RESUMEN DE LA TESIS

ANÁLISIS FORENSE A PAQUETES DE DATOS EN LA RED LAN DE LA UNIVERSIDAD TECNOLÓGICA EQUINOCCIAL COMO APORTE AL CUMPLIMIENTO DE LAS NORMAS PCI-DSS

Este trabajo no solo representa un análisis forense al interior de la Universidad Tecnológica Equinoccial, sino también una idea aproximada del estado actual en el que se encuentra la institución educativa como institución participante en el procesamiento, transmisión o almacenamiento de información de tarjetas de crédito en la aplicación del estándar Payment Card Industry – Data Security Standard (PCI - DSS), la cual tiene como finalidad la reducción del fraude relacionado con las tarjetas de crédito e incrementar la seguridad de estos datos. Previamente se realizó una evaluación en base a los requisitos que expone la norma para determinar el nivel de cumplimiento de la institución a nivel general de todos los controles de la norma PCI – DSS, teniendo en cuenta que el estándar se compone de controles físicos, lógicos y documentales. Luego del cual se realizó una búsqueda potencial de datos de tarjetas de crédito siendo esta la labor más importante ya que el núcleo del estándar es la protección de datos de tarjetas de crédito procesados, almacenados o transmitidos a través de la red, para lo cual se utilizó herramientas OpenSource para la identificación de datos de tarjeta de crédito en tráfico a través de la red LAN no cifrados ni encriptados con lo cual se determinó que la institución no cumple diferentes requisitos de la norma. Finalmente se generó un plan de acción basados en la norma para la ejecución dentro de la Universidad y gestionar los riesgos identificados.

ABSTRACT

This work represents not only a forensic analysis into the Universidad Tecnológica Equinoccial but also a rough idea of the current state of the educative institution, as a participant institution in the processing, transmission, or storage of information related to credit cards, in the application of the standard Payment Card Industry – Data Security Standard (PCI-DSS), which has the purpose of reducing credit card fraud and increasing data security. An evaluation based on the requisites set by the standard was previously done to determine the level of attainment of the institution on a general level to all the controls of the norm PCI – DSS, taking in consideration that this standard consists of physical, logical, and documental controls. A potential research of credit card data was then done as this was the most important task since the main focus of the standard is the protection of credit card data that has been processed, stored, or transmitted through the internet. OpenSource tools were used to identify non-encoded and unencrypted credit card data that was trafficking through the LAN; it was then determined that the Institution does not comply with several requisites of the norm. Finally, a plan of action based on the standards was made to be executed within the University and to manage the identified risks.