Universidad del Desarrollo
Universidad de Excelencia

Programa de Asignatura
Ciberseguridad

A. Antecedentes Generales

1. **Unidad Académica**	VICERRECTORÍA DE PREGRADO					
2. **Carrera**	TRACK RESPONSABILIDAD PÚBLICA					
3. **Código**	TRR291					
4. **Ubicación en la malla**	Bachillerato/Licenciatura.					
5. **Créditos**	8					
6. **Tipo de asignatura**	Obligatorio		Electivo	x	Optativo	
7. **Duración**	Bimestral		Semestral	x	Anual	
8. **Módulos semanales**	Clases Teóricas	2	Clases Prácticas		Ayudantía	
9. **Horas académicas**	Clases	68	Ayudantía	0		
10. **Pre-requisito**	No tiene					

B. Aporte al Perfil de Egreso

Teniendo en consideración los cambios en el entorno laboral, principalmente aquellos que tienen que ver con el ambiente global, la diversidad y la mirada interdisciplinaria, la Universidad del Desarrollo se ha propuesto formar a sus estudiantes a través de un Proyecto Educativo que, junto con entregar una sólida formación disciplinar y en coherencia con las necesidades del mundo del trabajo, desarrolle en los estudiantes nuevas habilidades, competencias y conocimientos que les permitan enfrentar con éxito el escenario profesional que les espera al término de su formación de pregrado. En este contexto surgen los cursos Track o vías temáticas cuyo objetivo es contribuir, a través de la formación extradisciplinar del estudiante, que éste participe de experiencias de aprendizaje más enriquecedoras que los preparen para un mundo laboral cambiante.

El curso "Ciberseguridad: conflictos y amenazas" forma parte del Track de Responsabilidad Pública y tributa a las competencias genéricas de Visión Analítica y Visión Global y tiene por objetivo entregar un panorama amplio del rol de las tecnologías de la información (TIC) como ámbitos de conflictos sociales y políticos. Se espera que el estudiante reflexione y analice el uso de las TIC y su impacto en el mundo no virtual, ya sea desde el reconocimiento de cambios de paradigma en diversas esferas sociales como también el prever situaciones de riesgo en la actualidad y en el futuro. De esta manera acompaña la capacidad técnica que pueda desarrollar el estudiante con respecto a las tecnologías de información (desde las bases de datos de un médico hasta el desarrollo de un producto o servicio innovador que utiliza internet en este mismo o en su logística) con una visión desde las ciencias sociales para un mejor entendimiento de sus acciones y la de otros.

C. Competencias y Resultados de Aprendizaje Generales que desarrolla la asignatura

Competencias Genéricas	Resultados de Aprendizaje Generales
Responsabilidad pública.	-Aplica el estudio multidisciplinario de las TIC para solución de problemas en contextos sociales. -Valora la importancia de las tecnologías como variables que afectan paradigmas sociales. -Analiza las consecuencias positivas y negativas del desarrollo tecnológico en nuestra sociedad.
Visión Global. *Visión Analítica.*	

D. Unidades de Contenidos y Resultados de Aprendizaje

Unidades de Contenidos	Competencia	Resultados de Aprendizaje
Unidad I: Introducción a las Relaciones Internacionales (RRII). • conceptos, teorías y paradigmas de Seguridad Internacional como subdisciplina mínima de las RR. II. para el desarrollo de las temáticas centrales del curso.	**Responsabilidad pública.**	• Identifica componentes de un problema en el ciberespacio; como desagregarlos y reorganizarlos racionalmente. • Identifica las diferentes aristas, de las TIC, y sus efectos sociales. • Analiza la evolución de las TIC y su importancia en redes sociales modernas. • Aplica contenidos de investigaciones, que dan solución al dilema de ciberseguridad en la sociedad.
Unidad II: Tecnologías de Información: • Definición, análisis, evolución y desarrollo de las TIC masivas, desde la imprenta hasta las redes sociales modernas.	**Visión Analítica.**	
Unidad III: Concepto Ciber. • Descripción de los conceptos y neologismos que aparecen a raíz de la masificación, desarrollo y explotación de Internet y ciberespacio como medio de comunicación masiva y otras actividades humanas. • Ciberespacio; Ciberseguridad; Ciberdefensa; Cibercriminal y delincuencia. • Hacktivismo; Privacidad y protección de datos; Información, ¿bien público o bien privado?.	**Visión Global.**	

E. Estrategias de Enseñanza

La estrategia metodológica será la de investigación y la de análisis: ya que la naturaleza de la temática a trabajar (contingente en los últimos años y para el futuro) requiere que el alumno desarrolle este conocimiento de la mano con una mentalidad exploratoria y de resolución de problemas sociales.

Análisis conceptual: Es principalmente necesario en el tema propio del curso en tanto corresponde en gran medida a neologismos que poco acuerdo académico existe hoy en día. El trabajar en el ámbito de la descripción y conceptualización de los fenómenos es esencial.

El estudio crítico de prensa y desarrollo de opinión pública: Es fundamental dentro de la estrategia de enseñanza en tanto el estudiante debe comprender los procesos de securización (cuándo algo debe ser protegido y asegurado) como del tratamiento, organización y validación de veracidad de la información, principalmente por que el espacio de análisis es fundamentalmente el flujo de información.

El estudio de casos: Como aplicación del razonamiento y estudio conceptual resulta necesario para que los alumnos pongan en práctica su capacidad de análisis y de interpretación de los fenómenos, además de consciencia del mapa global en los que se insertan cada vez que utilizan las tecnologías de la información.

F. Estrategias de Evaluación

La estrategia de evaluación corresponderá al desarrollo de trabajos de investigación, aprendiendo a desarrollar el método científico en la exploración de las ciencias sociales, y la capacidad de analizar y mapear problemáticas y sus soluciones con sus respectivos costos y beneficios.

Certamen 1.
Certamen 2.
Examen.

Requisito de Asistencia:
El curso contempla un requisito de asistencia obligatoria, lo que implica que se permitirá para todos los alumnos un máximo de 6 inasistencias, contabilizadas desde la finalización del proceso de Elimina-Agrega, que se señala en el calendario académico respectivo. El alumno que no cumpla con este requisito no tendrá derecho a rendir el Examen Final, según lo contempla el Reglamento Académico del Alumno Regular. En el caso de los alumnos que cursen la carrera de Derecho su inasistencia máxima será de 4 clases finalizado el proceso de Elimina – Agrega hasta la fecha establecida en el documento “Procedimiento de Justificaciones de Inasistencia en Cursos Track para alumnos de Derecho”.

G. Recursos de Aprendizaje.

Bibliografía Obligatoria:

- Ferguson, N. (2018). La Plaza y la Torre. El papel oculto de las redes en la historia: de los masones a Facebook. España, Debate.

- Turzi, M. L. (2017). Todo lo que necesitás saber sobre el (des) orden mundial. Paidos Argentina.
- Torres, Manuel R. (2013). Ciberguerra. En Jordán, Javier (ed.): Manual de Estudios Estratégicos y Seguridad Internacional. Madrid: Plaza y Valdés Editores. p. 333

Bibliografía complementaria:

- Shirky, c. (2011) 'The Political Power of Social Media', Foreign Affairs, 90(1): 28-41
- Ferguson, N. (2018). La Plaza y la Torre. El papel oculto de las redes en la historia: de los masones a Facebook. España, Debate.
- Keohane, R., & Nye, J. (1998). Power and Interdependence in the Information Age. Foreign Affairs, 77(5), 81-94.
- McEvoy Manjikian, M. (2010) From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. International Studies Quarterly, 54(2): pp. 381-401.
- Collins, Allan. (2010) Contemporary Security Studies. Oxford University Press.
- Ibañez Ferrándiz, I. (2014) Los cuatro jinetes del terrorismo internacional. FAES, Cuadernos de Pensamiento Político, (42):pp.67-83.
- Jarvis, Lee, Y Macdonald, S. (2014) Locating Cyberterrorism How Terrorism Researchers Use and View the Cyber Lexicon. Terrorism Research Institute, Perspectives on Terrorism, 2014, 8(2):pp.52-65. Disponible en: www.jstor.org/stable/26297136
- McDougal, T. (2015). Establishing Russia's Responsibility for Cyber-Crime Based on Its Hacker Culture. Int'l L. & Mgmt. Rev., 11, 55.
- Clarke, Richard A., y Knake, Robert K. (2011). Cyberwar, The next threat to National Security and what to do about it. Nueva York: HarperCollins Publishers. p. 70
- TeleGeography (2018). Submarine Cable Map.
- Clark, David (2010). Characterizing cyberspace: past, present and future. Office of Naval Research.
- Jervis, R. (2017). Perception and Misperception in International Politics: New Edition. Princeton University Press.