SISTEMA NACIONAL DE CAPACITACION
DISEÑO DE LA ACTIVIDAD

Nombre

EL CIBERCRIMEN, LA CIBERSEGURIDAD Y LA INVESTIGACIÓN CRIMINAL DE DELITOS INFORMÁTICOS

Código INAP IN35411/21 ***Estado*** Activo

Programa)Actividades Transversales ***Área***)Informática

Fundamentación

Propósito: Desarrollo y/o fortalecimiento de capacidades.

Con la digitalización del papel y el almacenamiento de información en bases de datos computarizadas durante la década del 1970, la creación de las computadoras personales (PC) y otros dispositivos como agendas electrónicas, celulares y beepers en los años 80s, la informática sale del ámbito de los laboratorios de investigación y de empresas contratistas militares para pasar al ámbito público y doméstico. Con la apertura comercial de Internet por parte del gobierno de los Estados Unidos a mediados de la década de 1990 y la expansión de la Web –el servicio más popular de Internet- aparecen nuevos peligros y amenazas para la seguridad de las personas a partir de la multiplicidad de oportunidades tecnológicas que ofrece este medio. El uso de dispositivos informáticos –tales como notebooks, smartphones, tablets, smarts TVs y consolas de videojuegos ocupan hoy en día un papel central en la vida cotidiana de las personas tanto para relaciones laborales, de estudio, de consumo y el ocio, lo que obliga a los diferentes Estados a incorporar a la agenda gubernamental la problemática de los delitos informáticos. Existen dos enfoques en cuanto al fenómeno criminal en Internet. El más común de ellos afirma que la nube brinda nuevas herramientas para la comisión de delitos tradicionales como el robo, el fraude y la pornografía, entre otros, adquiriendo nueva vida a partir del uso de medios electrónicos. Otra perspectiva, en cambio, alega que estas tecnologías otorgan posibilidades únicas para la comisión de nuevos delitos, tales como la piratería de software, los ataques de virus, el “hackeo” a sitios webs, etc., que se originan y tienen existencia únicamente a partir del uso de sistemas informáticos. El propósito del curso es abordar este nuevo fenómeno criminológico a partir del estudio de sus orígenes y clasificación, el contexto político-económico de surgimiento, las modalidades ilícitas en Internet a partir del uso de nuevas tecnologías de la información y la comunicación (TICs), tanto así como las nuevas técnicas de investigación en materia criminalística frente a un nuevo entorno virtual a nivel global; teniendo en cuenta que hoy, conviviendo en un espacio que ya no es solo físico sino también virtual, el conocimiento y la concientización de esta temática refieren una importancia sustancial para el desarrollo personal y profesional de cada ciudadano y/o servidor público.

A partir de lo mencionado y en línea con la Propuesta Formativa del INAP, en la presente actividad prevalecen los siguientes tipos de saberes: Saber (saberes objetivados sobre la realidad organizados en sistemas de conceptos y teorías) - Saber qué hacer (saberes de situación relacionados con la capacidad de tomar decisiones en situaciones y

contextos específicos) Saber reflexionar (saberes relacionados a la capacidad de volver el pensamiento sobre objetos, situaciones, hechos, creencias, etc).

Contribución esperada

Que los participantes finalicen la actividad con conocimientos básicos sobre cibercrimen, ciberseguridad y delitos informáticos, así como las formas de abordaje de la problemática; a fin de sensibilizar, concientizar y capacitar sobre los mismos para su prevención y buen uso del ciberespacio tanto en el área laboral como personal, y promover aspectos de mejoras en las áreas de la administración pública nacional donde desempeñen sus funciones.

Perfil del participante

Trabajadores de la Administración Pública Nacional.

Objetivos

Que los participantes logren:
• Conocer las modalidades delictivas cometidas mediante el uso de tecnologías de la información y comunicación (TICs) en Internet y offline más comunes.
• Entender las herramientas legales para el abordaje de la problemática.
• Adquirir conocimientos sobre técnicas de investigación de ciberdelitos, su forma de obtención y posterior incorporación como prueba en el proceso.
• Aplicar los contenidos adquiridos sobre cibercrimen en situaciones similares a las de su práctica laboral.

Contenido

Unidad 1: (2 horas y media): Historia de Internet y el cibercrimen
• Historia de Internet y los delitos informáticos.
• Cibercrimen y ciberseguridad. Definición. Diferencia con la ciberguerra.
• Áreas de abordaje de la problemática: el Derecho y la seguridad informática.

Unidad 2: (2 horas y media): Modalidades delictivas en la red
• Modalidades ilícitas comunes y crimen organizado en Internet.

Unidad 3: (2 horas): Marco legal en Argentina y formas de investigación criminal de delitos informáticos
• Legislación nacional e internacional en la materia.
• Investigación criminal de delitos informáticos.

Unidad 4: (2 horas): Análisis y estudio de casos prácticos
• Análisis y estudio valorativo de la evidencia digital para la determinación de la comisión de un delito.
• Exposición de casos actuales y fallos.

Estrategias metodológicas y recursos didácticos

Para el proceso de las clases se expondrán presentaciones dinámicas en power point, las cuales serán trabajadas durante los encuentros. Asimismo, se utilizará soporte de imagen y video en base a la temática. Se proveerá bibliografía obligatoria y complementaria para el curso.
En lo que respecta al desarrollo de las actividades, las mismas consistirán en las siguientes:
Actividades de desarrollo:
Casos para analizar dentro de la disciplina y el marco jurídico actual, a fin de identificar los diferentes tipos de delitos informáticos abordados.
Búsqueda y presentación de una noticia sobre la temática, a fin de trabajar en las modalidades delictivas expuestas.
Actividades de Integración:
Elaboración de una propuesta de mejora para su espacio laboral en base a la temática desarrollada.
Actividad múltiple choice, a fin de integrar todos los contenidos desarrollados.

Descripción de la modalidad

Virtual Sincrónico

Bibliografía

Sain, Gustavo. (2015). “CIBERCRIMEN: EL DELITO EN LA SOCIEDAD DE LA INFORMACIÓN”. En Eissa, S. (Coord.), Políticas públicas y seguridad ciudadana, pp. 163-185. Buenos Aires: Eudeba.

Ley Nº 26.388 de la República Argentina: “Ley de delitos informáticos”.

“¿QUÉ ES EL ROBO DE IDENTIDAD?” (documento de curso)

“SI CREÍAS QUE EL TIMO DEL PRÍNCIPE NIGERIANO NACIÓ CON INTERNET, ATENTO A SUS SIGLOS DE HISTORIA”. Sitio web Xataka. Recuperado de https://www.xataka.com/historia-tecnologica/si-creias-que-el-timo-del-principe-nigeriano-nacio-con-internet-atento-a-sus-siglos-de-historia

“LOS 6 TIMOS MÁS HABITUALES DE INTERNET”: Revista Computer Hoy, 14 de marso de 2020

¿QUÉ ES EL PHISHING?. Sitio web InfoSpyware. Recuperado de https://www.infospyware.com/articulos/que-es-el-phishing/

¿QUÉ ES BOTNET?. Sitio web About.com. Recuperado de http://aprenderinternet.about.com/od/Glosario/g/Que-es-Botnet.htm

¿QUÉ ES DENEGACIÓN DE SERVICIO?. Sitio web About.com. Recuperado de http://aprenderinternet.about.com/od/Glosario/g/Que-es-Denegacion-de-Servicio.htm

"QUÉ ES RANSOMWARE, LA DEFINICIÓN Y LOS 5 TIPOS PRINCIPALES". Sitio web Software Lab. Recuperado de https://softwarelab.org/es/que-es-ransomware/

"EL ACOSO SEXUAL POR INTERNET". Diario Página 12, 15 de abril de 2014.

"EL SEXO EN LA ERA DIGITAL". Diario Página 12, 26 de febrero de 2016.

"CREEPWARE", Revista Computer Hoy, 18 de abril de 2015

Oficina de Naciones Unidas contra la Droga y el Delitos (UNDOC): Sextorsion. Recuperado de https://www.unodc.org/documents/ropan/2020/Ciberdelito_junio2020/SEXTORSION.pdf

Tourliere, Mathieu. La Red oscura del Internet: pedofilia, narco, armas, artículos robados. Recuperado de https://www.proceso.com.mx/348354/la-red-oculta-del-internet-compra-de-droga-armas-articulos-robados.

Sain, Gustavo. (2017): "INTERNET, EL CIBERCRIMEN Y LA INVESTIGACIÓN CRIMINAL DE DELITOS INFORMÁTICOS". Sain, G. y Azzolin, H.: Delitos informáticos: investigación criminal, marco legal y peritaje, pp. 1-18. Montevideo: BdF.

Sain, Gustavo. (2007). Dificultades de la informática forense para investigación de delitos cometidos en Internet. Recuperado de http://www.rubinzalonline.com.ar/

Evaluación de los aprendizajes

Evaluación de proceso: se llevará adelante durante todo el desarrollo de la propuesta, a partir de la realización de actividades de diferente complejidad tendientes a la apropiación de los contenidos expuestos.
Evaluación de producto: se realizará a partir de una actividad integradora final multiple choice, abarcando todos los ejes de contenidos vistos en la materia.
Para la aprobación de la actividad, se aplicarán los siguientes criterios de evaluación:
-Identificación de delitos informáticos.
-Conocimiento del marco legal vigente respecto a la investigación de los mismos
-Reconocimiento de hechos delictivos asociados a la temática.
-Desarrollo de aspectos de mejora para su área de trabajo.

Instrumentos para la evaluación

Instrumentos para la evaluación de los aprendizajes: Informes de la plataforma. Matriz para la evaluación de las actividades.
Instrumentos para la evaluación de la actividad: Encuesta de satisfacción INAP.

Requisitos de Asistencia y aprobación

Se requerirá un 80% de asistencia al curso. Realización de las actividades propuestas. Realización y aprobación del cuestionario integrador final con la obtención de un puntaje mínimo de 70%.

Duración (Hs.)

9

Detalle sobre la duración

9 horas distribuidas en 4 encuentros virtuales sincrónicos organizados de la siguiente manera: Dos (2) encuentros virtuales sincrónicos de 2 horas y 30 minutos de duración cada uno y dos (2) encuentros virtuales sincrónicos de 2 horas de duración cada uno.

Lugar

Plataforma de videoconferencias CISCO Webex
Campus Virtual INAP

Perfil Instructor

Gabriela Lizio - Perito Criminalista Esp. En Investigación Criminal.

Origen de la demanda

Dirección Nacional de Ciberseguridad

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
27324752744	ELDRID,BRENDA