ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA EN SISTEMAS

IMPLEMENTACIÓN DE MECANISMOS DE CONTROL DE ACCESO A INFORMACIÓN DE IDENTIFICACIÓN PERSONAL (PII) DE ACUERDO CON LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES DEL ECUADOR

MECANISMOS PARA LA TRANSFERENCIA SEGURA DE PII.

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

DANNY ESTEBAN VENEGAS VILLAVICENCIO

danny.venegas@epn.edu.ec

DIRECTOR: DENYS ALBERTO FLORES ARMAS

denys.flores@epn.edu.ec

DMQ, Marzo 2023

CERTIFICACIONES

Yo, DANNY ESTEBAN VENEGAS VILLAVICENCIO declaro que el trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

Danny Venegas

Certifico que el presente trabajo de integración curricular fue desarrollado por DANNY ESTEBAN VENEGAS VILLAVICENCIO, bajo mi supervisión.

Denys Flores
DIRECTOR

Certificamos que revisamos el presente trabajo de integración curricular.

NOMBRE_REVISOR1	**NOMBRE_REVISOR2**
REVISOR1 DEL TRABAJO DE	**REVISOR2 DEL TRABAJO DE**
INTEGRACIÓN CURRICULAR	**INTEGRACIÓN CURRICULAR**

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

Adicionalmente, declaro que el contenido de este trabajo incluye material de artículos técnicos revisados por pares de mi autoría que han sido publicados durante el desarrollo de este proyecto, y que detallo a continuación:

Danny Venegas

Denys Flores

DEDICATORIA

Quiero expresar mi gratitud y dedicar el resultado de este trabajo a Dios, quien me ha brindado la fuerza y motivación necesarias para alcanzar esta meta.

A mi familia. En particular, a mis padres, quienes me brindaron su apoyo y contención en los momentos difíciles y no tan difíciles. Agradezco su enseñanza sobre cómo enfrentar las dificultades sin perder la cabeza ni rendirme, lo que me permitió convertirme en la persona que soy hoy en día. Todo lo que he aprendido de ellos, incluyendo mis principios, valores, perseverancia y empeño, ha sido transmitido con amor y sin esperar nada a cambio.

También quiero dedicar mi tesis a mis profesores y mentores, quienes han sido dedicados y apasionados en la enseñanza y han sido una guía fundamental en mi camino.

A mis compañeros de estudio, agradezco las risas, el aprendizaje y los momentos compartidos juntos, así como las conversaciones estimulantes que han enriquecido mi experiencia.

Finalmente, deseo expresar mi gratitud a mi Alma Mater y a todas las personas que la conforman por su apoyo incondicional. No podría haber llegado hasta aquí sin su ayuda y respaldo.

AGRADECIMIENTO

Quiero agradecer especialmente a mi familia por permitirme cumplir con excelencia en el desarrollo de esta tesis. Su apoyo incondicional, amor, bondad y aportes han hecho que el camino hacia la consecución de esta meta haya sido menos complicado. Les agradezco de todo corazón y quiero hacer presente mi gran afecto hacia ustedes, mi hermosa familia. Y por supuesto, gracias a Dios por permitirme vivir y disfrutar de cada día.

Quiero expresar mi agradecimiento a cada maestro que formó parte de este proceso integral de formación, el cual culmina con la graduación de nuestro grupo. Esta tesis es un producto terminado que será un recuerdo y una prueba viviente en la historia, y perdurará dentro de los conocimientos y el desarrollo de las generaciones que vendrán.

Por último, quiero agradecer a quien esté leyendo este apartado y más aún, a aquellos que hayan decidido adentrarse en mi tesis. Agradezco por permitir que mis experiencias, investigaciones y conocimientos formen parte de su repertorio de información mental.

Contenido

RESUMEN

En el Ecuador la ley orgánica de protección de datos pretende transformar la manera en que los datos de los ciudadanos viajen de manera segura por la red. Pero al ser una ley relativamente nueva muchas empresas no comprenden la forma correcta para implementar dentro de su organización. Es entonces donde se abre una oportunidad para que este proyecto presente una solución como: “El poder crear mecanismos de transferencia segura que estén acorde con la ley” dando como solución una nueva arquitectura en base a las tres referencias principales tales como: “Reglamento General de Protección de Datos (GDPR) europeo, la Ley Orgánica de Protección de Datos Personales (LOPDP) ecuatoriana y el Esquema Gubernamental de Seguridad de la Información (EGSI).” Siendo un proyecto pionero en su ámbito y permitiendo a las empresas tener una idea clara de cómo estructurar su organismo de acuerdo a LODPD. Evitando así posibles problemas e inconformidades que el estado pudiera presentar. El presente proyecto plantea una respuesta basada en la implementación de firmas digitales para el envió de documentos entre las partes de recolección de datos y almacenamiento. Como también, un protocolo de consultas para entidades externas que desean acceder a la información dentro de la compañía.

PALABRAS CLAVE: Transferencia de datos, Firma Digital, Query Web Service, Key Escrow, Ley orgánica de Protección de Datos.

ABSTRACT

In Ecuador, the organic law of data protection aims to transform the way in which citizens' data travels securely through the network. But being a relatively new law, many companies do not understand the correct way to implement within their organization. It is then where an opportunity opens for this project to present a solution as: "The power to create secure transfer mechanisms that are in accordance with the law" giving as a solution a new architecture based on the three main references such as: "European General Data Protection Regulation (GDPR), the Ecuadorian Organic Law on Personal Data Protection (LOPDP) and the Government Information Security Scheme (EGSI)." Being a pioneer project in its field and allowing companies to have a clear idea of how to structure their organization according to LODPD. Thus, avoiding potential problems and nonconformities that the state could present. This project proposes an answer based on the implementation of digital signatures for sending documents between the parties of data collection and storage. As well as |a protocol of queries for external entities that wish to access the information within the company.

KEYWORDS: Data Transfer, Digital Signature, Query Web Service, Key Escrow, Organic Law on Data Protection.

1. INTRODUCCIÓN

En este capítulo se abordan los aspectos generales del proyecto, incluyendo una visión general del componente, la meta principal, objetivos específicos, el ámbito de aplicación del proyecto, conceptos teóricos clave, y una revisión de los distintos trabajos relacionados con el proyecto.

1.1 Descripción del Componente

En Ecuador, a partir de 2021, se ha puesto en vigencia la Ley orgánica de protección de datos, que incluye varios artículos relacionados con las condiciones necesarias que se deben evaluar y verificar para garantizar que el tratamiento de datos personales sea legítimo. Además, la ley también aborda las diversas formas en que los titulares de datos personales pueden expresar su voluntad con respecto al tratamiento de sus datos. La ley otorga a los titulares de datos personales varios derechos importantes, como el derecho a la información, el derecho de acceso, el derecho de rectificación y actualización, el derecho de eliminación, el derecho de oposición, el derecho de portabilidad, el derecho a no ser objeto de decisiones basadas únicamente en valoraciones automatizadas, el derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, y el derecho a la educación digital.

En este sentido la ley obligó a las compañías a buscar nuevos mecanismos de transferencia segura de información y datos. Las empresas empezaron a buscar alternativas certificadas y acordes con la nueva ley como; usar cifrado de extremo a extremo, o el uso de encriptación de mensajes. En el ámbito de red y canales de comunicación la tendencia radica en el uso de protocolos de conexión como HTTPS u TLS. Sin embargo, no existe un estándar oficial para la implementación de estos mecanismos por lo que cada empresa genera sus propias arquitecturas para el uso de estos. Al ser una ley demasiado nueva no existen estudios relacionados que presenten una solución clara ante el problema de la implementación de esta nueva ley en la infraestructura interna de una empresa.

Por lo cual se logró identificar una excelente oportunidad para solucionar la problemática. En la cual se prevé implementar una un sistema seguro de transmisión que permita transferir datos de manera rápida y segura utilizando protocolos de red, internet, normas y arquitecturas. Que en conjunto permita acatar el reglamento estipulado en los diferentes artículos relacionados a la transferencia que plantea esta ley.

1.2 Objetivo general

Implementar mecanismos seguros de gestión de información de identificación personal (PII) durante su transferencia.

1.3 Objetivos específicos

1. Analizar el estado del arte de soluciones para la transferencia segura de PII.
2. Identificar los requerimientos funcionales y no funcionales relacionados con la seguridad y privacidad de PII durante su transferencia.
3. Implementar un prototipo experimental de acuerdo con los lineamientos del Reglamento General de Protección de Datos (GDPR) europeo, la Ley Orgánica de Protección de Datos Personales (LOPDP) ecuatoriana y el Esquema Gubernamental de Seguridad de la Información (EGSI).
4. Evaluar el prototipo propuesto en un entorno controlado, considerando su resiliencia ante la eventual manipulación de información en tránsito por parte de terceros no autorizados.

1.4 Alcance

El presente proyecto contempla la implementación de mecanismos de control durante la transferencia de la información de información personal (PII), evitando la manipulación de información en tránsito por parte de terceros no autorizados. Incluye el despliegue de un servicio seguro de intercambio de información entre entidades interesadas, considerando el GDPR europeo, la LOPDP ecuatoriana y el EGSI. El objetivo es identificar los requerimientos funcionales y no funcionales relacionados con la seguridad y privacidad de PII durante su transferencia. Estos mecanismos implementados son prototipos experimentales y serán evaluados en entornos controlados, sin que esto implique el despliegue de estos en alguna infraestructura productiva, ya sea pública o privada. A continuación, en la figura 2 explicamos la propuesta de implementación del componente para transferencia segura de PII, implementación de un servicio de seguro de intercambio entre entidades recomendadas con revocación.

En la figura 1, se muestra un escenario típico de transferencia segura, en el cual existe un emisor un receptor con la necesidad de enviar un mensaje, pero con la problemática de que este debe llegar seguro y sin ninguna alteración. Es por eso por lo que para solucionar dicho problema se implementa un sistema de cifrado asimétrico o de clave pública que actúa como asegurador de mensaje, con el fin de que el mensaje llegue a su destino intacto y respetando los pilares de la seguridad informática. El diagrama a continuación sirve como

base para la implementación y ejemplificación de la solución en la problemática que trata el proyecto.

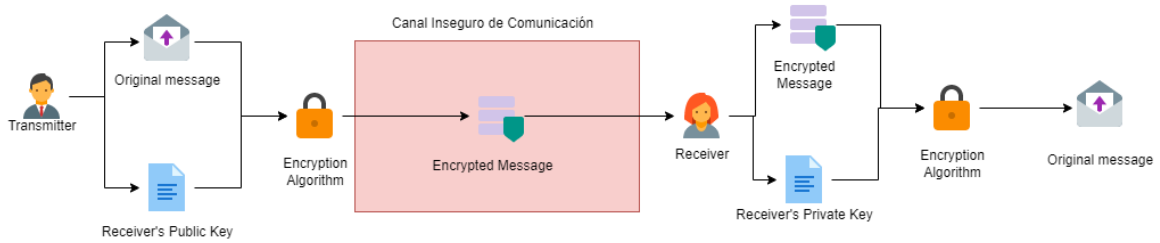

Figura 1. Escenario de comunicación entre las entidades de confianza.

[Autor: Danny Venegas]

1.5 Marco teórico

En esta unidad se hablará sobre los temas relacionados con los conceptos teóricos usados para desarrollar el proyecto permiten obtener los conocimientos necesarios para su subsecuente implementación.

1.5.1 Seguridad Informática

Introducción:

En las empresas, la información es considerada el activo más valioso e importante, ya sea que se trate de información propia de la empresa o información personal recolectada de sus clientes. Dado que este activo es importante, también existe el riesgo de perderlo, lo que hace que se busque siempre la protección contra cualquier tipo de amenaza o riesgo. Con la llegada del boom tecnológico, las empresas modernizaron sus equipos de recolección de información, pasando de simples hojas de papel o cuadernos a grandes bases de datos de información. Es en este momento donde nace la seguridad informática, cuyo objetivo es solucionar, proteger y prevenir cualquier riesgo o amenaza que pueda afectar a estos activos valiosos, también conocidos como datos o información. [1]

1.5.2 Características de la seguridad informática

Dentro de la seguridad informática existen varias características importantes donde las 3 principales son:

- La confidencialidad es una característica que implica que todas las etapas del procesamiento de información estén protegidas de tal manera que no exista acceso no autorizado. Esto se hace para prevenir alteraciones en la información, así como el robo de datos. [1]

- La integridad es una característica que asegura que los datos sean precisos, completos y no hayan sido alterados durante las diferentes etapas de procesamiento de la información. [1]
- Por otro lado, la disponibilidad garantiza que la información obtenida durante todas las etapas del procesamiento esté disponible para cualquier necesidad o requerimiento de la empresa. Sin embargo, es importante que el acceso a esta información sea controlado y monitoreado para garantizar su seguridad. [1]

Pero según el marco de gestión y de negocio global para el gobierno y la gestión de TI inglés COBIT, específica otras características tales como:

- La efectividad: Consiste en que la información sea la necesaria y adecuada para desarrollar cualquier tarea dentro de una empresa de tal manera que la información sea proporcionada de manera oportuna correcta consistente y accesible. [1]
- La eficiencia: Consiste en que la obtención y procesamiento de la información se realicen de manera correcta, eficiente y óptima utilizando los recursos de la empresa. [1]
- El apego a estándares: Consiste en que el procesamiento de la información se debe realizar acatando las leyes, reglamentos o acuerdos de internos y contractuales de la empresa o del país en el que se encuentra. [1]
- La confiabilidad: No es más que la característica en la que la información no haya sido alterada o manipulada inapropiadamente. [1]

En el campo de la seguridad informática, existen dos aspectos importantes: el control de acceso y la autenticación. El control de acceso se refiere al monitoreo, administración y gestión del acceso a la información por parte de los usuarios, con el objetivo de prevenir vulnerabilidades relacionadas con el acceso no autorizado de atacantes o usuarios maliciosos. [1]

Por otro lado, la autenticación consiste en verificar que la identidad del usuario sea la correcta como por ejemplo verificar que sí se ha realizado transacciones bancarias en la página oficial y no en un sitio malicioso. [1]

También existe el no repudio, que es la capacidad que se otorga a un sistema para evitar que un usuario ni ahí que haber efectuado determinadas acciones. En la actualidad los sistemas y la seguridad informáticos han diseñado métodos y pruebas irrefutables para

aumentar el no repudio como por ejemplo la generación de tickets de usuario que permita visualizar la acción de dicho usuario en el sistema. [1]

1.5.3 Objetivos de la seguridad informática

La seguridad informática no se limita a preservar solo las siete características mencionadas por COBIT, sino que tiene varios objetivos principales. Uno de estos objetivos es la creación de controles de prevención para proteger la información contra diferentes tipos de ataques, tanto internos como externos, físicos y electrónicos. Además, otro objetivo importante es el desarrollo de planes de contingencia para hacer frente a estas amenazas en caso de que ocurran dentro de la empresa, así como contar con planes para recuperar la información en su totalidad en caso de una pérdida de datos. [1]

1.5.4 ¿Qué es transferencia gestionada de archivos?

Uno de los términos más frecuentemente empleados para hacer referencia a la transferencia de archivos es descrito por Techopedia como "el proceso de copiar o mover un archivo de una computadora a otra a través de una red o conexión a Internet. Esta práctica permite compartir, transferir o transmitir archivos o datos entre distintos usuarios o computadoras, ya sea de manera local o remota". [2]

1.5.5 La importancia de la transferencia de archivos

Las transferencias de archivos son un aspecto fundamental de las operaciones empresariales, donde las compañías intercambian información diariamente con clientes, proveedores y socios. Esta actividad se ha convertido en una rutina dentro de las empresas, que abarca desde el envío de transacciones entre clientes hasta la simple acción de enviar un correo electrónico entre el personal. Por tanto, es importante que estas transferencias de archivos sean seguras y eficientes para garantizar la protección de los datos. [3]

1.5.6 Protocolos de transferencia.

Una forma sencilla de definir un protocolo de transferencia de archivos es que proporciona un medio para mover archivos de una ubicación a otra en una red. Una de sus funciones más importantes se puede observar en el modelo cliente-servidor, donde los archivos se cargan desde un cliente a un servidor y una aplicación o cliente puede acceder a ellos desde allí. [4]

Dentro de los protocolos de transferencia tenemos:

- FTP que es el protocolo más simple que existe, suministra un número simultaneo de tareas tales como listar directorios remotos, cambiar el directorio remoto actual,

crear y eliminar directorios remotos y transferir varios archivos en una sola petición. [5]

- El Protocolo Telnet: facilita un método estándar para que los equipos dentro de una terminal y los procesos orientados a terminal intercambien información. De entro los datos más importantes se encuentra que TCP/IP implementa TELNET en los mandatos de usuario tn, telnet o tn3270. [6]
- FTPS: Protocolo que asegura que los archivos viajen a través de FTP con seguridad dentro de la capa de transporte. [4]
- SFTP: Proporciona un monitoreo de transferencia de archivos a través de un solo canal SSH. [4]

1.5.7 Criptografías.

La criptología se refiere a la disciplina informática que se ocupa de la seguridad en la comunicación y el intercambio de mensajes cifrados entre dos entidades: un emisor y un receptor. En este proceso, la información se transmite a través de un canal de comunicación y se emplean técnicas de encriptación para proteger la confidencialidad e integridad de los datos transmitidos. [7]

1.5.8 Tipos de encriptado.

Existen varios tipos de cifrado tales como:

- El cifrado simétrico es un método de cifrado en el cual se utiliza una única clave para cifrar y descifrar el mensaje. Antes de 1976, este era el único método de cifrado disponible para la protección de datos en entornos computacionales. [8]
- Se puede describir el cifrado asimétrico como un tipo de cifrado que se diferencia del cifrado simétrico en que emplea un par de claves diferentes, una para cifrar y otra para descifrar la información. Por esta razón, se le llama asimétrico. En este proceso, la clave utilizada para cifrar la información no puede ser utilizada para descifrarla, lo que hace que el cifrado asimétrico sea más seguro que el cifrado simétrico. Este tipo de cifrado fue desarrollado como una alternativa más segura para la protección de datos en entornos computacionales. [9].
- La firma digital es un elemento en formato electrónico utilizado para verificar la integridad y autenticidad de otro dato en formato electrónico, conocido como dato firmado. Se trata de un tipo de firma electrónica que se genera a través de un proceso criptográfico que establece una relación única y exclusiva entre el dato

firmado y el firmante. Básicamente, la firma digital es un proceso que utiliza una "caja negra" que necesita un dispositivo seguro y el dato a ser firmado como entrada para generar una firma digital como salida. [10]

1.5.9 Key Escrow.

Según el Glosario Terminología Informática la definición de Key Escrow es: “Se puede describir un sistema de gestión de claves como un sistema en el cual una institución confiable es responsable de almacenar y custodiar la clave criptográfica en nombre del legítimo propietario. Luego, el personal autorizado puede obtener la clave de cifrado para su uso en una comunicación, siguiendo un procedimiento específico basado en la clave depositada. Este sistema garantiza la seguridad y la protección de las claves de cifrado al evitar que caigan en manos equivocadas.” [11]

Exponer el marco teórico relevante relacionado con el tema, incluyendo los argumentos que justifican la validez de lo realizado, con una revisión bibliográfica pertinente.

1.5.10 Servicio Web.

Según IBM los servicios web son: “Se puede describir los servicios web como módulos de aplicaciones autónomas que pueden ser publicados, localizados e invocados a través de una red.” [12]

1.5.11 Query web.

La habilitación de la Web Semántica requiere un acceso unificado a los datos en la Web, que se presentan en diversos formalismos, ya sea en la Web estándar (por ejemplo, (X)HTML, SVG o cualquier aplicación XML) o en otros formalismos específicos. Para lograr esto, se utilizan lenguajes de consulta que abarcan desde lenguajes de selección básicos hasta lenguajes de razonamiento completo. Los lenguajes de consulta pueden estar limitados a un formato de representación de datos, como XML o RDF, o pueden ser de propósito general y permitir la consulta de datos en ambos tipos de Web. [13]

1.5.12 SSL.

Un certificado SSL es un tipo de certificado digital que se utiliza para verificar la identidad de un sitio web y permitir una conexión segura a través de la encriptación de la información. El término SSL es una abreviatura de Secure Sockets Layer (Capa de sockets seguros), que se refiere a un protocolo de seguridad que establece un canal cifrado entre un servidor web y un navegador web. [14]

Las compañías y entidades necesitan incorporar certificados SSL a sus sitios web con el fin de garantizar la seguridad de las transacciones en línea y preservar la privacidad y protección de la información de los clientes. [14]

1.6 Estado del Arte y Trabajo Relacionado

En esta unidad hace referencia a los trabajos relacionados que dieron una ayuda y apoyo a la creación del documento.

1.6.1 Revisión sistemática de la lectura

Se realizó un análisis del estado del arte de soluciones para la transferencia segura de PII. El propósito de esta investigación es analizar los estudios existentes y sus hallazgos con el fin de entender la problemática planteada y encontrar todas las referencias posibles para dar solución a la pregunta de investigación planteada:

- ¿Qué mecanismos se debe implementar en el sistema al momento del proceso de transferencia para proteger la información personal y la privacidad de los usuarios?

En el documento del estado del arte proporcionó las siguientes contribuciones para aquellos que estén interesados, en transferencia segura de datos como también en mecanismos de transferencia:

- Se identificó 10 estudios principales relacionados a la transferencia de datos entre 2016 y el 2022. Otros investigadores pueden usar dichos estudios para trabajar en sus campos específicos.
- Se presentó un metanálisis del estado actual de los métodos en los que se puede implementar para transferir datos y para mejorar la seguridad de tecnologías cibernéticas existentes y emergentes.
- Se ha hecho una representación y se produjo pautas para apoyar más, trabajar en esta área.

Para lograr responder a la pregunta de investigación el presente SLR usó la metodología pública por PRISMA. Que define una sucesión de pasos para presentar el SLR de manera correcta y precisa. [15]

PRISMA es un conjunto mínimo de elementos basados en evidencias que tienen como objetivo facilitar la presentación de informes de revisiones sistemáticas y meta-análisis. Su propósito es asistir a los autores en la elaboración de estos informes, y aunque fue diseñado inicialmente para ensayos aleatorios, también es útil para otros tipos de revisiones sistemáticas y, en particular, para la evaluación de intervenciones. Además,

PRISMA puede ser empleado en la evaluación crítica de revisiones sistemáticas previamente publicadas, aunque no se utiliza como herramienta para evaluar su calidad. La lista de verificación de PRISMA consta de 27 elementos y se complementa con un diagrama de flujo de cuatro fases. [15]

A continuación, se mostrará los resultados obtenidos al implementar PRISMA en el estado del arte que es la base del documento de tesis del proyecto.

Para el artículo antes mencionado se realizó la búsqueda de información en tres fuentes importantes en el ámbito de la ingeniería las cuales son: IEEE, SpringerLink, Google Scholar. De los cuales hubo un total de 500 estudios que fueron arrojados en primera instancia al momento de realizar la primera búsqueda, los cuales se redujo a 250 en el momento que se usaron los filtros de años de referencia. A continuación, se aplicó los primeros criterios de exclusión e inclusión que redujo el número a 100. De los cuales se volvió aplicar el criterio de exclusión e inclusión que termino en 25. Después de leerlos en su totalidad se aplicó por última vez los criterios dejando como resultado 10 documentos principales. En la Figura 2 podemos visualizar el proceso de selección de los datos del proyecto como también las fuentes y los resultados iniciales de la búsqueda.

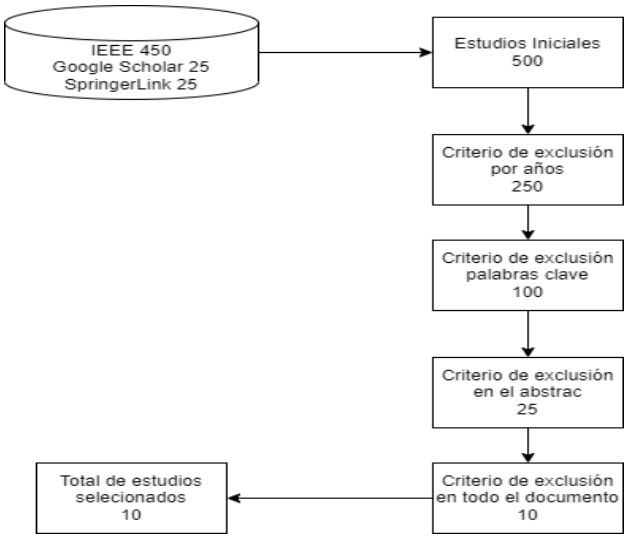

Figura 2. Representación del proceso de selección de información.

[Autor: Danny Venegas]

El artículo muestra uno sesgo importante el cual es representado por la Figura 3. Donde se puede observar el número de resultados obtenidos a lo largo del tiempo establecido para obtener referencias optimas y que sean relevantes. Esto se debe a que en el área de computación los descubrimientos cada vez son actualizados por lo que estudios de un

rango de tiempo muy alto podrían ser irrelevantes o podrían ser obsoletos e inservibles para resolver la problemática planteada.

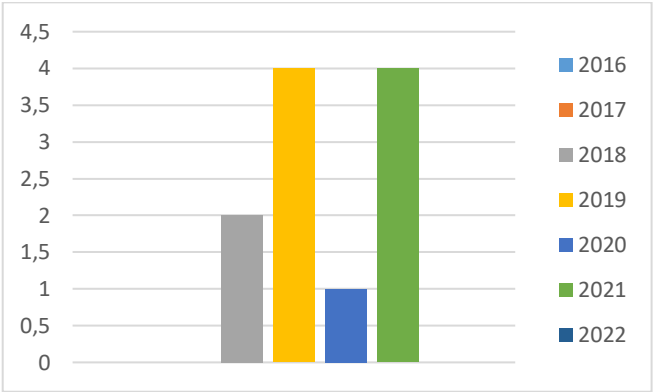

Figura 3. Representación de los trabajos obtenidos filtrado por años.

[Autor: Danny Venegas]

Entra los hallazgos más importantes que el documento menciona son:

Tabla 1. Resultados obtenidos del SLR.

[Autor: Danny Venegas]

No.	**Estudios Primarios**		
	Titulo	**Autores**	**Enfoque**
E1	C2CFTP: Direct and Indirect File Transfer Protocols Between Clients in Client-Server Architecture	MINGYU LIM	Protocolos y estándares
E2	Protocols for Transferring Bulk Data Over Internet: Current Solutions and Future Challenges	Khawar Khurshid; Imdad Ullah;Zawar Shah;Najm Hassan;Tariq Ahamed Ahanger	Protocolos y estándares
E3	An Encrypted Field Locating Algorithm for Private Protocol Data Based on Data	Qing Li;Yonghui Ju;Chang Zhao;Xintai He	Protocolos y estándares

No.	Estudios Primarios		
	Titulo	**Autores**	**Enfoque**
	Reconstruction and Moment Eigenvector		
E4	Multi-Level Time-Sensitive Networking (TSN) Using the Data Distribution Services (DDS) for Synchronized Three-Phase Measurement Data Transfer	Tanushree Agarwal; Payam Niknejad;M. R. Barzegaran;Luigi Vanfretti	Redes
E5	RCOAP: A Rate Control Scheme for Reliable Bursty Data Transfer in IoT Networks	Dang Hai Hoang; Thi Thuy Duong Le	Redes
E6	A Secure and Practical RFID Ownership Transfer Protocol Based on Chebyshev Polynomials	Zuming Shen; Peng Zeng;Yuyin Qian;Kim-Kwang Raymond Choo	Protocolos y estándares
E7	Enhancing Fast TCP's Performance Using Single TCP Connection for Parallel Traffic Flows to Prevent Head-of-Line Blocking	Sarfraz Ahmad; Muhammad Junaid Arshad	Protocolos y estándares
E8	Delay-Bounded Wireless Network Based on Precise Time Synchronization Using	A Survey on Multipath Transport Protocols Towards 5G Access Traffic Steering, Switching and Splitting	Redes

No.	Estudios Primarios		
	Titulo	**Autores**	**Enfoque**
	Wireless Two-Way Interferometry		
E9	A Novel Encryption Algorithm based on DNA Cryptography	A. Vikram; S. Kalaivani; G. Gopinath	Protocolos y estándares
E10	A Novel Key Agreement Protocol Based on RET Gadget Chains for Preventing Reused Code Attacks	Wu Fusheng; Zhang Huanguo; Ni Mingtao; Wang Jun; Ji Zhaoxu	Protocolos y estándares

En los cuales cada uno está clasificado por su enfoque. Los estudios que se centraron en las redes y la gestión de redes virtuales fueron agrupados en la categoría de redes. En cambio, los estudios que tenían un enfoque relacionado con los intercambios entre pares, la trasferencia de datos y protocolos se agrupa en la categoría de protocolos y estándares.

Y en otro de los principales aportes se encuentra los trabajos futuros, presenta potenciales ideas de trabajos futuros como:

- Estudio potencia 1.- La investigación sobre la seguridad de IoT utilizando protocolos mostrados en el documento que permita reducir la latencia de envíos de datos en gran cantidad. A los efectos de este trabajo, no fue posible cuantificar dichos datos debido a la variabilidad en las soluciones empleadas por cada grupo de investigadores. El trabajo futuro podría incluir una evaluación de los diferentes protocolos mostrados y su rendimiento al ser implementados en el IoT el cual maneja cantidades masivas de datos.
- Estudio potencia 2.- Los ataques cibernéticos cada día son más perjudiciales y pueden causar muchas perdidas. La investigación y creación de protocolos de seguridad para transferir información podría ayudar a reducir el riesgo. El trabajo futuro podría incluir nuevos modelos de seguridad como también evaluar el rendimiento de los protocolos ante amenazas.

2. METODOLOGÍA

En esta sección se identificará la metodología utilizada como también las herramientas que apoyan la implementación y desarrollo del prototipo experimental que dará solución a la problemática planteada.

2.1 Selección de Herramientas

Las herramientas que se utilizaron para la implementación y el despliegue de la solución y sus diferentes componentes radican en gran medida en el Desing Science Reserch o DSR por sus siglas, que es la metodología por la cual se construye todo el proyecto. DSR permite que mientras se den como resultado un nuevo conocimiento, existe un prototipo que permita resolver dicha problemática. También se utilizó la metodología SCRUM que complementa al DSR en la parte del prototipo ya que permite implementar un modelo de pasos para ir construyendo el prototipo final del proyecto. A continuación, se describe a las herramientas antes mencionadas.

2.1.1 Design Science Research (DSR)

Es un proceso de investigación, que permite crear o producir una construcción innovadora, que intenta resolver un problema de la vida real, como también contribuye teóricamente en la disciplina en la que se aplica. [16]

En esta metodología de investigación se divide en 3 partes fundamentales las cuales son: las entradas: que son las relevancias prácticas entre el problema y la solución como también las conexiones con la teoría previa o teoría que ya ha sido comprobada. Las construcciones: son los entregables que el proceso permite producir. Las salidas: son los entregables importantes o finales tales como el artefacto que da la solución práctica al problema y las contribuciones teóricas sobre el estudio. [16]

El proceso del DSR.

El proceso para desarrollar un DSR se divide en 5 partes, la primera parte es identificar y evaluar el problema donde el problema debe ser relevante, debe ser de un tamaño correcto también se debe investigar el problema de raíz y examinar el potencial a largo plazo de la solución. [16]

En la segunda parte es obtener un profundo conocimiento tanto práctico como teórico, esto quiere decir, que se debe realizar una revisión literaria del problema y aprender o establecer la teoría que se va a usar para solucionar el problema. [16]

Cómo tercera parte tenemos innovar una idea para solucionar, en esta parte se desarrollan varias ideas como posibles soluciones y conceptos, también se evalúa y se justifica porque se seleccionó la idea de la solución final. [16]

Como cuarto paso tenemos la evaluación de la solución, en esta sección se simula y se presenta ya un prototipo funcional de resolución del problema. En esta sección hay que tener en cuenta que muchas veces el prototipo no brinda una solución completamente exitosa en la parte práctica, pero es significativamente excelente en la parte teórica. [16]

Por último, tenemos la sección de reflexionar, en donde se especifica la contribución del conocimiento y reflexiona sobre la aplicabilidad más amplia del prototipo función al final. [16]

En la figura 4 tenemos una representación de la metodología general de un DSR que representa los pasos a seguir para aplicar esta metodología.

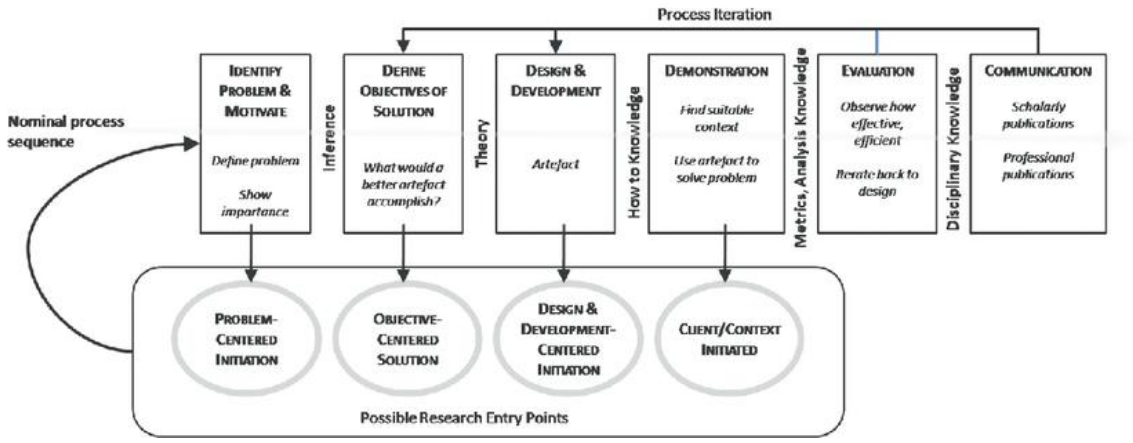

Figura 4. Representación de la Metodología General de la DSR. [17]

En la figura 5 en cambio tenemos la representación de la interacción entre los componentes del DSR donde muestra cada etapa que se llevará a cabo dentro de la aplicación de la metodología y como estas se conectan. Teniendo en cuenta que esta metodología aporta un prototipo y un nuevo concepto teórico para la solución del problema.

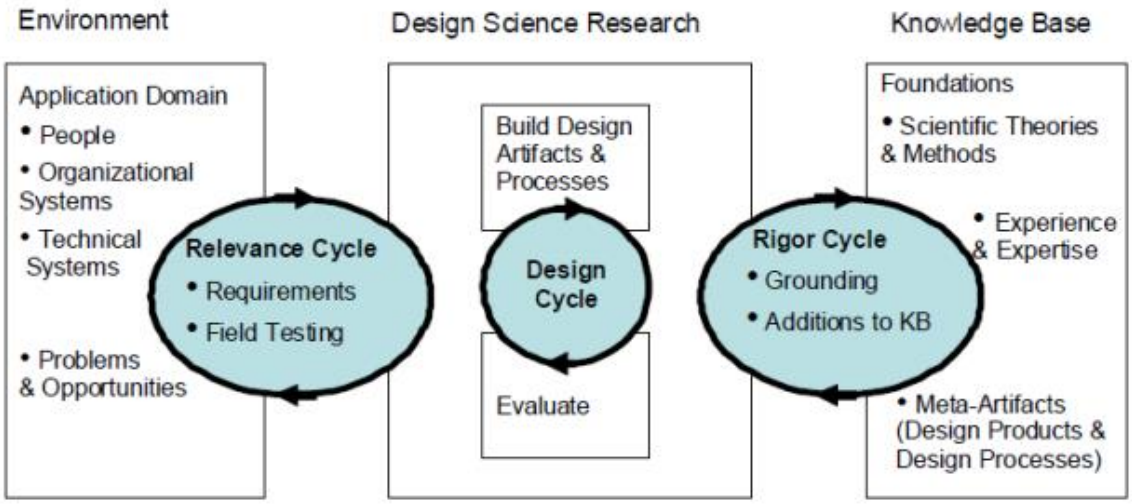

Figura 5. Representación de la conexión entre componentes del DSR. [18]

2.1.2 SCRUM.

Scrum es una metodología o marco de trabajo que permite el desarrollo e interacción colaborativa entre equipos. Por otro lado, también es considerada a menudo un marco de gestión de proyectos ágil o de metodologías agiles. Pero scrum incluye un conjunto de enseñanzas, herramientas y funciones que, de forma coordinada, ayudan a los equipos a estructurar y gestionar su trabajo. [19]

Dentro de Scrum podemos encontrar la herramienta de los Sprints que son períodos breves de tiempo fijo en el que un equipo de scrum trabaja para completar una cantidad de trabajo establecida. [19]

También podemos encontrar el Product Backlog que es una “lista de trabajo ordenado por prioridades para el equipo de desarrollo que se obtiene de la hoja de ruta y sus requisitos.” [19]

2.1.3 PYTHON.

Python es un lenguaje de programación que combina potencia y facilidad de aprendizaje. Sus estructuras de datos de nivel superior son eficientes y su sistema de programación orientada a objetos es sencillo pero efectivo. La sintaxis elegante de Python y su tipado dinámico, junto con su naturaleza interpretada, hacen de él una opción ideal para el desarrollo rápido de aplicaciones y scripting en muchas áreas y para la mayoría de las plataformas. [20]

Tanto el intérprete de Python como su amplia librería estándar están disponibles de forma gratuita en código fuente y binario para la mayoría de las plataformas, y se pueden obtener

desde la página web oficial de Python en https://www.python.org/. Además, en esa misma web se pueden encontrar distribuciones y referencias a una gran cantidad de módulos, programas, herramientas y documentación adicional desarrollados por terceros que también están disponibles de forma gratuita. [20]

2.1.4 Microsoft Threat Modeling Tool.

La herramienta de modelado de amenazas, conocida como "Threat Modeling Tool", es una parte fundamental del ciclo de vida de desarrollo de seguridad (SDL) de Microsoft. Esta herramienta permite a los arquitectos de software identificar y mitigar posibles problemas de seguridad en una etapa temprana del proceso, cuando son más fáciles y menos costosos de resolver, lo que contribuye significativamente a reducir el costo total de desarrollo. La herramienta ha sido diseñada específicamente para expertos no relacionados con la seguridad, lo que hace que sea fácil para todos los programadores crear y analizar modelos de amenazas gracias a las instrucciones claras proporcionadas. [21]

La herramienta ofrece la posibilidad a cualquier persona de:

- Comunicar el diseño de seguridad de sus sistemas. [21]
- Analizar los diseños en busca de posibles problemas de seguridad mediante una metodología probada. [21]
- Sugerir y gestionar las soluciones para posibles problemas de seguridad. [21]

2.1.5 PyCharm.

El editor de código avanzado de PyCharm cuenta con una compatibilidad de alto nivel con una amplia gama de lenguajes, como Python, JavaScript, CoffeeScript, TypeScript, CSS, lenguajes de plantillas populares y muchos otros más. Con la ayuda de la función de finalización de código, que toma en cuenta el lenguaje, la detección de errores y la corrección de código en tiempo real, podrá aprovechar al máximo su experiencia de programación. [22]

2.2 Descripción de la Solución

En la figura 6 podemos ver una representación de los componentes que presenta la solución planteada en la cual está dividida en 2 partes fundamentales las entidades y los componentes.

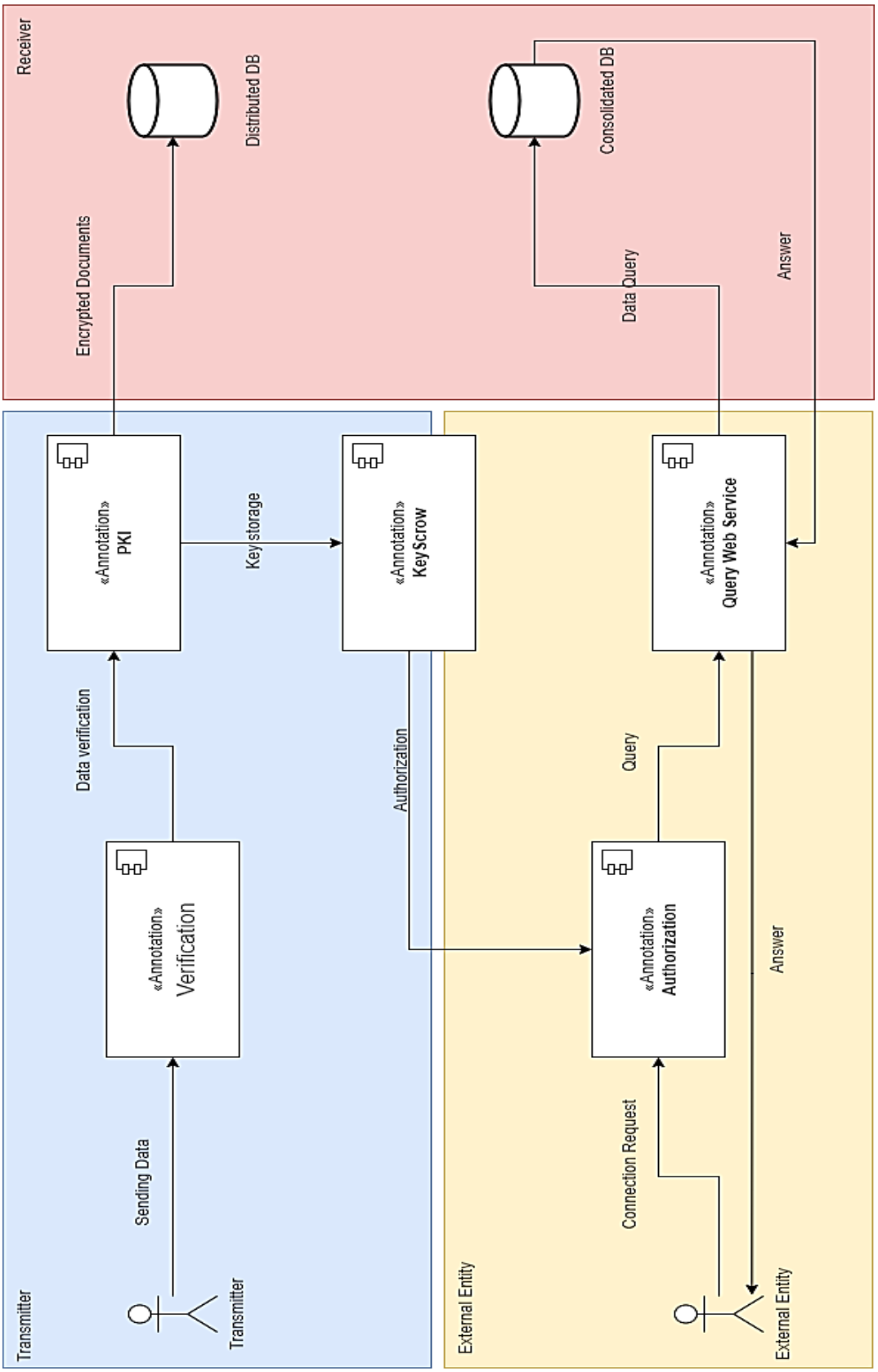

Figura 6. Diagrama de componentes para él envió seguro de información.

[Autor: Danny Venegas]

2.2.1 Descripción del diagrama de componentes

Como se puede observar en la Figura 6, el diagrama de componentes para la transferencia segura de PII, es necesario describir cada componente para su posterior implementación. Se plantea la siguiente Tabla 2 para su descripción.

Tabla 2: Descripción de cada componente.

[Autor: Danny Venegas]

Componente	***Descripción***
Entidades	Simulan los actores que tomarán parte dentro del sistema ya sea el módulo de recolección de datos, el módulo de almacenamiento, o la entidad externa que necesita consultas.
Verificación	Es el componente que valida si los datos son del origen correcto y no fueron modificados.
PKI	Es el módulo que se encarga de que se firmen los datos digitalmente para que lleguen intactos a la sección de almacenamiento.
Key Escrow	Es el encargado de almacenar los usuarios y las claves públicas y privadas de los actores.
Query Web Service	Es el encargado de crear el Query de consulta de la base de datos de la entidad externa.
Autorización	Este componente se encarga de validar y autorizar a la entidad externa para realizar consultas.

2.2.2 Pseudocódigo de diseño de solución para transferencia segura de PII.

En esta subsección se describe el pseudocódigo con los pasos del proceso de transferencia segura de PII. El pseudocódigo se muestra a continuación:

```
1. Inicio
2. Cargar Archivo;
3. Validación {
4.         ME = Ejecutar clase Mensaje (Archivo);
5. }
6. Crear Clave {
7.         Llave = Numero Randomico;
8. }
9. Encriptar Mensaje {
10.        ECM = Ejecutar la Clase Encriptado (Llave, ME);
```

```
11. }
12. Enviar ECM {
13.         Enviar al Emisor el ECM junto con la Llave
14. }
15. Fin
```

```
1.  Inicio
2.  Leer archivo;
3.  Si archivo = archivo_MTD {
4.          mensaje = archivo;
5.  } Caso contrario {
6.          imprimir "El formato de archivo no es el correcto"
7.  }
8.  Devolver mensaje;
9.  Fin
```

```
1.  Inicio
2.  Leer Mensaje;
3.  Leer Clave;
4.  Cargar Clave {
5.          Llave = Leer Llave enviada por la clase main;
6.  }
7.  Cifrar Mensaje {
8.          Cifrar mensaje;
9.          EM = Mensaje Firmado;
10. }
11. Devolver EM;
12. Fin
```

```
1.  Inicio
2.  Si se autoriza {
3.          Si la solicitud es correcta {
4.                  Realizar la consulta indicada;
5.          } Caso Contrario {
6.                  Enviar el código del error correspondiente;
7.                  Solucionar el error;
8.                  Tratar de nuevo;
9.          }
10. } Caso Contrario {
11.         Enviar el código del error correspondiente;
12.         Solucionar el error;
13.         Tratar de nuevo;
14. }
15. Fin
```

2.2.3 Solución para la transferencia de los datos personales

Como ya se había comentado en la sección 2.1.1, se creará un programa cuyo diseño deberá cumplir con las siguientes funcionalidades:

- La aplicación validará si la información proporcionada cumple con los lineamientos establecidos para la preparación del cifrado.

- La aplicación realizará un cifrado asimétrico de la información con el fin de enviarla segura a su destino.
- La aplicación crea un par de llaves públicas y privadas las cuales se almacenarán en una base de datos intermedia.
- La aplicación permitirá una conexión al sistema de manera externa y temporal que será restringida y permitirá poder realizar consultas que serán verificadas por el encargado del área de sistemas.

Este proceso se verá respaldado por el responsable del mantenimiento del sistema, quien es el representante del área de sistemas.

2.2.4 Requerimientos para la transferencia segura de datos personales

Para que el mecanismo a diseñarse cumpla con el alcance planteado, es necesario establecer un listado de requerimientos que formen parte del sistema. Los requerimientos planteados para el sistema se muestran a continuación en la siguiente Tabla 3:

Tabla 3: Requerimientos del sistema.

[Autor: Danny Venegas]

ID	**Nombre del Requerimiento**	**Descripción**	**Observación**
RF-01	Validación del Mensaje	El mecanismo debe permitir validar la información entrante.	El mecanismo autentificara si la información recibida, viene del receptor autorizado.
RF-02	Firma del documento.	El mecanismo debe permitir el firmado de la información validada.	El mecanismo firmará el documento que previamente llega de parte del componente de recolección.

RF-03	Envío de mensaje	El mecanismo debe permitir enviar el mensaje firmado por el canal de comunicación.	El mecanismo enviará el mensaje firmado por el canal de comunicación previamente creado entre las dos partes.
RF-04	Consulta de datos	El mecanismo debe permitir realizar consultas a la base de datos.	El mecanismo deberá permitir consultar datos de la base de datos consolidada.
RF-05	validación del documento	El mecanismo debe permitir validar la información que llega previamente captado.	El mecanismo validará el documento firmado de tal manera que la integridad del documento este intacta.
RF-06	Entrega de la respuesta	El mecanismo debe presentar las repuestas de las consultas.	El mecanismo mostrará las respuestas de las consultas a la base de datos consolidada.
RF-07	Creación de llaves	El mecanismo debe permitir crear llaves para el cifrado asimétrico del mensaje.	El mecanismo creará un par de llaves asimétricas que permitirán el cifrado y el descifrado del mensaje.

RF-08	Almacenado de las llaves	El mecanismo permitirá almacenar las llaves asimétricas.	El mecanismo almacenará el par de llaves asimétricas en una base de datos intermedia (Key Escrow).
RF-09	Servicio Seguro	El mecanismo permitirá autorizar las entidades que desean hacer consultas.	El mecanismo autorizará y comprobará que la entidad externa puede realizar consultas.
RF-10	Transferencia segura	El mecanismo debe permitir transmitir. los mensajes de manera segura.	El mecanismo transferirá los mensajes y las consultas al sistema de manera segura mediante cifrado asimétrico.

2.2.5 Mapeo de requerimientos entre leyes y la literatura

Una vez planteados y escritos los requerimientos que debería tener el sistema, es conveniente para el desarrollo de nuestro estudio mapear estos mecanismos o principios junto con las leyes y las investigaciones encontradas en la revisión sistemática de la literatura. Es por esto por lo que, se muestra la Tabla 4 con todo el mapeo y el cotejamiento ya mencionado.

Tabla 4: Mapeo entre requerimientos, leyes y literatura.

[Autor: Danny Venegas]

Req. No.	**Mecanismo**	**Estudio Primario SLR**				**Instrumentos**		
		Título	**Autor(es)**	**Enfoque**	**Referencia No.**	**GDRP**	**LOPDP**	**EGSI**
RF-01 ,03, 04, 06, 08,10	Transferencia	C2CFTP: Direct and Indirect File Transfer Protocols Between Clients in Client-Server Architecture	MINGYU LIM	Protocolos y estándares	[23]	Art. 12, Art. 17, Art. 33, Art. 34, Art. 54	Art. 15, Art. 18, Art. 32, Art. 45	Control 9.1.1, 9.1.2, 9.1.3, 9.2.1, 9.2.2, 9.2.4

RF-01 ,03, 04, 06, 08,10	Transferencia	Protocols for Transferring Bulk Data Over Internet: Current Solutions and Future Challenges	Khawar Khurshid; Imdad Ullah; Zawar Shah; Najm Hassan;Tariq Ahamed Ahanger	Protocolos y estándares	[24]	Art. 12, Art. 17, Art. 33, Art. 34, Art. 54	Art. 15, Art. 18, Art. 32, Art. 45	Control 9.1.1, 9.1.2, 9.1.3, 9.2.1, 9.2.2, 9.2.4
RF-02, 05,07, 08	Encripción	An Encrypted Field Locating Algorithm for Private Protocol Data Based on Data Reconstruction and Moment Eigenvector	Qing Li; Yonghui Ju; Chang Zhao; Xintai He	Protocolos y estándares	[25]	Art. 12, Art. 17, Art. 33, Art. 34, Art. 54	Art. 15, Art. 18, Art. 32, Art. 45	Control 9.1.1, 9.1.2, 9.1.3, 9.2.1, 9.2.2, 9.2.4
RF-01 ,03, 04, 06, 08,10	TSN Y DDS	Multi-Level Time-Sensitive Networking (TSN) Using the Data Distribution Services (DDS) for Synchronized Three-Phase Measurement Data Transfer	Tanushree Agarwal; Payam Niknejad; M. R. Barzegaran; Luigi Vanfretti	Redes	[26]	Art. 12, Art. 17 Art. 54	Art. 15, Art. 18, Art. 45	Control 9.1.1, 9.1.2, 9.1.3
RF-01 ,03, 04, 06, 08,10	Transferencia	RCOAP: A Rate Control Scheme for Reliable Bursty Data Transfer in IoT Networks	Dang Hai Hoang; Thi Thuy Duong Le	Redes	[27]	Art. 12, Art. 17 Art. 54	Art. 15, Art. 18, Art. 44	Control 9.1.1, 9.1.2, 9.1.3
RF-01 ,03, 04, 06, 08,10	RFID	A Secure and Practical RFID Ownership Transfer Protocol Based on Chebyshev Polynomials	Zuming Shen; Peng Zeng; Yuyin Qian;Kim-Kwang Raymond Choo	Protocolos y estándares	[28]	Art. 12, Art. 17, Art. 33, Art. 34, Art. 54	Art. 15, Art. 18, Art. 32, Art. 45	Control 9.1.1, 9.1.2, 9.1.3, 9.2.1, 9.2.2, 9.2.4

RF-01 ,03, 04, 06, 08,10	Trafico Paralelo de TCP	Enhancing Fast TCP's Performance Using Single TCP Connection for Parallel Traffic Flows to Prevent Head-of-Line Blocking	Sarfraz Ahmad; Muhammad Junaid Arshad	Protocolos y estándares	[29]	Art. 12, Art. 17, Art. 33, Art. 34, Art. 54	Art. 15, Art. 18, Art. 32, Art. 45	Control 9.1.1, 9.1.2, 9.1.3, 9.2.1, 9.2.2, 9.2.4
RF-01 ,03, 04, 06, 08,10	Wireless Two-Way Interferometry	Delay-Bounded Wireless Network Based on Precise Time Synchronization Using Wireless Two-Way Interferometry	Yamasaki, Yusuke and Chauvet, Nicolas and Shiga, Nobuyasu and Yasuda, Satoshi and Takizawa, Kenichi and Horisaki, Ryoichi and Naruse, Makoto	Redes	[30]	Art. 12, Art. 17 Art. 54	Art. 15, Art. 18, Art. 44	Control 9.1.1, 9.1.2, 9.1.3
RF-02, 05,07, 08	Encripción	A Novel Encryption Algorithm based on DNA Cryptography	A. Vikram; S. Kalaivani; G. Gopinath	Protocolos y estándares	[31]	Art. 12, Art. 17, Art. 33, Art. 34, Art. 54	Art. 15, Art. 18, Art. 32, Art. 45	Control 9.1.1, 9.1.2, 9.1.3, 9.2.1, 9.2.2, 9.2.4
RF-01 ,03, 04, 06, 08,10	RET Gadget Chains	A Novel Key Agreement Protocol Based on RET Gadget Chains for Preventing Reused Code Attacks	Wu Fusheng; Zhang Huanguo; Ni Mingtao; Wang Jun; Ji Zhaoxu	Protocolos y estándares	[32]	Art. 12, Art. 17, Art. 33, Art. 34, Art. 54	Art. 15, Art. 18, Art. 32, Art. 45	Control 9.1.1, 9.1.2, 9.1.3, 9.2.1, 9.2.2, 9.2.4

2.2.6 Propuesta de transferencia segura de datos

De acuerdo con los documentos de historias de usuario (Anexo II), Sprint Backlogs (Anexo II) y el cronograma (Anexo II), se presenta a continuación los diagramas que muestran el diseño del algoritmo, de las actividades, de las secuencias y el diagrama de clases obtenido al realizar el diseño de los componentes.

En la figura 7 se puede visualizar el flujo de trabajo que tendrá el sistema, en esta se puede visualizar con mayor detalle como estarán constituidos los componentes como también las

interacciones que estos tendrán entre sí. Empezando desde que el XML firmado del componente de recolección llega al sistema, pasando por la validación de este, donde a continuación se lo vuelve a firmar para obtener dos grados de verificación y se procede a enviar. En su segunda parte dónde se guardan las claves las cuales fueron usadas para firmar los documentos que se recibe. Y como tercera parte y final cuando llega una autorización para consultar datos, pasando a la creación del Query, realizando las consultas de la base de datos y regresando una respuesta a la parte de recolección.

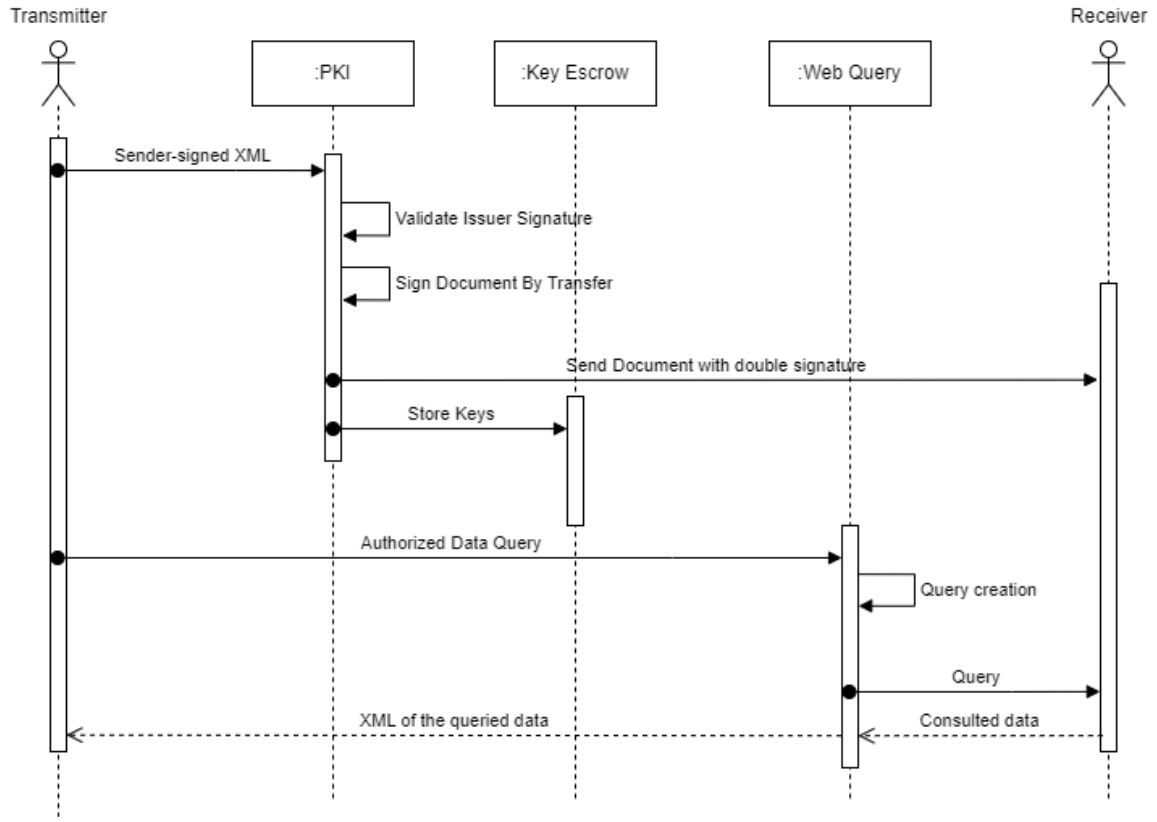

Figura 7. Flujo de trabajo del sistema de transferencia segura.

[Autor: Danny Venegas]

En la figura 8 se puede apreciar los pasos algorítmicos que toma realizar la actividad en la cual el emisor envía los datos al componente PKI, en este gráfico se puede apreciar que el sistema recibe un mensaje en este caso un XML y el algoritmo verifica sí está en este formato, en el caso de no estar en el formato adecuado presentará un mensaje de error y terminará su trabajo.

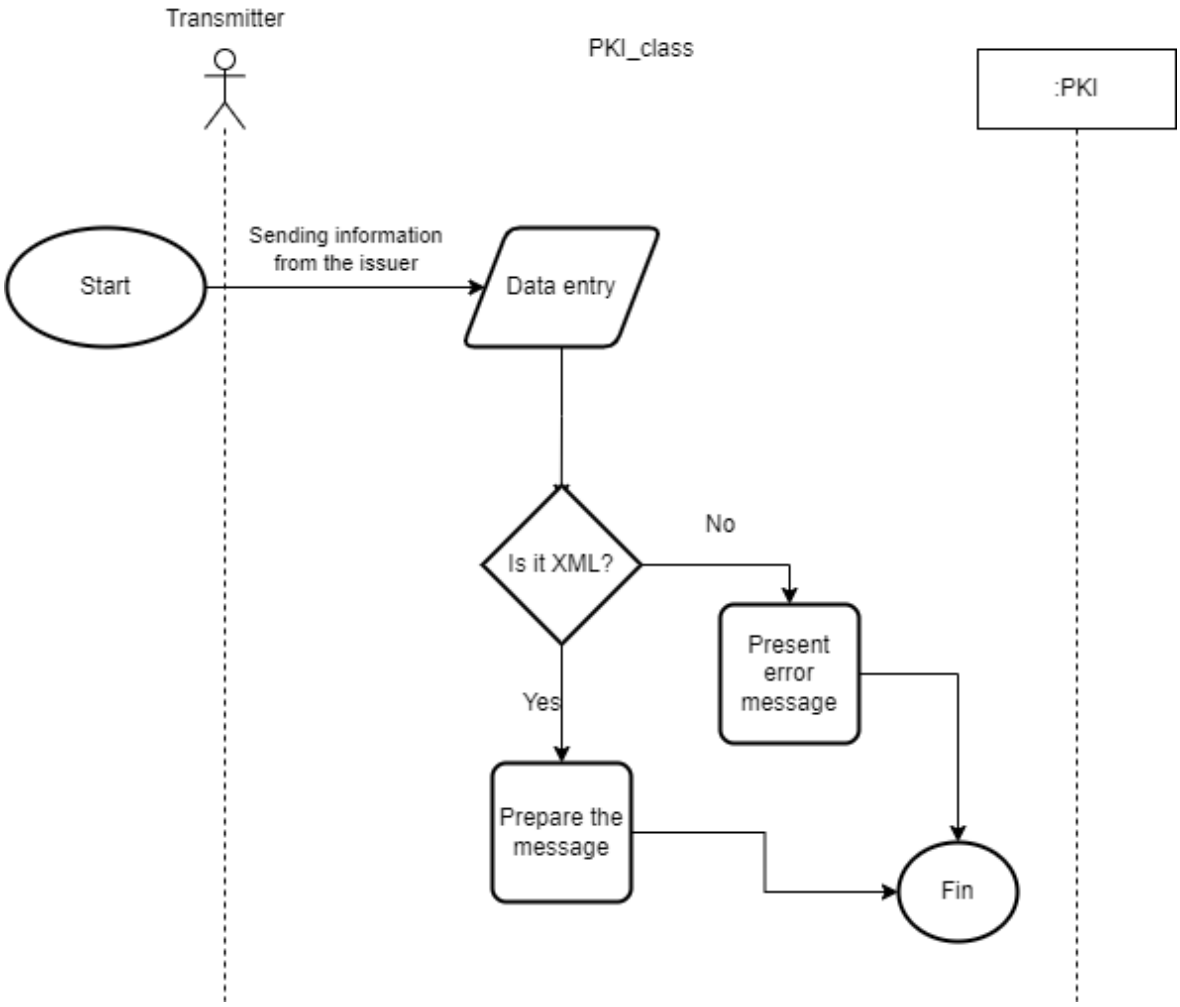

Figura 8. Diagrama de la actividad XML firmado por el emisor.

[Autor: Danny Venegas]

En la figura 9, en cambio, se puede observar los pasos algorítmicos que toma realizar la actividad que valida la procedencia del archivo XML, en este proceso se valida si la firma de la parte de recolección es válida o no, en caso de no hacerlo presentará un mensaje de error y terminará el proceso, pero si es válida se preparará el documento para la siguiente parte del flujo.

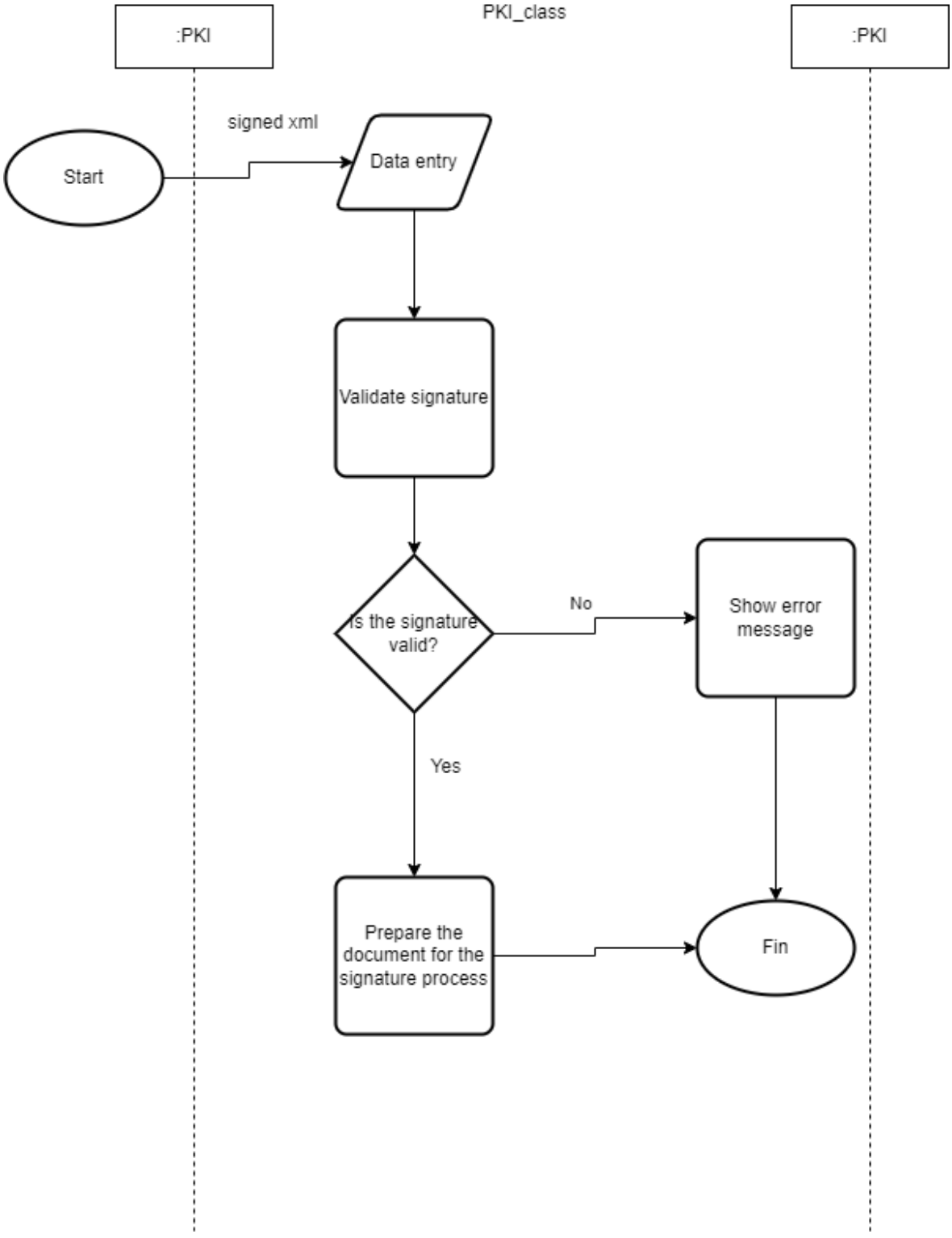

Figura 9. Diagrama de la actividad Validar Firma Emisor.

[Autor: Danny Venegas]

En la figura 10, en cambio, se puede observar los pasos algorítmicos que toma realizar la actividad que firmará el documento por parte de la transferencia, primero se recibe el XML validado, luego se crean las llaves públicas y privadas; y la firma digital. Estas llaves se guardan en una variable luego el documento se firma por segunda vez y se prepara para poder ser enviado.

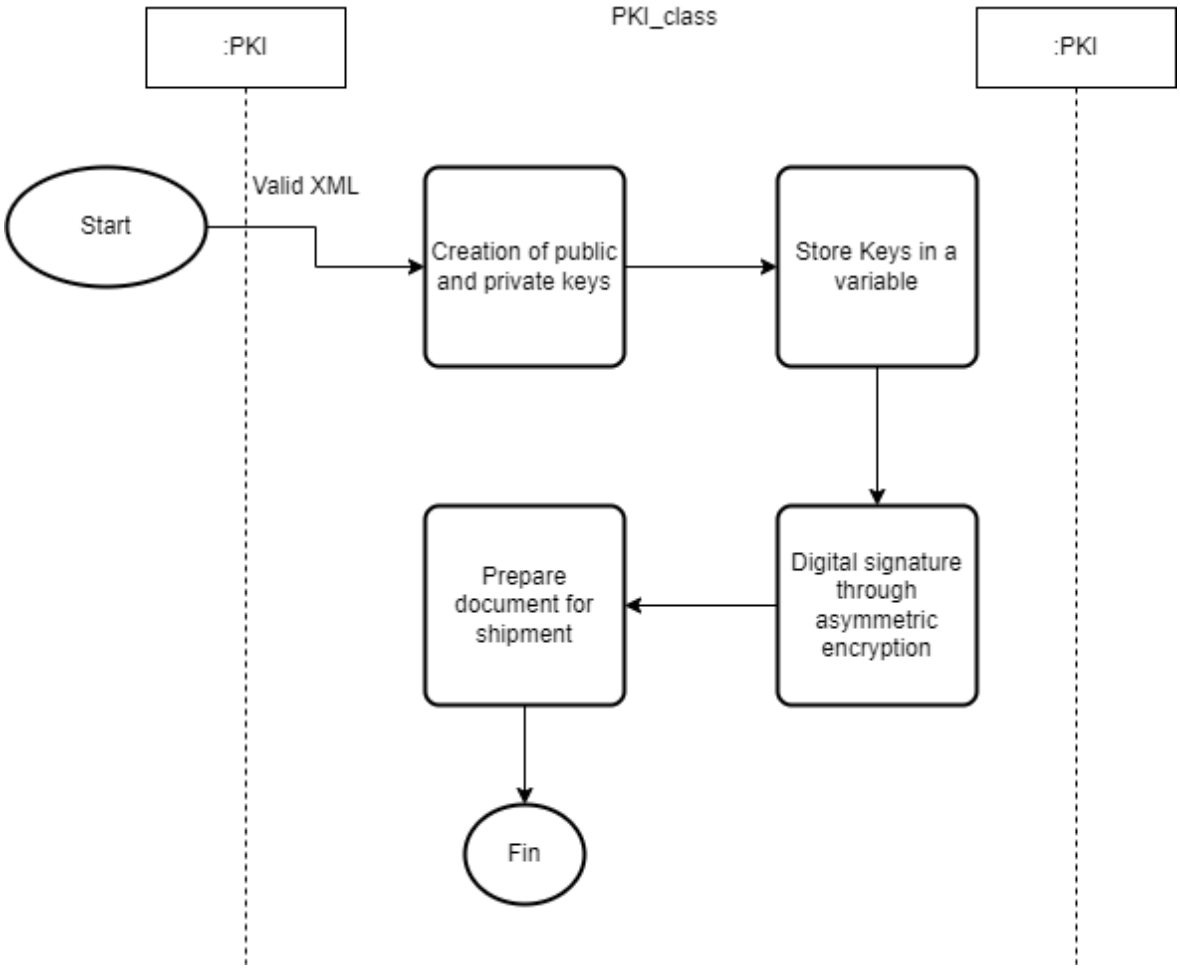

Figura 10. Diagrama de la actividad Firma del Documento.

[Autor: Danny Venegas]

En la figura 11, en cambio, se puede observar los pasos algorítmicos que toma realizar la actividad que enviará el documento con dos firmas que verifiquen su integridad, en este gráfico se presentan el algoritmo de cómo primero el documento doblemente firmado se prepara para su envío, luego se crea una conexión entre la base de datos y el componente de transferencia y este componente envía el documento doblemente firmado al componente de almacenamiento para su pertinente inserción o en caso de haber error su pertinente aviso.

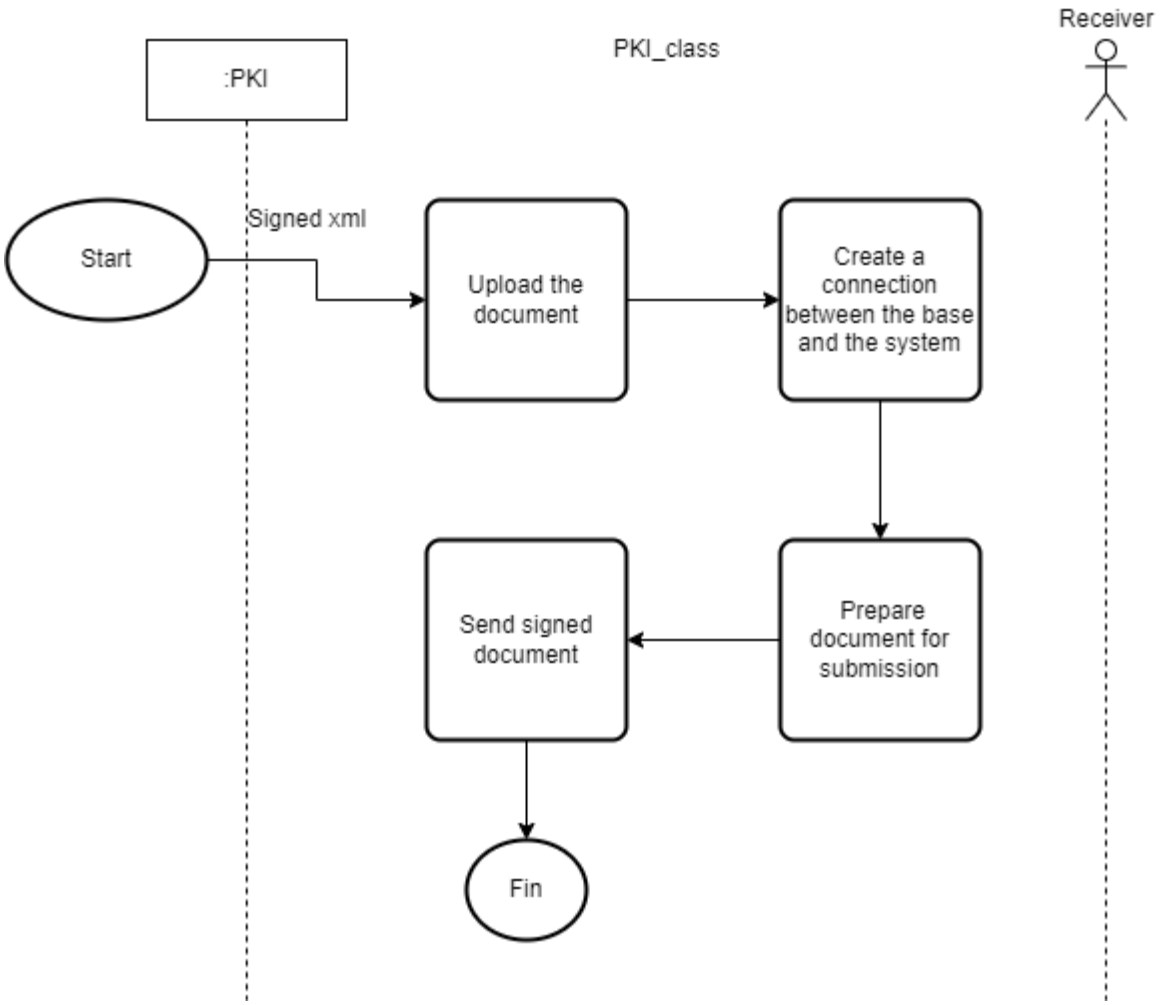

Figura 11. Diagrama de la actividad Envió de datos.

[Autor: Danny Venegas]

En la figura 12, en cambio se puede observar cómo se guardan las claves dentro del Key Escrow ya que el primer paso es cargar estas en una variable, luego crear una conexión con una base de datos intermedia crear un Query general para cargar esta variable en él Query y enviarlo a la base donde se guardarán.

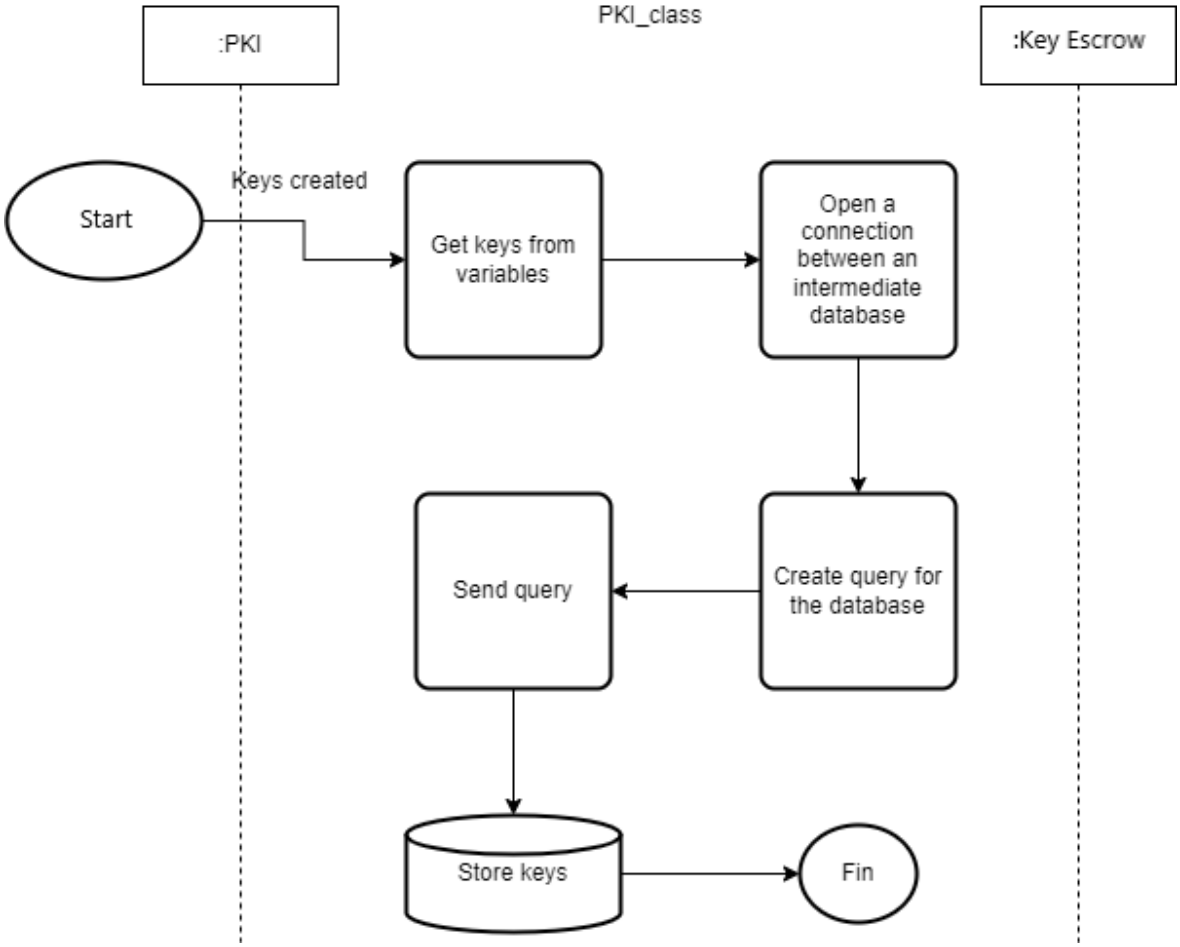

Figura 12. Diagrama de la actividad Almacenar Llaves.

[Autor: Danny Venegas]

En la figura 13, en cambio, se puede observar los pasos algorítmicos que toma realizar la actividad que pedirá consultar autorizadamente los datos de la base, se obtiene información de la parte de recolección ya sea la autorización o el permiso para ejecutar la consulta luego se revisa si esta autorización es válida o no si es válida se prepara el mensaje para la creación del cuerpo y si no se presenta un mensaje de error.

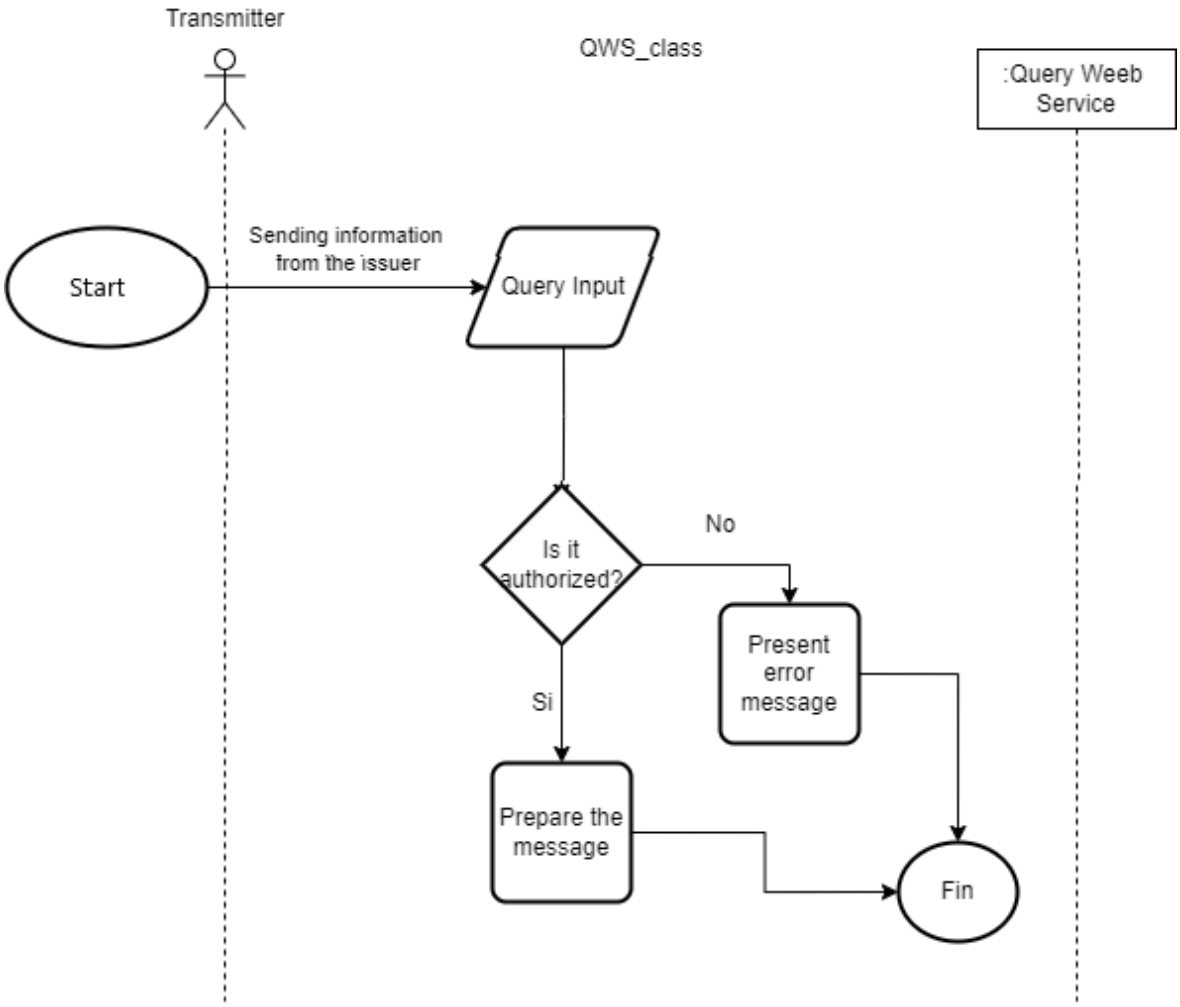

Figura 13. Diagrama de la actividad Consulta de datos autorizados.

[Autor: Danny Venegas]

En la figura 14, en cambio, se puede observar los pasos algorítmicos que toma realizar la actividad que crear una sentencia que permitiera consultar los datos, en el primer paso se obtienen los datos de la consulta, estos vienen por la parte de recolección, a continuación, cargamos esos datos en una variable, creamos un Query, insertamos las variables en el Query y preparamos la sentencia para enviársela a la base de datos para la consulta.

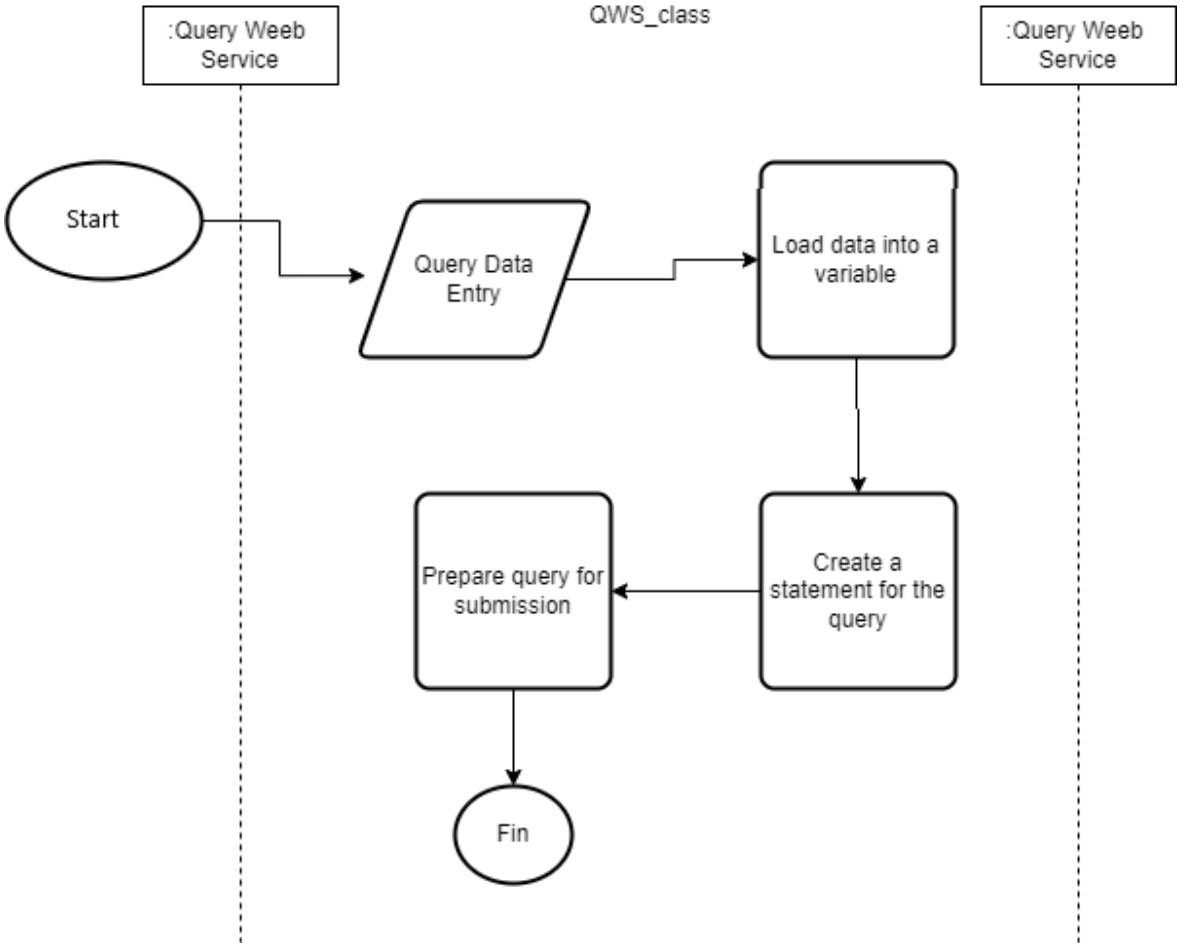

Figura 14. Diagrama de la actividad Creación de Query.

[Autor: Danny Venegas]

En la figura 15, en cambio, se puede observar los pasos algorítmicos que toma realizar la actividad que enviará la consulta a la base de datos, como en la figura anterior ya obtuvimos la sentencia Query ahora lo primero que se hace es realizar una conexión a la base de datos, enviamos el Query, obtenemos los datos que nos da de resultado haber hecho esa consulta y preparamos un XML para presentarlo y enviarlo a la parte de recolección que es la encargada de mostrar los resultados a la entidad externa.

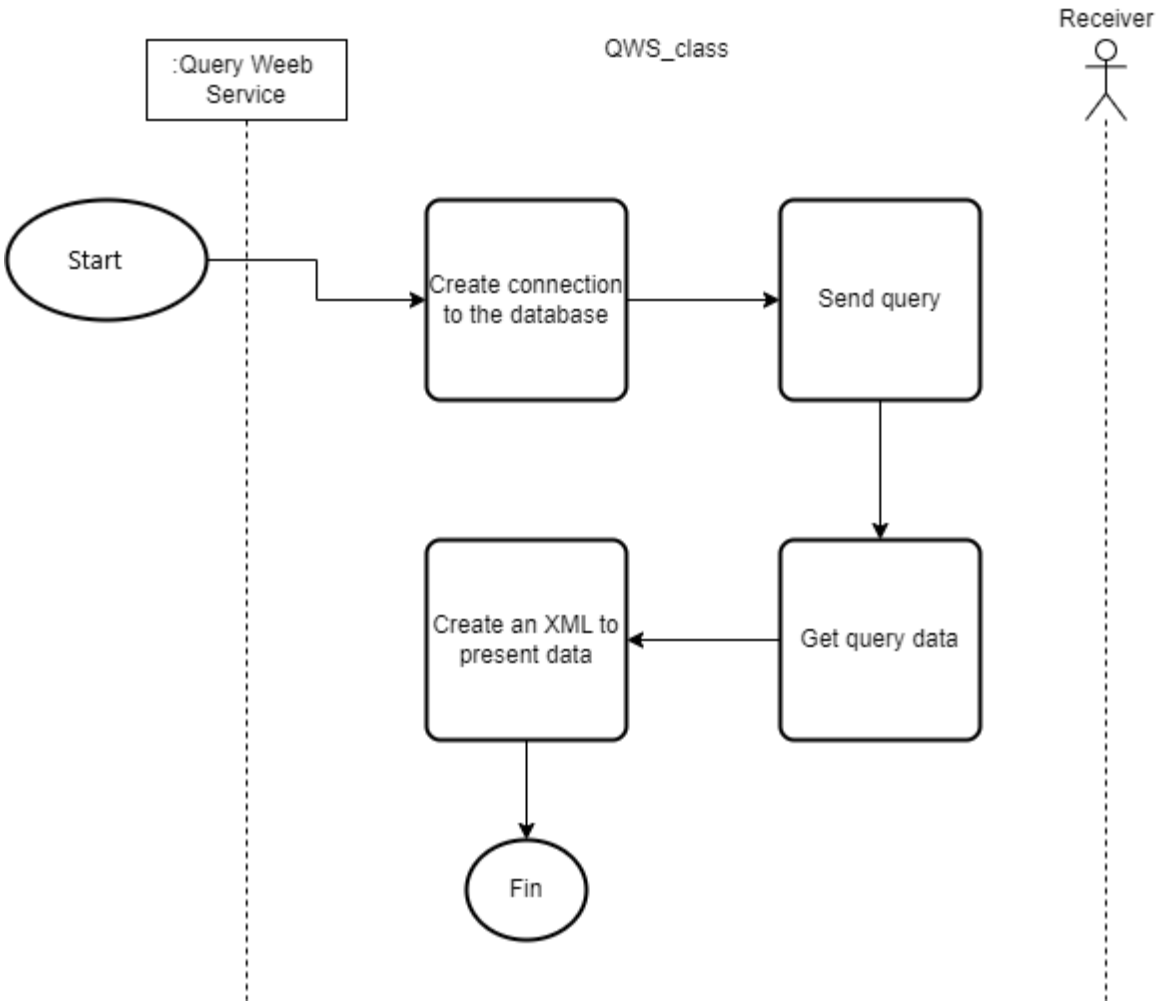

Figura 15. Diagrama de la actividad Consultar.

[Autor: Danny Venegas]

Por último, en la figura 16 se puede apreciar el diagrama de clase que se obtuvo al obtener todas las actividades y completar el flujo de trabajo de la solución, podemos apreciar cómo terminó el diagrama de clases donde tenemos 3 clases importantes que son PKI que es la clase que se va a encargar de verificar las firmas, firmar documentos y enviar el documento firmado, después esta la clase KS qué es la encargada de almacenar las llaves públicas privadas con las que se firman los documentos y los usuarios que se crean tanto para la entidad externa como también los usuarios recurrentes de la empresa. y por último la clase Query web service que es la encargada de crear los Querys para consultar datos como también de verificar que las autorizaciones que reciben de parte del componente de recolección sean válidos y correctos.

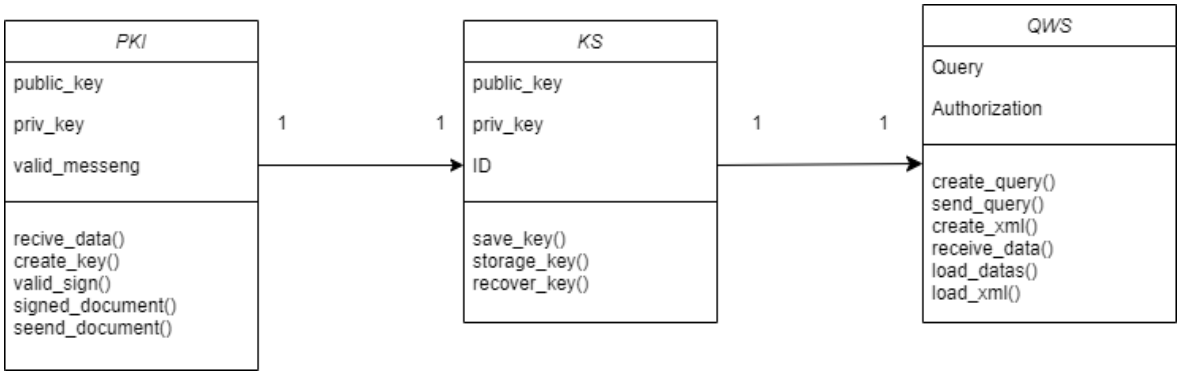

Figura 16. Diagrama de clases de la solución.

[Autor: Danny Venegas]

En la figura 17 podemos apreciar cómo terminó siendo la arquitectura del componente dentro proyecto integrador curricular, en la figura podemos apreciar en cómo se divide en los tres partes y cuáles son el PKI la entidad encargada del envió de los datos, el key Escrow encargado del almacenamiento de las llaves y el Query web servide encargado de las consultas a las bases consolidadas. Para ver la arquitectura completa del proyecto TIC mirar el Anexo III.

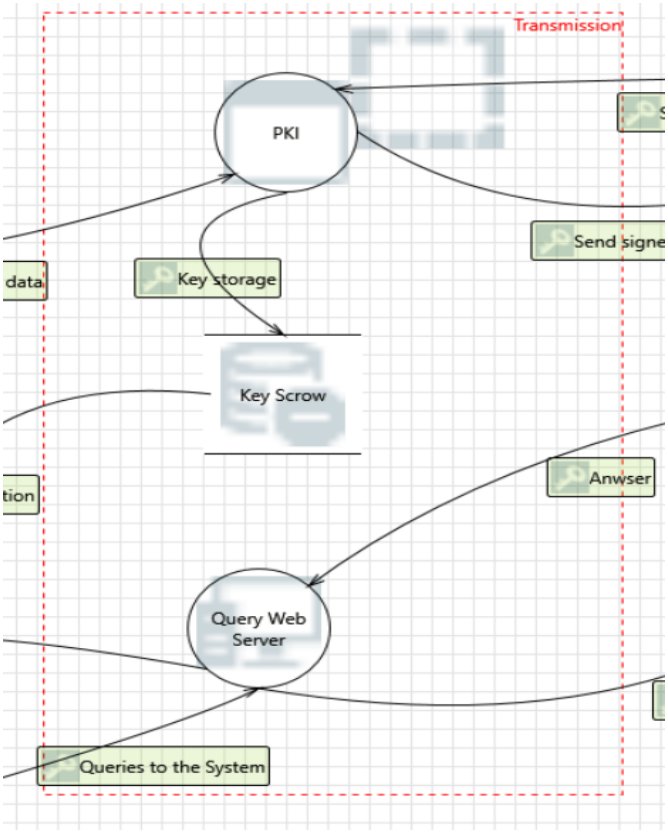

Figura 17. Arquitectura del Componente de transferencia del Proyecto TIC.

[Autor: Danny Venegas]

3. EVALUACIÓN, CONCLUSIONES Y RECOMENDACIONES

3.1 Pruebas

Dentro de las pruebas que se realizaron para obtener resultados al proyecto se encuentran dos tipos de estas; las pruebas funcionales y las pruebas de rendimiento. A continuación, presentaremos los resultados obtenidos al implementar estos dos tipos de pruebas.

3.1.1 Pruebas Funcionales.

En la figura 18 se puede visualizar cómo está estructurado la sección que corresponde al PKI, donde se verifica que las firmas sean correctas y se procede a firmar el documento nuevamente para su envío y así tener dos factores de autenticación, el resultado de esto se puede apreciar en la figura 19 dónde se muestra una impresión en consola del proceso.

```python
@app.route('/recibirDanny', methods = ['POST'])
def recibirDanny():
    # Recibir el XML como un diccionario
    xml_firmado_william = request.get_json()
    if verificar_xml(xml_firmado_william):
        (pubkey2, privkey2) = obtenerClaves("danny.venegas")
        xml_firmado_danny = firmar_xml(xml_firmado_william, privkey2, pubkey2)
        cert = ('certificados/cert.pem', 'certificados/key.pem')
        #url = 'http://127.0.0.1:5000/recibirCris'
        url = 'https://127.0.0.1/recibirCris'
        headers = {'Content-type': 'application/json'}
        response = requests.post(url, data=json.dumps(xml_firmado_danny),
                                 headers=headers,
                                 #cert=cert,
                                 verify = False
                                 )
        if response.status_code == 200:
            print("Datos enviados exitosamente.")
        else:
            print("Error al enviar los datos: %s" % response.text)
    return "Respuesta válida"
```

Figura 18. Algoritmo de PKI.

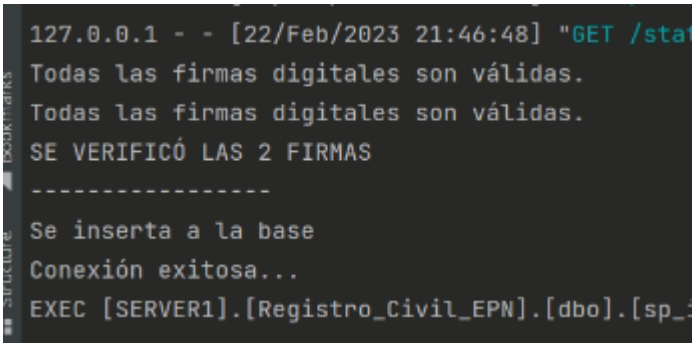

Figura 19. Algoritmo de PKI.

En la figura 20 tenemos representado como está constituido el Query web service en el que el algoritmo está dividido por niveles cada uno con su seguridad dependiendo de la autorización que llegue de la parte de recolección y su resultado podemos apreciarlo en la figura 21 en cuál es una representación en formato XML de los datos qué se consultaron a la base.

```
def obtener_datos():
    # Llamar la función y pasar los parámetros necesarios
    #cedula = "1726264961"
    #SQL = "SELECT nombres, apellidos, lugar_nacimiento FROM Persona where cedula = \'"+ str(cedula) + "\'"
    usuario = session.get("usuario")
    if usuario == 'empresa1':

        #Nivel 1
        SQL = 'SELECT * FROM v_obtenerDatosNivelUno'
        #Nivel 2
        #SQL = 'SELECT * FROM v_obtenerDatosNivelDos'
    if usuario == 'empresa2':
        #Nivel 3
        SQL = 'SELECT * FROM v_obtenerDatosNivelTres'
        #Nivel 4
        #SQL = 'SELECT * FROM v_obtenerDatosNivelCuatro'
    if usuario == 'empresa3':
        #Nivel 5
        SQL = 'SELECT * FROM v_obtenerDatosNivelCinco'
    datos_xml = obtenerDatosSqlServerXML('SERVER1', 'Salva_Datos_EPN', 'sa', 'smile', SQL)
    #datos_xml = obtenerDatosSqlServerXML('172.28.32.52', 'mi_bd', 'sa', 'smile', "SELECT * FROM persona")
    # Devolver los datos XML con el tipo de contenido adecuado
    return Response(datos_xml, mimetype='text/xml')
```

Figura 20. Algoritmo de QWS.

Figura 21. Consulta a la base de datos.

En la figura 22 se visualizar el código necesario para la inserción de datos en el Key Escrow esto para que se guarden las llaves de los usuarios que estarán a cargo de la transferencia y que serán quienes firmen los documentos, y en la figura 23 podemos observar los datos guardados en la base llamada keys Escrow.

```python
def scrow_key(username,pubkey, privkey):
    # Convierte las claves a cadenas de texto en formato pkcs1 para poder almacenarlas en la base de datos
    pubkey_str = pubkey.save_pkcs1().decode('utf-8')
    privkey_str = privkey.save_pkcs1().decode('utf-8')

    # Crea un documento de la clave en la colección
    key_document = {
        'username': username,
        'pubkey': pubkey_str,
        'privkey': privkey_str
    }
    keys_collection.insert_one(key_document)  # Inserta el documento en la colección
```

Figura 22. Insertar Llaves Key Escrow.

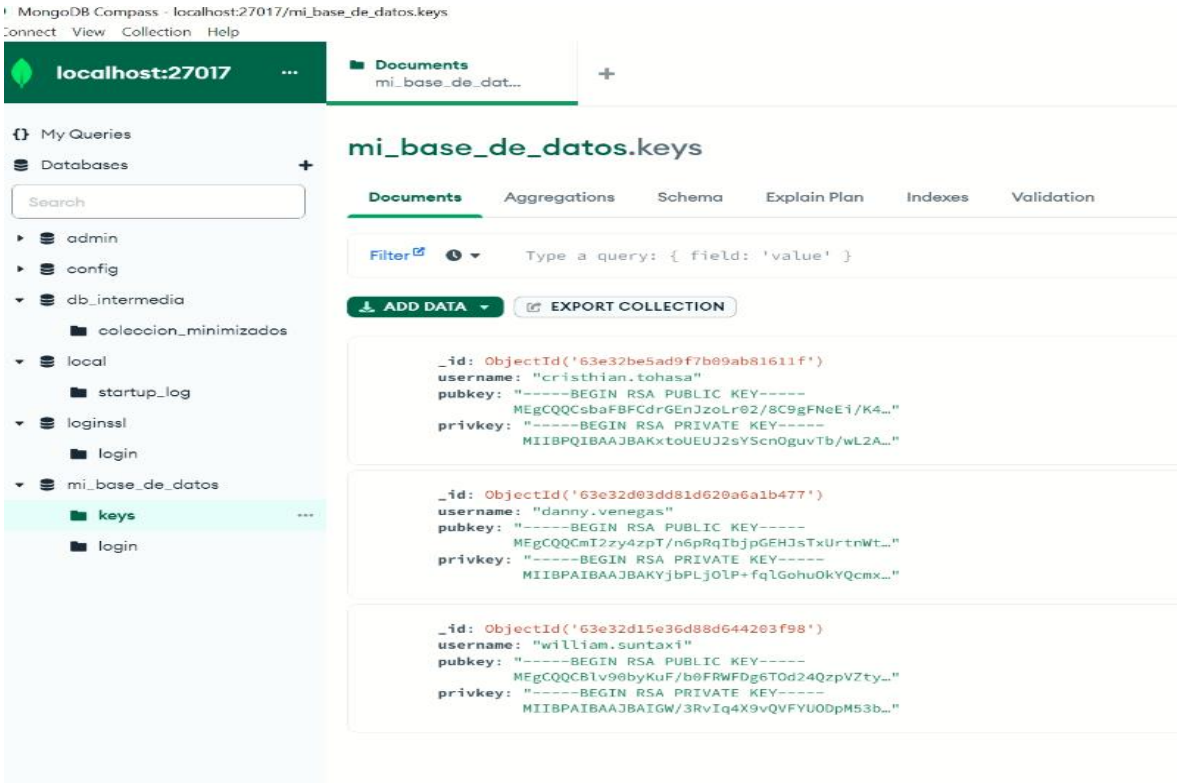

Figura 23. Key Escrow.

3.1.2 Pruebas Rendimiento.

En esta sección visualizaremos los resultados y graficas obtenidas al hacer las pruebas de rendimiento del sistema, cabe aclara que la aplicación se realizo de manera local y sin ser cargada en un servidor en línea. Esto debido a las limitantes económicas del grupo como también al ser desarrollado en entornos virtualizados llamados VDI otorgados por la Escuela Politécnica Nacional. Por lo que los valores de red, tales como, throughput de red, el ancho de banda entre otros, no serán tomado en cuento debido a que la herramienta de monitoreo de rendimiento de Windows daba estos valore como cero, o no recolectaba ningún valor.

En la figura 24 podemos apreciar las métricas que se iban agregando para que la herramienta Windows recolecte los valores de las pruebas de rendimiento.

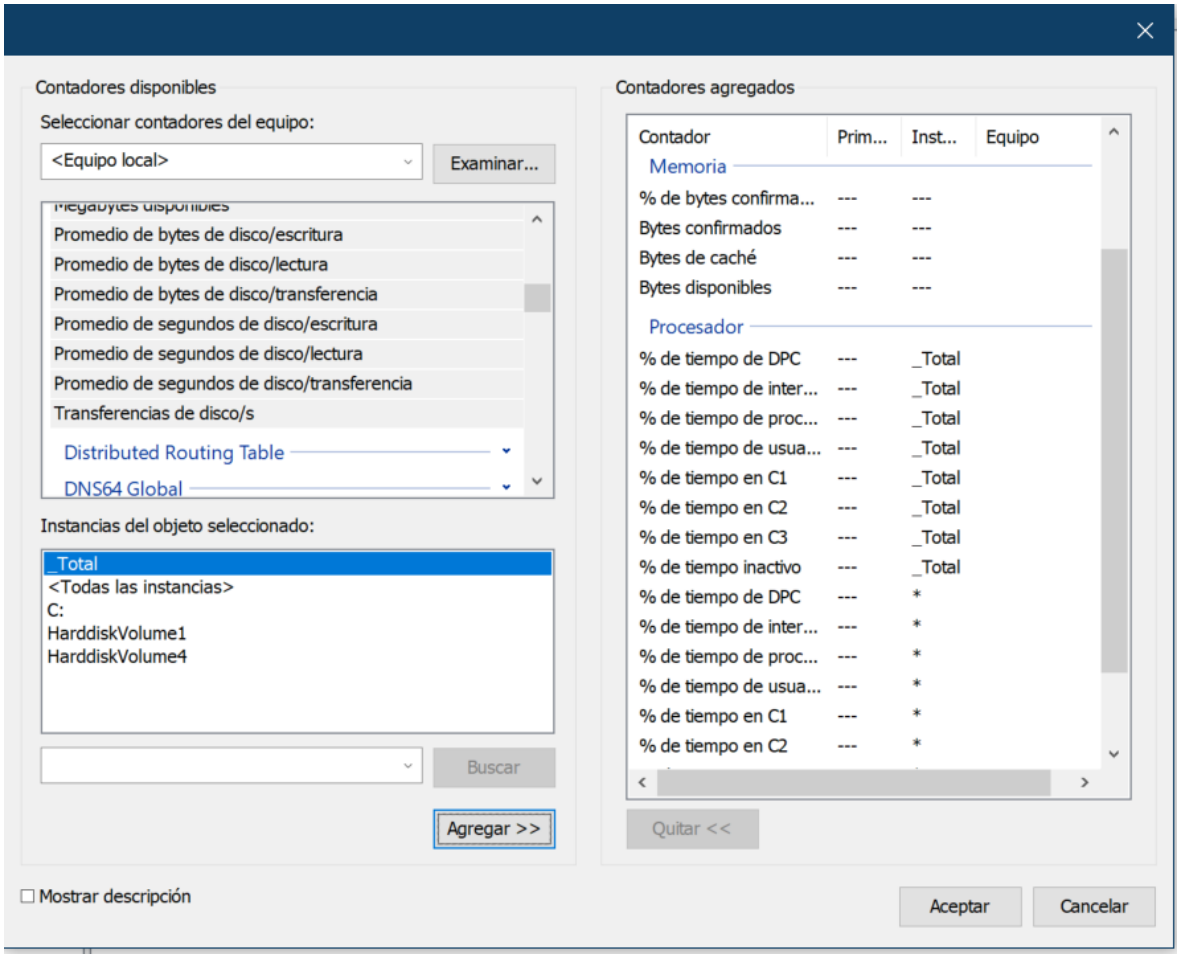

Figura 24. Herramienta de recolección de datos de Windows.

En la figura 25 se puede visualizar la cantidad de bytes que el disco físico recibe al momento de escribir cuando se realizan las iteraciones del programa.

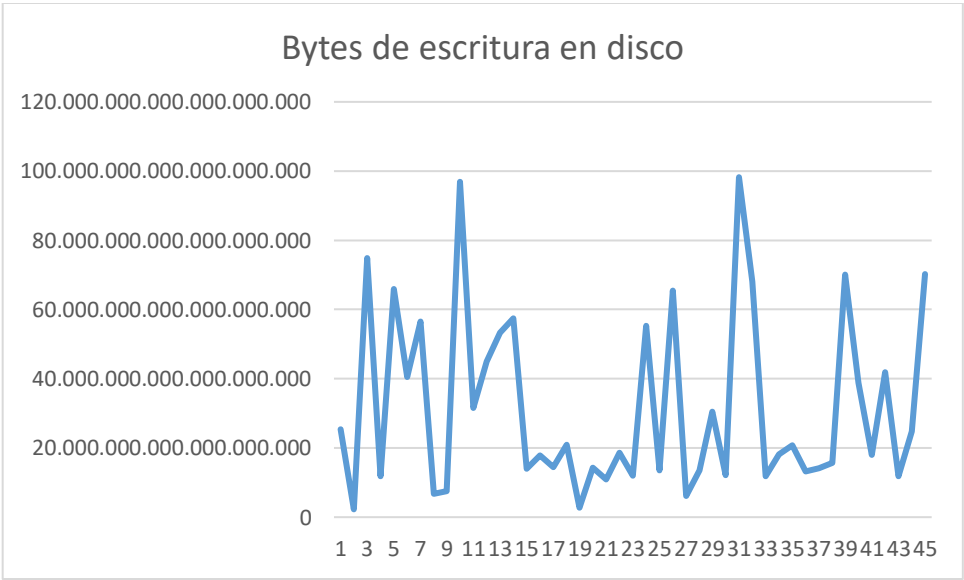

Figura 25. Resultados de las pruebas de rendimiento de escritura en el disco.

En la figura 26 en cambio podemos visualizar los bytes al momento de la lectura del disco igual que en el anterior mientras se están realizando las iteraciones del programa.

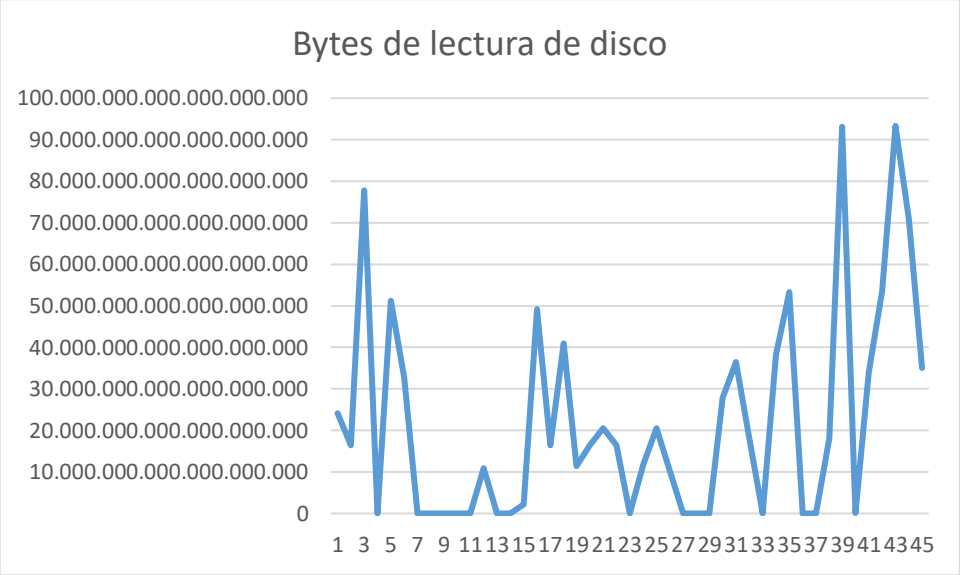

Figura 26. Resultados de las pruebas de rendimiento de lectura en el disco.

En la figura 27 se puede apreciar los bytes que se guardaban en caché al momento qué se realizaba cada iteración del programa.

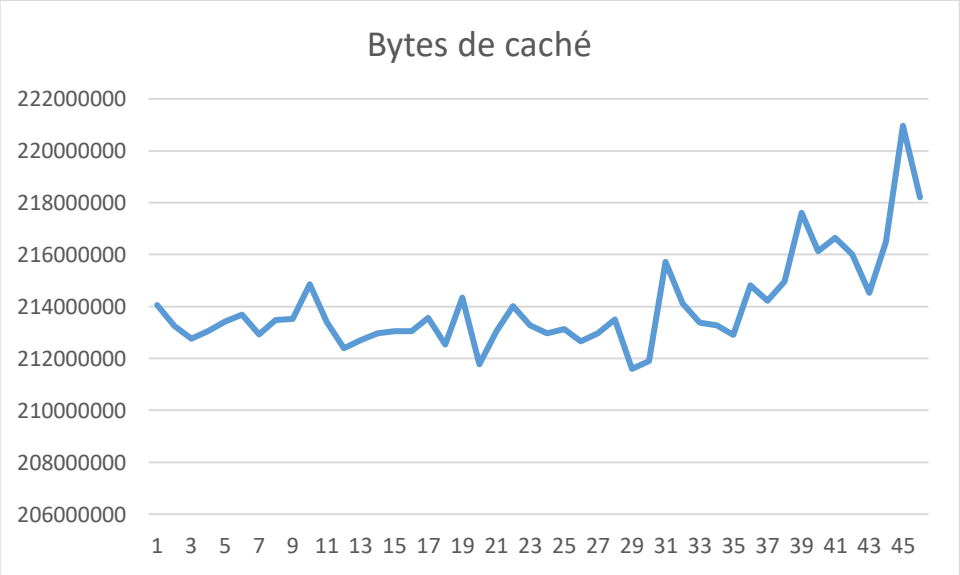

Figura 27. Resultados de las pruebas de rendimiento de los Bytes usados en la memoria cache.

En la figura 28 se puede visualizar los bytes de la memoria que estaban disponibles al momento de ejecutar cada iteración del programa.

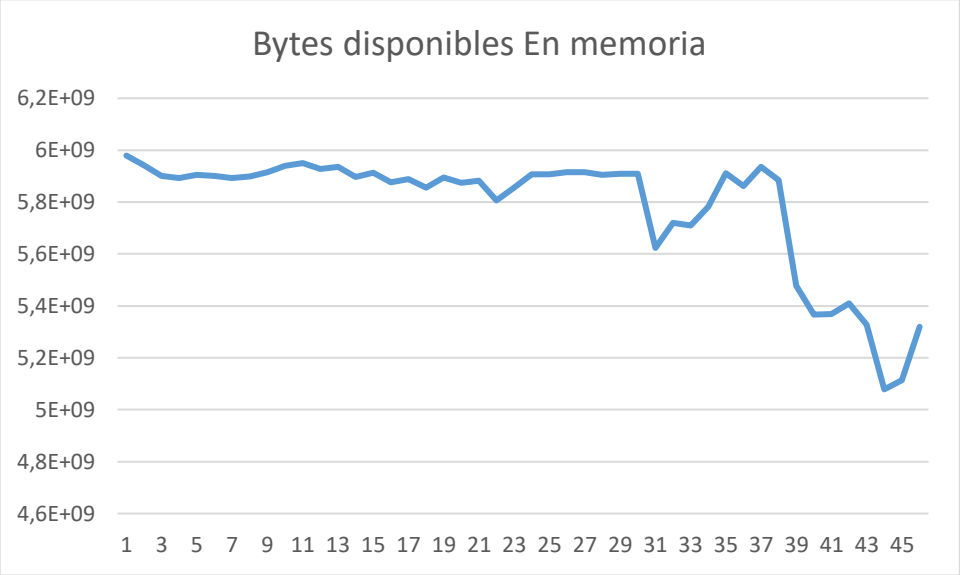

Figura 28. Resultados de las pruebas de rendimiento de los Bytes disponibles en memoria.

En la figura 29 podemos observar el porcentaje del tiempo de procesador en cada iteración del programa. Hay que tener en cuenta que este tiempo esta denotado por ciclos de procesador.

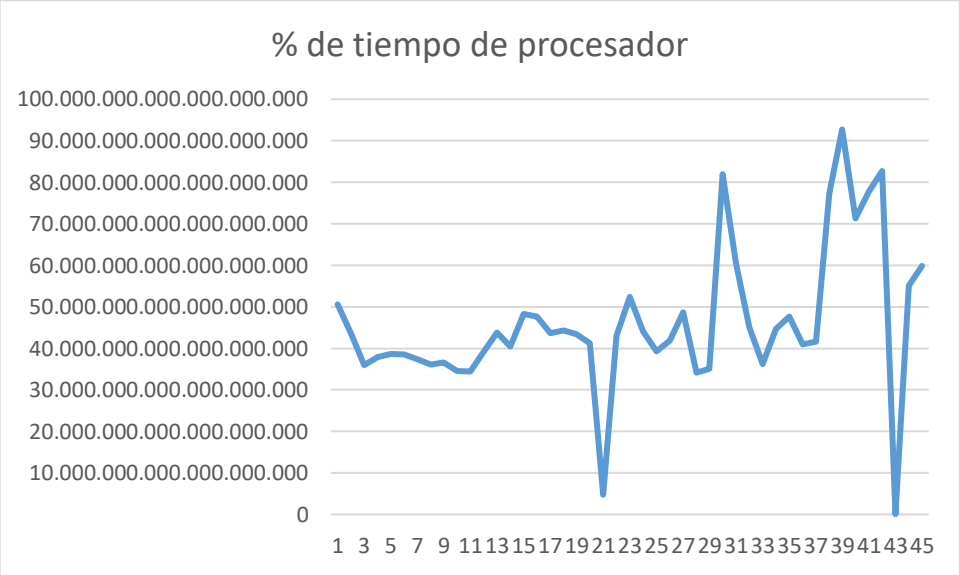

Figura 29. Resultados de las pruebas de rendimiento del procesador.

En la figura 30 podemos observar el porcentaje de tiempo en el que el procesador estaba inactivo durante cada iteración. Al igual que en el anterior estos valores muy grandes son dados porque están medidos en ciclos del procesador.

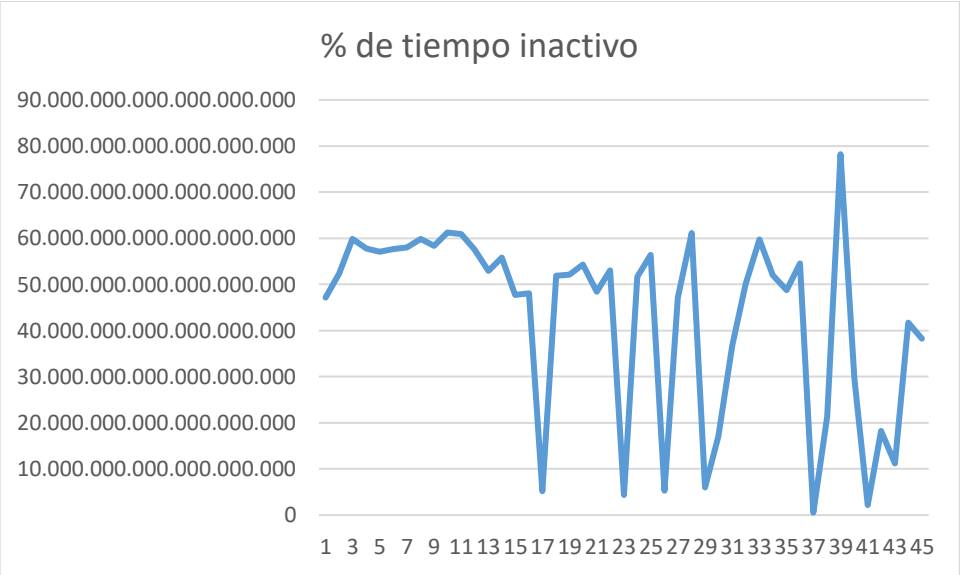

Figura 29. Resultados de las pruebas de rendimiento del procesador cuando estuvo inactivo.

3.1.3 Modelado de Amenazas.

Usando la herramienta Microsoft Threat Modeling Tool, se ingresó la arquitectura vista de la figura 17 la cual permitió obtener un reporte (Véase Anexo III) detallado de las amenazas que nuestra arquitectura pudiera recibir.

En la tabla 5 mostrada a continuación podremos ver una descripción de las amenazas más importantes y los controles implementados para su mitigación. Estos controles fueron implementados en el proyecto para obtener un grado de seguridad contra amenazas externas e internas que pudiese tener la arquitectura, A si teniendo un grado aceptable de resiliencia ante estas.

Tabla 5: Evaluación de Riesgo.

Nro.	Amenaza	Descripción	Responsable	Riesgo	Opción (1,2,3,4)	Control (si opción = 1)
R8	Elevation by Changing the Execution Flow in Browser Client	An attacker may pass data into Authentication in order to change the flow of program execution within Authentication to the attacker's choosing.	Danny Venegas	3	1	Verificación de dos factores de autenticación

R16	Persistent Cross Site Scripting	The web server 'Query Web Server' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'Consolidated database' inputs and output.	Danny Venegas	4	1	verificación de dos factores de autenticación y niveles de autorización
R17	Cross Site Scripting	The web server 'Query Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input	Danny Venegas	4	1	verificación de dos factores de autenticación y niveles de autorización
R39	Elevation Using Impersonation	Query Web Server may be able to impersonate the context of Authentication in order to gain additional privilege.	Danny Venegas	4	1	validación de autorización
R54	The SQL Database Data Store Could Be Corrupted	Data flowing across Send signed XML may be tampered with by an attacker. This may lead to corruption of Distributed database. Ensure the integrity of the data flow to the data store.	Danny Venegas	3	1	Firma digital
R62	Elevation by Changing the Execution Flow in Native Application	An attacker may pass data into PKI in order to change the flow of program execution within PKI to the attacker's choosing.	Danny Venegas	4	1	validación de autorización
R69	Elevation by Changing the Execution Flow in Native Application	An attacker may pass data into PKI in order to change the flow of program execution within PKI to the attacker's choosing.	Danny Venegas	4	1	validación de autorización

3.2 Discusión de resultados

Si visualizamos las figuras mostradas en la sección anterior podemos denotar que el programa cumple con su función, que es enviar los datos desde un formulario hasta la base de datos. De manera segura, ya que este componente es un medio de transporte seguro de datos. El componente implementa controles de seguridad muy eficaces contra atacantes externos ya que el programa cuenta con doble factor de autentificación reflejado en la doble firma digital, por parte del componente de recolección y del componente de transferencia. El cual el componente de almacenamiento verificara. Este control permite comprobar la integridad en todo el trayecto del documento.

Otro aspecto fundamental es la implementación del Query web Service. Con el fin de otorgar a entidades externas un acceso remoto a consultas de la base de datos. Pero sin descuidar la seguridad. Esta sección fue pensada e implementada teniendo en cuenta las necesidades de auditoria de una empresa. Dando un acceso controlado y sin elevación de privilegios. Obteniendo una seguridad para el sistema. El funcionamiento de esta parte de la arquitectura radica en la autorización por niveles proporcionada por la parte de recolección y verificada por la parte de la transferencia otorgando un nivel de visibilidad de los datos de la empresa. Entre las pruebas se dieron los casos en que una empresa de auditoria pedía revisar los datos de la base, y en el otro el presidente de la república pedía entrar y consultar datos de la base. En esos dos escenarios las vistas dependían de cada autorización donde en la primera se entregaban datos muy generales y en los otros datos completos almacenados.

Ahora en cuestión de rendimiento la aplicación fue desarrollada en el lenguaje Python, usando el IDE de PyCharm ya que este es un estudio profesional para trabajar Python. A su vez que la EPN proporciona licencias profesionales para trabajar de mejor manera en este IDE. Para el equipo se utilizó una aplicación de escritorio virtual VDI con las especificaciones de 500 GB de disco, y 16 GB de RAM. Y un procesador que tenía cuatro núcleos. Con el fin que se ejecutar de manera rápida y sin problemas computacionales. Esto se puede ver reflejado en las gráficas de rendimiento anteriores. Donde le programa tiende a tener un consumo moderado y aceptable de recursos, sin tener picos muy altos ni tampoco un uso excesivo de estos. También podemos denotar que tanto como la memoria y el disco. Aumentaban después de cada iteración esto ya que en el disco almacenaba más información de llaves de empresas guardándose en el Key Escrow por cada iteración. Como también en la memoria cache se iba almacenados procesos para agilizar el proceso y no gastar más recurso del computador. Luego de realizar 45 iteraciones, el rendimiento de la aplicación seguía rápido y sin demoras. Un gran logro ya que el componente de

transferencia llevaba a cabo los proceso sin demora y sin problemas que aumenten la latencia de respuesta del envió de documentos y la obtención de datos para las consultas.

En cuestión de las evaluaciones de amenazas y riesgos. Como se puede observar en la tabla 5 existen amenazas que tiene un valor de riesgo muy alto. Es por este motivo que se implementaron controles que mitiguen este valor y lo reduzcan. Esto obtuvo como resultado que el valor del riesgo se reduzca de manera drástica permitiendo así tener un impacto y probabilidad muy baja y así demostrando que el componente no solo es ágil, sino que seguro y resistente. Como también resiliente a posibles ataques. Para otras posibles amenazas se decidieron otras vías de tratamiento tales como aceptar que no se puede controlar. Esto para amenazas con un grado de riesgo extremadamente bajo, otra forma fue transferir ya que son partes de la arquitectura que pueden contratar servicios de otras empresas y que estas implementen los controles requeridos. Para una información mas detallada véase el Anexo IV donde se encuentra la evaluación completa y los valores de impacto y probabilidad luego del tratamiento con los controles.

3.3 Conclusiones

Al finalizar el proyecto se pudo obtener conclusiones muy acertadas tales como:

- El análisis del estado del arte fue una pieza fundamental dentro del proyecto dándonos las bases teóricas y trabajos relacionados que nos ayuden y nos guíen para crear nuestra arquitectura y desarrollar la aplicación computacional.
- Se logro identificar los correctos requisitos fundamentales del proyecto los cuales dieron inicio a idealización y posteriormente a la implementación de los controles que asegurarían la aplicación. Lo que llevo a dar solución a las amenazas mas importantes visualizadas al realizar la evaluación de riesgos.
- De acuerdo con los requerimientos y el mapeo realizado de las bases legales como GDPR europeo. La LOPDP ecuatoriana y el EGSI junto con los estudios primarios obtenidos se logró desarrollar un prototipo experimental que cumple con los parámetros establecidos de estas bases. Tal prototipo cumple con los parámetros de agilidad y seguridad.
- Gracias a un entorno controlado dentro de las VDI. Se pudo lograr una evaluación del prototipo. La cual fue dividida en tres secciones. Funcionalidad: La cual cumple exitosamente con el propósito del proyecto. Rendimiento: La aplicación es altamente eficiente y sin ningún problema de recursos. Resiliencia: Los controles

implementados lograr mitigar las amenazas más relevantes permitiendo así tener un gran grado de seguridad.

- Se consiguió implementar un mecanismo de gestión PII durante la transferencia. Dando la posibilidad de que las empresas ejecuten este mecanismo dentro de su organización y puedan cumplir con la ley de protección de datos

3.4 Recomendaciones

- Se recomienda realizar la investigación que permita que el proyecto pueda ejecutarse como un servidor en línea que permita evaluar el rendimiento y compararlo con el otro servicio en línea como lo es “Dato Seguro”.

- Se recomienda el estudio de otras formas de cifrado, el proyecto utilizo el sistema de firmado digital. Debido a que permite comprobar la integridad del documento y evita sus alteraciones. Pero existen otras formas como la marca de aguda digital o el cifrado asimétrico en sus diferentes variables.

- Se recomienda realizar un estudio comparativo que permita evaluar y comparar las diferentes formas de cifrado y en que influirían si estas son implementadas en la arquitectura en ves de la firma digital.

- Se recomienda realiza un estudio de componentes relevantes que pudieran ser añadidos al proyecto. Y que permitan una mejor eficiencia, capacidad y aumento de la seguridad. Con el fin de agregar más funcionalidades permitiendo que el proyecto tenga un mejor escaldo y una gran capacidad de adaptabilidad.

4. REFERENCIAS BIBLIOGRÁFICAS

[1] Gabriel Baca Urbina, *Introdución a la Seguridad informatica*. Mexico D.F., Mexico: Grupo Editorial Patria, 2016.

[2] Technopedia. File Transfer. [Online]. https://www.techopedia.com/definition/7192/file-transfer

[3] IBM. Transferencia de archivos. [Online]. ibm.com/es-es/topics/file-transfer

[4] Progress Software Corporation. ¿Qué es el Protocolo de transferencia de archivos (FTP)? [Online]. https://www.ipswitch.com/es/blog/que-es-el-protocolo-de-transferencia-de-archivos-ftp

[5] IBM. FTP. [Online]. https://www.ibm.com/docs/es/aix/7.1?topic=protocols-file-transfer-protocol

[6] IBM. Protocolo Telnet. [Online]. https://www.ibm.com/docs/es/aix/7.1?topic=protocols-telnet-protocol

[7] Santiago Fernández, "LA CRIPTOGRAFÍA CLÁSICA," *LA CRIPTOGRAFÍA CLÁSICA*, Abril 2004. [Online]. https://d1wqtxts1xzle7.cloudfront.net/38520592/9_Criptografia_clasica-with-cover-page-v2.pdf?Expires=1667957071&Signature=MYCpVbOp6pL1pYYTdWP7seijbNitfq5xQfYx30TcE6k5o1pdr7CQbhrt8PwPZ6DcufyT6Z5RsSsBe~mndQSKw0WCli4GnB~lVxxIFDdcviSTVNeQ8-EQ7v~-Sx0n4PoMf2LpH

[8] José Roberto Tirado Salas, "Encriptado de datos para proteger información de las empresas," Diciembre 2017. [Online]. http://repositorio.upsin.edu.mx/Fragmentos/tesinas/EncriptadoDeDatosParaProtegerInformacionDeLasEmpresasTiradoSalasJoseRoberto6628.pdf

[9] Julio César Mendoza, "Demostración de cifrado simétrico y asimétrico," 2022. [Online]. https://dspace.ups.edu.ec/bitstream/123456789/8185/1/Demostraci%C3%B3n%20de%20cifrado%20sim%C3%A9trico%20y%20asim%C3%A9trico.pdf

[10] GUILLERMO HERRERA, AMANDA BENITES, VIOLETA MORENO, and JORGE GRIJALVA,. Lima, Peru: PUNTO Y GRAFIA S.A.C, 2015.

[11] José-Luis Prieto. (2022) Glosario Terminología Informática. [Online]. http://www.tugurium.com/gti/termino.php?Tr=key%20escrow

[12] IBM. (2023) Servicios web. [Online]. https://www.ibm.com/docs/es/was/9.0.5?topic=services-web

[13] James Bailey, Fran¸cois Bry, Tim Furche, and Sebastian Schaffert, "Web and Semantic Web Query Languages: A Survey," 2005.

[14] Kaspersky Lab. (2023) Qué es un certificado SSL: definición y explicación. [Online]. https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate

[15] PRISMA. (2022) PRISMA. [Online]. https://prisma-statement.org//

[16] Vijay K. Vaishnavi and William Kuechler, *Design Science Research Methods and Patterns*, 2nd ed.: CRC Press, 2015.

[17] Carl Lawrence, Tuure Tuunanen, and Michael David Myers, "Extending Design Science Research Methodology for a Multicultural World," 2010.

[18] Alan Hevner, Salvatore March, Jinsoo Park , and Sudha Ram, "Design Science in Information Systems Research," pp. 75-105, 2004.

[19] CLAIRE DRUMOND. (2022) Scrum. [Online]. https://www.atlassian.com/es/agile/scrum

[20] Python Software Foundation. (2023) El tutorial de Python. [Online]. https://docs.python.org/es/3/tutorial/#the-python-tutorial

[21] Microsoft. (2023) Microsoft Threat Modeling Tool. [Online]. https://learn.microsoft.com/es-es/azure/security/develop/threat-modeling-tool

[22] JetBrains. (2023) PyCharm. [Online]. https://www.jetbrains.com/es-es/pycharm/features/

[23] Mingyu Lim, "C2CFTP: Direct and Indirect File Transfer Protocols Between Clients in Client-Server Architecture," vol. VIII, 2022.

[24] Khawar Khurshid, Imdad Ullah, Zawar Shah, Najm Hassan, and Tariq Ahamed Ahanger, "Protocols for Transferring Bulk Data Over Internet: Current Solutions and Future Challenges," vol. IX, 2021.

[25] Qing Li, Yonghui Ju, Chang Zhao, and Xintai He, "An Encrypted Field Locating Algorithm for Private Protocol Data Based on Data Reconstruction and Moment Eigenvector," vol. IX, 2021.

[26] Tanushree Agarwal, Payam Niknejad, Mohammadreza Barzegaran, and Luigi Vanfretti, "Multi-Level Time-Sensitive Networking (TSN) Using the Data Distribution Services (DDS) for Synchronized Three-Phase Measurement Data Transfer," vol. VII, 2019.

[27] Dang Hai Hoang and Thi Thuy Duong Le, "RCOAP: A Rate Control Scheme for Reliable Bursty Data Transfer in IoT Networks," vol. IX, 2021.

[28] Zuming Shen, Peng Zeng, Yuyin Qian, and Kim-Kwang Raymond Choo, "A Secure and Practical RFID Ownership Transfer Protocol Based on Chebyshev Polynomials," vol. VI, 2018.

[29] Sarfraz Ahmad and Muhammad Junaid Arshad, "Enhancing Fast TCP's Performance Using Single TCP Connection for Parallel Traffic Flows to Prevent Head-of-Line Blocking," vol. VII, 2019.

[30] YUSUKE YAMASAKI et al., "Delay-Bounded Wireless Network Based on Precise Time Synchronization Using Wireless Two-Way Interferometry," vol. IX, 2021.

[31] A. Vikram, S. Kalaivani, and G. Gopinath, "A Novel Encryption Algorithm based on DNA Cryptography," 2020.

[32] Wu Fusheng, Zhang Huanguo, Ni Mingtao, Wang Jun, and Ji Zhaoxu, "A Novel Key Agreement Protocol Based on RET Gadget Chains for Preventing Reused Code Attacks," vol. VI, 2018.

5. ANEXOS

En esta sección se encuentran los documentos pertinentes que apoyaron la realización del proyecto y estos documentos son:

ANEXO I. Estado del Arte

ANEXO II. Documentos Scrum

ANEXO III. Reporte de Amenazas

ANEXO IV. Evaluación de Riegos

ANEXO V. Video demostrativo

ANEXO VI. Código fuente de la aplicación

ANEXO I

En el enlace a continuación se puede encontrar el documento inicial. Un estado de arte realizado por el autor del proyecto. Que monta las bases teóricas y prácticas para la realización de la tesis.

Enlace: https://epnecuador-my.sharepoint.com/:f:/g/personal/danny_venegas_epn_edu_ec/EsiuMfGe4MJOsGaWKF7BSFoBeMFRxeMRioXni26m8oFz1Q?e=TEPwrH

ANEXO II

En el enlace a continuación se puede encontrar los documentos obtenidos al realizar Scrum. Entre ellos se encuentran las historias de usuario, los Sprints y la calendarización del proyecto.

Enlace: https://epnecuador-my.sharepoint.com/:f:/g/personal/danny_venegas_epn_edu_ec/EgJnQRBSdndKrb1ZVPpW13IB5Rd1MSY7ZElwK10Wl8dR2g?e=gCR6hB

ANEXO III

En el enlace a continuación se puede encontrar el documento que dio de resultado la herramienta de modelado de amenazas. Un documento que contiene las 76 amenazas que fueron visualizadas por la herramienta.

Enlace: https://epnecuador-my.sharepoint.com/:f:/g/personal/danny_venegas_epn_edu_ec/EsSQDuCwqWxKiQJZx1SFbbwByKrOWO4Ts5an_zkJmMMLDw?e=mu1kNY

ANEXO IV

En el enlace a continuación se puede encontrar el documento que dio de resultado el análisis de riegos. Un documento que contiene las amenazas y las contingencias del componente de Transferencia.

Enlace: https://epnecuador-my.sharepoint.com/:f:/g/personal/danny_venegas_epn_edu_ec/EibEchDZvIpJsQPcSeZ-ebkBHbez9oIZ61HZbh94_wCvEg?e=LmEXsO

ANEXO V

En el enlace a continuación se puede encontrar el video que muestra el funcionamiento del prototipo. Aquel que fue obtenido al realizar el proyecto de integración curricular (TIC).

Enlace: https://epnecuador-my.sharepoint.com/:v:/g/personal/denys_flores_epn_edu_ec/EQTmyNQEVtBPjo8SuBOEBA0BLrub-5gvysXW0s5d4sJh-g?e=Eho21k

ANEXO VI

En el enlace a continuación se puede encontrar el código fuente de la aplicación integrada de los tres componentes. Aquel que fue obtenido al realizar el proyecto de integración curricular (TIC).

Enlace: https://github.com/WILLIAMSUNTAXI/Tesis_2023