



UBA FCE

Escuela de Estudios de Posgrado

CURSO DE POSGRADO

DISEÑO DE ESCENARIOS Y ESTRATEGIAS

PARA LA CIBERDEFENSA Y CIBERSEGURIDAD DE LAS ORGANIZACIONES

CONTENIDOS MÍNIMOS

- **De la metafísica a la cibernética**

Evolución en la concepción del rol de la tecnología en la sociedad, los modelos organizacionales y el paradigma cibernético. Conflicto de tiempos y lógicas: El tiempo analógico y secuencial del cambio versus el tiempo del cambio digital exponencial. ¿Qué tan preparado me siento? Aspectos centrales del contexto VICA y de la dinámica de cambio global. Incidencia de las tecnologías disruptivas. Cómo pensamos los ciudadanos y ejecutivos nuestra vida y nuestro trabajo. Cómo piensan sobre nuestra vida y trabajo quienes delinquen informáticamente. El abordaje sistémico de los riesgos y el abordaje integral de los riesgos cibernéticos. La emergencia de la gestión de riesgos como una lógica de supervivencia organizacional y empresaria. Mapeo de riesgos contextuales y organizacionales, aplicando dos herramientas específicas para cada nivel de análisis. ¿Qué tan preparada está mi organización?

- **Diagnóstico, Teoría y Práctica de la estrategia**

Principios del pensamiento estratégico: racionalidad interdependiente, dialéctica de voluntades, conceptos y opciones estratégicas. Teoría del conflicto, intereses, actores, trama, escenarios, opciones estratégicas. Práctica de la estrategia: inteligencia, análisis de la situación. Evolución, evaluación, apreciación, resolución, supervisión. Teoría de Juegos aplicadas al diagnóstico de escenarios agresiones, intromisiones, y delitos cometidos en el dominio cibernético.

- **Planeamiento de escenarios y estrategias**

Planeamiento estratégico en contextos competitivos (hipótesis de conflicto cibernéticos). Planeamiento estratégico en contextos cooperativos (capacidades y competencias cibernéticas). Planeamiento estratégico en contextos socio cognitivos y sistémicos (matriz racional y emocional). Planeamiento estratégico en contextos asimétricos y entornos VICA (organizaciones ágiles).

- **Ejecución y Gestión Estratégica**

Estrategizar como proceso cibernético y de auto aprendizaje. Evolución de los enfoques estratégicos y situacionales acordes a las necesidades organizacionales. Cómo introducir la consideración de los riesgos cibernéticos y la idea de transformación organizacional en el planeamiento y la gestión. Los componentes de una estrategia de cambio organizacional apoyada en la transformación digital y cultural. Aplicación a mi propia realidad. Implementación y evaluación de los distintos tipos de estrategias. Priorización de metas, comunicación, medición y la rendición de cuentas. Organizaciones dedicadas a la ciberseguridad y ciberdefensa. Capacidades. Operaciones cibernéticas.

- **Normas y Dilemas Éticos**

Marco ético para la defensa y seguridad del ciberespacio. Dilemas de atribución. Hacktivismo ético y criminal. Poder de policía de los estados. Tratados y regulaciones internacionales para el acceso y uso del ciberespacio. Normativas nacionales para la prevención de los ciberdelitos. Estándares de control y calidad para el gobierno electrónico público y privado. Prevención de delitos en redes sociales, comunidades virtuales y en aplicaciones del Big Data.