programación y operaciones de sistemas. Aplicación de la seguridad efectiva en computación. Inventario de Riesgos de seguridad. Revisión de Seguridad. Componentes de un marco de trabajo organizacional para la seguridad y control. Casos de estudio en seguridad.

UNIDAD 3 : CONTROL INTERNO Y GESTIÓN DE RIESGO EMPRESARIAL (ERM)
Control Interno: Concepto. Elementos. Tipos de Controles. Principios. Informe COSO. Evolución COSO I y COSO III. COSO III: Objetivos. Estructura. Entorno de Control. Evaluación de Riesgo. Actividades de control. Información y Comunicación. Actividades de Monitoreo. ERM (Enterprise Risk Managament): Origen del Riesgo. Componentes del riesgo. Mapa de Riesgo. Auditoría Interna y ERM. Las funciones de control interno y auditoria informática. Similitudes y analogías

UNIDAD 4: CONTROLES DE LAS APLICACIONES
Concepto de Aplicaciones: Objetivos. Tipos de los Controles: Controles de entrada, controles de procesamiento y controles de salida. Controles Generales de TI (ITGC). Controles de las Aplicaciones vs. Controles Generales de TI. Beneficios de los Controles de las Aplicaciones. Enfoque de Evaluación de Riesgos. Enfoque de Revisión de Aplicaciones –Técnicas de Documentación. Gtag 8

UNIDAD 5: SEGURIDAD INFORMÁTICA:
Seguridad y control de la información. Seguridad Informática y Ciberseguridad. Criterios de Seguridad. Otros Criterios relacionados. Protección de la Información: Seguridad Informática. Hardware. Software. Datos. Personas. Concepto de amenazas, vulnerabilidades y ataques. Tipos de amenazas, vulnerabilidades y ataques. Medidas de Seguridad. Políticas de Seguridad. Marco de referencia ISO/IEC 27001. Ley 26388 Delitos Informáticos. GTAG 9: Definición del proceso IAM. Abordaje del proceso IAM. Conceptos claves. Puesta en marcha del proceso IAM. Auditoria del Proceso IAM. Herramientas para la salvaguarda de los recursos de Información: Firewalls. Sistema de detección de intrusos. Antivirus y antispyware. Seguridad en la nube. Ciberseguridad.

UNIDAD 6: GESTIÓN DE DATOS Y PLATAFORMAS DE BASES DE DATOS
Conceptos básicos: Base de datos. Estructura de datos. Sistema de Gestión de Base de datos. Lenguajes. Uso y conocimiento de programas de manejo de base de datos. Importancia de su conocimiento como herramienta tecnológica para afianzar aspectos de seguridad de la información. Introducción a SQL: Definición y Manejo de datos en base de datos. SQL como Herramienta para Definir y Manipular Datos. Aplicación de Conceptos de Gestión de Bases de Datos en Entornos Reales. Laboratorio de Administración de Bases de Datos con SQL. GTAG 16: Técnicas de análisis de

datos. Definición. Etapas. Beneficios del análisis de datos. Aplicaciones para administrar base de datos: ACL-EXCEL-ACCESS.

UNIDAD 7: ASPECTOS ÉTICOS
Introducción a los Aspectos Generales de la Ética en el Ejercicio Profesional. Principios Éticos. Aspectos éticos, sociales y políticos de los Sistemas de Información. Dimensiones morales de la era de la información: Derechos y obligaciones de información. Derechos y obligaciones de propiedad. Rendición de cuentas y control. Calidad del sistema. Calidad de vida. Tendencias de tecnología clave que generan aspectos éticos. Conciencia de relaciones no evidentes (Nora). Conceptos básicos: responsabilidad, rendición de cuentas y responsabilidad legal. Análisis éticos. Principios éticos candidatos. Código profesional de conducta. Dilemas éticos del mundo real.

Metodología

Objetivos y descripción de estrategias pedagógicas por unidad de aprendizaje:

UNIDAD 1: MARCO CONCEPTUAL DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN:
Resultado del Aprendizaje: Que el estudiante sea capaz de identificar y comprender los principios deontológicos aplicables al uso y gestión de los sistemas de información en contextos tecnológicos, así como reconocer la importancia del control interno y sus modelos asociados, tanto en los procesos operativos como en los sistemas informáticos.
Estrategias de enseñanza y aprendizaje: Exposición teórica participativa para introducir conceptos fundamentales. Análisis de casos reales sobre dilemas éticos y control interno en sistemas de información. Actividades prácticas de aplicación, como mapas conceptuales y ejercicios guiados, para reforzar la comprensión de los modelos de control interno y su vinculación con la seguridad.

UNIDAD 2: PROCESO DE CONTROL PARA LA PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN
Resultado de aprendizaje: Que el estudiante comprenda e implemente los procesos de control necesarios para proteger los sistemas de información, identificando vulnerabilidades, evaluando riesgos y aplicando medidas preventivas, detectivas y correctivas, conforme a estándares y buenas prácticas de seguridad. Desarrolle las competencias sociales e intelectuales necesarias para el trabajo interdisciplinario eficiente y cooperativo.
Estrategias de enseñanza y aprendizaje: Clases expositivas con apoyo de recursos visuales y normativas aplicables. Estudio de casos para analizar fallos de control en sistemas reales. Talleres prácticos orientados al diseño y evaluación de controles de seguridad (lógicos, físicos y administrativos). Simulación de escenarios de riesgo para aplicar procesos de mitigación y respuesta.
UNIDAD 3: CONTROL INTERNO Y GESTIÓN DE RIESGO EMPRESARIAL (ERM)
Resultado de aprendizaje: Que el estudiante sea capaz de analizar y aplicar los componentes del control interno y del modelo de Gestión de Riesgos Empresariales (ERM), identificando amenazas potenciales, evaluando su impacto en los activos de información y proponiendo estrategias de mitigación alineadas con los objetivos organizacionales.
Estrategias de enseñanza y aprendizaje: Clases teóricas con apoyo en marcos de referencia como COSO, para contextualizar los conceptos de control interno y gestión de riesgos. Análisis de casos prácticos para identificar debilidades de control y evaluar el impacto de riesgos no gestionados. Actividades colaborativas (como mapas de calor, matriz de riesgos o líneas de defensa) que fomenten la toma de decisiones fundamentadas. Ejercicios de simulación o role-playing para experimentar la aplicación de un enfoque ERM en entornos organizacionales simulados.
UNIDAD 4: CONTROLES DE LAS APLICACIONES:
Resultado de aprendizaje: Que el estudiante identifique, evalúe y aplique los diferentes tipos de controles en aplicaciones informáticas —como controles de entrada, procesamiento, salida, integridad y acceso— con el fin de garantizar la confiabilidad, confidencialidad e integridad de los datos en los sistemas de información.
Estrategias de enseñanza y aprendizaje: Clase expositiva para introducir los tipos y objetivos de los controles de aplicación. Análisis de ejemplos reales de fallos por ausencia de controles y sus consecuencias organizacionales. Prácticas guiadas en entornos simulados o herramientas de software para identificar y documentar controles de aplicación. Estudio de casos para evaluar la eficacia de controles existentes y proponer mejoras. Diseño de esquemas de control para flujos de información en aplicaciones empresariales, utilizando herramientas como diagramas de flujo o modelos y notación de procesos de negocios.
UNIDAD 5: SEGURIDAD INFORMÁTICA:
Resultado de aprendizaje: Que el estudiante comprenda los principios fundamentales de la

seguridad informática y logre los conocimientos y habilidades necesarios para desempeñarse con idoneidad en materia de sistemas, logrando conocimientos básicos en seguridad informática. Que sea capaz de identificar amenazas y vulnerabilidades en entornos digitales, aplicando medidas de protección adecuadas para salvaguardar la confidencialidad, integridad y disponibilidad de la información.
Estrategias de enseñanza y aprendizaje: Exposición teórica de los conceptos clave de seguridad informática. Análisis de casos reales de incidentes de seguridad para contextualizar los riesgos y sus impactos. Laboratorios prácticos sobre protección de sistemas, análisis de malware, uso de antivirus y firewalls. Uso de recursos multimedia (videos, simuladores, infografías) para reforzar el aprendizaje conceptual y práctico.
UNIDAD 6: GESTIÓN DE DATOS Y PLATAFORMAS DE BASES DE DATOS
Resultados del aprendizaje: Que el estudiante comprenda los principios de la gestión de datos y su importancia en la seguridad y eficiencia de los sistemas de información. Que el estudiante sea capaz de manipular, organizar y gestionar datos empresariales de manera eficiente, aplicando herramientas y técnicas que permitan transformar datos en información útil para la toma de decisiones, garantizando la calidad, seguridad y disponibilidad de los mismos.
Estrategias de enseñanza y aprendizaje: Clases teóricas apoyadas en ejemplos reales para introducir conceptos clave de bases de datos y gestión de datos. Actividades prácticas en laboratorios para la creación, consulta, mantenimiento y aseguramiento de bases de datos en distintas plataformas (por ejemplo, MySQL, PostgreSQL, MongoDB, etc.).Uso de simuladores o entornos virtuales para practicar configuraciones de seguridad (roles, permisos, cifrado, respaldos).
UNIDAD 7: ASPECTOS ÉTICOS
Resultado del Aprendizaje: Que el estudiante analice y aplique los principios éticos fundamentales que rigen el ejercicio profesional del contador en el contexto de la seguridad de los sistemas de información, identificando dilemas éticos, responsabilidades legales y buenas prácticas en el manejo, protección y uso de datos e información sensible.
Estrategias de enseñanza y aprendizaje: Clases teóricas sobre ética profesional, confidencialidad, integridad y responsabilidad en el uso de sistemas de información. Análisis y debate de casos reales sobre conflictos éticos en la práctica contable vinculada a la seguridad informática. Lectura y reflexión crítica de códigos de ética profesional. Actividades colaborativas para identificar riesgos éticos en entornos digitales (uso indebido de datos, acceso no autorizado, manipulación de información). Desarrollo de ensayos o presentaciones en los que el estudiante proponga soluciones éticas a situaciones problemáticas en el ámbito contable-digital.

Carga Horaria por unidad de aprendizaje:

Unidad	Horas teóricas	Horas de trabajos prácticos	Horas de actividades de formación práctica	Horas de estudio	Horas de trabajo autónomo	Evaluaciones
Unidad 1	1	0	0	2	8	1
Unidad 2	2	0	0	3	6	1
Unidad 3	2	1	1	5	8	1
Unidad 4	6	3	4	10	9	2
Unidad 5	7	4	3	10	10	2
Unidad 6	6	4	3	10	10	2
Unidad 7	6	4	3	10	9	1

Programa de trabajos prácticos y/o aplicaciones:

Bibliografía (Obligatoria y Complementaria):

ACCESS, MANUAL DEL USUARIO, Colección Manuales USERS, (MP ediciones, Buenos Aires, 2010). -Complementaria.
ACCESS DESDE CERO, Colección coordinada por Benchimal Daniel (Buenos Aires, Fox Andina, 2011).-Complementaria.
ALDEGANI, Gustavo, Seguridad Informática,, (Bs. As., MP ediciones SA, 1997).Complementaria.
ALONSO RIVAS, Gonzalo, "Auditoría Informática", (Nadird, Diaz Santos, 1987).Complementaria
ARENS, Alvin A. y LOEBBECKE, James K., Auditoría, un enfoque inte-gral, (México, Prentice Hall Inc., 6ta. Ed.).
BANCO CENTRAL DE LA REPUBLICA ARGENTINA CONAU 1.-Complementaria.
BURGOS, Alexis, "Como proteger la PC", Colección Manuales USERS, (Buenos Aires, 2007).Complementaria.
CASTELLO, Ricardo J.,"Auditorías en Entornos Informáticos", 1ra. ed. (Córdoba, U.N. de Córdoba, 1998). Obligatoria.
COBIT, Objetivos de Control, Comité Directivo del COBIT y la Informa-tion Systems audit. And Control Foundation, tr. Gustavo Solís Montes (CISA). Obligatoria
COMPUTACIÓN PARA CONTADORES, Colección Manuales USERS, Buenos Aires, 2005.Complementaria.
COOPERS & LYBRAND: Los nuevos conceptos del control interno (In-forme COSO), tr. I.A.Internos España y Coopers & L. (Ed. Díaz Santos, Madrid, 1997). Complementaria.
DAVILA LADRÓN DE GUEVARA, Fernando, Hacia la inteligencia del negocio con Excel 2003, (Bogotá, Editorial Politécnico Grancolombiano, 2005).Complementaria.
DE WINDOWS A LINUX, Colección Manuales USERS, (MP ediciones, Buenos Aires, 2010). Complementaria.
CAMPO, Roberto Daniel, "Manual Práctico de Auditoría Interna"-1ª ed. (Ciudad Autónoma de Buenos Aires, CPCECABA, 2012) Obligatoria.
CAMPO, Roberto Daniel, "Manual Práctico II de Auditoría Interna"-1ª ed. (Ciudad Autónoma de Buenos Aires, Edición Fondo Editorial Consejo, 2015).Obligatoria.
PUNGITORE, José Luis, "Sistemas Administrativos y Control Interno"2ª ed. (Ciudad Autónoma de Buenos Aires, Osmar D. Buyatti, 2013).Obligatoria.
ESTUPIÑÁN GAITÁN, Rodrigo, "Administración o Gestión de Riesgos E.R.M. y la Auditoria Interna.(Bogotá, Ecoe Ediciones, 2006). Obligatoria.
LEONARD, H.Fine, " Seguridad en el Centro de Cómputos-Políticas y Procedimientos- 2ª ed.
9
(México, Trillas, 1990). Obligatoria.
VELTHUIS, Mario Gerardo, "Auditoria Informática-un enfoque práctico"(Madrid, Rama 1998). Complementaria.
DRUCKER, Peter F., "El ejecutivo eficaz", (Bs. As., Editorial Sudamericana, 1999). Complementaria.
DU MORTIER, Gustavo, Macros en Office, (Buenos Aires, PC Forum SA, 2005, Segunda edición). Complementaria.
ECHENIQUE GARCÍA, José, "Auditoría e Informática", (México, Mc. Graw Hill, 1990).Obligatoria.
FEDERACION ARGENTINA DE COLEGIOS DE GRADUADOS DE CIENCIAS ECONOMICAS Instituto Técnico de Contadores Públicos (ITCP): Dictámenes, recomendaciones e informes pertinentes.Complementaria.
FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES DE CIEN¬CIAS ECONOMICAS Centro de Estudios Científicos y Técnicos (CECyT), Manual de auditoría (Informe nro. 5 del Area Auditoría).Complementaria.

FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES DE CIEN¬CIAS ECONOMICAS Centro de Estudios Cientí¬ficos y Técnicos (CECyT), Pautas para el examen de estados contables en un contexto computadorizado (Informe nro. 6 del Area Auditoría).Complementaria.
FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES DE CIEN¬CIAS ECONOMICAS Centro de Estudios Cientí¬ficos y Técnicos (CECyT), Auditoría en ambientes computadorizados (Informe nro. 15 del Area Auditoría).Complementaria.
FEDERACION ARGENTINA DE CONSEJOS PROFESIONALES DE CIENCIAS ECONOMICAS Centro de Estudios Científicos y Técnicos (CECyT): Resoluciones técnicas 7 y 15 e informes pertinentes.Complementaria.
FIRTMAN, Sebastián, Seguridad Informática , Colección Manuales USERS, Buenos Aires, 2006.Complementaria.
GARCÍA FRONTI, Matías y otros, Auditoría del negocio con Microsoft Excel, Herramientas Informáticas para la pequeña y Mediana Empresa, (Buenos Aires, Omicron System S.A. 2002).Complementaria.
GONZÁLEZ, Darío Angel y ACOSTA, Adrián, Técnicas avanzadas. Mi-crosoft Office 2000, (Bs. As., MP ediciones SA, 1999).Complementaria.
INSTITUTO AMERICANO DE CONTADORES PÚBLICOS (AICPA), "Normas Internacionales de Auditoría", 3 ed., (Ediciones Foc SA, México, 1997).Complementaria.
LAUDON Kenneth y LAUDON Jane.- Sistemas de Información gerencial- Organización y tecnología de la empresa conectada en red. 6ta. Edición (2002).Complementaria.
LEONARD, William P., Auditoría Administrativa, (Editorial Diana, México, 1972).Complementaria.
MAZZOLA, Nicolás, Windows XP, Manuales USERS, (Buenos Aires, MP Ediciones,
10
2005).Complementaria.
NARDELLI, Jorge, "Auditoría y seguridad en los sistemas de computación", (Buenos Aires, Cangallo, 1990).Obligatoria.
Normas internacionales de Contabilidad (NICs).Complementaria.
Normas internacionales de Auditoría (NIAs).Obligatoria.
PORTANTIER, Fabián, "Seguridad Informática", 1ra. Ed. (Buenos Aires, Fox Andina, Dalaga, 2012)
PREVENCION Y DETECCION DE DELITOS INFORMATICOS - ISBN 844151545X - Autor LITTLE JOHN SHINDER DEBRA - Editorial ANAYA MULTIMEDIA - Nivel MEDIO – AVANZADO.Complementaria.
PROTECCION INFORMATICA 1998- Pierre Gratton -Edit. Trillas.Complementaria.
Resolución C.P.C.E. Mza. N° 1350/2001: Código de ética unificado para Profesionales en Ciencias Económicas de la Rep. Argentina – R. 204/2000 FACPCE. y las Normas de Organización y Procedimientos del Tribunal de Ética.Obligatoria.
SANCHEZ Claudio, Excel XP 100 respuestas avanzadas, Manuales USERS, (MP ediciones, Buenos Aires, 2002). Complementaria.
SEGURIDAD INFORMATICA: Técnicas Criptográficas - Pino Caballero -Edit.:RA-MA.Obligatoria.
SEGURIDAD, PROTEJA SUS DATOS, Colección Manuales USERS, (MP ediciones, Buenos Aires, 2010). Complementaria.
Sindicatura General de la Nación – Pautas de Control Interno – Sistemas Computarizados y Tecnología de Información.Complementaria.
SLOSSE, Carlos A. y otros, Auditoría, un nuevo enfoque empresarial, (Bs.As., Macchi).Complementaria.
STOLTZ, Kevin, Todo acerca de ...Redes de computación, (México, Prentice Hall, 1995).Complementaria.
www.tectimes.com.Complementaria.
www.redusers.com.ar.Complementaria.
ZANINI, Viviana, "Macros en Excel 2013", 1ra. Ed. (Buenos Aires, Fox Andina 2013.Complementaria.

Metodología de enseñanza y aprendizaje:

- Para alcanzar los objetivos generales planteados, se procurará trabajar didácticamente para promover el aprendizaje significativo y funcional, mediante la comunicación directa e interacción entre alumnos y docentes.
- En especial, se tratará de superar la mera ilustración, promoviendo el máximo razonamiento lógico de cada educando próximo a egresar, e incentivando la formación de criterios profesionales genéricos, que permitan su aplicación correcta de herramientas para salvaguardar la seguridad de los sistemas de información.
- Las clases tendrán el carácter de aula taller. Se suministrarán guías de aprendizaje con planteo de problemas, sus resoluciones y fundamento de las mismas. Se encararán trabajos grupales e individuales. Se suministrará material de lectura y se fomentará su búsqueda, referido a temas complementarios a las clases que se dicten, intentando crear inquietudes adicionales a las planteadas en el programa de la materia.
- La asignatura se desarrollará con: exposiciones docentes, ejercicios grupales, talleres, presentación de trabajos escritos por los alumnos, charlas debate y haciendo uso de la plataforma educativa de la Facultad.
- En especial se utilizará la técnica de talleres de planificación y trabajo, privilegiando en ellos las actividades prácticas. Se exaltará la utilidad y valor del taller como actividad que favorece la participación, la interacción, la idea de equipo y de solidaridad entre sus integrantes, de modo que todos (coordinador y alumnos) aportan sus experiencias y habilidades a fin de lograr un resultado común que incremente los conocimientos del grupo.

Sistema y criterios de evaluación

El régimen de evaluación consistirá en : - Dos evaluaciones parciales - Un recuperatorio de parciales - Examenes finales programados en el calendario académico.
Las inasistencias a los exámenes programados equivalen a aplazos. Se tomará un mínimo de 2 (dos) evaluaciones parciales. Los temas incluidos en dicha evaluación tendrán relación con lo dictado en el cursado de la materia, pudiendo también incluir temas específicos que la cátedra disponga.
El alumno para rendir el examen parcial, deberá acreditar una asistencia no menor al 70% sobre el total de las clases desarrolladas en las distintas modalidades adoptadas durante el cursado. Las evaluaciones parciales serán escritas o bajo la utilización de la plataforma Econet. Los requisitos para su aprobación serán consignados claramente en el encabezado de cada examen a rendir, consignando el puntaje mínimo que deberá alcanzar en el supuesto que el examen se divida en partes. No obstante como pauta general para su aprobación, el puntaje a obtener será el equivalente al 60% sobre un total de 100%. Si el examen se divide en partes, deberán alcanzar como mínimo el 50% de cada una de ellas.Los examenes parciales incluirán casos prácticos y de contenido conceptual.
Los alumnos que resultaren desaprobados o estuviesen ausentes en una de las evaluaciones parciales, tendrán la posibilidad de rendir un examen recuperatorio. Este tipo de exámenes serán rendidos después de haberse comunicado la nota del segundo examen parcial.
El examen integrador constará de desarrollos teóricosy prácticos, bajo el mismo sistema de calificación descripto en párrafos anteriores.

Requisitos para obtener la regularidad

Finalizado el cursado el alumno adquiere la regularidad en las siguientes condiciones: a) Alumno "Regular": La metodología de evaluación se instrumentará a través de la exigencia de dos (2) exámenes parciales, con posibilidad de recuperar uno (1) de ellos Por lo tanto se considerará en esta categoría al alumno que haya aprobado todas las evaluaciones programadas o un parcial y recuperatorio. Cada uno de estos instrumentos de evaluación deberá aprobarse con un mínimo del

60 %.Si cualquiera de los examenes se divide en partes, deberán alcanzar como mínimo el 50% de cada una de ellas. Deberá registrar una asistencia a clases del 70%. b) El alumno que no alcance las condiciones de regularidad, por haber desaprobado dos parciales o un parcial y su correspondiente recuperatorio podrá rendir un examen integrador según el articulo duodécimo de la ordenanza 18/03 CD y modificaciones, que en caso de ser aprobado , le dará la condición de regular.

Requisitos para aprobación

a) Promoción: aprobando todas las evaluaciones (parciales o sus respectivos recuperatorios) con un mínimo de 70 puntos cada una
b) Alumno regular: Los alumnos definidos en esta categoría, rendirán en los turnos que establece el Art. 11 de la ordenanza 18/03 CD y modificaciones, siendo las fechas consignadas en la Programación Anual de Actividades de la Facultad, debiendo cumplirse con el requisito de inscripción en las condiciones que la misma defina. La asignatura será aprobada por el alumno que habiendo alcanzado la regularidad apruebe el examen final. Este examen final podrá ser oral, escrito o bajo la utilización de la plataforma de Econet, según disposición de la Cátedra en cada oportunidad, con puntaje mínimo del 60% sobre un total de 100%. Si el examen se divide en partes, deberán alcanzar como mínimo el 50% de cada una de ellas .Las consignas de los exámenes podrán referirse tanto a aspectos exclusivamente prácticos como teóricos, o la combinación de ambos.Entre las formas de regularizar la materia se encuentra la especificada por el art. 12 de la Ord. 18/2003-CD modificado Ord 2/2016- CD
c) Alumno libre: Los alumnos que se encuentren en la condición de "libre" aprobarán la asignatura con una evaluación que tendrá dos partes. En primer lugar desarrollarán una prueba escrita de carácter excluyente con relación a la segunda parte, con las mismas características que el examen del alumno regular. Una vez aprobada esta instancia, los alumnos en cuestión deberán rendir un examen oral o escrito. Aprobado este último, se considera aprobada la asignatura.
A continuación se expone la escala de calificaciones, Ord. 108/10-CS: Las categorías establecidas refieren a valores numéricos que van de 0 (cero) a 10 (diez) fijándose las siguientes correspondencias: (0) cero para puntaje de 0% - No aprobado (1) uno para puntaje de 1% a 12% - No aprobado (2) dos para puntaje de 13% a 24% - No aprobado (3) tres para puntaje de 25%a 35% - No aprobado (4) cuatro para puntaje 36% a 47% - No aprobado (5) cinco para puntaje 48% a 59% - No aprobado (6) seis para puntaje de 60% a 64% - Aprobado (7) siete para puntaje de 65% a 74% - Aprobado (8) ocho para puntaje 75% a 84% - Aprobado (9) nueve para puntaje 85% a 94% - Aprobado (10) diez para puntaje de 95% a 100% - Aprobado Cuando la primera cifra decimal en la escala porcentual sea de 5 (cinco) o más, se aproximará al valor entero inmediato superior. La adopción de la escala requerirá por parte de los docentes la discusión, análisis y acuerdo sobre los saberes mínimos exigidos para la aprobación de la obligación curricular y la ponderación de los mismos según el grado de importancia establecido. Esta tabla es de aplicación para toda evaluación durante el cursado y para la calificación final en la asignatura.