Nº 4	**Criminalidad informática y ciberdelincuencia**
Destinatarios	Un material docente. Un curso en línea para Escalafón Primario (Ministras y ministros de Cortes de Apelaciones / Juezas y jueces).
Descripción	El rápido y gran avance que han tenido las tecnologías va de la mano con los delitos que involucran el uso redes de información así como de dispositivos utilizados para la comisión de delitos, robo de información, daño de sistemas informáticos, bloqueos de flujos de información y otros similares. Lo anterior, unido a la dictación de la Ley 21.359 que regula la criminalidad informática tipificando un buen número de figuras penales, con la consecuente variación de ciertos procedimientos, introduciendo circunstancias modificatorias de responsabilidad penal, así como técnicas de investigación, hacen necesario que un texto y curso en línea que se preocupen de esta particular forma de comisión de ilícitos. El abordaje de estas materias debe contemplar, particularmente, los aspectos normativos asociados a este tipo de delincuencia, los procedimientos que asociados y los aspectos esenciales probatorios que requiere conocer la judicatura al enfrentarse a estos casos, siempre procurando una perspectiva desde lo práctico y con una visión multidisciplinaria y comparada de tan particular tipo de ilícitos.
Aspectos relevantes (No constituye exclusividad ni prelación)	1.- Importancia de la seguridad informática y la información, además de las formas de comisión de delitos que incorporar nuevas tecnologías. 2.- Marco jurídico internacional. Convenio de Budapest sobre ciberdelincuencia. Reservas al Convenio. Modelo de cooperación internacional que establece el Convenio. 3.- Ley 21.459 y los delitos de: ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos, falsificación informática, receptación de datos informáticos, fraude informático y el abuso de dispositivos. Circunstancias modificatorias (cooperación eficaz) y reglas especiales en materia de procedimiento. Las técnicas especiales de investigación. 4.- Modalidades frecuentes de ciberataques tales como robo de identidad, ransomware, phishing, ciber espionaje, malware, DDoS, ingeniería social, etc. 5.- Delitos asociados a la explotación de menores de edad por internet, especialmente del gromming. 6.- Brigadas policiales encargadas de la ciberdelincuencia. Principales peritajes utilizados en materia de ciberdelincuencia y problemas frecuentes para la comprensión judicial. 7.- Recolección y cadena de custodia de la evidencia digital a utilizar en juicio. Pruebas digitales. Problemas probatorios asociados. 8.- Ciberdelincuencia transnacional. Problemas relacionados con la jurisdicción y competencia de los tribunales. 9.- Ley 21.577: Registro remoto de equipos informáticos, registros de llamadas y otros antecedentes de tráfico comunicacional.