REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACION CON MENCIÓN EN SEGURIDAD INFORMATICA

EVALUACIÓN DE LA APLICABILIDAD DE LA NORMATIVA DE SEGURIDAD FÍSICA Y ELECTRÓNICA EN LOS PROCESOS DE IMPLEMENTACIÓN DE CAJEROS AUTOMÁTICOS EN LA CIUDAD DE ESMERALDAS, ECUADOR.

Proyecto del Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática

AUTOR: ING. LENIN VICENTE QUISPE MERA

DIRECTOR: MSC. VICENTE ALEXANDER GUEVARA VEGA

ASESOR: MSC. JOSÉ FERNANDO GARRIDO SÁNCHEZ

IBARRA - ECUADOR

2023

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

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	0802951681		
APELLIDOS Y NOMBRES	Quispe Mera Lenin Vicente		
DIRECCIÓN	Esmeraldas, barrio San Jorge calle 8va 007 y B		
EMAIL	lvquispem@utn.edu.ec		
TELÉFONO FIJO	062015016	**TELÉFONO MÓVIL:**	0993312221
DATOS DE LA OBRA			
TÍTULO:	EVALUACIÓN DE LA APLICABILIDAD DE LA NORMATIVA DE SEGURIDAD FÍSICA Y ELECTRÓNICA EN LOS PROCESOS DE IMPLEMENTACIÓN DE CAJEROS AUTOMÁTICOS EN LA CIUDAD DE ESMERALDAS, ECUADOR.		
AUTOR (ES):	QUISPE MERA LENIN VICENTE		
FECHA: DD/MM/AAAA	30/11/2023		
SOLO PARA TRABAJOS DE GRADO			
PROGRAMA DE POSGRADO	Computación con Mención en Seguridad Informática		
TITULO POR EL QUE OPTA	Magíster en Computación con Mención en Seguridad Informática		
TUTOR	MSc. Guevara Vega Vicente Alexander		

CONSTANCIA

El autor Lenin Vicente Quispe Mera, 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 esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 30 días del mes de noviembre del 2023

EL AUTOR

LENIN VICENTE QUISPE MERA

Digitally signed by LENIN VICENTE QUISPE MERA
Date: 2023.11.30 17:07:00 -05'00'

Lenin Vicente Quispe Mera
C.I: 0802951681

APROBACIÓN DEL TUTOR

Yo MSc. Guevara Vega Vicente Alexander, en calidad de director de la tesis titulada: "EVALUACIÓN DE LA APLICABILIDAD DE LA NORMATIVA DE SEGURIDAD FÍSICA Y ELECTRÓNICA EN LOS PROCESOS DE IMPLEMENTACIÓN DE CAJEROS AUTOMÁTICOS EN LA CIUDAD DE ESMERALDAS, ECUADOR." de autoría de la Ing. Lenin Vicente Quispe Mera, para optar por el grado de Magister en Computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 30 días del mes de noviembre de 2023

Lo certifico

VICENTE ALEXANDER GUEVARA VEGA

Firmado digitalmente por VICENTE ALEXANDER GUEVARA VEGA
Fecha: 2023.11.30 16:21:30 -05'00'

MSc. Guevara Vega Vicente Alexander
DIRECTOR DE TESIS

AGRADECIMIENTO

Agradezco a la Universidad Técnica del Norte de Ibarra, así como a todos mis profesores y en especial a mi tutor, por haberme guiado con sus valiosos conocimientos, paciencia y dedicación para el desarrollo del presente trabajo de titulación.

Lenin Vicente Quispe Mera

DEDICATORIA

Dedico el presente trabajo de investigación a mi familia por su apoyo incondicional en cada decisión y proyecto realizado, porque ustedes son el motor que me permite seguir adelante cada día, todo mi esfuerzo lo hago pensando siempre en ustedes, lo cual ha hecho de mi un hombre humilde, responsable y decidido a cumplir exitosamente cada una de mis metas propuestas a lo largo de mi existencia.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

EVALUACIÓN DE LA APLICABILIDAD DE LA NORMATIVA DE SEGURIDAD FÍSICA Y ELECTRÓNICA EN LOS PROCESOS DE IMPLEMENTACIÓN DE CAJEROS AUTOMÁTICOS EN LA CIUDAD DE ESMERALDAS, ECUADOR.

Autor: Lenin Vicente Quispe Mera

Tutor: Vicente Alexander Guevara Vega

Año: 2023

RESUMEN

La seguridad de los cajeros automáticos es fundamental para las entidades financieras, con el paso del tiempo las organizaciones criminales descubren nuevos métodos de ataques, creando brechas de seguridad para cometer delitos. En el Ecuador hasta mayo de 2023, se registró una base de 4837 cajeros automáticos en funcionamiento, así lo indicó la Asociación bancaria del Ecuador (ASOBANCA) y en lo que va del año 2023 se han reportado 53 robos y más de 280 ataques físicos, afectando la integridad de las máquinas y la seguridad ciudadana. La presente investigación versa sobre el objetivo de evaluar la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos en la ciudad de Esmeraldas, a través de este estudio se ofrece generar recomendaciones útiles y prácticas para evaluar la base de cajeros automáticos ya instaladas en cada entidad financiera y en futuras instalaciones enmarcados en la seguridad, los métodos aplicados en el estudio fueron de investigación de campo, descriptiva, explicativa y exploratoria, con visión cualitativa y cuantitativa, utilizando técnicas de entrevista, encuestas y ficha de observación, con una acotación de revisión documental y fuentes bibliográficas para el fundamento teórico; con carácter no experimental, no se manipulo ninguna variable a favor del investigador. Como resultado obtenido de la investigación, se observa que el 49,22% de los cajeros automáticos de la ciudad de Esmeraldas son medianamente seguros, entorno al riesgo ciudadano y las medidas de seguridad aplicadas actualmente en la normativa, también es importante mencionar el resultado obtenido de la comparativa de la seguridad en los cajeros automáticos en países de Latinoamérica, donde se sitúa en tercer lugar con relación a 6 países evaluados. Como punto de interés se expusieron algunas alternativas viables para afrontar la problemática en las que se destacan el establecimiento de alianzas estratégicas institucionales y cooperación internacional.

Palabras clave: cajeros automáticos, normativas, seguridad, riesgo

EVALUATION OF THE APPLICABILITY OF PHYSICAL AND ELECTRONIC SECURITY REGULATIONS IN THE IMPLEMENTATION PROCESSES OF ATMS IN THE CITY OF ESMERALDAS, ECUADOR.

Author: Lenin Vicente Quispe Mera

Tutor: Vicente Alexander Guevara Vega

Year: 2023

ABSTRACT

The security of ATMs is essential for financial institutions; over time, criminal organizations discover new methods of attacks, creating security gaps to commit crimes. In Ecuador until May 2023, a base of 4,837 ATMs was registered in operation, as indicated by the Banking Association of Ecuador (ASOBANCA) and so far in 2023, 53 thefts and more than 280 physical attacks have been reported. affecting the integrity of the machines and public safety. The present research deals with the objective of evaluating the applicability of physical and electronic security regulations in the implementation processes of ATMs in the city of Esmeraldas, through this study it is offered to generate useful and practical recommendations to evaluate the basis of ATMs already installed in each financial institution and in future installations framed in security, the methods applied in the study were field research, descriptive, explanatory and exploratory, with a qualitative and quantitative vision, using interview techniques, surveys and data sheets. observation, with a note of documentary review and bibliographic sources for the theoretical foundation; On a non-experimental basis, no variable was manipulated in favor of the researcher. As a result obtained from the investigation, it is observed that 49.22% of the ATMs in the city of Esmeraldas are moderately safe, regarding citizen risk and the security measures currently applied in the regulations, it is also important to mention the result obtained of the comparison of security in ATMs in Latin American countries, where it is placed in third place in relation to 6 countries evaluated. As a point of interest, some viable alternatives were presented to address the problem, highlighting the establishment of institutional strategic alliances and international cooperation.

Keywords: ATMs, regulations, security, risk

1. CAPITULO I EL PROBLEMA

1.1. Problema de la investigación

En esta era digital moderna la seguridad y la privacidad son factores importantes para cada individuo en cualquier parte del mundo, debido al rápido avance de la tecnología y sus desafíos contra la seguridad y la privacidad, los próximos desarrollos se fomentan en soluciones de seguridad sólidas, de la misma manera, también aparecen métodos para violar estos niveles de seguridad. (Sabani & Rishan, 2019)

A pesar del hecho de que la mejora en la automatización tiene un resultado constructivo en términos generales, sin embargo, diferentes empresas relacionadas con el dinero como los bancos y cooperativas que implementan cajeros automáticos todavía están expuestas a robos y fraudes (Balaji & Poornima, 2021).

En los delitos o fraudes a cajeros automáticos hay un factor a considerar que es tan importante como lo delincuentes externos, se trata de personal interno, capacitado en la manipulación, mantenimiento, control y administración de los cajeros automáticos, teniendo accesos de manera más abierta. Dando claridad a que parte de la problemática también se encuentra en funcionarios que puedan cometer actos ilícitos. (Baez Sánchez, 2019)

En la actualidad países vecinos como Colombia sufren el crecimiento constante y acelerado de la delincuencia organizada a través de la sustracción de información personal obtenida de distintas maneras tanto físicas como digitales, los diferentes métodos y tácticas utilizadas para sustraer y hurtar diversos tipos de información han sido dinámicas e incrementales, siendo uno de los mayores objetivos los productos financieros, a través de la suplantación de identidad el consumidor financiero o ataques directos a los canales de entidades

bancarias (especialmente plataformas digitales y cajeros automáticos). Dentro de las modalidades de hurto más utilizadas a la fecha y que tienen impacto directo con los productos financieros, se encuentran: El Skimming, Malware, Phishing, Smishing, Vishing, Estafa Cibernética y Cambiazo, perjudicando a las entidades financieras y a los clientes. (And21)

En Ecuador, con el objetivo de combatir la delincuencia relacionada con el robo de cajeros automáticos, el Banco Central del Ecuador ha emitido la Resolución Administrativa Nro. BCE-GG-017-2021. Esta resolución establece el proceso que se debe seguir para la instalación y uso de un sistema avanzado que previene el robo de efectivo en los cajeros automáticos. Este sistema es conocido como dispositivo de entintado o sistema inteligente neutralizador de billetes (Banco Central del Ecuador, 2022).

Las bandas delincuenciales cada vez más desarrollan mecanismos innovadores para realizar robos y fraudes, de la misma manera la destrucción de los cajeros automáticos usando material explosivo para sustraer el dinero es algo inevitable, cuando los delincuentes aplican estos métodos para llevar a cabo dicha acción (Coba, 2022). El aumento de los niveles de inseguridad en Ecuador le pasa factura a los bancos y a las cooperativas. Asaltos a agencias y vehículos blindados que trasladan dinero, daños a cajeros automáticos y ciberataques están entre los riesgos que enfrentan las entidades financieras (Finkle, 2016).

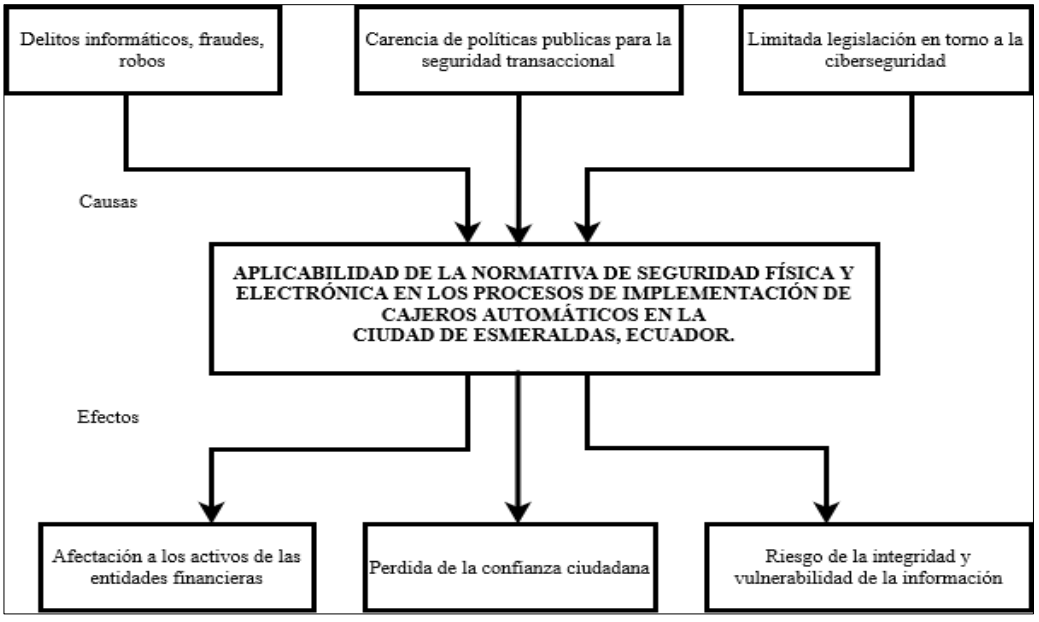
En Guatemala existen diversas entidades bancarias que ofrecen el servicio a través de cajeros automáticos propios y otras que lo realizan a través de una entidad intermediaria. Muchos de estos equipos han sufrido alguna alteración de parte de criminales para poder obtener los datos impresos en el plástico y número de PIN asociado y con estos poder realizar la clonación o robo de identidad del tarjetahabiente (Martinez Ralón, 2021).

En la ciudad de Esmeraldas progresivamente se han realizado instalaciones de cajeros automáticos por parte de las entidades financieras en distintos lugares, pero se han realizado pocos estudios sobre la aplicabilidad de la normativa de seguridad en los procesos de instalación y en cajeros automáticos que se encuentran en producción, tomando en consideración la seguridad pública local actual.

1.2. Árbol del problema

Un primer diagnóstico de la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos (ATMs) en la ciudad de Esmeraldas, permitió observar una serie de consecuencias que podrían afectar el entorno de los servicios que ofrecen los cajeros automáticos. Como lo muestra la siguiente figura:

Figura 1. Árbol del problema



Elaborado por: El autor

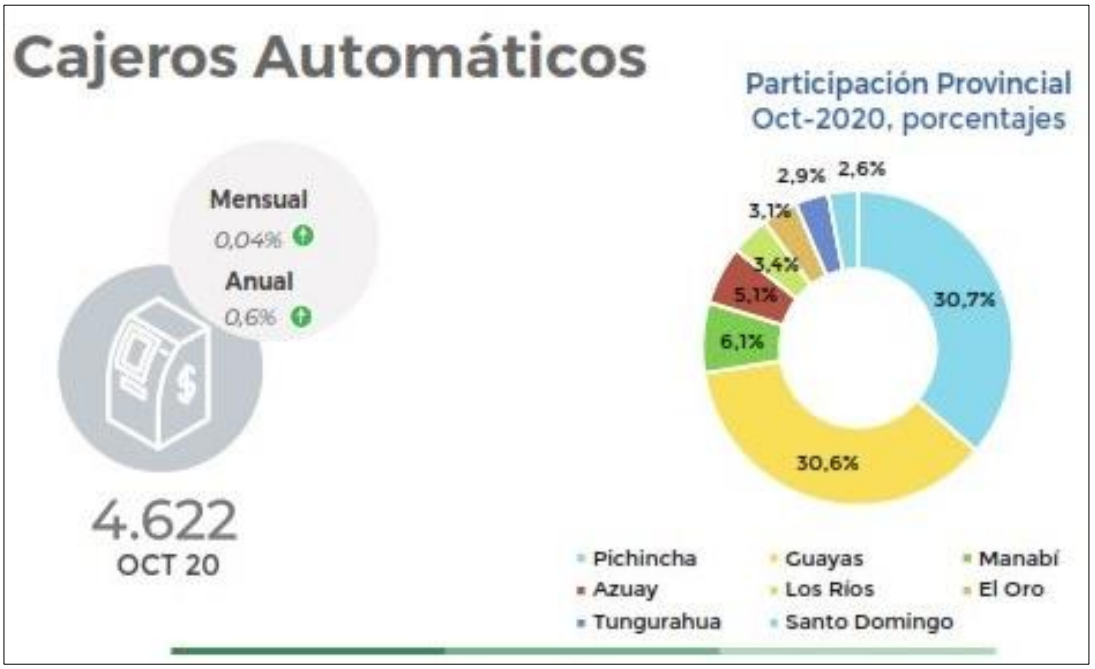
1.3. Antecedentes

De acuerdo al boletín de servicios financieros de la ASOBANCA del Ecuador en octubre 2020, los ATMs se registraron 4.622 unidades funcionales, respectivamente a nivel nacional con una variación mensual del 0,04 % y anual de 0,6% con un crecimiento notable, mientras en octubre 2017 existían 3962 unidades a octubre 2020 con 4622, esta información nos permite conocer de manera evolutiva el comportamiento de los ATMs en el entorno de la automatización de los servicios financieros, para poder llegar a más sitios y satisfacer las necesidades de los, clientes también es importante mencionar que los ATMs fuera de oficina o sitios remotos, comprenden el 51,2% y en las oficinas bancarias un 48.8%. (Asobanca, 2021)

Figura 2. Evolución número de ATMs funcionales de en el Ecuador

Fuente: Boletín de servicios Financiero (ASOBANCA, 2021) https://asobanca.org.ec/

Figura 3. Flota de ATMs funcionales en el Ecuador hasta el 2020



Fuente: Boletín de servicios Financiero (ASOBANCA, 2021) https://asobanca.org.ec/

En la investigación realizada por Tamas (2021) titulada "Descripción general de la seguridad de los ATMs" indica que, el principal mecanismo de protección física de un ATMs es la caja fuerte, que contiene el dispensador de efectivo que contiene billetes de banco. El método más primitivo para superar esta línea de defensa es el uso de sopladoras, fresadoras o explosivos, también hay casos en que los atacantes utilizaron equipos de construcción pesados para derribar muros y obstáculos de protección, así como para quitar y quitar todo el ATM con el fin de abrirlo en un lugar apartado. (Tamas, 2021)

En la investigación realizada por Milind (2016) titulada "A Review Paper on Improving Security of ATM System" indica que, la seguridad es un problema grave en el sistema ATM, las estafas involucran a ladrones que insertan una funda de plástico delgada, transparente y rígida en la ranura de la tarjeta de ATM, debido a esto, la máquina no puede leer la tira cuando el usuario

inserta la tarjeta, por lo tanto, seguirá pidiéndole que vuelva a ingresar su contraseña, en ese momento, el hacker notará el toque de su dedo en el número, los ladrones luego quitan la funda de plástico y usan la cuenta. (Milind, 2016)

De acuerdo con Singh (2019) indica que, con el aumento de la tecnología, la necesidad de seguridad de la información de las personas también se está convirtiendo en una preocupación importante. Los ATMs son un dispositivo común muy utilizado para realizar transacciones bancarias, es mundialmente famoso entre el público debido a sus características como accesibilidad y facilidad de uso, el acceso a la información privada en los ATMs es posible mediante el uso de contraseñas, ya que son fáciles de usar, pero aun así está indefenso contra los diversos tipos de ataque como: phishing, ataque de suplantación de identidad, rastreo, entre otros (Singh, 2019).

De acuerdo con Finkle (2016) indica que, aunque los ciberdelincuentes han estado atacando los ATMs durante al menos cinco años, involucraron principalmente a una pequeña cantidad de ATMs porque los piratas informáticos necesitaban tener acceso físico a los ATMs, los atracos recientes en Europa y Asia se llevaron a cabo en modo remoto, lo que permitió la extracción de efectivo antes de que los bancos descubran los ataques (Finkle, 2016).

1.4. Interrogantes de la investigación

1.4.1. Interrogante General

- ¿Cómo evaluar de la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos en la ciudad de Esmeraldas, Ecuador?

1.4.2. Interrogantes Específicos

- ¿Cómo caracterizar la seguridad física y electrónica de los cajeros automáticos en los procesos de instalaciones y producción?
- ¿Cómo diagnosticar las vulnerabilidades en los entornos de servicios de los cajeros automáticos de las entidades financieras?
- ¿Cómo realizar un análisis comparativo de la norma nacional e internacional de seguridad física y electrónica en los procesos de implementación de los cajeros automáticos?
- ¿Cuáles serían las medidas de seguridad basado en el análisis de la normativa ecuatoriana, para mitigar ataques y fraudes a los cajeros automáticos?

1.5. Objetivos de la investigación

1.5.1. Objetivo general

Evaluar de la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos en la ciudad de Esmeraldas, Ecuador.

1.5.2. Objetivos específicos

- Caracterizar la seguridad física y electrónica de los cajeros automáticos en los procesos de instalaciones y producción.
- Diagnosticar las vulnerabilidades en los entornos de servicios de los cajeros automáticos de las entidades financieras.
- Realizar un análisis comparativo de la norma nacional e internacional de seguridad física y electrónica en los procesos de implementación de los cajeros automáticos.

- Medir el nivel de seguridad física y electrónica de los cajeros automáticos, de acuerdo con la normativa ecuatoriana.

1.6. Justificación

La presente investigación es necesaria, por cuanto es notable el crecimiento exponencial de la base de cajeros automáticos en la institución financiera del Ecuador, esto conlleva a una competencia en servicios de automatización y canales digitales para llegar a sitios donde no hay entidades financieras o sitios remotos, con el objetivo de brindar los diferentes servicios que ofrecen a sus clientes, garantizando la seguridad de la información y sus propios activos. De manera paralela el crimen organizado, bandas centradas en fraudes informáticos, ingeniería social y robos, crecen progresivamente creando más brechas de seguridades y haciendo visibles las vulnerabilidades en los ambientes físicos y electrónicos de los cajeros automáticos (Fiscalia General del Estado, 2022).

Por lo ante expuesto, es procedente realizar una investigación para matizar las posibles brechas de seguridad que se pueden presentar en distintos escenarios de los ATMs en la ciudad de Esmeraldas y diagnosticar las medidas de seguridad en los sitios ya establecidos bajo el marco de las normativas y políticas vigentes.

Poder comparar la normativa nacional con referentes internacionales y evaluar la implementación de procesos de seguridad física y electrónica de los ATMs, permitirá determinar si la legislación vigente está acorde a la realidad actual con relación a la seguridad pública y los nuevos avances tecnológicos que también son usados para cometer actos ilícitos.

De acuerdo con lo establecido en el plan de creación de oportunidades 2021 – 2025, en su objetivo 10, que menciona “Garantizar la soberanía nacional, integridad territorial y seguridad

del Estado, indicado por la política 10.1 Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente amenazas provenientes del ciberespacio y proteger su infraestructura critica. Con el propósito de incrementar el índice de ciberseguridad global de 26,3 a 51,3 (Secretaria Nacional de Planificacion, 2021).

Figura 4. Plan Nacional de Desarrollo 2021 – 2025

Fuente: Boletín jurídico, https://boletin.novedadesjuridicas.com.ec/pndd/ (2021)

La línea de investigación de la UTN a la que contribuye la presente investigación es la numero 10 “Desarrollo, aplicación de software y cyber security (seguridad cibernética)”

2. CAPITULO II MARCO REFERENCIAL

2.1. Marco teórico

2.1.1. Proceso de revisión de la literatura

Toda investigación debe establecer restricciones claras, como el nivel de análisis a utilizar, el período de tiempo previsto, la delimitación del contexto que será objeto de estudio y la definición precisa del alcance de la revisión. En este punto, es esencial determinar la entidad o unidad de análisis que se utilizará para examinar la literatura.

2.1.2. Identificando la literatura relevante

Una revisión de alta calidad debe abordar de manera exhaustiva toda la literatura relevante en relación con un tema particular.

Se recomienda los siguientes pasos para la búsqueda de documentos:

1) Explorar y examinar conferencias y artículos publicados en revistas prestigiosas es fundamental, ya que es en estos lugares donde se puede hallar la mayor cantidad de información valiosa para llevar a cabo una investigación.
2) Tras examinar los artículos, es importante investigar las citas incluidas en cada uno de los documentos, ya que en este contexto también es posible descubrir información adicional que pueda resultar útil en la revisión.
3) En algunas ocasiones, las bases de datos bibliográficas pueden presentar artículos recientes que hacen referencia a los mismos documentos que ya has buscado.

Podría afirmarse que el proceso de análisis está casi concluido cuando la compilación de documentos no revela nuevos conceptos.

2.1.3. Unidad de análisis

Saber si en los cajeros automáticos de la ciudad de Esmeraldas, Ecuador. Se aplica la normativa y políticas vigente en los procesos de implementación, con énfasis en la seguridad física y electrónica, información que se obtendrá a través de la aplicación de instrumentos como son: fichas de observación en campo, entrevistas y encuestas.

2.1.4. Cadena de búsqueda

Según las interrogantes de investigación, se generó la siguiente secuencia de búsqueda de datos de los últimos cinco años en los 3 buscadores académicos asignados SCOPUS, REDALYC Y GOOGLE SCHOLAR, la cual fue utilizada para adquirir la información y datos necesarios en el proceso de realización del proyecto de investigación de tesis, tal como se detalla en la tabla # de cadena de búsqueda de datos científicos.

Tabla 1. Secuencia de búsqueda utilizada en la base de datos científica

Criterio	Scopus	Redalyc	Google Scholar
Cadena de búsqueda	Riesgo, seguridad ciudadana, control de accesos	Atm, cybersecurity, physical security, electronic security, normativa	seguridad en bancos, ataques físicos, robos digitales, hackeo en Atm
SUBTOTAL	202	162	409
TOTAL		773	

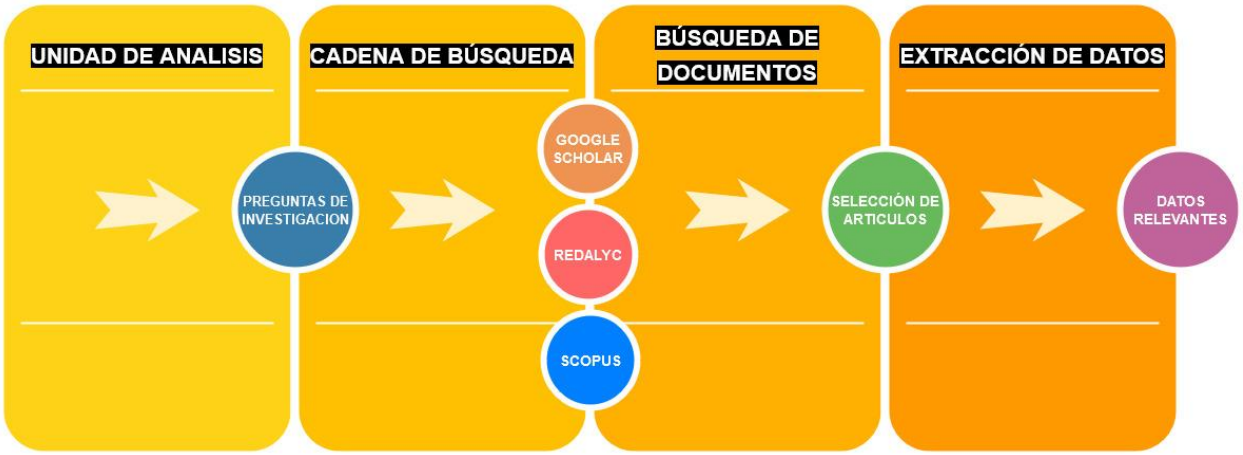
Fuente: (Redalyc), (Google Scholar), (Scopus)

2.1.5. Búsqueda de documentos

Es factible encontrar de manera eficaz la literatura que sea importante, adecuada y de confianza, incluso en medio de la abundante información disponible en línea y en formatos impresos que, aunque puedan parecer desactualizados, aún tienen relevancia y utilidad. Esto incluye títulos de libros que continúan siendo publicados exclusivamente en papel, así como

revistas, tesis, ensayos, series, entre otros recursos Huerta Ibarra (2019). La búsqueda de documentos como se indica en la figura 5, se realizó a través de los buscadores bibliográficos Scopus, Redalyc y Google Scholar, también se utilizó otras fuentes como tesis universitarias y artículos de revistas. Se encontró un total de 1063 documentos al filtrarse por los últimos 5 años se obtuvo los siguientes resultados: 774 de los cuales 202 pertenecen a Scopus, 162 a Redalyc y 409 a Google Scholar.

Figura 5. Procesos de investigación



Fuente: El autor

2.1.6. Selección de artículos

Para la selección de los artículos se tomaron en cuenta tres fases: para la primera fase se aplicaron criterios de inclusión y exclusión, trabajos de tesis, fechas de publicación de los artículos de investigación de los últimos 5 años, investigaciones relacionadas con: cajeros automáticos, procesos de implementación, normativas de seguridad física y electrónica, entidades financieras, medios de pagos digitales y toda documentación relacionada con el tema de investigación.

En la segunda etapa, se seleccionaron los artículos más relevantes e importantes para la revisión utilizando la cadena de búsqueda, y se organizaron según su título, año de publicación, resumen y palabras clave.

En la etapa final, se examinó y evaluó la información presente en cada documento de investigación, centrándose en el resumen, la introducción y las recomendaciones. Se prestaron especial atención a los documentos que estaban relacionados con el tema de investigación. Los documentos seleccionados después de completar las tres fases se enumeran en la tabla 2.

Tabla 2. Selección de artículos

Base de datos	**Fase I**	**Fase II**	**Fase III**
Redalyc	162	15	5
Scopus	202	25	5
Google Scholar	409	22	5
Total	773	62	15

Fuente: (Redalyc), (Scopus) y (Google Scholar)

Tabla 3. Artículos seleccionados

Código	**Titulo**	**Autor**	**Información relevante**
A1	A review paper on improving security of ATM system	Milind, N. (2016)	Seguridad en ATM, autenticación por huella dactilares, seguridad por niveles
A2	A novel approach to secure NFC electronic payment between ATM and smartphone	Samir Chabbi. (2022)	Tecnología NFC, Ataques a datos personales, pagos electrónicos entre ATM y teléfonos inteligentes
A3	A Systematical Review Study to Investigate the Use of Biometric Security Techniques in Automatic Teller Machines: Insight from the Past 15 Years	Ahmed M. (2020)	Transacciones financieras en ATM, incremento de ataques fraudulentos, puntos de seguridad

A4	Amenazas a la seguridad de los cajeros automáticos	Mosunov A.A. (2021)	Seguridad periférica, métodos de influencia física, intrusiones, autenticación y cifrado
A5	ATM Heist Threats: A Proposed ICT Governance Strategy	Dayu Kao. (2019)	Mercado negro cibernético, malwares, gobernanza, ciberdelincuencia organizacional
A6	Attack and optimizing security management on atm machines using des (Data Encryption Standard)	Eriyani I. (2020)	Sistemas criptográficos, algoritmos de simetría, autoprotección, resiliencia del sistema ATM
A7	ATM Security: A case study of Emerging Threats	Kasanda EN. Phiri J. (2018)	Automatización de servicios usuarios, ataques lógicos, PCI DSS
A8	Card-Less ATM Transaction using Biometric and Face Recognition– A Review	Manish CM. (2020)	Biometría fisiológica, reconocimiento facial, patrones faciales
A9	Card-Less ATM Transaction using Biometric and Face Recognition– A Review	Poornima B. (2021)	Algoritmo mejorado, tiempo de respuesta, Biométricos módulos de alarmas
A10	Una descripción general de la seguridad de los ATM	Tamas B. (2021)	Jackpotting, Blackbox attack, XFS, Cash dispenser
A11	ATM Hacking and Implications	Shun-Yung K. Ming-Li H. (2019)	Cibercrimen, ciberseguridad, DDoS, Phising
A12	Implementación de criptografía profunda en sistemas de seguridad ATM	Efendi F. (2019)	Método Pin, DES, Triple DES, IDEA
A13	Robo de identidad y clonación de tarjetas de crédito y débito utilizando cajeros automáticos alterados	Martínez M. (2021)	Metal tray, ATM, clone, computer, cards, PIN, data breach, technology, mobile phone
A14	Microcontroller based ATM monitoring system for security purpose	Aman J. (2021)	Microcontroladores, ATM sistema de monitoreo, seguridad, sensores
A15	la ciberseguridad en el Ecuador, una propuesta de organización	Tales C. (2019)	Estrategias y Políticas Nacionales de Ciberdefensa, Ciberseguridad, Ciberespacio, Infraestructura Crítica.

Fuente: (Redalyc),(Scopus) y (Google Scholar)

2.1.7. Extracción de datos relevantes.

Después de identificar este proceso de extracción recolectada en 15 artículos, se realizó una matriz de temas importantes en los cuales están encajados a describir la relación de aplicabilidad de la normativa de seguridad física y electrónica vigente en los proceso de implementación de cajeros automáticos de la ciudad de Esmeraldas, su caracterización, diagnostico, comparación y medición del nivel de seguridad, mismos que tienen relación con el proyecto de investigación como son: evaluación de la normativa, procesos de implementación, riesgos ciudadanos, métodos de fraudes, salvaguardas, mitigación, entre otros, los mismos que permitirán identificar o tener base teórica muy especializada sobre el campo de estudio.

Tabla 4. Matriz de conceptos

concepto / articulo	seguridad de atm por niveles (pin, biometría, otp)	autenticación, pagos electrónicos, elementos de seguridad en atm	puntos débiles de seguridad en atm, ataques fraudulentos,	protección de la información, métodos de ataques a atm	marco de gestión y gobernanza en atm, tecnología financiera	normativas, políticas, procedimientos en atm	procesos de implementación de atm,	criptografía, cifrado de la información en atm	procesos transaccionales en atm, zonas de riesgo ciudadano	salvaguardas, mitigación de puntos vulnerables en los atms
A1	X	X								X
A2		X							X	
A3			X	X						X
A4				X		X				
A5					X		X			
A6	X					X				
A7		X	X							
A8	X							X		X
A9							X	X		
A10				X				X		
A11			X		X				X	
A12										
A13		X						X		
A14	X						X			
A15			X			X			X	X

Elaborado por: El autor

2.2. Marco conceptual

2.2.1. ¿Qué es normativa?

Generalmente se refiere a un conjunto de reglas, regulaciones o normas establecidas por una autoridad, organización o gobierno para regir el comportamiento, estándares o procedimientos dentro de un contexto o industria específica, es esencialmente un conjunto de regulaciones y pautas que describen el comportamiento o estándares esperados o requeridos en un dominio particular.

Para Calva Vega (2022) basándose en su estudio sobre las normativas, concuerdo en que son importantes este conjunto de reglas, regulaciones, directrices, estándares o normas establecidas por una autoridad, organización o entidad gubernamental para guiar y regular el comportamiento, prácticas y procedimientos en un contexto especifico.

2.2.2. Que debe tener una normativa

Una normativa, ya sea legal, industrial, ética o de cualquier otro tipo, debe tener ciertos elementos para ser efectiva y cumplir con su propósito. Los componentes clave que debe tener una normativa incluyen: Objetivo claro, alcance definido, requisitos específicos, procedimientos de cumplimiento y aplicación, fecha de vigencia y revisión, lenguaje claro y comprensible, justificación y fundamento (Calva Vega, 2022).

Estos elementos son fundamentales para crear una normativa efectiva que pueda cumplir con sus objetivos y facilitar el cumplimiento por parte de las personas y organizaciones afectadas. La estructura y el contenido específico de la normativa pueden variar según su ámbito de aplicación y su propósito. Los requisitos para las normativas se expresan de mejor manera en la siguiente figura:

Figura 6. Requisitos de una normativa

Elaborado por: Estudio de normativa infraccional (Calva Vega, 2022)

2.2.3. ¿Qué es seguridad?

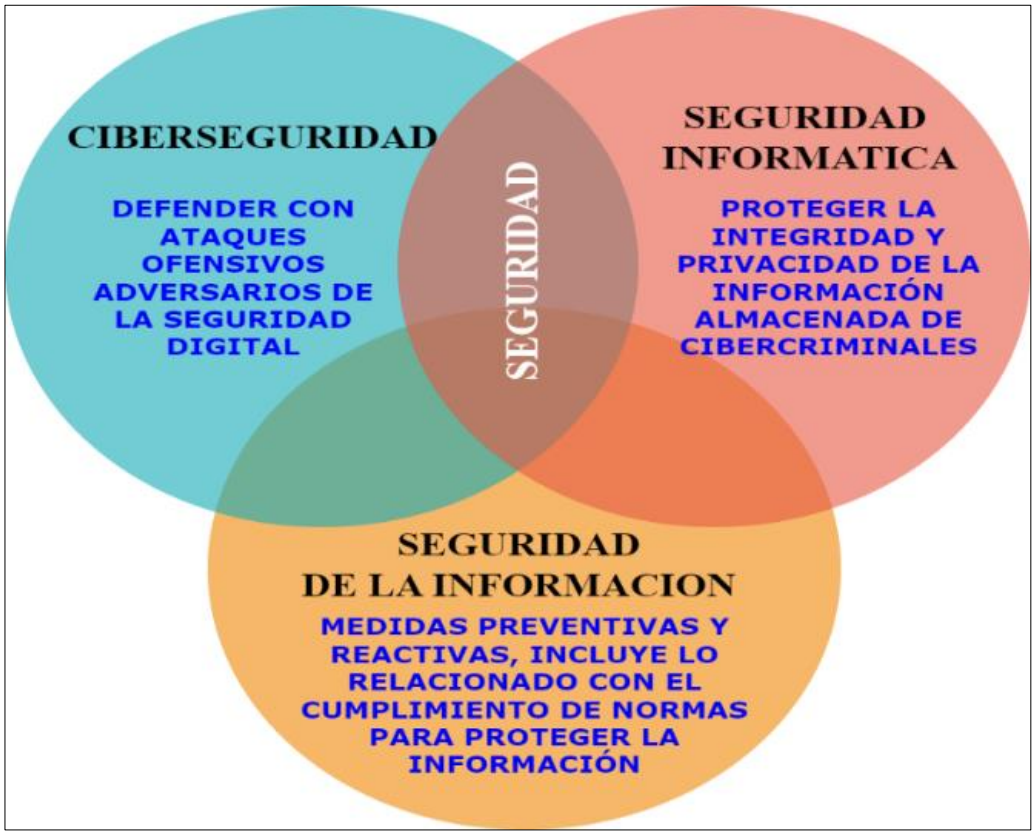
La seguridad es un concepto amplio que se refiere a la condición de estar protegido contra peligros, riesgos, amenazas o daños. Puede aplicarse a diferentes aspectos de la vida y la sociedad, y su significado puede variar según el contexto en el que se utilice.

En su obra "Marco de seguridad en tiempo real para la detección de eventos anormales en las instalaciones de ATMs" Vikas & Mittal (2016) en el cual comparto su criterio, presenta una perspectiva interesante sobre la seguridad como un concepto en constante evolución cada vez más relevante a medida que el mundo ha experimentado cambios en la naturaleza de las amenazas.

2.2.4. Diferencia entre seguridad informática, ciberseguridad y seguridad de la información.

Es importante diferenciar estos conceptos en los ambientes de seguridad, para conocer en donde se deben aplicar, concordando con el estudio de Balaji & Poornima (2021) donde indica que normalmente la seguridad de la informacion comienza con la seguridad informatica, que consiste en brindar seguridad a las ubicaciones fisicas, hardware y software frente las amenazas.

Figura 7. Seguridad de la información, ciberseguridad y seguridad informática



Elaborado por: El autor

2.2.5. Seguridad física

La seguridad física es un conjunto de medidas y sistemas diseñados para proteger activos, instalaciones y personas contra amenazas físicas, como robos, intrusiones, daños, incendios,

desastres naturales, entre otros. Los elementos y componentes clave de la seguridad física varían según la aplicación y el entorno. De acuerdo con Tamas (2021) en sus estudios de seguridad en ATMs, indica que los ataques fisicos cada vez son mas novedosos, lo que conlleva a evolucionar en los metodos de defensa, enfatisando en la seguridad fisica.

Para responder a las diferentes necesidades y características de las empresas, organización o instituciones basado en lo indicado por Tamas 2021 nos centramos en analizar los ataques y contramedidas existentes basados en técnicas conocidas y proponer mecanismos defensivos desde múltiples perspectivas, los servicios de seguridad física se clasifican en las siguientes categorías:

- Seguridad física en instalaciones
- Seguridad física industrial
- Seguridad física de protección a personas

Estos elementos trabajan en conjunto para garantizar una protección adecuada en una variedad de entornos, la selección y aplicación de estos elementos puede variar según las necesidades y riesgos específicos de cada ubicación.

De acuerdo Tamas (2021) en sus estudios de seguridad en ATMs enfatiza en los elementos clave de la seguridad física, como una guía para los fabricantes y las instituciones financieras con el fin de ayudar a proteger los productos y activos. En la siguiente figura se muestran los elementos adecuados para mejorar la seguridad física:

Figura 8. Elementos de la seguridad física

Elaborado por: El autor

2.2.6. Seguridad Electrónica

La seguridad electrónica se refiere a la aplicación de tecnologías electrónicas y sistemas de seguridad para proteger personas, propiedades, datos y activos contra amenazas y riesgos. Estos sistemas utilizan componentes electrónicos y tecnología de la información para monitorear, detectar, prevenir y responder a intrusiones, incendios, inundaciones y otros eventos no deseados.

De acuerdo con Sabani & Rishan (2019) en su estudio de efectividad de los mecanismos de seguridad de los ATMs indica que es muy importante la seguridad electronica para todas las personas en cualquier lugar del mundo. Debido al rapido avance de la ciencia, la tecnologia y sus desafios contra la seguridad y la privacidad.

Estos son algunos de los elementos clave de la seguridad electrónica que se utilizan para proteger sistemas, datos y activos frente a amenazas cibernéticas y riesgos de seguridad. De acuerdo con Sabani & Rishan (2019) en su estudio de efectividad de los mecanismos de seguridad de los ATMs, la implementación de una combinación adecuada de estos elementos es fundamental para mantener la seguridad electrónica de manera efectiva, la seguridad electrónica se refiere a la protección de sistemas y dispositivos electrónicos contra amenazas, intrusiones y ataques. Los elementos clave de la seguridad electrónica incluyen en la figura #:

Figura 9. Elementos de la seguridad electrónica

Elaborado por: El autor

Existen varios tipos de seguridad electrónica, cada uno diseñado para abordar diferentes aspectos de la seguridad en entornos digitales y físicos, la combinación adecuada de estos tipos de seguridad puede ayudar a proteger tanto los activos digitales como los físicos de manera más

efectiva, De acuerdo con Sabani & Rishan (2019) en su estudio de efectividad de los mecanismos de seguridad de los ATMs, sin embargo tambien se presentan riesgos al violar estos niveles de seguridad que se describen algunos de los tipos más comunes de seguridad electrónica:

Figura 10. Componentes de la seguridad electrónica

Elaborado por: El autor

2.2.7. Aplicabilidad

Aplicabilidad se refiere a la capacidad o adecuación de una idea, norma, regla, proceso, tecnología o principio para ser utilizado o implementado en una determinada situación, contexto o entorno. En otras palabras, se trata de evaluar si algo es relevante o útil en una circunstancia específica. La aplicabilidad implica considerar si una solución o concepto es apropiado y efectivo para abordar un problema o cumplir un propósito particular (Creswell, 2017)

La aplicabilidad se relaciona con la pertinencia y la idoneidad de una cosa en un contexto dado. Por ejemplo, cuando se desarrolla una política de seguridad cibernética para una empresa, se debe evaluar su aplicabilidad para las operaciones y necesidades de seguridad de la empresa

en particular. Del mismo modo, en el ámbito legal, se considera la aplicabilidad de las leyes a situaciones y casos específicos.

2.2.8. ¿Qué es un proceso?

Un proceso es una secuencia de pasos o actividades interrelacionadas que se llevan a cabo con el objetivo de alcanzar un resultado o un fin específico. Los procesos son fundamentales en una amplia variedad de campos, como la industria, la administración, la ciencia, la tecnología y muchas otras áreas de la vida cotidiana (Sandoval Sucre, 2017)

La interconexión de los pasos es un aspecto fundamental de los procesos. Un paso en un proceso generalmente está vinculado a los pasos anteriores y posteriores, y cualquier cambio o alteración en un paso puede tener un impacto en el conjunto del proceso.

Es una parte o un conjunto de pasos dentro de un proceso más grande. Estos subprocesos son secuencias de actividades relacionadas que contribuyen a la realización de un objetivo específico dentro del proceso general. Los subprocesos suelen ser más detallados y específicos que el proceso principal y se utilizan para dividir el trabajo en unidades más manejables o para abordar aspectos particulares de un proceso más amplio (Sandoval Sucre, 2017).

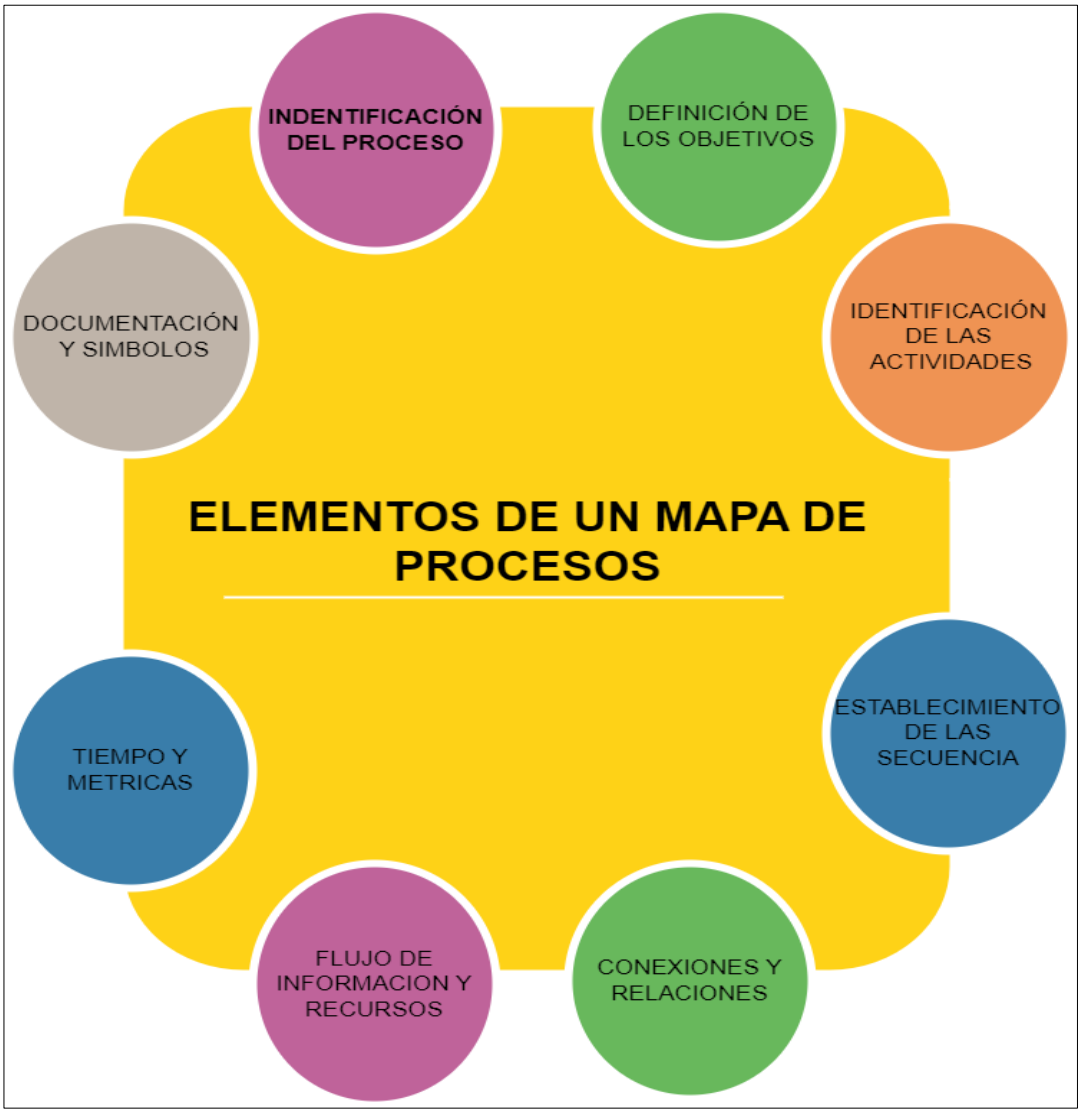
La diferencia principal entre un proceso y un subproceso radica en su alcance y nivel de detalle dentro de una estructura jerárquica de actividades relacionadas, En resumen, un proceso es una entidad más amplia que abarca un conjunto general de actividades, mientras que un subproceso es una subdivisión más detallada y específica de un proceso principal (Sandoval Sucre, 2017).

2.2.9. Mapa de procesos y elementos de procesos

Un mapa de procesos, también conocido como diagrama de procesos, es una representación gráfica que muestra la secuencia de actividades y la interacción entre ellas en un proceso específico. Estos mapas son herramientas visuales que ayudan a comprender, analizar y mejorar la ejecución de los procesos en organizaciones y empresas, El mapa de procesos permite representar los procesos y sus interrelaciones. La principal labor para realizar esto implica la identificación de los procedimientos de la organización y su conexión secuencial de forma estructurada, en función de su secuencia de ejecución (Sandoval Sucre, 2017).

Los mapas de procesos son herramientas esenciales en la gestión de procesos y la mejora continua. Proporcionan una visión clara de cómo se realizan las actividades en una organización y permiten optimizar la eficiencia, la calidad y la coherencia en la ejecución de los procesos. La creación de un mapa de procesos es una herramienta valiosa para comprender, analizar y optimizar los procesos dentro de una organización. Contribuye a detectar deficiencias, puntos críticos y zonas con potencial de mejora en el funcionamiento. La representación gráfica facilita la comunicación y la colaboración entre los equipos y los miembros de la organización. (Sandoval Sucre, 2017)

Figura 11. Elementos de un mapa de procesos



Elaborado por: El autor

2.2.10. Proceso de implementación

Se refiere al conjunto de pasos y actividades necesarios para llevar a cabo y poner en práctica una decisión, un proyecto, un sistema o un plan estratégico en una organización. La implementación es una fase crítica en la gestión, ya que es donde se pasa de la planificación a la acción con el objetivo de lograr los resultados deseados (Sandoval Sucre, 2017)

2.2.11. Diferencia entre implementación e implantación, guía de implementación

La diferencia entre implementación e implantación radica en el contexto y el significado específico de cada término, aunque a menudo se utilizan indistintamente, tienen connotaciones ligeramente diferentes, la implementación se refiere al proceso de llevar a cabo o poner en práctica una decisión, plan, proyecto, sistema, políticas, estrategia o cualquier otro tipo de cambio en una organización o contexto específico, mientras que implantación se refiere a la acción de fijar o insertar algo de manera permanente en un lugar o posición específica (Sandoval Sucre, 2017)

La creación de una guía o instructivo de implementación es esencial para asegurar que un proceso, proyecto o cambio se lleve a cabo de manera efectiva. Esta guía proporciona un conjunto de pasos y directrices detalladas que ayudan a las personas involucradas a comprender cómo realizar la implementación (Efendi, 2019)

2.2.12. Modelo de negocio financiero

Es un enfoque o estrategia que una empresa utiliza para gestionar sus operaciones y generar ingresos a través de la gestión de sus recursos financieros. Este modelo se centra en cómo una empresa planea ganar dinero, invertirlo y administrarlo para lograr sus objetivos financieros y comerciales, representa uno de los pilares fundamentales de la economía del país, razón por la cual se buscó profundizar en el comportamiento de las entidades bancarias, un modelo de negocio financiero es la estrategia que una empresa utiliza para generar ingresos y gestionar sus recursos financieros. Estos modelos pueden variar ampliamente según la industria, el tipo de empresa y los objetivos financieros (Ordoñez, 2020)

También conocido como sistema de gestión bancaria, se refiere a la herramienta informática primordial de un banco, en otras palabras, es el esquema de IT de las entidades financieras, tiene como objetivo procesar las transacciones bancarias y manejar los datos de los clientes, se puede definir como un sistema back-end, el cual procesa transacciones bancarias y publica sus actualizaciones en cuentas y otros registros financieros. (Cisneros Alvarado, 2022)

2.2.13. Superintendencia de Bancos

La Superintendencia de Bancos (SB) de Ecuador desempeña el rol de supervisar, regular y controlar el sistema financiero nacional. Además, su responsabilidad incluye garantizar que las entidades supervisadas cumplan con la legislación vigente y velar por la protección de los usuarios, todo ello con el fin de fomentar la confianza en el sistema financiero. La importancia de esta entidad es destacada en la Constitución de la República, específicamente en el Artículo 309 (Superintendencia de Bancos Ecuador, 2019).

Las normas de control interno para entidades financieras en Ecuador, incluyendo bancos, están establecidas por la Superintendencia de Bancos (SB), se han desarrollado para garantizar la seguridad, la estabilidad y la transparencia del sistema financiero en el país, es importante destacar que estas normas de control interno pueden cambiar con el tiempo y varían según las circunstancias económicas y las políticas gubernamentales, las instituciones financieras en Ecuador deben estar al tanto de las regulaciones vigentes y adaptarse a ellas para garantizar su cumplimiento y mantener la solidez y seguridad del sistema financiero (Superintendencia de Bancos Ecuador, 2019)

Es el organismo técnico de supervisión y control de las entidades del sector Financiero Popular y Solidario, y de las organizaciones de la Economía Popular y Solidaria del Ecuador

que, en el ámbito de su competencia, promueve su sostenibilidad, correcto funcionamiento y con procesos técnicos, transparentes y confiables, para contribuir al bienestar de sus integrantes y de la comunidad en general (Superintendencia de Economía Popular y Solidaria, 2022)

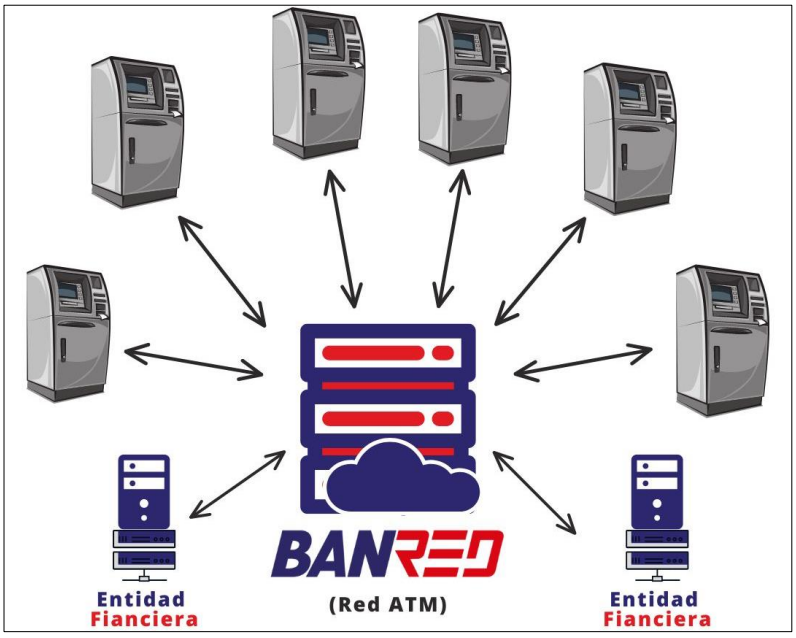
2.2.14. Banred

Se trata de una compañía que se especializa en ofrecer soluciones para la gestión electrónica de transacciones financieras, la liquidación de pagos y cobros, así como la facilitación del intercambio de datos, con una base de 5800 ATMs conectados a su sistema (Banred, 2023).

Dentro de sus servicios tiene 2 modalidades: Back-End y Front-End.

- Front-End bajo este esquema de conexión, los ATMs de la entidad financiera se enlazan a la red interbancaria de forma directa.
    1. Monitoreo y administración permanente de cajeros.
    2. Ruteo de las transacciones durante todo el ciclo.
    3. Configuración para el ingreso de nuevos cajeros.
    4. Pruebas técnicas en ambiente de desarrollo y certificaciones operativas gestionadas en producción.

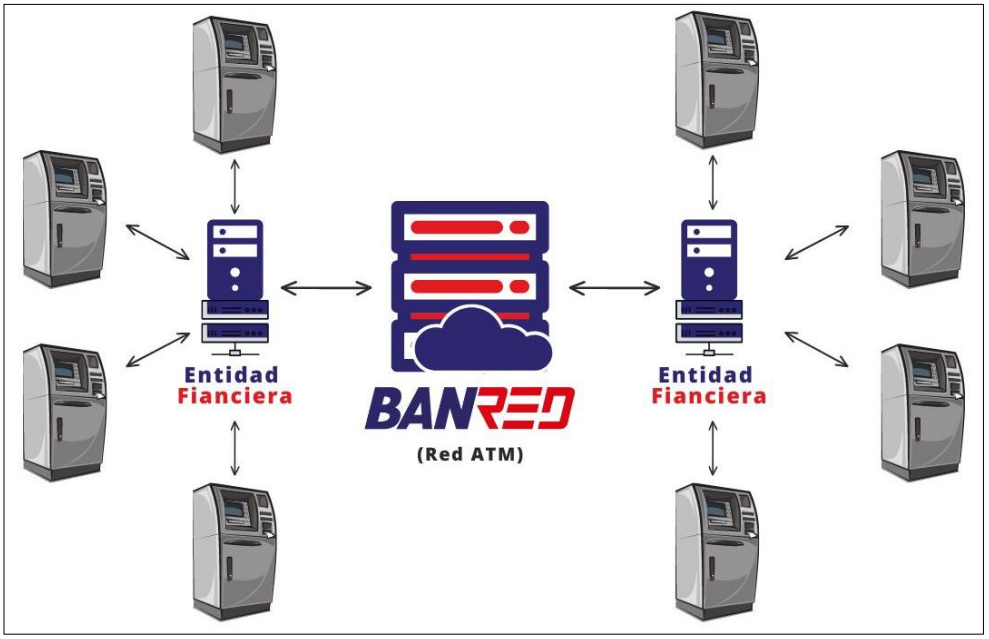
Figura 12. Modalidad Front-End Banred



Fuente: Modalidad Front-End Banred 2023 https://www.banred.fin.ec/

- Back-End en esta modalidad la institución financiera conserva la administración y operación de sus ATMs utilizando su propia infraestructura.

Figura 13. Modalidad Back-End Banred



Fuente: Modalidad Front-End Banred 2023 https://www.banred.fin.ec/

2.2.15. Instituciones financieras del Ecuador conectadas a Banred.

La interconexión de los cajeros automáticos, corresponsales no bancarios y dispositivos de las distintas instituciones que forman parte del sistema financiero del Ecuador, Banred presta sus servicios a 12 Bancos, 12 cooperativas de ahorro y crédito de manera directa y existen bancos los cuales prestan sus servicios financieros a cooperativas como por ejemplo Banco del Austro quien tiene a su cargo 13 cooperativas, cabe indicar que existe una empresa llamada RTC Coonecta que presta los mismos servicios de Banred pero a Cooperativas (Banred, 2023)

Tabla 5. Entidades financieras conectadas a Banred

Entidades financieras conectadas a Banred		
Bancos	**Cooperativas**	**Otros**
Banco Pichincha	Coopmego	Mutualista Ambato
Banco Guayaquil	Coop. 23 de Julio	Mutualista Pichincha
Banco Bolivariano	Coop. 29 de Octubre	Servipagos
Banco Internacional	Coop. Oscus	
Banco Del Pacífico	Coop. Atuntaqui	
Banco De Machala	Coop. Andalucía	
Banco Solidario	Coop. Ambato	
Banco DelBank	Coop. Alianza del Valle	
Banco Procredit	Coop. Fernando Daquilema	
Banco Desarrollo	Coop. JEP	
Banco Produbanco	Coop. Policía Nacional	
Banco Del Austro	Coop. Jardín Azuayo	
Banco Del Austro (Coop. Chone)		
Banco Del Austro (Coop. San Francisco)		
Banco Del Austro (CCCA)		
Banco Del Austro (Coop. Santa Rosa)		
Banco Del Austro (Coop. SAC)		
Banco Del Austro (Coop. Juan Pío de Mora)		
Banco Del Austro (Coop. Textil 14 de marzo)		
Banco Del Austro (Coop. Artesanos)		
Banco Del Austro (CACECH)		
Banco Del Austro (COACMES)		
Banco Del Austro (Coop. Comercio)		
Banco Del Austro (CACSPMEC)		
Banco Del Austro (Coop. La Dolorosa)		

Elaborado por: El autor

Tabla 6. Entidades financieras conectas a RTC Coonecta

Red Transaccional Coonecta (RTC)		
(RTC) Mutualista Azuay	(RTC) Coop. 4 de Octubre	(RTC) Coop. Santa Anita
(RTC) Coop. Tulcán	(RTC) Coop. 15 de Abril	(RTC) Coop. 9 de Octubre
(RTC) COOPROGRESO	(RTC) Coop. Pedro Moncayo	(RTC) Coop. Once de Junio
(RTC) COOPCCP	(RTC) Coop. Crea	(RTC) Coop. Pablo Muñoz Vega
(RTC) Coop. San José	(RTC) Coop. Fortuna	(RTC) Coop. Santa Ana
(RTC) CACPE Biblián	(RTC) COOPAC Austro	(RTC) Coop. San Antonio
(RTC) Coop. Mushuc Runa	(RTC) Coop. Futuro Lamanense	(RTC) CACPE Yantzaza
(RTC) CACPE Pastaza	(RTC) Coop. Nueva Huancavilca	(RTC) CACMU
(RTC) CACPECO	(RTC) Coop. Padre Julian Lorente	(RTC) Coop. Minga
(RTC) CACPE Gualaquiza	(RTC) COOPAC Santo Domingo	(RTC) Coop. Antorcha
(RTC) Coop. San Miguel de los Bancos	(RTC) Coop. Semilla del Progreso	(RTC) Coop. Sierra Centro
(RTC) Coop. La Benéfica	(RTC) COOPERCO	(RTC) CACEZCH
(RTC) Coop. Calceta	(RTC) Coop. Lucha Campesina	(RTC) CACPE Loja
(RTC) Cacpe Zamora	(RTC) Coop. Chibuleo	(RTC) MULTICOOP
(RTC) Coop. La Merced	(RTC) Coop. Unión Mercedaria	(RTC) Coop. KullkiWasi
(RTC) Coop. Guaranda	(RTC) CAJA	(RTC) Mutualista Ambato
(RTC) Coop. Coca	(RTC) Coop. Tena	(RTC) Coop. Alianza Minas
(RTC) Coop. Andina	(RTC) Coop. Maquita Cushunchic	(RTC) Coop. San Isidro
(RTC) Coop. Luz del Valle	(RTC) Coop. Santa Isabel	(RTC) Coop. Virgen del Cisne

Elaborado por: El autor

2.2.16. ¿Qué es un cajero automático (ATM)?

Un ATM es una maquina computarizada diseñada para realizar transacciones de los usuarios sin necesidad de interacción humana. A medida que pasa el tiempo, aumenta el número de usuarios de ATM. Utilizan tarjetas, móviles, biometría para transacciones, solicitudes de saldo, retiro, depósitos, etc. (Nurlaela, 2019)

2.2.17. Tipos de ATMs

También conocidos como ATMs (Automatic Teller Machines), pueden venir en varios tipos dependiendo de su funcionalidad y ubicación. Entre los más utilizados se encuentran:

1. Outdoor Through-the-Wall Cash Dispenser (Módulos de pared)
2. Lobby ATM Self-Service Solutions (Vestíbulos o Hall)
3. Drive-Up ATM Systems (desde el vehículo)
4. Outdoor ATM Solutions (módulos al aire libre).

Figura 14. Tipos de ATMs

Fuente: Modelos de ATMs https://www.dieboldnixdorf.com/

2.2.18. Características de un cajero ATM

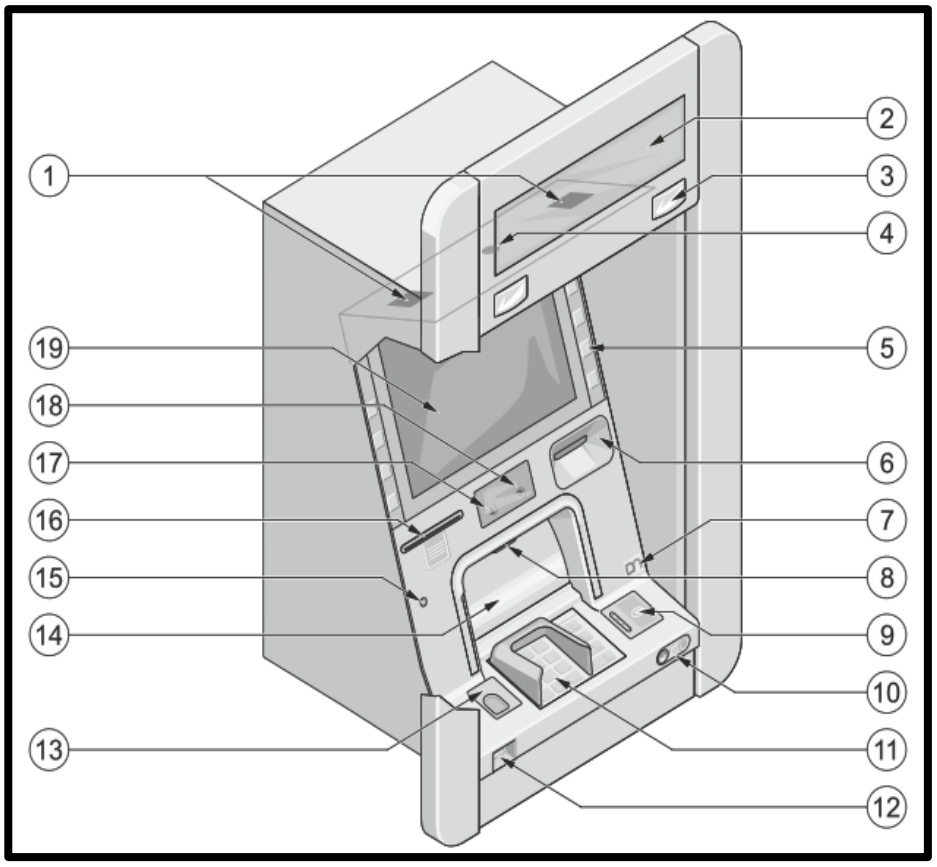
Es importante tener claro las características generales de un ATM, para poder utilizar sus funciones adecuadas y conocer que tipo transacciones realiza y el cliente tiene acceso, de esta manera optimizar de mejor forma este equipo (Nurlaela, 2019)

Figura 15. Características de un ATM

Fuente: El autor

2.2.19. Componentes del ATM

Figura 16. Parte Frontal de ATM



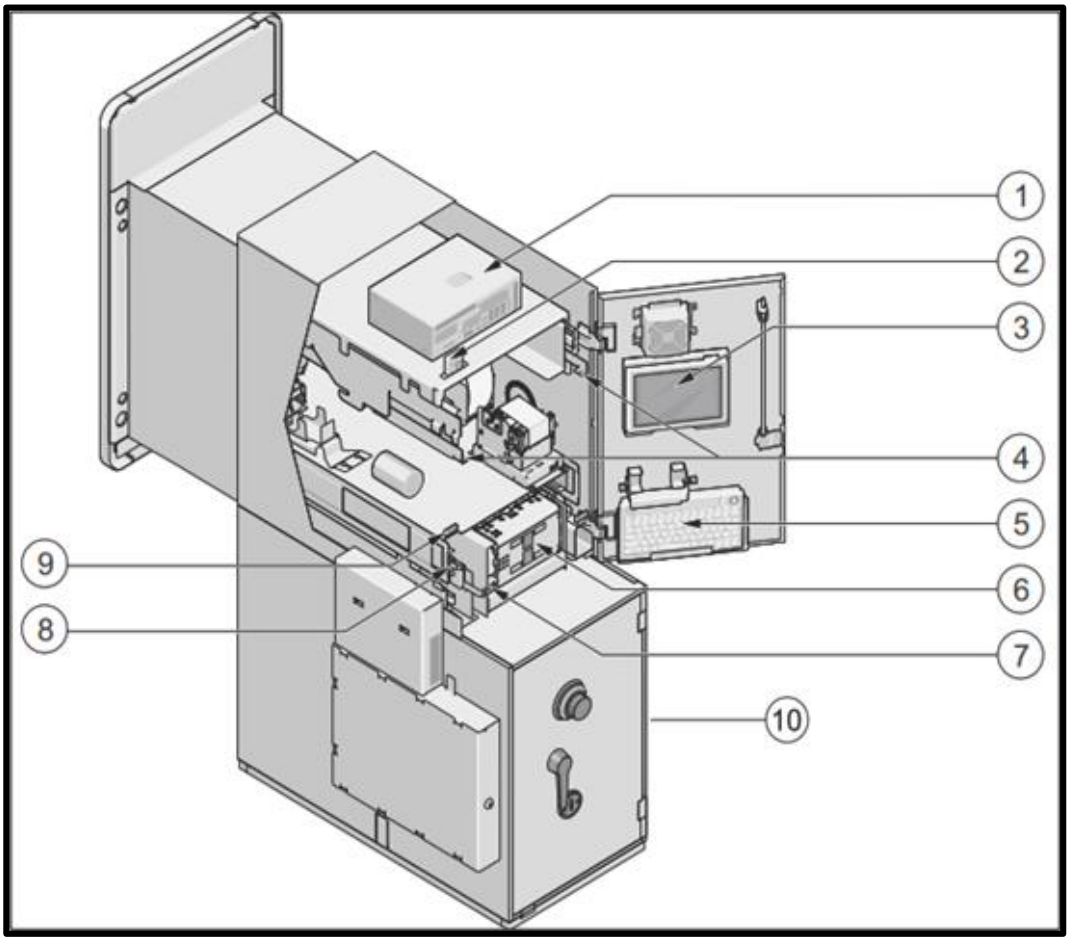
Fuente: Modelos de ATMs https://www.dieboldnixdorf.com/

Tabla 7. Parte frontal de ATM

Parte frontal de ATM			
1	Altavoces	11	Teclado EPP
2	Superficie de publicidad	12	Escáner para código de barras
3	Espejo de entorno retrovisor	13	Sensor de Huellas dactilares
4	Iluminación del panel de mando	14	Entrada y salida de dinero
5	Teclas de funciones	15	Sensor de luminosidad
6	Lector de tarjetas y Antiskiming	16	Impresora de recibos
7	Superficie para logotipo	17	Cámara de rostro
8	Cámara de compartimiento de dinero	18	Cámara panorámica
9	Lector de tarjetas sin contacto (NFC)	19	Pantalla LCD
10	Conexión para auriculares		

Elaborado por: El autor

Figura 17. Parte Trasera de ATM



Fuente: Modelos de ATMs https://www.dieboldnixdorf.com/

Tabla 8. Parte trasera del ATM

Parte trasera de ATM	
1	Pc procesador
2	Sistema de Encendido y apagado
3	Panel LCD del operador
4	Bandeja de impresora y lectora
5	Teclado del operador
6	Unidad de reciclaje o dispensado
7	Desbloqueo de modulo reciclado o dispensado
8	Banco de baterías
9	Acceso al sistema de ventilación
10	Bóveda de seguridad, dispensador de dinero

Elaborado por: El autor

2.2.20. La normativa de la seguridad de ATMs en el ámbito internacional

La normativa de seguridad también establece pautas claras para la ubicación estratégica de los ATMs, por ejemplo, la Asociación Internacional de cajeros automáticos (ATMIA, por sus siglas en inglés) ha desarrollado estándares que recomiendan instalar los ATMs en áreas bien iluminadas y de alta visibilidad, lo que disuade a posibles delincuentes y aumenta la seguridad de los usuarios (PCI-SSC, 2013).

De acuerdo al informe del European Association for Secure Transactions EAST (2019) las pérdidas por ataques físicos relacionados con ATMs fueron de 36 millones de euros, un aumento del 16% con respecto a los 31 millones de euros registrados durante 2017, la pérdida de efectivo promedio por ataque con explosivos o gas se estima en 17103 EUR, la pérdida de efectivo promedio por robo se estima en 13.682€ por incidente y la pérdida de efectivo promedio por una redada de ariete o un ataque con robo se estima en 13.198 €. estas cifras no tienen en cuenta los daños colaterales a equipos o edificios, que pueden ser significativos y, a menudo, superan el valor del dinero perdido en ataques exitosos, el director ejecutivo de EAST, Lachlan Gunn, dijo: “La tasa de éxito de los ataques con explosivos sólidos es motivo de especial preocupación: estimamos que la pérdida de efectivo promedio por ataque con explosivos sólidos es de 27065 €. Dichos ataques continúan propagándose geográficamente y dos países los informaron por primera vez a principios de 2019. Actualmente existen grupo de expertos en ataques físicos a ATMs y está monitoreando activamente la situación y proporciona una plataforma transfronteriza para que la industria y las fuerzas del orden puedan compartir inteligencia relacionada y medidas que se pueden tomar para mitigar los riesgos (EAST, 2019).

2.2.21. Estado de la ciberseguridad en el sector bancario en Latinoamérica

Además de ser un objetivo para los grupos criminales internacionales en el futuro cercano, los bancos latinoamericanos tienen sus sofisticados atacantes locales con los que lidiar. Los ataques a cajeros automáticos son un área en la que los ciberdelincuentes latinoamericanos se encuentran entre los líderes mundiales, los exploits de ATMs desarrollados en América Latina, como la familia de Malware Ploutus, han demostrado ser tan efectivos y adaptables que los delincuentes latinoamericanos han comercializado con éxito este software para la exportación (Organization of American States, 2018).

Es importante resaltar En lo que respecta a las capacidades para identificar y analizar eventos relacionados con la seguridad digital, fundamentales para abordar de manera sistemática este tipo de riesgo, más del 90% de las instituciones financieras en la región han incorporado tanto firewalls como programas antivirus automatizados, además de mantener actualizaciones del sistema. Asimismo, el 85% de estas entidades bancarias en la región ha implementado tanto Sistemas de Detección/Prevención de Intrusiones (IDS y IPS) como Procesos de Monitoreo de Amenazas y Vulnerabilidades. (Organization of American States, 2018).

2.2.22. Descripción General de la Seguridad de los ATMs

En términos de ciberseguridad para terminales de ATMs, Poornima & Dr. Savadam (2021) indican que, la aplicación de medidas como el cifrado de datos, la autenticación de usuarios, la detección de dispositivos fraudulentos y la monitorización continua son esenciales para proteger los ATMs de ataques cibernéticos, estas medidas ayudan a prevenir la clonación de tarjetas, la manipulación de dispositivos y el acceso no autorizado a los sistemas de los ATMs, la biometría de huellas dactilares, junto con las tecnologías de tarjetas inteligentes y GSM,

proporcionarán la mejor solución a este problema al aumentar los niveles de seguridad de la cuenta de usuario si se aplica un algoritmo mejorado para el reconocimiento de huellas dactilares que se puede utilizar en todos los terminales de ATMs en toda la India con un tiempo de respuesta rápido (Balaji & Poornima, 2021).

La normativa de seguridad física y electrónica es fundamental para asegurar la protección y confidencialidad de los datos financieros de los usuarios, aseguramiento del dinero en efectivo y prevenir actividades delictivas relacionadas con los ATMs. Un autor importante en este campo es Tamas (2021), quien destaca la importancia de implementar medidas de seguridad física, como la instalación de sistemas de vigilancia, sensores de movimiento y cerraduras de alta resistencia, para proteger los ATMs contra fraudes, robos y vandalismos, advirtiendo de los métodos de ataques y una guía técnica sobre la defensa (Tamas, 2021).

2.2.23. Robo de identidad y clonación de tarjetas utilizando ATMs alterados

De acuerdo con los datos obtenidos para la realización del análisis, el indicio objeto de estudio fue recolectado en la ciudad de Guatemala en el último trimestre del año 2017, luego de que la Policía Nacional Civil, la entidad bancaria y el Ministerio Público recibieran varias denuncias de robos a usuarios del cajero automático. El indicio le fue incautado a uno de los delincuentes en flagrancia, mientras lo colocaba en la parte superior de un cajero automático, con el objetivo de copiar información de las tarjetas de débito y crédito de los usuarios para posteriormente clonar las tarjetas y robar dinero. (Martinez Ralón, 2021)

2.2.24. Amenazas Emergentes en los ATMs se extiende a nivel mundial

La delincuencia en cajeros automáticos ha seguido creciendo y extendiéndose a nivel mundial a pesar de la variación regional de la frecuencia de la delincuencia. Los bancos

comerciales y los profesionales de seguridad de TI de todo el mundo se han concentrado en combatir los delitos tradicionales de cajeros automáticos, como el robo de tarjetas de cajero automático (Kasanda & Phiri, 2019)

Sobre hackeos realizados en el mismo sitio donde se encuentran los ATMs Shun-Yung & Ming-Li (2021) en su libro titulado “Robo Digital, Hackeo de ATMs e implicaciones” indican que, al procesar una transacción en un ATMs, la computadora recibe entradas del lector de tarjetas y el teclado, se comunica con el centro de procesamiento del banco (servidores) a través de una red cableada o inalámbrica, y dispensa dinero en efectivo al recibir una solicitud confirmada, interceptar cualquier sección de todas las comunicaciones puede comprometer la seguridad de los ATMs objetivo, infectar los ATMs con malware, obtener información de la tarjeta y robar efectivo. los hackers pueden insertar una "caja negra", una mini computadora preprogramada que envía comandos falsos, entre la computadora del ATMs y la caja fuerte, este tipo de ataques requiere que los piratas informáticos estén físicamente al lado de los ATMs objetivo y redirijan las comunicaciones entre la computadora y la caja fuerte, como se indicó anteriormente, por lo tanto, un malware portador de USB se puede utilizar para hackear la computadora de los ATMs y luego controlar el dispensador (Shun-Yung & Ming-Li, 2021).

2.2.25. Políticas del sector financieros en la implementación de ATMs

En Ecuador, al igual que en otros países la implementación de ATMs ha sido fundamental para brindar servicios financieros a la población. Sin embargo, esta innovación tecnológica también ha conllevado desafíos en términos de seguridad. En este ensayo se pretende explorar la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de ATMs en Ecuador, analizando cómo estas regulaciones, políticas y normativas, contribuyen a proteger la integridad, confidencialidad y disponibilidad de los ATMs

y garantizar la seguridad de las transacciones realizadas a través de ellos (Superintendencia de Bancos Ecuador, 2019).

En lo que respecta a la seguridad electrónica, el BCE establece requisitos específicos para proteger las transacciones realizadas a través de los ATMs. esto incluye la implementación de sistemas de encriptación y autenticación robustos, así como el monitoreo continuo de la infraestructura de red y la detección de posibles amenazas cibernéticas, en términos de seguridad física, el BCE exige la instalación de sistemas de vigilancia, alarmas y sistemas de bloqueo en los ATMs (Superintendencia de Bancos Ecuador, 2019).

De acuerdo con un informe realizado por la Superintendencia Económica Popular y Solidaria enmarcado a la realidad de los servicios digitales y seguridad de la información, los procesos de transformación digital implican nuevos retos en la ciberseguridad, debido a los avances tecnológicos conlleva a vulnerabilidades a las que están expuestos los clientes según los datos de la fiscalía general del Estado, hasta agosto del 2020 se registraron 5048 denuncias de delitos informáticos, en el Ecuador. El 92% se concentra en los delitos como: suplantación de identidad (43%), falsificación y uso de documento falso (29%) y apropiación fraudulenta por medios electrónicos (20%) (Seps, 2021).

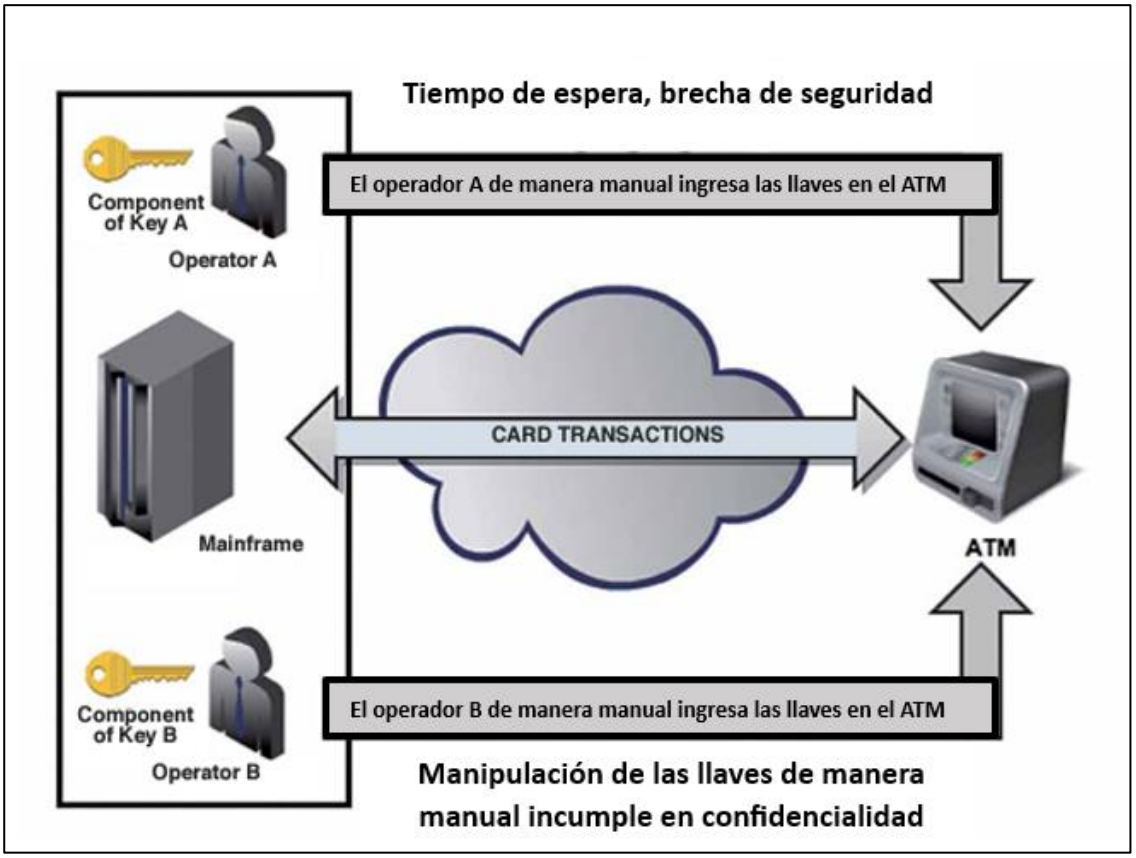
2.2.26. Métodos criptográficos para la información del ATM

Se refieren a técnicas de cifrado y seguridades utilizadas para proteger la información y las transacciones realizadas en estos dispositivos financieros. Las claves son esencialmente secuencias numéricas que permiten tomar información, asegurarla y luego enviarla. Esta información solo puede descifrarse con la introducción de una clave privada. La confidencialidad de las claves es esencial para garantizar la seguridad y proteger los datos, existen claves públicas

y privadas. La clave pública, en esencia, "abre" la clave privada, la cual se refuerza aún más mediante medidas de seguridad. Se emplean múltiples claves como parte de una estrategia deliberada. Se utiliza un código complejo para evitar la manipulación de los cajeros automáticos. (Kasanda & Phiri, 2019).

Se cifra para protegerlo durante la transmisión y el almacenamiento. Los algoritmos de cifrado como Triple DES o AES se utilizan para garantizar la seguridad del PIN, el método que se describe es un ingreso de llaves manuales en 2 códigos de 32 bits generados para ser ingresado por el personal asignado.

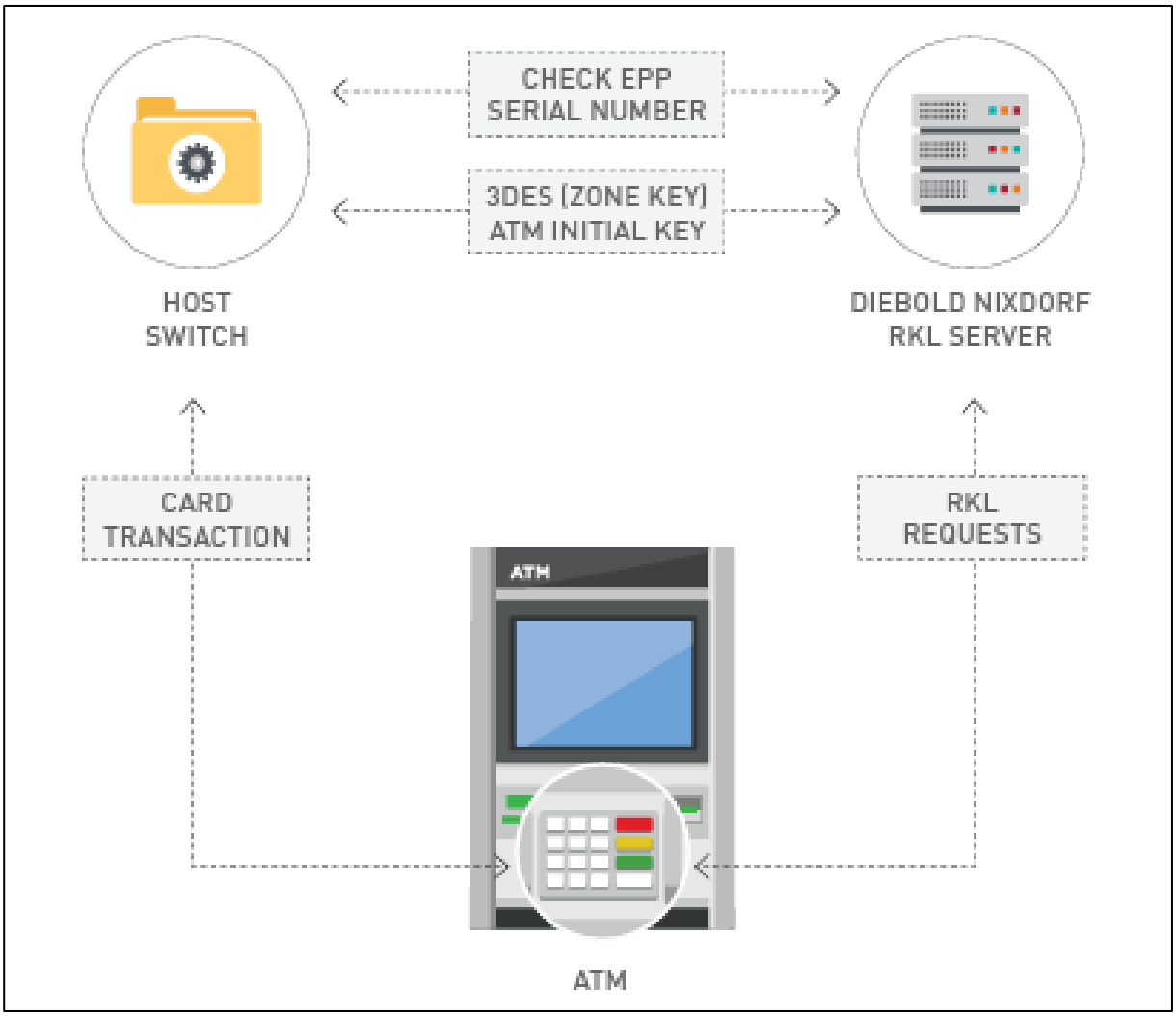
Figura 18. Procedimiento de ingreso de llaves manuales



Fuente: Datasheet-Cryptosec-RKL – www.realsec.com

Se describe el proceso cifrado en un ATM, utilizando el método RKL, el cual consiste en generación de llaves remotas, las cuales son generadas por un servidor e ingresada mediante una trama de información, esto reduce los temas de confidencialidad al ser menos manipulado por el ser humano. De la misma manera que el método manual, la generación de las llaves contienen el mismo cifrado 3DES, lo cual garantiza la seguridad de la información.

Figura 19. Procedimiento de ingreso de llaves remotas



Fuente: Diebold Nixdorf – www.dieboldnixdorf.com

2.3. Marco legal

En el Ecuador existe un marco jurídico enfocado a la protección y reconocimiento de la ciberseguridad entre las que se encuentran: la Constitución de la República del Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública, Ley Orgánica del Sistema Nacional de Registro de Datos Públicos y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y el Código Orgánico Integral Penal, Ley Orgánica de protección de datos personales, Ley Orgánica de Telecomunicaciones.

A pesar de lo expuesto, aun es insuficiente teniendo en cuenta que las disposiciones jurídicas están dispersas y muchas de ellas están incompletas y rezagadas ante el desarrollo tecnológico actual.

2.3.1. Constitución de la República del Ecuador

La ciberseguridad se ha convertido en un tema crítico para garantizar la protección de los datos, la privacidad y la integridad de la información. En Ecuador, la Constitución de la República establece los principios y derechos fundamentales que garantizan la seguridad en el país. En esta investigación, examinaremos la relación entre la Constitución de la República del Ecuador y la ciberseguridad, destacando cómo esta normativa contribuye a salvaguardar los derechos y proteger a los ciudadanos en el entorno digital.

El estado ecuatoriano garantiza la seguridad humana a través de políticas y acciones integradas, para prevenir las formas de violencia y discriminación, para lo cual se encargará a órganos especializados en los diferentes niveles de gobierno la planificación y aplicación de estas políticas, tal como se establece en el artículo 393 de su carta magna (Constitución de la Republica del Ecuador, 2008).

2.3.2. Código Orgánico Integral Penal

Es importante destacar que el Código Orgánico Integral Penal (COIP) también aborda otros delitos informáticos, como el acceso ilícito a redes y sistemas de telecomunicaciones, el daño a programas o datos informáticos, la interceptación de comunicaciones electrónicas y el fraude informático. Estas disposiciones reflejan el compromiso de Ecuador en la lucha contra los delitos cibernéticos y la protección de la seguridad en línea, dentro de lo expuesto es importante indicar la importancia de la investigación, con el fin de alinearse en el propósito de la seguridad, como lo tipifica el artículo 234 y 235 del COIP (Código Orgánico Integral Penal, 2014)

2.3.3. Cooperación Internacional con Ecuador en la ciberseguridad

Gracias a la colaboración internacional, Ecuador ha desarrollado su Estrategia Nacional de Ciberseguridad. Ha recibido orientación y asesoramiento del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (CICTE/OEA) y del Proyecto de Resiliencia Cibernética para el Desarrollo de la Unión Europea (CYBER4DEV). Este documento establece las directrices para la seguridad cibernética a nivel nacional y ha sido elaborado con la participación de más de 170 actores, incluyendo representantes de la sociedad civil, académicos, expertos en ciberseguridad, entidades gubernamentales, el sector privado y todas las instituciones que integran el Comité Nacional de Ciberseguridad. Este comité, creado en la actual administración gubernamental, reúne a los Ministerios de Telecomunicaciones y de la Sociedad de la Información, Defensa Nacional, Gobierno, Interior, Relaciones Exteriores y Movilidad Humana, el Centro de Inteligencia Estratégica y la Secretaría General de la Administración Pública de la Presidencia. (Mintel, 2022).

Mediante la ciberseguridad, podemos promover otros avances en el ámbito digital, como el impulso del comercio electrónico, la protección de nuestra información y transacciones financieras, el resguardo de datos personales de los ciudadanos, y la seguridad de la información comercial a nivel local e internacional. Esto se debe a que los datos se han convertido en un recurso sumamente valioso a nivel global y son el epicentro de la reconfiguración de los gobiernos en el siglo actual, garantizar su seguridad es crucial, ahora más que nunca. En la actualidad, un simple clic nos conecta con el mundo, lo que subraya la importancia de contar con una estrategia en ciberseguridad que se base en las mejores prácticas a nivel mundial. (Mintel, 2022).

2.3.4. Ley Orgánica de telecomunicaciones

La Ley de Telecomunicaciones del Ecuador aborda la ciberseguridad en diversas dimensiones. En primer lugar, establece la responsabilidad de los proveedores de servicios de telecomunicaciones de implementar medidas de seguridad adecuadas para salvaguardar la integridad de los datos y la información de los usuarios. Esto implica la adopción de protocolos de cifrado, sistemas de autenticación sólidos y mecanismos de protección contra amenazas cibernéticas, tal como lo describe el Artículo 76, el cual se refiere a las medidas técnicas de seguridad e invulnerabilidad. Estas medidas se diseñarán de manera que proporcionen un nivel de seguridad apropiado en función de los riesgos existentes. En caso de que surja un riesgo específico que amenace la seguridad de la red, el proveedor de servicios de telecomunicaciones tiene la obligación de informar a sus abonados, clientes o usuarios acerca de dicho peligro. Además, si las soluciones para mitigar o eliminar dicho riesgo no están bajo su control, también debe comunicar posibles alternativas (Ley Orgánica de Telecomunicaciones).

Además, la legislación también establece la creación de un Centro de Respuesta a Incidentes de Seguridad Informática (CERT) en el país. Este centro tiene como objetivo coordinar las acciones necesarias para prevenir, detectar y responder a incidentes de seguridad cibernética.

A pesar de los esfuerzos realizados a través de la Ley de Telecomunicaciones del Ecuador en materia de ciberseguridad, existen desafíos significativos que aún deben abordarse. Uno de los principales desafíos es el aumento constante de las amenazas cibernéticas y la evolución de las técnicas utilizadas por los ciberdelincuentes. Esto requiere una constante actualización de las medidas de seguridad y una mayor colaboración entre el sector público y privado para enfrentar estas amenazas.

2.3.5. Ley Orgánica de protección de datos personales (LOPD)

En el sector bancario, donde se manejan gran cantidad de datos personales sensibles, la (LOPD) es especialmente relevante. Los bancos recopilan información personal de sus clientes, como nombres, números de identificación, direcciones, historial crediticio y transacciones financieras. La LOPD establece que los bancos deben obtener el consentimiento informado de los titulares de los datos antes de recopilar y tratar su información personal.

Además del consentimiento, la LOPD exige que los bancos implementen medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales y prevenir su acceso no autorizado, pérdida o alteración. Esto implica el uso de protocolos de seguridad robustos, como el cifrado de datos, la adopción de políticas de gestión de riesgos y la capacitación de su personal en materia de protección de datos, como lo tipifica el articulo 37 Seguridad de datos personales. El responsable del tratamiento de datos personales según sea el

caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo con la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos (Ley Orgánica de protección de datos personales, 2021).

2.3.6. Codificación de las Normas de la Superintendencia de Bancos

Es importante destacar que estas normas son dinámicas y están sujetas a cambios y actualizaciones. La Superintendencia de Bancos del Ecuador emite regularmente circulares y resoluciones complementarias que modifican y actualizan las disposiciones existentes. Por lo tanto, las instituciones financieras y otros actores involucrados en la operación de cajeros automáticos deben mantenerse actualizados con respecto a las últimas regulaciones emitidas por la Superintendencia de Bancos en el marco de la seguridad y disponibilidad de dichos dispositivos.

Es un examen con observaciones detalladas de las bases legales que respaldan la investigación, incluyendo la identificación de los documentos legales que establecen el contexto del tema investigado y proporcionan pautas para su progreso.

La Superintendencia de Bancos del Ecuador ha emitido una serie de normas específicas que regulan el funcionamiento de los cajeros automáticos en el país. Estas normas tienen como objetivo establecer los requisitos mínimos de operación, seguridad y atención al cliente para los cajeros automáticos, con el fin de proteger los intereses de los usuarios y garantizar la estabilidad del sistema financiero.

Una de las normas relevantes en este contexto es la Resolución No. JB-2018-190, emitida por la Superintendencia de Bancos en el año 2018. Esta resolución establece disposiciones generales sobre los cajeros automáticos, incluyendo aspectos relacionados con su instalación, ubicación, mantenimiento y operación. Además, se establecen medidas de seguridad que deben ser implementadas por las instituciones financieras, como el uso de sistemas de videovigilancia, alarmas y controles de acceso (Superintendencia de Bancos Ecuador, 2019).

2.3.7. Norma para las entidades de los sectores financieros público y privado

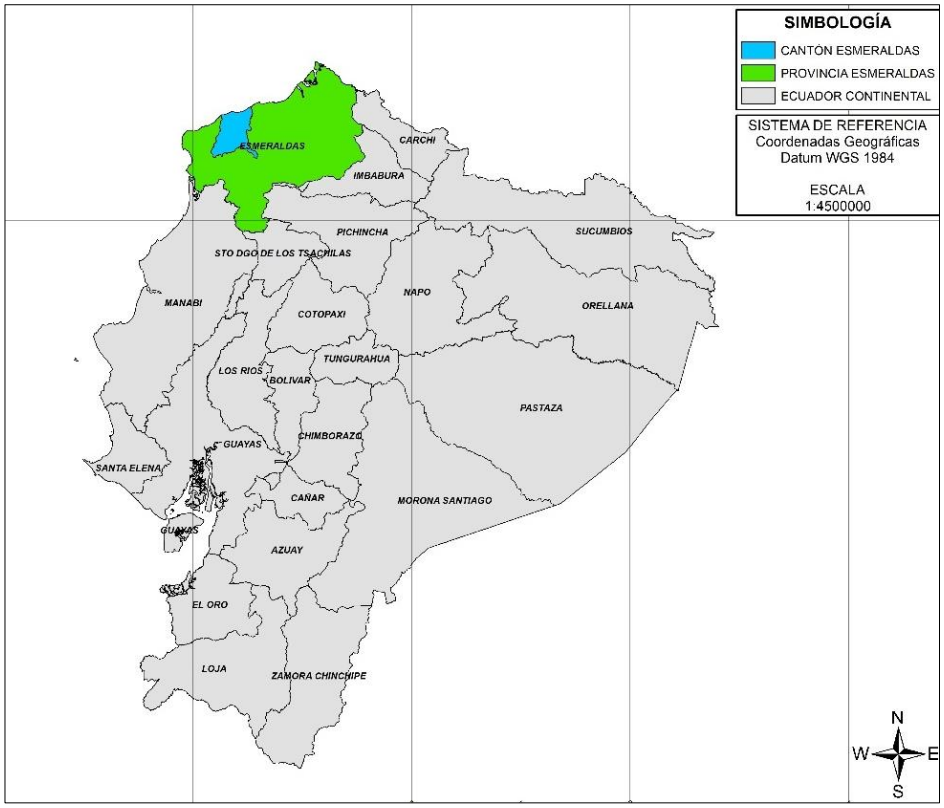
Las normas de control para las entidades de los sectores financieros público y privado en Ecuador están diseñadas para regular y supervisar las actividades financieras y asegurar la estabilidad del sistema financiero del país. Estas normas son establecidas y supervisadas por la Superintendencia de Bancos y Seguros de Ecuador, que es la entidad encargada de regular el sistema financiero. Es importante destacar que estas normas y regulaciones pueden evolucionar con el tiempo, y las entidades financieras están obligadas a mantenerse actualizadas y cumplir con los requisitos establecidos por las autoridades regulatorias en Ecuador (Superintendencia de Bancos Ecuador, 2019).

3. CAPITULO III MARCO METODOLOGICO

3.1. Descripción del área de estudio

El presente proyecto se desarrolló en la ciudad de Esmeraldas, donde se encuentran distribuidas distintas entidades financieras públicas y privadas, teniendo bajo su custodia ATMs. Esmeraldas se encuentra localizada en la costa noroccidental del Ecuador, capital de la provincia del mismo nombre, situada a 00°59' de latitud norte y 79°39' de longitud Oeste. Sus límites más próximos lo constituye: al Norte con el Océano Pacífico, al Sur con la Parroquia Vuelta Larga, al Este con el Río Esmeraldas, y al Oeste con el Cantón Atacames. El área urbana tiene una superficie aproximada de 2847,58 hectáreas, dividida territorialmente en 5 parroquias urbanas (Luís Tello, Bartolomé Ruiz, Esmeraldas, 5 de agosto, y Simón Plata Torres).

Figura 20. Mapa de área de estudio



Elaborado por: El autor

3.2. Enfoque y tipo de investigación

El presente estudio asumió la investigación de campo, descriptiva, explicativa y exploratoria, con visión cuantitativa y cualitativa, es decir, buscó evaluar la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos en la ciudad de Esmeraldas. Se consiguió la unificación y análisis conjunto de los datos, lo que permitió derivar conclusiones a partir de toda la información recopilada y mejorar la comprensión del fenómeno en estudio.

Se utilizó fuentes de información para caracterizar y diagnosticar, utilizando tres instrumentos de investigación (encuesta, entrevista y ficha de observación), La revisión sistemática permitió levantar la línea base de un marco referencial para contestar o entender la situación actual en los entornos de producción e instalación de los ATMs enfatizando en la seguridad física y electrónica y diagnosticar vulnerabilidad con relación a la situación de seguridad ciudadana que vive la ciudad de Esmeraldas.

Este enfoque permitió abordar el hecho de interés investigativo, en este caso es particular, lo constituyó la evaluación de la aplicabilidad de la normativa en los procesos de implementación de ATMs, dentro del marco de la seguridad física y electrónica, así como también conocer su nivel con relación a otros países que realizan los mismos procesos de implementación normados por un ente regulador.

3.3. Procedimiento de investigación

3.3.1. Análisis documental

Se analizó la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos del Ecuador frente a la legislación de países como: El Salvador, Bolivia, Colombia, Costa Rica, Paraguay, etc.

Así mismo, el estudio se sustentó en elementos teóricos de libros, artículos científicos, revistas, boletines y estudios especializados en distintos idiomas indizados en las bases de datos Journal of Cyber Security Technology, Science Direct, Scopus, Google scholar,Springer, Redalyc y ProQuest; a través del método análisis-síntesis.

3.3.2. Investigación de campo

Geolocalización de los cajeros automáticos.

Se realizo un levantamiento de información GPS, mediante un recorrido por todas las oficinas y sucursales bancarias de la ciudad en el perímetro urbano y la red de cajeros que se encuentran fuera de las oficinas o cajeros automáticos islas. para identificar y determinar su localización geoespacial. Esto servirá para comparar la ubicación de estos ATMs con respecto a las zonas de baja, media o alta seguridad ciudadana.

Evaluación de seguridad física de los cajeros automáticos

Se elaboró una lista de chequeo en función de los requisitos normativos de seguridad física para el funcionamiento de un cajero automático, con el objetivo de comparar su cumplimiento en territorio.

Evaluación de la seguridad electrónica de los cajeros automáticos

Se elaboró una lista de chequeo en función de los requisitos normativos de seguridad electrónica para el funcionamiento de un cajero automático, con el objetivo de comparar su cumplimiento en territorio.

Encuestas y entrevistas a especialistas de seguridad física y electrónica en ATMs

Se preparó cuestionarios con preguntas abiertas para la entrevistas y preguntas cerradas para las encuestas; estas fueron dirigidas a especialistas en seguridad física y electrónicas de ATMs, los cuales estarán agrupados de la siguiente manera:

1. Lideres de Cuenta expertos en ATMs ex situ
2. Especialistas u Oficiales de seguridad de entidades financieras in situ
3. Especialistas de seguridad electrónica en sectores financieros

4. CAPITULO IV RESULTADOS Y DISCUSIÓN

En este capítulo se aplicó una ficha de observación en campo para el levantamiento de información de todos los ATMs en conjunto de un check list para la verificación y constatación in situ y ex situ, una encuesta y una entrevista dirigido a profesionales con experiencia en procesos de implementación y administración de red cajeros automáticos a nivel nacional como técnicas y estrategias para la presente investigación que fueron validadas por expertos, obteniendo excelentes resultados que fueron tabulados y presentados en gráficos de pastel, en los cuales se observan los indicadores, la frecuencia y el porcentaje, dando como información relevante para la realización del presente documento.

El instrumento de la entrevista se desarrolla basándose en descriptiva abierta, donde cada pregunta es clara, ordenada y pertinente, de tal manera que es de fácil comprensión y su respuesta precisa. A demás de contar con todos los tramites necesario para la aplicación de dichos instrumentos a los entes ya indicados.

El instrumento de la encuesta se desarrolla basándose en la escala de Likert, donde cada pregunta es clara, ordenada y pertinente, de tal manera que es de fácil comprensión y su respuesta precisa. A demás de contar con todos los tramites necesario para la aplicación de dichos instrumentos a los entes ya indicados.

El instrumento de una ficha de observación en campo se direcciona a recolectar la información de toda la flota de ATMs de la ciudad de Esmeraldas, para tener indicadores y criterios acordes a la realidad actual. Utilizando esta guía para medir situaciones que se desconocían.

4.1. Entrevista estructurada dirigida a profesionales en ATMs a nivel nacional

Las entrevistas fueron dirigidas a 7 profesionales con experiencia en procesos de implementación o administración de red de ATMs a nivel nacional, en el cual se presentaron 10 preguntas de respuestas abiertas, de acuerdo con su experiencia, preparación y conocimientos técnicos en procesos de implementación, mecanismos de defensas, aplicación de las normas de seguridad, métodos de vandalismos y robos, tipos de ATMs.

Hallazgos clave de la entrevista:

1. Nuevos métodos de seguridad como salvaguardas adicionales
2. Personal calificado para las funciones establecidas en el área de ATMs
3. La seguridad por entidad financiera es distinta, unas más robustas que otras.
4. Los ATMs islas son más propensos a ataques, son vulnerables.
5. Los entrevistados coinciden en actualizar la normativa vigente en base a los nuevos métodos de ataques que se evidencian en la actualidad.

Figura 21. Hallazgos clave

Elaborado por: El autor

Tabla 9. Resultado de entrevistas a profesionales en ATMs

PREGUNTAS GENERADAS A PROFESIONALES EN LA ENTREVISTA	RESPUESTAS
1. ¿Cuál es su cargo actual en la institución o empresa que trabaja?	El 90% de los entrevistados son especialistas técnicos en implementación de ATMs
2. Realice una breve explicación de las funciones y responsabilidades a su cargo	El 90% de los entrevistados tienen funciones y responsabilidades en el sector tecnológico financiero en automatización y autoservicios
3. ¿Conoce de la normativa vigente en procesos de implementación de ATMs en el Ecuador?	El 65% de los entrevistados conoces acerca de la normativa para bancos y cooperativas, el ente que regula las normas de seguridad en administración e implementación de ATMs
4. Sobre las medidas de seguridad física y electrónica que actualmente están implementadas en su empresa o institución ¿Tienen implementado el sistema de entintado de billetes?	El 85% de los entrevistados tiene conocimientos acerca del sistema de entintado de billetes, realizando instalaciones a entidades financiera y mantenimientos para su correcto funcionamiento
5. Para instalar un ATM en un sitio remoto o punto isla ¿Qué tipo de estudio o investigación realizan o toman en consideración?	El 60% de los entrevistados coinciden que la investigación que se realiza es más orientada a un estudio de mercado y el tema de seguridad es mínimo, el cual debería ser fortalecido por la situación actual de seguridad en el Ecuador
6. ¿Cada cuánto tiempo realizan procesos de mejoras tecnológicas o upgrade en los ATMs?	El 80% de los entrevistados indican que se debe realizar los upgrade en hardware cada 5 años y en software 1 vez por año, teniendo claro este punto como medida dispuesta por los fabricantes
7. ¿Considera usted que mejora la seguridad física del ATM la instalación de chalecos blindados a las bóvedas?	el 85% de los entrevistados coinciden que la capa física de seguridad instalada como protección, genera un entorno más robusto, mejorando la seguridad y reduciendo los ataques físicos
8. De acuerdo con su criterio profesional ¿Cuál cree usted que sea más propenso a temas de ataques, un ATM isla o de agencia?	el 100% de los entrevistados coinciden que los ATMs islas son más propensos ataques, puesto que, al encontrarse en un sitio remoto, los tiempos respuesta a incidentes son más extendidos. Indicando que, al ser vulnerables, las medidas de seguridad deberían ser mejorada

9. Sobre los métodos de ataques físicos en los ATMs evidenciados en Ecuador, los cuales han sido realizados en su mayoría por extranjeros de acuerdo con información de la fiscalía general del Estado ¿Cree usted que nuestros sistemas de seguridad son más vulnerables a comparación de otros países?	El 90% de los entrevistados coinciden que la mayoría de los ataques, fraudes y métodos de robos son perpetrados por personas extranjeras, quienes en su país de origen ya han resuelto dichas vulnerabilidades y buscan países donde no hayan sido aplicado las salvaguardas para cometer los delitos
10. Los nuevos métodos y procedimientos de seguridad para ATMs que existen en la actualidad, entre ellos chalecos blindados, sistema entintado, cortinas de humo entre otros ¿Cree usted que sea necesario aplicar alguno de estos métodos dentro de la normativa actual en el Ecuador?	El 100% de los entrevistados coinciden que además de utilizar estos mecanismos de seguridad como política interna de cada entidad financieras, se debería aplicar como norma exigida por el ente regulador

Elaborado por: El autor

4.2. Encuesta dirigida a profesionales en ATMs a nivel nacional

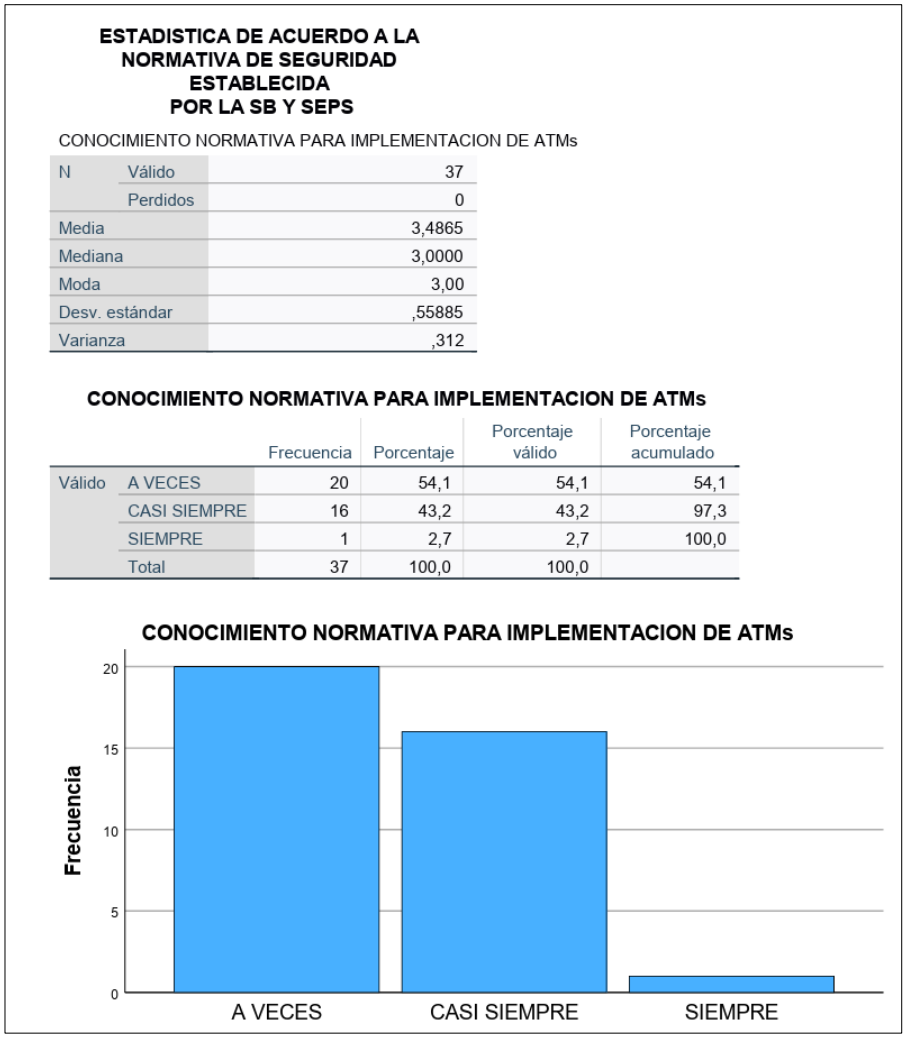
La encuesta fue dirigida a 37 profesionales con experiencia en procesos de implementación o administración de red de ATMs a nivel nacional, en el cual se presentaron 15 preguntas, enfocados a recolectar datos demográficos, conocimientos acerca de procedimientos de implementación, mecanismos de defensas, aplicación de las normas de seguridad, métodos de vandalismos y robos, tipos de ATMs.

De acuerdo con los datos recolectados en el instrumento de investigación tipo encuesta, como se evidencia en el anexo 6, se puede apreciar los resultados en la figura 22, con la aplicación de la estadística descriptiva y exploratoria, para comprender los datos de diferentes perspectiva, 7 preguntas del cuestionario estaban orientadas a la normativa de seguridad vigente, sus diferentes variaciones de acuerdo al entorno donde se aplica, la perspectiva desde el ámbito profesional en el trabajo de campo, como los procesos de instalación y administración de ATMs, donde se muestra resultados con indicadores, donde el 54,1% aplica a veces la normativa de

seguridad en instalaciones, proyectos, upgrade y procesos que obligatoriamente están establecidos en las normas de la superintendencia de bancos del Ecuador.

También se puede apreciar los datos estadísticos que son muy importante como la media con un valor de 3,4865, es la misma tendencia de resultados indicado por los profesionales encuestados, su aplicación de la normativa de seguridad en un rango del 1 al 5 como se estableció en la escala, este es un valor aceptable sobre la información adquirida, que concuerda con la varianza con 0,312 y la desviación estándar que están dentro del rango de la investigación.

Figura 22. Resultados de las encuestas sobre normativas de seguridad en el Ecuador



ESTADISTICA DE ACUERDO A LA NORMATIVA DE SEGURIDAD ESTABLECIDA POR LA SB Y SEPS

CONOCIMIENTO NORMATIVA PARA IMPLEMENTACION DE ATMs

N	Válido	37
	Perdidos	0
Media		3,4865
Mediana		3,0000
Moda		3,00
Desv. estándar		,55885
Varianza		,312

CONOCIMIENTO NORMATIVA PARA IMPLEMENTACION DE ATMs

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A VECES	20	54,1	54,1	54,1
	CASI SIEMPRE	16	43,2	43,2	97,3
	SIEMPRE	1	2,7	2,7	100,0
	Total	37	100,0	100,0	

Elaborado por: El autor

De acuerdo con los datos recolectados en el instrumento de investigación tipo encuesta, como se evidencia en el anexo 6, se puede apreciar los resultados en la figura 23, con la aplicación de la estadística descriptiva y exploratoria, para comprender los datos de diferentes perspectiva, 8 preguntas del cuestionario estaban orientadas a la seguridad aplicada a entidades financieras, sus mecanismo de seguridad, nuevas tendencias de seguridad, mecanismos de defensas, perspectiva de seguridad desde el área técnica y sus implicaciones en el trabajo de campo, donde se muestra resultados con indicadores, donde el 48,6% de los profesionales encuestados, casi siempre aplica los métodos de seguridad en las actividades con los ATMs, entre ellos lo que establece cada entidad financiera, custodia de seguridad por parte de la entidad, aseguramiento de los sites, revisión de los dispositivos antifraudes y demás mecanismos skimmer.

Como en el resultado obtenido anteriormente, son similares con referencia a la media, mientras que la mediana si muestra un resultado de 4,000 como referencia a la tendencia de resultados indicado por los profesionales encuestados, en un rango del 1 al 5 como se estableció en la escala, este es un valor aceptable sobre la información adquirida, que concuerda con la varianza con 0,312 y la desviación estándar que están dentro del rango de la investigación.

Estos resultados pueden ser apreciados de manera minuciosa, con tablas de referencias, gráficos, analisis e interpretación por cada una de las preguntas realizadas a los 37 profesionales en los anexos del instrumento de investigación tipo encuesta.

Figura 23.Resultados de las encuestas de seguridad aplicada a entidades financieras

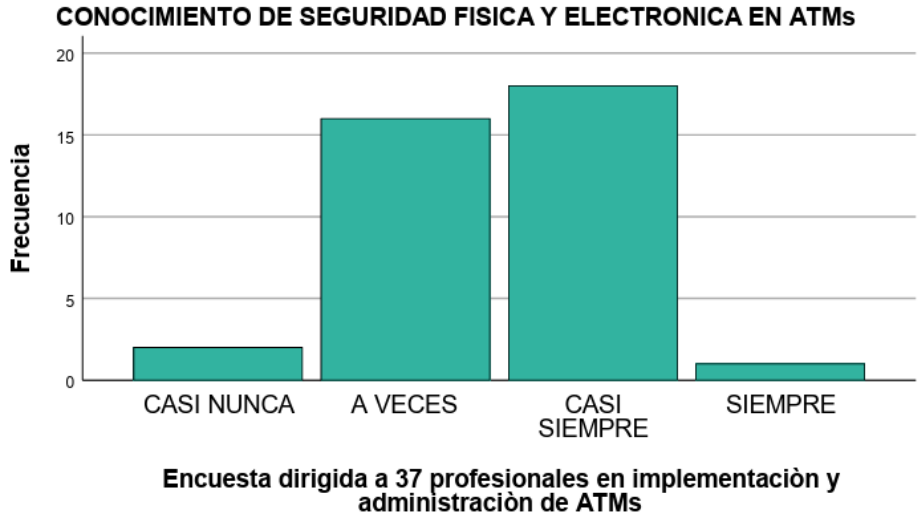
ESTADISTICA DE ACUERDO A LA SEGURIDAD APLICADA A ENTIDADES FINANCIERAS

CONOCIMIENTO DE SEGURIDAD FISICA Y ELECTRONICA EN ATMs

N	Válido	37
	Perdidos	0
Media		3,4865
Mediana		4,0000
Moda		4,00
Desv. estándar		,65071
Varianza		,423

CONOCIMIENTO DE SEGURIDAD FISICA Y ELECTRONICA EN ATMs

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CASI NUNCA	2	5,4	5,4	5,4
	A VECES	16	43,2	43,2	48,6
	CASI SIEMPRE	18	48,6	48,6	97,3
	SIEMPRE	1	2,7	2,7	100,0
	Total	37	100,0	100,0	



Elaborado por: El autor

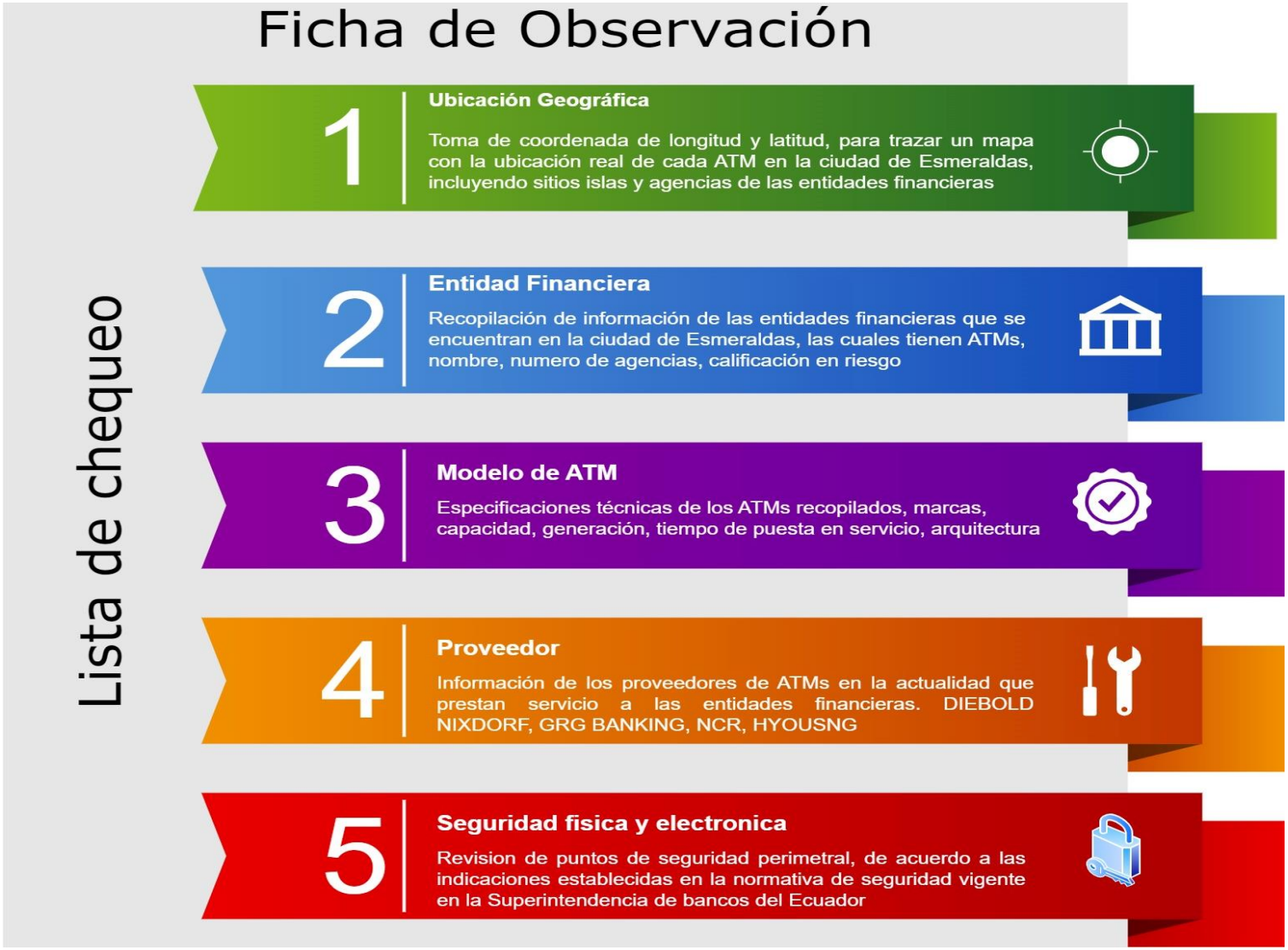
4.3. Ficha de observación en campo

Con una lista de chequeo se pudo obtener información real del cumplimiento de la normativa establecida en proceso de implementación y jerarquizar cada uno de ellos, se utilizó como requisito, la entidad financiera mejor calificada en riesgos en el año 2022 de acuerdo con la información de la Junta Bancaria del Ecuador, para poder comparar con lo evidenciado en el trabajo de campo de cada uno de los ATMs.

En cada sitio se tomó información de riesgo ciudadano de los sectores, usando la escala de Likert, inseguro, medianamente seguro y seguro para poder conocer el riesgo que implica realizar transacciones para los usuarios, actividades de carga de dinero por parte de la entidad y trabajos de mantenimientos por parte del personal técnico.

Los resultados de este instrumento permitieron realizar el levantamiento de información completa de toda la flota de ATMs en la ciudad de Esmeraldas con un total de 63 máquinas, incluyendo agencias de bancos, cooperativas de ahorro y sitios islas. Los cuales fueron segregados de la siguiente manera:

Figura 24. Ficha de observación



Elaborado por: El autor

Análisis e interpretación

Dentro del proceso de levantamiento de información, se pudo tomar datos importantes de todos los ATMs de la ciudad de Esmeraldas, enfatizando en su geolocalización, entidad financiera a quien pertenece, marcas, modelos, proveedores, para poder crear un mapa con su ubicación. Este mapa fue elaborado con la colaboración del departamento cartográfico SIG de la Universidad San Francisco de Quito y Universidad Luis Vargas Torres Esmeraldas, utilizando el software ArcGis Pro.

Tabla 10. Lista de ATMs de la ciudad de Esmeraldas

PUNTO	Y	X	ENTIDAD FINANCIERA	MODELO	AGENCIA	PROVEEDOR
1	0,96631	-79,6519	PICHINCHA	DN450	ESMERALDAS	DIEBOLD NIXDORF
2	0,96631	-79,6519	PICHINCHA	DN450	ESMERALDAS	DIEBOLD NIXDORF
3	0,96631	-79,6519	PICHINCHA	DN450	ESMERALDAS	DIEBOLD NIXDORF
4	0,96631	-79,6519	PICHINCHA	DN450	ESMERALDAS	DIEBOLD NIXDORF
5	0,96522	-79,65323	PICHINCHA	DN250	ISLA HOTEL PERLA VERDE	DIEBOLD NIXDORF
6	0,963583	-79,65284	PICHINCHA	DN450	ISLA OLMEDO ESMERALDAS	DIEBOLD NIXDORF
7	0,963583	-79,65284	PICHINCHA	DN450	ISLA OLMEDO ESMERALDAS	DIEBOLD NIXDORF
8	0,963583	-79,65284	PICHINCHA	DN450	ISLA OLMEDO ESMERALDAS	DIEBOLD NIXDORF

9	0,963583	-79,65284	PICHINCHA	DN450	ISLA OLMEDO ESMERALDAS	DIEBOLD NIXDORF
10	0,984507	-79,65415	PICHINCHA	DN450	ISLA PRIMAX MARGARITA	DIEBOLD NIXDORF
11	0,976517	-79,65331	PICHINCHA	DN200V	ISLA MULTIPLAZA	DIEBOLD NIXDORF
12	0,988789	-79656945	PICHINCHA	SS27	ISLA PARQUE LAS PALMAS	NCR
13	0,963423	-79,65396	PICHINCHA	SS26	ISLA PARQUE INFANTIL	NCR
14	0,963423	-79,65396	PICHINCHA	SS26	ISLA PARQUE INFANTIL	NCR
15	0,963423	-79,65396	PICHINCHA	SS26	ISLA PARQUE INFANTIL	NCR
16	0,918232	-79,6828	PICHINCHA	SS27	LA TOLITA	NCR
17	0,918232	-79,6828	PICHINCHA	SS27	LA TOLITA	NCR
18	0,918232	-79,6828	PICHINCHA	SS27	LA TOLITA	NCR
19	0,96966	-79,6517	PICHINCHA	SS27	ISLA AKI PLAZA CIVICA	NCR
20	0,96966	-79,6517	PICHINCHA	SS27	ISLA AKI PLAZA CIVICA	NCR
21	0,918232	-79,6828	PICHINCHA	GRGRECYCLER	LA TOLITA	GRG BANKING
22	0,918232	-79,6828	PICHINCHA	GRGRECYCLER	LA TOLITA	GRG BANKING
23	0,965583	-79,6522	GUAYAQUIL	720	ESMERALDAS	DIEBOLD NIXDORF
24	0,965328	-79,65157	GUAYAQUIL	720	CLARO CENTRO	DIEBOLD NIXDORF
25	0,965583	-79,6522	GUAYAQUIL	562	ESMERALDAS	DIEBOLD NIXDORF
26	0,965583	-79,6522	GUAYAQUIL	562	ESMERALDAS	DIEBOLD NIXDORF

27	0,965583	-79,6522	GUAYAQUIL	562	ESMERALDAS	DIEBOLD NIXDORF
28	0,976456	-79,6534	GUAYAQUIL	720	MULTIPLAZA	DIEBOLD NIXDORF
29	0,976456	-79,6534	GUAYAQUIL	562	MULTIPLAZA	DIEBOLD NIXDORF
30	0,976434	-79,65337	GUAYAQUIL	720	CLARO MULTIPLAZA	DIEBOLD NIXDORF
31	0,968012	-79,652341	GUAYAQUIL	SS27	ISLA TIA BOLIVAR	NCR
32	0,932461	-79,67219	GUAYAQUIL	SS27	ISLA TIA CODESA	NCR
33	0,933422	-79,6714	GUAYAQUIL	SS27	ISLA AKI PUERTO GREEN	NCR
34	0,976588	-79,65344	GUAYAQUIL	SS27	ISLA MULTIPLAZA	NCR
35	0,963575	-79,65113	PACIFICO	ILT9900	ESMERALDAS	DIEBOLD NIXDORF
36	0,930492	-79,67224	PACIFICO	3750	ISLA COMERCIAL HERRERA	DIEBOLD NIXDORF
37	0,983386	-79,64759	PACIFICO	3750	ISLA CAC PUERTO	DIEBOLD NIXDORF
38	0,976588	-79,65344	PACIFICO	3700	ISLA MULTIPLAZA	DIEBOLD NIXDORF
39	0,966297	-79,65324	PACIFICO	5550	ISLA SANTA MARIA	DIEBOLD NIXDORF
40	0,92308	-79,66977	PACIFICO	MX5700	ISLA GASOLINERA PRIMAX	HYOSUNG
41	0,963575	-79,65113	PACIFICO	MX8200	ESMERALDAS	HYOSUNG
42	0,963575	-79,65113	PACIFICO	MX8200	ESMERALDAS	HYOSUNG
43	0,963575	-79,65113	PACIFICO	MX8200	ESMERALDAS	HYOSUNG
44	0,967232	-79,65264	INTERNACIONAL	5550	ESMERALDAS	DIEBOLD NIXDORF

45	0,967232	-79,65264	INTERNACIONAL	5550	ESMERALDAS	DIEBOLD NIXDORF
46	0,923067	-79,66979	INTERNACIONAL	5500	ISLA GASOLINERA PRIMAX	DIEBOLD NIXDORF
47	0,933422	-79,6714	PRODUBANCO	DN200A	ISLA PUERTO GREEN	DIEBOLD NIXDORF
48	0,976588	-79,65344	PRODUBANCO	DN200A	ISLA MULTIPLAZA	DIEBOLD NIXDORF
49	0,963696	-79,65136	PRODUBANCO	DN450	ESMERALDAS	DIEBOLD NIXDORF
50	0,963696	-79,65136	PRODUBANCO	DN250	ESMERALDAS	DIEBOLD NIXDORF
51	0,965258	-79,6515	PRODUBANCO	DN250	SERVIPAGOS	DIEBOLD NIXDORF
52	0,966854	-79,65197	AUSTRO	562	ESMERALDAS	DIEBOLD NIXDORF
53	0,975123	-79,65426	CPN	562	ESMERALDAS	DIEBOLD NIXDORF
54	0,932516	-79,66167	CPN	562	ISLA COMANDO POLICIAL	DIEBOLD NIXDORF
55	0,963882	-79,65258	SOLIDARIO	SS26	ESMERALDAS	NCR
56	0,989865	-79,6598	COOP JEP	3750	ISLA LAS PALMAS	DIEBOLD NIXDORF
57	0,96163	-79,65254	COOP JEP	3750	ISLA PARQUE INFANTIL	DIEBOLD NIXDORF
58	0,976588	-79,65344	COOP JEP	522	ISLA MULTIPLAZA	DIEBOLD NIXDORF
59	0,963635	-79,6513	COOP29OCT	3700	ESMERALDAS	DIEBOLD NIXDORF

60	0,963687	-79,65117	COOP29OCT	GRGCASHDISP	ESMERALDAS	GRG BANKING
61	0,932461	-79,67219	BOLIVARIANO	SS26	ISLA TIA CODESA	NCR
62	0,963103	-79,65127	BGR	DN250A	ESMERALDAS	DIEBOLD NIXDORF
63	0,933743	-79,66154	BGR	DN250A	ISLA BIMOT	DIEBOLD NIXDORF

Elaborado por: El autor

Análisis e Interpretación

Para poder tener un criterio estructurado, se realizó una escala con indicadores de riesgo ciudadano e indicadores de salvaguardas adicionales, las cuales fueron determinadas por: S: Seguro, MS: Medianamente seguro, I: Inseguro.

Figura 25. Escala e indicadores de riesgo

ESCALAS		**RIESGO**		**DEGRADACIÓN**		
INDICADOR DE RIESGO CIUDADANO	**INDICADOR DE SALVAGUARDAS ADICIONALES**			**I**	**MS**	**S**
S: SEGURO	**S: SEGURO**	**VALOR**	**S**	**MS**	**S**	**S**
MS: MEDIANAMENTE SEGURO	**MS: MEDIANAMENTE SEGURO**		**MS**	**I**	**MS**	**S**
I: INSEGURO	**I: INSEGURO**		**I**	**I**	**I**	**MS**

Elaborado por: El autor

4.4. Indicadores de riesgo ciudadano

Dentro del levantamiento de información en campo, al realizar los recorridos por cada sector de la ciudad, para considerar este aspecto, se tomó información de zonas de alto índice delincuencial, determinado por el ministerio del interior del Ecuador y el ECU911.

4.5. Indicador de salvaguardas adicionales

Para considerar salvaguardas adicionales, se tomó la normativa interna de seguridad física y electrónica en procesos de implementación de ATMs, de la entidad financiera con mejor calificación en riesgo del 2022 de acuerdo con lo indicado por la superintendencia de bancos del Ecuador, con una calificación AAA/AAA-. Dicha entidad cuenta con 17 requisitos a comparación con lo indicado en la normativa vigente que son 10.

Tabla 11. Caracterización de seguridad para implementar ATM

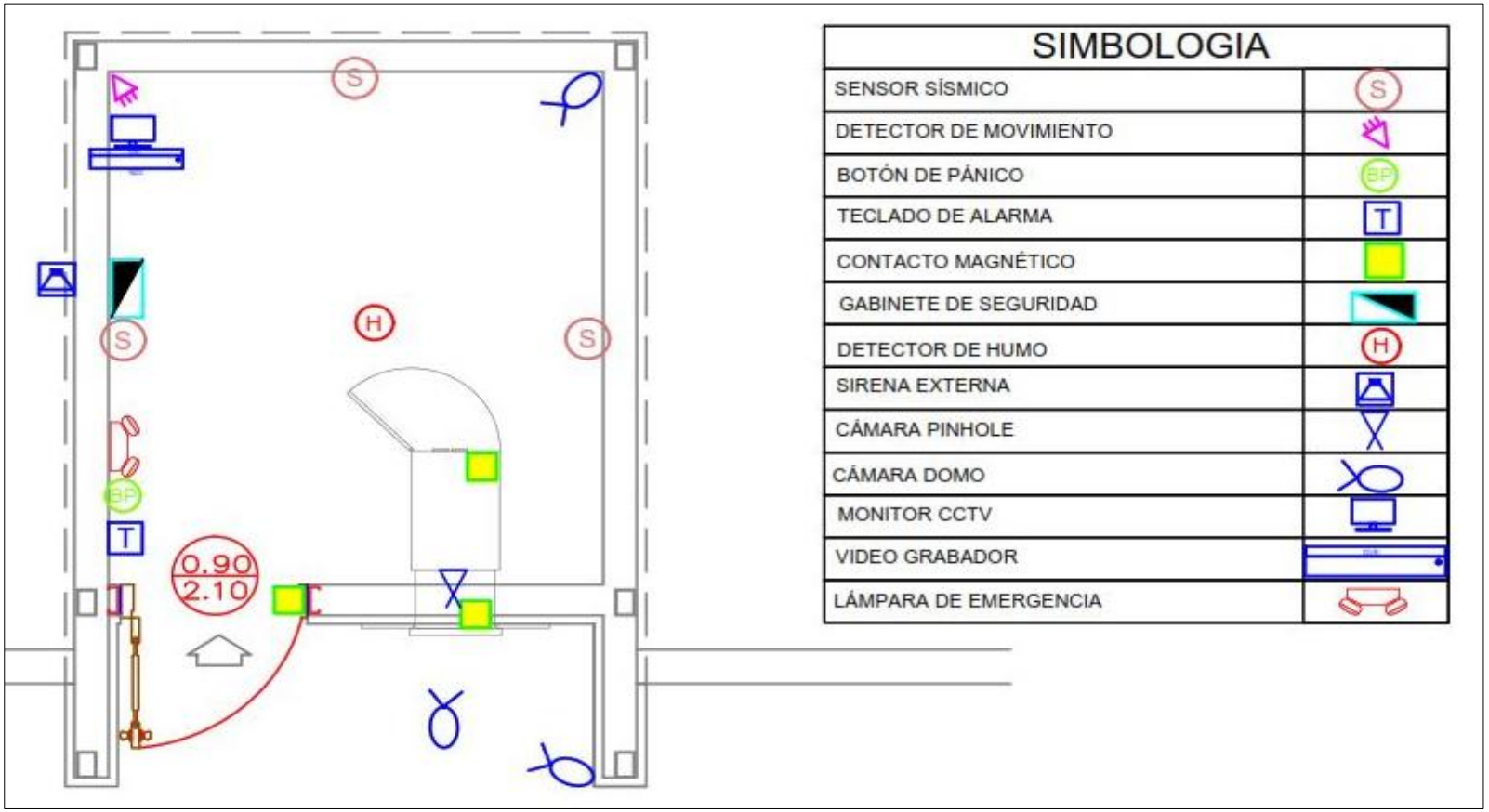
Requisitos para implementar ATMs	
• Ubicación y Entorno • Protección al teclado • Protección contra clonación de tarjetas • Iluminación • Programas de vigilancia en sitio • Mecanismo de anclaje • Mantenimiento preventivo y correctivo • Accesos físicos al interior de los ATMs • Sistema de entintado	• Cámaras de vigilancia • Sistema de grabación de video • Backup de iluminación de emergencia • Detector de movimiento • botón de pánico • Detector de humo • Sensor sísmico • Sirena externa

Elaborado por: El autor

4.6. Esquema de seguridad electrónica en ATMs

El presente esquema es elaborado tomando en caracterización de los requisitos de seguridad de la entidad financiera con mejor calificación el riesgo en el año 2022 de acuerdo con la superintendencia de bancos en el Ecuador y los que exige la normativa actual.

Figura 26. Esquema de seguridad física y electrónica en ATMs



Elaborado por: El autor

4.7. Comparativa de normativas de seguridad de ATMs en varios países

Figura 27. Comparativa de países vs los requisitos de la entidad mejor calificada en riesgo del Ecuador 2023

ENTIDAD FINANCIERA CON MEJOR CALIFICACIÓN DE RIESGO EN ECUADOR	ECUADOR	EL SALVADOR	BOLIVIA	COSTA RICA	PARAGUAY	COLOMBIA
NORMAS DE SEGURIDAD FISICA Y ELECTRONICA PARA IMPLEMENTAR ATMs						
Progreso:						
100%	65%	47%	53%	65%	76%	53%
Totales: 17	Totales: 17	Totales: 17	Totales: 17	Totales: 17	Totales: 17	Totales: 17
Completadas: 17	Completadas: 11	Completadas: 8	Completadas: 9	Completadas: 11	Completadas: 13	Completadas: 9
STATUS / Requisitos para implementar ATMs	STATUS	STATUS	STATUS	STATUS	STATUS	STATUS
✓ Ubicación y Entorno	✓	✓	✓	✓	✓	✓
✓ Proteccion al teclado	✓	!	!	!	✓	✓
✓ Proteccion contra clonación de tarjetas	✓	✓	✓	!	✓	✓
✓ Iluminacion	✓	!	✓	✓	✓	✓
✓ Programas de vigilancia en sitio	✓	✓	✓	✓	✓	✓
✓ Mecanismo de anclaje	✓	✓	✓	✓	✓	✓
✓ Mantenimiento preventivo y correctivo	✓	✓	✓	!	✓	!
✓ Accesos fisicos al interior de los ATMs	✓	!	✓	✓	✓	✓
✓ Camaras de vigilancia	✓	✓	✓	✓	✓	✓
✓ Sistema de grabacion de video	✓	✓	✓	✓	!	!
✓ Backup de iluminacion de emergencia	!	!	!	✓	!	!
✓ Detector de movimiento	!	!	!	✓	✓	✓
✓ Boton de panico	!	!	!	!	!	!
✓ Detector de humo	!	✓	!	!	✓	!
✓ Sensor sismico	!	!	!	✓	✓	!
✓ Sirena externa	!	!	!	!	!	!
✓ Sistema de entintado	✓	!	!	✓	✓	!

Elaborado por: El autor

Se realizó un estudio de diferentes normativas relacionadas a la seguridad en procesos de implementación de ATMs en varios países de Latinoamérica, utilizando como valor ponderado la entidad financiera con mejor calificación el riesgo en el año 2022 de acuerdo con la superintendencia de bancos del Ecuador, estos resultados son importantes porque muestran la situación actual de cada país y permitió realizar una comparativa y saber en qué posición se encuentra Ecuador.

Se tomó como referencia 6 países de Latinoamérica y se los comparo con la normativa de la entidad financiera con mejor calificación el riesgo en el año 2022 de acuerdo con la superintendencia de bancos del Ecuador.

Tabla 12. Cumplimento de la normativa de seguridad en ATMs por países

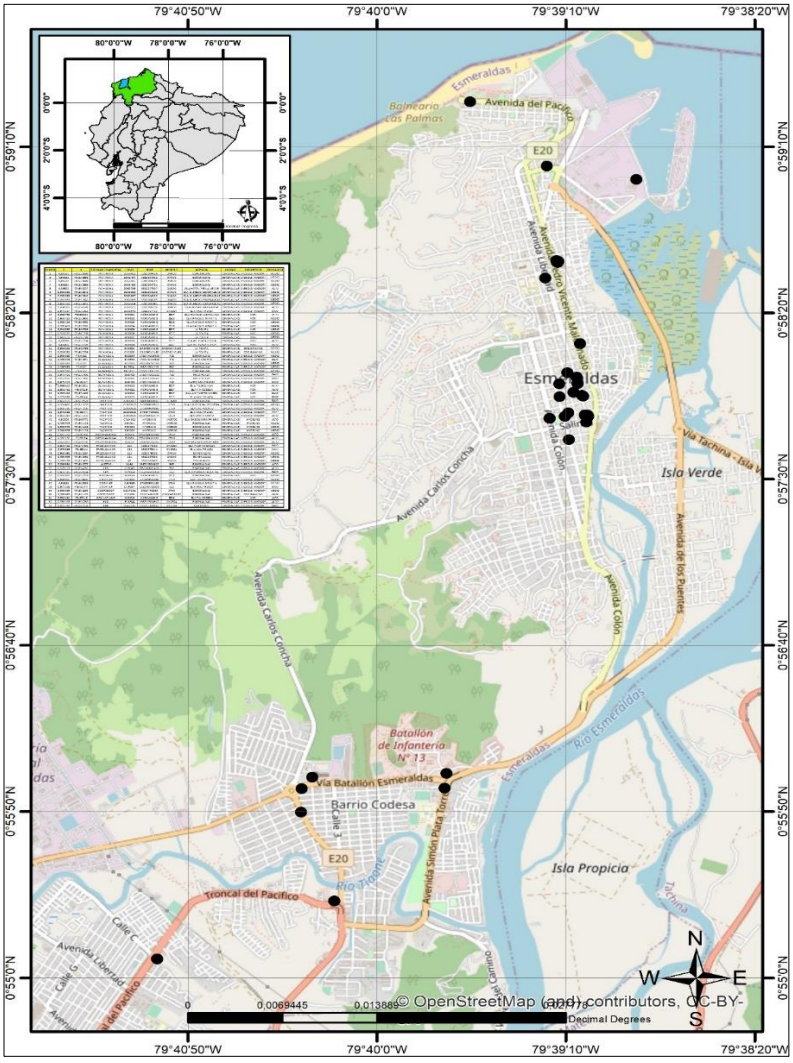
Cantidad	Referencia	Porcentaje
1	Entidad financiera con mejor calificación de riesgo del Ecuador 2022	100%
2	Paraguay	76%
3	Costa Rica	65%
4	Ecuador	65%
5	Colombia	53%
6	Bolivia	53%
7	El Salvador	47%

Elaborado por: El autor

Este resultado muestra que entre los países de Latinoamérica que se realizó la revisión de las normativas, Paraguay cuenta con mayor número de requisitos con un 76%, dando entender que es más exigente el ente regulador en dicho país a comparación de los otros países, el cual le permite tener una mejor seguridad, mientras que Ecuador y Costa Rica obtuvieron un 65%, indicando que cuentan con normativas similares.

Se muestra en la figura 49, la ubicación real y actualizada de los ATMs de la ciudad de Esmeraldas, como punto inicial de la toma de coordenadas en cada sitio para determinar su ubicación y conocer el entorno donde están ubicados, esta información es importante para poder considerar las zonas claves enmarcadas en la seguridad ciudadana y el riesgo que se puede tener al realizar transacciones como retiros, depósitos, transferencias y demás. Cabe indicar que las consideraciones también son importantes para el personal que realiza los mantenimientos o carga de efectivo por parte de las entidades financieras.

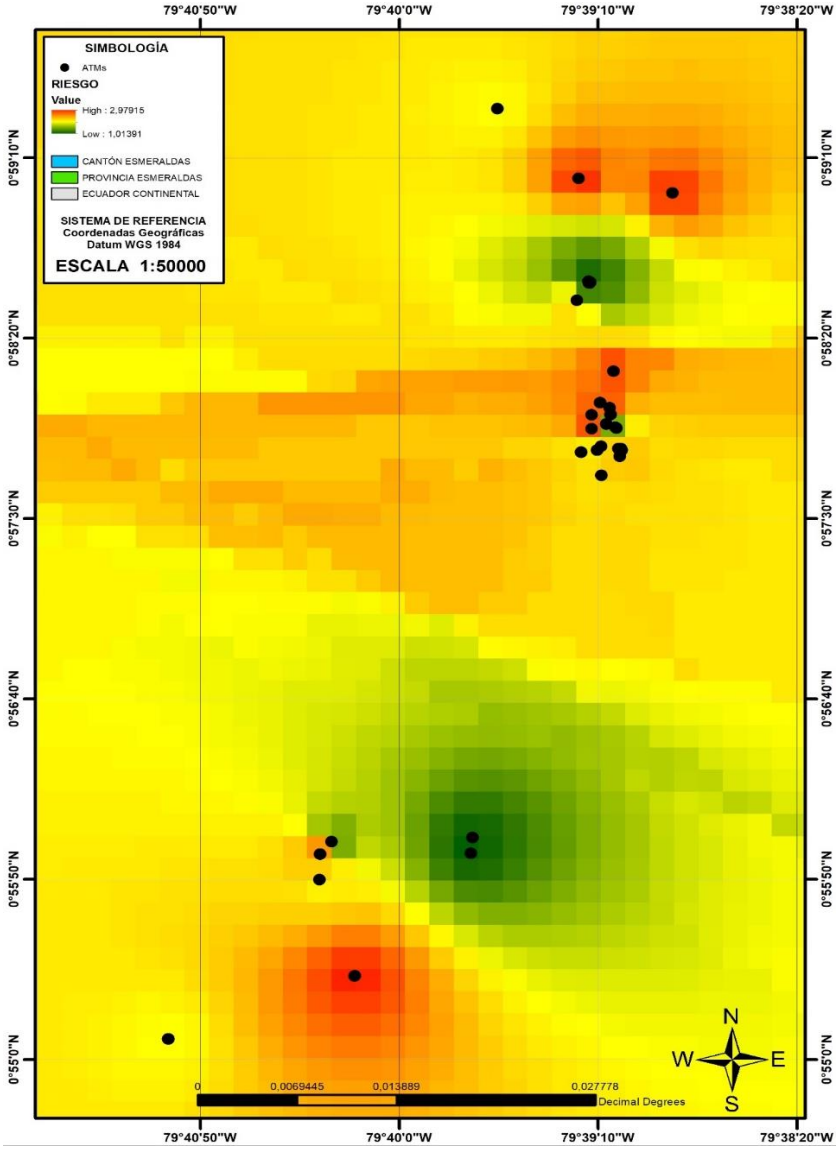
Figura 28. Mapa de geolocalización de 63 ATMs de la ciudad Esmeraldas



Elaborado por: El autor

Se muestra en la figura 50 los resultados obtenidos, utilizando indicadores de riesgo ciudadano con escala de Likert, donde el 22,2% son seguro, 49,22 medianamente seguro y 28,57% inseguro. Esta información del mapa de densidad es muy importante, puede ser utilizada tanto por las entidades financieras para aplicar salvaguardas y mitigar el riesgo, de la misma manera la policía nacional puede hacer uso de esta y aplicar correctivos necesarios en el bien de la comunidad.

Figura 29. Mapa de densidad de vulnerabilidades en los entornos de los ATMs



Elaborado por: El autor

4.8. Resultado de diagnóstico de vulnerabilidades en los entornos de los ATMs

Los resultados son contundentes dentro del instrumento de ficha de campo, la recolección de la información brindó resultados importantes para poder conocer la realidad e importancia de las zonas seguras e inseguras, tanto para los usuarios, personal de abastecimiento de la entidad financiera y personal técnico que realiza mantenimientos.

Tabla 13. Indicador de riesgo ciudadano en los entornos de los ATMs

Indicador	Porcentaje	Cantidad ATMs
Seguro	22,2	14
Medianamente seguro	49,22	31
Inseguro	28,57	18
Total	**100%**	**63**

Elaborado por: El autor

4.9. Indicador de salvaguardas adicionales

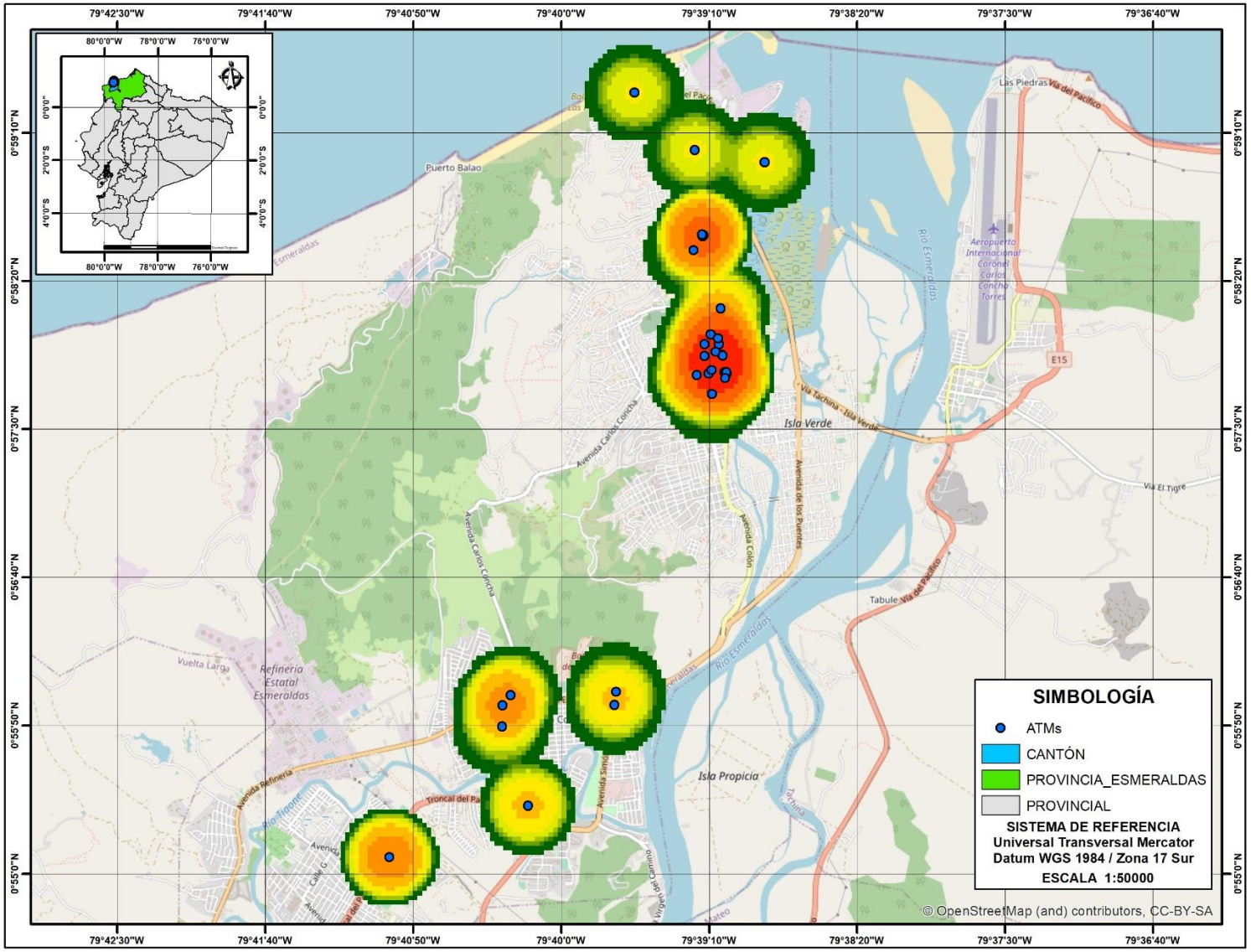
Para obtener estos resultados, se utilizó como base de evaluación los requisitos para implementar un ATM de acuerdo con lo establecido por la entidad financiera con mejor calificación en riesgo del 2022 en el Ecuador, el cual consta de 17 puntos de seguridad a comparación con la normativa de seguridad que establece la superintendencia de bancos en el cual son 10 puntos. Con los valores adicionales se crea una tabla con los 7 requisitos extras.

Tabla 14. Indicador de salvaguarda adicional

Indicador	Salvaguardas adicionales
Seguro	5 a 7
Medianamente seguro	3 a 4
Inseguro	1 a 2

Elaborado por: El autor

Figura 30. Densidad y riesgo de ATM ciudad Esmeraldas



Elaborado por: El autor

4.10. Resultado de indicador de salvaguardas adicionales

En los 63 ATMs donde se realizó el levantamiento de información, se tomó el nivel de seguridad de la entidad financiera con mejor calificación en riesgo del 2022 en el Ecuador, el cual consta de 17 puntos de seguridad y medirlo con la base de ATMs de la ciudad e Esmeraldas para mostrar los siguientes resultados:

Tabla 15. Resultados de indicador de salvaguarda adicional

Indicador	Porcentaje	Cantidad ATMs
Seguro	42,86%	27
Medianamente seguro	38,10%	24
Inseguro	19,05%	12
Total	**100%**	**63**

Elaborado por: El autor

4.11. Resultado de análisis de riesgo

Con los indicadores de riesgo ciudadano y el indicador de salvaguardas adicionales, se obtiene resultados importantes con información actualizada, usando la tabla de riesgo.

Tabla 16. Resultado de análisis de riesgo

Indicador	Porcentaje	Cantidad ATMs
Seguro	42,86%	27
Medianamente seguro	36,51%	23
Inseguro	20,63%	13
Total	**100%**	**63**

Elaborado por: El autor

Este resultado muestra que el 42,86% de los ATMs cumplen con niveles seguros, 36,51% medianamente seguros y 20,63% inseguros en el análisis de riesgo.

4.12. Discusión

De acuerdo con los resultados obtenidos en la investigación planteada, se asemeja con lo que Balaji & Poornima (2021) plantearon en su estudio, donde indica que es esencial crear soluciones de seguridad mediante la adopcion de un marco o normativas de seguridad, para que cualquier organización encuentre soluciones a la mayoria de vulnerabilidades y fallas, esto se debe a que las actualizaciones de las normativas de seguridad en el Ecuador deben ser acorde a los nuevas tecnologias, porque han sido evidenciados nuevo metodos de ataque fisicos, fraudes, amenazas y carencia de informacion en la normativa sobre tipos de cifrados.

Tener clara la caracterizacion de la seguridad fisica y eletronica, cuando se instala un ATM de una zona establecida, es importante, como lo señalan Milind (2016) y Ahmed (2020) concuerdan sus resultados, donde indican que los ataques son posibles a través de los puntos débiles de seguridad establecidos, es importante adoptar y caracterizar la seguridad de los ATMs, esto se debe a que al no tener la caracterización de una base de ATMs establecida en este caso en la ciudad de Esmeraldas, es más difícil proponer posibles temas de soluciones o salvaguardas en futuros procesos de instalación.

Los resultados obtenidos muestran un criterio importante sobre la realidad actual de la base de ATMs instalada en la ciudad de Esmeraldas, enmarcada en las vulnerabilidades del entorno de servicio, con la apreciación de Martinez Ralón (2021) y Tamas (2021) concuerdan sus resultados, que se debe realizar un diagnostico externo e interno de las vulnerabildades de la estructura del ATM y su entorno, para verificar dispositivos skimmers, individuos sospechosos y artefactos extraños, esto se debe que el diagnostico de las vulnerabilidades se debe hacer periodicamente con personal calificado, utilizando un marco de referencia, porque los requisitos

minimos que indica la normativa vigente no son suficiente para contrarrestar los ataques efectivizados.

De los resultados obtenidos en la investigación de normas, políticas, marcos y procedimientos de otros países, nos da una posición real a comparación de las normas de seguridad en implementación de ATMs de nuestro país. Estar en tercer lugar entre los 6 países de Latinoamérica investigados, con un 65% de cumplimiento y se discrepa con Kasanda & Phiri, (2019), donde indica que los propietarios de los ATMs debe asegurarse de emplear las normas requeridas para garantizar la disponibilidad y mitigar riesgo, los resultados dan un criterio de discrepar y orientar a que los requisitos de implementación sean obligatorios y en constante revisión por el máximo organismo de las entidades financieras, de esta manera reevaluar nuestras medidas de seguridad mínima, para implementar nuevos métodos adicionales porque no son suficientes para contrarrestar los novedosos ataques y métodos de fraudes evidenciados. Cabe indicar que, de acuerdo con el nivel de medición de seguridad física y electrónica, el 100% de los ATMs de la ciudad de Esmeraldas, cumplen con los requisitos mínimos, porque lo demanda el ente regulador para su instalación y funcionamiento, ya que deben pasar por ciertos criterios de auditoría interna y externa.

5. CONCLUSIONES

La presente investigación fue de gran importancia, gracias a la aplicación del modelo revisión de literatura y la extracción de información de campo, se logró definir la línea base y sustento para la evaluación de la aplicabilidad de la normativa de seguridad física y electrónica de los ATMs de la ciudad de Esmeraldas

Luego de haber realizado el análisis, se puede indicar que la caracterización de la seguridad en la flota de ATMs de Esmeraldas, el 100% cumple con los requisitos mínimos y está dentro de lo que indica la máxima autoridad de regulación de las entidades financieras, cabe indicar que, un 42,86% utilizan medidas de seguridad adicionales de manera interna, cada entidad tiene sus propias políticas y normas de seguridad, las cuales se aplican según la apreciación de cada entidad financiera.

El diagnóstico de la investigación sobre los entornos de servicios, nos indica que el alto índice delincuencial en el cual se encuentra la ciudad de Esmeraldas, con relación a los puntos donde se encuentran ubicados los ATMs, da como resultado que el 49,22% son medianamente seguro para la ciudadanía, el cual ha reducido su índice de transaccional.

La comparación de la normativa de Ecuador con otros de Latinoamérica nos da un claro panorama en el ámbito internacional en temas de seguridad, estando en 3er lugar en cumplimiento de requisitos para instalar un ATM, con lleva a realizar una revisión y posible actualización de la normativa vigente de nuestro país.

El 100% de los ATMs en el Ecuador cumple lo exigido por la normativa, pero al realizar una comparativa con la entidad financiera de mejor calificación en riesgo del 2022, nos arroja que sus requisitos se reducen a un 65%, esto conlleva a tener posibles brechas de seguridad.

6. RECOMENDACIONES

- Se recomienda a la Superintendencia de Bancos del Ecuador y la Superintendencia Económica Popular y Solidaria, realizar una revisión de la normativa de seguridad actual, en conjunto con el ministerio de telecomunicaciones y de la sociedad de la información, para poder hacer los ajustes a la normativa en el marco de los procedimientos no aplicados, como por ejemplo: la utilización de métodos criptográficos para la seguridad de la información y así mitigar temas de ataques, robos, fraudes y delitos asociados, creando medidas más sólidas y robustas por el bienestar de la ciudadanía.
- Se recomienda a las entidades financieras, con lo evidenciado in situ, quienes tengan ATMs con más de 10 años de funcionamiento, realizar procesos upgrade o reemplazar el equipo completo, con el fin de mejorar la tecnología de las maquinas.
- Es importante indicar, por el resultado del diagnóstico, reubicar los ATMs que presentan índices de alto riesgo ciudadano, considerar hacer inspecciones previas para identificar las zonas seguras donde se puedan reubicar.
- Tener en consideración, solicitar la cooperación internacional a entidades como: la asociación de la industria de cajeros automáticos (ATMIA), para poder estar actualizados en el marco de la seguridad, como lo hacen otros países de Latinoamérica y el mundo
- Se recomienda a la ciudadanía en general, realizar procesos transaccionales en horarios de afluencia publica, en sitios recomendados como seguros por la policía nacional, acatar las indicaciones de seguridad de su entidad financiera para proteger la integridad de su información y los fondos.

REFERENCIAS

(s.f.).

Agesic. (19 de agosto de 2021). *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.* Obtenido de https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad/marco-ciberseguridad

Ahmed, M. (2020). A Systematical Review Study to Investigate the Use of Biometric Security Techniques in Automatic Teller Machines: Insight from the Past 15 Years. *IEEE*, 202-229. Obtenido de https://ieeexplore.ieee.org/abstract/document/8965494

Asobanca. (14 de Enero de 2021). *Asociacion de Bancos del Ecuador*. Obtenido de https://asobanca.org.ec/wp-content/uploads/2021/07/BoletI%CC%81n-de-Servicios-Financieros-Ene-2021-FINAL_0.pdf

Baez Sánchez, J. (Diciembre de 2019). *Fraude electronico a un cajero automatico ATM.* Obtenido de http://prcrepository.org/xmlui/bitstream/handle/20.500.12475/1264/ANALISIS%20DE%20CASO%20%20United%20States%20v%20Chris%20Suhail%20Folad,%20%20Khaled%20Nabil%20Abdel%20Fattah.pdf?sequence=1

Balaji, S., & Poornima, B. (2021). Cyber Security for Atm Terminals. *Annals of the Romanian Society for Cell Biology*, 8785-8789. Obtenido de http://annalsofrscb.ro/index.php/journal/article/view/3599

Banco Central del Ecuador. (17 de Enero de 2022). *Banco Central del Ecuador*. Obtenido de https://www.bce.fin.ec/boletines-de-prensa-archivo/el-banco-central-emite-resolucion-sobre-billetes-entintados

Banred. (2023). *Banred Red interbancaria mas grande del Ecuador*. Obtenido de Banred Red interbancaria mas grande del Ecuador: https://www.banred.fin.ec/servicios/red-de-cajeros-automaticos

Calva Vega, Y. G. (2022). *Estudio de normativa infraccional en las contravenciones penales contra agentes del control del orden público en Ecuador* (14 ed.). Santo Domingo: Universidad Y Sociedad. Obtenido de https://rus.ucf.edu.cu/index.php/rus/article/view/3287

Cisneros Alvarado, R. (12 de Enero de 2022). *Plan De Gestión Del Proyecto De Gap Análisis Para La Implementación Del Nuevo Core Bancario De Cs Grupo Financiero.* Obtenido de UNIVERSIDAD PARA LA COOPERACIÓN INTERNACIONAL: https://www.ucipfg.com/biblioteca/files/original/033ddb575dc3c381957684bb58ec9514.pdf

Coba, G. (29 de Diciembre de 2022). *Primicias*. Obtenido de Asobanca: https://www.primicias.ec/noticias/economia/bancos-cooperativas-inseguridad-costos/

Código Orgánico Integral Penal. (10 de Febrero de 2014). *Código Orgánico Integral Penal.* Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Constitución de la Republica del Ecuador. (20 de Octubre de 2008). *Ministerio de Defensa del Ecuador.* Obtenido de https://www.defensa.gob.ec/wp-

content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Creswell, J. (2017). *Research design Qualitative quantitative and mixed methods approaches.* Los Angeles: SAGE Publications. Obtenido de https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf

Defensoria del Pueblo Ecuador. (29 de Noviembre de 2021). *Asesorias 2021*. Obtenido de https://www.dpe.gob.ec/rc2021/1_Atencion/Asesorias%202021.pdf

EAST. (10 de Octubre de 2019). *ATM Physical Attacks in Europe on the increase.* Obtenido de https://www.association-secure-transactions.eu/atm-physical-attacks-in-europe-on-the-increase/

Efendi, F. (2019). Implementación de criptografía profunda en sistemas de seguridad de ATM. *Journal Informatic Upgris*, 2460-4801.

Finkle, J. (22 de Noviembre de 2016). *Hackers remotely steal ATM cash in latest twist on cyber bank.* Obtenido de https://www.insurancejournal.com/news/international/2016/11/22/433017.htm

Fiscalia General del Estado. (01 de Diciembre de 2022). *Fiscalia General del Estado Ecuador.* (D. d. Social, Ed.) Obtenido de https://www.fiscalia.gob.ec/fiscalia-procesa-a-presunta-organizacion-criminal-que-delinquia-en-cajeros-automaticos/

Garcia, N. (30 de junio de 2018). *Revista Española de Documentación Científica.* Obtenido de https://redc.revistas.csic.es/index.php/redc/issue/view/102

Hernandez, R., Fernandez, C., & Baptista, P. (01 de abril de 2014). *Metodología de la Investigación.* Obtenido de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Huerta Ibarra, I. (2019). Enseñanza de la informática biomédica en las escuelas de medicina de Mexico. *Instituto Politécnico Nacional, Coordinación Editorial*, 15-33. Obtenido de https://www.redalyc.org/journal/1794/179462793002/179462793002.pdf

Kasanda, E., & Phiri, J. (2019). ATM Security: A case study of Emerging Threats. *International Journal of Advanced Studies in Computer Science and Engineering*.

Ley Orgánica de protección de datos personales. (26 de mayo de 2021). *Ministerio de Telecomunicaciones.* Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Ley Orgánica de Telecomunicaciones. (s.f.). *Ministerio de Telecomunicaciones y de la sociedad de la información.* Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Lincoln, Y., & Denzin, N. (2012). *Manual de investigación cualitativa.* Obtenido de https://dialnet.unirioja.es/servlet/libro?codigo=490631

Martinez Ralón, M. (2021). Robo de identidad y clonación de tarjetas de crédito y débito utilizando cajeros automáticos alterados. *Revista Científca Diálogo Forense*, 1-9.

Medina Pesantez, E. (2016). *Repositorio integrado a la Red de Repositorios de Acceso Abierto del Ecuador.* Obtenido de Propuesta de un modelo de confiabilidad para cajeros

automáticos de marca Diebold de la serie 510, 512, 520, 522, 560, 562 ubicados en el Azuay: https://dspace.uazuay.edu.ec/handle/datos/6488

Milind, N. (Marzo de 2016). A Review Paper on Improving Security of ATM System. *International Journal on Recent and Innovation Trends in Computing and Communication*, 33-36. doi:https://doi.org/10.17762/ijritcc.v4i3.1828

Mintel. (3 de Agosto de 2022). *Estrategia nacional de ciberseguridad.* Obtenido de https://www.gobiernoelectronico.gob.ec/estrategia-nacional-de-ciberseguridad-del-ecuador/

Nurlaela, E. (2019). DESIGN AND IMPLEMENTATION SECURITY SYSTEM OF AUTOMATED MACHINE TELLER (ATM) USING ONE-TIME PASSWORD (OTP) BASED. *e-Proceeding of Engineering*, 3684.

Ordoñez, E. M. (2020). El sistema financiero en Ecuador. Herramientas innovadoras y nuevos modelos de negocio. *Revista Arbitrada Interdisciplinaria Koinonía*, 195-225. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7439111

Organization of American States. (17 de Enero de 2018). *State of Cybersecurity in the Banking Sector in Latin America and the Caribbean.* Obtenido de https://www.oas.org/es/sms/cicte/sectorbancarioeng.pdf

PCI-SSC. (2013). *PCI Standard Security Council.* Obtenido de https://docs-prv.pcisecuritystandards.org/Guidance%20Document/ATM/PCI_ATM_Security_Guidelines_Info_Supplement.pdf

Sabani, A., & Rishan, M. (28 de Noviembre de 2019). Effectiveness of ATM security mechanisms: a review analysis. *South Eastern University of Sri Lanka, University Park, Oluvil, Sri Lanka*, 234-243. Obtenido de http://ir.lib.seu.ac.lk/handle/123456789/3927

Sandoval Sucre, F. J. (2017). Gestion de proceso de negocio. *Research Gate*, 39-42. doi:10.13140/RG.2.2.16367.43682

Secretaria Nacional de Planificacion. (24 de 05 de 2021). *Plan de Creacion de Oportunidades 2021-2025.* Obtenido de https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf

See Zingbo. (01 de Febrero de 2018). *Meet Piolin, the first ATM Malware Jackpotting ATMs in US.* Obtenido de https://vdocuments.mx/meet-piolin-the-first-atm-malware-jackpotting-atms-in-us-piolin-the-first.html?page=1

Seps. (01 de AGOSTO de 2021). *INFORME ENCUESTA ESTADO Y REALIDAD DE LOS SERVICIOS DIGITALES Y SEGURIDAD DE LA INFORMACIÓN EN EL SFPS 2021*. Obtenido de https://www.seps.gob.ec/wp-content/uploads/Estudio_SEPS_ITAhora.pdf

Shun-Yung, K., & Ming-Li, H. (2021). *Digital Robbery ATM Hacking and Implications.* Stuttgart, Baden-Württemberg, Germany: Springer. Obtenido de https://link.springer.com/book/10.1007/978-3-030-70706-4

Singh, D. (Septiembre de 2019). Design and implementation of a secure ATM system using machine learning and crypto-stego methodology. *SN Applied Sciences* , 0. doi:https://doi.org/10.1007/s42452-019-0988-0

Superintendencia de Bancos Ecuador. (13 de Agosto de 2019). Obtenido de https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2022/02/L1_IX_cap_V.pdf

Superintendencia de Bancos Ecuador. (13 de Agosto de 2019). Obtenido de https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2022/02/L1_IX_cap_V.pdf

Superintendencia de Economía Popular y Solidaria. (2022). *Superintendencia de Economía Popular y Solidaria (SEPS)*. Obtenido de Superintendencia de Economía Popular y Solidaria (SEPS): https://www.seps.gob.ec/institucion/que-es-la-seps/

Tamas, B. (11 de 10 de 2021). ATM Security Overview. *Hungarian Technical Scientific Society of Transilvania*, 11. Obtenido de https://ojs.emt.ro/enelko-szamokt/article/view/630

Vikas, T., & Mittal, A. (2016). *Real time security framework for detecting abnormal events.* Berlin: Springer. doi:10.1007/s11554-016-0573-3

ANEXOS

Anexo 1. Autorización del gerente de servicio de la empresa Diebold Nixdorf Ecuador, para realizar proyecto de investigación, utilizando la base de ATMs instalados por su empresa en la ciudad de Esmeraldas y realizar recolección de información, entrevista y encuesta a sus empleados.

DieboldNixdorf

Guayaquil, 02 de Julio de 2023

Dra. Lucía Yépez
DECANA FACULTAD DE POSGRADO UTN

Me permito informar a usted que el señor Lenin Vicente Quispe Mera, con número de cédula 080295168-1 estudiante del Programa de Maestría en Computación con Mención en Seguridad Informática, ha sido aceptado en la empresa Diebold Ecuador S.A para realizar su trabajo de titulación. La Institución brindará las facilidades e información necesarias para el desarrollo de la investigación.

Agradezco su atención.

Atentamente,

Rafael Karim Jimenez Herrera
Gerente de Servicios

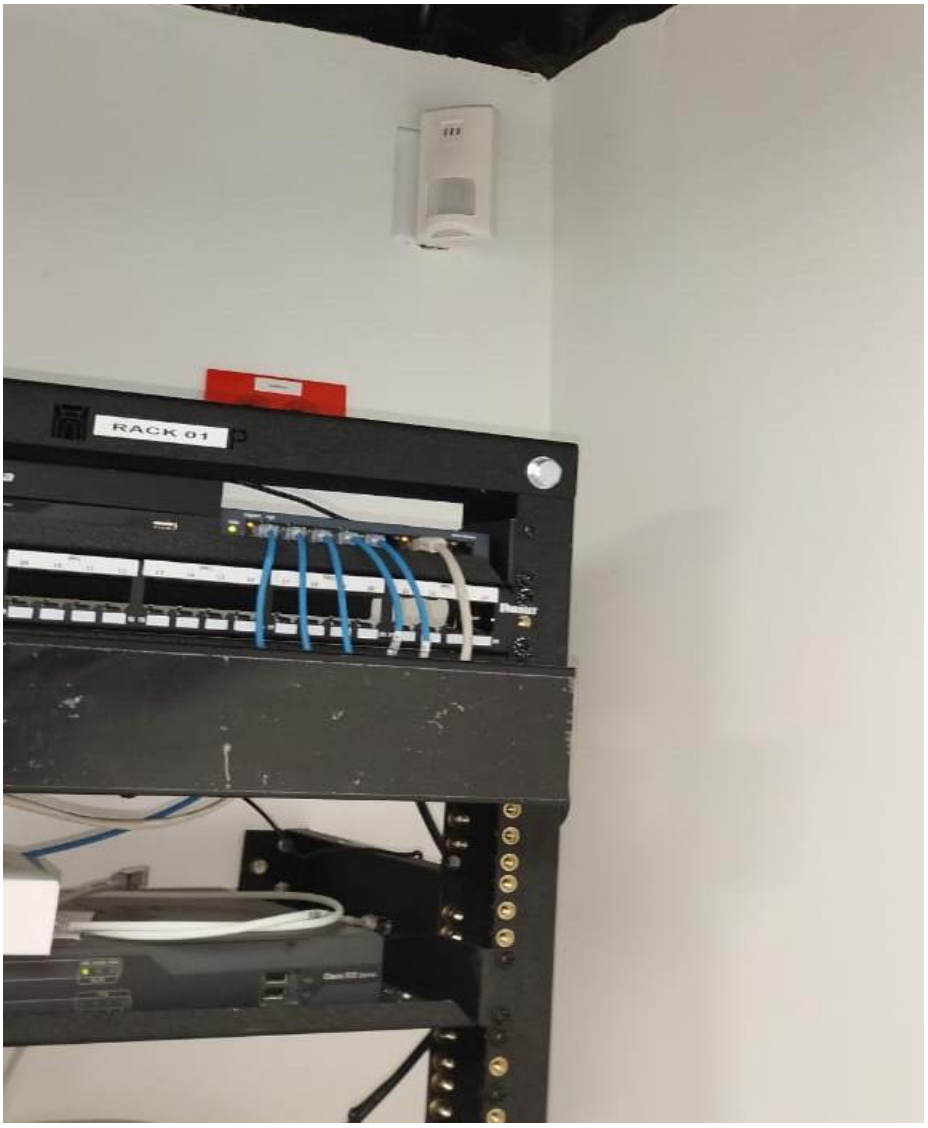
DieboldNixdorf

Diebold Nixdorf
Guayaquil: Km 1 ½ Vía a Samborondón
Edificio Los Arcos Plaza 2 Piso 4 Oficina 409 **Teléfono:** +593 4 6008 838
Quito: Av. República del Salvador N35-146
y Suecia, Edificio Prisma Norte Piso 7 **Teléfono:** +593 2 3822 300

DieboldNixdorf.com

Anexo 2. Reunión con la jefa de la agencia de la Cooperativa de la Policía Nacional Ag. Esmeraldas. Ing. Nidia Falcones, recopilación de información sobre la base de ATMs, componentes, partes, modelos, ubicación y tecnología.

Anexo 3. Evidencia de puntos de seguridad electrónica implementado en las entidades financieras, utilizado para crear esquema de seguridad utilizado como base en el desarrollo de la investigación: sirena, sensores de movimientos, sensores sísmicos, teclado, consola de seguridad, rack de equipos.


RACK 01


RACK 01

Anexo 4. Partes de ATMs evidenciados en la investigación.

Anexo 5. Encuestas y entrevistas validadas por expertos de la universidad Técnica del Norte, Ibarra

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

CUESTIONARIO DIRIGIDO A PROFESIONALES CON EXPERIENCIA EN PROCESOS DE IMPLEMENTACION Y ADMINISTRACION DE RED CAJEROS AUTOMATICOS A NIVEL NACIONAL

Estimado profesional, muchas gracias por formar parte del equipo de juicio de expertos del siguiente instrumento de investigación. Esta herramienta será utilizada dentro de la fase exploratoria de indagación con el fin de obtener variables cualitativas y cuantitativas para correlacionar con los resultados futuros asociados a la seguridad física y electrónica en los procesos de implementación de cajeros automáticos, basados en la aplicabilidad de la normativa vigente en el Ecuador.

Lineamientos Generales: El presente cuestionario hace parte de la tesis de maestría titulada: **"Evaluación de la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos en la ciudad de Esmeraldas, Ecuador"**, el mismo permite indagar en la base de cajeros ya existente y poder tener resultados actualizados con énfasis en la seguridad.

Este cuestionario, será manejado con total criterio de responsabilidad y confiabilidad de la información provista. El propósito es recolectar información relevante sobre el tema de investigación. El cuestionario está conformado por 15 preguntas que pretenden recoger información fidedigna del objeto de estudio.

Estimado validador a continuación se presenta el sistema de objetivos de la investigación con la finalidad de proporcionar información para la evaluación de la pertinencia y coherencia del presente instrumento.

Objetivo General

Evaluar de la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos en la ciudad de Esmeraldas, Ecuador.

Objetivos Específicos

Objetivo 1.- Caracterizar la seguridad física y electrónica de los cajeros automáticos en los procesos de instalaciones y producción.

Objetivo 2.- Diagnosticar las vulnerabilidades en los entornos de servicios de los cajeros automáticos de las entidades financieras.

Objetivo 3.- Realizar un análisis comparativo de la norma nacional e internacional de seguridad física y electrónica en los procesos de implementación de los cajeros automáticos.

Objetivo 3.- Medir el nivel de seguridad física y electrónica de los cajeros automáticos, de acuerdo con la normativa ecuatoriana.

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

CUESTIONARIO DIRIGIDO A PROFESIONALES CON EXPERIENCIA EN PROCESOS DE IMPLEMENTACION Y ADMINISTRACION DE RED CAJEROS AUTOMATICOS A NIVEL NACIONAL

Consentimiento Informado

¿Está usted de acuerdo en proporcionar información con fines investigativos para obtener datos reales sobre el tema a investigar?

Si	
No	

Años de experiencia en campo: de 1 a 2 años ( ) de 3 a 5 años ( ) de 5 a 10 años ( ) más de 10 años ( )

Fecha: dd/mm/aaa

PREGUNTAS	OPCIONES DE RESPUESTA
Consentimiento Informado ¿Acepta participar en la investigación descrita de forma libre y voluntaria?	SI ( ) NO ( )
Datos Informativos Sexo	Hombre ( ) Mujer ( )
Estado Civil	Soltero – Casado – Divorciado – Unión Libre - Viudo
Edad	Hasta 21 años Entre 22 y 25 años Entre 26 y 35 años Entre 36 y 45 años Entre 46 y 55 años Mayor de 55 años
Nacionalidad	Ecuatoriano – Colombiano – Venezolano – Otros ().
Etnia	Mestizo – Indígena – Afrodescendiente - Blanco
Nivel educativo más alto alcanzado	Educación básica - Bachillerato – Tercer nivel – Maestría – Doctorado (PhD)
1.- En los distintos entornos de producción de ATMs en el cual ha ingresado ¿Cree usted que los niveles de seguridad física y electrónica son iguales en todas las entidades financieras?	Nunca – Casi nunca – A veces – Casi siempre - Siempre

2.- La superintendencia de Bancos es el organismo que se encarga de supervisar y controlar el sistema financiero del Ecuador ¿Usted conoce y aplica los requisitos de seguridad física y electrónica que exige esta entidad para la habilitación de un ATM?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
3.- La superintendencia económica popular y solidaria es el organismo que se encarga de supervisar y controlar a las cooperativas de ahorro y crédito del Ecuador ¿Usted conoce y aplica los requisitos de seguridad física y electrónica que exige esta entidad para la habilitación de un ATM?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
4.- En las seguridades criptográficas que utiliza los ATMs para proteger la información de las transacciones ¿Cree usted que los nuevos procesos RKL son más seguros que la generación de las DESKEYS para ingresos manuales?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
5.- En los nuevos mecanismos de seguridad, que se utilizan para mitigar ataques físicos de los ATMs ¿Cree usted que el mecanismo de entintado de billete reduce los vandalismos y ataque físicos?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
6.- De acuerdo con su experiencia en campo ¿Cree usted que la seguridad física y electrónica de los ATMs isla es igual a los que se encuentran en las agencias?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
7.- En todas las revisiones técnicas de ATMs islas en el cual usted ha trabajado, además del personal de seguridad asignado por el banco ¿Ha recibido resguardo de la policía nacional?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
8.- Sobre la nueva implementación de chalecos blindados de seguridad para ATMs islas en ciertas entidades financieras ¿Cree usted que esta implementación mitiga los posibles vandalismos y robos?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
9.- Sobre los nuevos métodos de seguridad para mitigar robos y vandalismos, entre ellos el sistema de seguridad antirrobo cortina de humo ¿Cree usted que este método mitigaría los vandalismos y robos en los ATMs?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
10.- En la empresa que usted trabaja como profesional de ATMs ¿Ha recibido capacitaciones sobre la normativa que exige la Superintendencia de Bancos en procesos de implementación de ATMs?	Nunca – Casi nunca – A veces – Casi siempre - Siempre

11.- En los procesos de mantenimientos o trabajos realizados en ATMs islas de cualquier entidad financiera ¿Su integridad es resguardada en todo momento del personal de seguridad?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
12.- Sobre nuevas tecnologías de seguridad física y electrónica en el mercado ¿Cree usted que las entidades financieras del Ecuador realizan las actualizaciones adecuadas para proteger sus ATMs?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
13.- Sobre las medidas de seguridad física y electrónicas implementadas en los sites de los ATMs, de acuerdo con la normativa vigente ¿Cree usted que dichas medidas son suficientes para proteger los activos de ataques físicos y electrónicos?	Nunca – Casi nunca – A veces – Casi siempre - Siempre
14.- Sobre los 2 tipos de ATMS (cash dispenser y recycler) ¿Cuál cree usted que mejoraría los temas de disponibilidad del servicio?	CASH DISPENSER ( ) RECYCLER ( )
15.- Sobre la protección de clonación de tarjetas o dispositivos antiskiming ¿Cree usted que los ATMs en los cuales ha trabajado, cuentan con este dispositivo?	Nunca – Casi nunca – A veces – Casi siempre - Siempre

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

INSTRUMENTO DE VALIDACIÓN

Instrucciones: En el siguiente formato, indique según la escala excelente (E), bueno (B) o mejorable (M) en cada ítem, de acuerdo con los criterios de validación (coherencia, pertinencia, redacción), si es necesario agregue las observaciones que considere. Al final se deja un espacio para agregar observaciones generales.

Ítem Nro.	Validación			Observación
	Coherencia	Pertinencia	Redacción	
1	E	E	E	Cómo sugerencia, en algún apartado del documento poner que significa las siglas ATM.
2	E	E	E	
3	E	E	E	
4	E	E	E	
5	E	E	E	
6	E	E	E	
7	E	E	E	
8	E	E	E	
9	E	E	E	
10	E	E	E	
11	E	E	E	
12	E	E	E	
13	E	E	E	
14	E	E	E	
15	E	E	E	

Observaciones generales

Datos del Validador
Cathy Guevara, PhD.

1002334835 CATHY PAMELA GUEVARA VEGA

Firmado digitalmente por 1002334835 CATHY PAMELA GUEVARA VEGA
Fecha: 2023.10.20 13:08:51 -05'00'

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

ENTREVISTA ESTRUCTURADA DIRIGIDA A PROFESIONALES EN PROCESOS DE IMPLEMENTACIÓN O ADMINISTRACION DE RED DE CAJEROS AUTOMATICOS A NIVEL NACIONAL

Lineamientos Generales: La presente entrevista hace parte de la tesis de maestría titulada: **"Evaluación de la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos en la ciudad de Esmeraldas, Ecuador"**, el mismo permite indagar en la base de cajeros ya existente y poder tener resultados actualizados con énfasis en la seguridad.

Esta entrevista, será manejada con total criterio de responsabilidad y confiabilidad de la información provista. El propósito es recolectar información relevante sobre el tema de investigación. La entrevista está conformada por 13 preguntas que pretenden recoger información fidedigna del objeto de estudio.

Estimado validador a continuación se presenta el sistema de objetivos de la investigación con la finalidad de proporcionar información para la evaluación de la pertinencia y coherencia del presente instrumento.

Objetivo General

Evaluar de la aplicabilidad de la normativa de seguridad física y electrónica en los procesos de implementación de cajeros automáticos en la ciudad de Esmeraldas, Ecuador.

Objetivos Específicos

Objetivo 1.- Caracterizar la seguridad física y electrónica de los cajeros automáticos en los procesos de instalaciones y producción.

Objetivo 2.- Diagnosticar las vulnerabilidades en los entornos de servicios de los cajeros automáticos de las entidades financieras.

Objetivo 3.- Realizar un análisis comparativo de la norma nacional e internacional de seguridad física y electrónica en los procesos de implementación de los cajeros automáticos.

Objetivo 3.- Medir el nivel de seguridad física y electrónica de los cajeros automáticos, de acuerdo con la normativa ecuatoriana.

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

ENTREVISTA ESTRUCTURADA DIRIGIDA A PROFESIONALES EN PROCESOS DE IMPLEMENTACIÓN O ADMINISTRACION DE RED DE CAJEROS AUTOMATICOS A NIVEL NACIONAL

Consentimiento Informado

¿Está usted de acuerdo en proporcionar información con fines investigativos para obtener datos reales sobre el tema a investigar?

Si	
No	

Fecha: dd/mm/aaa

Nacionalidad: Ecuatoriano – Colombiano – Venezolano – Otro ()
Etnia: Mestizo – Indígena – Afrodescendiente - Blanco
Nivel educativo más alto alcanzado: Educación básica - Bachillerato – Tercer nivel – Maestría – Doctorado (PhD)

PREGUNTAS GENERADORAS	RESPUESTAS
1. ¿Cuál es su cargo actual en la institución o empresa que trabaja?	
2. Realice una breve explicación de las funciones y responsabilidades a su cargo	
3. ¿Conoce de la normativa vigente en procesos de implementación de ATMs en el Ecuador?	
4. Sobre las medidas de seguridad fisica y electrónica que actualmente están implementadas en su empresa o institución ¿Tienen implementado el sistema de entintado de billetes?	
5. Para instalar un ATM en un sitio remoto o punto isla ¿Qué tipo de estudio o investigación realizan y que criterios toman en consideración?	
6. ¿Cada cuánto tiempo realizan procesos de mejoras tecnológicas o upgrade en los ATMs?	
7. ¿Considera usted que la instalación de chalecos blindados a las bóvedas mejora la seguridad fisica del ATM?	

8. De acuerdo con su criterio profesional ¿Cuál cree usted que sea más propenso a temas de ataques, un ATM isla o un ATM de agencia?	
9. Sobre los métodos de ataques físicos en los ATMs evidenciados en el Ecuador, los cuales han sido realizados en su mayoría por extranjeros de acuerdo con información de la fiscalía general del Estado ¿Cree usted que nuestros sistemas de seguridad son más vulnerables a comparación de otros países?	
10. Adicional se abrirá un espacio de retroalimentación donde se abordará temas acerca de: • Ciberseguridad en entidades financieras • Protocolos de respuestas a incidentes • Nuevos mecanismos de defensas en procesos de implementación de ATMs • Mapas de riesgos ciudadano • Seguridad transaccional • Retos y desafíos de la ciberseguridad en el área financiera en el Ecuador	

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

FACULTAD DE POSGRADO

INSTRUMENTO DE VALIDACIÓN

Instrucciones: En el siguiente formato, indique según la escala excelente (E), bueno (B) o mejorable (M) en cada ítem, de acuerdo con los criterios de validación (coherencia, pertinencia, redacción), si es necesario agregue las observaciones que considere. Al final se deja un espacio para agregar observaciones generales.

Ítem Nro.	Validación			Observación
	Coherencia	Pertinencia	Redacción	
1	E	E	E	
2	E	E	E	
3	E	E	E	
4	E	E	E	
5	E	E	E	
6	E	E	E	
7	E	E	E	
8	E	E	E	
9	E	E	E	
10	E	E	B	Podría mejorar la redacción siendo más específicos en los ítems 2 y 5.

Observaciones generales

Datos del Validador
Cathy Guevara, PhD.

1002534835 CATHY PAMELA GUEVARA VEGA

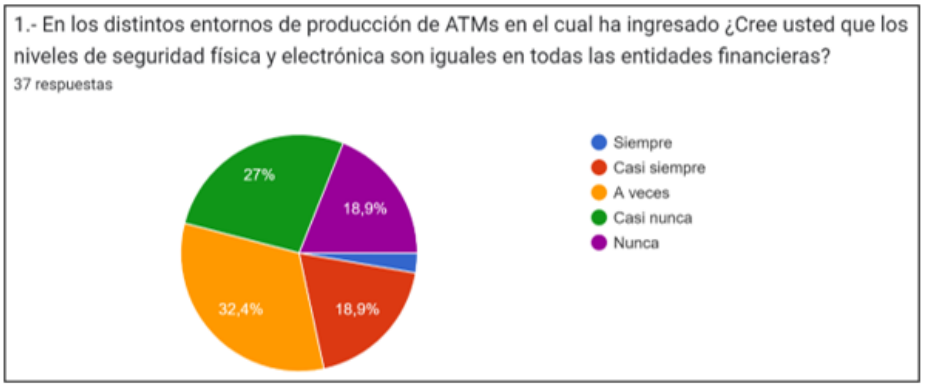
Firma

Tabla 14. Pregunta 1

Pregunta 1	Frecuencia	Porcentaje
Siempre	1	2,7%
Casi siempre	7	18,9%
A veces	12	32,4%
Casi nunca	10	27,0%
Nunca	7	18,9%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 1



Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

En el resultado de la investigación en esta pregunta indican: El 51,3% de los profesionales coinciden, como valor predominante tenemos siempre y casi siempre, se puede interpretar que los distintos entornos sea cooperativas o bancos, cumplen los requisitos de seguridad de acuerdo a la persepcion de los profesionales que realizan los servicios tecnologicos, administración de red ATMs y procesos de mantenimientos correctivos y preventivos.

Tabla 15. Pregunta 2

Pregunta 2	Frecuencia	Porcentaje
Siempre	11	29,7%
Casi siempre	16	43,2%
A veces	8	21,6%
Casi nunca	1	2,7%
Nunca	1	2,7%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 2

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

En el resultado de la investigación en esta pregunta indican: El 72,9% de los profesionales coinciden, como valor predominante tenemos siempre y casi siempre, podemos interpretar sobre los resultados obtenidos que los profesionales son capacitados en temas de seguridad en proceso de implementacion y tienen un criterio contundente al realizar un diagnosticos, proyectos o auditoria en las entidades bancarias.

Tabla 16. Pregunta 3

Pregunta 3	Frecuencia	Porcentaje
Siempre	10	27%
Casi siempre	15	40,5%
A veces	5	13,5%
Casi nunca	5	13,5%
Nunca	2	5,4%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 3

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

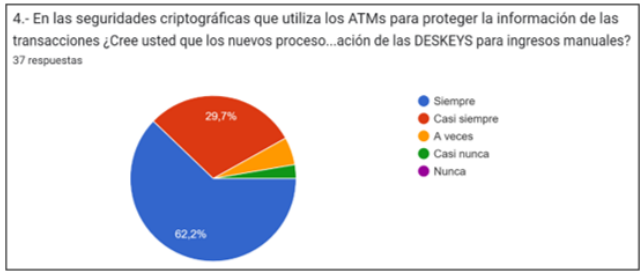
En el resultado de la investigación en esta pregunta indican: El 67,5% de los profesionales coinciden, como valor predominante tenemos siempre y casi siempre, podemos interpretar sobre los resultados obtenidos que los profesionales son capacitados en temas de seguridad en proceso de implementacion y tienen un criterio contundente al realizar un diagnosticos, proyectos o auditoria las cooperativas de ahorro y credito .

Tabla 17. Pregunta 4

Pregunta 4	Frecuencia	Porcentaje
Siempre	23	62,2%
Casi siempre	11	29,7%
A veces	2	5,4%
Casi nunca	1	2,7%
Nunca	0	0%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 4



Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

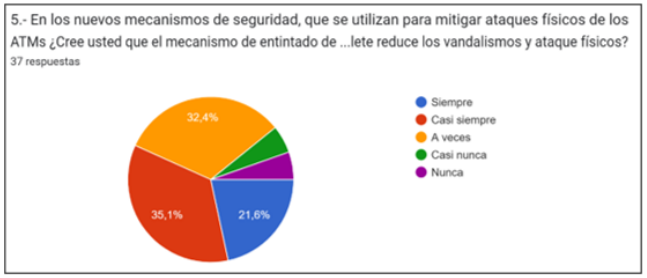
En el resultado de la investigación en esta pregunta indican: El 91,9% de los profesionales coinciden, como valor predominante tenemos siempre y casi siempre, podemos interpretar sobre los resultados obtenidos que los profesionales concuerdan sobre la seguridad criptografica para proteger la informacion de las transacciones se inclinan por las Remote Key Loading (RKL), mejora los niveles de confidencialidad y se expone menos.

Tabla 18. Pregunta 5

Pregunta 5	Frecuencia	Porcentaje
Siempre	8	21,6%
Casi siempre	13	35,1%
A veces	12	32,4%
Casi nunca	2	5,4%
Nunca	2	5,4%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 5



Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

En el resultado de la investigación en esta pregunta indican: El 67,5% de los profesionales coinciden, como valor predominante tenemos casi siempre y aveces, podemos interpretar sobre los resultados obtenidos que los profesionales pueden tener este metodo como medida de mitigacion, pero se puede implementar mas mecanismo para reducir la brecha de seguridad en temas de ataques fisicos.

Tabla 19. Pregunta 6

Pregunta 6	Frecuencia	Porcentaje
Siempre	2	5,4%
Casi siempre	6	16,2%
A veces	8	21,6%
Casi nunca	11	29,7%
Nunca	10	27%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 6

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

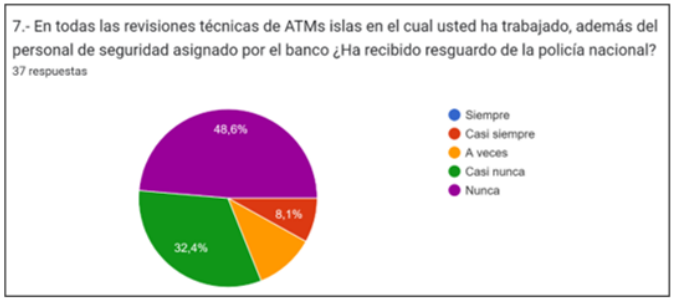
En el resultado de la investigación en esta pregunta indican: El 56,7% de los profesionales coinciden, como valor predominante tenemos casi nunca y nunca, este resultado da un mejor panorama sobre las medidas implementadas en agencias son mas robustas y los tiempos de respuestas son mas rapidos a comparacion de los ATMs implementados en sitios islas.

Tabla 20. Pregunta 7

Pregunta 7	Frecuencia	Porcentaje
Siempre	0	0%
Casi siempre	3	8,1%
A veces	4	10,8%
Casi nunca	12	32,4%
Nunca	18	48,6%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 7



Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

El 81% de los profesionales coinciden, como valor predominante tenemos casi nunca y nunca, podemos interpretar sobre los resultados obtenidos, la vulnerabilidad que son expuesto tanto el personal tecnico, el activo de la institucion financiera y el dinero. Esto muestra un notable riesgo ante cualquier ataque delincuencial que se pueda presentar.

Tabla 21. Pregunta 8

Pregunta 8	Frecuencia	Porcentaje
Siempre	1	2,7%
Casi siempre	15	40,5%
A veces	14	37,8%
Casi nunca	5	13,5%
Nunca	2	5,4%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 8

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

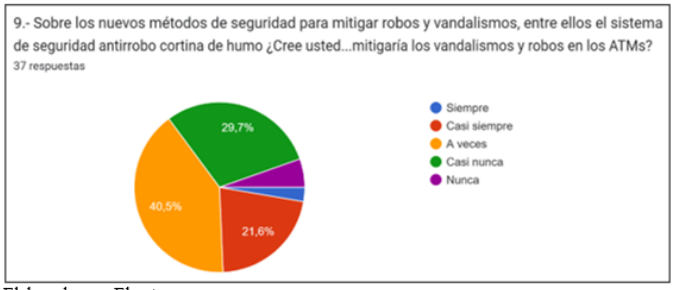
El 78.3% de los profesionales coinciden, como valor predominante tenemos casi siempre y a veces, podemos interpretar sobre los resultados obtenidos,que genera proteccion al ser una capa adicional a la seguridad ya implementada pero seria importante un mecanismo de seguridad adicional para mejorar los temas de ataques fisicos.

Tabla 22. Pregunta 9

Pregunta 9	Frecuencia	Porcentaje
Siempre	1	2,7%
Casi siempre	8	21,6%
A veces	15	40,5%
Casi nunca	11	29,7%
Nunca	2	5,4%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 9



Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

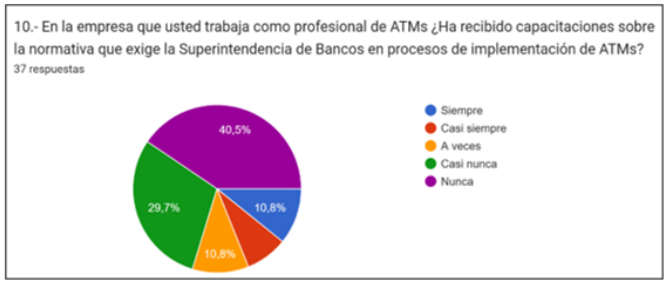
El 70.2% de los profesionales coinciden, como valor predominante tenemos casi nunca y a veces, podemos interpretar sobre los resultados obtenidos que este metodo de mitigación no es suficiente para reducir los ataques y robos en los site de los ATMs utilizado en varias entidades financieras como medida de seguridad para sitios remotos y de respuesta limitada.

Tabla 23. Pregunta 10

Pregunta 10	Frecuencia	Porcentaje
Siempre	4	10,8%
Casi siempre	3	8,1%
A veces	4	10,8%
Casi nunca	11	29,7%
Nunca	15	40,5%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 10



Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

El 70.2% de los profesionales coinciden, como valor predominante tenemos casi nunca y a veces, podemos interpretar sobre los resultados obtenidos que las instituciones y empresas que se dedican a realizar implementaciones, administraciones de red ATMs y proyectos, no capacitan a su personal en temas de la normativa de seguridad vigente en la superintendencia de bancos.

Tabla 24. Pregunta 11

Pregunta 11	Frecuencia	Porcentaje
Siempre	5	13,5%
Casi siempre	11	29,7%
A veces	11	29,7%
Casi nunca	7	18,9%
Nunca	3	8,1%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 11

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

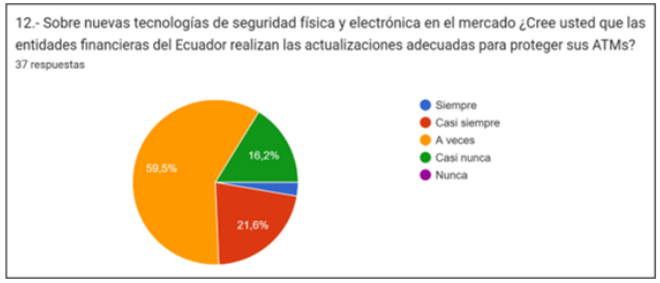
El 59.4% de los profesionales coinciden, como valor predominante tenemos casi siempre y a veces, podemos interpretar sobre los resultados que el personal de seguridad no realiza el acompañamiento para resguardar la integridad del personal tecnico y los activos de las entidad financiera, sabiendo que al ser un cajero en un sitio remoto, el nivel de riesgo es mayor.

Tabla 25. Pregunta 12

Pregunta 12	Frecuencia	Porcentaje
Siempre	1	2,7%
Casi siempre	8	21,6%
A veces	22	59,5%
Casi nunca	6	16,2%
Nunca	0	0%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 12



Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

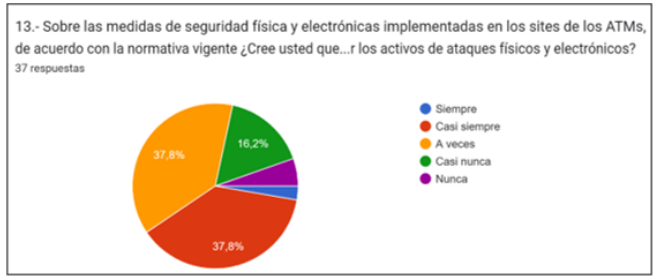
El 59.5% de los profesionales coinciden, como valor predominante tenemos a veces, podemos interpretar sobre los resultados, de acuerdo a su criterio tecnico, que las entidades deben realizar las actualizaciones necesarias en temas de seguridad física y electronica, para reducir el riesgo, de la manos de los nuevos avances tecnologico en el ambito de la defensa.

Tabla 26. Pregunta 13

Pregunta 13	Frecuencia	Porcentaje
Siempre	1	2,7%
Casi siempre	14	37,8%
A veces	14	37,8%
Casi nunca	6	16,2%
Nunca	2	5,4%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 13



Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

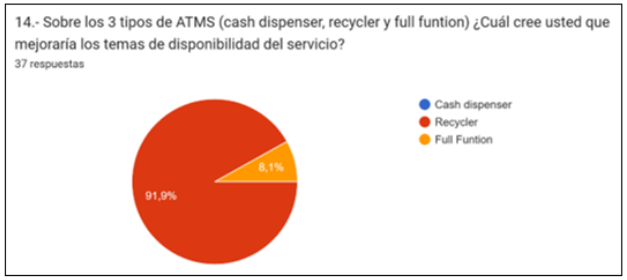
El 75.6% de los profesionales coinciden, como valor predominante tenemos casi siempre y a veces, podemos interpretar sobre los resultados, de acuerdo a su criterio, tienen proteccion para ciertos tipos de ataques y amenzas. No obstante, es importante prevenir realizando evaluacion de las medidas ya implementadas y aplicar adicionales.

Tabla 27. Pregunta 14

Pregunta 14	Frecuencia	Porcentaje
Cash Dispenser	0	0%
Recycler	34	91,9%
Full Funtion	3	8,1%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 14



Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

El 91.9% de los profesionales coinciden, que la disponibilidad del servicio es mejor con la utilizacion de los ATMs Recycler, los cuales permiten una retroalimentacion del dinero depositado, para que pueda ser utilizado en retiros. De esta manera reduce la carga de efectivo constante por parte del personal de la entidad financiera, reduciendo el tiempo de estar fuera de servicio por abastecimiento.

Tabla 28. Pregunta 15

Pregunta 15	Frecuencia	Porcentaje
Siempre	29	78,4%
Casi siempre	6	16,2%
A veces	2	5,4%
Casi nunca	0	0%
Nunca	0	0%
Total	**37**	**100%**

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Figura#
Pregunta 15

Elaborado por: El autor
Fuente: Encuesta aplicada a profesionales en ATMs - https://n9.cl/13eip

Analisis e interpretacion:

El 78.4 % de los profesionales coinciden, como valor predominante tenemos siempre, podemos interpretar sobre los resultados, de acuerdo a su criterio, cuentan con proteccion antiskiming, este dispositivo es obligatorio en todos los ATMs, de acuerdo a lo indicado en la norma de seguridad fisica y electronica de la superintendencia de Bancos y la superintendencia econmica popular y solidaria.