RESUMEN

En el Ecuador se reconocen a los ataques informáticos como amenazas reales y de ejecución inmediata que vulneran la seguridad y disponibilidad de sistemas, procesos, e información contenida en equipos tecnológicos, teléfonos celulares, entre otros dispositivos que almacenen datos personales o confidenciales que pueden ser interceptados, robados, manipulados, reproducidos, o desviados por gente conocedora del área informática para el mal uso de la información obtenida.

Los ataques y estrategias de invasión a la privacidad van siendo perfeccionados día tras día, lo cual ha generado en las personas, gobiernos e instituciones la necesidad de desarrollar organismos especializados en la operación y gestión de incidentes de seguridad llamados CSIRT (Equipo de Respuestas Ante Incidentes de Seguridad Informáticos), como una respuesta eficaz ante los nuevos riesgos y amenazas, que incluyen a la Informática Forense, como un área especializada que integra conceptos de seguridad, procedimientos y metodologías para el procesamiento de evidencias mediante el adecuado uso de la cadena de custodia, permitiendo a los investigadores el análisis de los vestigios e indicios informáticos recopilados en la escena, empleando equipamiento informático forense especializado, metodologías, y procedimientos legalmente establecidos, que permitan la recopilación y protección de los indicios obtenidos que pueden llegar a ser evidencias sustentables o probatorias, para el descubrimiento de los infractores, quienes posteriormente serán procesados en juicios basados en la Ley.

Palabras Clave: Equipo de Respuesta Ante Incidentes de Seguridad Informáticos (CSIRT), Informática Forense, activos informáticos, ataques informáticos, almacenamiento, amenazas, evidencias, cadena de custodia, indicios, infractores, registros, sistemas, vulnerabilidad de sistemas.