PROGRAMA DE CURSO
CIBERSEGURIDAD

A. Antecedentes generales del curso:

Departamento	Ciencias de la Computación							
Nombre del curso	Ciberseguridad		Código	CC5330	Créditos	6		
Nombre del curso en inglés	*Cybersecurity*							
Horas semanales	Docencia	3,0	Auxiliares	3,0	Trabajo personal	4,0		
Carácter del curso	Obligatorio	X		Electivo				
Ubicación del curso según malla	IX semestre							
Requisitos	CC4302: Sistemas Operativos, CC4401: Ingeniería de Software							

B. Propósito del curso:

El curso busca entregar a los y las estudiantes herramientas esenciales para diseñar e implementar sistemas y aplicaciones computacionales, considerando propiedades de ciberseguridad desde sus inicios, además de dar a conocer categorías de errores comunes de desarrollo, despliegue y configuración de los mismos con el objetivo de evitarlos. Al mismo tiempo, los y las estudiantes aprenderán cómo funcionan y se clasifican las amenazas de ciberseguridad más comunes, conocerán metodologías de modelamiento de riesgos tecnológicos y desarrollo seguro, y comprenderán el contexto legal, social y ético de la disciplina y su impacto en la privacidad y seguridad de las personas.

El curso tributa a las siguientes competencias específicas (CE) y genéricas (CG):

CE1: Analizar problemas computacionales, construir modelos, expresándolos en representaciones y lenguajes formales adecuados.

CE2: Analizar, diseñar y/o adoptar, algoritmos y estructuras de datos que cumplan con las garantías requeridas de correctitud y eficiencia.

CE4: Extraer información relevante, utilizando el proceso de descubrimiento de conocimiento de datos.

CE6: Desarrollar software en una amplia variedad de plataformas y lenguajes de programación.

CG1: Comunicación académica y profesional

Comunicar en español de forma estratégica, clara y eficaz, tanto en modalidad oral como escrita, puntos de vista, propuestas de proyectos y resultados de investigación fundamentados, en situaciones de comunicación compleja, en ambientes sociales, académicos y profesionales.

CG2: Comunicación en inglés

Leer y escuchar de manera comprensiva en inglés una variedad de textos e informaciones sobre temas concretos o abstractos, comunicando experiencias y opiniones, adecuándose a diferentes contextos y a las características de la audiencia.

CG3: Compromiso ético

Actuar de manera responsable y honesta, dando cuenta en forma crítica de sus propias acciones y sus consecuencias, en el marco del respeto hacia

	la dignidad de las personas y el cuidado del medio social, cultural y natural.

C. Resultados de aprendizaje (logros que cada estudiante demostrará al término del curso):

Competencias específicas	Resultados de aprendizaje
CE1	RA1: Propone un modelamiento de amenazas, acorde a una situación específica, comprendiendo conceptos básicos de ciberseguridad, manejando herramientas criptográficas e identificando principales riesgos y sus posibles mitigaciones.
CE2, CE6	RA2: Diseña e implementa sistemas y aplicaciones computacionales, considerando propiedades de ciberseguridad desde sus inicios y según contexto.
CE2	RA3: Analiza sistemas computacionales, identificando problemas de diseño e implementación relacionados con propiedades de ciberseguridad, para proponer mejoras.
CE1, CE2, CE4	RA4: Utiliza técnicas de seguridad defensiva e inteligencia de amenazas, siendo capaz de detectar intrusiones e identificar tipos de amenazas según los comportamientos asociados a ellas.
CE1	RA5: Identifica, a partir de ejemplos que se le presentan, en la regulación chilena e internacional las implicancias relacionadas con los delitos informáticos, políticas de ciberseguridad y políticas de protección de datos.
Competencias genéricas	**Resultados de aprendizaje**
CG1	RA6: Redacta documentos de modelamiento y análisis de amenazas, reportes de incidentes de ciberseguridad y/o informes de laboratorio, considerando claridad y coherencia en el escrito.
CG2	RA7: Utiliza bibliografía y terminología en inglés, referenciándolas cuando corresponda a fin de fundamentar sus decisiones y análisis sobre temas en ciberseguridad en casos que se le presentan.
CG3	RA8: Plantea su punto de vista, de forma clara y coherente, sobre decisiones de diseño, uso de herramientas de ciberseguridad y su impacto en la vida de las personas, distinguiendo entre actividades éticas y no éticas o ilegales.

D. Unidades temáticas:

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
1	RA1, RA6	Fundamentos de Ciberseguridad	2 semanas
Contenidos		**Indicador de logro**	
1.1. Definiciones y conceptos fundamentales de ciberseguridad. 1.2. Modelos de evaluación de riesgo. 1.3. Propiedades de ciberseguridad: Confidencialidad, integridad y disponibilidad. 1.4. Principios básicos de ciberseguridad 1.5. Autentificación, autorización y control de acceso.		El/la estudiante: 1. Identifica principios básicos y propiedades de ciberseguridad en sistemas, tales como amenaza, riesgo y mitigaciones. 2. Desarrolla y justifica modelos de evaluación de riesgo según los casos presentados. 3. Reconoce la necesidad de distintos modelos de autenticación, autorización y control de acceso en sistemas según las propiedades de ciberseguridad requeridas. 4. Produce textos relacionados con documentos de modelamiento y análisis de amenazas, considerando claridad y coherencia en su escrito.	
Bibliografía de la unidad		[1] Cap. 1, 2, 3, 6, 17, [2] Cap. 1, 3, [3] Cap. 1, 2, 3, 7, [c]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
2	RA1, RA2	Criptografía	2.5 semanas
Contenidos		**Indicador de logro**	
2.1. Criptografía de clave privada. 2.2. Criptografía de clave pública. 2.3. Acuerdo de claves y TLS. 2.4. Desafíos y criptografía post cuántica. 2.5. Aplicaciones (mensajería con seguridad punto a punto, blockchain, entre otros de similares características).		El/la estudiante: 1. Reconoce las propiedades específicas de algoritmos criptográficos de clave pública y privada y sus aplicaciones. 2. Selecciona los usos correctos de algoritmos criptográficos de clave pública y privada. 3. Selecciona los usos correctos de algoritmos de acuerdo con claves y TLS. 4. Identifica el impacto de la computación cuántica en algoritmos de criptografía moderna y reconoce estrategias para mitigarlo. 5. Utiliza librerías criptográficas para obtener propiedades de ciberseguridad deseadas en diseño de software.	
Bibliografía de la unidad		[1] Cap. 5, 20, [2] Cap. 2, 4, 8, [3] Cap. 6, 8, [4] Partes I, II, III, IV, [a], [e]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
3	RA3, RA7	Seguridad de Bajo Nivel y Seguridad de Redes	4 semanas

Contenidos	Indicador de logro
3.1. Definiciones de vulnerabilidades y debilidades. 3.2. Seguridad de bajo nivel (buffer overflow, control de flujo, y manejo de memoria). 3.3. Seguridad en sistemas operativos de escritorio. 3.4. Seguridad en sistemas operativos móviles. 3.5. Seguridad de red, conceptos y ataques básicos. 3.6. Mecanismos y estrategias para defensa de red (Firewalls/EDRs, Anti-Denegación de servicio, Virtual Private Networks (VPNs), y Zero Trust, entre otros). 3.7. Seguridad del Sistemas de nombres de dominio (DNS).	El/la estudiante: 1. Diferencia vulnerabilidades de otros tipos de errores de programación. 2. Clasifica vulnerabilidades en distintas categorías de debilidades. 3. Identifica las causas y el impacto de vulnerabilidades de bajo nivel. 4. Aplica los conceptos de control de acceso y permisos de sistemas operativos de escritorio y móviles, en casos que se le presentan. 5. Propone estrategias para evitar o mitigar las vulnerabilidades identificadas. 6. Aplica los conceptos de aislamiento en sistemas operativos de escritorio y móviles, en casos que se le presentan. 7. Aplica mecanismos de seguridad básicos en redes y sistemas operativos. 8. Utiliza bibliografía y terminología en inglés, sobre seguridad de redes, referenciándolas cuando corresponda, en los casos que se le presentan.
Bibliografía de la unidad	[1] Cap. 6, 21, [2] Cap. 5, 6, 10,11 [3] Cap. 5,9,10,11 [b]

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
4	RA3, RA6, RA7	Seguridad de Aplicaciones	1.5 semanas
Contenidos		**Indicador de logro**	
4.1. Modelo de seguridad web y Vulnerabilidades en aplicaciones web. 4.2 Seguridad en otras tecnologías (Inteligencia Artificial, Internet de las Cosas (IoT), Tecnologías Operacionales (OT), entre otras). 4.3 Etapas, componentes y estructura en informes de vulnerabilidades.		El/la estudiante: 1. Reconoce las restricciones que los navegadores exigen como parte del modelo de seguridad. 2. Analiza vulnerabilidades y debilidades conocidas y frecuentes en aplicaciones web. 3. Identifica vulnerabilidades y debilidades conocidas en tecnologías tales como AI, IoT, y OT entre otras. 4. Propone estrategias para evitar o mitigar las vulnerabilidades identificadas. 5. Utiliza bibliografía y terminología en inglés de fuentes confiables sobre vulnerabilidades y debilidades, referenciándolas según corresponda. 6. Redacta informes donde analiza vulnerabilidades y debilidades y propone estrategias para mitigar dichas vulnerabilidades, considerando claridad y coherencia en sus ideas.	
Bibliografía de la unidad		[1] Cap. 25.3, [2] Cap. 6, 9, [d]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
5	RA2, RA3	Ingeniería de Seguridad y Desarrollo seguro	1.5 semanas
Contenidos		**Indicador de logro**	
5.1 Seguridad por diseño y seguridad por defecto. 5.2. Manejo de vulnerabilidades y dependencias. 5.3. Monitoreo y Observabilidad 5.4. Herramientas para obtener mejores garantías de seguridad de aplicaciones: Análisis estático y dinámico, fuzzing y uso de lenguajes con seguridad de tipos.		El/la estudiante: 1. Aplica conceptos básicos de ingeniería de seguridad y considera su impacto en las propiedades de seguridad de un sistema o aplicación, en laboratorios en los que trabajan. 2. Aplica los pasos de un proceso de diseño y desarrollo seguro en sistemas y aplicaciones, argumentando brevemente sus decisiones. 3. Aplica herramientas de validación de desarrollo seguro para identificar debilidades en laboratorios en los que trabaja. 4. Identifica lenguajes con seguridad de tipos (type soundness), considerando sus ventajas en términos de seguridad.	
Bibliografía de la unidad		[1] Cap. 27, 28 [2] Cap. 8, [3] Cap. 11, 12, 13, 14, 15, 16, [5] Cap 1, [a],[c]	

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
6	RA4, RA6, RA7	Seguridad Defensiva e Inteligencia de Amenazas	2 semanas

Contenidos	Indicador de logro
6.1. Definiciones de Malware. 6.2. Definiciones de Inteligencia de Amenazas. 6.3. Amenazas Persistentes Avanzadas (APT). 6.4. Incidentes de Ciberseguridad.	El/la estudiante: 1. Identifica distintos tipos de malware, según sus características de comportamiento. 2. Analiza casos de estudio, aplicando técnicas básicas de seguridad defensiva e inteligencia de amenazas. 3. Analiza eventos de ciberseguridad determinando los pasos a seguir para dar respuesta al incidente. 4. Redacta un informe sobre seguridad defensiva e inteligencia de amenazas, considerando claridad y coherencia en su escrito. 5. Utiliza bibliografía y terminología en inglés sobre seguridad defensiva e inteligencia de amenazas, referenciándolas cuando corresponda.
Bibliografía de la unidad	[1] Cap. 21, [2] Cap. 7

Número	RA al que tributa	Nombre de la unidad	Duración en semanas
7	RA5, RA8	Gobernanza, Sociedad y Ética de la profesión	1.5 semanas

Contenidos	Indicador de logro
7.1. Hacking ético y reporte responsable de vulnerabilidades. 7.2. Leyes de delito informático, ciberseguridad y protección de datos. 7.3. Vigilancia y monitoreo. 7.4. Piratería, restricciones legales a la criptografía y censura.	El/la estudiante: 1. Utiliza las etapas del reporte responsable de vulnerabilidades, comprendiendo cómo se relaciona con la legislación chilena actual, a partir del análisis de casos concretos que se le presenten. 2. Reconoce las primitivas tecnológicas que habilitan los sistemas de vigilancia y monitoreo, antipiratería y censura, además de las medidas que empresas y gobiernos han tomado para evitar su elusión, así como el impacto que estas tienen en las propiedades de ciberseguridad y el manejo de datos. 3. Plantea su punto de vista, de forma clara y coherente, sobre decisiones de diseño, uso de herramientas de ciberseguridad y su impacto en la vida de las personas, distinguiendo entre actividades éticas y no éticas o ilegales.
Bibliografía de la unidad	[1] Cap. 26, [6], [7]

E. Estrategias de enseñanza-aprendizaje:

El curso considera las siguientes estrategias:

- **Clase expositiva** dos veces a la semana, a cargo del profesor o profesora de cátedra. Complementariamente, habrá *clases prácticas*, a cargo del profesor o profesora auxiliar.
- **Casos de estudio**, durante el bloque de auxiliar, a cargo del profesor o profesora auxiliar.
- **Laboratorios**, durante el bloque de auxiliar, a cargo del profesor o profesora auxiliar.

F. Estrategias de evaluación:

Al inicio de cada semestre, el académico o académica informará a los y las estudiantes sobre los tipos de evaluaciones, así como las ponderaciones correspondientes.

La evaluación se hará vía **casos de estudio**, durante el bloque de auxiliar, al menos 4 veces durante el semestre, y **Laboratorios**, durante el bloque de auxiliar, al menos 4 veces durante el semestre.

Tipo de evaluación	RA asociado a la evaluación	Ponderaciones
• Laboratorios (evaluaciones de carácter práctico, con su respectivo informe y código).	Evalúa RA1, RA2, RA3, RA4, RA6, RA7, RA8	50%
• Casos de estudio con sus respectivos reportes.	Evalúa RA1, RA2, RA3, RA4, RA5, RA6, RA7, RA8	50%

Cualquier modificación en las evaluaciones o ponderaciones correspondientes serán informadas al inicio del curso, considerando el plan de trabajo propuesto.

G. Recursos bibliográficos:

Bibliografía obligatoria:

[1] “Security Engineering”, 3rd edition, Ross Anderson. Willey, 2020.
[2] “Computer Security and the Internet”, Paul C. van Oorschot. Springer, 2020.
[3] “Thinking Security: Stopping Next Year’s Hackers”, Steven M. Bellovin. Addison-Wesley, 2016.
[4] “Serious Cryptography: A Practical Introduction to Modern Encryption”, 2nd edition, Jean-Philippe Aumasson. No Starch Press, 2024.
[5] “Secure by Design”, Johnsson, Deogun, Sawano. Manning Press, 2019.
[6] Ley Marco de Ciberseguridad (No. 21.663), Biblioteca del Congreso Nacional.
[7] Ley de Delito Informático (No. 21.459), Biblioteca del Congreso Nacional.

Bibliografía complementaria:

[a] “Practical Cryptography in Python”, Nielsen, Monson. Apress, 2019.
[b] “Attacking Network Protocols”, Forshaw. No Starch Press, 2017.
[c] “Ten laws of security”, Eric Diehl. Springer, 2016.
[d] “The Shellcoder 's Handbook”, Anley, Heasman, Lindner, Richarte. Willey, 2007.
[e] “Cryptography Engineering”, Ferguson, Schneier & Kohno. Wiley, 2010.

H. Datos generales sobre elaboración y vigencia del programa de curso:

Vigencia desde:	Primavera 2025
Elaborado por:	Alejandro Hevia y Eduardo Riveros Roca
Validado por:	Académico/a del área: Jocelyn Simmonds, Jefa Docente CTD mes de mayo 2025
Revisado por:	Área de Gestión Curricular