DELITOS INFORMÁTICOS E INFORMÁTICA FORENSE

A finales de los años 90, se produjo un notable incremento de delitos informáticos. Debido a ello y principalmente por la falta de personal cualificado y de la nula infraestructura adecuada, los estados no fueron capaces de detectar estos delitos.

Por todo ello apareció la Informática Forense, con la misión de cubrir las necesidades específicas que surgieron a raíz de esta nueva forma de evidencia electrónica.

Con la apertura de internet de forma masiva a los usuarios, cambió el ámbito, las posibilidades de interacción entre usuarios y el ciberespacio pasó a ser una extensión más en las relaciones humanas. El número de redes existentes en esta época facilitó el surgimiento de los delitos informáticos.

¿Qué es la Informática Forense?

La informática forense es, por lo tanto, una disciplina científico-técnica especializada, que ofrece un análisis de la información almacenada o registrada en cualquier equipo electrónico relacionado con un hecho delictivo.

Un buen perito informático forense debe seguir una metodología de trabajo, como es:

- Recopilación de información.
- Mantener y custodiar dicha información.
- Procesamiento de los datos.
- Reconstrucción de los hechos.
- Formulación de hipótesis.
- Síntesis e informe.

¿Qué entendemos por delito informático?

Aunque su extensión crece a cada día que pasa, los delitos informáticos tienen su base en la realidad asociada a la convivencia en la sociedad actual. Delitos de estafa y fraude que antes tenían su sede en los parques y jardines de nuestras ciudades, ahora ocurren en el ciberespacio. Delito informático sería:

- Cualquier tipo de fraude cometido a través de medios electrónicos.
- Alteración de programas, ingeniería inversa.
- Falseo interesado de resultados informáticos.
- Suplantación, sabotaje
- Virus, gusanos y bombas lógicas.
- Acceso no autorizado a Sistemas o Servicios de Información.
- Reproducción no autorizada de datos y/o programas informáticos con protección legal o derechos de autor.
- Producción / distribución / almacenamiento de contenidos ilícitos usando medios telemáticos.
- Extorsión y/o amenazas a través sistemas de comunicación informática.

En definitiva, cualquier delito que se pueda trasladar y aplicar al ciberespacio.

En la actualidad:

Aunque las fuerzas del orden cuentan en la actualidad con equipos especializados en delitos informáticos y de forma externa con expertos en la materia, los delitos relacionados se han multiplicado de forma alarmante. En los últimos años la información ha pasado de estar en papel a formato digital. Esto supone un cambio de mentalidad a nivel social. Los profesionales de la investigación han tenido que adaptarse a este cambio, esto es, en lo referente a la obtención de información, de pruebas.

¿Cuáles son los mayores problemas a los que nos enfrentamos?

- Falta de estándar en la recolección, recuperación y almacenamiento de pruebas y evidencias digitales.
- La gran mayoría de jueces y secretarios, no dominan esta materia y la lentitud en las actuaciones condiciona el estado de las pruebas.
- Los ataques a personas, empresas, e instituciones, en su mayoría, o no se detectan, o se detectan demasiado tarde, o las víctimas no quieren darle publicidad por lo que no se denuncia y no se investiga.
- Las sentencias condenatorias, no siempre conllevan la captura del delincuente por no estar al alcance de la justicia.

Continuará…

Por ML. Marín y equipo de mmv.es