DER296 CIBERCRIMEN

Fundamentación

En un mundo tan dinámico en el que vivimos hoy en día, los usuarios, empresas y gobiernos no se encuentran al margen de los delitos que se cometen a través de Internet. Y como consecuencia de ello, las cifras van en aumento, si consideramos que el Cibercrimen representa anualmente el 0.8 % del producto bruto interno (PBI) mundial, más de 6.100 millones de dólares, y año a año continúa acrecentándose considerablemente. Es por ello, que se requiere estar actualizado en estas temáticas, adquiriendo conocimientos prácticos, pero desde la mirada de diferentes ámbitos profesionales, ya que nadie está exento de ser vulnerable ante tales circunstancias.

La realidad nos lleva a una transformación constante, por consiguiente, existe una creciente necesidad de profesionales de distintas ramas que estén capacitados y que de manera directa o indirectamente tomen conciencia del valor que se le debe asignar a la seguridad de la Información, a fin de poder prevenir y proteger sus activos más preciados: la información y todos sus derivados.

En este sentido, la presente materia, es una opción altamente atractiva en función del contenido que abarca, ya que el alumno, no estudiará al cibercrimen desde una mirada tradicional, sino ir más allá de lo normativo, donde le permitirá al estudiante que no sea de carreras afines, de poder entender cómo en su campo de trabajo existen estos tipos de delitos, de qué manera puede prevenirse y a qué fuentes recurrir frente a estos acontecimientos desafortunados.

Objetivos

Generales

- Reconocer y comprender los conceptos generales del cibercrimen, su diferencia con los Delitos Informáticos, sus tipologías, aspectos legales y diferentes perfiles de cibercriminales que se encuentran para prevenir al respecto.

- Identificar a los ciberdelitos, discernir cómo en campos ajenos al derecho o la Ingeniería, existen estos delitos y saber cómo prevenirse desde sus campos profesionales.

Específicos

- Comprender qué aspectos legales se deben tener en cuenta frente a un cibercrimen para prevenirlo desde distintas áreas profesionales.

- Revisar e identificar diferentes modalidades delictivas desde casos prácticos.

- Identificar herramientas para investigaciones relacionadas a la detección del cibercrimen.

- Entender el valor relacionado a la seguridad de la información, desde la privacidad y la protección de datos (personal, empresarial y gubernamental).

Competencias

Genéricas

Gestión de la información y el conocimiento

Se espera que los alumnos logren:

- Aplicar los conocimientos obtenidos de los conceptos dados, con el objeto que puedan identificar los riesgos y lograr su prevención desde cualquier ámbito de trabajo.
- Comprender las diferencias conceptuales entre los distintos temas que comprenden al cibercrimen.

Soluciones innovadoras basadas en el conocimiento

- Entender los procesos de la cibercriminalidad que le permitirá generar distintas alternativas o instrumentos de prevención, poniendo en práctica las herramientas aprendidas.

Específicas

- Desde la Deontología profesional, se espera que el alumno comprenda desde las normas y valores adquiridos, cómo debe actuar frente a un caso de cibercrimen

- Capacidad de valoración del entorno y empatía, se busca que reconozca las distintas áreas y le sean amigables al momento de un caso particular.

- Nuevas Tecnologías aplicadas al ámbito jurídico, donde el alumno podrá conocer e identificar las herramientas necesarias para adaptar a cada caso concreto.

Contenidos

Módulo 1

1. Cibercrimen y la Seguridad de la Información

1.1. Introducción conceptual

1.1.1. Funcionamiento de Internet y la Seguridad Jurídica. Conceptos y sus derivados.

1.1.2. Información, manejo y su seguridad. Alcances. Estadios de la Información.

1.1.3. ¿Qué es el Cibercrimen?, tipologías y alcances con la Big Data, Cloud Computing, entre otros. Normativa Nacional e Internacional. Colaboración Internacional.

1.1.4. Evidencia Digital. Cadena de Custodia. Consideraciones. Nuevos desafíos en la Investigación. Desafíos Procesales.

Módulo 2

2. El rol del Cibercrimen y los datos personales

2.1. Datos personales y sus derivados

2.1.1. ¿Qué son los datos personales? Normativa vigente. Base de datos. Concepto y Alcance. Privacidad en el ámbito laboral y sus derivados.

2.1.2. ¿Cómo repercuten los datos personales en la Ingeniería social, social Media y Marketing Digital? Herramientas. Comunicación no Verbal.

2.1.3. Emprendedurismo en Internet. Régimen legal. Registro de un Software y Nombres de dominio. Contratos en sitios Web. Firma Digital y Electrónica. Alcances.

2.1.4. Propiedad Intelectual: Alcances y consecuencias. Marca y Patente. Su relación con el Cibercrimen y el Ciberespionaje.

Módulo 3

3. El Cibercrimen y el comercio electrónico

3.1. El comercio electrónico

3.1.1. Concepto, Tipologías, alcances. Normativa vigente.

3.1.2. Casos de Phishing, Pharming, Carding en el mundo del comercio electrónico

3.1.3. Comercios paralelos: Darknet (casos de investigación). Concepto. Mirada de distintos ámbitos profesionales. Diferencias con la Deep Web. Anonimato.

3.1.4. Cryptomonedas (bitcoin, etc.). Concepto, Alcances, Modelo Operacional.

Módulo 4

4. La Internet de las cosas (IoT) y las infraestructuras críticas

4.1. Ciberdelitos en todas partes

4.1.1. Internet de las cosas. Concepto, Alcance y Tipologías. Diferentes tipos de ataques.

4.1.2. Infraestructuras críticas. Concepto, Tipologías y su relación con la ciberseguridad

4.1.3. La Web 3.0: Inteligencia Artificial, la realidad aumentada, la realidad virtual y el ciberdelito.

4.1.4. Nuevas tendencias en el Cibercrimen: Bio-Crime, Drones, Impresoras 3D, entre otras.

Bibliografía

BASICA:

Altmark, D. R. y Molina Quiroga, E. (2012). *Tratado de Derecho* Informático (1a edición). Tomo I, II y III. Buenos Aires, Argentina: La Ley.

Palazzi, P. (2016). *Los Delitos Informáticos en el Código Penal -Análisis de la ley 26.388* (3a edición). Buenos Aires, Argentina: Abeledo Perrot.

Ampliatoria:

Barrera, S. (2016). *Claves de la Investigación en Redes Sociales* (1a edición). España: Círculo Rojo. Disponible en: https://sbarrera.es/tienda/libros/claves/

Borghello, C. (2017). Seguridad Informática. Argentina. Disponible en: http://www.segu-info.com.ar/articulos/

Borghello, C. y otros. (2017)**.** Glosario de Delitos Informáticos. Argentina. Disponible en: https://www.odila.org/glosario

Davara Rodríguez, M. A. (2015). *Manual de Derecho Informático (Duo) (11a edición).* España: Thomson Reuters Aranzadi. Disponible en: https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=aranz%2Fmonografias%2F163237639%2Fv11.2&titleStage=F&titleAcct=i0adc419000000147a1c91f053c81274e#sl=e&eid=bafa47940f4c6c6775b337c4c1b8976d&eat=%5Bbid%3D%221%22%5D&pg=1&psl=e

Elías, M. S. (2017). Informática legal. Argentina. Disponible en: http://www.informaticalegal.com.ar/legislacion-informatica/

Observatorio Español de Delitos Informáticos. (2017). legislación Delitos Informáticos. España. Disponible en: http://oedi.es/ciberdelitos/

Observatorio Iberoamericano de Protección de Datos. (2017). Jurisprudencia y Leyes. Iberoamérica. Disponible en: http://oiprodat.com/jurisprudencia-relacionada/

Oficina de las Naciones Unidas de Crímenes y Drogas. (2017). Repositorio Mundial de leyes relacionadas a Cibercrimen. Mundial. Disponible en: https://www.unodc.org/cld/index-sherloc-les.jspx?tmpl=cyb

Tobares Catalá, G. y otros. (2010). *Delitos Informáticos*. Argentina: Advocatus.

Recursos

Contenidos y materiales multimediales en plataforma.

I. Caso de Phishing. 2017. “Cómo obtener el usuario y contraseña de un móvil”. España. Web: https://www.youtube.com/watch?v=Ce8Jcrb7yOo

II. Caso de Acceso Indebido a las comunicaciones. 2016. “Como trackear una llamada”. Australia. Web. https://www.youtube.com/watch?v=1oA0O01SQUE

III. Ransomware. 2017. “¿Qué es el Ransomware, cómo actuar y como prevenirlo?”. España. Web: https://www.youtube.com/watch?v=tDdLWN4aWh4

IV. Bitcoin. 2015. “Que es el Bitcoin”. Argentina. Web. https://www.youtube.com/watch?v=KlzzlQBDBfI

V. BigData. 2014. “Indroducción a la BigData”. Online. Web: https://www.youtube.com/watch?v=mqMFMgVnRO8

VI. Cibercrimen. 2016. “Nuevas tendencias del Cibercrimen”. Estonia. Web. https://www.youtube.com/watch?v=a-19g06qIKM

VII. Internet de las Cosas (IoT). 2016. “Que es y para que funciona”. España. Web: https://www.youtube.com/watch?v=uY-6PcO96Bw

Leyes complementarias.

I. Ley de Delitos Informáticos: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

II. Convención de Budapest: Convenio completo. 2011. “Convención de Budapest”. Budapest. Europa. Web. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

III. Convención de Budapest: Reporte Explicativo. 2011. “Convención de Budapest”. Budapest. Europa. Web. https://rm.coe.int/16802fa403

IV. Ley de Protección de datos. 2000 “Ley completa de Protección de datos personales”. Argentina. 2000. Web. https://www.oas.org/juridico/pdfs/arg_ley25326.pdf

V. Normas Iso 27001. 2013. “Estándar para la Seguridad en la Información”. Mundial. Web. https://es.wikipedia.org/wiki/ISO/IEC_27001

Diccionario Jurídico.

I. **Real Academia Española.** 2017. “Diccionario Jurídico”. Español. Web**.** http://dej.rae.es/

II. **Symantec.** 2017. “Glosario de Términos en Seguridad Informática”. Español. Web. https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

III. **Panda Security.** 2017. “Glosario de Términos en Seguridad Informática”. España. Web. http://www.pandasecurity.com/spain/homeusers/security-info/glossary/

Bibliografía sugerida.

I. **Dr. Faustino Gudín Rodríguez-Magariños.** 2016. “Nuevos Delitos Informáticos, PHISING, PHARMING, HACKING Y CRACKING”. Colegio de Abogados de España. Web. http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf

II. Darknet. 2017. “Darknet”. Wikipedia. Web. https://es.wikipedia.org/wiki/Darknet

III. Infraestructuras críticas. 2017. “Introducción a las Infraestructuras Críticas”. Argentina Web. http://www.icic.gob.ar/

IV. Infraestructuras críticas. 2017. “Introducción a las Infraestructuras Críticas”. España. Web. http://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/infraestructuras

V. Alejandro Alagia y otros. Año III. Nº7.2014. “. Derecho Penal. Delitos Informáticos. Ministerio de Justicia de la Nación Argentina”. Argentina. http://www.saij.gob.ar/docs-f/ediciones/revistas/Penal_07.pdf

Buscadores vinculados a la profesión.

I. Buscador Jurídico -Legislaw. 2017. “Portales Jurídicos y Otras web de interés”. Argentina. Web. http://www.legislaw.com.ar/otros/busca.htm

II. Sistema Argentino de Información Jurídica. 2017. “Información Jurídica”. Argentina. Web: http://www.saij.gob.ar/

III. Buscador de Normas -Infoleg-. 2017. “Buscador de normas”. Argentina. Web: http://www.infoleg.gob.ar/

IV. Buscador de dominios -NIC.ar-. 2017. “Buscador de dominios disponibles y otros servicios”. Argentina. Web: https://nic.ar/

V. Registro de Software. 2017. “Información para registro de Software”. Argentina. Web. http://www.cessi.org.ar/tramites-registro-de-software-88/index.html

VI. Registro de Marcas. 2017. “Información para el registro de Marcas”. Argentina. Web. https://www.argentina.gob.ar/registro-de-marcas

VII. Instituto Nacional de Propiedad Intelectual. 2017. “Información registro Marcas y Patentes”. Argentina. Web. http://www.inpi.gov.ar/index.php?Id=338&criterio=3

Carga Horaria

La carga horaria semestral dedicada al dictado de clases teóricas y prácticas de la asignatura es de 43 horas reloj, asignándosele del total, 16 horas a las actividades prácticas.

Metodología

Las clases teóricas se organizarán tomando como base el material incluido en la bibliografía seleccionada. Las clases se desarrollarán a partir de las explicaciones relativas a los temas de la bibliografíaía por parte del profesor y de las intervenciones por parte de los alumnos dirigidas a aclarar conceptos o a profundizar en determinados temas que puedan resultar de interés. Se utilizará material didáctico de apoyo.

En las clases prácticas se revisarán investigaciones actuales y se discutirán los aspectos metodológicos más relevantes. En las clases prácticas el profesor asumirá la tarea de introducir y supervisar el desarrollo de la actividad programada, correspondiendo al alumno el papel protagonista al participar directamente en la revisión y discusión de las investigaciones, y en la resolución de las actividades propuestas.

Forma de Evaluación

En esta materia se evalúa el proceso de aprendizaje del alumno a través de las tareas realizadas por ellos en las fechas estipuladas institucionalmente.

La aprobación, se determina en función al cumplimento de los criterios de evaluación especificados. Estos criterios se basan en tres áreas claves/críticas: cumplimiento de tiempos de entrega (según cronograma), cumplimento de las especificaciones de forma del entregable y nivel de logro de las competencias vinculadas a esta materia.

La condición de regularidad de esta materia, se define según lo establecido en el Reglamento Institucional, de acuerdo a la condición del alumno (Regular, Libre, Promocionado).