PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

PROGRAMA DEL CURSO LA CIBERSEGURIDAD Y SU IMPACTO EN LA SEGURIDAD INTERNACIONAL

CURSO	:	LA CIBERSEGURIDAD Y SU IMPACTO EN LA SEGURIDAD INTERNACIONAL
SIGLA	:	ICP-5470
CRÉDITOS	:	10
PROFESOR	:	RICARDO NEEB CANTARERO
MÓDULOS	:	1
SESIONES	:	15 SESIONES de 2 HRS. PEDAGÓGICAS C/U (70 min)
HORARIO	:	Martes de 20:10 – 21:20 hrs.
INICIO	:	Martes 11 de marzo
FINALIZACIÓN	:	Martes 24 de junio

IMPORTANTE: Durante este semestre, se efectuarán 3 clases presenciales en el campus San Joaquín, en el horario del Curso, los días:

Martes 25 de marzo de 20:10 a 21:20 hrs.
Martes 6 de mayo de 20:10 a 21:20 hrs.
Martes 24 de junio de 20:10 a 21:20 hrs.

La sala se definirá en su momento.

I. DESCRIPCIÓN DEL CURSO

El desarrollo de las tecnologías de la información y operación, redes de comunicaciones y, en general, del ciberespacio, ha traído una innumerable cantidad de beneficios, pero también nuevas problemáticas en materias de seguridad.

La evolución que han tenido los ataques informáticos ha implicado que este problema ya no sea algo propio de la esfera de la privado y, hoy en día, pase a ser un problema que abarca la seguridad internacional y las relaciones entre los estados.

Este curso está orientado a discutir las temáticas de la ciberseguridad, con el fin de dar un entendimiento más amplio del impacto de esta disciplina en la sociedad de hoy.

II. RESULTADOS DE APRENDIZAJE

a. Entender las principales definiciones y conceptos involucrados en la ciberseguridad y el ciberespacio, así como también, de los elementos que lo componen.

b. Conocer las principales características de cómo operan las redes de comunicaciones y el ciberespacio.

c. Aplicar los conocimientos para identificar las principales amenazas existentes en el ciberespacio.

d. Analizar el impacto en la seguridad de las amenazas y entender su contexto nacional e internacional.

e. Entender la importancia de las políticas de ciberseguridad al interior de las organizaciones.

f. Interpretar los cambios tecnológicos sus las aplicaciones e impacto para la seguridad de los Estados.

g. Analizar los aspectos esenciales del gobierno de la ciberseguridad.

III. CONTENIDOS

1. Presentación del curso. La tecnología en las RRII, introducción a los conceptos de: tecnologías disruptivas, redes de comunicaciones, ciberespacio, seguridad de la información y ciberseguridad.

1.1. Introducción al curso.

1.2. La tecnología en las RRII.

1.3. Concepto de tecnologías disruptivas y su impacto en las RRII.

1.4. Introducción a las redes de comunicaciones, el ciberespacio, sus características, componentes, funciones y gobernanza.

1.5. La seguridad de la información y la ciberseguridad, características y diferencias.

Bibliografía:

Mallik, Amitav. "The Role of Technology in International Affairs". IDSA, Pentagon Press, 2016, pág. 3-66.

Daniel T. Kuehl. "From Cyberspace to Cyberpower: Defining the Problem" in "Cyberpower and National Security", NDU Press, 2009, cap. 2.

Illica, alejandra. "El Debate sobre los Sistemas de Armas Autónomos Letales: Perspectivas en el Sistema Internacional". Estudios del Centro de Estudios estratégicos de la Academia de guerra del Ejército. https://www.ceeag.cl/wp-content/uploads/2023/06/EC-AI-Sistemas-de-armas-autonomos-letales.pdf.

2. Introducción al análisis de riesgos, las amenazas en la red y su tipología, el concepto de infraestructuras críticas y los sistemas SCADA, los dispositivos móviles y la IoT.

2.1. Análisis de riesgos.

2.2. Tipología de las amenazas en el ciber espacio, sus características y medidas de mitigación.

2.3. Las amenazas a las infraestructuras críticas y a los sistemas de control industrial.

2.4. La Internet de las Cosas (IoT) y los peligros de la automatización.

Bibliografía: Israel and the Cyber Threat. Charles D. Freilich, Matthew S. Cohen, and Gabi Siboni, Oxford University Press. Oxford University Press 2023. DOI: 10.1093/ oso/ 9780197677711.003.0002, pág. 23-39

CCN-CERT. "Ciberamenazas y Tendencias", Edición 2023. Pág 8-66. https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html

Di Pietro, Roberto et al. "New Dimensions in Information Warfare", Springer, año 2021, pág. 157-197. https://doi.org/10.1007/978-3-030-60618-3

3. El impacto del ciber espacio en las relaciones internacionales, casos de estudio.

3.1. Concepto de ciberinteligencia.

3.2. Mini taller de ciberinteligencia.

3.3. Casos de estudio de ciberataques.

3.4. Casos de estudio de guerra de información en el ciberespacio.

Bibliografía: Quentin E. Hodgson, et al. "Fighting Shadows in the Dark". RAND 2019.

P.J. Blount. "How Cyberspace Changes International Conflict", https://www.e-ir.info/2019/12/08/how-cyberspace-changes-international-conflict/, 2019.

Roy, Kaushik. "A Global History of Warfare and Technology", Springer, Ia Ed., año 2022, pág. 163-175. https://doi.org/10.1007/978-981-19-3478-0

4. El gobierno de la ciberseguridad y las políticas sectoriales. Casos de estudio.

4.1. Qué es el gobierno de la ciberseguridad.

4.2. Las políticas de protección de las infraestructuras críticas y de ciberseguridad. Casos de Estudio: Israel, La Unión Europea, España, EEUU y Chile.

IV. METODOLOGÍA

- Clases expositivas de teoría y casos de estudio.
- Charlas de expertos en ciberseguridad.
- Lectura y discusión de textos.
- Trabajo de investigación y análisis.

V. EVALUACIÓN

La evaluación del curso consiste en:

A. Una disertación sobre la materia vista en clases. Este trabajo es grupal. Los grupos deberán escoger una temática de la materia y exponerla en no más de 25 minutos. La ponderación de la disertación es de 35%.

Fechas para la disertación: martes 20 y 27 de mayo.

B. Un trabajo de investigación, relacionado con un tema de actualidad de los tópicos vistos en el curso. La ponderación del trabajo final es de 65% y se distribuirá de la siguiente forma:

1. **Iª Etapa**
   Fecha: martes 15 de abril
   Contenido: tema a investigar, descripción, hipótesis, objetivos y bibliografía mínima a usar.
   Ponderación: 25% de la nota del trabajo
2. **IIª Etapa**
   Fecha: martes 13 de mayo
   Contenido: correcciones al feedback del profesor y resultados a la fecha
   Ponderación: 25% de la nota del trabajo
3. **IIIª Etapa y Entrega final**
   Fecha: viernes 27 de junio
   Contenido: trabajo completo
   Ponderación: 50% de la nota del trabajo

El trabajo final debe tener un mínimo 6500 palabras, sin incluir anexos.
El formato exigido es el siguiente.

Letra Arial 11.
Interlineado de 1 cm.
Margen izquierdo y derecho de 3 cm
Márgenes superior e inferior de 2,5 cm.
El trabajo debe ser hecho en Word y su archivo deberá ser nombrado de la siguiente manera:

Trabajo_Ciber2024_Nombre_Apellido.doc

Debe tener una tapa e índice, los que no serán considerados en el conteo de las palabras.
Las citas deben estar de acuerdo a las exigencias de la Universidad.

C. La nota final se calculará de la siguiente manera:
NF= Disertación*0,35+Trabajo final*0,65

D. Asistencia: se exige un mínimo de 75% de asistencia para aprobar el curso.

VI. INTEGRIDAD ACADÉMICA

Este curso reconoce la Integridad Académica como un pilar fundamental del proceso formativo de estudiantes, al centro de la construcción de una cultura de respeto e integridad en la UC. Los valores de la Integridad Académica son la honestidad, veracidad, confianza, justicia, respeto y responsabilidad. La copia, el plagio (hacer pasar el trabajo y las ideas de otros(as) como propias, o no citar o hacer referencia adecuada a las fuentes usadas) y el auto-plagio (entregar un trabajo propio, o partes de él, que ya ha sido presentado en otro curso o instancia) no son tolerables bajo ninguna circunstancia, así como tampoco otras faltas a la integridad académica, según se expresa en el Código de Honor UC (https://www.uc.cl/codigo-de-honor/).

Las faltas a la integridad académica serán calificadas con la nota mínima (1,0) e informadas a la subdirección de la unidad académica del curso y del/a estudiante, las que serán evaluadas por el Comité de Integridad Académica de la Facultad correspondiente.

Para mayor información sobre Integridad Académica UC y el proceso de gestión de faltas: https://integridadacademica.uc.cl/.

Las normas para citar todo tipo de fuentes, incluyendo páginas de internet, se encuentran claramente explicadas en la página web: http://guiastematicas.bibliotecas.uc.cl/normasapa. Se recomienda además revisar la siguiente página para entender qué es el plagio y como evitarlo: http://guiastematicas.bibliotecas.uc.cl/plagio.

Reglamento del alumno de magister, artículo 27: "Los alumnos deberán tener especial respeto por las normas relativas a la honestidad académica vigentes al interior de la Universidad. Se considerarán infracciones a la honestidad académica las siguientes: a) Cometer fraude en exámenes, controles u otras actividades académicas; b) Adulterar cualquier documento oficial, documento de asistencias, correcciones de pruebas o trabajos de investigación; c) Plagiar u ocultar intencionalmente el origen de la información en investigaciones y trabajos en general, y d) Cualquier otro acto u omisión que sea calificado fundadamente como infracción académica por una Facultad o Unidad Académica y/o el Secretario General. Todo acto contrario a la honestidad académica realizado durante el desarrollo, presentación o entrega de una actividad académica sujeta a evaluación, será sancionado con la suspensión inmediata de la actividad y con la aplicación de la nota mínima."

VII. BIBLIOGRAFÍA

Kramer, Franklin (Editor), "Cyberpower and National Security", Potomac Books, 1 Edición, año 2009.

Ozkaya, Erdal; Diogenes, Yuri. "Cybersecurity-Attack and Defense Strategies", Packt Publishing, 1 Edición, año 2018.

Andres, Jason; Winterfeld, Steve, "Cyber Warfare", Syngress, 2 Edición, año 2013.

Harrison, Richard. "Cyber Insecurity: Navigating the Perils of the Next Information Age", Rowman & Littlefield Publishers, 1 Edición, año 2016.

Jarpa, Pedro, "De la Ciberseguridad a la Ciberguerra", Editorial academia Politécnica Militar, 1 Edición, año 2016.

Nye, Joseph (Jr), "Cyber Power", Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.

Israel National Ciber Authority. "Cyber Defense Methodology for an Organization", June 2017.

Instituto Español de Estudios Estratégicos. "Ciberseguridad: La Cooperación Público Privada", Cuaderno de Estrategia N°185, 2017.

Gallager, Nancy. "Classifying Ciber Events: A Proposed Taxonomy", Center for International and Security Studies, Univ. Maryland, 2018.

Wright, Nicolas. "How Artificial Intelligence Will Reshape the Global Order", Foreign Affairs, Julio 2018.

Goldstein, Guy-Phillipe, "Cyber Weapons and International Stability", Military and Strategic Affairs, Vol 5, N°2,

Daniel T. Kuehl. "From Cyberspace to Cyberpower: Defining the Problem" in "Cyberpower and National Security", NDU Press, 2009

Dimauro, Carmelo and Hartung Thomas. "A structured approach to identifying European critical infrastructures", International Journal of Critical Infrastructures · June 2010.

CCN-CERT. "Ciberamenazas y Tendencias", Edición 2020.

Daniel Hughes and Andrew M. Colarik. "Predicting the Proliferation of Cyber Weapons into Small States", JFQ, 2016.

Gill, Singh, "Artificial Intelligence and International Security: The Long view", Ethics & International Affairs, Vol 33, N° 2, 2019, pp. 169-179.

Boden, Margaret edit. "Filosofía de la Inteligencia Artificial", 2da Edición, Fondo de Cultura Económica, 1994.