ACTIVIDAD CURRICULAR DE FORMACIÓN

Facultad o Instituto	:	Ciencias de la Ingeniería
Carrera	:	Ingeniería Civil Informática

I. IDENTIFICACIÓN DE LA ACTIVIDAD CURRICULAR

Nombre	:	Seguridad de la Información							
Código	:	INF-525							
Semestre lectivo	:	X semestre							
Horas	:	Presencial:	54	Autónomas:	96	TOTAL:	150		
Créditos SCT	:	5 SCT							
Duración	:	Trimestral		Semestral:	x	Anual:			
Modalidad	:	Presencial:	x	Semi-presencial:		A Distancia:			
Área de Formación	:	Disciplinar:		General:		Profesional:	x		
						Práctica:			
Pre-requisito (Si los hubiese)	:	Redes Avanzadas							

II. DESCRIPCIÓN Y CARACTERIZACIÓN DE LA ACTIVIDAD CURRICULAR

La actividad curricular de Seguridad de la Información, se desarrolla en el décimo semestre del Plan de estudios de la Carrera de Ingeniería Civil Informática, pertenece al área curricular de Formación Profesional, al ciclo final y es de carácter teórico-práctico.

Las empresas soportan sus procesos de negocio con Tecnologías y Sistemas de Información y personal altamente calificado. En este contexto, la información constituye un recurso valioso que las empresas deben resguardar para el logro de sus objetivos. Sin embargo, en muchos casos es un recurso que no se valora adecuadamente por su intangibilidad y se expone a nuevas amenazas de seguridad, incluyendo fraudes informáticos, espionaje, sabotaje, vandalismo, fuego o inundaciones, virus, ataques de hackers y otros riesgos.

La seguridad de la información se apoya principalmente en tres conceptos, disponibilidad, integridad y confidencialidad, que para mantenerlos en un nivel aceptable es necesario dedicar recurso y normalmente presupuesto económico, lo que convierte al mantenimiento de la seguridad en una tarea de gestión.

Se espera que el estudiante aplique metodologías, técnicas, herramientas y formule planes de contingencias en la empresa digital en función de las normas de calidad y seguridad establecidas en estándares internacionales.

La metodología utilizada será con clases expositivas- participativa, una lectura previa por parte de los estudiantes que será guiada, aprendizaje basado en análisis de casos, proyectos y aprendizaje colaborativo.

La evaluación será por medio de prueba escrita y de ejecución, controles de lectura guiado, proyectos, informes, disertaciones o exposiciones temáticas

III. COMPETENCIAS DEL PERFIL DE EGRESO ASOCIADAS A LA ACTIVIDAD CURRICULAR.

III.1 COMPETENCIAS PROFESIONALES.

COMPETENCIA	SUBCOMPETENCIA
Diseñar soluciones tecnológicas que involucren la integración de software y hardware para la interconectividad entre sistemas informáticos.	Integrar sistemas complejos en arquitecturas procesamiento remoto.
Gestionar información utilizando herramientas tecnológicas en la toma de decisiones de la organización.	Implementar arquitecturas (Hardware y Software) que permitan el análisis de datos estratégicos en la toma de decisiones de la organización

III.2 COMPETENCIAS GENÉRICAS.

COMPETENCIA	SUBCOMPETENCIA
Demostrar coherencia ética entre sus postulados valóricos y sus acciones, respetando los derechos humanos y participando activamente en las organizaciones comunitarias, haciendo primar la responsabilidad social desde una perspectiva cristiana.	Juzgar sus actuaciones basándose en fuentes primarias del cristianismo y referentes espirituales.
Comunicar ideas, tanto en la lengua materna como en el idioma inglés, haciendo uso de las tecnologías de la información para desenvolverse en diversos escenarios, dando soluciones a diversas problemáticas de la especialidad.	Comunicarse de forma oral en inglés de acuerdo a lenguaje científico haciendo uso de las tecnologías de la información en contextos propios de su profesión.

IV. RESULTADOS DE APRENDIZAJE - APRENDIZAJE ESPERADO.

RESULTADOS DE APRENDIZAJES
1.-Identificar los principios básicos de la seguridad de la información en las empresas y en la redes de computadores, considerando los elementos de las políticas, planes y procedimientos de seguridad y la importancia del factor humano.
2.-Analizar las vulnerabilidades, amenazas y principales tipos de ataques a los sistemas y redes informáticas proponiendo planes de respuesta a incidentes y continuidad del negocio basadas en las buenas prácticas de estándares internacionales.
3.-Aplicar herramientas y técnicas de seguridad para cubrir aspectos relacionados con la identificación y autentificación de usuarios en los sistemas informáticos.
4.- Establecer sugerencias de control de seguridad, a partir de los hallazgos de realización de una auditoría de seguridad de la información en una empresa considerando estándares internacionales.

V. UNIDADES DE APRENDIZAJE Y EJES TEMÁTICOS

R. AP.	UNIDAD	EJE(S) TEMÁTICO(S)
1	Principios básicos de la seguridad de la información	Conceptos de seguridad de la información Políticas, planes y procedimientos de seguridad Sistema de gestión de la seguridad basado en estándares Importancia del factor humano en la seguridad
2	Análisis de riesgo de la seguridad de la información	Análisis de Riesgo Vulnerabilidades de los sistemas Informáticos Amenazas de la seguridad informática Virus y otros códigos dañinos Respuesta incidentes de seguridad y planes para la continuidad del negocio
3	Herramientas y técnicas de seguridad de la información	Autenticación, autorización y registro de usuarios Sistemas biométricos Fundamentos y aplicaciones de la criptografía Firma electrónica Herramientas para la seguridad en redes de computadores Desarrollo seguro de aplicaciones en internet
4	Auditoría de seguridad de la información	Aspectos legales de la seguridad informática Estándares internacionales de seguridad Metodología de la auditoría de seguridad Basado en estándares de referencia

VI. ESTRATEGIAS DE ENSEÑANZA-APRENDIZAJE

De acuerdo al modelo educativo de la Universidad Católica del Maule, la metodología de trabajo propuesta para el desarrollo de la actividad curricular, se basa en un enfoque más bien activo-participativo; esto implica entregar un rol protagónico al estudiante que es entendido como eje y centro de acción y quien a través de su participación activa y con las orientaciones y lineamientos que le entrega el docente va construyendo su propio aprendizaje. Para lograr este objetivo, las distintas clases consideraran una serie de estrategias metodológicas, previamente seleccionadas por el docente, tales como:

- Lectura guiada
- Metodología expositiva
- Aprendizaje basado en estudio de casos
- Metodología de proyectos
- Aprendizaje colaborativo.

VII. PROCEDIMIENTOS DE EVALUACION DE APRENDIZAJES.

RESULTADO DE APRENDIZAJES	INDICADORES	INSTRUMENTO Y/O TÉCNICA EVALUATIVA	PONDERACIÓN (%)
1	Distingue la diferencia entre integridad, confidencialidad y disponibilidad. Describe los elementos de una política de seguridad. Diferencia entre política y procedimientos. Da ejemplos de procedimientos de seguridad en un contexto específico. Describe un sistema de gestión de seguridad considerando las buenas prácticas recomendadas por estándares. Argumenta la importancia del factor humano en la seguridad de la información.	Prueba escrita / Pauta corrección	25%
2	Diferencia los conceptos de amenaza, vulnerabilidad y riesgo. Distingue la relación entre conceptos de amenaza, vulnerabilidad, riesgo, controles de seguridad preventivos, detectivos, correctivos. Examina activos de información a partir de un análisis de riesgos. Selecciona planes de respuestas a incidentes y continuidad del negocio en función del análisis de riesgos	Estudio de Caso / Rúbrica Control de lectura guiada / Pauta corrección	25%

3	Identifica herramientas y técnicas para la detección de incidentes de seguridad. Distingue protocolos y técnicas para el control de acceso, autentificación e identificación de usuarios. Emplea herramientas y/o técnicas para la identificación y autentificación de usuarios. Demuestra capacidad investigativa a partir de fuentes primarias formales. Se comunica de forma oral en inglés de acuerdo a lenguaje científico haciendo uso de las tecnologías de la información en contextos propios de su profesión	Informe tipo paper escrito / Rúbrica Presentación Oral/ Rúbrica	25%
4	Distingue las fases de una auditoría de seguridad. Planea una auditoría de seguridad considerando estándares de seguridad. Ejecuta una auditoría de seguridad. Propone sugerencias de control de seguridad en base a los hallazgos de la auditoría. Emite juicio basada en fuentes en fuentes primarias del cristianismo. Se comunica de forma oral de acuerdo a lenguaje científico haciendo uso de las tecnologías de la información	Prueba Escrita / Pauta Proyecto / Rúbrica	25%

VIII. RECURSOS DE INFRAESTRUCTURA

Sala de clases, data, internet, laboratorio computación, Servidor (hardware) para proyectos y software, LMS-UCM.

IX. RECURSOS BIBLIOGRÁFICOS

	Autor, Título, Editorial, Año de Edición	Biblioteca donde se encuentra	N° Libros Disponibles
BÁSICA OBLIGATORIA	- Gómez V., Álvaro, Enciclopedia de la Seguridad Informática, Alfaomega-Ra-Ma, 2011.	-Talca	-11
	-Piattini, Mario; Del Peso, Emilio, Del Peso, Mar. Auditoría de técnologías y sistemas de información, Rama, 2008.	-Talca	-4
	-De Pablos, Carmen; López, Jose; Martín-Romo, Santiago; Medina, Sonia, Organización y transformación de los sistemas de información en la empresa, Alfaomega, 2013.	-Talca	-0
	-Vladimirov, Andrew; Gavrilenko, Konstantin; Mikhailovsky, Andrei, Hacking wireless seguridad en redes inalámbricas, Anaya, 2004.	-Talca	-7
	- Howard, Michael, The security development lifecycle :SDL : a process for developing demonstrably more secure software, Washington : Microsoft, 2006.	-Talca	-8
	-Egan, Mark, The executive guide to information security : threats, challenges, and solutions. Addison-Wesley, 2005	-Talca	-4
COMPLEMENTARIA	- Lardent, Alberto , Sistemas de Información para la gestión empresaria, Procedimientos, seguridad y auditoría, Pearson Education, 2001.	-Talca	-14
	-Jean_Marc Royer. Seguridad en la informática de empresa. Riesgos, amenzas, prevención y soluciones. Eni edidiones, 2004	-	-
	-Bejtlicj, Richard, Tao of Network Security Monitoring, The: Beyond Intrusion Detection, Addison-Wesley Professional, 2004.		

	-Migga Kizza, Joseph, A guide To Computer Network Security, Springer, London, Reino Unido, 2009		

X. OTROS RECURSOS

Nombre Recurso	Tipo de Recurso
Astudillo, Karina. Hacking ético101. Cómo hackear profesionalmente en 21 días o menos.2013 http://SeguridadInformaticaFacil.com. Registro IEPI, certificado N° GYE-004179	e-book
Tutoriales configuración firewall	audiovisual