Informática Forense y su Prueba Científica

En el transcurso de los últimos años la rama de la ciencias forenses y en especial la Informática Forense ha tomado gran trascendencia, de tal magnitud, que organismos de Gobiernos y Poderes Judiciales han tomado la iniciativa de crear áreas específicas relacionadas a esta especialidad, con el objetivo de dar respuesta a distintos ilícitos que tengan asociados dispositivos tecnológicos.

Para entender a qué se dedica esta disciplina es importante poder entender qué es la informática forense y cuál es la función que llevara adelante el informático forense o perito informático.

Si bien existen muchas definiciones aplicadas por distintos autores, podríamos definir a la **Informática Forense** como una disciplina de las ciencias forenses, que procura descubrir e interpretar la información almacenada en los medios informáticos para establecer los hechos y formular las hipótesis relacionado con el caso investigado.

El **Informático Forense** es aquel profesional que permitirá avanzar en la búsqueda de la verdad, analizando la información residente en los dispositivos tecnológicos. Esa información es convertida en **evidencia digital** mediante la intervención humana u otra semejante, aplicándose procedimientos, métodos, técnicas y Herramientas forenses. Es considerado **evidencia digital** a cualquier registro generado por o almacenado en un **sistema computacional** que puede ser utilizado como prueba en un proceso legal. En definitiva la evidencia digital es la materia prima de todo informático forense o perito informático.

En una **pericia informática** hay factores que se deben tener en cuenta, como por ejemplo, quienes intervinieron con los elementos informáticos secuestrados antes de la recepción por parte del Perito Informático o Laboratorio Pericial. Para ellos es indispensable analizar el procedimiento de **cadena de custodia** que se llevó adelante; verificando si el personal policial capacitado que intervino: registró, documentó, resguardó, fajó y trasladó dichos elementos correctamente, siguiendo un procedimiento establecido en un Protocolo de Actuación generado por algún Organismo del Estado, Poder Judicial, Ministerio Público o Ministerio de Gobierno, en donde se contemplan normas, estándares, guías de buenas prácticas y bibliografía académica, para su implementa-

ción, los cuales permitan garantizar la integridad de los elementos tecnológicos secuestrados desde el lugar del hecho hasta el Juzgado o laboratorio pericial informático forense. Otro de los factores a tener en cuenta es la **prueba documental,** la misma permitirá aportar datos importantes a la hora de realizar el análisis forense en la evidencia digital. Un dato no menor, son los **puntos de pericias** establecidos en una investigación, los mismos permitirán establecer la **hipótesis** de la pericia solicitada. La pericia informática llevara en su totalidad, a sustentar la argumentación de la Hipótesis planteada, obteniéndose así la llamada "prueba pericial" o "prueba científica".

El profesional especializado de la informática forense realizara la pericia informática mediante un modelo de trabajo, una metodología forense, procedimientos operativos estandarizados, técnicas y herramientas forenses que le permitirán obtener la "prueba científica", garantizando que la misma sea completa, precisa, comprensible y auditable.

Como conclusión a lo abordado en los conceptos de la informática forense y su prueba pericial o científica, me gustaría destacar que si bien las herramientas forenses son la base esencial del análisis de la evidencia digital en los medios informáticos y su utilización dependerá exclusivamente de la experticia del profesional o perito que las utilice, hay que saber y tener presente que para esta disciplina científica **las herramientas no hacen al perito, sino los métodos, técnicas y procedimientos forenses que este lleve adelante.**

Lic. Gaston Semprini

Jefe del Departamento de Informática Forense

Poder Judicial de la Provincia de Rio Negro