Descripción de las asignaturas de cursado virtual ofrecidas en la presente Convocatoria

UNIVERSIDAD MAYOR (CHILE):

Inicio de clases: agosto - Fin de clases: octubre

- **Gestión de Incidentes en Ciberseguridad (para alumnos/as que estén cursando 2° año)**

Se trata de una asignatura cuyo objetivo es proporcionar a los estudiantes los conocimientos teóricos y prácticos necesarios para comprender, prevenir, detectar y responder de manera efectiva a los incidentes de seguridad en entornos digitales. Esto debido a que en la actualidad, las organizaciones se enfrentan a un gran número y aumento exponencial de amenazas relacionadas a la ciberseguridad, tales como: ataques de malware, phishing, robo de datos y explotación de vulnerabilidades.
La materia busca que el estudiante pueda:

- Comprender los fundamentos de la gestión de incidentes en ciberseguridad, incluyendo los conceptos clave, los marcos de referencia y las mejores prácticas utilizadas en la industria, con la finalidad de que el estudiante tenga la capacidad para aplicar estos conocimientos en situaciones reales de la industria.
- Diseñar un plan integral de gestión de incidentes, considerando los aspectos organizacionales y técnicos, con el objeto de garantizar una respuesta eficaz ante cualquier incidente de seguridad que pueda afectar a una organización.
- Ejecutar actividades fundamentales de la respuesta ante incidentes, considerando la contención, erradicación y recuperación de los incidentes detectados, lo que permitirá recopilar la mayor cantidad de antecedentes y evidencias
- Aplicar un enfoque de aprendizaje posterior al incidente, analizando las causas subyacentes de los incidentes y proponiendo mejoras con el objetivo de prevenir futuros incidentes similares en relación a las lecciones aprendidas.

Metodología de enseñanza: Realización de trabajos prácticos, abordaje de casos de estudio, talleres de discusión y dictado de clases telemáticas.
Número de horas totales: 72 horas pedagógicas y 4 horas de trabajo autónomo.

- **Criptografía aplicada a la Ciberseguridad (para alumnos/as que estén cursando 2° año)**

El objetivo de la asignatura Criptografía Aplicada a la Ciberseguridad es proporcionar al estudiante una mirada práctica sobre los principales aspectos del uso de la criptografía, una de las ciencias más importantes en ciberseguridad. Dicha asignatura se desarrollará a través de múltiples actividades prácticas en las que el estudiante podrá conocer las principales aplicaciones de la criptografía y cómo ésta permite proteger los datos tanto en reposo como en tránsito.
Al finalizar la asignatura el estudiante podrá:

- Analizar los fundamentos teóricos de la criptografía, con el propósito de comprender los principios matemáticos y algorítmicos que sustentan los sistemas criptográficos modernos, aplicado a la protección de Información en las empresas.
- Implementar algoritmos criptográficos simétricos y asimétricos, con la finalidad de aplicar técnicas de cifrado y descifrado para garantizar la confidencialidad e integridad de la información
- Aplicar funciones HASH a la protección de la Integridad de los datos empleando estos en la detección de cambios no esperados en la Información, con el objetivo de asegurar la confidencialidad, integridad y autenticidad de la información.
- Gestionar infraestructuras de clave pública (PKI), con el objeto de implementar certificados digitales y mecanismos de autenticación segura en diversos escenarios.

Metodología de enseñanza: Dictado de clases telemáticas, análisis de casos de estudio, talleres de discusión y realización de trabajos prácticos.
Número de horas totales: 72 horas pedagógicas y 4 horas de trabajo autónomo.

- **Análisis Forense Digital (para alumnos/as que estén cursando 3° año)**

Esta asignatura se enfoca en el estudio y aplicación de metodologías y técnicas especializadas para la investigación y recuperación de evidencia digital, abordando su importancia tanto en el ámbito legal como empresarial. El curso proporciona a los estudiantes las habilidades necesarias para identificar, preservar, analizar y presentar información digital de manera sólida, con el objetivo de esclarecer incidentes de seguridad, delitos informáticos y otras situaciones que requieran la reconstrucción de eventos a partir de datos electrónicos.
A través de una combinación de teoría y práctica, los estudiantes desarrollarán competencias para aplicar el análisis forense digital en diversos contextos, incluyendo la investigación de ciberataques, el descubrimiento de fraudes, la recuperación de datos borrados y la auditoría de sistemas. Se enfatiza la comprensión de los aspectos legales y éticos relacionados con la recolección y el manejo de evidencia digital, así como la capacidad de comunicar eficazmente los hallazgos a diferentes audiencias. Al finalizar el curso, los estudiantes estarán capacitados para contribuir de manera efectiva en equipos de respuesta a incidentes, investigaciones forenses y otras áreas relacionadas con la seguridad de la información.

Metodología de enseñanza: Dictado de clases telemáticas, análisis de casos de estudio y prácticas de laboratorio (a través de estas prácticas, aplican las técnicas y herramientas de análisis forense informático en escenarios simulados, lo que les permite desarrollar habilidades prácticas y aprender a manejar la tecnología y los equipos forenses de actividades que se realizan en el curso, descritas brevemente)
Número de horas totales: 72 horas pedagógicas y 4 horas de trabajo autónomo.