RESUMEN

En Ecuador las entidades bancarias realizan grandes inversiones en infraestructura tecnológica encaminadas a disminuir los delitos financieros, sin embargo el porcentaje de delitos financieros no ha disminuido sino al contrario se han incrementado y la adopción de un estándar de seguridad de datos se convierte en la opción más importante a ser implementada a fin de elevar el nivel de seguridad y reducir el riesgo de pérdida de información de las tarjetas de pago sean de débito o crédito para mantener la fidelidad de sus clientes. PCI DSS es un estándar de seguridad de obligatorio cumplimiento para todas aquellas entidades que procesen, transmitan o almacenen información de tarjetas de pago, y por tanto las soluciones tecnológicas implementadas o a implementar en una entidad bancaria deben cumplir con los 12 requisitos descritos en 296 controles. El modelo de factibilidad para el cumplimiento de PCI DSS pretende guiar a todo el personal de IT para que las soluciones tecnológicas sean planteadas orientadas a cumplir los requisitos que establece PCI DSS, detalla recomendaciones técnicas, las organizaciones dependientes en el proceso, la información sobre sitios relacionados con el proceso y el análisis de justificación de la inversión que se debe realizar para obtener la certificación; pretendiendo que el momento que la entidad financiera inicie el proceso formal de certificación pueda reducir el tiempo y los costos que involucra dado que al contratar un asesor especializado QSA (Qualified Security Assessor) este realice un menor número de observaciones y cambios a ejecutar.

Palabras Claves:

- **PCI DSS**
- **SEGURIDAD EN TARJETAS DE PAGO**
- **ESTÁNDAR DE SEGURIDAD**
- **DELITOS FINANCIEROS**
- **FIREWALL PERIMETRAL**

ABSTRACT

At the Equator Banks entities, make invest heavy in technology infrastructure focus to reduce financial crime, however the percentage of financial crime hasn´t decreased. Instead that the adoption of a safety standard data becomes more important to be implemented. These do to get a safety level and risk reduction of information loss. Over all in payment cards, debit or credit card, which ensure maintain customer loyalty increasing incidents of security related to payment cards, and also the exponential growth of commercial banking transactions and the plastic makes the PCI DSS (Payment Card Industry Data Security Standard) certification one of the most important security requirements for the banking and commercial sector.

PCI DSS is a security standard mandatory for all entities that process, transmit or store payment card information, and therefore technological solutions implemented or to be implemented in a bank must comply with the 12 requirements outlined in 296 controls. The feasibility model for compliance with PCI DSS is intended to guide all IT staff for technological solutions are raised to comply the requirements of PCI DSS, Also, this detailed technical recommendations, depending of organizations in the process, Additional to this the information on sites related to the process and analysis to justify the investment must be performed to obtain certification. All of those is with the aim of financial institution initiate the formal certification process and can reduce the time and costs involved since to hire a consultant specialized QSA (Qualified Security Assessor) that make fewer comments and updates to run.

Key words:

- **PCI DSS**
- **SECURITY OF PAYMENT CARD**
- **SECURITY STANDARD**
- **FINANCIAL CRIMES**
- **PERIMETER FIREWALL**