UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Ingeniería en Sistemas Computacionales

IMPLEMENTACIÓN DE LA NORMATIVA INTERNACIONAL PCI-DSS, PARA LA SEGURIDAD DE CAJEROS AUTOMÁTICOS DE LA CARTERA DE CLIENTES DE LA EMPRESA GREENETICS SOLUCIONES S.A.

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS COMPUTACIONALES

AUTOR:
Diego Javier Suárez Chuquín

DIRECTORA:
Msc. Daisy Elizabeth Imbaquingo Esparza

Ibarra, 2020

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

Datos de Contacto			
Cédula de Identidad:	171852191-5		
Apellidos y Nombres:	Suárez Chuquín Diego Javier		
Dirección:	San Antonio de Ibarra, calle Ramón Teanga y Ezequiel Rivadeneira, N° 7-41		
Email:	djsuarez@utn.edu.ec		
Teléfono Fijo:	06 2 550 124	**Teléfono Móvil:**	0984985217

Datos de la Obra	
Título:	IMPLEMENTACIÓN DE LA NORMATIVA INTERNACIONAL PCI-DSS, PARA LA SEGURIDAD DE CAJEROS AUTOMÁTICOS DE LA CARTERA DE CLIENTES DE LA EMPRESA GREENETICS SOLUCIONES S.A.
Autor:	Suárez Chuquín Diego Javier
Fecha:	07 de febrero del 2020
Programa:	Pregrado
Título por el que Opta:	Ingeniero en Sistemas Computacionales
Director:	Msc. Daisy Imbaquingo

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 7 días del mes de febrero de 2020.

Diego Javier Suárez Chuquín
CI: 171852191-5

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

Ibarra, 7 de febrero 2020

CERTIFICACIÓN DIRECTOR

Por medio del presente, yo Msc. Daisy Imbaquingo, certifico que el Sr. Diego Javier Suárez Chuquín, portador de la cédula de identidad Nro.171852191-5. Ha trabajo en el desarrollo del proyecto de grado denominado: **"IMPLEMENTACIÓN DE LA NORMATIVA INTERNACIONAL PCI-DSS, PARA LA SEGURIDAD DE CAJEROS AUTOMÁTICOS DE LA CARTERA DE CLIENTES DE LA EMPRESA GREENETICS SOLUCIONES S.A."**, previo a la obtención del título de Ingeniero en Sistemas Computacionales, lo cual ha realizado en su totalidad con responsabilidad y esmero.

Es todo en cuanto puedo certificar en honor a la verdad.

Atentamente,

MSc. Daisy Imbaquingo

DIRECTORA DE TESIS

GREENETICS SOLUCIONES S.A.
RUC: 1792509920001
PBX: (+593) 2 603-4068

Quito, Febrero 07 del 2020

Yo, Marco Rivadeneira con cédula de ciudadanía N° 1720995883, en calidad de Representante Legal de la Empresa Greenetics Soluciones S.A. con Ruc No. 1792509920001, certifico que el Señor Diego Javier Suárez Chuquín con cédula de ciudadanía No. 171852191-5, hizo la entrega de su tema de Tesis "IMPLEMENTACIÓN DE LA NORMATIVA INTERNACIONAL PCI-DSS, PARA LA SEGURIDAD DE CAJEROS AUTOMÁTICOS DE LA CARTERA DE CLIENTES DE LA EMPRESA GREENETICS SOLUCIONES S.A.", tomando la empresa como documento entregado correcta y satisfactoriamente.

Es todo cuanto puedo certificar en honor a la verdad pudiendo el interesado hacer uso del presente certificado como estime conveniente.

Atentamente;

Ing. Marco Rivadeneira
REPRESENTANTE LEGAL
GREENETICS SOLUCIONES S.A.

Dedicatoria

Este Trabajo de Titulación está dedicado a mis padres: Jorge Suárez y Bertha Chuquín, quienes, con su amor, paciencia y apoyo absoluto, han estado siempre, guiándome e incentivándome para seguir adelante. A mis hermanos, sobrinos por siempre estar ahí dándome su apoyo incondicional.

También dedico a todas las personas que estuvieron apoyándome moralmente en todo instante, hasta alcanzar esta meta tan anhelada.

Agradecimiento

En primer lugar, quiero dar gracias a dios, por darme salud, sabiduría y paciencia, ya que sin su bendición diaria nada de esto hubiese sido posible.

A mis padres, hermanos, sobrinos, quienes confiaron en mí y me apoyaron en todo momento, durante el transcurso de mi vida estudiantil.

A la Universidad Técnica del Norte en especial a la Facultad de Ingeniería en Ciencias Aplicadas (FICA), porque en sus aulas recibí valiosos conocimientos y pasé los más bellos e inolvidables recuerdos.

A mis maestros, que con nobleza y entusiasmo vertieron en mí el conocimiento impartido en las aulas de clases.

Quiero extender un agradecimiento especial a mí tutora de trabajo de titulación, Msc. Daisy Imbaquingo, por darme la confianza, apoyo y guiarme, desde el inicio hasta la culminación del trabajo de titulación.

A la empresa GREENETICS soluciones S.A. por darme todas las facilidades en el desarrollo de mi trabajo de titulación brindándome la apertura necesaria en los procesos requeridos, especialmente al MSc. Marco Rivadeneira, por impartirme sus conocimientos y su aporte profesional para la implementación de este trabajo.

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Resumen

La presente investigación se basa en el estudio de la Normativa Internacional PCI DSS, para la seguridad de cajeros automáticos del sector financiero ecuatoriano, definiendo una serie de requisitos que deben cumplir las entidades bancarias para almacenar, procesar o transferir datos financieros. La normativa se encuentra enfocada a tarjetas de crédito, por tal motivo, la normativa PCI DSS conjuntamente con la PCI PTS permiten crean varios requisitos que deben cumplir los dispositivos para un óptimo funcionamiento, el principal objetivo es crear un estándar para auditar cajeros automáticos, tomando en cuenta los lineamientos del organismo regulador (SEPS - Superintendencia de Economía Popular y Solidaria) enfocado a los cajeros automáticos. El capítulo uno describe la teoría correspondiente a la normativa y los parámetros de control que debe implementarse en cada institución financiera para la seguridad en sus cajeros automáticos, el capítulo dos presenta el desarrollo de la normativa aplicada en un caso práctico, el capítulo tres se establece los resultados obtenidos en la implementación de la normativa PCI DSS/PTS.

Abstract

This research is based on the study of the International PCI Regulations for the security of ATMs in the Ecuadorian financial sector, defining a series of requirements that banks must meet to store, process or transfer financial data. The regulations are focused on credit cards, for this reason, the PCI DSS regulations together with the PCI PTS allow creating several requirements that devices must meet for optimal operation, the main objective is to create a standard for auditing ATMs, taking into account the guidelines of the regulatory body (SEPS - Superintendence of Popular and Solidarity Economy) focused on ATMs. Chapter one describes the theory corresponding to the regulations and the control parameters that must be implemented in each financial institution for the security of its ATMs, chapter two presents the development of the regulations applied in a practical case, chapter three establishes the results obtained in the implementation of the PCI DSS-PTS regulation

INTRODUCCIÓN

Antecedentes

La normativa internacional, Payment Card Industry Data Security Standar (PCI DSS), fue creada en el año 2006 por las compañías: VISA, MASTERCARD, AMERICAN EXPRESS, JCB Y DISCOVER. Esta metodología permite a las agencias bancarias tomar medidas de seguridad para salvaguardar información, de esta manera bajar el indice de fraudes relacionados con los cajeros automaticos y tarjetas de credito (ATMIA, 2014).

Ademas, la normativa está dirigida a entidades bancarias e instituciones que trabajen con datos de tarjetas de pago y cajeros automaticos, para salvaguardar la informacion de los usuarios, permitiendo a instituciones afectadas tomar sus debidas precauciones para no tener ningun tipo de problema con sus clientes (Acosta, 2008)(Clapper & Richmond, 2016).

En el 2014 la Superintendencia de Bancos del Ecuador adapta procedimientos internacionales para que las endidades financieras del pais apliquen la normativa y puedan tomar las debidas precauciones para asegurar la información que contienen de sus clientes (Vinicio & Sanchez, 2018).

Esta metodologia topa 6 plazas importantes de observación, que dominan 12 requerimientos de nivel superior para proteger la información(Acosta, 2008; ATMIA, 2014).

1. Construir y mantener una red segura.
    - Requisito 1.- Colocar y mantener una configuración de cortafuegos para preservar los datos de titulares de tarjetas.
    - Requisito 2.- No utilice los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
2. Proteger a tiulares de Tarjetas.
    - Requisito 3.- proteger los datos de titulares de tarjetas almacenados.
    - Requisito 4.- Cifrar la transmisión de los datos de titulares de tarjetas a través de redes públicas abiertas.
3. Mantener un programa de gestion de vulnerabilidad.
    - Requisito 5.- Proteger todos los sitemas contra malware y actualizar regularmente el software o programas antivirus.

- Requisito 6.- Desarrollar y mantener sistemas y aplicaciones seguras

4. Implementar medidas de control en accesos fuertes.
   - Requisito 7.- Restringir el acceso a los datos de titulares de tarjetas según necesidad-toknow.
   - Requisito 8.- Identificar y autentificar el acceso a los componentes del sistema.
   - Requisito 9.- Registrar el acceso físico a los datos de titulares de tarjetas.
5. Monitorear regularmente las redes de prueba.
   - Requisito 10.- Seguir y controlar todos los accesos a los recursos de red y datos de titulares de tarjetas.
   - Requisito 11.- Comprobar regularmente los sistemas y procesos de seguridad.
6. Mantener una politica de seguridad de la información.
   - Requisito12.- Mantener una politica que aborde la seguridad de la informacion para todo el personal.

GREENETICS SOLUCIONES S.A.

GREENETICS Soluciones S.A. es una empresa enfocada en brindar soluciones para seguridad de la información; contamos con una amplia experiencia en el área de Ciberseguridad, ofreciendo productos y servicios con plataformas avanzadas en protección contra amenazas, pérdida de datos, robo de información, suplantación de identidad, análisis forense informático, etc. (Greenetics Soluciones S.A., 2018).

Asumimos la responsabilidad integral de supervisar y mantener la seguridad de su empresa. Escuchamos sus necesidades y aplicamos las soluciones que mejor se ajusten a sus requerimientos. Nuestra amplia experiencia en el área de Ciberseguridad y tecnología le permitirá implementar soluciones eficaces para abordar sus mayores desafíos de TI (Greenetics Soluciones S.A., 2018).

Situación Actual

Los cajeros automáticos que tienen a su disposición las agencias bancarias para el uso de sus clientes, deben estar rotuladas de manera que los clientes puedan reconocer fácilmente que pertenece a su entidad financiera y que está sujeta al esquema tarifario que ofrece la institución (SBIF, 2018).

Para saber el horario de atención de los cajeros automáticos, únicamente deben ser reportados por los que se encuentran identificados y pertenecen a la agencia bancaria reconocida, el código de punto de atención es designado por la Superintendencia de Bancos caso contrario estos deben ser reportados (SBIF, 2018).

Los ciberdelincuentes realizan estafas a nivel nacional clonando tarjetas de credito vulnerando cajeros automaticos, realizando hurtos millonarios que han perjudicado a miles de clientes, muchos cajeros automaticos no cuentan con una infraestructura adecuada que permita a los usuarios realizar transacciones de manera segura (Telégrafo, 2012).

Prospectiva

Mediante la implementación de la normativa internacional PCI DSS, las agencias bancarias del país asociadas a la empresa GREENETICS Soluciones S.A., tomarán medidas de seguridad en cajeros automáticos, para brindar un servicio de calidad y salvaguardar la integridad de sus clientes, realizando mejoras en infraestructura, seguridades de red, entre otros.

Permitiendo de esta manera llevar un control eficiente de la seguridad e integridad de la infraestructura de cajeros automáticos como de sus usuarios, fomentando una cultura de seguridad en el sector financiero ecuatoriano logrando la mejora continua en sus procesos, procedimientos y normativa vigente.

Planteamiento del Problema

Falta de evaluación de seguridad en cajeros automáticos, utilizando un estándar Internacional en la cartera de clientes de la empresa GREENETICS Soluciones S.A.

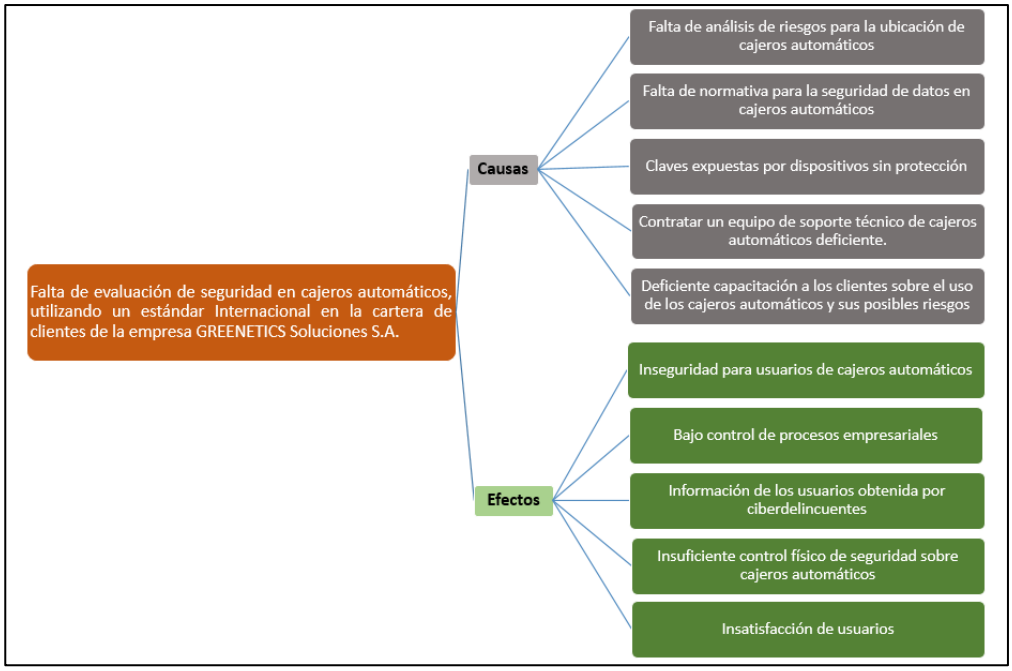


Fig. 1. Planteamiento del problema
Fuente: Propia

Actualmente, las agencias bancarias del país, no brindan un servicio de calidad en cajeros automáticos, exponen la integridad de sus clientes por no cumplir con una normativa específica que permita a las organizaciones llevar un control de los mismos, para que la información no sea vulnerada por ciberdelincuentes (Joel Meléndez Verdezoto, 2008). En muchos casos que han sido de conocimiento público se muestran falencias de seguridad que tienen dichos dispositivos, ya que los infractores poseen conocimientos muy avanzados sobre tecnologías de la información (TICs), (García Correa, García Camavilca, & Monzón Castillo, 2017).

Objetivos

Objetivo General

Implementar la normativa internacional PCI-DSS, para la seguridad de cajeros automáticos de la cartera de clientes de la empresa GREENETICS soluciones S.A.

Objetivos Específicos

- Construir el marco teórico como una línea base para la comprensión de la normativa internacional PCI DSS.
- Determinar los puntos vulnerables que deben considerarse como parte de un proceso de auditoría de seguridad de cajeros automáticos, aplicando la normativa internacional PCI DSS.

- Comprobar los resultados obtenidos de la normativa sobre los procesos de auditoría en cajeros automáticos de un cliente de la empresa GREENETICS Soluciones S.A.

Alcance

Implementación de la normativa internacional PCI DSS en procesos de auditoria de cajeros automáticos, para la cartera de clientes de la empresa GREENETICS Soluciones S.A., esta normativa será aplicada en un caso de estudio de un cliente de la empresa antes mencionada.

Expertos como (Acosta, 2008) y (García Correa et al., 2017) coinciden que los puntos a evaluar de la normativa internacional PCI DSS para cajeros automáticos son los siguientes:

- Objetivo 1.- Construir y mantener una red segura
- Objetivo 2.- Proteger titular de la tarjeta
- Objetivo 3.- Mantener un programa de gestión de vulnerabilidad
- Objetivo 4.- Implementar medidas de control en acceso fuertes
- Objetivo 5.- Monitorear regularmente y redes de prueba.
- Objetivo 6.- Mantener una política de seguridad de la información.

El cumplimiento de la normativa internacional PCI DSS modelo de mejora continua.

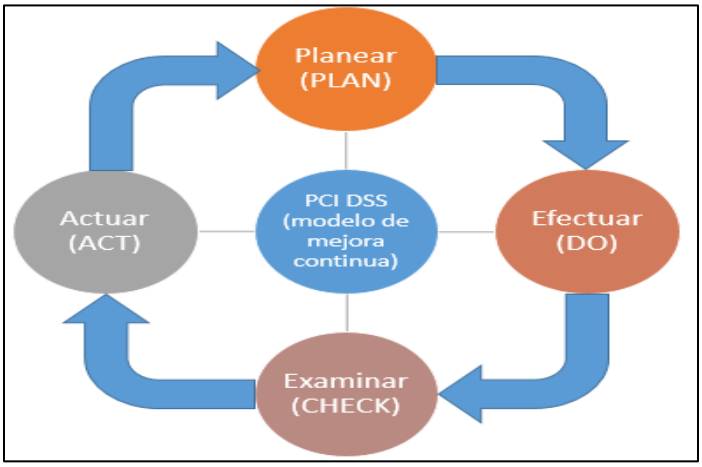


Fig. 2. Cumplimiento de la PCI DSS, modelo de mejora continua
Fuente: Propia

Como se ilustra en la Fig. 2. El proceso para la implementación de una metodología utilizando la normativa internacional PCI DSS, será efectuada empleando el Ciclo de “Derming” (Acosta, 2008). Consiste en la mejora continua de calidad siguiendo cuatro pasos repetitivos, es muy práctico para realizar una metodología de seguridad en los procesos de auditoría para cajeros automáticos (Garc, 2013).

Justificación

Esta investigación tiene como objetivo encontrar vulnerabilidades en cajeros automáticos que poseen los clientes de la empresa GEENETICS Soluciones S.A., aplicando la normativa internacional PCI DSS en procesos de auditoria de los cajeros automáticos. Al final de la evaluación se les dará a conocer a las organizaciones los resultados de la evaluación para que tomen las respectivas medidas de seguridad ante los puntos sensibles evaluados.

La implementación consiste en garantizar que los cajeros automáticos, estén resguardados mediante puntos de evaluación en el software y hardware, para evitar ataques de Ciberdelincuentes con la finalidad de salvaguardar la integridad de los usuarios de estos dispositivos, al mismo tiempo, disminuir las pérdidas económicas y capacitar al personal técnico de las instituciones que pertenecen a la cartera de clientes de la empresa GREENETICS soluciones S.A.

CAPITULO I

Marco teórico

1.1. Empresa Greenetics soluciones S.A

Greenetics Soluciones S.A. es una empresa enfocada en brindar soluciones para seguridad de la información; cuenta con una amplia experiencia en el área de Ciberseguridad, ofreciendo productos y servicios con plataformas avanzadas en protección contra amenazas, pérdida de datos, robo de información, suplantación de identidad, análisis forense informático, entre otros.

Asumen la responsabilidad integral de supervisar y mantener la seguridad de su empresa. Escuchan las necesidades y aplican las soluciones que mejor se ajusten a sus requerimientos. La amplia experiencia en el área de Ciberseguridad y tecnología le permite brinda opciones eficaces para abordar los mayores desafíos de TI.

1.2. Misión

Greenetics es una empresa que brinda soluciones tecnológicas confiables con énfasis en la seguridad de la información, que contribuyen al desarrollo empresarial de sus clientes, proporcionando herramientas integrales que garanticen la operación de sus sistemas (Greenetics Soluciones S.A., 2018).

1.3. Visión

Ser una empresa líder en el sector tecnológico, con presencia y liderazgo nacional e internacional; posicionarnos con excelencia en ventas de soluciones tecnológicas y de ciberseguridad, con énfasis en el mejoramiento continuo de procesos de interés para nuestros clientes, comprometidos con nuestro recurso humano, la sostenibilidad del medio ambiente y la contribución de la evolución de las sociedades (Greenetics Soluciones S.A., 2018).

1.4. Catálogo de servicios

Los principales servicios que la empresa ofrece a sus clientes se basan en la Seguridad de la información, ya que es un tema que día a día va tomando más protagonismo, convirtiéndose en una necesidad para las empresas y organizaciones (Greenetics Soluciones S.A., 2018).

Consciente de la importancia de proteger la información, GREENETICS tiene como uno de sus principales objetivos, ofrecer a sus clientes soluciones profesionales para el aseguramiento de la información y enmarcadas siguiendo la metodología PMO, las cuales trabajen de forma modular e integral, apoyados principalmente en los siguientes servicios especializados: (Greenetics Soluciones S.A., 2018).

Ofrece una serie de cursos, talleres y seminarios en la modalidad de educación 100% presencial, los cuales tienen diversos objetivos, alcances y orientación en la Seguridad de la Información. Los cursos de formación que se ofrecen de manera recurrente y bajo demanda se ilustra en la TABLA 1.1 detalladamente.

TABLA 1.1
Catálogo de productos de la empresa GREENETICS Soluciones S.A

Productos	Servicios
Análisis de vulnerabilidades	• Gestión de la seguridad. • Evaluación de la seguridad. • Fraude. • Continuidad de negocios. • Compliance. • Evaluación de la seguridad.
Cumplimiento de Normativa y Estándares	• Recuperación de datos digitales y particiones borrados. • Tomas de imágenes de Discos duros. • Investigación y evidencia digital (Evidencia Lógica). • Estenografía. • Investigación de Logs y Bitácoras. • Respuesta a Incidentes de Seguridad. • Análisis y Extracción de datos digitales. • Borrado permanente de Datos Digitales (Para que sean irrecuperables). • Recuperación de contraseñas usando técnicas de fuerza bruta o Diccionario. • Cálculos de Integridad en la información Digital. • Autoría informática y dictámenes técnicos ante incidentes relacionados con la seguridad de la información digital.

Procesos de Negocio RISK	• Montaje de SGSI (Sistemas de Gestión de Seguridad de la Información).
	• Análisis Integral, y tratamiento de Riesgos.
	• Implementación de Políticas de Seguridad.
	• Implementación y mantenimiento de Planes de Continuidad del Negocio BCM-BCP:
	  ◦ (Business Continuity Management).
	  ◦ (Business Continuity Planning).
	• Documentación del SGSI (Instructivos, Planes, Procedimientos, Alcance).

Gestión de la seguridad	• Auditorías Internas al SGSI (Sistemas de Gestión de Seguridad de la Información). • Detección y Respuestas a Incidentes. • Orientación hacia la Certificación del SGSI hacia abajo la NTC-ISO 27001. • Gestión de Cumplimiento. • Adquisición de sistemas de seguridad perimetrales a la medida. • Implementación y mantenimientos de SGSI (Sistemas de Gestión de Seguridad de la Información). • Análisis y tratamiento de Riesgos Tecnológicos. • Software propietario y de código abierto (Open Source) relacionado con seguridad tecnológica. • Certificaciones en seguridad informática y auditoria de sistemas. • Normas relacionadas con certificaciones de SGSI y buenas prácticas de seguridad informática. • Seguridad y Legalidad (Normatividades Jurídicas relacionadas con seguridad de la información). • Impactos y cuidados ante pruebas de penetración del tipo Ethical Hacking.

Procesos del negocio	• Montaje de SGSI (Sistemas de Gestión de Seguridad de la Información).
	• Análisis Integral, y tratamiento de Riesgos.
	• Implementación de Políticas de Seguridad.
	• Implementación y mantenimiento de Planes de Continuidad del Negocio BCM-BCP:
	  • (Business Continuity Management).
	  • (Business Continuity Planning).
	• Documentación del SGSI (Instructivos, Planes, Procedimientos, Alcance).
	• Auditorías Internas al SGSI (Sistemas de Gestión de Seguridad de la Información).
	• Detección y Respuestas a Incidentes.
	• Orientación hacia la Certificación del SGSI hacia abajo la NTC-ISO 27001.
	• Gestión de Cumplimiento.

CSIRT	• Gestión de incidentes informáticos. • Alertas y comunicados. • Monitoreo en tiempo real.
Análisis forense informático	• Recuperación de datos digitales y particiones borrados. • Tomas de imágenes de Discos duros. • Investigación y evidencia digital (Evidencia Lógica). • Estenografía. • Investigación de Logs y Bitácoras. • Respuesta a Incidentes de Seguridad. • Análisis y Extracción de datos digitales. • Borrado permanente de Datos Digitales (Para que sean irrecuperables). • Recuperación de contraseñas usando técnicas de fuerza bruta o Diccionario. • Cálculos de Integridad en la información Digital. • Autoría informática y dictámenes técnicos ante incidentes relacionados con la seguridad de la información digital.

Respuesta a incidentes	• Montaje de SGSI (Sistemas de Gestión de Seguridad de la Información).
	• Análisis Integral, y tratamiento de Riesgos.
	• Implementación de Políticas de Seguridad.
	• Implementación y mantenimiento de Planes de Continuidad del Negocio BCM-BCP:
	  • (Business Continuity Management).
	  • (Business Continuity Planning).
	• Documentación del SGSI (Instructivos, Planes, Procedimientos, Alcance).
	• Auditorías Internas al SGSI (Sistemas de Gestión de Seguridad de la Información).
	• Detección y Respuestas a Incidentes.
	• Orientación hacia la Certificación del SGSI hacia abajo la NTC-ISO 27001.
	• Gestión de Cumplimiento.

Capacitación	• Curso de Hacking Ético (Ethical Hacking). • Curso de Informática Forense. • Manejo de Kali Linux 2.0. • Instalación y aseguramiento de centrales IP-PBX. • Hacking Web. • Hacking Wireless. • Ingeniería Reversa y Análisis de Malware. • Taller de Seguridad Informática usando Software Libre. • Taller de Análisis de Vulnerabilidades. • ISO 27001. • Curso de oficial de Seguridad Informática.

Fuente: (Greenetics Soluciones S.A., 2018).

1.5. Sistema financiero ecuatoriano

Es un conjunto de organismos instituciones y entidades regulados por principios y normas legales, constitucionales y reglamentarias, que tiene como fin conseguir el desarrollo ordenado y equilibrado de la economía del país canalizando los recursos de las familias ecuatorianas, facilitando todos los beneficios acciones para lograr este objetivo (Andrade, 2003).

Según (Andrade, 2003). El sistema Financiero Ecuatoriano se encargan de facilitar los medios económicos para conseguir el desarrollo de la población, reduciendo la tasa de desempleo, la estabilidad de precios, el saldo positivo en la balanza de pago y una equilibrada distribución económica de los ingresos de las organizaciones, con la finalidad de que la población ecuatoriana no sea afectada por algún desfase en la economía del país.

Para el cumplimiento de objetivos del sistema financiero ecuatoriano dispone de funciones y responsabilidades en instituciones del sector público y privado como las entidades de supervisión y control social que son organismos técnicos de vigilancia, auditoria, intervención y control de actividades económicas, sociales y ambientales (Cooke, 2017).

Según (Cooke, 2017). Las superintendencias son los organismos que se encargan de controlar servicios de entidades públicas y privadas, así como ordenamientos legales de interés general, ellos procederán por gestión o exigencia ciudadana, por esta razón las superintendencias son las que auditaran, vigilaran y llevaran el control de las áreas que requieran ser inspeccionadas.

1.6. Superintendencia de Bancos (SB)

La Superintendencia de Bancos en el Ecuador es el organismo delegado de la inspección, frecuente del sistema financiero del país, regula que las entidades bancarias cumplan con estatutos de protección a los usuarios, permitiendo de esta manera confianza este organismo importante para el país, la Constitución de la República establece su relevancia en el siguiente artículo: (Bertha Romero, 2015).

> **Art. 309.** el sistema financiero se compone de los sectores público privado y del popular y solidario, que intermedian recursos del público. Cada uno de estos sectores contará con normas y entidades de control específicas y diferenciadas, que se encargarán de preservar su seguridad, estabilidad, transparencia y solidez. Estas entidades serán autónomas. Los directivos de las entidades de control serán responsables administrativa, civil y penalmente por sus decisiones (Junta de regulación monetaria y financiera, 2015).

La Superintendencia de Bancos (SB) aplica compendios de transparencia encargada de hacer oficial la indagación sobre estados financieros, tasas de interés, tarifas por servicios, estadísticas, leyes, normativas y brinda educación financiera (Bertha Romero, 2015).

En la TABLA 1.2, la autora (Bertha Romero, 2015). Indica que la Superintendencia de Bancos tiene el siguiente rol y funciones:

TABLA 1.2
Rol y funciones de la Superintendencia de Bancos

Rol	Funciones
El Estado quien es el encargado de velar por los derechos de los ciudadanos requiere de un ente de control para que vigile que las entidades financieras realicen las operaciones en cumplimiento de la ley, de esta manera garantizar los derechos de los habitantes.	Resguardar el logro habitual del contorno económico. Cuidar la seguridad, firmeza y delicada labor de los organismos sujetos a su control y en general que cumplan la norma que rige su funcionamiento. Pedir que las entidades intervenidas presenten y acojan las oportunas medidas correctivas y de reparación en los casos que así lo soliciten. Obtener y anunciar por lo menos trimestralmente el boletín de información financiera.

Fuente: (Bertha Romero, 2015).

1.7. Superintendencia de Economía Popular y Solidaria (SEPS)

La Superintendencia de Economía Popular y Solidaria (SEPS) es una entidad técnica de control con responsabilidad jurídica, se basa en normas para el correcto funcionamiento de las organizaciones, buscando el desarrollo, estabilidad, solidez y correcto funcionamiento del sector financiero, popular y solidario (SEPS, 2019).

Art 283. define al sistema económico como "social y solidario, que reconoce al ser humano como sujeto y fin; [que] propende a una relación dinámica y equilibrada entre sociedad, Estado y mercado, en armonía con la naturaleza; y [que] tiene por objetivo garantizar la producción y reproducción de las condiciones materiales e inmateriales que posibiliten el buen vivir". En concordancia a la Constitución, la Ley de Economía de Popular y Solidaria tiene por objeto: (SEPS, 2019).

- Reconocer a las organizaciones de la economía popular y solidaria como motor del desarrollo del país.
- Promover los principios de la cooperación, democracia, reciprocidad y solidaridad en las actividades económicas que realizan las organizaciones de la EPS.
- Velar por la estabilidad, solidez y correcto funcionamiento de las organizaciones de la EPS; Establecer mecanismos de rendición de cuentas de los directivos hacia los socios y miembros de las organizaciones de la economía popular y solidaria.
- Impulsar la participación activa de los socios y miembros en el control y toma de decisiones dentro de sus organizaciones, a diferencia de las actividades económicas privadas
- Identificar nuevos desafíos para el diseño de políticas públicas que beneficien, fortalezcan y consoliden al sector económico popular y solidario.
- Fortalecer la gestión de las organizaciones en beneficio de sus integrantes y la comunidad.

1.8. Seguridad bancaria en el Ecuador

La asociación de bancos privados del Ecuador tiene una gran preocupación por las entidades financieras, depositantes y beneficiarios en general, por tal motivo la banca en el ecuador se ha enfocado en implementar diversas medidas de seguridad para salvaguardar la integridad de sus clientes e Instituciones (Bancos Privados del Ecuador, 2015).

En el 2011 la Superintendencia de Bancos a través de la resolución 1851, estableció medidas de seguridad que las agencias bancarias debían cumplir a cabalidad, se implantaron las siguientes ordenanzas, mantenimiento de guardias de seguridad, espacios iluminados, sistema de vigilancia, puertas con cerradura y llaves cifradas, manuales de seguridad, políticas de protección y sistemas de seguridad acorde a las necesidades de los establecimientos bancarios (Bancos Privados del Ecuador, 2015).

1.9. Vulnerabilidades y Fraudes

Para poder entender el significado de vulnerabilidad y fraude, a continuación, se encuentran definidas como se ilustra en la TABLA 1.3, para tener una idea clara de estos términos que serán utilizados en el documento,

TABLA 1.3
Definición de vulnerabilidad y fraude

Palabras	Definición
Vulnerabilidad	Es el riesgo que un apersona, sistema u objeto puede sufrir frente a peligros inminentes, sean estos desastres naturales, desigualdades económicas, políticas, sociales o culturales. La palabra vulnerabilidad deriva del latín vulnerabilis Está compuesto por vulnus, que significa 'herida', y el sufijo abilis, que indica posibilidad; por lo tanto, etimológicamente, vulnerabilidad indica una mayor probabilidad de ser herido
Fraude	Es sinónimo de engaño, inexactitud consciente contra una persona u institución para obtener algún aprovecho, mientras que la otra parte es la perjudicada. La palabra fraude es de origen latín "fraus".

Fuente: (Significados, 2013).

En la TABLA 1.4, se encuentran los tipos de fraudes cometidos por Ciberdelincuentes, ellos se encargan de utilizar la tecnología para cometer estafas, por este motivo las instituciones financieras como sus clientes deben estar conscientes que están expuestos a este tipo de peligros (Esther & López, 2012).

TABLA 1.4
Tipos de Fraudes Electrónicos

Fraudes conocidos	Descripción
Fraude relacionado con claves	Los delincuentes realizan transferencias bancarias de clientes a otras cuentas para luego realizar retiros en efectivo.
Ofertas en páginas web	Ofrecen productos o servicios en la web que no existen.
Suplantación de identidad	Los delincuentes abren cuentas y realizan transferencias bancarias, a nombre de personas que han hurtado una cedula de identidad o pasaporte.
Phishing	Los delincuentes obtienen información confidencial a través de un correo electrónico, para obtener la información de los usuarios haciéndoles creer que es actualización de datos. Otra manera es suplantando la página web de una institución financiera por otra parecida.
Phaming	Es parecida a la anterior, pero en esta modalidad el delincuente re-direcciona al usuario, le envía a una página que se ve muy parecida a la original para de esta manera substraer la información del usuario.
Malware	El malware, los troyanos y keyloggers son todos programas utilizados para fines delictivos, como aquellos que son perfilados para captar y grabar las teclas que son digitadas por los usuarios en una página web.
Skimming	Al momento que un usuario entrega la tarjeta en un local comercial, el delincuente pasa por un aparato llamado skimmer que graba la información de la banda de la tarjeta y luego la clona en una tarjeta falsa.
Estafa piramidal	La estafa piramidal, el hoax y la carta nigeriana, se distribuyen por correo electrónico y tratan de convencer al usuario, que entregando una suma de dinero o su clave electrónica, obtendrán grandes ganancias a través de una red social donde aportan muchas personas.

Fuente: (Esther & López, 2012).

Actualmente existen muchos tipos de estafas electrónicas, permiten a los delincuentes mediante la tecnología cometer hurtos a usuarios de agencias bancarias sin que se den cuenta de lo sucedido, puesto que algunas organizaciones no cuentan con la debida seguridad para mantener la información de sus clientes resguardada, así como su integridad por no cumplir con algunas normas de seguridad establecidas por Superintendencia de Bancos del Ecuador.

1.10. Historia de cajeros automáticos.

El 27 de junio de 1967, en la ciudad de Londres se da origina el primer cajero automático que proporcionaba billetes a los usuarios de agencias bancarias, ideada por John Shepherd-Barron, el inventor elaboró seis distribuidores de billetes e integró luces en los nuevos modelos, lo que permitió que muchos clientes puedan retirar dinero a cualquier hora del día sin largas filas en los bancos (BBC Mundo, 2017).

La primera máquina era capaz de detectar los cheques que eran impregnados de carbono 14, para que sean reconocidos y cobrados con el valor que el documento contenía, luego de un tiempo el científico tiene una nueva idea correspondiente a la seguridad que debe implementarse en los dispositivos, estableciendo un pin de seguridad de 4 dígitos, que hasta la fecha se ha convertido en un estándar a nivel mundial (BBC Mundo, 2017).

En Ecuador el año de 1979 el Banco del Pacifico es la primera institución en instalar el primer cajero automático a nivel nacional, también convirtiéndose en el primer cajero en línea en toda américa del sur, actualmente existen varios cajeros automáticos de diferentes bancos en el país (Banco Pacifico, 2019).

En el año de 1994, once bancos del Ecuador y una administradora de tarjetas como son: REDBANC S.A. y MULTIRED CIA LTDA., deciden fusionarse y mejorar la gran red de cajeros automáticos que actualmente es BANRED (Patlán Pérez & Martínez Torres, 2017).

Es la Red Interbancaria más grande del Ecuador que permite la comunicación entre varias entidades financieras. Entre las principales funciones que permite hoy en día es las transferencias interbancarias online, migración a tarjetas con CHIP para dar una mayor seguridad a los clientes al momento de retirar o realizar una transacción en los cajeros, implementación de la certificación PCI-DSS para la seguridad de los datos, entre otros servicios que permitan a sus usuarios agilizar trámites bancarios (BANRED, 2019).

Los cajeros automáticos están orientados a agilizar los procesos de las entidades financieras del país, permitiendo ejecutar transacciones online incluso si la entidad financiera se encuentra cerrada en esos momentos. Para mejorar la atención a sus usuarios al momento de realizar transacciones comunes como es el “retirar de dinero”, cada entidad financiera, instala cajeros

automáticos en diferentes puntos estratégicos en la ciudad, como en plazas, supermercados, centros comerciales (Cooke, 2017).

Como se ilustra en la Fig. 3., se puede observar la cantidad de cajeros por cada 100.000 habitantes en América Latina. La principal opción para realizar transacciones bancarias es la utilización de cajeros automáticos.

Fig. 3. Cajeros Automáticos en América Latina
Fuente: (BSLatAm, 2018)

1.11. Proceso de Cajeros automáticos

El proceso en un cajero automático, inicia al introducir la tarjeta de débito en la ranura, ingresar el PIN de 4 dígitos, seleccionar la transacción que desea realizar, si realiza un retiro selecciona

la cantidad y se recibe el dinero por la ranura, ese proceso es de conocimiento de todas las personas que utilizan estos dispositivos (Aron, 2019).

Lo que internamente sucede en un cajero automático entiende el fabricante de estos dispositivos, a continuación la empresa BBVA explica en siete pasos que describen el proceso interno de estos dispositivos: (Aron, 2019).

Como se observa en la Fig. 4., los procesos suceden en cuestión de segundos, los contenedores internos de dinero pueden tener hasta 3000 billetes, por tal motivo se deben manejar altos estándares de seguridad para evitar cualquier tipo de fraude que afecte a los usuarios de cajeros automáticos (Aron, 2019).

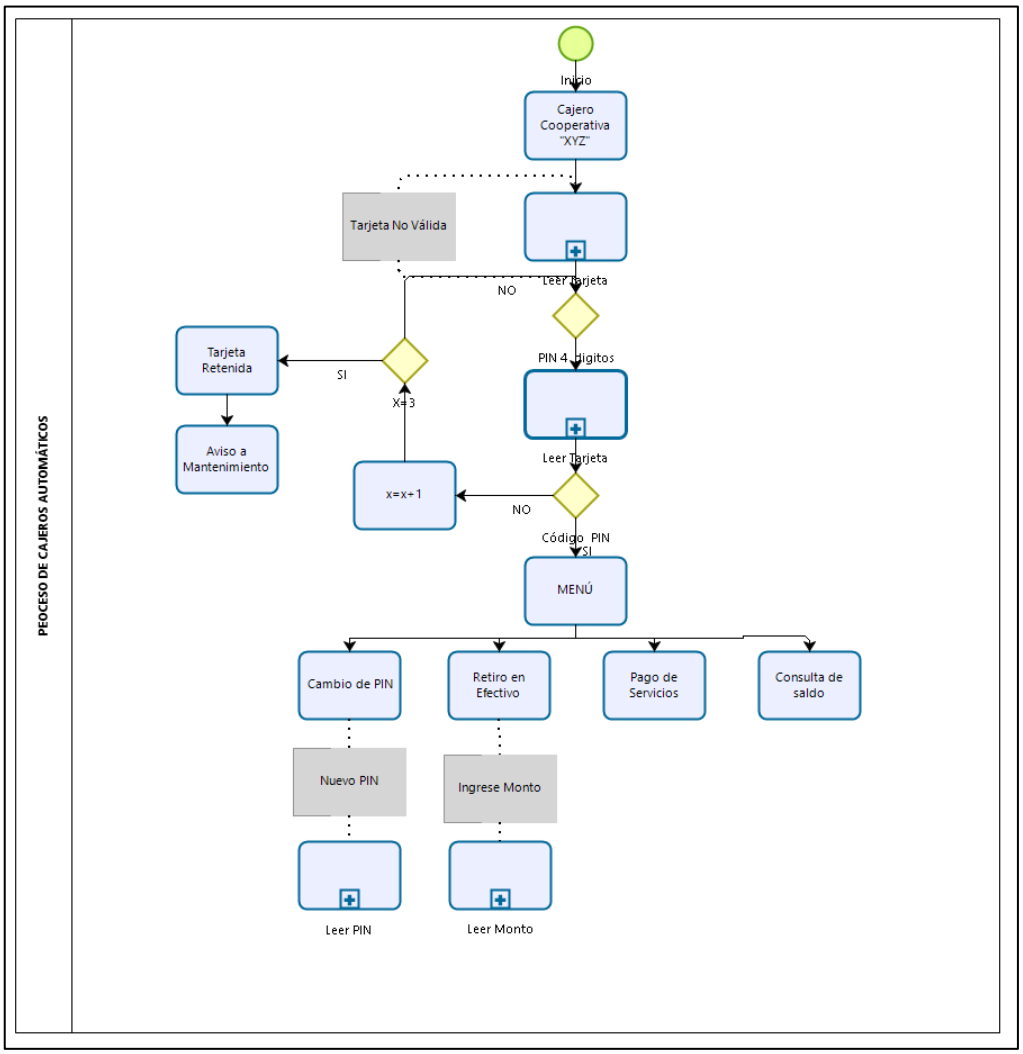


Fig. 4. Procesos de cajeros Automáticos
Fuente: Propia

1.11.1. Transacciones en cajeros automáticos

Los ATM sus siglas significan (Automatic Taller Machines o máquina de cajero automático), Son dispositivo que permiten a clientes de agencias bancarias hacer retiros de dinero, ver estados de cuenta, utilizar tarjetas con chips, entre otros, sin tener que acudir al banco, a cualquier hora del día. Para realizar estas transacciones se emplea una tarjeta de crédito o de débito, que contiene un código de identificación individual caracterizado, conocido como PIN (Díaz Céspedes, 2018).

La tarjeta se inserta en una ranura donde se observa la información del usuario que contiene una banda magnética enviando información a la computadora central, de donde se realiza la transacción que el cliente desee, el mecanismo que entrega el efectivo se llama ojo electrónico, contiene agregado un sensor que cuenta los billetes para entregar la cantidad solicitada. Las transacciones realizadas son grabadas en un diario electrónico denominado Log (Díaz Céspedes, 2018).

1.11.2. Medidas de seguridad de cajeros automáticos del Ecuador Superintendencia de Bancos (SB)

La Superintendencia de Bancos define normas generales que las instituciones financieras ecuatorianas deben cumplir a cabalidad para el control de cajeros automáticos, basándose en la resolución No. JB-2014-3053 de 27 de agosto del 2014 (SB, 2014).

En la sección VII.- De las medidas de seguridad (incluida con resolución No. JB-2011-1851 de 11 de enero del 2011) (SB, 2014).

Articulo 40.- Los cajeros automáticos de las instituciones financieras deben cumplir con las siguientes medidas de seguridad: (Substituido con resolución No. JB-2011-1851 de 26 de abril del 2011) (SB, 2014).

La TABLA 1.5 detalla cada uno le los literales que contiene el Artículo 40 de la Superintendencia de Bancos, para la administración de cajeros automáticos, proporcionando información que será útil al momento de implementar la normativa internacional PCI DSS, estipulando que se convierta en una guía estándar, para auditar estos dispositivos.

TABLA 1.5

Artículo 40 de la Superintendencia de Bancos (SB)

Literales Articulo 40	Nombre Literal de Articulo 40	Descripción del literal del articulo 40
40.1	Protección al teclado	Contar en todo momento con los dispositivos conocidos como “protectores de teclado”, que de una manera efectiva impidan la visibilidad al momento que el usuario digita su clave personal.
40.2	Protección contra clonación de tarjetas	Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito o de crédito, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales (sustituido con resolución No. JB-2012-2148 de 26 de abril del 2012).
40.3	Iluminación	Los cajeros automáticos instalados en áreas externas a las oficinas de las instituciones financieras, deberán estar ubicados en zonas suficientemente iluminadas que permitan la visualización de toda actividad a su alrededor.
40.4	Programas de vigilancia en sitio	Contar con un programa regular de visitas al sitio donde se encuentra instalado el cajero automático, con la finalidad de garantizar que no existan objetos extraños, dispositivos u otros mecanismos sospechosos instalados en el cajero automático.
40.5	Mecanismo de anclaje	Los cajeros automáticos deben asegurarse adecuadamente al piso u otro soporte a fin de que dificulte su remoción, salvo el caso de aquellos que estén empotrados a la pared.
40.6	Protección al software e información del cajero automático	Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberá instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución (sustituido con resolución No. JB-2012-2148 de 26 de abril del 2012).
40.7	Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos	Disponer de procedimientos auditables debidamente acordados y coordinados entre la institución y los proveedores internos o externos para la ejecución de las tareas de mantenimiento preventivo y correctivo del hardware y software, provisión de suministros y recarga de dinero en las gavetas. Las claves de acceso tipo “administrador” del sistema del cajero automático deben ser únicas y reemplazadas periódicamente (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012).
40.8	Accesos físicos al interior de los cajeros automáticos	Disponer de cerraduras de alta tecnología y seguridades que garanticen el acceso controlado al interior del cajero automático por parte del personal técnico o de mantenimiento que disponga de las respectivas llaves. Estas cerraduras deben operar con llaves únicas y no genéricas o maestras (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012).
40.9		Establecer los mecanismos y procedimientos adecuados

	40.9.1	Revisar periódicamente los anclajes, iluminación y entorno del cajero automático.
	40.9.2	Abastecer de dinero permanentemente a los cajeros automáticos.
	40.9.3	Atender las alarmas generadas por los dispositivos electrónicos de control instalados en los cajeros automáticos.
	40.9.4	Contar con personal capacitado para la operación y mantenimiento diario del cajero.
40.10	Cámaras de vigilancia	Para su operación, cada cajero automático debe contar al menos con dos cámaras de vigilancia en las siguientes ubicaciones. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014).
	40.10.1	Una periférica con vista panorámica de arriba hacia abajo, que permita captar el entorno del equipo. Una cámara frontal que permita captar al usuario. Si en alguna localización existen cajeros contiguos, las entidades pueden disminuir el número total de cámaras periféricas, con el sustento técnico respectivo. De ninguna manera se pueden disminuir el número de las cámaras frontales.
	40.10.2	Las cámaras de vigilancia deben operar de forma ininterrumpida las veinticuatro (24) horas del día. El funcionamiento de las cámaras debe ser evaluado permanentemente y mantener un registro actualizado de sus niveles de operación, a fin de garantizar la nitidez y fidelidad de las grabaciones realizadas.
40.11	Sistema de grabación de video	Para su operación, cada cajero automático debe tener un grabador de videos exclusivo, mismo que debe registrar la grabación sin degradar la definición capturada por sus cámaras. (reformado con resolución No. JB2013-2642 de 26 de septiembre del 2013 y numeral sustituido resolución No. JB-2014-3066 de 2 de septiembre del 2014). Las instituciones del sistema financiero deben mantener un archivo de grabaciones que cubra por lo menos noventa (90) días, mientras que de las transacciones que sean objeto de reclamo, se guardarán hasta que haya una resolución en firme del órgano competente.

Fuente: (SB, 2014).

1.11.3. Medidas de seguridad en cajeros automáticos del Ecuador bajo la Superintendencia de Economía Popular y Solidaria (SEPS)

La Superintendencia de Economía Popular y Solidaria, tiene normas generales que las instituciones financieras del país deben cumplir a cabalidad para el control de cajeros automáticos en el Ecuador, basándose en la resolución No. SEPS-IGT-IR-IGJ-2018-021 (SEPS, 2019).

Artículo 9.- Medidas de seguridad en cajeros automáticos. Las entidades que cuenten con cajeros automáticos propios o proporcionados por un tercero deberán considerar las siguientes medidas: (SEPS, 2019).

La TABLA 1.6 detalla cada uno le los literales que contiene el Artículo 9 de la Superintendencia de Economía Popular y Solidaria (SEPS), para la administración de cajeros automáticos, proporcionando información útil al implementar la normativa internacional PCI DSS, estipulando que se convierta en un estándar que todas las instituciones financieras del país se guíen al auditar estos dispositivos.

TABLA 1.6

Artículo 9 de la Superintendencia de Economía Popular y Solidaria (SEPS)

Literales Articulo 9	Nombre literal de articulo 9	Descripción del literal del articulo 9
9.1	Ubicación y entorno	Deben ser instalados en lugares cuya ubicación y entorno minimicen, en la mayor medida posible, el riesgo de que tanto el cajero automático como sus socios, cliente, usuarios o el público en general, puedan ser objeto o víctimas de actos delictivos.
9.2	Protección del teclado	Contar en todo momento con los dispositivos conocidos como "protectores de teclado", que de una manera efectiva impidan la visibilidad al momento que el usuario digita su clave personal.
9.3	Protección contra clonación de tarjetas	Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjeta de débito, crédito o prepago, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales.
9.4	Iluminación	Los cajeros automáticos deberán estar ubicados en zonas suficientemente iluminadas que permitan la visualización de toda actividad a su alrededor.
9.5	Programas de vigilancia en sitio	Contar con un programa regular de visitas al sitio donde se encuentra instalado el cajero automático, con la finalidad de garantizar que no existan objetos extraños, dispositivos u otros mecanismos sospechosos instalados en el cajero automático.
9.6	Mecanismos de anclaje	Los cajeros automáticos deben asegurarse adecuadamente al piso u otro soporte a fin de impedir su remoción, salvo el caso de aquellos que estén empotrados en la pared.
9.7	Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos	Disponer de procedimientos auditables debidamente acordados y coordinados entre la entidad y los proveedores internos o externos para la ejecución de las tareas de mantenimiento preventivo y correctivo del hardware y software, provisión de suministros y recarga de dinero en gavetas. Las claves de acceso tipo "administrador" del sistema del cajero automático deben ser únicas y reemplazadas periódicamente.
9.8	Accesos físicos al interior de los cajeros automáticos	Disponer de cerraduras de alta tecnología y seguridades, que garanticen el acceso controlado a la caja fuerte que se encuentra en el interior del cajero automático por parte del personal encargado de la provisión y cuadratura del efectivo. Estas cerraduras deben operar con llaves únicas y no genéricas o maestras. El acceso a las cajas fuertes de los cajeros automáticos deberá lograrse únicamente con la intervención simultánea de dos o más personas encargadas de la custodia de las llaves y/o códigos de acceso diferentes entre sí.

9.9	Establecer los mecanismos y procedimientos adecuados	
	a)	Revisar periódicamente los anclajes, iluminación y entorno del cajero automático.
	b)	Abastecer de dinero permanentemente a los cajeros automáticos.
	c)	Atender oportunamente las alarmas generadas por los dispositivos electrónicos de control, instalados en los cajeros automáticos.
	d)	Contar con personal capacitado para la operación y mantenimiento diario del cajero.
9.10	Cámaras de vigilancia	Para su operación, cada cajero automático debe contar al menos con dos cámaras de vigilancia en las siguientes ubicaciones.
	a)	Una periférica con vista panorámica de arriba hacia abajo, que permita captar el entorno del equipo.
	b)	Una cámara frontal que permita captar al socio, cliente o usuario.

Fuente: (SEPS, 2019).

1.12. Tarjetas de Crédito

Estos mecanismos constituyen un medio práctico para realizar: créditos, pagos, retiros, entre otros, realizando cobros de manera segura ya sean estos al contado o a crédito. El origen de las tarjetas se remonta a mediados del siglo XX, por compañías de los Estados Unidos con el fin de facilitar a sus clientes el pago diferido, percibiendo sus beneficios se expande a Europa en donde tiene gran acogida, con el tiempo las entidades financieras se fueron convirtiendo en los principales emisores de tarjetas para realizar transacciones bancarias (Zunzunegui, 2006).

Hay dos categorías de las tarjetas que son: crédito y débito. Las tarjetas de débito, permite pagar en puntos de venta con cargo a la cuenta corriente, a su vez, las tarjetas de crédito sirven como herramienta para obtener crédito. El servicio de tarjetas es siempre una relación triangular entre: la agencia bancaria, el titular de la tarjeta y el negociante adherido al sistema (Zunzunegui, 2006).

1.12.1. Tarjetas de crédito en Ecuador

Según el estudio de (Martínez & Merchán, 2010), el origen de las tarjetas de crédito en el Ecuador es a partir de la década de los años 70, es decir, Cuando apareció el petróleo en el país hubo más ingresos e inicializo el sistema de consumo, esto permitió la incorporación de las primeras tarjetas de crédito en el sistema bancario ecuatoriano, percibiendo por primera vez el

crédito instantáneo. La primera tarjeta de crédito que se utilizó en el país, fue Diners Club, brindando un servicio nacional e internacional.

En el Ecuador el uso de tarjetas de crédito ha aumentado considerablemente, el hábito de consumo por parte de los ecuatorianos ha permitido que estos objetos sean de gran interés para la población, debido a que actualmente hay muchos establecimientos afiliados a las agencias bancarias, donde se realizan: pagos, créditos, consultas, entre otros, con estos dispositivos (Martínez & Merchán, 2010).

1.12.2. Tipos de Tarjetas de Crédito

Existen varios tipos de tarjetas de crédito emitidas por entidades financieras, cada una de estas tiene su perfil de solvencia, actualmente los bancos ponen a disponibilidad de sus clientes tarjetas especializas para cubrir algunos usos como son: viajes (Tarjeta Viajero), negocios, compras, etc. Por lo general las entidades financieras ofrecen tres tipos de tarjetas a sus clientes que son: Oro, Platinum y Premium (Daza, 2014).

Las agencias bancarias habitualmente ofrecen a sus clientes dos tipos de tarjetas de crédito, Oro y Platinum, que cumplen con las normas más altas de entradas y contenido solvente. En muchos casos las tarjetas tienen tasas de interés muy altas, por tal motivo se debe tomar en cuenta las ofertas que brindan las tarjetas antes de usarlas. Existen otras denominaciones, dependiendo sus usos como son: (Daza, 2014).

- **Tarjetas aseguradas:** Requieren un depósito de seguridad y son apropiadas para aquellos que no tienen antecedentes de crédito o cuyos antecedentes son negativos.
- **Tarjetas convencionales:** No requieren ni un depósito, pero ofrecen escasas ventajas. Poseen un límite de crédito es más amplio que las tarjetas aseguradas.
- **Tarjetas de primera línea:** (Oro, Platino, Titanio) brindan límites de crédito más amplios y regularmente tienen ventajas adicionales.

1.12.3. Ventajas y desventajas al usar tarjetas de crédito

La TABLA 1.7 Es un cuadro descriptivo de pros y contras, que clientes de agencias bancarias deben tomar en cuenta al momento de adquirir las tarjetas de crédito o débito, para que tengan conocimiento de los riesgos y puedan hacer buen uso de las mismas y no permitan ser timados por no saber los riesgos a los que se encuentran expuestos al obtener este tipo de dispositivos bancarios.

TABLA 1.7
Cuadro de Ventajas y Desventajas al usar tarjetas de crédito

Ventajas del uso de tarjetas bancarias	Desventajas del uso de tarjetas bancarias
Se obtiene crédito inmediato en establecimientos del país que sean asociados al uso de estos dispositivos electrónicos, para la adquisición de bienes y servicios.	Es posible que exista fraude por mal uso intencional, robo o pérdida de la tarjeta
La sustitución de pagos en efectivo y el uso de cheques con la emisión de una cancelación mensual.	Descontrol en gastos del usuario, debido a que el dueño de la tarjeta en ocasiones no es consiente del consumo, que efectúa hasta que llega a copar el cupo y llega a tener mensualmente los valores a cancelar.
Utilizar tarjetas de crédito disminuye el riesgo de robos, las personas no necesitan circular con grandes cantidades de dinero	Los artículos son más costosos, por el interés y los cargos por financiamiento que algunas empresas añaden al valor del producto/servicio que se está comprando.
Mejora la administración del dinero	La principal desventaja que acarrea la empresa afiliada al aceptar el pago de facturas a través del uso de tarjetas, es la de no poder convertir facturas en efectivo en un plazo menor de 48 horas, al menos que este posea una cuenta bancaria en el banco emisor de la tarjeta.
Sirve para resolver emergencias, es decir; para cubrir gastos que no se tienen proyectados o de improviso.	

Fuente: (Nacional, Morazán, & Galo, 2014).

1.13. Normativa Internacional PCI DSS

La normativa internacional PCI DSS fue creada en el año 2006 por las compañías: VISA, MASTERCARD, AMERICAN EXPRESS, JCB Y DISCOVER, para reducir los riesgos y evitar que las tarjetas de crédito se encuentren comprometidas, permite que exista varios puntos a evaluar para salvaguardar la integridad de sus clientes (Piazza, Fernandes, Anderson, & Olmsted, 2016).

La normativa debe ser vista como un grupo de objetivos que serán analizados continuamente llevando un control paulatino al momento de aplicarla para tener éxito en su implementación, el error común que rodea a la normativa PCI DSS, es si un año tuvo éxito el próximo año no se asegura lo mismo, se debe realiza nuevamente una nueva evaluación, por tal motivo el aspecto más desafiante de PCI DSS es que tenga estabilidad (Coburn, 2010).

El proveedor del servicio de tarjetas de crédito al realizar un control, evaluando los diferentes puntos que contiene la normativa internacional PCI DSS y si pasa por un examen forense realizado por la asociación de tarjetas de crédito, el proveedor del servicio estaría absuelto de cualquier tipo de responsabilidad si hay alguna anomalía en el uso de estos dispositivos (Ataya, 2011).

Las sanciones que enfrentan las firmas que han sufrido pérdidas por no llevar el debido control y ocasionaron daños a terceros, para los peores casos en los que iban a finalizar su actividad económica. Esos daños pueden incluir:(Ataya, 2011).

- Sanciones económicas
- Retiro de equipos en puntos de venta
- Revocación de la membresía de la red de tarjetas de crédito
- Publicidad Negativa
- Pérdida de Clientes
- Reducción de Ingresos

PCI DSS es una normativa internacional que es aplicable a cualquier tipo de entidad en donde se procesan o trasfieren datos de propietarios de tarjetas o datos confidenciales de autenticación, por lo tanto, se aplica en cajeros automáticos para salvaguardar la integridad física y datos de usuarios de estos dispositivos (ATMIA, 2014).

1.13.1. Cumplimiento de la Normativa Internacional PCI DSS

Para el cumplimiento de la normativa internacional PCI DSS existen cuatro niveles, que serán puestos a disposición dependiendo lo que el negocio necesite, tomando en cuenta estos dos factores: (Klever, 2018).

- La magnitud de actividad comercial
- La forma de procesar la información de las actividades comerciales

Los requisitos de la PCI Security Standards Council (Consejo de normas de seguridad), ha definido y especificado una serie de necesidades que deben cumplir las entidades que almacenan, procesan o transfieren datos, por tal motivo, la normativa internacional PCI DSS define un grupo de doce exigencias de alto nivel que abordan seis áreas importantes: (ATMIA, 2014).

En la TABLA 1.8 se encuentra cada uno de los objetivos que contiene uno o más requisitos de la Normativa Internacional PCI DSS, los cuales deberán ser seleccionados al momento de realizar una auditoría enfocada a la evaluación de cajeros automáticos, realizando una guía práctica que ayude a los auditores al momento de evaluar los dispositivos.

TABLA 1.8
Puntos de evaluación de la Normativa Internacional PCI DSS

Nro.	Objetivo	Requisito
1	Desarrollar y mantener una red segura	1. Instalar y mantener una configuración de firewall para proteger los datos de los tarjetahabientes 2. No usar contraseñas del sistema y otros parámetros de seguridad provistos por los proveedores
2	Proteger los datos de los propietarios de las tarjetas de crédito	3. Proteger los datos de los propietarios de las tarjetas de crédito que estén almacenados. 4. Cifrar los datos de los propietarios de tarjetas de crédito transmitidos a través de redes públicas abiertas.
3	Mantener un programa de gestión de vulnerabilidad.	5. Utilizar software antivirus y actualizarlo regularmente. 6. Desarrollar y mantener sistemas y aplicaciones seguras.
4	Implementar medidas solidas de control de acceso.	7. Restringir el acceso a los datos de los propietarios de tarjetas de crédito conforme con la necesidad del funcionario de conocer la información 8. Asignar una identificación única a cada persona que tenga acceso al sistema informático. 9. Limitar el acceso físico a los datos de los propietarios de tarjetas de crédito.
5	Monitorear y probar regularmente las redes.	10. Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas de crédito. 11. Probar los sistemas y procesos de seguridad regularmente
6	Mantener una política de seguridad de la información.	12. Mantener una política que contemple la seguridad de la información.

Fuente: (ATMIA, 2014).

1.14. Proceso para el análisis de la normativa internacional PCI DSS

Las organizaciones deben tratar de completar el análisis del estado actual y realizar un análisis de brecha, según (Ruiz, 2015). Explica que el análisis de brecha es una herramienta que compara el estado y el desempeño real de una organización, con el estado o situación de un momento dado, respecto a uno a más puntos de referencia seleccionados de orden local, regional, nacional o internacional.

La evaluación de las normas de gestión de identidad y seguridad existentes, comparándolas con la descripción PCI y repitiendo en áreas que necesitan mejoras, cumpliendo con la normativa internacional PCI DSS, recopilando esta información como base, para la implementación de un modelo que sea aplicado a una organización sabiendo sus falencias y necesidades (Coburn, 2010).

El proceso común para implementar la normativa internacional PCI DSS es el ciclo de Deming, según (Garc, 2013). Este ciclo consiste en planificar, Implementar, revisar y actuar, para conseguir la mejora continua en cualquier paso, en la TABLA 1.9, se define cada una de las fases del ciclo de implementación de la normativa PCI DSS.

TABLA 1.9
Faces para la implementación de la normativa PCI DSS

FASE	DETALLE
Planificar	Consiste en identificar las dificultades y potenciales fuentes de debilidad o error en el sistema, recopilando información para elaborar un plan de mejora utilizando la información recopilada.
Implementa	Efectuar el plan que se haya elaborado y poner el plan en acción
Revisar	Se refiere al proceso de seguimiento, será importante evaluar la eficacia del trabajo que se ha realizado, utilizando técnicas de revisión y auditoria. Si está orientado a la debilidad de la organización se recomienda realizar un estudio piloto de los problemas a resolver.
Actuar	Se debe realizar cualquier acción correctiva y luego se vuelve a comprobar para asegurarse que la solución a funcionado.

Fuente: (Garc, 2013).

Como se ilustra en la Fig. 5. El proceso que emplea la normativa internacional PCI DSS, para su implementación es la evaluación constante que permite analizar los puntos vulnerables de las entidades financieras.

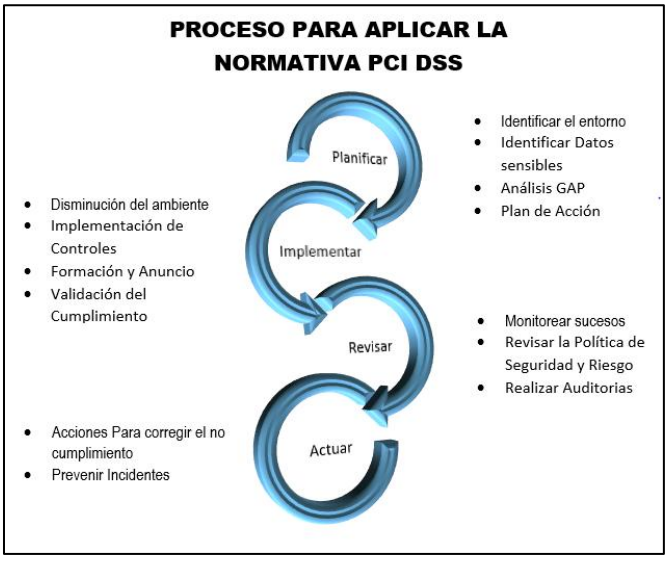


Fig. 5. Proceso para el análisis de la normativa Internacional PCI DSS
Fuente: Propia

1.14.1. Métodos de investigación

En la TABLA 1.10 se describen los métodos de investigación que se aplican para implementar la normativa PCI DSS, tomando en cuenta en que parte del estudio se aplica cada una de ellas.

TABLA 1.10
Métodos de Investigación

Tipo de investigación	Descripción
Explicativa	Ayuda a conocer por que se realizan dichas actividades, analizando las interrelaciones que produce un fenómeno, profundizando la comprensión. Explica de forma coherente todos los descubrimientos que se vayan presentando en el transcurso del proyecto.
Descriptiva	También es parte del proyecto ya que describirá la realidad actual y el comportamiento dentro de la institución para diseñar el modelo de mejoramiento a los procesos operativos identificando características y comportamientos específicos del proyecto.
Exploratoria	Es primordial realizar una investigación de este tipo para determinar el problema, recopilando información proporcionada por los responsables actuales de los procesos y por los directivos lo cual tiene capacidad para la toma de decisiones.

Fuente: (Patlán Pérez & Martínez Torres, 2017).

1.14.2. Actores en PCI DSS

Como se ilustra en la Fig. 5. Los actores que intervienen en la implementación de la normativa internacional PCI DSS son los siguientes:

Fig. 6. Actores en PCI DSS
Fuente: Propia

1.15. Norma PCI PTS

La norma PCI PTS (PIN Transaction Security – Seguridad de Transacciones con PIN), contiene requerimientos de seguridad para transacciones con PIN, se encuentra enfocada a la seguridad de unidades de pago, en este caso está dirigido a las ATM's (Cajeros Automáticos), puntualizando los requisitos que se deben tomar en cuenta para mantener un buen funcionamiento de estos dispositivos en las entidades financiera (PCI Security Standards Council LLC., 2013).

El objetivo de esta norma es evaluar conjuntamente con la normativa internacional PCI DSS el software y hardware en cajeros automáticos, para encontrar las vulnerabilidades que tienen los dispositivos y generar un plan de acción para corregir los fallos que se encuentren al realizar la evaluación, esto evitara que la integridad e información de usuarios de ATM's, se encuentre expuesta a cualquier tipo de fraude (PCI Security Standards Council LLC., 2013).

CAPITULO II

Desarrollo

2.1. Metodología de la investigación.

El desarrollo de esta investigación se ha considerado aplicar técnicas de investigación como: observación, encuestas y cuestionarios, estos estarán dirigidos a los representantes directos en el transcurso de la auditoria.

2.2. Técnicas de investigación, instrumentos de recolección y procesamiento de datos e información.

La investigación está basada en auditoria física de cajeros automáticos implementando la normativa PCI DSS conjuntamente con la PCI PTS, siguiendo los lineamientos de la Superintendencia de Bancos y la Superintendencia Economía Popular y Solidaria, enfocado en ATM's para llevar un control de eficacia y disposición.

Para el desarrollo del presente trabajo se tomará en cuenta los parámetros de la Normativa PCI (Security Standards Council – Consejo de normas de seguridad), permitirá a los auditores pertenecientes a la empresa GREENETICS soluciones S.A., realizar un trabajo competente, además, de estandarizar un modelo evaluador para realizar auditoria de cajeros automáticos de la cartera de clientes de la empresa antes mencionada.

La parte evaluadora debe tomar en cuenta las recomendaciones de la agencia bancaria para el levantamiento de información, como parte de la metodología específica de Ethical Hacking Externo, empleada en el presente proyecto se tienen las siguientes fases que serán detalladas en la (TABLA 2.1).

TABLA 2.1
Fases para implementación de la normativa PCI DSS/PTS

Fases	Detalle
Búsqueda de información.	Consiste en recopilar la información del cajero automático evaluado, para documentar la búsqueda de vulnerabilidades y se revisará cuáles son los puntos que cumplen con la normativa aplicada a estos dispositivos.
Identificación de causa raíz de los problemas	Se realiza el análisis tomando en cuenta los problemas encontrados y reportados en el área de quejas o por BANRED con respecto al cajero automático evaluado.
Generación de valores estadísticos	Los valores serán tomados en cuenta después de aplicar la normativa PCI DSS/PTS, en cajeros automáticos.
Análisis de la información obtenida	Se analizará la información obtenida de cajeros automáticos, para verificar las vulnerabilidades que se encuentra expuesto y se informará al departamento de Tecnologías de la Información para que tomen las medidas correctivas.

Fuente: Propia

2.3. Diseño metodológico

El presente estudio se encuentra implementado con dos tipos de investigación, que servirán de gran ayuda para cumplir con este fin, los que se detallarán a continuación:

2.3.1. Investigación Exploratoria

Es primordial realizar una investigación de este tipo para determinar el problema, recopilando información proporcionada por responsables de los procesos y directivos, quienes tiene la capacidad para la toma de decisiones (Klever, 2018).

2.3.2. Investigación Documental

Esta investigación es realizada apoyándose en documentos de cualquier índole, extrayendo los aspectos relevantes relacionados con el tema, estos documentos ayudaran a los auditores llevar la información de manera correcta para presentar el informe final de auditoría(Klever, 2018).

2.4. PCI DSS/PTS

La Fig. 7. Es el logo de la normativa internacional PCI (Security Standarts Council) Consejos de normas de Seguridad, para evaluación y control de cajeros automáticos pertenecientes a entidades financieras, para llevar un control riguroso y puedan cumplir con normas de seguridad físicas de los dispositivos, además de brindar un excelente servicio a sus clientes

Fig. 7. Normativa PCI
Fuente: (PCI Security Standards Council LLC., 2013).

En la TABLA 2.2 se encuentra un resumen de la Normativa PCI DSS y la Normativa PCI PTS, estas dos normativas son complementarias para realizar evaluaciones físicas a cajeros automáticos, brindando a los auditores ítems para la evaluación de dichos dispositivos.

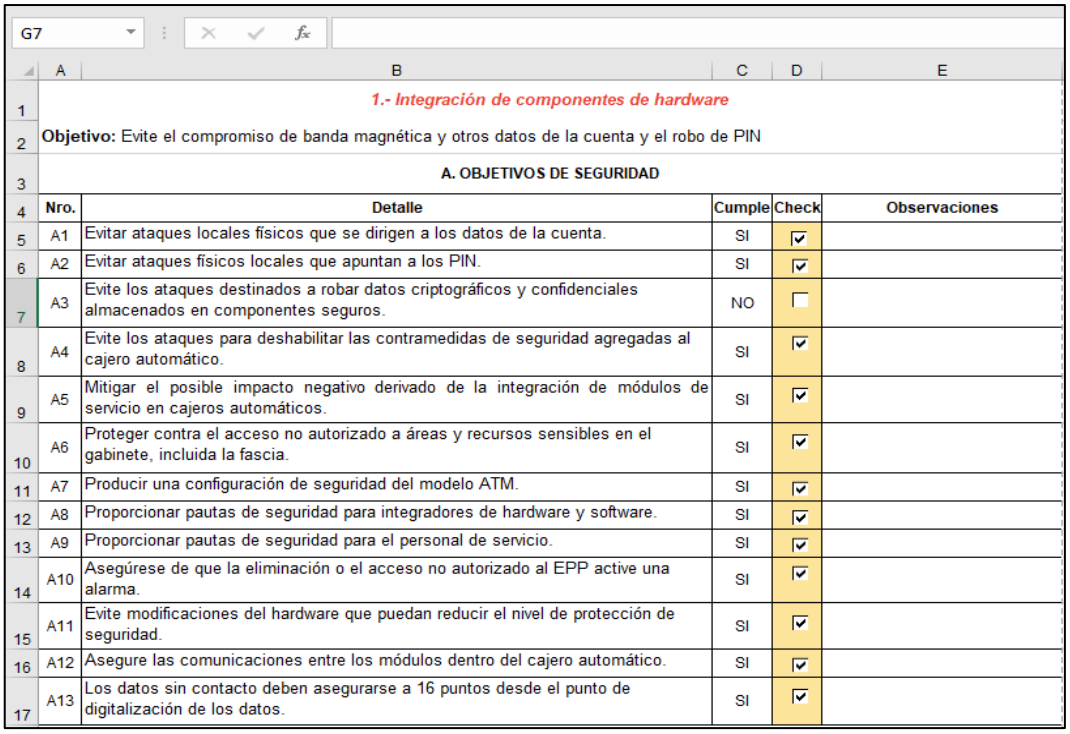
TABLA 2.2
Normativa PCI DSS Normativa PTS

Normativa Internacional PCI DSS	Normativa Internacional PCI PTS
Las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago (ATMIA, 2014).	Es un manual que ayuda a identifica las pautas de seguridad para los cajeros automáticos, considerando la protección que puede proporcionar el hardware y el software del cajero automático contra ataques dirigidos a comprometer los datos confidenciales adquiridos, almacenados, exportados o procesados de cualquier forma por el dispositivo El estándar PCI PIN está alineado con el enfoque de seguridad y la modularidad del conjunto de requisitos de seguridad de PCI PTS POI (Punto de Interacción) y está destinado a proporcionar una guía de seguridad para los compradores y operadores de cajeros automáticos que compran, implementan y/u operar cajeros automáticos; además de una orientación de seguridad y mejores prácticas para las partes interesadas de la industria de cajeros automáticos (PCI Security Standards Council LLC., 2013).

Fuente: Propia

2.5. Ítems técnicos para la evaluación de cajeros automáticos PCI DSS/PTS

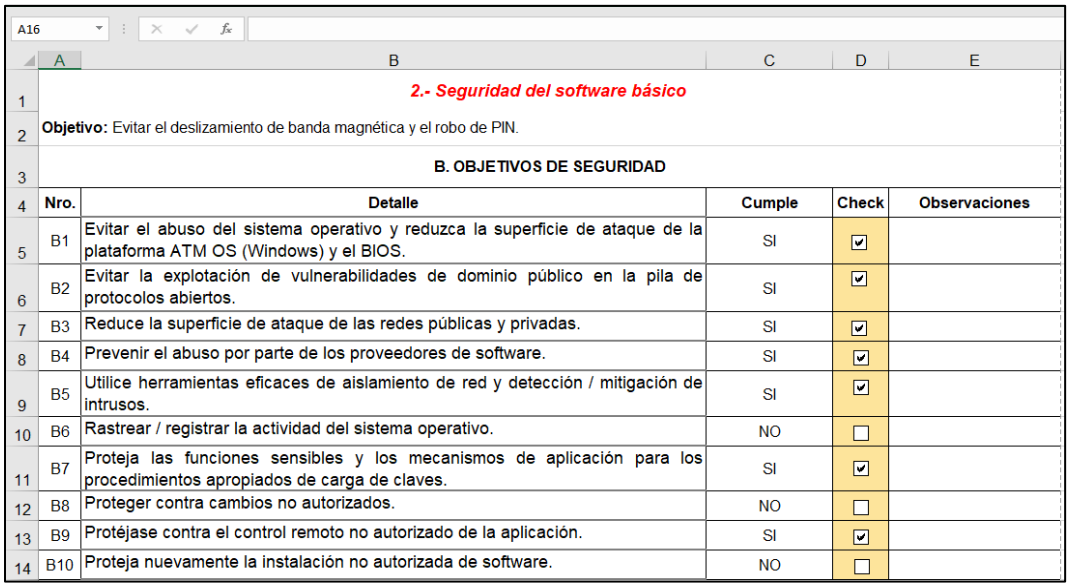
En la Fig. 8. Se encuentran los ítems de integración de componentes de Hardware para evaluar cajeros automáticos, basados en los lineamientos de la normativa PCI DSS/PTS, que es el órgano regulador que emite los patrones necesarios para realizar una evaluación correcta de los dispositivos.



	A	B	C	D	E
1		*1.- Integración de componentes de hardware*			
2		**Objetivo:** Evite el compromiso de banda magnética y otros datos de la cuenta y el robo de PIN			
3		**A. OBJETIVOS DE SEGURIDAD**			
4	**Nro.**	**Detalle**	**Cumple**	**Check**	**Observaciones**
5	A1	Evitar ataques locales físicos que se dirigen a los datos de la cuenta.	SI	☑	
6	A2	Evitar ataques físicos locales que apuntan a los PIN.	SI	☑	
7	A3	Evite los ataques destinados a robar datos criptográficos y confidenciales almacenados en componentes seguros.	NO	☐	
8	A4	Evite los ataques para deshabilitar las contramedidas de seguridad agregadas al cajero automático.	SI	☑	
9	A5	Mitigar el posible impacto negativo derivado de la integración de módulos de servicio en cajeros automáticos.	SI	☑	
10	A6	Proteger contra el acceso no autorizado a áreas y recursos sensibles en el gabinete, incluida la fascia.	SI	☑	
11	A7	Producir una configuración de seguridad del modelo ATM.	SI	☑	
12	A8	Proporcionar pautas de seguridad para integradores de hardware y software.	SI	☑	
13	A9	Proporcionar pautas de seguridad para el personal de servicio.	SI	☑	
14	A10	Asegúrese de que la eliminación o el acceso no autorizado al EPP active una alarma.	SI	☑	
15	A11	Evite modificaciones del hardware que puedan reducir el nivel de protección de seguridad.	SI	☑	
16	A12	Asegure las comunicaciones entre los módulos dentro del cajero automático.	SI	☑	
17	A13	Los datos sin contacto deben asegurarse a 16 puntos desde el punto de digitalización de los datos.	SI	☑	

Fig. 8. Integración de componentes de Hardware
Fuente: Propia

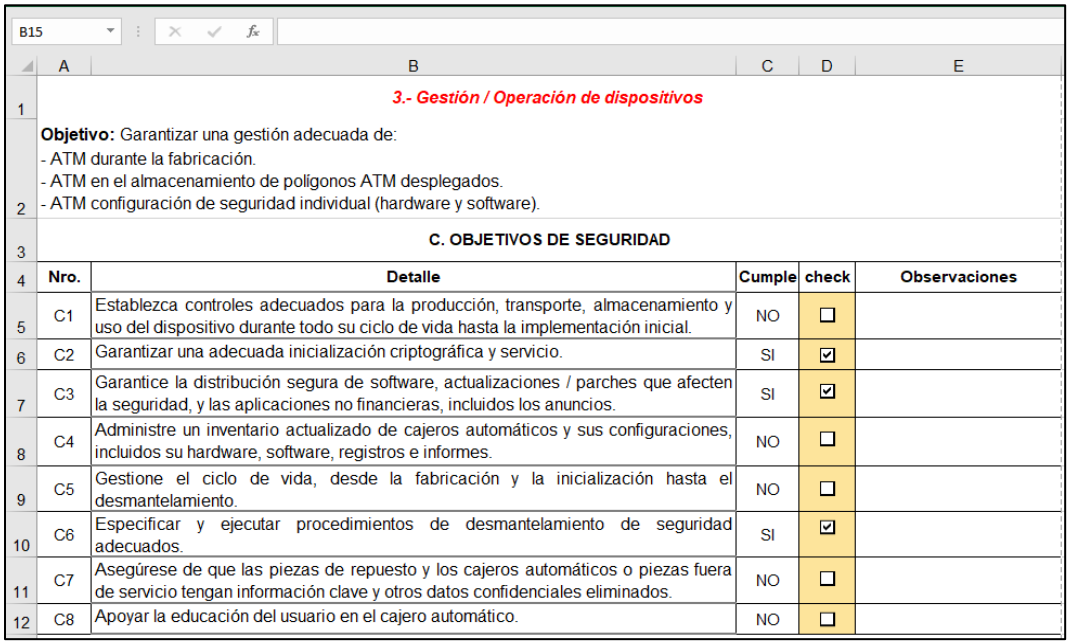
En la Fig. 9. Se encuentran los ítems de Seguridad de software básico para evaluar cajeros automáticos, basados en los lineamientos de la normativa PCI DSS/PTS, que es el órgano regulador que emite los patrones necesarios para realizar una evaluación correcta de los dispositivos.



	A	B	C	D	E
1		*2.- Seguridad del software básico*			
2		**Objetivo:** Evitar el deslizamiento de banda magnética y el robo de PIN.			
3		**B. OBJETIVOS DE SEGURIDAD**			
4	**Nro.**	**Detalle**	**Cumple**	**Check**	**Observaciones**
5	B1	Evitar el abuso del sistema operativo y reduzca la superficie de ataque de la plataforma ATM OS (Windows) y el BIOS.	SI	☑	
6	B2	Evitar la explotación de vulnerabilidades de dominio público en la pila de protocolos abiertos.	SI	☑	
7	B3	Reduce la superficie de ataque de las redes públicas y privadas.	SI	☑	
8	B4	Prevenir el abuso por parte de los proveedores de software.	SI	☑	
9	B5	Utilice herramientas eficaces de aislamiento de red y detección / mitigación de intrusos.	SI	☑	
10	B6	Rastrear / registrar la actividad del sistema operativo.	NO	☐	
11	B7	Proteja las funciones sensibles y los mecanismos de aplicación para los procedimientos apropiados de carga de claves.	SI	☑	
12	B8	Proteger contra cambios no autorizados.	NO	☐	
13	B9	Protéjase contra el control remoto no autorizado de la aplicación.	SI	☑	
14	B10	Proteja nuevamente la instalación no autorizada de software.	NO	☐	

Fig. 9. Seguridad del Software básico
Fuente: Propia

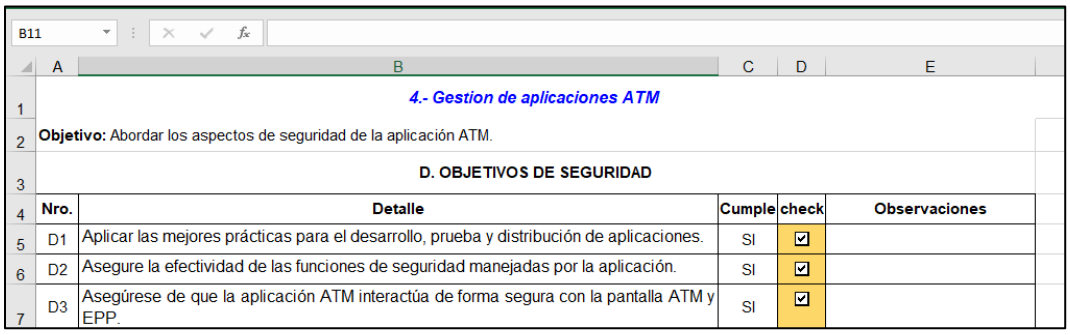
En la Fig. 10. Se encuentran los ítems de Gestión/Operación de dispositivos para evaluar cajeros automáticos, basados en los lineamientos de la normativa PCI DSS/PTS, que es el órgano regulador que emite los patrones necesarios para realizar una evaluación correcta de los dispositivos.



	A	B	C	D	E
1		***3.- Gestión / Operación de dispositivos***			
2		**Objetivo:** Garantizar una gestión adecuada de: - ATM durante la fabricación. - ATM en el almacenamiento de polígonos ATM desplegados. - ATM configuración de seguridad individual (hardware y software).			
3		**C. OBJETIVOS DE SEGURIDAD**			
4	**Nro.**	**Detalle**	**Cumple**	**check**	**Observaciones**
5	C1	Establezca controles adecuados para la producción, transporte, almacenamiento y uso del dispositivo durante todo su ciclo de vida hasta la implementación inicial.	NO	☐	
6	C2	Garantizar una adecuada inicialización criptográfica y servicio.	SI	☑	
7	C3	Garantice la distribución segura de software, actualizaciones / parches que afecten la seguridad, y las aplicaciones no financieras, incluidos los anuncios.	SI	☑	
8	C4	Administre un inventario actualizado de cajeros automáticos y sus configuraciones, incluidos su hardware, software, registros e informes.	NO	☐	
9	C5	Gestione el ciclo de vida, desde la fabricación y la inicialización hasta el desmantelamiento.	NO	☐	
10	C6	Especificar y ejecutar procedimientos de desmantelamiento de seguridad adecuados.	SI	☑	
11	C7	Asegúrese de que las piezas de repuesto y los cajeros automáticos o piezas fuera de servicio tengan información clave y otros datos confidenciales eliminados.	NO	☐	
12	C8	Apoyar la educación del usuario en el cajero automático.	NO	☐	

Fig. 10. Gestión/Operación de dispositivos
Fuente Propia

En la Fig. 11. Se encuentran los ítems de Administración de aplicaciones ATM para evaluar cajeros automáticos, basados en los lineamientos de la normativa PCI DSS/PTS, que es el órgano regulador que emite los patrones necesarios para realizar una evaluación correcta de los dispositivos.



	A	B	C	D	E
1		***4.- Gestion de aplicaciones ATM***			
2		**Objetivo:** Abordar los aspectos de seguridad de la aplicación ATM.			
3		**D. OBJETIVOS DE SEGURIDAD**			
4	**Nro.**	**Detalle**	**Cumple**	**check**	**Observaciones**
5	D1	Aplicar las mejores prácticas para el desarrollo, prueba y distribución de aplicaciones.	SI	☑	
6	D2	Asegure la efectividad de las funciones de seguridad manejadas por la aplicación.	SI	☑	
7	D3	Asegúrese de que la aplicación ATM interactúa de forma segura con la pantalla ATM y EPP.	SI	☑	

Fig. 11. Gestión de aplicaciones ATM
Fuente: Propia

2.6. Implementación de un caso práctico de Evaluación de Auditoria a Entidad Financiera Cooperativa “XYZ”

Por confidencialidad de la auditoría realizada, la información de la entidad financiera evaluada no se puede divulgar, motivo por el cual se ha creado un nombre de entidad financiera ficticia, en este caso práctico la llamaremos Cooperativa “XYZ”, la misma que contiene datos reales de una auditoria de cajeros automáticos.

2.6.1. Cooperativa “XYZ”

En el presente análisis se plantea un estudio sobre el servicio ofrecido por el cajero automático perteneciente a la Cooperativa “XYZ”, mediante este informe se expone un análisis físico sobre el manejo, medición y monitoreo de los procesos básicos ejecutados por el cajero, ligados exclusivamente a los problemas encontrados y reportados por el área de quejas y reclamos de la Cooperativa “XYZ”.

2.7. Análisis técnico implementando la normativa internacional PCI DSS para cajeros automáticos conjuntamente con la normativa PTS

Es importante realizar un diagnóstico del nivel de madurez del servicio entregado por el cajero automático, se ilustra en la Fig. 12., las cuatro fases para realizar el diagnostico de las vulnerabilidades de los cajeros automáticos.

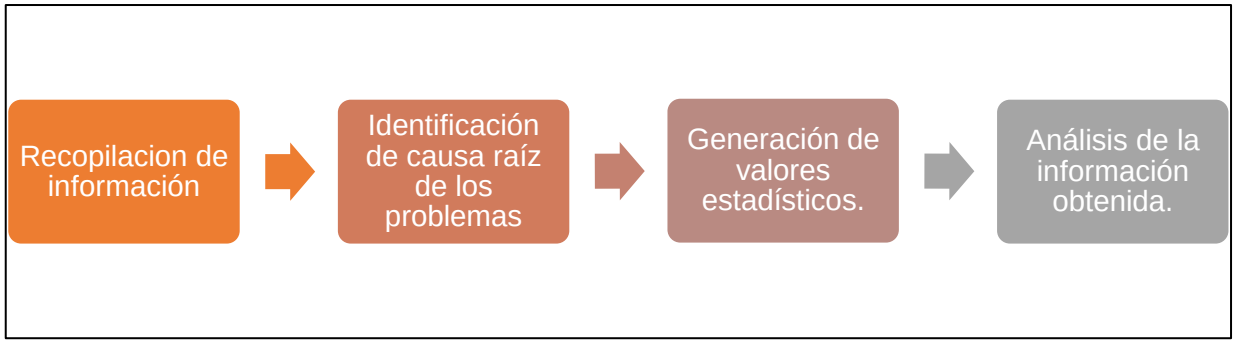


Fig. 12. Fases de diagnostico
Fuente Propia

2.7.1. Fase 1 Recopilación de Información

Se recopila información relevante para el análisis del estado y funcionamiento del cajero automático evaluado, para presentar un informe al administrador de estos dispositivos y les permita tomar las medidas preventivas y correctivas en infraestructura de cajeros automáticos pertenecientes a la Cooperativa “XYZ”, para mejorar la seguridad de sus dispositivos.

2.7.2. Fase 2 Identificación de la causa raíz de los problemas

Es importante mencionar que el cajero automático analizado no presentó problemas encontrados y reportados hacia el área de Quejas y Reclamos de la Cooperativa, por ello se tomó la decisión de realizar este análisis tomando en cuenta los problemas reportados y encontrados por BANRED con respecto a este cajero.

- **Análisis Técnico**

Con respecto a las actividades de revisión y cumplimiento tomando en cuenta aspectos normativos, estándares y buenas prácticas, se realizó el análisis mostrado a continuación.

- **Auditoria de cumplimiento Normativa emitida por entidad de control (SEPS**)

Llevar a cabo una evaluación del grado de cumplimiento de la seguridad a los ATM´s con los mínimos controles emitidos por el ente de control y no limitándose a:

1.- Protección al teclado. - Contar en todo momento con los dispositivos conocidos como "protectores de teclado", que de una manera efectiva impidan la visibilidad al momento que el usuario digita su clave personal.

2.- Protección contra clonación de tarjetas. - Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito o de crédito, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales; (sustituido con resolución No. JB-2012-2148 de 26 de abril del 2012).

3.- Iluminación. - Los cajeros automáticos instalados en áreas externas a las oficinas de las instituciones financieras, deberán estar ubicados en zonas suficientemente iluminadas que permitan la visualización de toda actividad a su alrededor.

4.- Programas de vigilancia en sitio. - Contar con un programa regular de visitas al sitio donde se encuentra instalado el cajero automático, con la finalidad de garantizar que no existan objetos extraños, dispositivos u otros mecanismos sospechosos instalados en el cajero automático.

5.- Mecanismo de anclaje. - Los cajeros automáticos deben asegurarse adecuadamente al piso u otro soporte a fin de que dificulte su remoción, salvo el caso de aquellos que estén empotrados a la pared.

6.- Protección al software e información del cajero automático. - Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberá instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución; (sustituido con resolución No. JB-2012-2148 de 26 de abril del 2012).

7.- Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos. - Disponer de procedimientos auditables debidamente acordados y coordinados entre la institución y los proveedores internos o externos para la ejecución de las tareas de mantenimiento preventivo y correctivo del hardware y software, provisión de suministros y recarga de dinero en las gavetas. Las claves de acceso tipo “administrador” del sistema del cajero automático deben ser únicas y reemplazadas periódicamente; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012).

8.- Accesos físicos al interior de los cajeros automáticos. - Disponer de cerraduras de alta tecnología y seguridades que garanticen el acceso controlado al interior del cajero automático

por parte del personal técnico o de mantenimiento que disponga de las respectivas llaves. Estas cerraduras deben operar con llaves únicas y no genéricas o maestras; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012).

9.- Reportes de nivel de seguridad de los cajeros. - Comunicar oportunamente la información sobre los estándares de seguridad implementados en los cajeros automáticos, incidentes de seguridad (vandalismo y/o fraudes) identificados en sus cajeros automáticos y/o ambientes de software o hardware relacionados; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012).

10.- Establecer los mecanismos y procedimientos adecuados para: (renumerado con resolución No. JB-2012-2148 de 26 de abril del 2012)

- Revisar periódicamente los anclajes, iluminación y entorno del cajero automático.
- Abastecer de dinero permanentemente a los cajeros automáticos.
- Atender las alarmas generadas por los dispositivos electrónicos de control instalados en los cajeros automáticos.
- Contar con personal capacitado para la operación y mantenimiento diario del cajero.

11.- Campañas de capacitación a usuarios sobre medidas preventivas y buen uso del sistema. - Llevar a cabo campañas educativas para los usuarios acerca del uso, ubicación y medidas de seguridad pertinentes durante el uso del cajero, incluyendo la colocación de letreros alusivos a éstas en los recintos de los cajeros; y, (renumerado con resolución No. JB-2012-2148 de 26 de abril del 2012).

12.- Sistema de grabación o archivo de imágenes. - Las instituciones financieras deberán mantener un archivo de cintas, de discos de video digital (DVD) o cualquier otro sistema de grabación o su equivalente en cámaras fotográficas que cubra por lo menos noventa (90) días de archivo de imágenes. (renumerado con resolución No. JB-2012-2148 de 26 de abril del 2012).

En la TABLA 2.3 se encuentran los hitos o puntos evaluados de la Normativa PCI DSS/PTS con respecto al cumplimiento de la normativa emitida por la Superintendencia Económica Popular y Social, con respecto a cajeros automáticos de agencias bancarias del país.

TABLA 2.3
Hitos de cumplimiento de la normativa SEPS.

Nro.	Hitos de normativa (SEPS)	Cumplimiento
1	Protección al teclado.	SI
2	Protección contra clonación de tarjetas.	NO
3	Iluminación	SI
4	Programas de vigilancia en sitio.	SI
5	Mecanismo de anclaje.	SI
6	Protección al software e información del cajero automático.	SI
7	Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos.	SI
8	Accesos físicos al interior de los cajeros automáticos.	SI
9	Reportes de nivel de seguridad de los cajeros.	SI
10	Establecer los mecanismos y procedimientos	
A	Revisar periódicamente los anclajes, iluminación y entorno del cajero automático.	SI
B	Abastecer de dinero permanentemente a los cajeros automáticos.	SI
C	Atender las alarmas generadas por los dispositivos electrónicos de control instalados en los cajeros automáticos.	SI
D	Contar con personal capacitado para la operación y mantenimiento diario del cajero.	SI
11	Campañas de capacitación a usuarios sobre medidas preventivas y buen uso del sistema.	N0
12	Sistema de grabación o archivo de imágenes.	SI

Fuente: Propia

Luego de la evaluación realizada físicamente a cajeros automáticos basado en la normativa emitida por entidad de control (SEPS) Superintendencia Económica Popular y Social, se observa que la mayoría de ítems cumplen con la ley, siendo un minino de ítems que no cumplen y deben ser solucionados de manera inmediata.

- **Pruebas de análisis físicas y vulnerabilidades web realizadas**

Dentro de los principales requerimientos del análisis en las revisiones físicas y análisis web pertenecientes al ATM de la cooperativa “XYZ”, se tienen:

- Escaneo y análisis de vulnerabilidades sobre direcciones IP.
- Auditoría de accesos a información sensible compartida.
- Pruebas de técnicas de cumplimiento de Directrices ATM establecidas en PCI PIN (Transaction Security Point of Interaction Security Requirements PCI PTS):

  - ✓ A – Integración de componentes de hardware.
  - ✓ B – Seguridad de software básico.
  - ✓ C – Gestión / funcionamiento del dispositivo.
  - ✓ D – Gestión de aplicaciones.

Para el éxito de la prueba fue necesario escoger un adecuado kit de herramientas. Para cada dispositivo analizado se empleó un diverso número de herramientas con funcionalidades y características especiales. Hay muchas herramientas disponibles, que pueden ser comerciales y de libre distribución. En la TABLA 2.4 se ilustran las herramientas utilizadas en la evaluación.

TABLA 2.4
Herramientas para el análisis de vulnerabilidades

Nro.	Herramienta	Descripción
1	Nmap Free	Análisis de puertos
2	WinAudit Free	Análisis de Software y Hardware de ATM´s
3	Sparta Free	Análisis de puertos y vulnerabilidades
4	Nikto Free	Análisis de vulnerabilidades web
5	Uniscan Free	Análisis de vulnerabilidades web
6	Kali Linux Free	Sistema Operativo de Ciberseguridad

Fuente: Propia

- **Nmap**

Es una herramienta para el escaneo de puertos disponibles en un equipo, se presenta la información del equipo analizado como se ilustra en la Fig. 13.

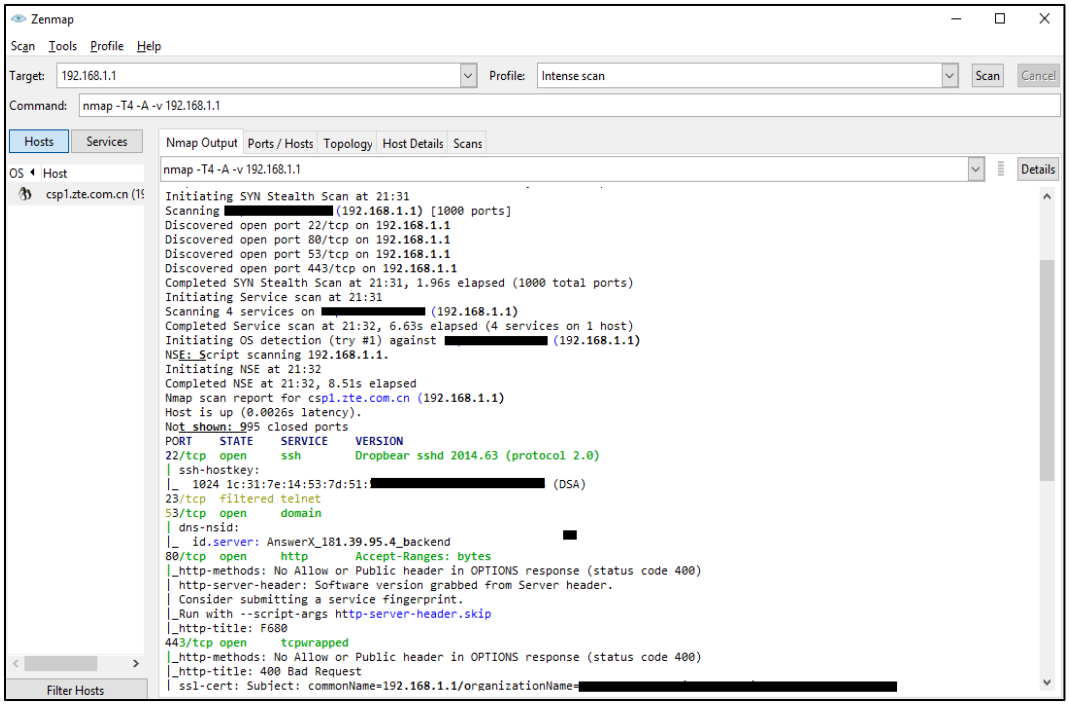


Fig. 13. Escaneo de puertos
Fuente: Propia

En la Fig. 14. Se ilustra los puertos habilitados que contiene el cajero automático analizado, por medio de un informe se presenta al administrador, quien tomarán las medidas correctivas correspondientes, para evitar ataques externos e internos al dispositivo.

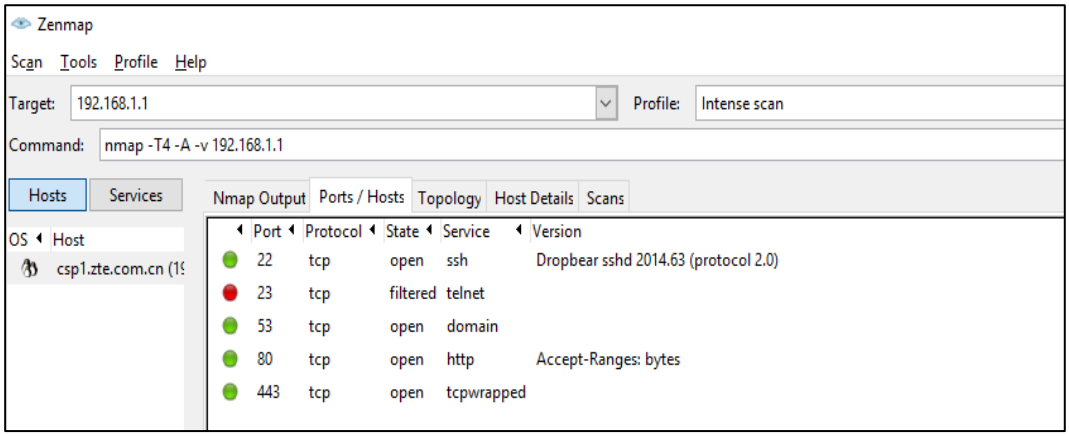


Fig. 14. Puertos abiertos y cerrados
Fuente: Propia

- **WinAudit**

Es una herramienta que permite realizar un diagnóstico exhaustivo de software y hardware presentes en un equipo como se ilustra en la Fig. 15.

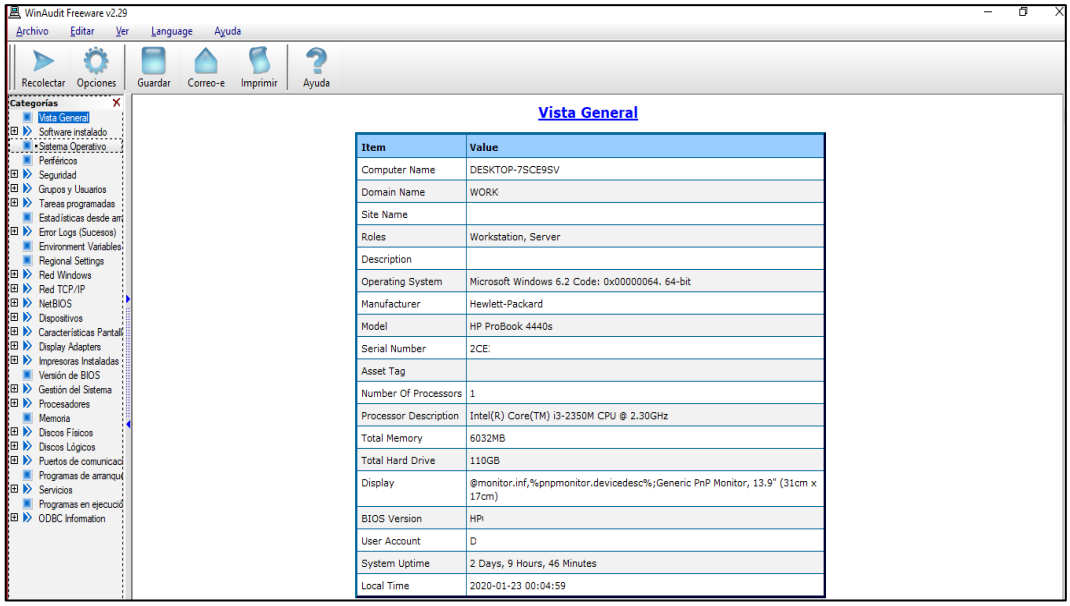


Fig. 15. Escaneo de Hardware y Software
Fuente: Propia

- **Sparta**

Es una herramienta que permite realizar ataques de vulnerabilidades que presentan los equipos, como se ilustra en las Fig. 16.

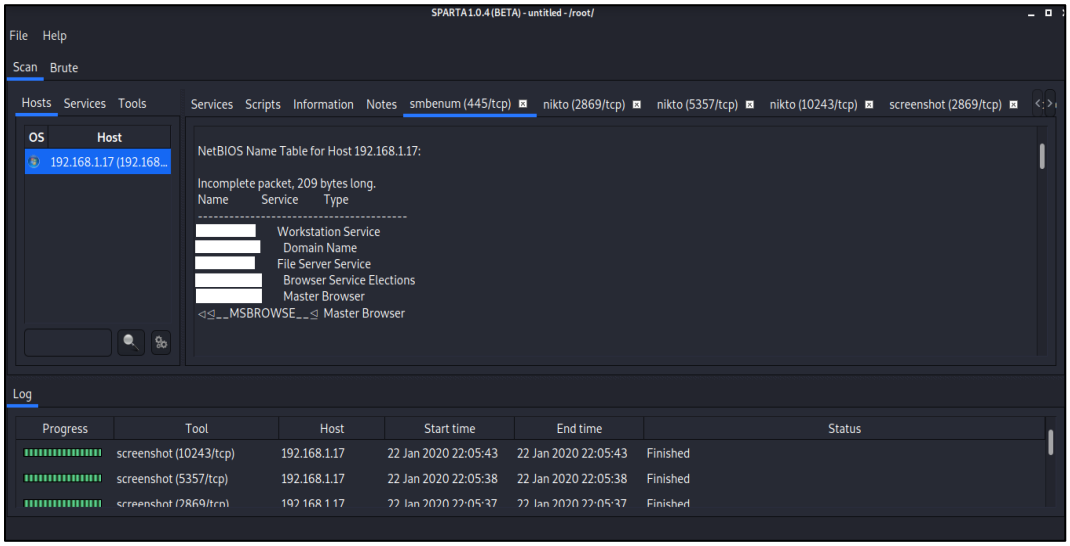


Fig. 16. Detalles del equipo inspeccionado
Fuente: Propia

En la Fig. 17. Se ilustra información del sistema operativo, dirección MAC dirección IP puertos habilitados, del dispositivo escaneado.

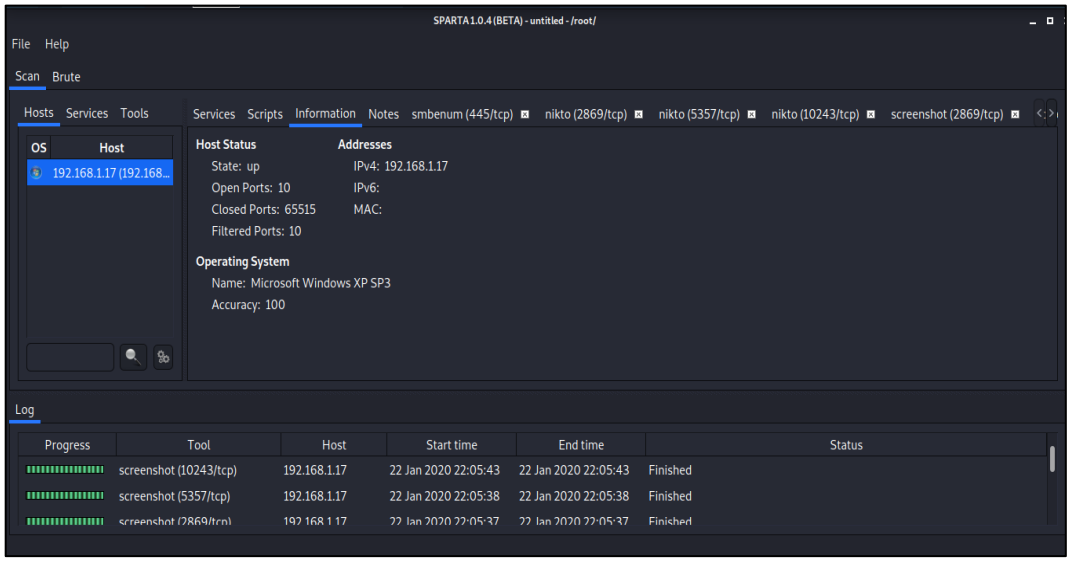


Fig. 17. Información del Sistema Operativo
Fuente: Propia

En la Fig. 18. Se observa un análisis de fuerza bruta en cajero automático analizado, para encontrar las vulnerabilidades a las que se encuentra expuesto.

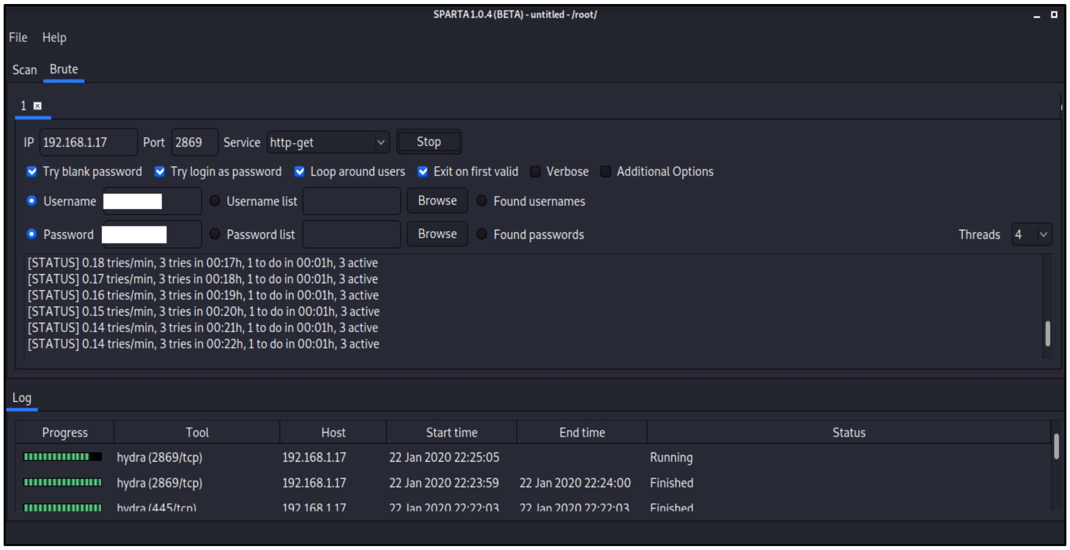


Fig. 18. Análisis de Fuerza bruta
Fuente: Propia

- **Nikto**

Es una herramienta que permite verificar los datos de un servidor instalado en una máquina, también permite saber los niveles de seguridad, para evitar cualquier ataque dirigido de servidores.

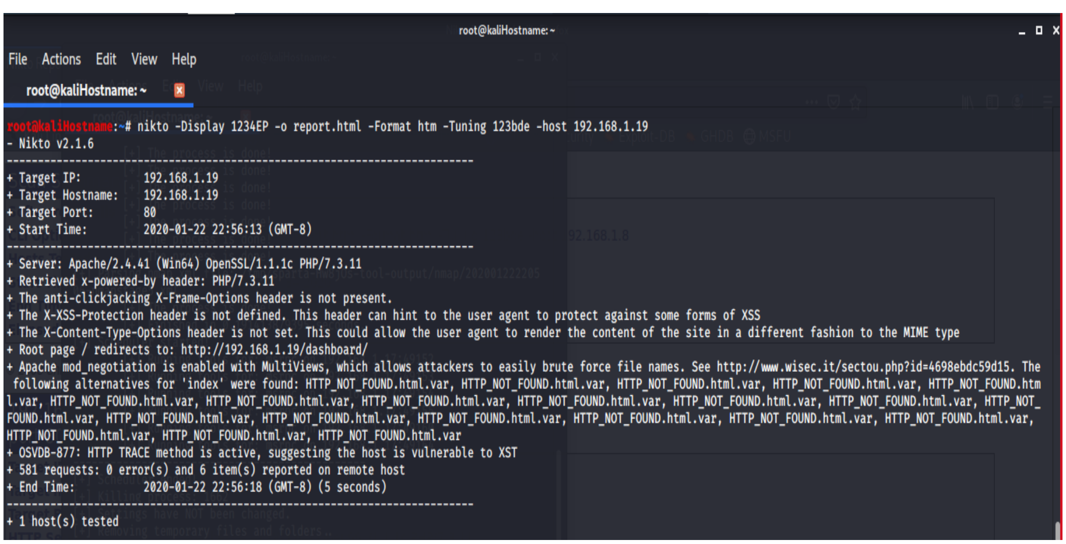


Fig. 19. Análisis de Servidores
Fuente: Propia

- **Uniscan**

Es una herramienta que permite buscar vulnerabilidades en cualquier sitio web, como se ilustra en la Fig. 20.

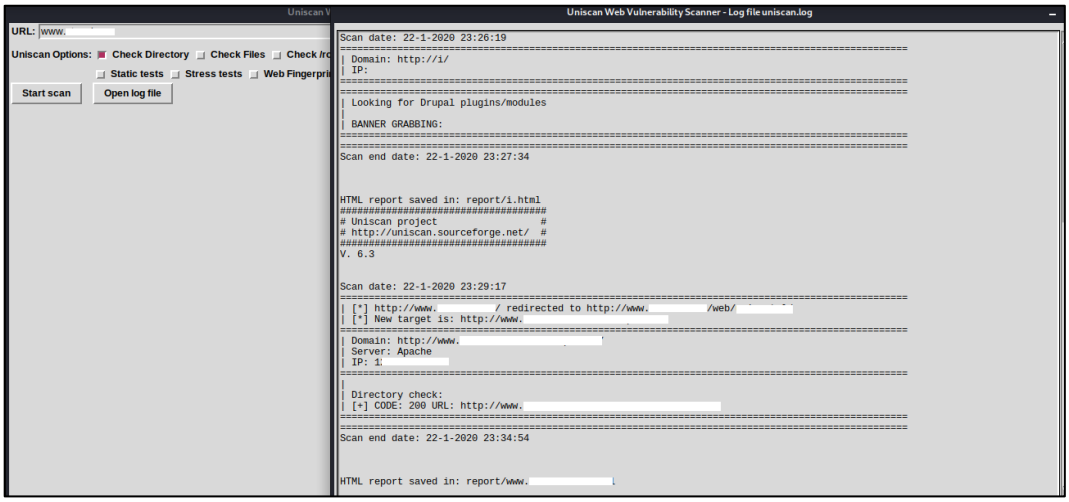


Fig. 20. Vulnerabilidad de un sitio Web
Fuente: Propia

- **Kali linux**

Sistema operativo que contiene varias herramientas para auditoria y seguridad informática

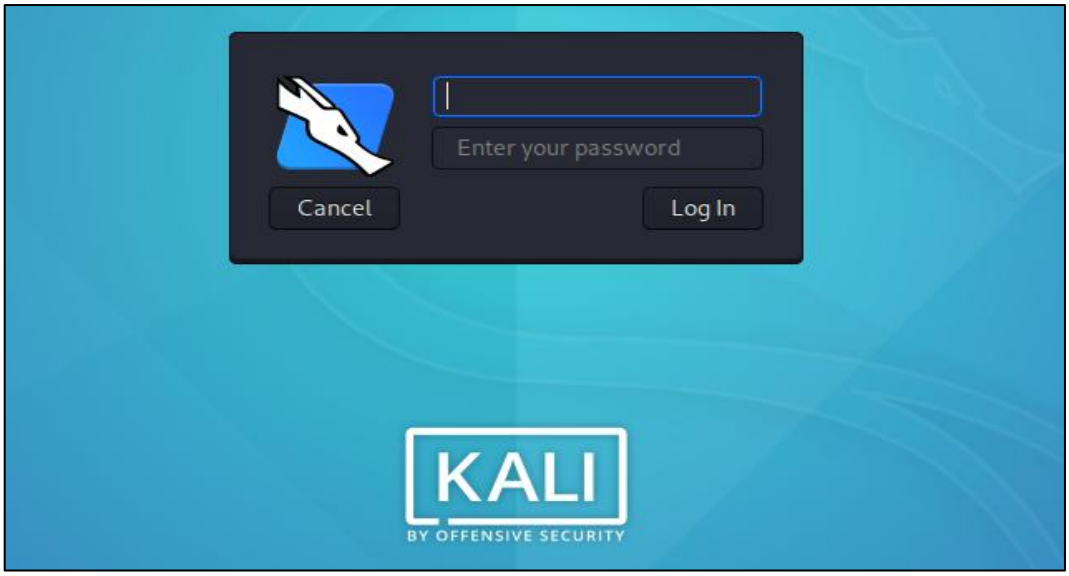


Fig. 21. Kali Linux
Fuente: Propia

En la TABLA 2.5 se encuentran las directrices para la auditoria de cajeros automáticos, basados en la normativa PCI DSS/PTS, mismos que servirán como una guía práctica para los auditores de la empresa Greenetics soluciones S.A.

TABLA 2.5
Directrices ATM establecidas en PCI DSS/PTS

Objetivo	Descripción	Cumplimiento
	A - Integración de componentes de hardware	
A1	Evitar ataques físicos locales que se dirigen a los datos de la cuenta.	SI
A2	Evitar ataques físicos locales que apuntan a los PIN.	SI
A3	Evita los ataques destinados a robar datos criptográficos y confidenciales almacenados en componentes seguros.	NO
A4	Evita los ataques para deshabilitar las contramedidas de seguridad agregadas al cajero automático.	SI
A5	Mitigar el posible impacto negativo derivado de la integración de módulos de servicio en cajeros automáticos.	SI
A6	Proteger contra el acceso no autorizado a áreas y recursos sensibles en el gabinete, incluida la fascia.	SI
A7	Producir una configuración de seguridad del modelo ATM.	SI
A8	Proporcionar pautas de seguridad para integradores de hardware y software.	SI
A9	Proporcionar pautas de seguridad para el personal de servicio.	SI
A10	Asegúrese de que la eliminación o el acceso no autorizado al EPP active una alarma.	SI
A11	Evite modificaciones del hardware que puedan reducir el nivel de protección de seguridad.	SI
A12	Asegure las comunicaciones entre los módulos dentro del cajero automático.	SI
A13	Los datos sin contacto deben asegurarse a 16 puntos desde el punto de digitalización de los datos.	SI
	B - Seguridad de software básico	
B1	Evitar el abuso del sistema operativo y reduzca la superficie de ataque de la plataforma ATM OS (Windows) y el BIOS.	SI
B2	Evitar la explotación de vulnerabilidades de dominio público en la pila de protocolos abiertos.	SI
B3	Reduce la superficie de ataque de las redes públicas y privadas.	SI
B4	Prevenir el abuso por parte de los proveedores de software.	SI
B5	Utilice herramientas eficaces de aislamiento de red y detección / mitigación de intrusos.	SI
B6	Rastrear / registrar la actividad del sistema operativo.	NO
B7	Proteja las funciones sensibles y los mecanismos de aplicación para los procedimientos apropiados de carga de claves	SI
B8	Proteger contra cambios no autorizados.	NO
B9	Proteja contra el control remoto no autorizado de la aplicación.	SI
B10	Proteger nuevamente la instalación no autorizada de software.	NO
	C - Gestión / funcionamiento del dispositivo	
C1	Establecer controles adecuados para la producción, transporte, almacenamiento y uso del dispositivo durante todo su ciclo de vida hasta la implementación inicial.	NO
C2	Garantizar una adecuada inicialización criptográfica y servicio.	SI

C3	Garantizar la distribución segura de software, actualizaciones / parches que afecten la seguridad, y las aplicaciones no financieras, incluidos los anuncios.	SI
C4	Administrar un inventario actualizado de cajeros automáticos y sus configuraciones, incluidos su hardware, software, registros e informes.	NO
C5	Gestionar el ciclo de vida, desde la fabricación y la inicialización hasta el desmantelamiento.	NO
C6	Especificar y ejecutar procedimientos de desmantelamiento de seguridad adecuados.	SI
C7	Asegurar de que las piezas de repuesto y los cajeros automáticos o piezas fuera de servicio tengan información clave y otros datos confidenciales eliminados.	NO
C8	Apoyar la educación del usuario del cajero automático.	NO
	D - Gestión de aplicaciones ATM	
D1	Aplica las mejores prácticas para el desarrollo, prueba y distribución de aplicaciones.	SI
D2	Asegura la efectividad de las funciones de seguridad manejadas por la aplicación.	SI
D3	Asegura que la aplicación ATM interactúe de forma segura con la pantalla ATM y el EPP.	SI

Fuente: Propia

Luego de evaluar las directrices ATM establecidas en la normativa PCI DSS/PTS, aplicada a cajeros automáticos se obtuvo que la mayoría de ítems cumplen con la normativa implementada en la cooperativa “XYZ”, siendo un minino de ítems que no cumplen y deben ser solucionados de manera inmediata.

2.7.3. Fase 3 Generación de valores estadísticos

Se realiza un análisis de las pruebas de seguridad física en cajero automático evaluado para obtener datos estadísticos con las vulnerabilidades encontradas en el dispositivo.

- **Pruebas físicas en cajeros automáticos**

Estas pruebas se realizaron con acceso físico al cajero automático, contando con previa autorización de la Cooperativa y acompañamiento por parte del personal correspondiente. En la (TABLA 2.6), se presenta la revisión llevada a cabo en el cajero automático de la Cooperativa “XYZ”, de nombre Cajero1 y haciendo uso del usuario provisto:

TABLA 2.6

Pruebas de seguridad y revisiones físicas sobre cajero

HOST NAME: Cajero1 / IP: 192.168.30.19

HALLAZGO	**VALORACIÓN**
El sistema operativo instalado en el cajero automático es Windows Microsoft Windows 7 Professional 32-Bit	
Sistema operativo con antivirus instalado	
El antivirus cuenta con listas de software permitido, en busca de evitar la ejecución de software o archivos maliciosos.	
El antivirus no permite su inhabilitación localmente a pesar de contar con una cuenta de administrador.	
El Firewall de Windows: No habilitado	
Es posible acceder a la BIOS, pero no es posible realizar cambios en la configuración de la misma, dado que existe restricción por contraseña.	
No es posible acceder al boot del sistema, dado que se encuentra protegido por contraseña.	
Se cuenta con una solución de DLP instalada.	
Existen restricciones de uso de dispositivos USB y CD/DVD.	
El sistema operativo no posee credenciales de usuario por defecto.	
Es posible cargar el modo seguro del sistema operativo, pero no es posible evadir los controles de acceso.	
Es posible usar consola de comandos (cmd).	
Es posible ejecutar comandos administrativos, pero no elevar privilegios a SYSTEM.	
No es posible detener servicios del sistema.	
Es posible acceder y modificar información del registro del sistema.	
Se cuenta con políticas de uso de contraseñas y bloqueo de cuenta por número de intentos de acceso fallidos.	
Es posible crear y modificar elementos en el sistema de archivos (discos C y D).	
Es posible crear nuevos usuarios y modificarlos posteriormente.	
Es posible acceder y modificar la configuración de conexiones de red y otras herramientas administrativas.	
No es posible evadir la pantalla transaccional para pasar a la pantalla de inicio de sesión de Windows.	
Permite la instalación de paquetes	
Permite la descarga de información de archivos remotamente vía web	
Sustracción de contraseñas almacenadas	
Puertos abiertos	

Fuente Propia

Con respecto a los 24 controles revisados como parte de las buenas prácticas de seguridad recopiladas en base a estándares, normativas y procedimientos de seguridad sobre cajeros automáticos se tiene que 19 controles se encuentran cumpliendo lo cual representa el 79.17% y 5 controles que no se encuentran implementados, lo cual representa el 20.83%. Esta información se encuentra representada en la Fig. 22.

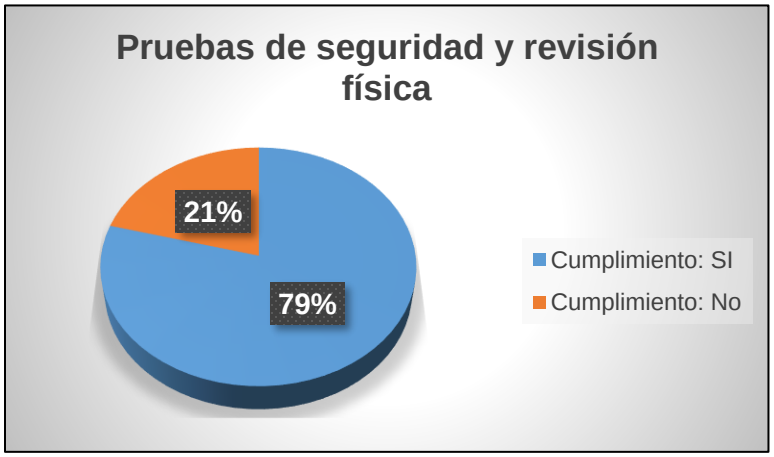


Fig. 22. Pruebas de seguridad y revisiones físicas sobre cajero 1
Fuente: Propia

Descargar el archivo remoto

Factor de Riesgo: **Crítico**

CVE: No disponible

Elementos afectados

A continuación, se presenta la dirección IP de los elementos afectados:

- 192.168.30.19 / XYZ

Evidencia

En las siguientes Fig. 23. Se puede observar la materialización del hallazgo encontrado en la evaluación realizada.

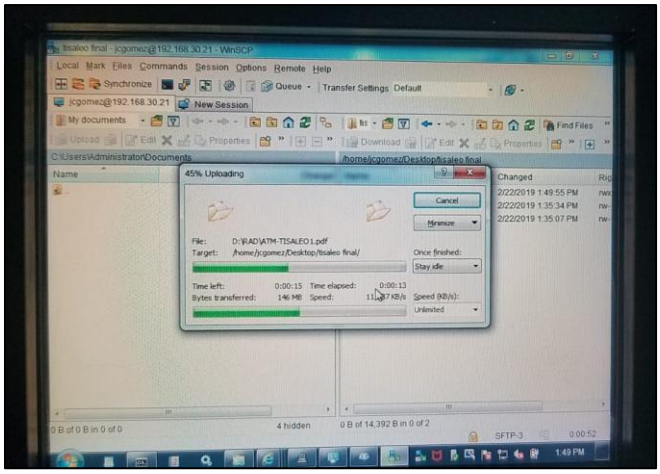


Fig. 23. Descarga Remota de Archivos
Fuente: Propia

Firewall de Windows deshabilitado

Factor de Riesgo: **Medio**

CVE: No disponible

El equipo tiene el firewall de Windows deshabilitado, lo cual podría permitir conexiones entrantes o salientes no autorizadas que puedan llegar a comprometer la confidencialidad, integridad y disponibilidad del equipo y su información.

Elementos afectados

A continuación, se presenta la dirección IP de los elementos afectados:

- 192.168.5.17 / XYZ

Evidencia

En la Fig. 24. Se puede observar la materialización del hallazgo que el Firewall de Windows se encuentra deshabilitado, siendo un factor de riesgo medio.

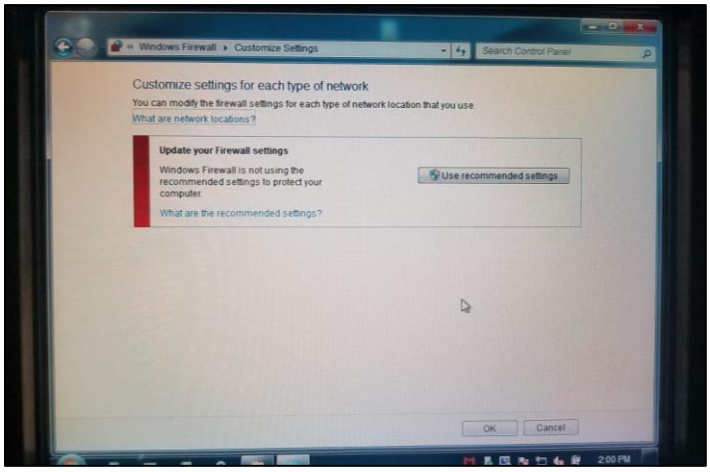


Fig. 24. Firewall deshabilitado en equipo Cajero1
Fuente: Propia

2.7.4. Fase 4 Análisis de la información obtenida

Se analiza cada uno de los eventos realizados en la auditoria, para elaborar un informe final detallando las vulnerabilidades que se han encontrado en el cajero automático, para que los administradores de estos dispositivos ejecuten medidas correspondientes.

- **Estado de los puertos**

Luego del escaneo de puertos del cajero automático se tuvieron los resultados que contiene la (TABLA 2.7).

TABLA 2.7
Estado de los puertos de la ATM

Puerto	Protocolo	Estado	Servicio	Versión
0.0.0.0:135	TCP	Abierto	msrpc	Microsoft Windows RPC
0.0.0.0:139	TCP	Abierto	netbios-ssn	Microsoft Windows netbios-ssn
0.0.0.0:2291	TCP	Abierto	netprobe	Mega System Technologies NetProbe Lite environmental sensor
0.0.0.0:5700	TCP	Abierto	tcpwrapped	
0.0.0.0:6217	TCP	Abierto	mc-nmf	.NET Message Framing
0.0.0.0:8043	TCP	Abierto	http	MS .NET Remoting httpd (.NET CLR 4.0.30319.36415)
0.0.0.0:8081	TCP	Abierto	http	McAfee AntiVirus
0.0.0.0:9338	TCP	Abierto	unknown	
0.0.0.0:49152	TCP	Abierto	msrpc	Microsoft Windows RPC
0.0.0.0:49153	TCP	Abierto	msrpc	Microsoft Windows RPC

0.0.0.0:49154	TCP	Abierto	msrpc	Microsoft Windows RPC
0.0.0.0:49176	TCP	Abierto	msrpc	Microsoft Windows RPC
0.0.0.0:49248	TCP	Abierto	msrpc	Microsoft Windows RPC
127.0.0.1:4141	TCP	Abierto		
127.0.0.1:4141	TCP	Abierto		
127.0.0.1:4141	TCP	Abierto		
127.0.0.1:8118	TCP	Abierto		
127.0.0.1:9000	TCP	Abierto		
127.0.0.1:10001	TCP	Abierto		
127.0.0.1:49463	TCP	Abierto		
127.0.0.1:49463	TCP	Abierto		
127.0.0.1:49464	TCP	Abierto		
127.0.0.1:49465	TCP	Abierto		
127.0.0.1:49466	TCP	Abierto		
127.0.0.1:51204	TCP	Abierto		
127.0.0.1:51205	TCP	Abierto		
127.0.0.1:53271	TCP	Abierto		
127.0.0.1:53271	TCP	Abierto		
127.0.0.1:53272	TCP	Abierto		
127.0.0.1:53273	TCP	Abierto		
127.0.0.1:53476	TCP	Abierto		
127.0.0.1:53476	TCP	Abierto		
127.0.0.1:53476	TCP	Abierto		
127.0.0.1:53477	TCP	Abierto		
127.0.0.1:53478	TCP	Abierto		
127.0.0.1:53479	TCP	Abierto		
192.168.30.19:139	TCP	Abierto		
92.168.30.19:49372	TCP	Abierto		
92.168.30.19:49601	TCP	Abierto		
0.0.0.0:500	UDP	Abierto		
0.0.0.0:4500	UDP	Abierto		
0.0.0.0:8082	UDP	Abierto		
192.168.30.19:137	UDP	Abierto	netbios-ns	
192.168.30.19:138	UDP	Abierto	netbios-dgm	

Fuente: Propia

- **Hurto de contraseñas**

Una contraseña débil puede llegar a exponer el equipo o grupo de equipos a los cuales tenga acceso el usuario que sea propietario de la contraseña, por lo cual después de extraer el hash de

contraseñas del Directorio Activo previamente comprometido, se procedió a romper el hash de contraseñas y a efectuar un análisis sobre las mismas el cual se presenta en la (TABLA 2.8).

TABLA 2.8
Accesos a contraseña

Username	Password	Domain
Service_USR	mP?5=4KafG!72oY-{N3yn1$FJb0+*Bz68s}C/9Mt3w&XW%0j_6rRAi%24Zk?e8_Q1}Hdx9!E5Sc/g7+LDp5-$1Tq0Yq*{y8N2Rn	ATM-XYZ
Manage_ATM	Am********o23	ATM-XYZ
Service_USR	n}S-3PrCy1%{7GeoL&58gA$+H4xb2/KRj6_9!zQwE*7M0t?8=Wdq5-T4%DpN6s&3+ZiJ9c_=X1km{F2Ya8!3B$fZb4*n/K17e?DwF0}%6iWCy	ATM-XYZ
Servantivir	**rvi***	Xxxxx
Diebold_ATM	Null	ATM-XYZ
LOCAL SERVICE	Null	NT AUTHORITY
ATM-TISALEO1$	Null	WORKGROUP
Null	Null	Null
ATM-TISALEO1$	Null	WORKGROUP

Fuente Propia

- **Resumen del Sistema**

Se puede observar en la Fig. 25. Como el software de análisis obtiene la información importante y así es como en la primera tabla muestra el resumen general del sistema como: nombre de la PC, nombre del Dominio, S.O., procesador, memoria, disco duro, etc.; con ese tipo de información ya se puede obtener una idea de cómo está trabajando el dispositivo.

Item	Value
Computer Name	ATM- XYZ
Domain Name	WORKGROUP
Site Name	
Roles	
Description	
Operating System	Microsoft Windows 7 Professional 32-Bit
Manufacturer	XYZ
Model	VoyagerHP
Serial Number	To Be Filled By O.E.M.
Asset Tag	To Be Filled By O.E.M.
Number Of Processors	1
Processor Description	Intel(R) Core(TM) i5-4570TE CPU @ 2.70GHz
Total Memory	3504MB
Total Hard Drive	465GB
Display	XYZ 104, 10.2" (21cm x 15cm)
BIOS Version	XYZ - 3 BIOS Date: 02/24/17 11:35:23 Ver: 04.06.05 BIOS Date: 02/24/17 11:35:23 Ver: 04.06.05
User Account	Manage_ATM
System Uptime	0 Days, 0 Hours, 22 Minutes
Local Time	2019-02-22 13:15:45

Fig. 25. Análisis del Software
Fuente: Propia

- **Programas instalados**

En la Fig. 26. Se ilustra el grafico porcentual con la información obtenida de software, la misma que dio como resultado la existencia de 305 programas instalados de los cuales 26 mantienen configuración activa, siendo tan solo el 8 %.

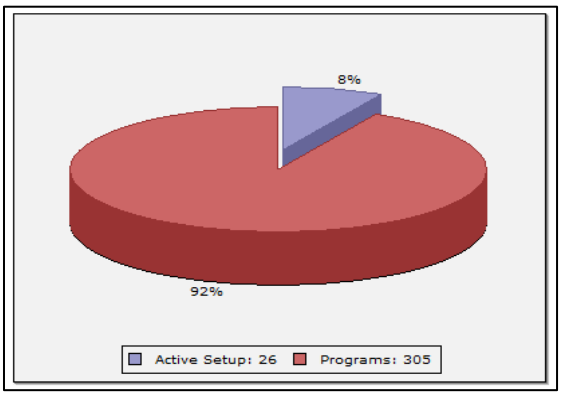


Fig. 26. Información de Programas Instalados
Fuente: Propia

- **Sistema Operativo**

En la Fig. 27. Se ilustra el detalle del sistema operativo Windows 7 Profesional Service Pack 1 en análisis realizado al dispositivo, según registro ha funcionado adecuadamente desde su instalación el 1 de enero del 2018, no se debe confundir un funcionamiento adecuado con un funcionamiento óptimo.

Name	Value
Name	7
Edition	Professional
Install Date	1/15/2018
Registered Owner	XYZ
Registered Organization	
Product ID	00371-OEM-8992671-00593
Major Version Number	6
Minor Version Number	1
Build Number	7601
Service Pack	Service Pack 1
Service Pack Version	1.0
Plus! Version Number	
DirectX Version	9.0c
Windows Directory	C:\Windows\
System Directory	C:\Windows\system32\
Temporary Directory	C:\Users\ADMINI~1\AppData\Local\Temp\
Operating System Language	English - United States
Number Of Bits	32

Fig. 27. Información del Sistema Operativo
Fuente: Propia

- **Periféricos**

En la Fig. 28. Se ilustra una tabla de los periféricos a los que el dispositivo tiene acceso, la mayoría de los cuales debe ser de uso exclusivo para personal de mantenimiento del sistema.

Name	Description
Mouse	5 Button Mouse, has wheel
Keyboard	IBM enhanced (101- or 102-key), 12 function keys
Display Description	XYZ , 10.2" (21cm x 15cm)
Printer	Star Journal Printer
Printer	Snowhaven
Printer	EPSON BA-T500 Color Receipt
Network Installed	Yes

Fig. 28. Periféricos que el dispositivo tiene acceso
Fuente: Propia

- **Navegadores de Internet**

En la Fig. 29. Se visualiza dos programas que permiten acceso a la red, siendo el uno Navegador y el otro de tipo email.

Type	Name	Version	Data Update?
Browser	Internet Explorer(TM)	9.11.9600.18977	
E-mail	Windows Mail(TM)	6.1.7601.17514	

Fig. 29. Programas que permiten acceso a la red
Fuente: Propia

- **Grupos y Usuarios**

En cuanto a Grupos y Usuarios como se observa en la Fig. 30. Se encontró un Grupo Local con 3 miembros y todos con privilegios de Administrador.

Administrators

Name	Value
Group Type	Local
Group Name	Administrators
Comment Item	Administrators have complete and unrestricted access to the computer/domain

Members

Group Name	Member Name
Administrators	Manage_ATM
Administrators	Service_ATM
Administrators	SYSTEM

Fig. 30. Grupos y Usuarios
Fuente: Propia

- **Red TCP/IP**

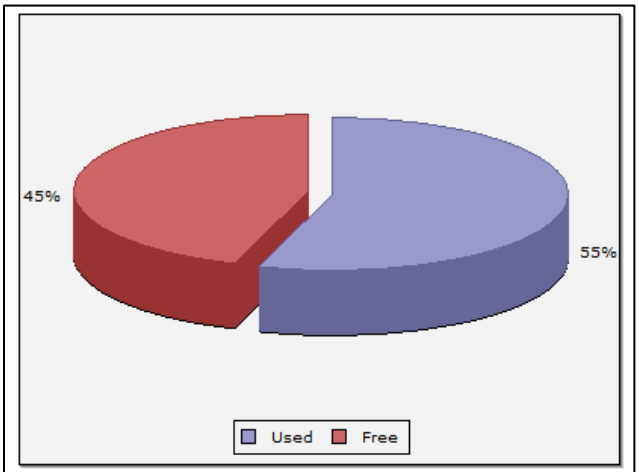
En el análisis realizado ilustra la Fig. 31. Información de la red como IP, DNS, DHCP, DNS Host Name y MAC Address que es la identificación única que tienen todos los dispositivos.

Item	Value
Adapter Number	1
Adapter Name	Intel(R) I210 Gigabit Network Connection
DNS Host Name	ATM-XYZ
DNS Servers	192.168.[redacted]
IP Address	192.168.[redacted]
IP Subnet	255.255.255.248
Default IP Gateway	192.168.[redacted]
DHCP Enabled	No
DHCP Server	
DHCP IP Address	
Status Code	0
Adapter Status	This device is working properly.
Adapter Type	Ethernet 802.3
MAC Address	[redacted]
Connection Status	Connected
Connection Speed	100 Mbps

Fig. 31. Información de red
Fuente: Propia

- **Memoria**

En la Fig. 32. Se observa el funcionamiento adecuado de la memoria, tiene el 55 % trabajando en procesos asignados.



Item	Value
Total Memory	3504MB
Free Memory	1591MB
Maximum Swap File	8192MB
Free Swap File	9802MB

Fig. 32. Estado de la memoria del dispositivo
Fuente: Propia

En la TABLA 2.9 se observa que el Disco Duro tiene 4 unidades de almacenamiento y en la Fig. 33. Se ilustra el espacio ocupado según la partición:

TABLA 2.9
Estado del disco duro

Unidad	Espacio Total	Espacio Libre	Espacio Ocupado
C:	325GB	283	42,4
D:	140GB	138	2,49
E:	CD-ROM	0	0
F:	28,8GB	28,6	0,2

Fuente Propia

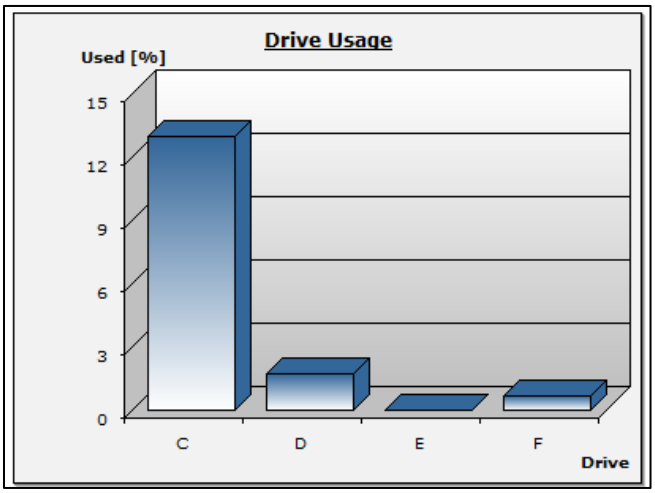


Fig. 33. Espacio del disco duro según su partición.
Fuente: Propia

- **Puertos de comunicación**

En la Fig. 34. Se observa una lista de los puertos de Comunicación que posee el dispositivo y se encuentran habilitados.

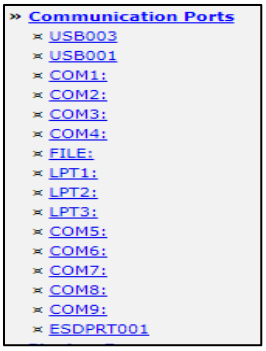


Fig. 34. Listado de puertos habilitados
Fuente: Propia

- **Información ODBC (Conectividad de Base de Datos Abierta)**

En la Fig. 35. Se observa el análisis realizado de los drivers ODBC que tiene instalado el dispositivo que les permitirían el acceso a diferentes bases de datos.

Fig. 35. Drivers ODBC (Conectividad de Base de Datos Abierta)
Fuente: Propia

- **Análisis de componentes físicos**

Como parte de un análisis y test de intrusión de los ATM´s, también se debe considerar la parte externa del dispositivo, porque el buen o mal funcionamiento del mismo dependerá tanto del estado físico externo e interno del dispositivo.

- **Estado del ATM**

En la Fig. 36. Se ilustra, la evaluación del estado General externo del dispositivo tal y como pantalla, teclado y toda la parte exterior que tenga la señalización y la iluminación adecuada.

Fig. 36. Visualización del cajero automático externamente
Fuente Propia

- **Cámaras de seguridad**

Como se ilustra en la Fig. 37. El cajero evaluado cuenta con las seguridades respectivas tanto externas como internas con las cámaras de seguridad en los puntos específicos para tener una visión completa del entorno del dispositivo.

Fig. 37. Ubicación de cámaras de seguridad
Fuente: Propia

- **Cableado interno**

Se encontró cableado ubicado de forma incorrecta y de manera improvisada, siendo que es la parte más importante para mantener la conectividad del dispositivo como se ilustra en la Fig. 38.

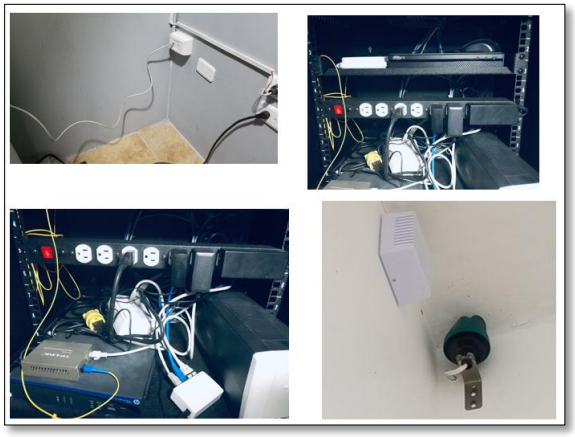


Fig. 38. Cableado Interno de la Cooperativa XYZ
Fuente: Propia

- **Seguridad interna ATM**

En la Fig. 39. Se ilustra la seguridad interna del ATM que posee acceso llaves, puerta magnética, control de acceso mediante libreta de apuntes y por otro lado el efectivo es resguardado mediante caja fuerte.

Fig. 39. Seguridad Interna del ATM
Fuente: Propia

- **Fuente alternativa de energía**

En caso de que la fuente principal de energía eléctrica se suspenda, existe una fuente alterna que provee de energía por un lapso aproximado de 30 minutos. El equipamiento utilizado se ilustra en la Fig. 40.

Fig. 40. Seguridad de la Fuente interna del ATM
Fuente: Propia

- **Sensores**

Se encontraron dispositivos de monitoreo que registran los procesos o sucesos que se van dando en el interior del cajero automático y en el funcionamiento del dispositivo analizado como se ilustra en la Fig. 41.

Fig. 41. Dispositivos de monitoreo
Fuente: Propia

- **Periféricos Externos**

Los periféricos externos como mouse, teclado y pantalla se utilizan para dar los respectivos mantenimientos y no está permitido introducir dispositivos de almacenamiento extraíble como CD´s, USB´s, DVD´s, etc., para efectos del análisis para comprobar las seguridades del dispositivo ATM se procedió a introducir una USB 3.0 Kingston y fue rechazada automáticamente tal y como se muestra en las imágenes a continuación como se ilustra en la Fig. 42.

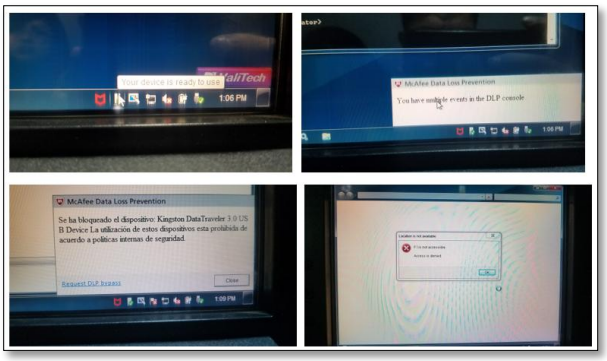


Fig. 42. Conexiones de puertos seguras
Fuente: Propia

CAPITULO III:

Resultados

3.1. Comprobación de resultados obtenidos con la implementación de la normativa PCI DSS/PTS

Previo al análisis realizado en la empresa Greenetics Soluciones S.A., no se ha encontrado una normativa internacional que permita a la empresa realizar auditorías en cajeros automáticos, para solventar este inconveniente se ha procedido a implementar la normativa internacional PCI-DSS conjuntamente con la PTS, estableciendo una lista con controles de seguridad física a cajeros automáticos que cada entidad bancaria debe mantener. Es necesario establecer la normativa PCI-DSS/PTS para establecer una máxima seguridad a un cajero automático.

Con respecto al cumplimiento y tomando en cuenta la auditoria basada en los hitos de la Normativa emitida por ente de control (SEPS) se obtuvo que el cajero evaluado cumple con 13 controles de seguridad, lo cual representa el 87% de los controles, mientras que 2 de los controles no cumplen con la normativa, lo cual representa el 13%, esta información se encuentra representada en la Fig. 43.

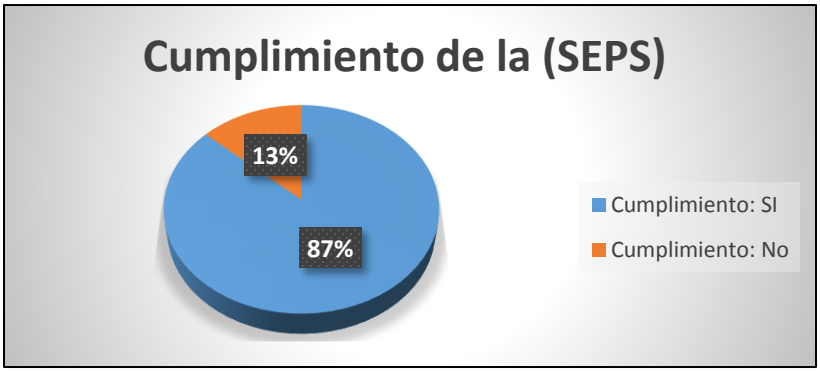


Fig. 43. Resumen de cumplimiento de hitos de normativa SEPS
Fuente: Propia

En la TABLA 3.1 se encuentra el análisis de los resultados obtenidos al realizar la evaluación en el cajero automático perteneciente a la Cooperativa XYZ, exponiendo cada uno de los literales cumplidos por la normativa para cajeros automáticos de la (TABLA 2.3) directrices ATM establecidas en PCI DSS/PTS.

TABLA 3.1
Resumen de Directrices ATM establecidas en PCI

Objetivo	Descripción	Cumplimiento		
		SI	**NO**	**TOTAL**
A	Integración de componentes de hardware	12	1	13
B	Seguridad de software básico	7	3	10
C	Gestión / funcionamiento del dispositivo	3	5	8
D	Gestión de aplicaciones	3		3
	TOTAL	**25**	**9**	**34**

Fuente Propia

Respecto a los 34 controles establecidos en la normativa PCI DSS/PTS se evidencio un total de 25 controles lo cual representa el 74%, no se evidenció un total de 9 controles lo cual representa un 26% esta información se encuentra representada en la Fig. 44.

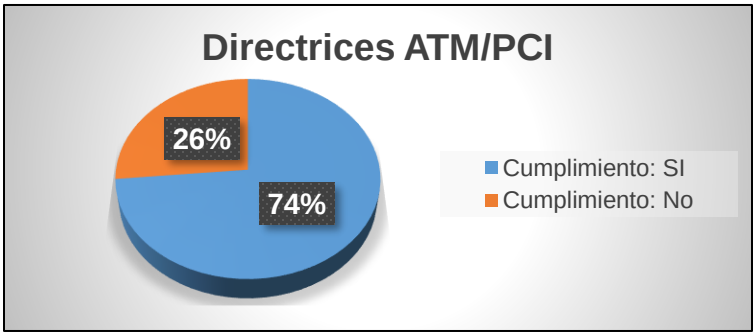


Fig. 44. Cumplimiento de Requerimientos ATM basado en PCI
Fuente: Propia

3.2. Análisis de Impacto

El siguiente análisis se establece el impacto económico, social y ambiental presentes en el proyecto, en la TABLA 3.2, se plantea la calificación según el impacto positivo o negativo, los cuales serán valorados de la siguiente manera:

TABLA 3.2
Valor de Impacto

Valor	Impacto
-3	Alto negativo
-2	Medio negativo
-1	Bajo negativo
0	No hay impacto
1	Bajo positivo
2	Medio positivo
3	Alto positivo

Fuente: (Nathan & Scobell, 2012)

3.2.1. Impacto económico

En la TABLA 3.3, se realizará una matriz que contendrá en el lado izquierdo el indicador, el cual será valorado con el nivel de impacto, para obtener información que permita matemáticamente saber cuál es el nivel de impacto económico del proyecto. Los valores se han considerado tomando en cuenta la información recopilada en auditoria del cajero automático de la cooperativa “XYZ”.

TABLA 3.3
Matriz impacto económico

Nivel de impacto / Indicador	-3	-2	-1	0	1	2	3	Total
Transferencias directas							X	3
Pago de servicios							X	3
Seguridad en inmediaciones bancarias							X	3
Total							**9**	**9**

Fuente: (Nathan & Scobell, 2012)

Total, de impacto social = 9/3
Total, de impacto social = 3
Nivel de impacto social = Alto positivo

Análisis

El resultado final correspondiente al impacto social del proyecto es:

- Transferencias directas - Alto positivo.
- Pago de servicios - Alto positivo.
- Seguridad en inmediaciones bancarias - Alto positivo.

Gracias a la implementación de los cajeros automáticos en el territorio ecuatoriano, los usuarios de cada entidad bancaria pueden realizar transacciones de forma ágil y sin largas filas permitiendo realizar pagos inmediatos como son los servicios básicos, trasferencia de dinero entre clientes o también conocidas como trasferencias directas, así promoviendo la seguridad y reducir el riego de robo en las afueras de las inmediaciones bancarias.

3.2.2. Impacto social

En la TABLA 3.4, se realizará una matriz que contendrá en el lado izquierdo el indicador, el cual será valorado con el nivel de impacto, para obtener información que permita matemáticamente saber cuál es el nivel de impacto social del proyecto. Los valores se han considerado tomando en cuenta la información recopilada en auditoria del cajero automático de la cooperativa “XYZ”.

TABLA 3.4
Matriz impacto social

Nivel de impacto / Indicador	-3	-2	-1	0	1	2	3	Total
Hábitos de Uso de ATM’s							X	3
Implementación de ATM’s					X			1
Bienestar de usuarios en ATM’s						X		2
Total					**1**	**2**	**3**	**6**

Fuente: (Nathan & Scobell, 2012)

Total, de impacto social = 6/3
Total, de impacto social = 2
Nivel de impacto social = Medio positivo

Análisis

El resultado final correspondiente al impacto social del proyecto es:

- Hábitos de uso ATM´s - Alto positivo.
- Implementación de ATM´s - Bajo positivo.
- Bienestar de usuarios en ATM´s - Medio positivo.

El impacto social del proyecto incidirá, a corto, mediano y largo plazo, el cambio de hábitos en el uso de cajeros automáticos, la ubicación de diferentes puntos de retiro de dinero (ATM’s) en la provincia donde se encuentra ubicada la Cooperativa “XYZ” y velar por el bienestar de los clientes de la organización, reduciendo suplantación de identidad, atracos físicos, clonación de tarjetas, entre otros.

3.2.3. Impacto ambiental

En la TABLA 3.5, se realizará una matriz que contendrá en el lado izquierdo el indicador, el cual será valorado con el nivel de impacto, para obtener información que permita matemáticamente saber cuál es el nivel de impacto ambiental del proyecto. Los valores se han considerado tomando en cuenta la información recopilada en auditoria del cajero automático de la cooperativa “XYZ”.

TABLA 3.5
Matriz impacto ambiental

Nivel de impacto / Indicador	-3	-2	-1	0	1	2	3	Total
Comprobantes electrónicos vía correo electrónico.							X	3
Comprobantes por medio de papel reciclado.					X			1
Sin uso de comprobantes.					X			1
Total					**2**		**3**	**5**

Fuente: (Nathan & Scobell, 2012)

Total, de impacto social = 5/3

Total, de impacto social = 1.7

Nivel de impacto social = Bajo positivo

Análisis

El resultado final correspondiente al impacto ambiental del proyecto es:

- Comprobantes electrónicos vía correo electrónico - Alto positivo.
- Comprobantes por medio de papel reciclado - Bajo positivo.
- Sin uso de comprobantes - Bajo positivo.

El impacto ambiental del proyecto incidirá, a corto, mediano y largo plazo, es necesario reducir el uso de papel en impresiones de comprobantes de retiro en ATM´s, se debe implementar una suscripción gratuita a cada cliente, es decir, si realiza una transacción en un cajero automático su comprobante debe llegar a su correo electrónico de forma

CONCLUSIONES

- En base a los datos obtenidos, la empresa GREENETICS soluciones S.A., no presenta un estándar para realizar auditoria de cajeros automáticos en Ecuador, por tal motivo con el análisis de la normativa PCI DSS/PTS y lineamientos de la Superintendencia de Economía Popular y Solidaria (SEPS), se implementó una normativa internacional con parámetros de seguridad física para auditoria de estos dispositivos.

- Para determinar las vulnerabilidades presentes en cajeros automáticos es necesario establecer controles de seguridad implementando una normativa o estándares internacionales que permitan la integración de componentes de hardware en cajeros automáticos para la implementación, reparación y reacondicionamiento de los mismos.

- Es necesario realizar análisis periódicos sobre la seguridad del software utilizado para asignar privilegios entre usuario, así como del middleware encargado de la gestión de datos, servicios de aplicaciones, mensajería, autenticación y gestión de API (Interfaz de programación de aplicaciones) para garantizar la eficacia de las funciones de seguridad y aplicando las mejores prácticas para el desarrollo de aplicaciones.

- Con respecto al cumplimiento de la normativa llevada a cabo la auditoria emitida por ente de control (SEPS) se obtuvo que el cajero evaluado cumple con 13 controles de seguridad, lo cual representa el 87% de los controles, mientras que 2 de los controles no fueron evidenciados, lo cual representa el 13%. Con respecto a los 34 controles establecidos en la normativa PCI DSS/PTS se obtuvo como resultado que el cajero analizado tiene 25 controles evidenciados obteniendo un cumplimiento total del 74%, no se evidenció un total de 9 controles lo cual representa un 26%.

- Con respecto a las vulnerabilidades encontradas en el análisis de ATM se puede decir que existe un riesgo catalogado ALTO, permite descargar archivos de manera remota y sin control alguno, otra de riesgo MEDIO con respecto a una falta de activación del firewall, lo cual permite conexiones entrantes o salientes no autorizadas que puedan llegar a comprometer la confidencialidad, integridad y disponibilidad del equipo y su información.

RECOMENDACIONES

- Se recomienda a la empresa GREENETICS soluciones S.A, seguir empleando la normativa internacional PCI DSS/PTS, para la auditoria en cajeros automáticos permitiendo establecer un control de seguridad exhaustivo en cada uno de los dispositivos electrónicos ATM´s, esto permitirá que los usuarios se sientan seguros al momento de realizar cualquier tipo de transacción en sus cuentas bancarias.

- Es importante considerar una revisión integral periódica de los sistemas informáticos utilizados en la institución, en lo referente a la falta de instalación de actualizaciones y parches de seguridad que generan los fabricantes, de este modo se podrá reducir el riesgo ocasionado por las vulnerabilidades generadas por este tipo de problemas.

- Para mantener un ambiente seguro en equipos informáticos como son los cajeros automáticos, es necesario el uso de herramientas para la auditoría y seguridad informática. Las herramientas son esenciales al momento de verificar vulnerabilidades que afecten a sistemas en su funcionalidad y privacidad, después de la comprobación se procede a utilizar parches de seguridad en cada vulnerabilidad descubierta. Una de las herramientas con mayor acogida en el ámbito de seguridad, es el sistema operativo Kali Linux con varias aplicaciones relacionadas con la seguridad informática y la auditoria de redes.

- Se recomienda al departamento de TI, definir inmediatamente un “Plan de Acción”, para ejecutar las medidas correctivas sobre cada una de las vulnerabilidades encontradas en el informe entregado. Una vez ejecutado el plan de acción, es importante realizar un segundo escaneo y analizar vulnerabilidades para comprobar la corrección de estas.

- Llevar a cabo un análisis de seguridad del tipo Ethical Hacking sobre todos los dispositivos informáticos relacionados con cajeros automáticos de la institución, puesto que si un dispositivo no es analizado representa un alto riesgo de seguridad.

BIBLIOGRAFIA

Acosta, D. E. (2008). *Gestión de eventos y monitoreo en el estándar PCI DSS*.

Andrade, R. D. (2003). Legislación económica del Ecuador - Ruben Dario Andrade - Google Libros. Retrieved November 27, 2019, from https://books.google.com.ec/books?id=FhwTXzBdtVIC&pg=PA65&dq=sociedades+mercantiles+en+el+ecuador&hl=es-419&sa=X&ved=0ahUKEwjy3NrcjtLlAhUCjVkKHdJVCf4Q6AEIKDAA#v=onepage&q&f=false

Aron, M. (2019). Cómo funcionan los cajeros automáticos | Cuida tu dinero. Retrieved January 13, 2020, from https://www.cuidatudinero.com/13121861/como-funcionan-los-cajeros-automaticos

Ataya, G. (2011). PCI DSS audit and compliance. *Information Security Technical Report*, *15*(4), 138–144. https://doi.org/10.1016/j.istr.2011.02.004

ATMIA. (2014). *ATM Software Security Best Practices Guide Version 3*. Retrieved from https://www.atmia.com/files/Best Practices/ATMIA Best Practices v3.pdf

Banco Pacifico. (2019). Nuestra institución | Banco del Pacífico. Retrieved November 26, 2019, from https://www.bancodelpacifico.com/grupo-bdp/grupo-banco-del-pacifico/menu/nuestra-institucion

Bancos Privados del Ecuador. (2015). *Informa*. 2466701–2466702.

BANRED. (2019). BANRED > La Empresa > Historia. Retrieved November 26, 2019, from https://www.banred.fin.ec/La-Empresa/Historia

BBC Mundo. (2017). La curiosa historia de cómo nació el cajero automático hace 50 años. Retrieved November 22, 2019, from http://www.bbc.com/mundo/noticias-40417156

Bertha Romero. (2015). El Rol de la Superintendencia de Bancos del Ecuador - Finanzas Personales Ecuador. Retrieved November 27, 2019, from https://tusfinanzas.ec/blog/2015/09/29/el-rol-de-la-superintendencia-de-bancos-del-ecuador/

BSLatAm. (2018). *Mercado de terminales ATM en América Latina 2018-2022 Brasil , Uruguay y Costa Rica : Podio regional en cobertura de red de ATMs*.

Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information and Decision Science*, *19*(1), 54–67.

Coburn, A. (2010). Fitting PCI DSS within a wider governance framework. *Computer Fraud and Security*, *2010*(9), 11–13. https://doi.org/10.1016/S1361-3723(10)70121-4

Cooke, R. (2017). ProQuest Ebook Central. https://doi.org/10.5260/chara.19.2.39

Daza, J. (2014). Las tarjetas de crédito y la cultura financiera crediticia en Sucre. *Handbooks - ©ECORFAN-Bolivia*, 24. Retrieved from http://www.ecorfan.org/bolivia/handbooks/ciencias economicas I/articulo 10.pdf

Díaz Céspedes, R. (2018). *Auditoría Forense Analysis of Security Elements Used By a Bank To Prevent Phishing Scams in Transactions of Equal Nature in Relationship With Forensic Auditing*. 7–37.

Esther, M., & López, R. (2012). *Universidad Politécnica Salesiana Sede Guayaquil*. 198. Retrieved from http://dspace.ups.edu.ec/bitstream/123456789/3633/1/UPS-GT000348.pdf

Garc, P. (2013). Mejora Continua de Procesos. *Ainia*, 2–18.

García Correa, G., García Camavilca, M., & Monzón Castillo, E. (2017). Las auditorías de desempeño y su rol en el fortalecimiento de la gestión pública : evaluación de cuatro casos de estudio. *Repositorio de La Universidad Del Pacífico - UP*.

Greenetics Soluciones S.A. (2018). SEGURIDAD INFORMÁTICA | ETHICAL HACKING | SGSI | CAPACITACIÓN. Retrieved November 9, 2019, from https://www.greenetics.com.ec/

Joel Meléndez Verdezoto. (2008). Derecho Ecuador - DELITOS INFORMÁTICOS O CIBERDELITOS. Retrieved November 9, 2019, from Delitos Informáticos O Ciberdelitos website: https://www.derechoecuador.com/delitos-informaticos-o-ciberdelitos

Junta de regulación monetaria y financiera, J. (2015). *Resol132.pdf*.

Klever, C. (2018). *Vicerrectorado de investigación, innovación y transferencia de tecnología*. 1. Retrieved from https://repositorio.espe.edu.ec/bitstream/21000/13743/5/T-ESPE-057806.pdf%0Ahttp://repositorio.espe.edu.ec/bitstream/21000/10846/1/T-ESPE-049674.pdf

Martínez, F., & Merchán, X. (2010). *La Universidad Católica de Loja ESCUELA DE BANCA Y FINANZAS " ANÁLISIS DE LOS PATRONES DE CONSUMO DE LA TARJETA DE CRÉDITO Fernanda Anabel Martínez Torres*.

Nacional, P., Morazán, F., & Galo, L. M. (2014). *Tema : Informe de Investigación Uso de Tarjetas de Crédito*. 1–62.

Nathan, A. J., & Scobell, A. (2012). How China sees America. *Foreign Affairs*, *91*(5), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Patlán Pérez, J., & Martínez Torres, E. (2017). Evaluación de la imagen organizacional universitaria en una institución de educación superior. *Contaduría y Administración*, *62*(1), 105–122. https://doi.org/10.1016/j.cya.2016.07.002

PCI Security Standards Council LLC. (2013). Standard : PCI PIN Transaction Security Point of Version : Date : Author : Information Supplement : ATM Security Guidelines. *Pci Dss*

Information Supplement, (January).

Piazza, M., Fernandes, J., Anderson, J., & Olmsted, A. (2016). *Cloud Payment Processing without Ritualistic Sacrifices*. 166–168.

Ruiz, X. (2015). Planificación estratégica e indicadores de desempeño en el sector público. Manual 69. *Universidada Nacional de Colombia . Sede Bogota*, 2012.

SB. (2014). *Sistema Financiero Sistema Financiero Privado Capitulo I . - Apertura Y Cierre De Oficinas En El País Y En El Públicas Sometidas Al Control De La Superintendencia De*. 144–164. Retrieved from http://www.superbancos.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_II_cap_I.pdf

SBIF. (2018). *Superintendencia de Bancos e Instituciones Financieras*. Retrieved from https://www.sbif.cl/sbifweb/servlet/Portada?indice=0.0

SEPS. (2019). ¿Qué es la SEPS? - SEPS. Retrieved December 17, 2019, from Superintendencia de economía popular y solidaria website: https://www.seps.gob.ec/interna?-que-es-la-seps-

Significados. (2013). Significado de Paradigma:Qué es, Concepto y Definición. Retrieved January 14, 2020, from Convenio website: https://www.significados.com/vulnerabilidad/

Telégrafo, E. (2012). Fraude informático se multiplica en tres años. Retrieved November 9, 2019, from https://www.eltelegrafo.com.ec/noticias/judicial/12/fraude-informatico-se-multiplica-en-tres-anos

Vinicio, M., & Sanchez, S. (2018). *Maestría En Auditoria De Tecnología*.

Zunzunegui, F. (2006). *Rdmf*. 2. Retrieved from https://rdmf.files.wordpress.com/2006/12/que-son-las-tarjetas-de-credito.pdf