PROGRAMA DE ASIGNATURA

IDENTIFICACIÓN DE LA ASIGNATURA	NOMBRE ASIGNATURA	Fundamentos de ciberseguridad
	CÓDIGO	13171 / 13233 / 13268 / 13269 / 13270
	CARRERA	Ingeniería de ejecución en computación e informática / Ingeniería civil en informática
	DICTA DEPARTAMENTO	Ingeniería informática
	NIVEL	7
	CRÉDITOS SCT-CHILE	6 SCT
	T-E-L	4-0-2
	TRABAJO AUTÓNOMO SEMANAL	6 horas
	REQUISITOS	
	ENFOQUE DISCIPLINAR	Monodisciplinar
	TIPO	Teórica/Práctica
	ÁREA DE FORMACIÓN	*Electivo/Tópico de la especialidad*
	PERFIL DEL DOCENTE	Debe poseer especialización y experiencia tópicos de ciberseguridad. Formación y experiencia de trabajo en metodologías de aprendizaje activas. Es deseable experiencia en la dirección de equipos de trabajo para la implementación de estándares y buenas prácticas de ciberseguridad en organizaciones.
	VERSIÓN	2/2021
	RESOLUCIÓN PLAN DE ESTUDIO	1638 / 2014

RESULTADO DE APRENDIZAJE GENERAL
Planificar soluciones orientadas a fortalecer la integridad, confidencialidad y disponibilidad de los activos de digitales de una organización.

UNIDADES TEMÁTICAS	
UNIDAD 1: Introducción	
Comprender los conceptos y sus relaciones sobre ciberseguridad.	Motivación
	Conceptos relacionados con la ciberseguridad
	Relaciones entre conceptos
	Tipos de controles
	Glosario de conceptos
	Análisis de riesgos cualitativo básico
UNIDAD 2: Buenas prácticas, estándares y metodologías	
Aplicar metodologías, normativas y/o estándares para proteger los activos digitales en las organizaciones.	El valor de las buenas prácticas, estándares y metodologías en ciberseguridad
	Estándares para la ciberseguridad
	Metodologías para la ciberseguridad
	Buenas prácticas
UNIDAD 3: Gobierno y gestión de la ciberseguridad	
Planear la ciberseguridad en las organizaciones.	Gobierno de la seguridad de la información y ciberseguridad
	Gestión de la seguridad de la información
	Gestión riesgos
	Gestión de la ciberseguridad
UNIDAD 4: Implementación y operación de la ciberseguridad	
Proponer soluciones que den seguridad a los activos digitales de acuerdo con el perfil de la organización	Funciones de la ciberseguridad
	Alineando la gestión con la operación
	Aplicación de la ciberseguridad en la operación

CONTRIBUCIÓN AL PERFIL DE EGRESO

DESEMPEÑOS INTEGRALES COMUNES

- Diseñar sistemas, componentes o procesos, considerando buenas prácticas, estándares y tecnologías pertinentes, así como variables económicas, ambientales, culturales y sociales.
- Formular, evaluar y gestionar proyectos del ámbito de la ingeniería, considerando equipos de trabajo, aspectos y contextos involucrados y los impactos de su quehacer profesional.

DESEMPEÑOS INTEGRALES ESPECÍFICOS

- Construir abstracciones de fenómenos del mundo real, transformando datos en información útil, que contribuyan a la gestión y toma de decisión en la organización, resguardando la calidad del proceso, privacidad, veracidad y buen uso de la información.
- Gestionar la implementación y operación de TICs de acuerdo con los objetivos estratégicos de personas y organizaciones, colaborando como miembro o líder de equipos de trabajo, tomando decisiones basadas en conocimiento disciplinar y los avances en las tecnologías de información y comunicación, aplicando criterios de calidad, sostenibilidad y éticos.

ELEMENTOS DEL SELLO INSTITUCIONAL	ATRIBUTOS I+E
- Trabajar en equipo - Aprender de manera autónoma - Postura ética - Responsabilidad social y conciencia ciudadana - Adaptabilidad	- Comunicación - Trabajo grupal e individual - Diseño - Proyectos con usuarios reales - Seguridad y riesgos - Ética y profesionalismo

ESTRATEGIAS METODOLÓGICAS

Breve descripción de cómo se aborda el curso en términos de estratégicas y metodologías didácticas, considerando los espacios de teoría, ejercicios y laboratorio, según corresponda, además del tiempo de trabajo autónomo.

Se utilizarán estrategias metodológicas de enseñanza-aprendizaje-evaluación que fortalezcan el logro de los aprendizajes, para ello se considera lo siguiente:

- Clases teóricas-prácticas basadas en una acción de aprendizaje planificada y en la experimentación.
- Se utilizarán, como ejemplo, casos contingentes relacionados con los tópicos vistos en clases para que el estudiante asocie el contenido de los temas a su día a día.
- Clases teóricas y prácticas para explicar los fundamentos de la asignatura, para lo cual se considera el diseño y simulación en forma computacional de problemas cotidianos
- Autoaprendizaje guiado mediante la lectura de apuntes y resolución de problemas.
- Colaboración en la construcción del conocimiento mediante la discusión de los temas estudiados.
- Clases de consolidación donde se resuelvan problemas complejos integrando todos los contenidos estudiados hasta el momento con la guía del profesor.
- Laboratorios prácticos donde se simularán diferentes escenarios y problemáticas planteados durante la enseñanza de los temas.
- Los laboratorios están guiados para la aplicación de los conceptos enseñados en la cátedra, los cuales son abordados a un nivel aplicativo.

EVALUACIÓN

Cátedra: 70 %

La nota de cátedra está compuesta por 2 PEPs de igual ponderación.

P.E.P. 1:

- 25% Actividad grupal 1: Unidad 1 - Introducción
  - Entrega: 6 de octubre 2021
- 25% Control 1: Unidad 1 - Introducción
  - 21 al 22 de octubre 2021
- 25% Actividad grupal 2: Unidad 2 - Buenas prácticas, estándares y metodologías
  - Entrega: 10 de noviembre 2021
- 25% Control 2: Unidad 2 - Buenas prácticas, estándares y metodologías
  - 18 al 19 de noviembre 2021

P.E.P. 2:

- 25% Actividad grupal 3: Gobierno y gestión de la ciberseguridad
  - Entrega: 15 de diciembre 2021
- 25% Control 3: Gobierno y gestión de la ciberseguridad
  - 22 al 23 de diciembre 2021
- 25% Actividad grupal 4: Implementación y operación de la ciberseguridad
  - Entrega: 12 de enero 2022
- 25% Control 4: Implementación y operación de la ciberseguridad
  - 20 al 21 de enero 2022

Sobre los controles:

- Entra toda la materia vista en las unidades correspondientes y las presentaciones del resto de los grupos.
- Comienzan a las 15:20 del día indicado y finaliza al siguiente día a las 23:59. (ej. empieza el miércoles a las 15:20 y termina el jueves a las 23:59).
- Se tienen 3 horas disponibles para responder.
- Estos se diseñan para que sean respondidos en un máximo de 1 hora 30 minutos.
- Cualquier problema técnico al realizar el control debe ser informado a la brevedad al profesor al correo juan.iturbe@usach.cl y con evidencia de este (pantallazos y/o video).

Laboratorio: 30%

Se evalúan 3 experiencias, los cuales tienen igual ponderación.

Laboratorio 1 (25%):

- Entrega: 29 de octubre 2021

Laboratorio 2 (25%):

- Entrega: 3 de diciembre 2021

Laboratorio 3 (25%):

- Entrega: 7 de enero 2022

Importante:

- Se descontará 2 puntos por cada día de atraso.
- Cualquier copia será calificada con nota mínima.
- Cátedra y laboratorio tienen aprobación independiente.

BIBLIOGRAFÍA

Bibliografía Básica

Stallings W. (2019). Effective Cybersecurity: A guide to using Best Practices and Standards. Addison-Wesley.
NIST (2018). Framework for Improving Critical Infrastructure Cybersecurity
Bellovin, S. M. (2016). Thinking security: Stopping next year's hackers. Addison-Wesley.

Bibliografía Complementaria

Gibson, D. (2012). SSCP Systems Security Certified Practitioner: Exam guide: All in one. McGraw-Hill.
HARRIS, S. (2018). CISSP All in one exam guide. McGraw-Hill .
Walker, M. (2017). CEH Certified Ethical Hacker: All-in-one exam guide. McGraw-Hill.