



Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería Electrónica y Eléctrica
Escuela Profesional de Ingeniería de Telecomunicaciones

**Diseño de un sistema de acceso biométrico mediante
huella dactilar en la red de cajeros automáticos del
Banco de la Nación para mejorar la seguridad de la
entidad financiera**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero Telecomunicaciones

AUTOR

Jhonatan Antonio ROJAS SALAZAR

ASESOR

Mg. Wilbert CHAVEZ IRAZABAL

Lima, Perú

2021



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Rojas, J. (2021). *Diseño de un sistema de acceso biométrico mediante huella dactilar en la red de cajeros automáticos del Banco de la Nación para mejorar la seguridad de la entidad financiera*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería de Telecomunicaciones]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	JHONATAN ANTONIO ROJAS SALAZAR
DNI	47047388
URL de ORCID	
Datos de asesor	
Nombres y apellidos	WILBERT CHAVEZ IRAZABAL
DNI	08121733
URL de ORCID	https://orcid.org/0000-0002-7978-7031
Datos de investigación	
Línea de investigación	No aplica.
Grupo de investigación	No aplica.
Agencia de financiamiento	. Sin financiamiento.
Ubicación geográfica de la investigación	Edificio: Banco de la Nación (Sede principal) País: Perú Departamento: Lima Provincia: Lima Distrito: San Borja Calle: Av. Javier Prado Este N° 2499 Latitud: -12.0873715 Longitud: -77.0004088
Año o rango de años en que se realizó la investigación	Enero 2017 - Diciembre 2017
URL de disciplinas OCDE	Ciencias de la computación. https://purl.org/pe-repo/ocde/ford#1.02.00 Ingeniería Tecnología https://purl.org/pe-repo/ocde/ford#2.00.00



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERIA ELECTRÓNICA Y ELÉCTRICA
PROGRAMA DE TITULACIÓN EXTRAORDINARIA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL Nº 041/FIEE-EPIE/2021

Los suscritos Miembros del Jurado, nombrados por la Comisión Ejecutiva del Programa de Perfeccionamiento Profesional de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha, bajo La Presidencia Del **Ing. Huablocho Perez, Teofilo Matias** integrado por **Mg. Chavez Irazabal, Wilbert** y **Mg. Malca Fernandez, Jean Carlos**.

Después de escuchar la Sustentación de Trabajo de Suficiencia Profesional del **Bach. ROJAS SALAZAR, JHONATAN ANTONIO** con código Nº **10190200** que para optar el Título Profesional de Ingeniero de Telecomunicaciones sustentó el Trabajo de Suficiencia Profesional titulada **“DISEÑO DE UN SISTEMA DE ACCESO BIOMÉTRICO MEDIANTE HUELLA DACTILAR EN LA RED DE CAJEROS AUTOMÁTICOS DEL BANCO DE LA NACIÓN PARA MEJORAR LA SEGURIDAD DE LA ENTIDAD FINANCIERA”**

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió **aprobar** otorgándole el calificativo de diecisiete (17)

Ciudad Universitaria, 25 de junio del 2021

Ing. Huablocho Perez, Teofilo Matias
Presidente de Jurado

Mg. Chavez Irazabal, Wilbert
Miembro de Jurado

Mg. Malca Fernandez, Jean Carlos
Miembro de Jurado

RESUMEN

La presente investigación tiene como objetivo el diseño de un sistema de control de acceso por identificación biométrica mediante huella dactilar en la red de cajeros automáticos del Banco de la Nación que permita mejorar la seguridad de este canal de atención.

Dicha propuesta tiene un alcance para todos los cajeros automáticos del Banco de la nación en el Perú. Se dará a conocer la propuesta de diseño, el costo estimado de la infraestructura a implementar y los beneficios en cuanto a mejora de seguridad para este canal de atención.

Se determinará que la tecnología biométrica por huella dactilar es la mejor opción, frente a los demás métodos biométricos disponibles, para contrarrestar algunos tipos de fraude realizados en cajeros automáticos.

Se usará el lector MorphoSmart300 por que cumple los requisitos para acceder al servicio de verificación biométrico de la RENIEC.

La plataforma implementada de lector biométrico para las agencias del Banco, sirvió de modelo para definir el diseño de esta investigación.

Al final se exponen los resultados y los beneficios en cuanto a seguridad, en donde se concluye que la implementación de biometría en cajeros automáticos permitirá erradicar algunos tipos de fraude tal como, suplantación, cambiao y clonación de tarjeta.

Palabras clave: ATM, STRATUS, Agente Biométrico, Gateway Biométrico y Monitor Biométrico.

ABSTRACT

The objective of this research is to design an access control system by biometric identification through fingerprint in the network of ATMs of the Banco de la Nación that allows to improve the security of this service channel.

This proposal has a scope for all ATMs of Banco de la Nación in Peru. The design proposal, the estimated cost of the infrastructure to be implemented and the benefits in terms of security improvement for this service channel will be announced.

It will be determined that biometric fingerprint technology is the best option, compared to the other biometric methods available today, to counteract some types of ATM fraud.

The biometric fingerprint reader MorphoSmart300 will be used because it meets all the requirements to access the biometric verification service of the RENIEC.

The platform that is already implemented of biometric fingerprint reader for the agencies of the Bank, served as a model to define the design of the biometric system of this research.

At the end, the results and benefits in terms of security are presented, where it is concluded that the implementation of biometrics in ATMs will allow to eradicate some types of fraud such as card spoofing, swapping and cloning.

Keywords: ATM, STRATUS, Biometric Agent, Biometric Gateway and Biometric Monitor.

INDICE

RESUMEN	i
ABSTRACT	ii
INDICE	iii
INDICE DE TABLES	v
INDICE DE FIGURAS	vi
CAPÍTULO I	1
INTRODUCCIÓN	1
CAPÍTULO II	2
INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD 2	
2.1 Institución donde se desarrolló la actividad	2
2.2 Periodo de duración de la actividad	2
2.3 Finalidad de la entidad	2
2.4 Objetivo de la entidad	3
2.5 Razón social	3
2.6 Correo electrónico del profesional a cargo	3
CAPÍTULO III	4
DESCRIPCIÓN DE LA ACTIVIDAD	4
3.1 Finalidad y Objetivos de la actividad	4
3.1.1 Finalidad	4
3.1.2 Objetivos	5
3.2 Problemática	5
3.2.1 Problema principal	5
3.2.2 Problemas Específicos	5
3.2.3 Justificación e importancia de la investigación	6
3.3 Metodología	6
3.3.1 Antecedentes de la investigación	6

3.3.2 Bases teóricas	8
3.4 Procedimiento	26
3.4.1 Tipo de investigación	26
3.4.2 Diseño de la investigación	26
CAPÍTULO IV	56
CONCLUSIONES	56
4.1 Justificación	56
4.2 Presentación de Resultados	56
4.2.1 Seguridad	56
4.2.2 Costos	57
4.3 Conclusiones	59
CAPÍTULO V	60
RECOMENDACIONES	60
CAPÍTULO VI	61
BIBLIOGRAFIA	61

INDICE DE TABLAS

Tabla 1. Muestra biométrica según la tecnología dactilar.....	15
Tabla 2. Comparación de métodos de sistemas biométricos	16
Tabla 3. Comparativa de tecnologías biométricas	17
Tabla 4. Descripción de actores	34
Tabla 5. Descripción de casos de uso	35
Tabla 6. Procesos Biomatch Client	48
Tabla 7. Procesos Servicios Gateway Biomérico	49
Tabla 8. Procesos Motor Biométrico.....	50
Tabla 9. Procesos Portal Monitor Web.....	50
Tabla 10. Estimación de costos.....	58

INDICE DE FIGURAS

Figura 1. Cajero automático de tipo: Retiro.....	9
Figura 2. Cajero automático de tipo: Multifunción.....	11
Figura 3. Huella dactilar, “crestas y valles”.....	18
Figura 4. DNI Electrónico	21
Figura 5. MorphoSmart 300.....	23
Figura 6. Diagrama de paquetes.....	31
Figura 7. Diagrama caso de uso – Agente Biométrico (Capturar y Validar huellas)	31
Figura 8. Diagrama caso de uso – Agente Biométrico (Capturar y Validar Huellas MOC).....	32
Figura 9. Diagrama caso de uso – Agente Biométrico (Capturar y Validar Huellas Transacciones	32
Figura 10. Diagrama caso de uso – Central de Huellas.....	33
Figura 11. Diagrama caso de uso – Monitor de Biometría	33
Figura 12. Servidores de la arquitectura.....	38
Figura 13. Arquitectura básica del sistema biométrico para cajeros automáticos.....	39
Figura 14. Vista General de la Arquitectura de Desarrollo	40
Figura 15. Vista Lógica de BiomatchClient.....	41
Figura 16. Vista Lógica del Gateway Biométrico	42
Figura 17. Vista Lógica del Portal Monitor Web	43
Figura 18. Vista Lógica Motor Biométrico Moo	43
Figura 19. Paquetes de diseño	44
Figura 20. Paquetes de diseño del Biomatch Client.....	44
Figura 21. Paquetes de diseño Servicio Gateway Biométrico	45
Figura 22. Paquetes de diseño Portal Monitor Web.....	46
Figura 23. Paquetes de diseño Motor Biométrico.....	47

Figura 24. Interpretación General de los Casos de Uso	48
Figura 25. Vista Básica de Despliegue.....	51
Figura 26. Vista de Implementación	53

CAPITULO I

INTRODUCCIÓN

Hoy en día uno de los principales problemas que afronta el país es la inseguridad ciudadana. Esto conlleva a que las instituciones públicas y privadas busquen mejorar sus sistemas de seguridad.

En este ámbito, las entidades bancarias, vienen trabajando en desarrollar mecanismos que buscan dar mayor seguridad y bienestar a sus clientes en temas de acceso a los servicios que ofrecen.

El incremento de la actividad económica en los últimos años en el Perú ha ido de la mano con el esfuerzo de la banca en tratar de descentralizar los servicios que brinda a través de todos sus canales de atención.

Un canal de atención que tiene una gran acogida entre los usuarios, es el canal de cajeros automáticos, esto se debe a que las entidades financieras están proporcionando cada vez más opciones de transacciones y operaciones por este medio.

El presente trabajo consiste en el diseño de un sistema de control de acceso biométrico por huella dactilar en cajeros automáticos y los beneficios que se tendrá en seguridad respecto al acceso a los servicios que el Banco de la Nación brinda por este canal.

CAPITULO II

INFORMACION DEL LUGAR DONDE SE DESARROLLO LA ACTIVIDAD

2.1 Institución donde se desarrolló la actividad

Banco de la Nación

2.2 Periodo de duración de la actividad

Enero a diciembre del año 2017.

2.3 Finalidad de la entidad

El Banco de la Nación tiene como finalidad principal proporcionar a todos los órganos del Sector Público Nacional los servicios bancarios que dichas entidades requieren para el cumplimiento de sus funciones.

2.4 Objetivo de la entidad

El objetivo principal es administrar por delegación las sub cuentas del Tesoro Público y proporcionar al Gobierno Central servicios bancarios para la administración de los fondos públicos, también otorgar

servicios financieros a los trabajadores y a los pensionistas del sector público.

2.5 Razón social

Banco de la Nación.

2.6 Correo electrónico del profesional a cargo

dmarcelo@bn.com.pe

CAPÍTULO III

DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Finalidad y Objetivos de la actividad

3.1.1 Finalidad

Actualmente uno de los principales problemas que tienen las entidades bancarias es el de la seguridad que brinda a sus clientes en el tema de las transacciones que realiza en cajeros automáticos.

Existen delitos informáticos que intentan vulnerar los sistemas de seguridad de los bancos. Además, diversos tipos de fraude como la suplantación, clonación de tarjetas mediante instalación de dispositivos en los periféricos de los cajeros automáticos.

En una nota de prensa del diario Correo (2017) se indicó lo siguiente:

Entre noviembre y diciembre del 2017, se registraron 50 asaltos en cajeros automáticos en el Perú con diversas modalidades de fraude. Según la PNP (Policía Nacional del Perú) por fiestas de fin de año los robos se incrementan hasta en un 10%.

Lo que hace estimar que en el año 2017 se dieron 278 robos en cajeros automáticos de diversas entidades financieras en Perú.

Debido a esta problemática hay malestar en la población, ya que generan pérdidas económicas para los clientes. A raíz de lo expuesto es que nace este trabajo como una propuesta para mejorar la seguridad en el canal de cajeros automáticos.

3.1.2 Objetivos

3.1.2.1 Objetivo de la investigación. Diseñar un sistema de control de acceso por identificación biométrica mediante huella dactilar en la red de cajeros automáticos del Banco de la Nación que permita mejorar la seguridad de este canal de atención.

3.1.2.2 Objetivos Específicos. Analizar y evaluar las características técnicas de los equipos para la implementación de biometría mediante huella dactilar en la red de cajeros automáticos del Banco de la Nación.

Diseñar un sistema de biometría mediante huella dactilar en la red de cajeros automáticos del Banco de la Nación.

Evaluar las mejoras respecto a seguridad en la red de cajeros automáticos del Banco de la Nación.

3.2 Problemática

3.2.1 Problema principal

¿Es posible mejorar la seguridad del canal de atención de cajeros automáticos del Banco de la Nación mediante un sistema de control de acceso por identificación biométrica mediante huella dactilar?

3.2.2 Problemas Específicos

¿Cómo elegir los equipos a utilizar en una implementación de biometría mediante huella dactilar en la red de cajeros automáticos del Banco de la Nación?

¿Cómo optimizar el control de accesos utilizando un sistema biométrico de huella dactilar en la red de cajeros automáticos del Banco de la Nación?

¿Cómo medir las mejoras respecto a seguridad en la red de cajeros automáticos del Banco de la Nación con la implementación de biometría por huella dactilar?

3.3 Metodología

3.3.1 Antecedentes de la investigación

El Banco de la Nación, es actualmente una de las principales entidades financieras en el país. Tiene llegada, mediante sus diversos canales, a la mayor cantidad de localidades del país. El canal más usado para llevar banca a los lugares recónditos es el canal de cajeros automáticos.

Los cajeros automáticos de los diversos bancos del país, tienen muchas similitudes en cuanto a la seguridad que brindan, esto también es debido a que existen dos marcas predominantes de cajeros automáticos hoy en día en el mercado peruano: Diebold y NCR.

En el marco internacional Sánchez (2012), indicó que “el banco polaco BPS, es el primer banco de Europa en instalar un cajero automático biométrico, en el que se puede retirar dinero usando solo la huella dactilar”.

En un estudio de la revista Semana de Colombia (2014), se indica que:

En un futuro no muy lejano, se podrá comprar y sacar dinero usando la huella digital, según un proyecto piloto a prueba en dos ciudades de Francia. Esta tecnología, desarrollada por la empresa Natural Security, pretende también aplicarse en los cajeros automáticos de los bancos para sacar dinero. Lo primero que se precisa es registrar las huellas digitales del usuario en el banco donde tiene su cuenta y éstas figurarán en una tarjeta bancaria y un estuche especial para tal efecto. Cuando vaya a pagar, el cliente pone su dedo en el lector biométrico y éste envía una señal a la tarjeta que lleva con él para ver si las huellas digitales coinciden. Si son idénticas, la terminal valida la

transacción. La diferencia con otros sistemas en vigor, alegan los desarrolladores, es que el banco no guarda los datos biométricos de sus clientes, sino que estos están contenidos en la tarjeta.

A nivel de América Latina, López (2017), señala lo siguiente:

A finales de 2017, los cajeros automáticos de BBVA Bancomer requerirán las huellas digitales de los usuarios para hacer operaciones, con lo que se busca aumentar la seguridad, informó el director general de la entidad financiera, Eduardo Osuna. Comentó que ya tienen algunos cajeros con pruebas piloto, e incluso las adquisiciones nuevas de estos equipos ya incluyen esta medida de identificación de los usuarios. Indicó en conferencia de prensa que también se aplicarán pruebas biométricas (además de las huellas dactilares, reconocimiento de voz y facial) para la adquisición de tarjetas de crédito o de cuentas de cheques y otros productos que se podrán contratar a distancia. "Se está destinando mucho dinero a esto", dijo el directivo luego de reconocer que BBVA Bancomer ya tuvo casos de suplantación de identidad, tanto en créditos de auto como en créditos de casa, aunque sin mencionar una cifra al respecto. Explicó que en estos casos una persona se presenta con una identificación falsa a una sucursal bancaria para solicitar un crédito, el banco investiga el nombre y si ve que es un cliente sujeto de crédito lo otorga, pero en realidad, no es la persona verdadera. Hoy ya cuentan con biométricos para el otorgamiento de créditos de autos y la entidad está lista para cumplir con los nuevos requerimientos que establecerá la autoridad para combatir el robo de identidad, argumentó el directivo.

INFOTECHNOLOGY (2018), menciona lo siguiente:

El Banco San Juan implementó junto a Red Link el primer cajero automático con reconocimiento de huellas dactilares del país. En esta primera etapa, el desarrollo alcanza al segmento de jubilados y pensionados, quienes mediante este dispositivo de identificación biométrica pueden realizar el trámite de la fe de vida para el cobro de

sus retribuciones. El cajero está disponible en la sucursal de Banco San Juan, ubicado en la ciudad de Buenos Aires y en breve se expandirá a las demás localidades de la provincia de San Juan y la provincia de Mendoza, anunció la entidad financiera, también destacaron que el desarrollo y la implementación estuvo a cargo de los profesionales de Red Link y del Banco.

En la segunda parte del desarrollo de esta implementación los clientes podrán realizar cualquier transacción en un cajero automático sin necesidad de contar con la tarjeta de débito. Esta experiencia implementada por el Banco San Juan se expandirá a los demás bancos del Grupo Petersen (Banco de Entre Ríos, Banco Santa Fe y Banco Santa Cruz).

Toda su red de cajeros estará en diversos puntos del país, posicionándose, una vez más, a la vanguardia de las soluciones e innovaciones tecnológicas del sector financiero.

En el Perú, el diario Gestión (2017) mencionó que:

La identificación biométrica a través de huellas dactilares en cajeros automáticos en el país aún se encuentra en una etapa incipiente. Además, menciona que el 81% de los consumidores en el mundo señalan al reconocimiento de huellas digitales como el método más seguro de autenticación biométrica, seguido por el escaneo del iris (76%) de acuerdo al análisis Visa Europe de 2016.

3.3.2 Bases teóricas

3.3.2.1 Cajeros Automáticos. Según la Universidad Latina de América (2015) indica que: El cajero automático es un equipo automatizado con el que se maneja tanto la recepción como la entrega de dinero en efectivo; se realizan consultas de saldos y algunas operaciones sobre los diferentes servicios que ofrece una institución bancaria, entregando al usuario un comprobante de la operación en un mínimo de tiempo.

3.3.2.2 Tipos de Cajeros Automáticos. Los cajeros automáticos en el Perú varían dependiendo de la necesidad de cada banco. Principalmente se dividen en dos tipos: Retiro y Multifunción como son mostrados en las (Figuras 1 y 2).



Figura 1: Cajero automático de tipo: Retiro. Fuente: Universidad Latina de América-2015.

Los cajeros automáticos Multifunción son aquellos que permiten extraer dinero como así también realizar depósitos.



Figura 2: Cajero automático de tipo: Multifunción. Fuente: Marcelogaona-2009.

3.3.2.3 Partes de Cajeros Automáticos. Actualmente, en el mercado peruano, Diebold y NCR son los principales proveedores de cajeros automáticos, se presentará información respecto a estas dos empresas. Se dividirá las partes en dos grupos, dispositivos exteriores e interiores según el Banco de la Nación (2015):

3.3.2.3.1 Dispositivos exteriores:

- **Pantalla de usuario:** Monitor frontal que interactúa con el usuario en el proceso de las transacciones.
- **Lector de tarjeta:** Dispositivo que captura la información del chip o la banda magnética de la tarjeta para que se pueda identificar al usuario y sus cuentas.
- **Teclado de usuario:** Dispositivo donde el usuario puede ingresar datos numéricos, también aceptar, corregir y rechazar acciones.
- **Botones complementarios:** Botones ubicados a los lados de la pantalla del usuario, sirven para seleccionar opciones de los diversos menús que se muestran en el monitor.
- **Impresora:** Dispositivo que imprime recibos de las transacciones a solicitud del usuario.

- **Boqueta o Shutter:** Es la parte visible del dispensador de billetes, su función es presentar los billetes cada vez que un usuario haga un retiro.
- **Bandeja de depósito:** Dispositivo que se encarga de recibir dinero, solo presente en cajeros automáticos multifunción.

3.3.2.3.2 Dispositivos interiores:

- **Parlante:** Dispositivo emisor de sonidos en respuesta a determinadas acciones del usuario.
- **Bóveda:** Es una caja fuerte de acero que contiene en su interior el dispensador. Por lo general se encuentra ubicada en la parte inferior del cajero.
- **Dispensador:** Dispositivo que cuenta, por lo general, con 4 o 5 maletas para billetes y 1 maleta de rechazos (Donde se alojan los billetes que no cumplen con la calidad física requerida y los billetes que son presentados y no recogidos del cajero). Además, cuenta con un sistema para la extracción de billetes que lleva los billetes desde la maleta hasta presentarlos en el shutter.
- **Gaveta de rechazos de tarjetas:** Compartimiento ubicado detrás de la lectora de tarjetas, sirve de almacén para las tarjetas retenidas.
- **Pantalla de operador:** Monitor, por lo general ubicado en la parte posterior del cajero, sirve para que el operador técnico realice configuraciones locales en el equipo.
- **CPU:** Computador local responsable de establecer comunicación entre el sistema operativo Windows, el software principal propietario de la marca del cajero y el servidor controlador de cajeros del banco. También realiza el manejo de los distintos dispositivos externos e internos. Los CPU de cajeros automáticos en la actualidad, cuentan con las siguientes especificaciones técnicas mínimas:
 - Procesador de 2da Generación, arquitectura de 32 Bits, velocidad de procesador 2.2 Ghz (2 núcleos).
 - Memoria RAM DDR2 de 4Gb.

- Puerto USB 2.0 (4).
- Disco duro de 500 Gb.
- Sistema Operativo Windows XP SP3.
- Lectora de CD/DVD.

3.3.2.4 Sistema eléctrico en cajeros automáticos. Los cajeros automáticos se encuentran ubicados en algunas de las 637 agencias con las que cuenta el banco, también en centros comerciales o lugares estratégicos en todo el territorio peruano.

Los ATM cuentan con un estabilizador de voltaje externo y están conectados a la red eléctrica del predio donde se encuentran, con un respaldo en caso de corte de energía, de UPS o generador eléctrico.

Dentro del cajero automático existe un Power Box (regleta de tomacorriente) que alimenta cada dispositivo del cajero automático.

Según DIEBOLD NIXDORF (2019) se requiere:

3.3.2.4.1 Tomacorriente eléctrico donde ingresa la energía comercial. Un tomacorriente independiente con distribución tipo monofásica, con 3 alambres conductores. El alambrado conectado al tomacorriente debe incluir un tercer alambre para conexión directa a un pozo de tierra. El circuito eléctrico monofásico en el tablero de distribución debe contar con un ITM independiente (25 amp).

- Medición en toma corriente:

L – N :220 VAC (Tensión de salida: 220 VAC +/- 3 %) estabilizado

L – T :220 VAC (Tensión de salida: 220 VAC +/- 3 %) estabilizado

N – T : 0 VAC

3.3.2.4.2 Estabilizador Sólido (1.5 KVA). El estabilizador de tensión brinda protección eléctrica al ATM, su función es mantener un voltaje de salida estable mientras la tensión de entrada se encuentre dentro del rango permitido (Valor nominal +/- 5%).

- Medición de voltajes a la salida del Estabilizador Sólido:

L – N :220 VAC (Tensión de salida: 220 VAC +/- 3 %) estabilizado

L – T :220 VAC (Tensión de salida: 220 VAC +/- 3 %) estabilizado

N – T : 0 VAC

3.3.2.4.3 Power Box. Es la regleta de tomacorriente que alimenta cada dispositivo del cajero automático.

- Medición de voltajes a la entrada del ATM en el Power Box:

L – N :220 VAC (Tensión de salida: 220 VAC +/- 3 %) estabilizado

L – T :220 VAC (Tensión de salida: 220 VAC +/- 3 %) estabilizado

N – T : 0 VAC

3.3.2.5 Dispositivos de Seguridad. Según el Banco de la Nación (2015):

El Banco cuenta con un concentrador, servidor de eventos y alertas, que son generados por los cajeros automáticos, este concentrador permite detectar cualquier accionamiento de los dispositivos electrónicos, tales como sensores y dispositivos antifraude, los cuales deberán ser reportados a la central de monitoreo utilizando los canales de red propios del cajero.

Entre los dispositivos de seguridad se tiene:

- Sensores que monitorean la salida de dinero del presentador.
- Sensores que no permiten la colocación de dispositivos extraños sobre el teclado.
- Sensores de seguridad en la bóveda: sensor de temperatura, sensor de vibración, sensor de apertura de bóveda.
- Señal sonora como acción disuasiva cuando se active cualquier sensor de los mencionados anteriormente.

3.3.2.6 Telecomunicaciones. El Banco de la Nación, actualmente, utiliza servicios de comunicación de un operador local para interconectar su central con los equipos terminales de sus agencias, en este caso con los cajeros automáticos.

Los cajeros automáticos, pueden operar con un ancho de banda mínimo de 256 Kbps. Debido a que el Banco tiene cajeros automáticos en distintos lugares del país, se utilizan los siguientes tipos de acceso:

- ADSL: Tecnología de conexión a internet mediante el uso de la línea telefónica tradicional, transmite información digital de modo analógico a

través de cable trenzado de cobre. Actualmente se tiene un servicio ADSL con ancho de banda de 80 Mbps.

- Satelital: El Banco de la Nación usa este tipo de acceso para conectar agencias y cajeros en lugares recónditos del país, donde no llega otro tipo de comunicación. Actualmente se cuenta con un servicio Satelital de 10 Mbps.

3.3.2.7 Operaciones en los cajeros automáticos. En el Perú generalmente todos los bancos tienen disponible en sus cajeros automáticos las mismas operaciones, en este caso se mostrará las operaciones que se pueden realizar en el Banco de la Nación según Banco de la Nación (2020):

- Retiro de efectivo.
- Emisión y cobro de giros.
- Pago de Servicios.
- Pago de Tasas de Entidades Públicas.
- Consulta de estado de cuentas, movimiento y código de cuenta interbancario (CCI).
- Transferencias de soles y dólares entre tus propias cuentas.
- Transferencias de soles y dólares a otras cuentas.
- Cambio de PIN.

3.3.2.8 Biometría. De acuerdo a BY (2018): La biometría es una forma de reconocimiento de seres humanos basado en sus características de comportamiento o características fisiológicas. Es un procedimiento parecido al que realiza habitualmente el ser humano, al reconocer e identificar a otros seres humanos por su voz, su aspecto físico, entre otros.

3.3.2.8.1 Clasificación. Se clasificará la biometría de acuerdo al rasgo según BY (2018):

- **Fisiológico:** el reconocimiento de iris, huella dactilar, retina, geometría de manos y rostro.

- **De comportamiento:** el reconocimiento de firma, de voz o de la forma de escritura en el teclado.

Los métodos más difundidos en la actualidad son el reconocimiento de iris y el reconocimiento de huella dactilar. Esto es debido a que estas técnicas son poco intrusivas y su costo de implementación es menor en comparación al resto. De acuerdo a que técnica biométrica se use, los parámetros para la identificación son distintos: geometría de la mano, surcos de la huella dactilar, etc. De acuerdo a estos parámetros se extrae un patrón único para cada ser humano, el mismo será utilizado en comparaciones posteriores. En la (tabla 1) se observa la muestra biométrica según la tecnología dactilar.

TABLA 1: Muestra biométrica según la tecnología dactilar.

TECNOLOGIA	MUESTRA BIOMETRICA
Huella dactilar	Imagen o minucio de la huella dactilar
Reconocimiento de voz	Grabacion de voz
Reconocimiento facial	Imagen facial
Reconocimiento de iris	Imagen de iris
Reconocimiento de retina	Imagen de retina
Reconocimiento de la geometria de la mano	Imagen en 3D de la parte superior y lateral de mano y dedos
Reconocimiento de firma	Imagen de la firma y registro de medidas relacionadas con la dinámica
Reconocimiento de escritura de teclado	Registro de las teclas pulsadoas y registro de medidas relacionadas con la dinámica

Fuente: Blog BY

3.3.2.8.2 Factores de métodos biométricos. Para Landi (2007):

“Teniendo en cuenta los factores de los diversos tipos de métodos biométricos, se considera: nivel de precisión, barreras contra los ataques, facilidad de uso, aceptabilidad de usuario y la estabilidad a largo plazo”. En la (tabla 2) se muestra la comparación de métodos de sistemas biométricos.

TABLA 2: Comparación de métodos de sistemas biométricos

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándares	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Imitaciones	Suciedad, heridas, asperezas	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...
Costo	Alto	Alto	Medio	Medio	Medio	Bajo

Fuente: Landi, C. Introducción a la biometría informática y análisis de huella dactilar como fuentes de autenticación en sistemas de seguridad. p. 20

Según Clarke, Modet (2018): “es importante saber las tasas de error (EER), falso rechazo (FRR), falsa aceptación (FAR) y fallo en el registro entre las principales técnicas biométricas dependiendo de los factores físico y físico-comportamiento”. En la (tabla 3) se muestra la comparativa de tecnologías biométricas.

TABLA 3: Comparativa de tecnologías biométricas

	Huella	Facial	Iris	Voz
Tipo	Físico	Físico	Físico	Físico-Comportamiento
Método	Activo	Pasivo	Activo	Activo
Tasa de error igual (EER)	2-3.3%	4.1%	4.1 – 4.96%	0.1 – 0.86%
Tasa de falsa aceptación (FAR)	2.5%	4%	6%	0.75%
Tasa de falso rechazo (FRR)	0.1%	10%	0.001%	0.75%
Fallo en el registro	4%	-0%	4.1 – 4.6%	0.1 – 0.86%
Coste	Medio	Alto	Muy alto	Medio - bajo
Aceptación social	Media	Alta	Baja	Alta

Fuente: Clarke, Modet (2018) Biometría.

La tecnología biométrica por huella es la mejor opción actualmente para lograr una rápida y correcta autenticación del usuario; se considera esto debido a que su tasa de error es (2-3.3%) en comparación con la tecnología biométrica Facial (4.1%) y de iris (4.1-4.96%), la tasa de falso rechazo de la tecnología por huella es (0.1%) en comparación a la tecnología biométrica por voz (0.75%).

3.3.2.9 Huella dactilar. Para Inngresa (2018):

Los seres humanos tienen características únicas tales como las huellas dactilares. Estas tienen las denominadas “crestas y valles” que son formadas por una combinación de factores ambientales y genéticos. Cada huella dactilar posee un diseño único.

3.3.2.9.1 Funcionamiento de lectores biométricos de huella digital. Según Inngresa (2018):

Como primer paso, se almacena en la base de datos del sistema, las huellas dactilares de todos los usuarios. Cada huella va junto a sus datos personales. Las huellas se almacenan como códigos encriptados, los cuales son imposibles de descifrar.

Posterior, los usuarios deben colocar el dedo índice en el lector de huellas para que el sistema obtenga la huella dactilar en imagen.

El sistema implementado debe comparar el patrón de crestas y valles de la imagen obtenida con los patrones almacenados en la base de datos.

En la (figura 3) se observa la Huella dactilar, “crestas y valles”.



Figura. 3: Huella dactilar, “crestas y valles”. Fuente: Techlandia-2018.

3.3.2.9.2 Tipos de lectores de huellas dactilares. Existen varios tipos de lectores de huellas dactilares, algunos de ellos vamos a definir a continuación según Guías Prácticas (2018):

- Lector de huellas dactilares ópticos reflexivos: es un tipo de sensor que se está compuesta de una superficie de cristal o también denominado prisma que es iluminada con un diodo LED. Cuando se coloca el dedo sobre la superficie de cristal, la luz del diodo LED es absorbida, las partes oscuras que se producen por las crestas de las huellas y la luz resultante se registran como una imagen, dicha imagen identifica la huella de un individuo. Este tipo de sensor presenta problemas en la calidad de imagen de las huellas obtenidas, cuando los dedos están con polvo o húmedos. A su vez pueden presentar problemas con dedos con pieles deterioradas.
- Lectores de huellas dactilares ópticos transmisivos: es un tipo de sensor que no requiere el contacto directo del dedo con la

superficie que cubre el sensor. En este caso la luz atraviesa el dedo, a la vez que una cámara enfoca directamente la huella y captura una imagen. Este sensor es muy efectivo y es complicado de vulnerar.

- Lectores de huellas dactilares capacitivos: es un tipo de sensor que es un circuito de silicio, posee una superficie repleta de componente transductores. Estos componentes a su vez, poseen electrodos que son sensibles al contacto del dedo.
- Lectores de huellas dactilares mecánicos: es un tipo de sensor que posee miles de transductores de presión, estos están colocados sobre una superficie y reaccionan a la presión del dedo.
- Lectores de huellas dactilares térmicos: es un tipo de sensor que es capaz de detectar la temperatura del dedo y capta una imagen de la huella dactilar: Esto se debe a que las crestas poseen mayor temperatura que las partes llanas del dedo.

3.3.2.10 Tipos de fraudes en cajeros automáticos. El Banco de la Nación (2020) menciona los siguientes tipos de fraude:

- *Cambiao de Tarjeta*

Un cliente está cerca de un cajero automático y una persona se acerca (puede ser de cualquier sexo). Esta persona ofrece ayuda y a través de engaños logra confundir al usuario para cambiarle rápidamente su tarjeta por otra similar de la misma entidad financiera, usualmente es de otra víctima. Posterior, cuando el usuario intente realizar su operación, una tercera persona, que es cómplice, observará la clave secreta. Una vez que obtengan la tarjeta y la clave secreta estas personas realizan consumos y/o retiros fraudulentos. Esta modalidad también puede suceder cuando se van a realizar pagos en centros comerciales.

- *Accesorio en ATM – “Lazo libanes”*

Este tipo de fraude es usado en cajeros automáticos, donde personas inescrupulosas insertan un dispositivo dentro de la ranura del lector

de tarjetas. Posterior a ello se acerca un cómplice con el fin de observar la clave secreta. Al no poder recuperar la tarjeta del cajero, el cliente se retira convencido que la tarjeta quedo retenida. Luego, los delincuentes extraen la tarjeta del cajero y como ya conocen la clave realizan retiros o consumos fraudulentos.

- Clonación de Tarjeta

Es una modalidad que utilizan personas inescrupulosas cuando se realizan pagos con tu tarjeta en algún establecimiento comercial, sin que lo notes utilizan un pequeño dispositivo conocido como “skimmer” mediante el cual obtienen la información grabada en la banda magnética de tu tarjeta luego discretamente sin ser advertidos observan tu clave secreta, con esta información logran crear tarjetas “clonadas” o “mellizas” con las que posteriormente realizan consumos indebidos que afectan tu cuenta.

Esta modalidad también se puede presentar en los cajeros automáticos, donde se instalan dispositivos extraños en los lectores del cajero e instalan cámaras para filmar el momento que se digita la clave secreta.

Los tipos de fraude antes mencionados, tienen en común que los delincuentes deben obtener la tarjeta del cliente, ya sea con el método del cambiao, con un dispositivo que lo retenga o con la clonación. Esta propuesta agrega un sistema de validación biométrico, una vez implementado, para realizar alguna operación en cajero automático, el cliente debe estar presente y utilizar su huella.

Entonces con esta propuesta implementada se contrarrestaría los tipos de fraude: cambiao de tarjeta, lazo libanes y clonación de tarjeta.

3.3.2.11 DNI Electrónico. Según Perú (2018):

El DNI electrónico es una tarjeta inteligente que contiene un chip criptográfico con tres funciones:

- Aplicación avanzada de Identidad (en formato ICAO – Organización de Aviación Civil Internacional).

- Contar con una computadora con las siguientes características mínimas:
- Sistema Operativo Windows XP y Windows 7.
- Memoria RAM no menor de 512 MB.
- Contar con conexión a Internet (mínimo 512 Kbps).
- Espacio en disco duro mínimo 4 GB.
- Tener instalado el equipo biométrico y su licencia de codificación biométrica respectiva, de ser necesaria.

3.3.2.11.2 Características Técnicas mínimas del Lector Biométrico. Por cada estación que realice la consulta, la entidad debe adquirir un lector biométrico con las siguientes características:

- El lector debe contar con el certificado del FBI: PIV SINGLE FINGER CAPTURE DEVICES y deberá estar en el listado de dispositivos autorizados por el FBI.
- Debe ser compatible con los sistemas operativos Windows XP y Windows 7.
- El tipo de Lector debe ser mono dactilar para captura plana de impresiones dactilares.
- Contar con resolución de 500 dpi.
- Tener un área de captura mínima de 256 píxeles de ancho por 360 de alto y píxeles a 500 dpi.
- El área de captura debe garantizar una resolución forense de 500dpi.
- El tipo de sensor óptico debe ser de tipo CMOS o CCD.
- Debe generar imágenes en escala de grises de 256 tonos de 8 bits y ser de formato BMP.
- Contar con una conexión a PC mediante cable USB.

3.3.2.11.3 Características Técnicas Mínimas del Software de Codificación. Dado el caso que el lector biométrico no proporcione plantillas biométricas compatibles con el formato AFIS del RENIEC, el usuario deberá adquirir el software SDK y su licencia para codificar huellas biométricas, esta huella deberá ser almacenada en formato estándar ANSI/INCITS 378 o

ISO/IEC 19794-2. Este software SDK permitirá realizar la captura y posterior codificación biométrica, la licencia runtime permitirá el despliegue y ejecución de la aplicación desarrollada a partir del software SDK.

3.3.2.11.4 Sensor biométrico MorphoSmart300. Para Biotime Technology (2019):

Los dispositivos MorphoSmart son pequeños sensores biométricos USB de alta gama que permiten registrar, autenticar e identificar a los usuarios. El MorphoSmart 300 (MSO300) es un sensor de huella multiaplicación para una toma de huella de alta calidad, codificación de las platillas biométricas y comparación de empleos (en autenticación y en identificación).

Se usan tanto en grandes instituciones gubernamentales como en empresas comerciales o de industria. Se adaptan a todo tipo de ambiente y de usuarios (jóvenes, adultos mayores, obreros, etc.). La calidad de su toma de huella se ha reforzado con una superficie de captura más amplia.

En la (figura 5) se observa un lector de huella digital MorphoSmart 300.



Figura 5: MorphoSmart 300. Fuente: Biotime Technology-2019.

Características técnicas:

- Velocidad de autenticación menor a 0.7s.
- Superficie de captura 23 por 23 mm y 500 dpi.
- Velocidad de identificación menor a 0.9 s en 1 por 1000.
- Formatos de plantillas: ANSI/INCITS 378, ISO 19794-2, ISO19794-4.
- Certificación PIV IQS del FBI para calidad de imagen, algoritmos conformes a FIPS 201, MINEX, STQC.
- Lectores de tarjetas con chip, seguridad contra dedos falsos, protección de la comunicación entre el host y el sensor.
- Capacidad mínima de 500 hasta 5000 usuarios en la base de datos.
- SDK disponible para la creación de aplicaciones.
- La precisión FAR, tasa de aceptación falsa, debe ser ajustable hasta 10^{-8} dependiendo del grado de seguridad que se requiera.

Este dispositivo es el que se usara en la estimación de costos debido a que cumple todos los requisitos para acceder al servicio de verificación biométrica de la RENIEC.

3.3.2.12 Servidor dedicado, virtual (VPS) y Cloud. Para Clavei (2018): Respecto al servidor dedicado y virtual, tienen similitudes, cada uno se adapta según para el tamaño de proyecto que se necesite, se debe ajustar a las necesidades y/o requisitos del proyecto o diseño. Un servidor es un tipo de computador que cumple la función de gestionar, almacenar y procesar información, brindara las respuestas a las peticiones que realicen los usuarios desde sus equipos. A continuación, definimos el servidor virtual y servidor dedicado.

•Servidor Dedicado

El servidor dedicado es también llamado servidor físico, debido a que como su nombre lo menciona es palpable y ocupara un espacio en el lugar donde se desee instalar. Es un conjunto de hardware y software concretos.

- Servidor virtual VPS

Las siglas VPS son de “Virtual Private Server”, un servidor virtual, no físico. Se trata de una instalación de software realizada sobre un servidor físico; este servidor físico puede alojar diferentes virtuales que comparten entre sí el hardware y los recursos, pero su funcionamiento es completamente independiente. Los servidores virtuales permiten ahorrar en costos si se requiere varios servidores, ya que se puede tener varios virtuales dentro de uno físico.

- Servidores Cloud

Este tipo de servidor, que cobra cada día más relevancia, son los servidores en la nube. Su principal ventaja, su escalabilidad en tiempo real; estos servidores se adaptan a las necesidades al momento, con redundancia de datos y difícilmente presenta caídas, al funcionar sobre diferentes servidores simultáneamente.

- ¿Cuál elegir entre servidor virtual o dedicado?

Depende de la necesidad. Para entornos de prueba o primeras fases de un proyecto, sin duda lo ideal serían uno virtual; además, una gran ventaja que se tiene con los virtuales es su facilidad para migrarlo a uno superior manteniendo todo el sistema tal cual. Por otro lado, los servidores dedicados están más enfocados a grandes proyectos, que necesitan de muchos recursos, un gran control sobre estos o cuando se requiera desplegar varios subproyectos; montando varios virtuales dentro de uno dedicado.

De acuerdo a estas definiciones y ya que este proyecto está orientado a la red de cajeros automáticos en todo el país, se utilizará servidores dedicados.

3.4 Procedimiento

3.4.1 Tipo de investigación

El presente trabajo es de tipo descriptivo.

3.4.2 Diseño de la investigación

El diseño comprende analizar las características técnicas, tomando en cuenta la situación actual del Banco de la Nación y la infraestructura adicional necesaria para la implementación del sistema biométrico en los cajeros automáticos.

Se tendrá como modelo la plataforma ya implementada de lector biométrico por huella dactilar para ventanillas de las agencias del Banco en el año 2017, debido a que esta plataforma tuvo un proceso exitoso de adecuación con la infraestructura y mainframe del Banco.

3.4.2.1 Situación actual del Banco de la Nación. El Banco de la Nación provee servicios a las entidades del estado, promueve la inclusión y la bancarización financiera en beneficio de la ciudadanía complementando al sector privado. Impulsa que el país crezca descentralizadamente, mediante una gestión auto-sostenible y eficiente. Actualmente brinda sus servicios a través de los siguientes canales de atención:

- 1 Agencias.
- 2 Agentes.
- 3 Cajeros automáticos.
- 4 Banca por internet.
- 5 Banca móvil.

Hoy en día el Banco posee una infraestructura tecnológica que le permite dar un óptimo servicio a todos sus clientes. Para conseguir este

propósito el Banco de la Nación posee la tecnología óptima y constantemente desarrolla proyectos de. Según el Banco de la Nación (2016):

La infraestructura de cómputo se basa en un equipo IBM de la serie z/BC12-2828 que da soporte al Core Bancario y a la red de Teleproceso, los cuales cuentan con canales en línea la atención al público usuario; adicionalmente con herramientas de monitoreo que permiten prevenir y actuar proactivamente como parte del soporte al Core bancario.

La red que actualmente soporta la red de cajeros automáticos, se encuentra balanceada a nivel de configuración en 2 computadores de alta disponibilidad.

3.4.2.2 Infraestructura. Se usará los siguientes componentes de software y hardware:

- **Agente Biométrico (Biomatch):** En la actualidad es el Software Gestor de Huellas encargado de la integración del sistema biométrico con la plataforma Saraweb (Plataforma propia de las agencias del Banco). El objetivo será desplegar otro gestor similar que cumpla la función de integración del sistema biométrico con el computador controlador de cajeros automáticos.
- **Central de huellas (Gateway Biométrico):** En esta plataforma (Base de datos centralizada del Banco) ya está grabada la información de huellas dactilares asociada al DNI del cliente (validadas por RENIEC). Se tendrá que implementar una réplica a este servidor para dar servicio dedicado a la red de cajeros automáticos.
- **Monitor Biométrico:** Actualmente se guarda en este aplicativo los registros y consultas de auditoría de las operaciones biométricas realizadas en las agencias. Se tendrá otro aplicativo igual para guardar los registros y consultas en operaciones biométricas en cajeros automáticos.
- **Lector Biométrico:** Equipo biométrico de captura de huellas de la marca: Morpho.

3.4.2.2.1 **Agente Biométrico.** Según el Banco de la Nación (2017):

El Software Gestor de Huellas será desplegado en un servidor de aplicaciones y permitirá utilizar las funcionalidades siguientes:

- Captura de huellas.
 - ✓ El agente biométrico expone como servicio la captura de huellas, considerando como parámetros de entrada: Marca del equipo biométrico.
 - ✓ El agente biométrico realiza un test de conexión con el equipo biométrico.
 - ✓ El agente biométrico permite el control de calidad de la imagen a capturar.
 - ✓ El agente biométrico captura la huella dactilar.
 - ✓ El agente biométrico genera plantillas biométricas en formato Morpho, para los equipos Morpho.
 - ✓ El agente biométrico obtiene la imagen de la huella en formato WSQ, para cualquier otro equipo que no sea Morpho.
 - ✓ El agente biométrico genera plantillas biométricas en formato estándar ISO19794-2, para el DNle.
- Grabar las huellas de los usuarios en la base de datos centralizada.
- Validar huellas capturadas con huellas de la base de datos.
 - ✓ El agente biométrico realiza una solicitud de contrastación de huella dactilar capturada con huellas dactilares de la base de datos al Servidor Central de Huellas, considerando como parámetros: DNI e índice requerido (derecho o izquierdo).
- Validación de huella capturada con huella del chip de Tarjeta EMV o DNle.
 - ✓ El agente biométrico realiza una validación de la huella capturada con la huella del chip de tarjeta EMV o DNle en la tarjeta, considerando como parámetros: DNI e índice requerido (derecho o izquierdo)
 - ✓ El agente biométrico obtiene el Nro. De DNI (CIU) del DNle.
- Validación de huella con servicio en línea de RENIEC.

- ✓ El agente biométrico realiza una solicitud de validación de huella capturada con el servicio línea del RENIEC, considerando como parámetros: DNI e índice requerido (derecho o izquierdo)
- ✓ El Agente biométrico encripta la huella con una clave definida por el banco.
- Registro de auditoría del uso de las funcionalidades.
- Módulo de Log de consultas de auditoría.
- Módulo de Log que guarda las estadísticas y operaciones de las funcionalidades que fueron ejecutadas.
- Módulo de seguridad que guarda los registros de accesos a los módulos.
- Autenticación para usar las funcionalidades.
- Contador de errores por validaciones fallidas.
- Capacidad de portabilidad de los servicios para ser utilizados en equipos externos (OFF LINE): PC, Laptop, entre otros.
- Capacidad de integrarse con servicios externos para el envío y validación de la huella capturada.
- Capacidad de integrarse con equipos externos para la ejecución de comandos APDU alojados en el chip de una tarjeta EMV o DNle.

3.4.2.2.2 Central de huellas (Gateway Biométrico). Para el Banco de la Nación (2017): Es la plataforma que cuenta con las siguientes funcionalidades:

- El Gateway biométrico recibe una solicitud de validación de la huella dactilar capturada con huellas dactilares de la base de datos al Servidor Central de Huellas, considerando como parámetros: DNI e índice requerido (derecho o izquierdo).
- El Gateway biométrico recibe una solicitud de validación de huella capturada con el servicio en línea del RENIEC, considerando como parámetros: DNI e índice requerido (derecho o izquierdo).

- El Gateway biométrico expone como servicio la contratación de huellas dactilares capturadas con huellas dactilares de la base de datos.
- El Gateway biométrico expone como servicio la validación de huella con servicio en línea de RENIEC.
- El Gateway biométrico descripta la huella con una clave definida por el banco.
- El Gateway biométrico expone como servicio el registro de las huellas dactilares en la base de datos.
- El Gateway biométrico graba las huellas dactilares en la base de datos centralizada.
- El Gateway biométrico graba la huella encriptada.
- El Gateway biométrico guarda los registros de auditoría de las transacciones efectuadas.

3.4.2.2.3 Monitor Biométrico. Según el Banco de la Nación (2017):

Aplicativo que cuenta con las siguientes características:

- El Monitor de Biometría registra las transacciones realizadas el Central de Huellas (Gateway Biométrico).
- El Monitor de Biometría muestra todo el detalle de un registro en el Central de Huellas (Gateway Biométrico) de acuerdo a los filtros de búsqueda ingresados.
- El Monitor de Biometría muestra información resumen de acuerdo a los criterios de agrupación y filtros de búsqueda ingresados.
- El Monitor de Biometría muestra información de la huella “Enrolada” por persona asociado a un documento de identidad.

El módulo de seguridad del Monitor de Biometría es capaz de integrarse con el computador controlador de cajeros automáticos del Banco.

3.4.2.3 Modelo de paquetes. En la (figura 6) se muestra el diagrama de paquetes.



Figura 6: Diagrama de paquetes. Fuente: Banco de la Nación (2017) y elaboración propia.

3.4.2.4 Modelo de Casos de Uso. En las (figuras 7, 8 y 9) se muestran los diagramas caso de uso del agente biométrico.

▪ **AGENTE BIOMÉTRICO (BIOMATCH)**

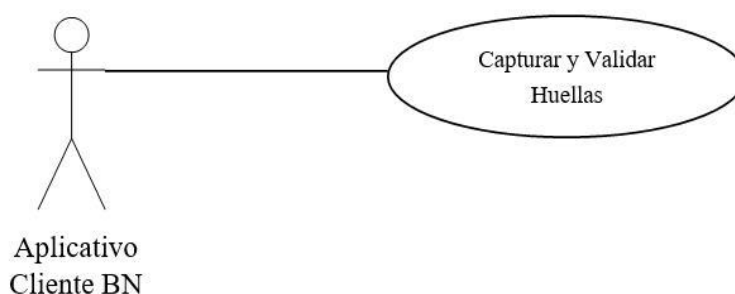


Figura 7: Diagrama caso de uso – Agente Biométrico (Capturar y Validar Huellas). Fuente: Banco de la Nación (2017).

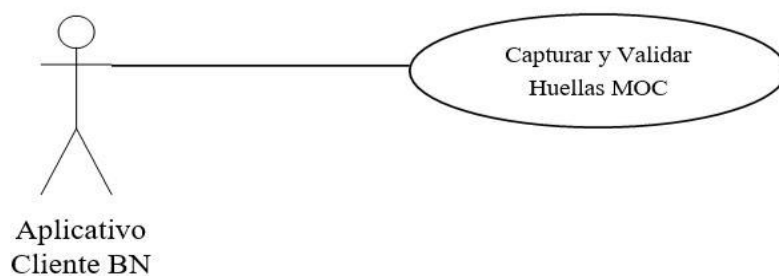


Figura 8: Diagrama caso de uso – Agente Biométrico (Capturar y Validar Huellas MOC). Fuente: Banco de la Nación (2017).

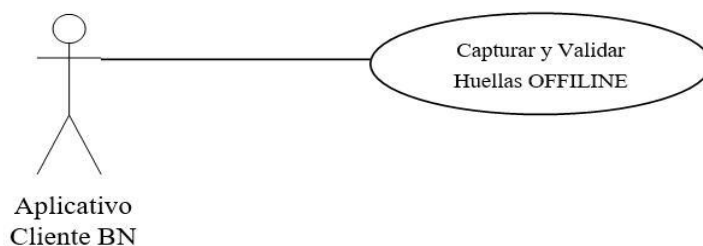


Figura 9: Diagrama caso de uso – Agente Biométrico (Capturar y Validar Huellas Transacciones OFFLINE). Fuente: Banco de la Nación (2017).

▪ CENTRAL DE HUELLAS (GATEWAY BIOMÉTRICO)

En la (figura 10) se observa el diagrama caso de uso de la central de huellas.

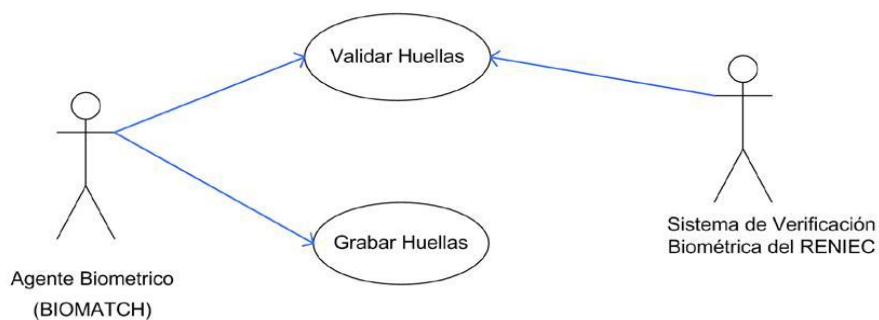


Figura 10: Diagrama caso de uso – Central de Huellas. Fuente: Banco de la Nación (2017).

▪ MONITOR DE BIOMETRÍA

En la (figura 11) se muestra el diagrama caso de uso del monitor de biometría.

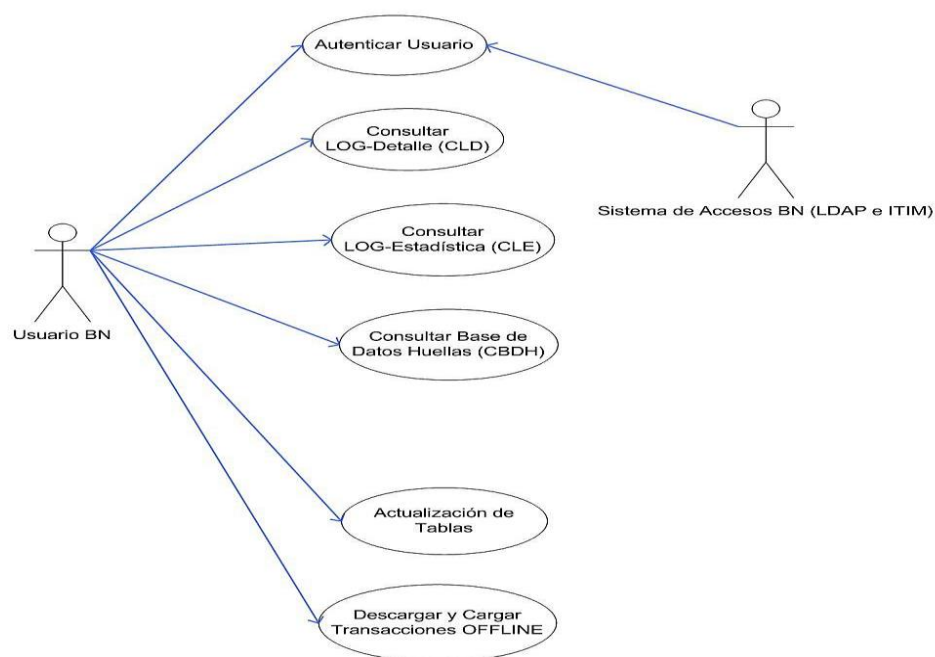


Figura 11: Diagrama caso de uso – Monitor de Biometría. Fuente: Banco de la Nación (2017).

3.4.2.5 Actores y Casos de uso. En la (tabla 4) se muestra la descripción de actores.

TABLA 4: Descripción de actores.

Actor	Descripción
Aplicativo BN	Este actor representa a los aplicativos del Banco que consumirán los servicios y funcionalidades del Agente Biométrico (Biomatch).
Agente Biométrico	Este actor representa el Agente Biométrico que consumirá los servicios de la Central de Huellas (Gateway Biométrico).
Usuario BN	Este actor representa a los usuarios del BN que accederán a la aplicación web Monitor de Biometría, estos usuarios ingresarán con determinados perfiles.

Fuente: Banco de la Nación (2017) y elaboración propia

En la (tabla 5) se observa la descripción de casos de uso.

TABLA 5: Descripción de casos de uso.

Casos de uso	Descripción
Capturar Huellas – Agente Biométrico	La captura de huellas del Agente Biométrico (Biomatch) es el encargado de realizar la captura de huellas y generación imagen o plantillas biométricas de acuerdo al tipo de lector biométrico que realiza la captura.
Validar Huellas – Agente Biométrico	La validación de huellas del Agente Biométrico (Biomatch) en el encargado de enviar y recibir la información necesaria al central de Huellas (Gateway Biométrico), en el caso de la huella, esta será encriptada antes de ser enviada. Si se indica que es una validación con DNle, la validación se realizará localmente.
Validar Huellas – Central de Huellas	La validación de huellas del Central de Huellas (Gateway Biométrico) es el encargado de realizar las siguientes validaciones, según sea la solicitud del Agente Biométrico: - Contrastación de huella dactilar capturada con las huellas dactilares de la base de datos al Servidor Central de Huellas, si no

	encontrase registro, se invocará la validación de huellas con el servicio en línea del RENIEC. - Validación de huella capturada con el servicio en línea del RENIEC.
Grabar Huellas – Central de Huellas	El grabado de las huellas del Central de Huellas (Gateway Biométrico) es el encargado de guardar la huella encriptada cuando se registra una nueva persona y de todas las transacción realizadas en el Software Gestor de Huellas.
Autenticar Usuario – Monitor de Biometría	La autenticación del usuario se realizará a través de la integración con la solución Active Directory e ITIM del Banco de la Nación, para acceder a la aplicación Web Monitor de Biometría.
Consultar LOG-Detalle (CLD)	Consultar Log- Detalle permite mostrar todo el detalle de un registro de acuerdo a los filtros de búsqueda ingresados.
Consultar LOG- Estadística (CLE)	Consultar Log-estadística permite mostrar información resumen de acuerdo a los criterios de agrupación y filtros de búsqueda ingresados.
Consultar Base de Datos Huellas (CBDH)	Consultar Base de Datos Huella permite mostrar información de la huella “Enrolada” ´por persona asociado a un documento de

	identidad.
Actualización de Tablas	La Actualización de tablas permite crear/editar/buscar los datos de las tablas que permiten la configuración de sistemas, oficinas y usuarios.
Descargar y Cargar transacciones Offline	Descargar Transacciones Offline: Permite registrar los datos del proceso Offline. Seguidamente cargar los DNIs desde un archivo y actualizar el detalle del proceso con los DNIs existentes en el archivo. Cargar Resultados Transacciones Offline: Permite listar el detalle de los procesos, así como generar los archivos de las plantillas a descargar, descargar los archivos generados. Luego permite cargar y procesar los archivos generados por las validaciones realizadas con el biomatch.

Fuente: Banco de la Nación (2017) y elaboración propia

3.4.2.6 Representación de la Arquitectura. A continuación, se muestra el conjunto de servidores que son la base de la arquitectura de este proyecto. Para que la plataforma soporte la carga de los cajeros de la red del Banco de la Nación, se considera los servidores: balanceador, HTTP y WAS con las siguientes características.

En la (figura 12) se muestra los servidores de la arquitectura.

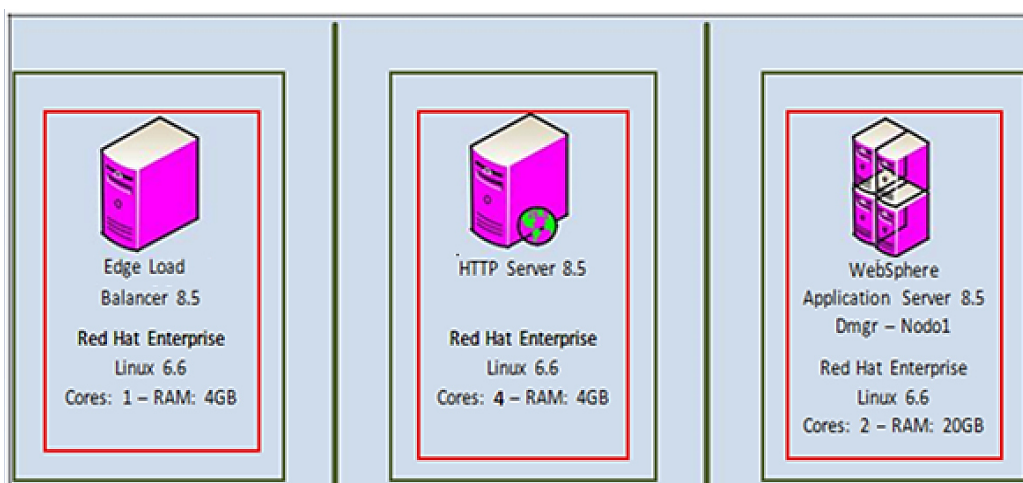


Figura 12: Servidores de la arquitectura. Fuente: Banco de la Nación (2017) y elaboración propia.

Además de estos servidores se necesitará un servidor base de datos. Ahora, se mostrará un gráfico de la arquitectura básica que tendrá el sistema biométrico para cajeros automáticos. En la (figura 13) se muestra la arquitectura básica del sistema biométrico para cajeros automáticos.

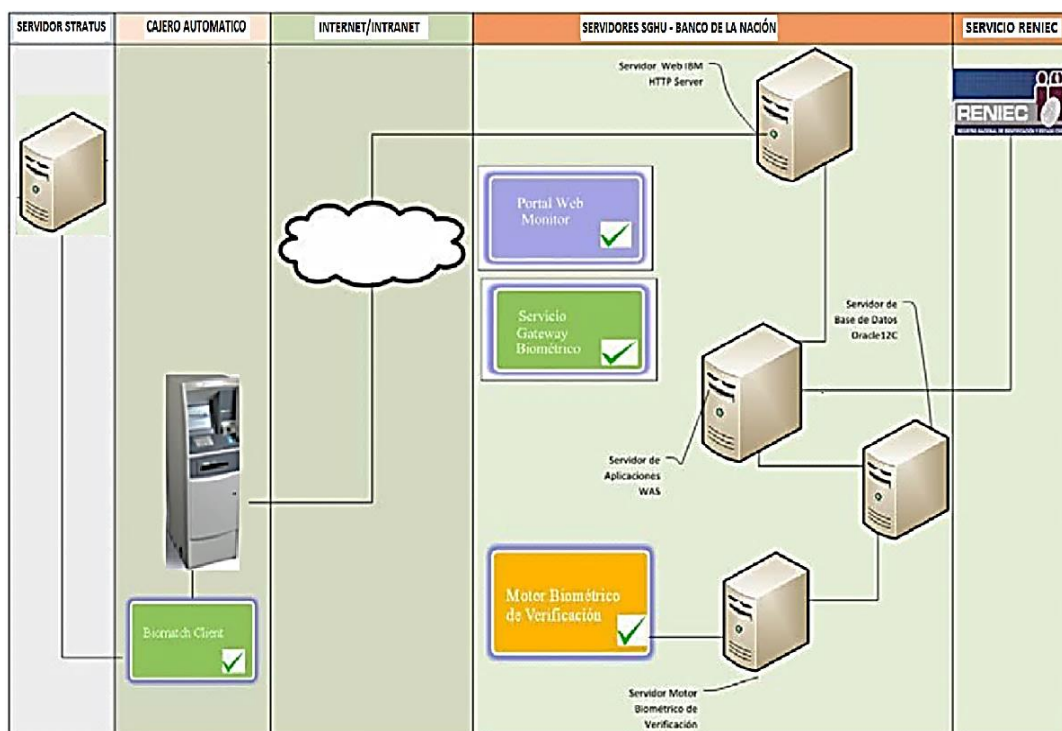


Figura 13: Arquitectura básica del sistema biométrico para cajeros automáticos. Fuente: Banco de la Nación (2017) y elaboración propia.

3.4.2.7 Vista General de la Arquitectura de Desarrollo. La (figura 14) muestra una visión general de la arquitectura de desarrollo donde se observa la distribución en tres capas.

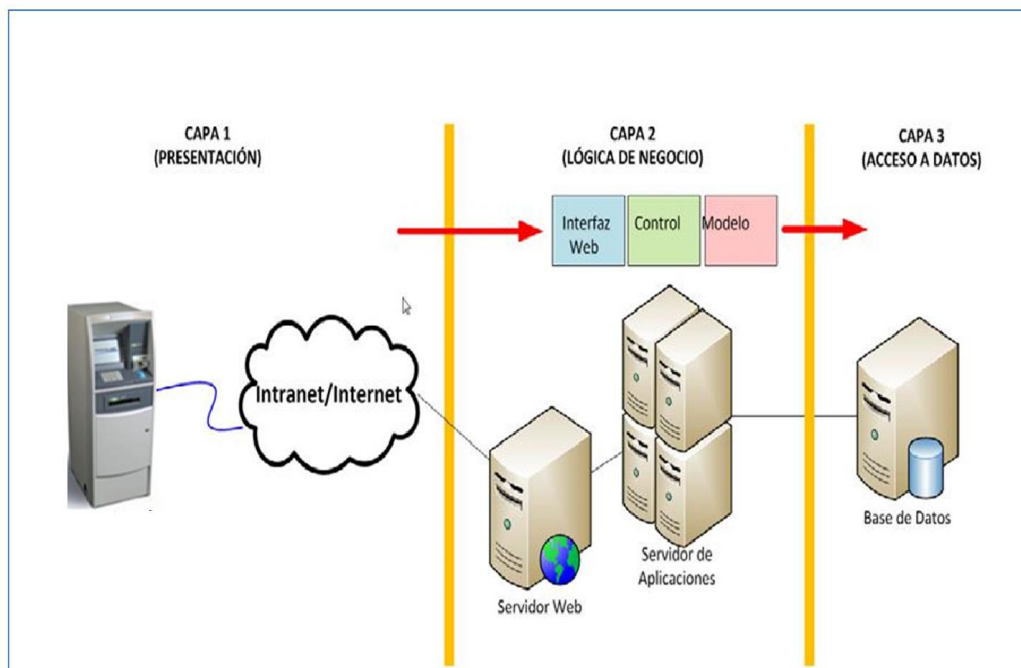


Figura 14: Vista General de la Arquitectura de Desarrollo.

Fuente: Banco de la Nación (2017) y elaboración propia.

El Banco de la Nación (2017) define estos tres niveles o capas de la siguiente manera:

- **Nivel 1: Presentación**

En este nivel está la aplicación Web que se encarga de la presentación de los sistemas de la solución, estará integrada de las pantallas de presentación.

- **Nivel 2: Lógica de Negocio**

Este nivel proporciona todo lo referente a las reglas del negocio, en concreto brinda la funcionalidad de los sistemas de la solución.

- **Nivel 3: Acceso a dato**

Este nivel proporciona los servicios y las conexiones a la base de datos que son requeridos por el novel de Lógica de Negocio.

3.4.2.8 Generalidades

3.4.2.8.1 Vista Lógica del BiomatchClient. La figura (15) muestra la vista lógica de BiomatchClient y brinda una idea clara de la distribución de las capas y las interfaces de este componente.

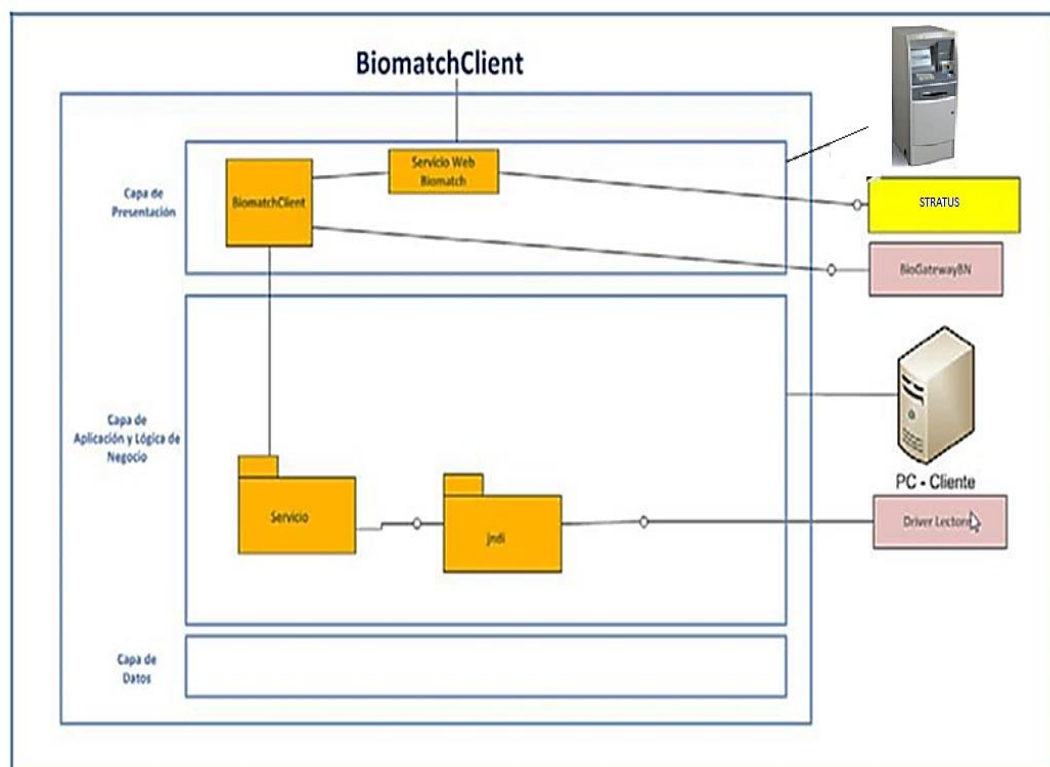


Figura 15: Vista Lógica de BiomatchClient. Fuente: Banco de la Nación (2017) y elaboración propia.

3.4.2.8.2 Vista Lógica del Gateway Biométrico. La (figura 16) muestra la vista lógica del Gateway biométrico y brinda una idea clara de la distribución de las capas y las interfaces de este componente.

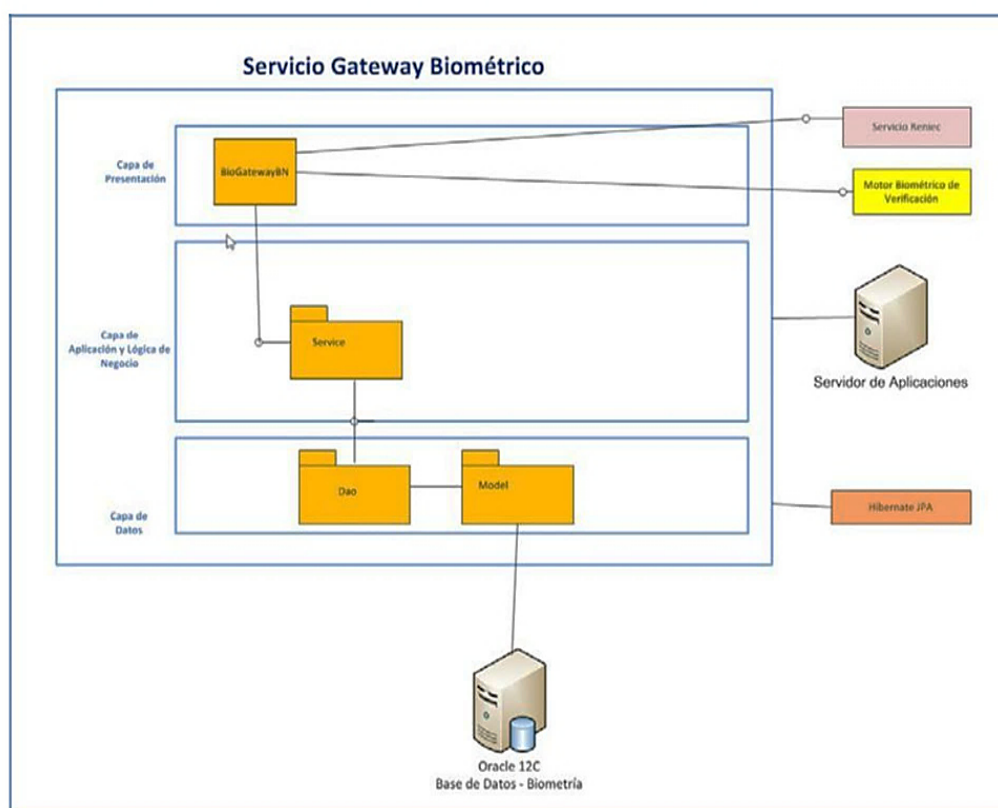


Figura 16: Vista Lógica del Gateway Biométrico. Fuente: Banco de la Nación (2017) y elaboración propia.

3.4.2.8.3 Vista Lógica del Portal Web Monitor. La (figura 17) muestra la vista lógica del portal monitor web y brinda una idea clara de la distribución de las capas y las interfaces de este componente.

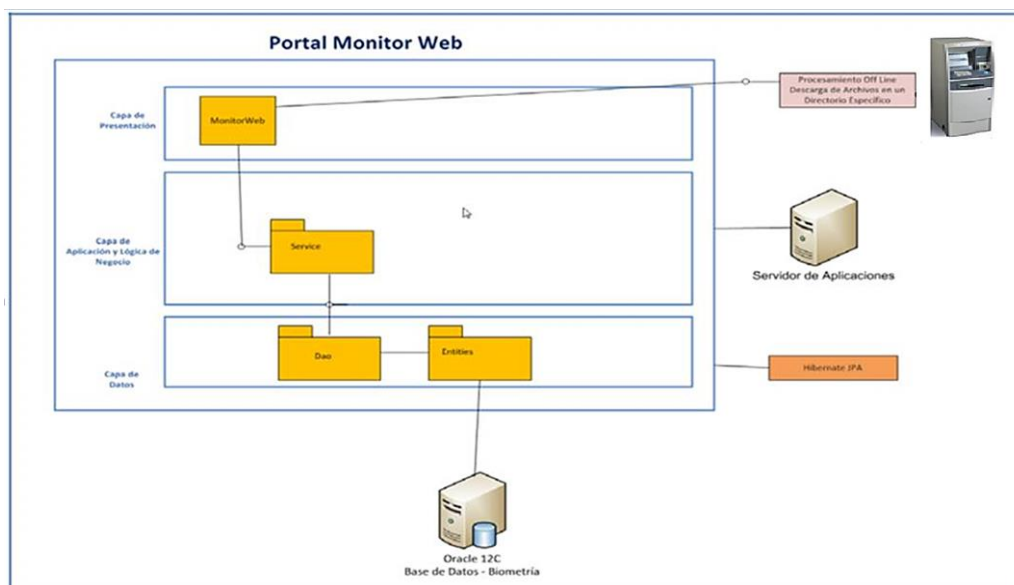


Figura 17: Vista Lógica del Portal Monitor Web. Fuente: Banco de la Nación (2017) y elaboración propia.

3.4.2.8.4 Vista Lógica Motor Biométrico Moo. La (figura 18) muestra la vista lógica del motor biométrico Moo y brinda una idea clara de la distribución de las capas y las interfaces de este componente.

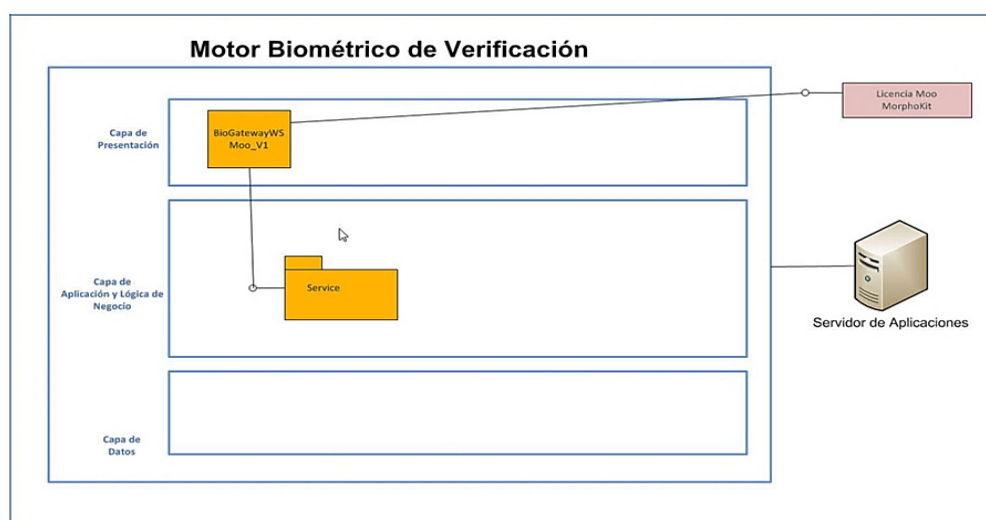


Figura 18: Vista Lógica Motor Biométrico Moo. Fuente: Banco de la Nación (2017).

3.4.2.9 Paquetes de Diseño Arquitectónicamente Significativos. En la (figura 19) se muestra los paquetes de diseño.

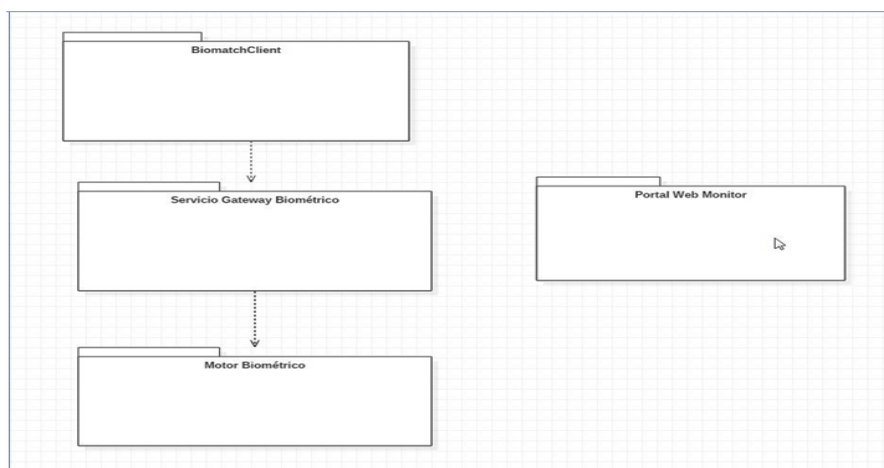


Figura 19: Paquetes de diseño. Fuente: Banco de la Nación (2017).

3.4.2.9.1 Paquete BiomatchClient. En la (figura 20) se muestra los paquetes de diseño del Biomatch Client.

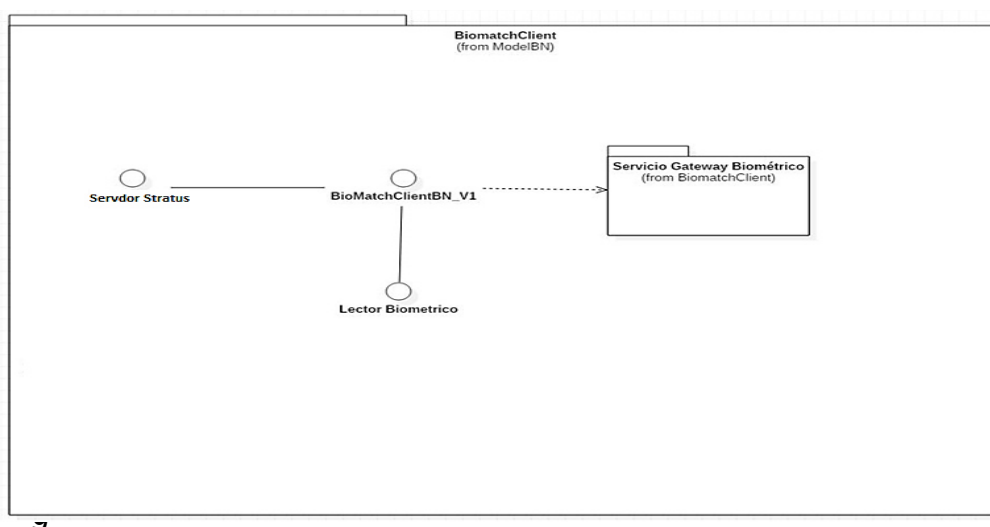


Figura 20: Paquetes de diseño del Biomatch Client. Fuente: Banco de la Nación (2017) y elaboración propia.

3.4.2.9.2 Paquete Servicio Gateway Biométrico. En la (figura 21) se observa los paquetes de diseño del servicio Gateway biométrico.

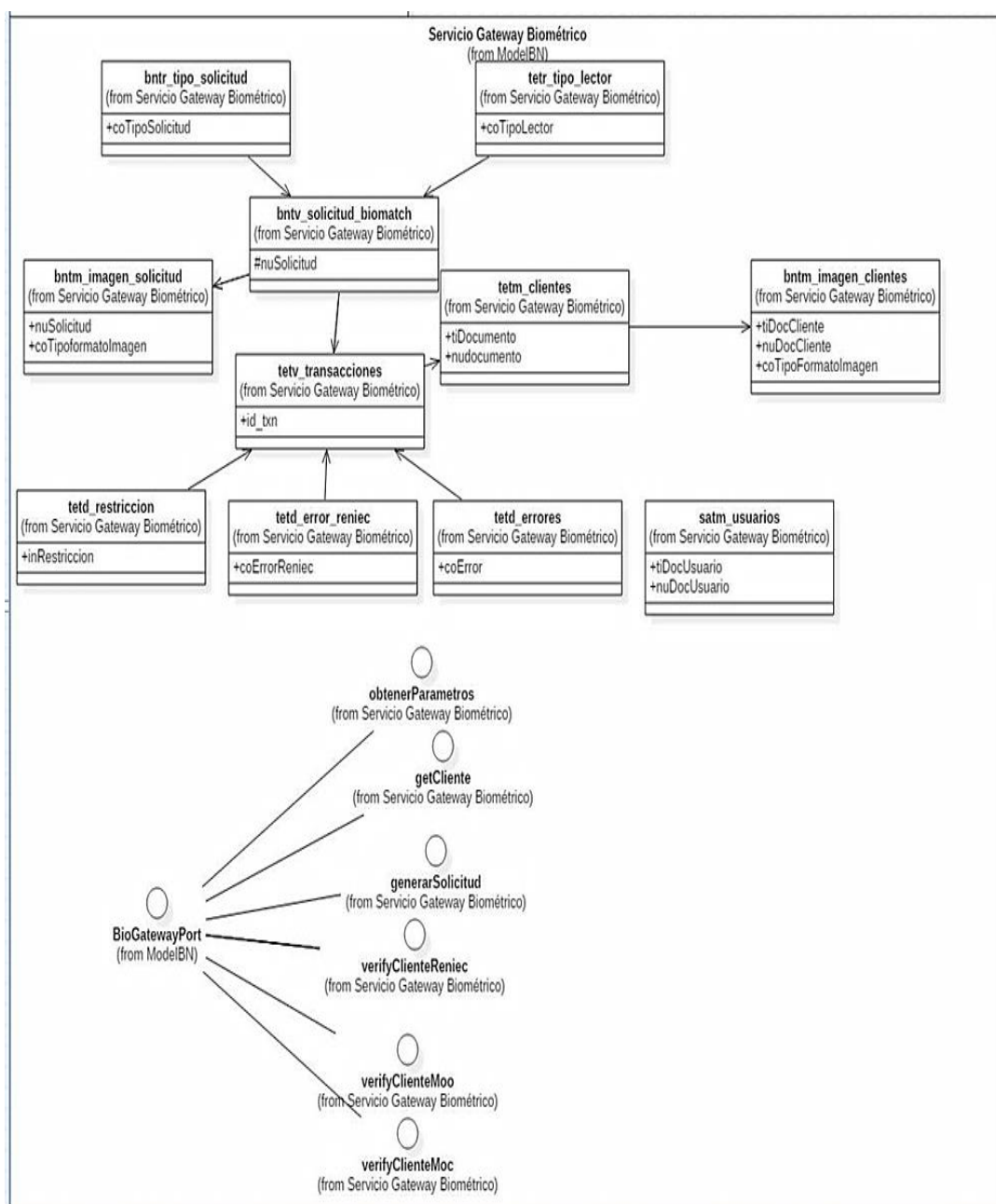


Figura 21: Paquetes de diseño Servicio Gateway Biométrico.

Fuente: Banco de la Nación (2017) y elaboración propia.

3.4.2.9.3 Paquete Servicio Portal Web Monitor. En la (figura 22) se muestra los paquetes de diseño del portal monitor web.

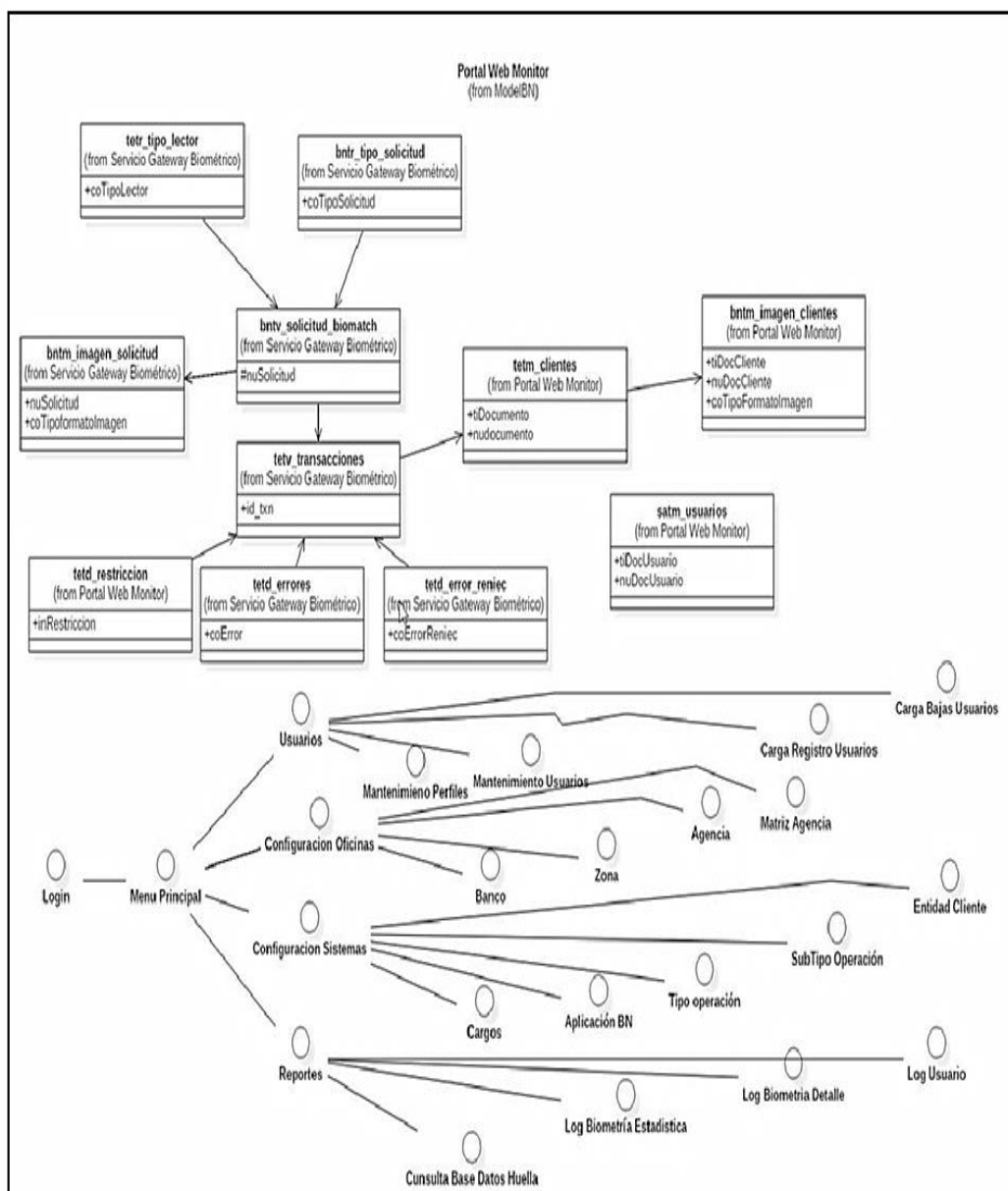


Figura 22: Paquetes de diseño Portal Monitor Web. Fuente: Banco de la Nación (2017) y elaboración propia.

3.4.2.9.4 Paquete Motor Biométrico. En la (figura 23) se observa los paquetes de diseño del motor biométrico.

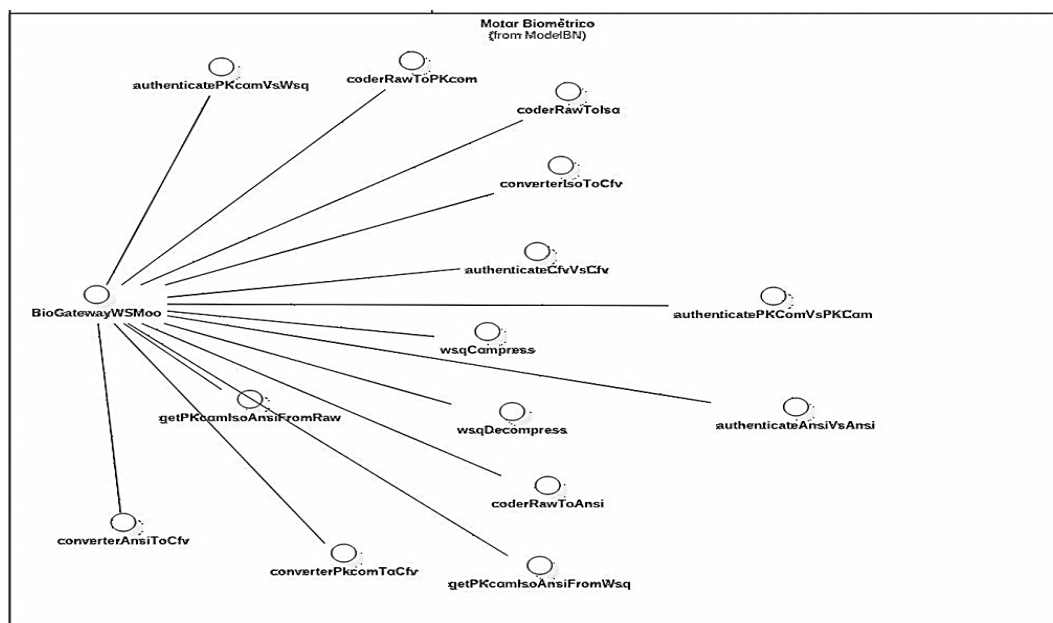


Figura 23: Paquetes de diseño Motor Biométrico. Fuente: Banco de la Nación (2017).

3.4.2.10 Interpretaciones de los Casos de Uso. En la (figura 24) se muestra la interpretación general de los casos de uso.

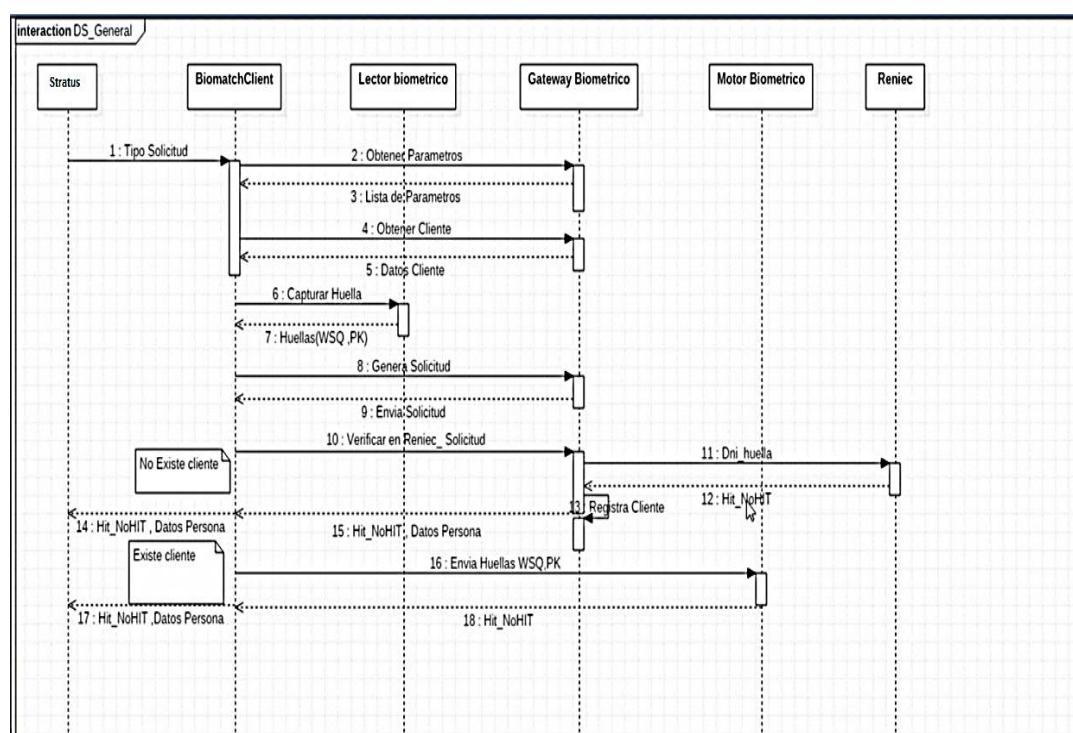


Figura 24: Interpretación General de los Casos de Uso. Fuente: Banco de la Nación (2017).

3.4.2.11 Vista de Procesos. En la (tabla 6) se muestra los procesos Biomatch Client.

TABLA 6: Procesos Biomatch Client.

BiomatchClient	
Descripción de los procesos del componente BiomatchClient	
Nro.	Descripción
1	Las aplicaciones del Banco de la Nación invocan pasando parámetros
2	Obtener Parámetros, invoca al Servicio Web Biométrico
3	Generar Solicitud, invoca al Servicio Web Biométrico
4	Obtener datos del cliente , invoca al Servicio Web Biométrico
5	Capturar Huella
6	Enviar datos y Huellas , invoca al Servicio Web Biométrico
7	Compara Huella , Local cuando la solicitud es una verificación Moc , invoca al servicio web biométrico

Fuente: Banco de la Nación (2017)

En la (tabla 7) se muestra los procesos servicios gateway biometrico.

TABLA 7: Procesos Servicios Gateway Biométrico.

Servicio Gateway Biométrico	
Descripción de los procesos del componente Servicio Gateway Biométrico	
Nro.	Descripción
1	Expone el método <code>obtenerParametros</code>
2	Obtiene los parámetros de la base de datos y los devuelve un objeto <code>OutputBean</code>
3	Expone el método <code>generarSolicitud</code>
4	Inserta en la base de datos las invocaciones de las solicitud realizadas por el componente <code>Biomatchclient</code> , devuelve un objeto <code>OutputBean</code>
5	Expone el método <code>getClient</code>
6	Obtiene los datos del Cliente de la base de datos y devuelve en un objeto <code>bioResponseExt</code>
7	Expone el método <code>verifyClienteReniec</code>
8	Encripta las huellas las huellas
9	Invocar al servicio web de Reniec
10	Insertar como cliente en la base de datos para los casos cuyo resultado sea HIT
11	Devuelve el resultado al componente Biomatch
12	Expone el método <code>verifyClienteMoo</code>
13	Invoca al componente Servicio Motor Biométrico
14	Registra movimiento en la base de datos
15	Expone el método <code>verifyClienteMoc</code>
16	Registra movimiento en la Base de Datos

Fuente: Banco de la Nación (2017) y elaboración propia

En la (tabla 8) se muestra los procesos del motor biométrico.

TABLA 8: Procesos Motor Biométrico.

Servicio Web Motor Biométrico	
Descripción de los procesos del componente Servicio Web Motor Biométrico	
Nro.	Descripción
1	Expone los métodos (coderRawToIso, converterIsoToCfv, authenticateCfvVsCfv, wsqCompress, wsqDecompress, coderRawToAnsi, coderRawToPKcom, getPKcomIsoAnsiFromWsq, getPKcomIsoAnsiFromRaw, authenticatePKcomVsWsq, converterAnsiToCfv, converterPkcomToCfv, authenticatePKComVsPKCom, authenticateAnsiVsAnsi)
2	Convierte y transforma las plantillas a formatos comparables
3	Compara las plantillas
4	Devuelve resultados de comparación

Fuente: Banco de la Nación (2017)

En la (tabla 9) se muestra los procesos del portal monitor web.

TABLA 9: Procesos Portal Monitor Web.

Portal Monitor Web	
Descripción de los procesos del componente Servicio Web Motor Biométrico	
Nro.	Descripción
1	Autentica usuarios con el LDAP
2	Registra Usuarios
3	Registra perfiles
4	Cargar Masiva de Usuarios
5	Baja Masiva de Usuarios
6	Registra Oficinas
7	Registra Banco
8	Registra Zona
9	Registra Agencia
10	Mantener Aplicaciones BN
11	Mantener Tipos de Aplicación
12	Mantener Sub Tipos de Operación
13	Mantener Entidad Clientes
14	Generar Reportes de Consulta de Base de datos de Huella
15	Generar Reportes de Log de Biometría Estadística
16	Genera Reporte Log Biometría Detalle
17	Genera Reporte de Log de Usuario

Fuente: Banco de la Nación (2017)

3.4.2.12 Vista Básica de Despliegue. En la (figura 25) se muestra la vista básica de despliegue de componentes que comprenderá la solución biométrica.

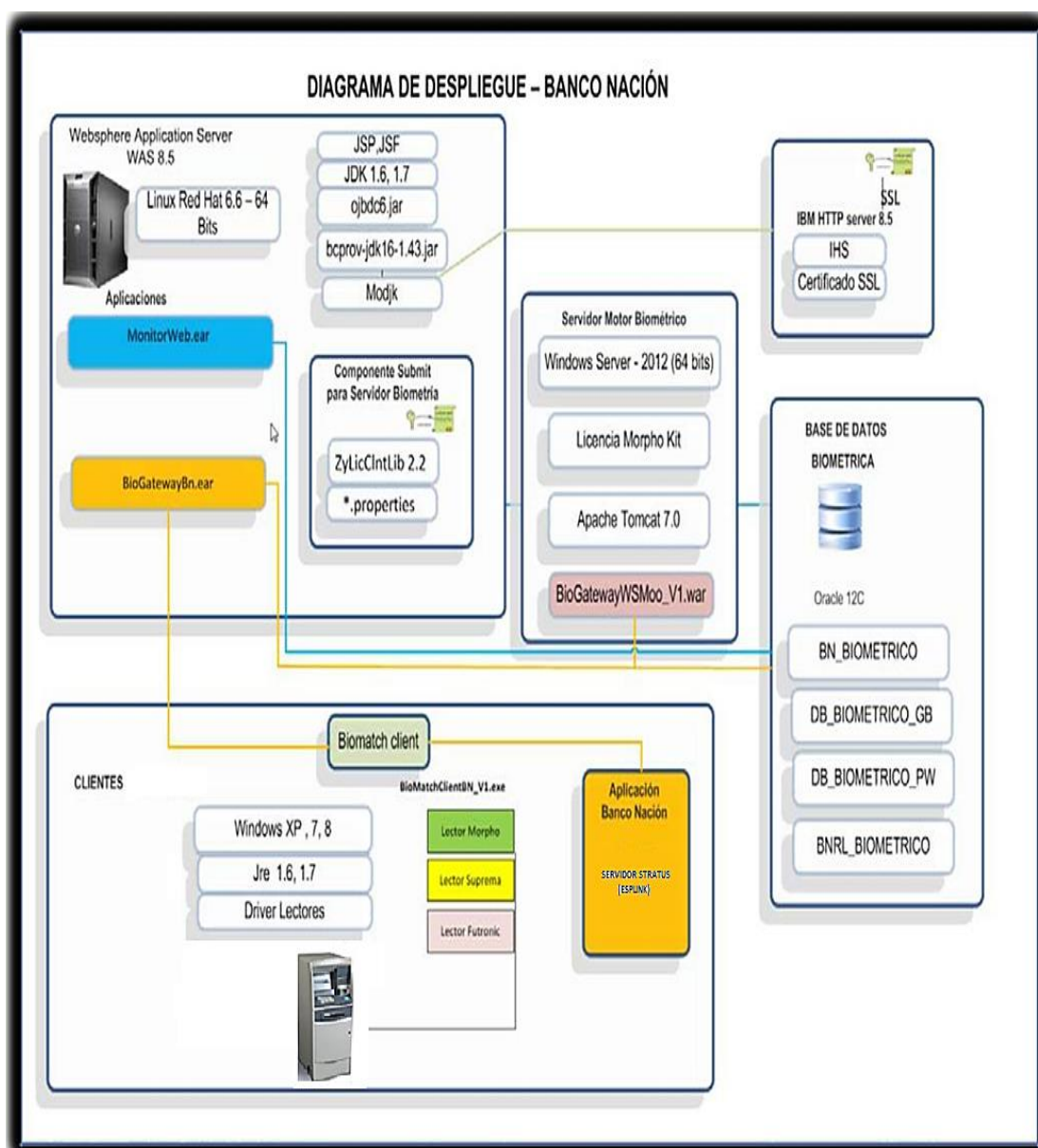


Figura 25: Vista Básica de Despliegue. Fuente: Banco de la Nación (2017) y elaboración propia.

El Banco de la Nación (2017) define:

3.4.2.12.1 Websphere Application Server WAS 8.5. Servidor de aplicaciones donde se desplegarán los archivos. ear de las aplicaciones y servicios web.

3.4.2.12.2 Linux Red Hat 6.6 – 64 Bits. Sistema Operativo del Servidor de aplicaciones.

3.4.2.12.3 MonitorWeb.ear. Aplicación de Monitoreo y generación de reportes de transacciones.

3.4.2.12.4 BioGatewayBn.ear. Servicio Web Biométrico que interactuará con el Biomatch Client y el Servidor del Motor biométrico. Este servicio enviará las huellas a RENIEC.

3.4.2.12.5 BioGatewayWsMoo_V1.ear. Servicio Web de Verificación biométrica que permitirá realizar las validaciones biométricas localmente.

3.4.2.12.6 ZyLicCIntLib2.2. Componente de licenciamiento para realizar las validaciones biométricas.

3.4.2.12.7 Biomatch Client (BiomatchClient_V1.ear). Componente que interactuará con las aplicaciones del Banco de la Nación y también permitirá realizar la captura de las huellas a través de los lectores biométricos.

3.4.2.13 Vista de Implementación. La (figura 26) muestra la vista de implementación de la solución biométrica.

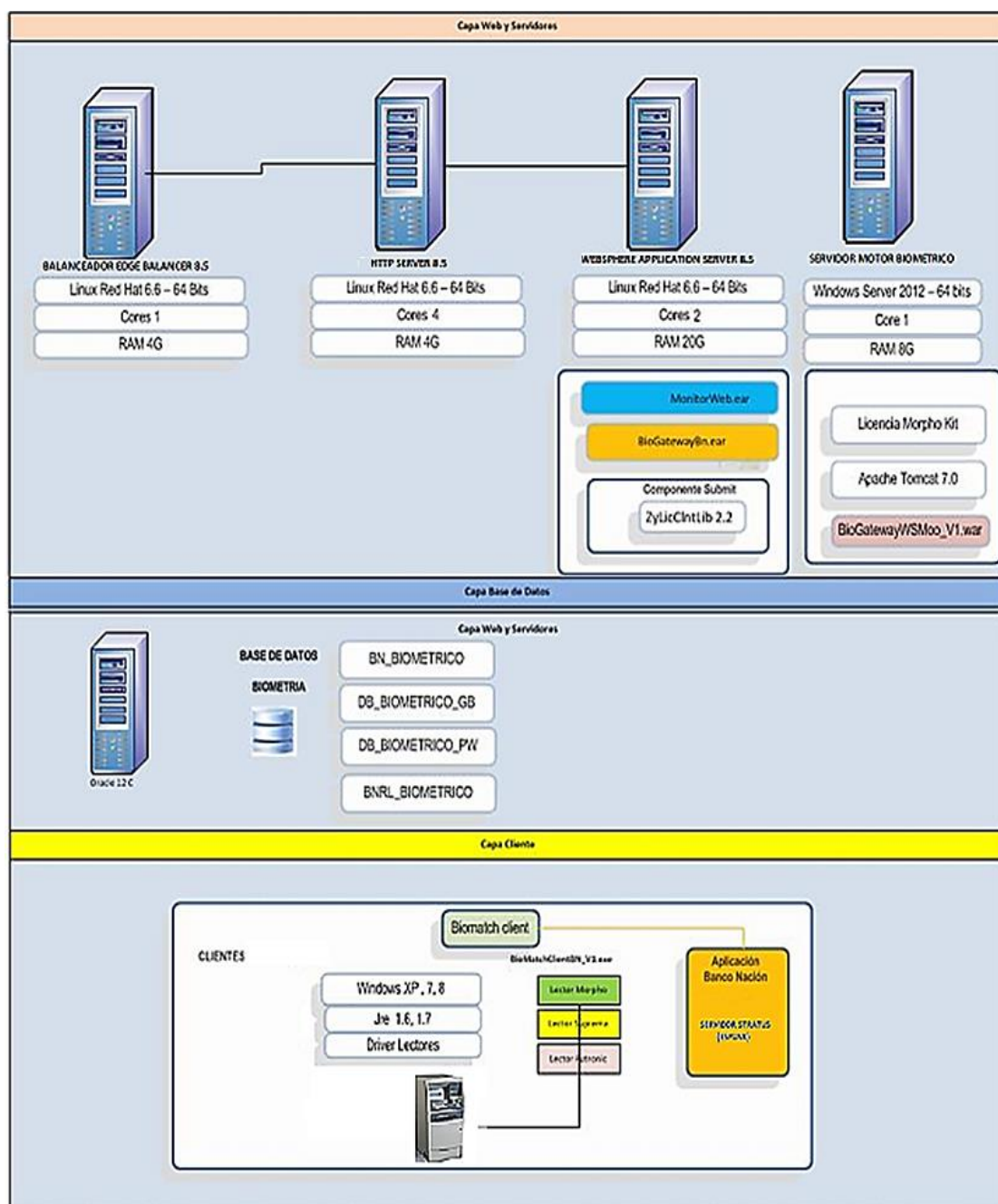


Figura 26: **Vista de Implementación.** Fuente: Banco de la Nación (2017) y elaboración propia.

3.4.2.13.1 Capas Web y servidores. En esta capa se ven los componentes de los servidores (Balanceador, HTTP server, Servidor de Aplicaciones, Servidor Motor Biométrico).

En el servidor de aplicaciones WebSphere es necesario desplegar y configurar los componentes (MonitorWeb.ear, BioGatewayBn.ear, ZyLicCIntLib 2.2). En el servidor Motor biométrico es necesario instalar el servidor de aplicaciones tomcat y desplegar el componente BioGatewayWSMoo_V1.war

3.4.2.13.2 Capas Base de Datos. En esta capa se van a desplegar los objetos de la base de datos, se crearán los usuarios y roles necesarios para el funcionamiento correcto de las aplicaciones y servicios web que componen la solución.

3.4.2.13.3 Capas Cliente. En esta capa es necesario desplegar los componentes BiomatcClient, instalar los drivers de los lectores en los cajeros automáticos.

El Banco de la Nación (2017) define:

3.4.2.14 Requerimientos No Funcionales

3.4.2.14.1 Desempeño. El software Gestor de huellas debe considerar el uso de ancho de banda (BW) máximo de 15 Kbps por cajero automático para su operatividad.

3.4.2.14.2 Facilidad de Soporte. El Agente biométrico tiene que ser un solo agente para todos los equipos biométricos de las marcas SUPREMA, FUTRONIC y MORPHO.

3.4.2.14.3 Restricciones de Diseño

- Restricciones sobre la Arquitectura: El Software Gestor de Huellas deberá estar basado en tecnología Web, en lenguaje Java JEE, desarrollado en java versión 1.6_30 y superior y motor de base de datos Oracle.
- Restricciones sobre los Componentes: Agente Biométrico – Biomatch: compatible con Windows XP, 7, Windows Server 2003 y 2008 de 32 y 64 bits.

3.4.2.14.4 Interfaces

- Interfaces de Usuarios

- ✓ Agente Biométrico – Biomatch: La interfaz de usuario contemplada es para la captura de huella, las demás funcionalidades son servicios del sistema.
- ✓ Central de Huellas - Gateway Biométrico: No contempla interfaces de usuario, las funcionalidades son servicios del sistema.
- ✓ Aplicación Web - Monitor de biometría: contemplará interfaces de usuario para el uso de sus funcionalidades.
- Interfaces de Hardware
El Agente Biométrico – Biomatch: contempla las interfaces de hardware con los equipos lector biométrico y el lector de DNle.
- Interfaces de Software
 - ✓ Central de Huellas - Gateway Biométrico: contempla la interfaz con el Servicio en Línea del RENIEC y la comunicación con el HSM del Banco de la Nación.
 - ✓ El Agente Biométrico – Biomatch: contempla la interfaz con la Central de Huellas (Gateway Biométrico).
- Interfaces de Comunicación
 - ✓ La transmisión de la huella se realizará sobre un canal seguro SSL.

3.4.2.14.5 Requerimientos de Licencia

- Central de Huellas - Gateway Biométrico.
- Agente Biométrico – Biomatch.

CAPÍTULO IV

CONCLUSIONES

4.1 Justificación

El uso de lectores biométricos en cajeros automáticos del Banco de la Nación permitirá mejorar la seguridad frente a posibles fraudes.

4.2 Presentación de Resultados

4.2.1 Seguridad

En cuanto a la seguridad, la implementación de un sistema de acceso biométrico mediante huella dactilar en la red de cajeros evitara los siguientes tipos de fraude: suplantación, cambiazo y clonación de tarjeta.

Los tipos de fraude antes mencionados, tienen en común que los delincuentes deben obtener la tarjeta del cliente, ya sea con el método del cambiazo, con un dispositivo que lo retenga o con la clonación. Esta propuesta agrega un sistema de validación biométrico, una vez implementado, para realizar alguna operación en cajero automático, el cliente debe estar presente y utilizar su huella.

Entonces, esta propuesta implementada contrarrestaría los tipos de fraude mencionados.

4.2.2 Costos

Para realizar una estimación de costos, se consideró:

- El costo de los equipos biométricos de captura de huella dactilar.
- El costo de la instalación de los lectores en cada cajero automático.
- El costo de software para los cajeros automáticos.
- El costo de los servidores.
- El costo de software para los servidores.

El costo de la instalación por cajero se obtuvo por parte del proveedor Diebold (comunicación personal, mayo 2019), el costo de los lectores biométricos marca Morpho, además, del software para cajeros y servidores se obtuvo por parte de proveedor ZyTrust (comunicación personal, mayo 2019), el costo de los servidores se obtuvo por parte del proveedor IBM (comunicación personal, junio 2019), el costo para modificar el software transaccional se obtuvo por parte del proveedor Bevertec (comunicación personal, junio 2019) y el costo del software Windows Server 2012 y Oracle 12c se obtuvo de las páginas web de los mismos.

En la (tabla 10) se muestra la estimación de costos para la solución biométrica.

TABLA 10: Estimación de Costos.

Ítem	Marca	Descripción	Costo	Cantidad	Total
Lector Biométrico	Morpho		\$ 240.00	1170	\$ 280,800.00
Instalación		Instalación de huellero en ATM	\$ 100.00	1170	\$ 117,000.00
Software para cajero automático	Biomatch	Biomatch Client	\$ 10,000.00	1	\$ 10,000.00
Servidores	IBM	Servidores: WAS (2), HTTP, Base de datos y balanceador de carga	\$ 3,000.00	5	\$ 15,000.00
Software para servidores	Oracle	Oracle 12C	\$ 10,000.00	1	\$ 10,000.00
Software para servidores	Microsoft	Windows Server 2012	\$ 6,000.00	1	\$ 6,000.00
Software para servidores	Biomatch	MonitorWeb, BioGatewayBn, ZyLicCintLib, BioGatewayWSMoo, Agente Biomatch, Gateway Biometrico, Websphere Application Server WAS 8.5, Linux Red Hat 6.6 – 64 Bits	\$ 250,000.00	Paquete completo	\$ 250,000.00
Modificar software	Bevertec	Modificar el flujo transaccional en el servidor Stratus	\$ 40,000.00		\$ 40,000.00
				Total	\$ 728,800.00

Fuente: Elaboración propia

El presupuesto de la subgerencia Agentes Corresponsales y ATMS para la futura compra de cajeros automáticos (220 cajeros a \$ 20,000 c/u) es aproximadamente \$ 4400,000. Este monto se obtuvo a través de un integrante del equipo de la subgerencia antes mencionada, (comunicación personal, junio 2019).

Se considera los 950 cajeros que se tienen implementados más los 220 de la futura compra, siendo un total de 1170 cajeros.

El costo de la implementación de este proyecto es \$728.800 equivalente a 16.5636% del total de la futura compra.

4.3 Conclusiones

1. La tecnología biométrica por huella es la mejor opción frente a los métodos tradicionales logrado una rápida y correcta autenticación del usuario; se considera esto debido a su tasa de error (2-3.3%) y su tasa de falso rechazo (0.1%).
2. Se determinó que la implementación de este sistema biométrico permite contrarrestar los siguientes tipos de fraude en el canal de cajeros automáticos tal como, suplantación, cambiazo y clonación de tarjeta.
3. El lector biométrico MorphoSmart300 cumple todos los requisitos para acceder al servicio de verificación biométrica de la RENIEC en forma satisfactoria.
4. El modelo de la plataforma implementada de lector biométrico por huella dactilar para las agencias del Banco, ayudo a definir el tipo de servidores y sus respectivas características para el diseño propuesto.

CAPÍTULO V

RECOMENDACIONES

1. Se recomienda a las áreas del Banco de la Nación que estén a cargo de las diversas plataformas de cajeros automáticos, evaluar la factibilidad de la implementación en forma masiva de la solución planteada en este trabajo.

CAPÍTULO VI

VI. BIBLIOGRAFIA

- Anicama, Nakamura, Proaño, Quenaya (2015) *Plan Estratégico de Scotiabank Perú del 2016 al 2020*. (Tesis de Postgrado). Lima. Pontificia Universidad Católica del Perú. Recuperado de: <http://tesis.pucp.edu.pe/repositorio/handle/123456789/7419>
- Aredo, U.J (2016) *Influencia de los canales alternativos en la satisfacción de los clientes del centro de contacto del Banco de Crédito del Perú – Sede Trujillo 2015*. (Tesis de Pregrado). Trujillo. Universidad Nacional de Trujillo. Recuperado de: <http://dspace.unitru.edu.pe/handle/UNITRU/4960>
- Avila, Injante, Murrugarra, Pacheco, Schroeder (2012) *Planeamiento Estratégico del Sector Bancario Peruano*. (Tesis de Postgrado). Lima. Pontificia Universidad Católica del Perú. Recuperado de: <http://tesis.pucp.edu.pe/repositorio/handle/123456789/4557>
- Banco de la Nación (2013) *Actualización de hardware y sistema operativo de la solución que actualmente soporta la red de Cajeros Automáticos y sus servicios*. Lima. Recuperado de: <http://www.bn.com.pe/transparenciabn/informes/2013/informe-tecnico-hardware-sistema-operativo-cajeros.pdf>
- Banco de la Nación (2015) *Características técnicas de Cajeros Automáticos*. Lima, Perú. Documento interno.
- Banco de la Nación (2016) *Adquisición de Lectores Biométricos para el uso del Canal Ventanilla y Plataforma de Servicios*. Lima. Recuperado de: <http://www.bn.com.pe/transparenciabn/informes/2016/informe-tecnico-lectores-biometricos-04042016.pdf>

- Banco de la Nación (2016) *Mayor seguridad con la identificación biométrica*. Recuperado de: <http://www.bn.com.pe/nosotros/boletines/2016/boletin-98-2016.pdf>
- Banco de la Nación (2016) *Renovación y Mantenimiento de Software de Sistemas de Gestión de Eventos Mainframe*. Lima. Recuperado de: <http://www.bn.com.pe/transparenciabn/informes/2016/informe-tecnico-eval-sw-mainframe.pdf>
- Banco de la Nación (2017) *Software Gestor de Huellas. Documento de Arquitectura de Software (SAD)*. Lima. Documento interno.
- Banco de la Nación (2017) *Software Gestor de Huellas. Documento de Diseño Detallado de Software (SAD)*. Lima. Documento interno.
- Banco de la Nación (2020) *Principales Modalidades de Fraude*. Lima. Recuperado de: <http://www.bn.com.pe/seguridad/modalidad-fraude.asp>
- Banco de la Nación (2020) *Preguntas Frecuentes sobre Cajeros Automáticos (ATMs)*. Recuperado de: <http://www.bn.com.pe/canales-atencion/documentos/preguntas-frecuentes-atms.pdf>
- Beltran, Vázquez, Gómez, Flores (2016) *La biometría dactilar vs la suplantación humana*. Santander. Universidad de Investigación y Desarrollo. Recuperado de: https://www.researchgate.net/publication/309205096_La_biometria_dactilar_vs_la_suplantacion_humana
- Biotime Technology (2019) MorphoSmart 300. Recuperado de: <https://www.biotime-technology.com/es/sensores-biometricos/morphosmart-300/#tab-id-2>
- BY (2018) *¿Qué es la biometría?* España. Recuperado de: <https://www.by.com.es/blog/que-es-la-biometria/>
- Clavei (2018) *¿Cuál es la diferencia entre un servidor dedicado y un servidor virtual VPS?* Recuperado de: <https://www.clavei.es/blog/cual-es-la-diferencia-entre-un-servidor-dedicado-y-un-servidor-virtual-vps/>
- Clarke, Modet (2018) *Biometría*. Madrid. Universidad Politécnica de Madrid. Recuperado de: http://catedraupmclarkemodet.es/wp-content/uploads/2011/11/20110610_Catedra_Clarke_Modet-UPMBoletin_VT_Biometria.pdf

- Cribillero, Cuba (2011) *Contribución del Banco de la Nación en distritos no atendidos por la empresa bancaria privada, para el desarrollo inicial de sus mercados financieros, entre los años 2001 y 2008*. (Tesis de Pregrado). Lima. Universidad Nacional de Ingeniería. Recuperado de: http://cybertesis.uni.edu.pe/bitstream/uni/786/1/cribillero_bd.pdf
- Diario Correo (2017) *PNP registra 50 robos de cajeros automáticos*. Recuperado de: <https://diariocorreo.pe/edicion/lima/pnp-50-robos-cajeros-automaticos-791868/>
- Diario El Comercio (2017) *MWC: los próximos cajeros automáticos usarán huellas dactilares*. Recuperado de: <https://elcomercio.pe/tecnologia/actualidad/mwc-proximos-cajeros-automaticos-usaran-huellas-dactilares-402884>
- Diario Gestión (2017) *Tecnología biométrica para las finanzas: ¿Cómo va el Perú y el mundo?* Recuperado de: <https://gestion.pe/tecnologia/tecnologia-biometrica-finanzas-peru-mundo-126002>
- Diario HuffPost (2017) *Necesitaras usar tu huella digital para usar cajeros automáticos de BBVA Bancover*. México. Recuperado de: https://www.huffingtonpost.com.mx/2017/07/27/necesitaras-usar-tu-huella-digital-para-usar-los-cajeros-automat_a_23053106/
- DIEBOLD NIXDORF (2019) *Checklist de inspección del sistema eléctrico en site de ATM*. Lima, Perú. Documento interno.
- ECURED (2018) *Cajero Automático*. Cuba. Recuperado de: https://www.ecured.cu/Cajero_autom%C3%A1tico
- Etchart, Alvez, Benedetto (2013) *Gestión de datos biométricos en bases de datos objeto-relacionales*. Entre Ríos. Universidad Nacional de Entre Ríos. Recuperado de: http://sedici.unlp.edu.ar/bitstream/handle/10915/27105/Documento_completo.pdf?sequence=1
- Gómez, R.A (2014) *Análisis técnico, económico y estratégico para una empresa de servicios predictivos para el retiro y abastecimiento de dineros custodiados de las entidades bancarias*. (Tesis de Postgrado). Santiago de Chile. Universidad de Chile. Recuperado de: <http://repositorio.uchile.cl/handle/2250/117027>

Guías Prácticas (2018) Tipos de lectores de huellas dactilares. Recuperado de: <http://www.guiaspracticas.com/controles-de-acceso/tipos-de-lectores-de-huellas-dactilares>

Gutiérrez, J.E (2007) *Estudio de factibilidad para el control de acceso biométrico, en una empresa empleando lectores de huella digital*. (Tesis de Pregrado). Bogotá. Universidad de La Salle. Recuperado de: <http://repository.lasalle.edu.co/bitstream/handle/10185/2158/T91.07%20G985e.pdf?sequence=1&isAllowed=y>

Inngresa (2018) *Como funcionan los lectores biométricos de huella digital*. Lima. Recuperado de: <https://inngresa.com/como-funcionan-lectores-biometricos-huella-digital/> inngresa.com

Landi J (2007) *Introducción a la biometría informática y análisis de huella dactilar como fuentes de autenticación en sistemas de seguridad*. (Tesis de Pregrado) Ecuador. Universidad Politécnica Salesiana. Recuperado de: <https://dspace.ups.edu.ec/handle/123456789/814>

Microsoft (2019) *Precios y licencias de Windows Server*. Recuperado de: <https://www.microsoft.com/es-es/cloud-platform/windows-server-pricing>

Monjaraz, C.A (2015) *Estudio de pre factibilidad para implementar biometría mediante huella digital en la red de cajeros automáticos, Banco de Crédito del Perú*. (Tesis de Pregrado). Lima. Universidad Científica del Sur. Recuperado de: http://repositorio.cientifica.edu.pe/bitstream/handle/UCS/479/TL_Monjaraz-Mazzei.pdf?sequence=1&isAllowed=y

Moreno, Villanueva (2012) *Sistema biométrico para cajeros automáticos del banco BBVA*. (Tesis de Pregrado). Lima. Universidad Tecnológica del Perú. Recuperado de: <http://studylib.es/doc/831159/sistema-biometrico-para-cajeros-automaticos-del-banco-bbva>

Oracle (2019) *Price list* <https://www.oracle.com/lad/corporate/pricing/>

Perú (2018) *DNI electrónico: usos, características y como tramitarlo*. Lima. Recuperado de: <https://peru.com/actualidad/nacionales/dni-electronico-usos-caracteristicas-y-como-tramitarlo-noticia-473721>

- RENIEC (2019) *Especificaciones técnicas para acceder al servicio de verificación biométrica*. Recuperado de: <http://sib.reniec.gob.pe/svbTools/SERVICIO%20DE%20VERIFICACION%20BIOMETRICA%20-%20Especificaciones%20Tecnicas%20Lector%20y%20Software%20Biometrico.pdf>
- Revista INFOTECHNOLOGY (2018) *¿Cómo funciona el primer cajero automático con huellas dactilares del país?* Argentina. Recuperado de: <https://www.infotechnology.com/online/Como-funciona-el-primer-cajero-automatico-con-huellas-dactilares-del-pais-20170718-0015.html>
- Revista Semana (2014) *Huella dactilar en vez de tarjetas para pagar*. Colombia. Recuperado de: <https://www.semana.com/tecnologia/novedades/articulo/huella-dactilar-vez-tarjetas-para-pagar/372652-3>
- Sánchez, M (2012) *El origen del cajero automático*. México. CONDUSEF. Recuperado de: <http://www.condusef.gob.mx/Revista/PDF-s/2013/164/cajero.pdf>
- Simón, Ortega (2003) *Reconocimiento automático mediante patrones biométricos de huella dactilar*. (Tesis de Postgrado) Madrid. Universidad Politécnica de Madrid. Recuperado de: <http://oa.upm.es/79/1/09200327.pdf>
- Techlandia (2018) *¿Que son los sistemas biométricos de huellas dactilares?* Recuperado de: https://techlandia.com/son-sistemas-biometricos-huellas-dactilares-info_224048/
- Universidad Latina de América (2015) *Cajeros Automáticos*. México. Recuperado de: <http://www.unla.mx/iusunla14/actualidad/CAJEROS%20AUTOMATICOS.htm>

Vargas, C.G (2016) *Diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital Francisco José de Caldas mediante el uso de torniquetes controlados por carnet con tecnología nfc y lector biométrico de huella dactilar*. (Tesis de Pregrado). Ciudad. Universidad Distrital Francisco José de Caldas. Recuperado de: <http://repository.udistrital.edu.co/bitstream/11349/3430/1/VargasGarciaCristianGeman2016.pdf>