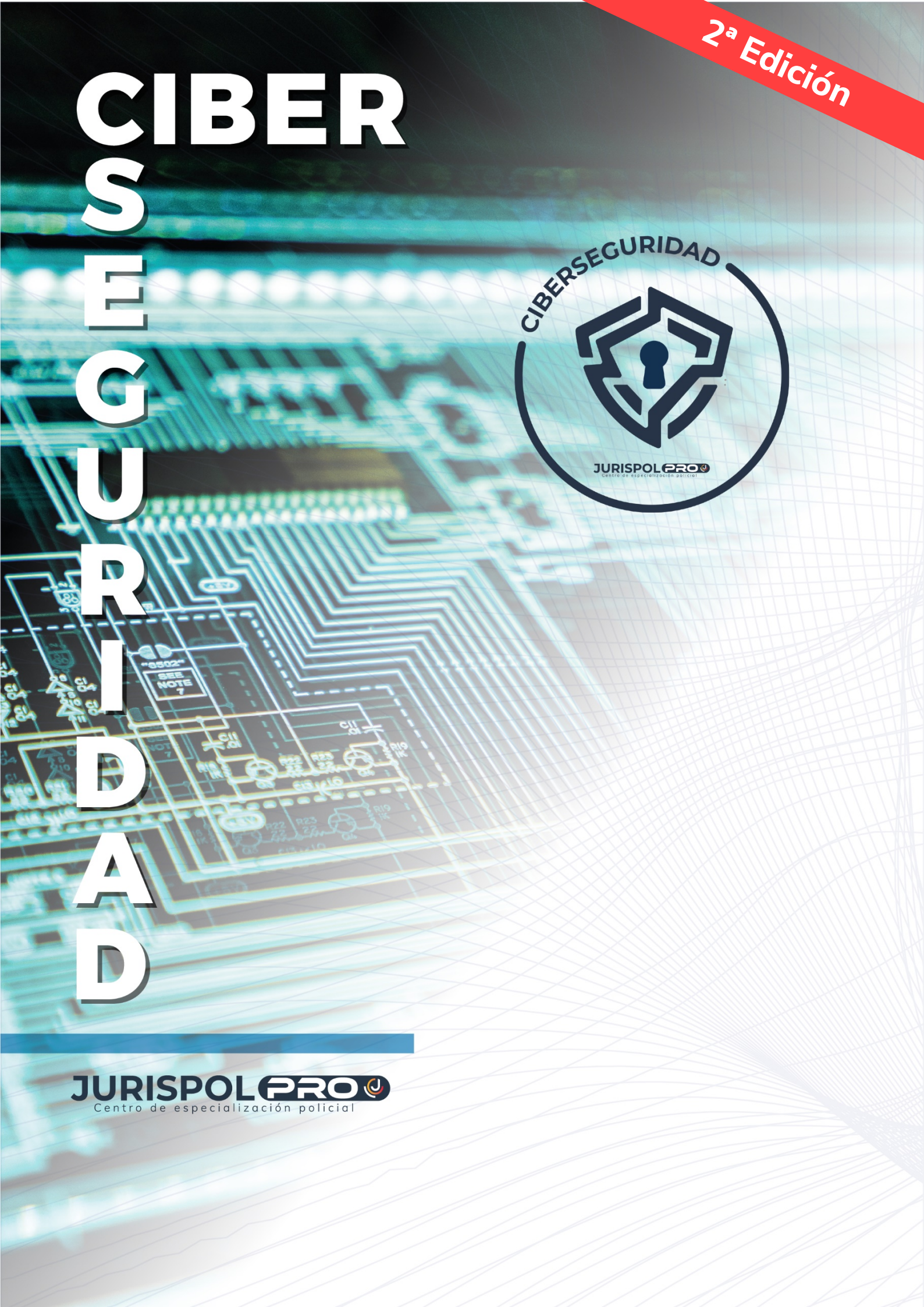
2ª Edición

CIBERSEGURIDAD



JURISPOL PRO
Centro de especialización policial

MEMORIA DE CURSO DE ESPECIALIZACIÓN

CIBERSEGURIDAD

La ciberdelincuencia no es el futuro de la criminalidad, sino ya el presente. Y es que, según los distintos cuadros estadísticos extraídos del "Estudio sobre la cibercriminalidad en España", realizados por el Ministerio del Interior y basados en la información recopilada por el SEC (Sistema Estadístico de Cibercriminalidad), se observa cada año un constante crecimiento, no solo del uso de dispositivos tecnológicos e internet en los hogares españoles, sino también de los delitos cometidos que se relacionan con el mundo virtual o cibernético.

Las características del cibermundo facilitan la conversión del delincuente habitual en delincuente tecnológico, ya sea por la comodidad de actuar en cualquier sitio y en cualquier momento, por la dificultad de ser identificado, o por la facilidad de obtener mejores resultados con un riesgo mínimo, todo ello gracias, además, a la continua evolución de los dispositivos tecnológicos y la mejora de la conexión a internet.

Por todo lo dicho es imprescindible una Policía preparada en la lucha contra el ciberdelito. Y es que, si no sabemos a qué nos enfrentamos, ¿cómo podemos combatirlo? Así pues, debemos ineludiblemente conocer no solo al cibercriminal sino también cómo actúa, cuáles son las distintas conductas que puede llevar a cabo y saber tipificarlas en el ámbito penal, sin olvidar lo más importante, cómo investigarlas para finalmente concluir con éxito el trabajo policial y llevar al autor de estos delitos ante la justicia.

- **UNIDADES DIDÁCTICAS:**

El presente curso consta de **cinco unidades temáticas**, que a continuación paso a detallar:

Unidad 1: Conocimientos previos básicos.

Obviamente, para llevar a cabo la investigación tecnológica es fundamental tener unos conocimientos previos suficientes del mundo virtual, por ello se tratan de manera concreta lo que es internet y sus organismos reguladores, los protocolos de comunicación necesarios en el ámbito de las redes informáticas, y las compañías que proveen del acceso a internet. Se enseña lo que es una dirección IP, y a distinguirla según sea pública o privada, estática o dinámica, IP NAT, o según la versión de su protocolo, tanto IPv4 como IPv6, o a diferenciar entre un navegador web y un motor de búsqueda. El alumno conocerá también lo que es un dominio y un subdominio, así como los distintos tipos de dominios que hay, además de aprender el funcionamiento básico de una comunicación en la red, o de acceso a una página web, ello a través de lo que son los DNS o Servidores de Nombres de Dominio, sin olvidar lo que es un registrador de dominios y cómo funciona. Además estudiará lo que es un correo electrónico y los distintos tipos que hay según su ubicación (webmail y clientes de correo), o los protocolos de comunicación que utilizan (SMTP, POP e IMAP). Para terminar se explica lo que es un anonimizador y qué tipos hay (proxy, webproxy, VPN, navegación de incógnito y redes TOR).

Unidad 2: Ciberdelincuentes.

No todos los delincuentes actúan en el ámbito cibernético, así que debemos saber diferenciarlos. Por tal motivo, se indican cuáles son los cibercriminales y sus distintas características, distinguiéndose de entre

ellos al cracker, que no hacker, a los acosadores cibernéticos y a los ciberacosadores sexuales, de los que específicamente diferenciamos al pedófilo y el pederasta, pero también a los ciberestafadores y ciberactivistas, los sextorsionadores, el trol, el insider informático, el defacer, script kiddie, sexter, fisher, y por último el botmaster. Terminando el tema se hace una distinción del delincuente (tecnológico o no) y la forma de proceder según su edad, ya sea menor de edad o adulto, así como del mulero o mula, que no es más que otra víctima del engaño consecuencia de un delito mayor.

Unidad 3: Riesgos habituales.

Las conductas delictivas determinarán la forma de proceder en una investigación, por ello es importante saber de qué manera puede actuar un cibercriminal. En este tema se ven los distintos comportamientos delictivos, como son la ingeniería social, o como obtiene un delincuente tecnológico la información de la víctima, así como los distintos tipos de phishing o de estafas o fraudes a través de la red, pero también el pharming, los ataques de intermediario o de denegación de servicio (DoS y DDoS), los distintos tipos de malware y virus informáticos, explicándose además qué es el spoofing así como cuanto tiene que ver con el grooming, o ciberacoso sexual a menores de edad por parte de adultos, haciendo finalmente referencia también al ciberbullying y el sexting.

Unidad 4: Delitos relacionados con el ámbito tecnológico.

Conociendo ya al cibercriminal y su comportamiento delictivo, lo que queda es identificarlo en el amplio espectro legal. Y de eso trata este tema, de señalar según la conducta su referencia legal, de ayudar al alumno a diferenciar los delitos “online” o del mundo virtual con los “offline” o fuera de internet. Se distinguen pues los delitos de amenazas y coacciones, calumnias e injurias, descubrimiento y revelación de secretos, extorsión y sextorsión, contra la propiedad intelectual e industrial, o contra los servicios de radiodifusión e interactivos. También se trata el delito de usurpación de identidad, que no es lo mismo que suplantación de identidad, y los relativos a la pornografía infantil, estafa, o daños informáticos, sin dejar de lado los delitos de odio y los de ciberterrorismo.

Unidad 5: Investigación tecnológica.

Todo lo que se ha visto hasta ahora en el curso busca una finalidad concreta: la investigación tecnológica. Cómo, tras una denuncia o una información, se llega al culpable de los hechos, al ciberdelincuente. Para empezar vemos quiénes son, tanto en Policía Nacional como en Guardia Civil, las unidades o grupos encargados de llevar a cabo la investigación, y después se dan unas nociones de la plataforma SITEL, imprescindible para solicitar por ejemplo la titularidad de una línea telefónica o remitir solicitudes de información a redes sociales, sitios de correo electrónico, etc., solicitudes que pueden venir en forma de mandamiento judicial u oficio policial, para lo cual se enseña al futuro policía investigador no solo la diferencia entre ambos sino también cuándo solicitar uno y cuándo usar el otro. Se aportan, además, numerosos recursos que el policía podrá utilizar en el día a día de una investigación y para obtener la información que permita seguir con las gestiones y pesquisas: dónde, cómo y a quién pedir la información, qué poner en el pie del escrito de solicitud, qué requisitos exige cada sitio, cómo enviarlo, cuánto tiempo hay de límite..., sin olvidar para los casos extremos, cuando exista riesgo de que la información pueda eliminarse o perderse, cómo solicitar una salvaguarda de los mismos. Se muestra lo fundamental sobre las leyes de protección de datos, y para terminar se explica cómo investigar una dirección IP, tratándose el tema de la geolocalización de IPS, los registros públicos de dominios, los comandos de consola, los husos horarios y la investigación de dominios “.es”.

- ## CONFERENCIANTE:

José Ángel Fernández Fernández, policía con carné profesional nº 84444, destinado actualmente en la Comisaría Provincial de Policía Nacional de Ávila, en Policía Judicial, Delitos tecnológicos.

- ## ESTRUCTURA DEL CURSO:

GLOSARIO DEL CURSO	DOCENTE	HORAS LECTIVAS
Introducción y conocimientos generales de la Unidad Central de Ciberdelincuencia	Francisco RIUS DIEGO y José Ángel Fernández Fernández	**1 h.**
Tema 1 Conocimientos previos básicos	José Ángel Fernández Fernández	**8 h.**
Tema 2 Ciberdelincuentes	José Ángel Fernández Fernández	**5 h.**
Tema 3 Riesgos habituales	José Ángel Fernández Fernández	**7 h.**
Tema 4 Delitos relacionados con el ámbito tecnológico	José Ángel Fernández Fernández	**5 h.**
Tema 5 Investigación tecnológica	José Ángel Fernández Fernández	**8 h.**

Un total de 34 horas lectivas componen este curso, dado que las 5 temáticas del mismo llevarán sus propios videos explicativos (más de 15 horas en video), preguntas de autoevaluación, además de documentación en ".pdf" para su estudio (27 páginas), todo lo cual llevará a la realización de un examen final de prueba de conocimientos adquiridos, y diferentes actividades prácticas que deberán superar antes de la finalización del curso.

Jefatura de Estudios de Jurispol.-