TEMA: PROPUESTA DE UN MODELO PARA ANALISIS FORENSE A DISPOSITIVOS MOVILES CON SISTEMA OPERATIVO ANDROID.

Resumen

El crecimiento vertiginoso que está teniendo el uso de dispositivos móviles con Sistema Operativo Android es importante, debido a la multifuncionalidad y portabilidad se han convertido en una herramienta poderosa, enfocándose en el mundo de los negocios en línea; mejorando la productividad en las organizaciones públicas y privadas; la conectividad con amigos, familiares, clientes, jefes, empleados, reuniones de negocio; las actividades con el sector financiero; las actividades laborales, académicas, diversión y entretenimiento. Debido a esto, los dispositivos móviles son vulnerables al cibercrimen por tanto pueden estar involucrados en una investigación; por otro lado la carencia de organismos locales e internacionales que regulen y controlen el uso de dispositivos móviles; la falta de parámetros, modelos, procesos y procedimientos metodológicos; la falta de conocimiento en cuanto a las vulnerabilidades que los aplicativos poseen, crea la necesidad de cumplir con un objetivo fundamental en la presente investigación que es realizar un análisis forense a dispositivos móviles con Sistema Operativo Android basándonos en lineamientos de la cadena de custodia, cumplimientos etapas y fases establecidas y así detectar hallazgos; no conformidades; localizar vulnerabilidades y determinar cuáles fueron las causas principales de los diferentes tipos de eventos o delitos realizados desde un dispositivo móvil. Además mediante un Cuadro de Mando Integral (CMI) se evalúa indicadores o métricas enfocadas desde la perspectiva del Proceso y del Cliente, brindando un seguimiento frecuente en un tablero RGY – Sistema de Semáforos.

Palabras clave: DISPOSITIVO MÓVIL, ANDROID, ANÁLISIS FORENSE, CADENA DE CUSTODIA, CUADRO DE MANDO INTEGRAL.

Abstract

The huge growth that is having to use of mobile devices with Android Operating System is important due to the multifunctionality and portability, these have become a powerful tool, focusing on the world of online business; improving the productivity in public and private organizations; the connectivity with friends, family, clients, bosses, employees, business meetings; activities with the financial sector; industrial, academic, fun and entertainment. Because of this, mobile devices are vulnerable to the cybercrime therefore they may be involved in an investigation; on the other hand the lack of local and international agencies that regulate and control the use of mobile devices; the lack of parameters, models, processes and methodological procedures; the lack of knowledge about the vulnerabilities that the applications have create the need to meet a key objective of this research that is to conduct a forensic analysis to mobile devices with Android Operating System based on guidelines of the chain of custody, compliance stages and phases and thus to detect established findings; disagreements; locate vulnerabilities and determine what were the main causes of the different types of events or crimes made from a mobile device. Using a Balanced Scorecard evaluate indicators or metrics focused from the perspective of the Process and the Client, providing frequent monitoring by Traffic System.

Key words: MOBILE DEVICE, ANDROID, FORENSIC ANALYSIS, CHAIN OF CUSTODY, SCORECARD.