

SISTEMA NACIONAL DE CAPACITACION DISEÑO DE LA ACTIVIDAD

Nombre

INTRODUCCIÓN AL CIBERDELITO

Código INAP IN34364/20 **Estado** Activo

Programa)Actividades Transversales **Área**)TIC Aplicadas a la Gestión

Fundamentación

Actualmente, muchas de las conductas delictivas ya no ocurren en el mundo real, sino en el cibernético. Son los llamados CIBERDELITOS: los delitos realizados a través de las tecnologías de la información y la comunicación (TIC) en el ciberespacio o aquellos cuya planificación, organización o resultado se encuentra expuesta en el ciberespacio. Internet, la red de redes, se ha convertido en terreno fértil para toda clase de infracciones a la ley; allí coexisten varias modalidades de delito, desde las más clásicas hasta las más modernas.

Los ciberdelitos son difíciles de perseguir. Los ciberdelincuentes actúan amparados en el anonimato que proporciona Internet, además del carácter transfronterizo de los mismos, es decir, el delito puede cometerse en nuestro país y el ciberdelincuentes estar en otro.

A nivel mundial, las organizaciones internacionales y regionales, los gobiernos de otros países, los organismos encargados de hacer cumplir la ley y las organizaciones no gubernamentales, entre otros, están abordando los delitos tecnológicos y los ciberdelitos de diferentes formas, que incluyen medios legislativos, de aplicación de la ley y de fomento de la capacidad.

En este contexto, la DIRECCIÓN DE INVESTIGACIONES DEL CIBERDELITO del MINISTERIO DE SEGURIDAD, órgano rector en la materia, ha diseñado y propuesto el PLAN FEDERAL DE PREVENCIÓN DE DELITOS TECNOLÓGICOS Y CIBERDELITOS, aprobado mediante la Resolución, N° 977 del 4 de noviembre de 2019, cuyas metas principales son la coordinación federal de lucha contra el ciberdelito, el fortalecimiento de la capacitación, la cooperación internacional y la cooperación entre el sector público y privado, entre otras.

En este orden de ideas, resulta imperativo poner especial atención en el fomento de las capacidades de los agentes públicos en todos sus niveles, para lograr una utilización de Internet consciente y con conocimientos plenos de las herramientas legales de protección que en nuestro ordenamiento existen como así también, en caso de ser víctimas, saber cómo ampararse.

Contribución esperada

Que las y los agentes de la Administración Pública reconozcan los tipos de ciberdelito más frecuentes, los métodos y herramientas utilizados por los ciberdelincuentes y el marco normativo nacional de protección, de manera de contribuir a preservar la información personal y la de las organizaciones y su propia integridad física.

Perfil del participante

- Trabajadoras y trabajadores de la Administración Pública Nacional, Provincial y Municipal.

Objetivos

Que los participantes logren:

- a) Identificar los principales ciberdelitos.
- b) Conocer los principales factores que posibilitan la ocurrencia de los ciberdelitos.
- c) Reconocer técnicas utilizadas por los ciberdelincuentes.
- d) Conocer el marco legal nacional, las sanciones aplicables y los canales de denuncia y contención.

Contenido

UNIDAD 1: Aspectos generales del ciberdelito

- Concepto de ciberdelito.
- Tipos.
- Legislación nacional: Leyes 26388 y 26904.
- Técnicas y herramientas utilizadas por los ciberdelincuentes.

UNIDAD 2: FORMAS DE PREVENCIÓN DEL CIBERDELITO

- Recomendaciones.
- Dónde denunciar.

Estrategias metodológicas y recursos didácticos

Con el fin de favorecer el alcance de los objetivos de aprendizaje propuestos, las estrategias metodológicas se centran en el desarrollo de los ejes temáticos desde lo general hacia lo particular. En una primera instancia se abordarán los aspectos conceptuales y normativos y posteriormente se trabajarán situaciones concretas y herramientas prácticas. Se busca favorecer la vinculación entre los contenidos y los diversos aspectos del entorno laboral de los participantes.

El formato es digital. El contenido está distribuido en el entorno virtual en sucesivas pantallas que integran los distintos recursos como ser: textos, infografías, videos, documentos en formato pdf y bibliografía de consulta.

La secuencia didáctica incluye actividades de distinto tipo y nivel de complejidad que los participantes deberán completar a lo largo del trayecto de manera individual. Se trata de ejercicios de autocomprobación con valoración automática por parte del sistema, que ofrece una retroalimentación al participante sobre su progreso, además de la calificación correspondiente.

Descripción de la modalidad

VIRTUAL AUTOGESTIONADO

Bibliografía

Ley 26388: Modificación del Código Penal.

Ley 26904: Se incorpora la figura de 'Grooming' o 'Ciberacoso' sexual al art. 131 del Código Penal.

Guía Ciberdelitos de la Unión Internacional de telecomunicaciones (ITU)

Comprensión del Ciberdelito de la Unión Internacional de telecomunicaciones (ITU)

Internet la nueva era del Delito. Ciberdelito, ciberterrorismo, legislación y ciberseguridad - Revista Latinoamericana de Estudios de Seguridad

Con vos en la Web Digital - Ministerio de Justicia Argentina

Resolución Organización Estados Americanos - Asamblea General 1939 XXXIII O-03

Evaluación de los aprendizajes

Evaluación de proceso: El participante realizará actividades de autocomprobación que lo informarán sobre sus logros y dificultades en sus procesos de aprendizaje

Evaluación de producto: Los participantes deberán realizar una actividad final integradora de resolución individual y de carácter obligatorio mediante una prueba de opción múltiple a realizar en el entorno virtual de aprendizaje. Se ofrecerán dos intentos de resolución de la actividad final integradora.

Instrumentos para la evaluación

Instrumentos para la evaluación de los aprendizajes: Pruebas de autocomprobación en entorno virtual de aprendizaje.

Prueba final integradora multiple choice.

Instrumentos para la evaluación de la actividad: encuesta de satisfacción de los participantes.

Requisitos de Asistencia y aprobación

Navegación por todos los contenidos del entorno virtual de aprendizaje; lectura de los materiales, visionado de videos.

Resolución y aprobación de todas las actividades de autocomprobación, con 60 % de respuestas correctas.

Resolución y aprobación de la prueba final integradora de tipo multiple choice con 60 % de respuestas correctas.

Duración (Hs.)

5

Detalle sobre la duración

Cinco horas distribuidas en dos semanas de trabajo.

Lugar

CAMPUS VIRTUAL INAP



Perfil Instructor

Especialista en la temática. Contenidista: Mariana GALÁN

Origen de la demanda

INAP/MINISTERIO DE SEGURIDAD DE LA NACIÓN

El desarrollo del curso está a cargo del INAP.

Prestadores Docentes

CUIT/CUIL	APELLIDO Y NOMBRE
	ACTIVIDAD,AUTOADMINISTRADA