ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PROYECTO DE DESARROLLO

PROPUESTA DE MODELO DE GESTIÓN DOCUMENTAL ACADÉMICA INTELIGENTE EMPLEANDO BLOCKCHAIN

PROYECTO PREVIO A LA OBTENCIÓN DEL GRADO DE MÁSTER EN SOFTWARE CON MENCIÓN EN SEGURIDAD

GLADYS MARIBEL RONQUILLO MAIGUA
gladys.ronquillo@epn.edu.ec

DIRECTOR: PhD. Jenny Gabriela Torres Olmedo
jenny.torres@epn.edu.ec

CODIRECTOR: PhD. Pamela Catherine Flores Naranjo
pamela.flores@epn.edu.ec

2021

APROBACIÓN DEL DIRECTOR

Como director del trabajo de titulación PROPUESTA DE MODELO DE GESTIÓN DOCUMENTAL ACADÉMICA INTELIGENTE EMPLEANDO BLOCKCHAIN desarrollado por Gladys Maribel Ronquillo Maigua, estudiante de Maestría en Software con Mención en Seguridad, habiendo supervisado la realización de este trabajo y realizado las correcciones correspondientes, doy por aprobada la redacción final del documento escrito para que prosiga con los trámites correspondientes a la sustentación de la Defensa oral.

PhD. Jenny Torres

DIRECTOR

DECLARACIÓN DE AUTORÍA

Yo, Gladys Maribel Ronquillo Maigua declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Gladys Maribel Ronquillo Maigua

DEDICATORIA

A mis pequeños sobrinos Dylan, Damaris, Scarleth y Danna, por ser ese pilar fundamental de alegría y sobre todo de amor, los mismos que me sustentaron el coraje necesario para poder culminar con éxito esta etapa de mi vida.

A mis padres Víctor y Gladys, por siempre estar conmigo, guiándome y llenándome de sus sabios consejos para poder sobresalir en las diferentes adversidades que la vida nos tiene.

Gladys.

AGRADECIMIENTO

A Dios, por ser el motor fundamental de mi vida y darme la confianza y seguridad que necesito para poder llevar a cabo todo lo que me proponga.

A mi directora de tesis PhD. Jenny Torres y Daniel Maldonado, por su valiosa ayuda y colaboración durante la elaboración de este proyecto de titulación.

A mis padres Víctor y Gladys por su apoyo incondicional en esta etapa de mi vida.

A David Onofre, por acompañarme y ser mi soporte durante este proceso de formación académica.

Gladys.

CONTENIDO

LISTA DE FIGURAS i
LISTA DE TABLAS ii
RESUMEN iii
ABSTRACT iv
1. INTRODUCCIÓN 1
1.1. Pregunta de investigación 3
1.2. Objetivo general 3
1.3. Objetivos específicos 3
1.4. Alcance 4
1.5. Marco Teórico 4
1.5.1. Criptografía 4
1.5.2. Tecnología Blockchain 6
1.5.3. Algoritmos de consenso 7
1.5.4. Estructura Blockchain 9
1.5.5. Tipos de blockchain 9
1.5.6. Plataformas blockchain principales 10
1.5.7. Evaluación de plataformas 12
1.5.8. Contratos inteligentes 13
1.5.9. Profundizando en Hyperledger 13
1.5.10. Serverless 14
1.5.11. Amazon Web Services (AWS) 14
1.5.12. Metodología Goal Question Metric (GQM) [8] 16
1.5.13. Norma ISO 15489 [27] 17
1.5.14. Componentes de un Sistema de Gestión 24
1.5.15. Sistema Educativo en Ecuador [28] 26
1.6. Revisión Sistemática de la literatura 30
1.6.1. Fase de búsqueda 30
1.6.2. Fase de Ejecución 31
1.6.3. Fase de Extracción 33
2. METODOLOGÍA 38
2.1. Propuesta del modelo 39

2.1.1. Identificación del contexto 39
2.1.2. Partes interesadas 40
2.1.3. Diseño de la propuesta 41
2.1.4. Protocolos propuestos 46
2.1.5. Arquitectura en la nube 48
2.2. Evaluación 52
2.2.1. Preparación 53
2.2.2. Ejecución 56
2.2.3. Evaluación 57
3. DISCUSIÓN 63
4. CONCLUSIONES Y RECOMENDACIONES 64
4.1 Conclusiones 64
4.2 Recomendaciones 65
REFERENCIAS BIBLIOGRÁFICAS 66
ANEXOS 69
Anexo I 70

LISTA DE FIGURAS

Figura 1: La metodología DIRKS 19
Figura 2: Estructura Institución Educativa 39
Figura 3: Lineamientos propuesta 41
Figura 4: Red - actores 45
Figura 5: Diagrama caso de uso - Carga documento 47
Figura 6: Diagrama caso de uso - Verificar documento 48
Figura 7: Diagrama de arquitectura (elaborado por el autor) 49
Figura 8: Diagrama de secuencia – Carga del autor (elaborado por el autor) 50
Figura 9: Diagrama de secuencia – Verificar (elaborado por el autor) 52
Figura 10: Información demográfica 57
Figura 11: Nivel de educación 57
Figura 12: Resultado - Pregunta 1 58
Figura 13: Resultado - Pregunta 2 58
Figura 14: Resultado - Pregunta 3 58
Figura 15: Resultado - Pregunta 4 59
Figura 16: Resultado - Pregunta 6 59
Figura 17: Resultado - Pregunta 7 60
Figura 18: Resultado - Pregunta 8 60
Figura 19: Resultado - Pregunta 9 60
Figura 20: Resultado - Pregunta 10 61
Figura 21: Resultado - Pregunta 11 61
Figura 22: Resultado - Pregunta 12 62
Figura 23: Resultado - Pregunta 13 62

LISTA DE TABLAS

Tabla 1: Comparativa entre Ethereum y Hyperledger Fabric 12
Tabla 2: Etapas metodología DIRKS 24
Tabla 3: Proceso de emisión de certificados 28
Tabla 4: Proceso de legalización de certificados ministeriales 29
Tabla 5: Cadenas de búsqueda 30
Tabla 6: Criterios de inclusión y exclusión 30
Tabla 7: Fuentes digitales 31
Tabla 8: Trabajos potencialmente relevantes 32
Tabla 9: Trabajos relevantes 32
Tabla 10: Información de trabajos relevantes 33
Tabla 11: Detalle de fase de extracción 35
Tabla 12: Partes interesadas 40
Tabla 13: Necesidades partes interesadas 41
Tabla 14: Procesos e instrumentos 42
Tabla 15: Estructura documento 44
Tabla 16: Estructura contrato inteligente - Carga 51
Tabla 17: Estructura contrato inteligente - Verificar 52
Tabla 18: Objetivos GQM 54
Tabla 19: Métricas 54
Tabla 20: Cuestionario de evaluación 55
Tabla 21: Información demográfica 56
Tabla 22: Referencia encuesta 56

RESUMEN

Esta tesis de Maestría presenta un modelo de gestión documental académica inteligente empleando Blockchain para Instituciones Educativas privadas, modelo que se encuentra sustentado en la norma ISO 15489 como lineamiento base para la identificación de los principios y características que un sistema de gestión documental debe presentar, permitiendo contribuir y sustentar la gestión de documentos académicos, tales como: documentos, procesos, políticas y responsabilidades. Además, con el apoyo de la amplia cartera tecnológica que Amazon Web Services (AWS) provee, se establece una guía arquitectónica que fundamentan los lineamientos para una posible implementación. Por tanto, esta solución permitirá garantizar la seguridad, disponibilidad, integridad y autenticidad de los documentos mediante el uso de contratos inteligentes de HyperLedger Fabric. Este modelo no presenta los costos que implicaría la implementación en AWS.

Palabras clave: Norma ISO 15849, Sistema de Gestión Documental, Blockchain, Contratos Inteligentes, Amazon Web Services, HyperLedger Fabric.

ABSTRACT

This Master's thesis presents a smart academic document management model using Blockchain for private Educational Institutions, this model is supported on ISO 15489 standard as a base guideline for identification the principles and characteristics that a document management system must present, allowing contribute and support the management of academic documents, such as: documents, processes, policies and responsibilities. In addition, with the support of the broad technological portfolio that Amazon Web Services (AWS) provides, it establishes an architectural guide that bases the guidelines for a possible implementation. Therefore, this solution will ensure the security, availability, integrity and authenticity of documents through the use of HyperLedger Fabric's smart contracts. This model does not present costs involved in implementing on AWS.

Keywords: ISO 15849 Standard, Document Management System, Blockchain, Smart Contracts, Amazon Web Services, HyperLedger Fabric.

1. INTRODUCCIÓN

Con la llegada de Bitcoin (moneda virtual) se ha iniciado una revolución no solo el en ámbito económico en el cual ha tenido éxito fortaleciéndose como una moneda alternativa, sino también en el ámbito tecnológico donde Blockchain se ha establecido como el referente en el concepto de registro distribuido[1]. Por tanto, el éxito de esta tecnología ha permitido comprobar la seguridad y robustez que tiene, permitiendo registrar de forma eficaz y segura las transacciones de elementos virtuales; resolviendo el problema de integridad y seguridad.

Por otro lado, el proceso de emisión de un documento que avale la información que presenta de acuerdo al contexto requerido por un solicitante en el Ecuador, en su mayoría de veces es realizado de forma manual y emitida de forma física mediante la impresión de un documento, con las respectivas firmas de las autoridades correspondientes. Sin embargo, la información de estos documentos puede ser vulnerable a posibles falsificaciones o manipulaciones, así como tampoco se puede garantizar la veracidad de su procedencia. Identificándose así que los documentos siguen un proceso poco eficiente, totalmente manual y operado por personas que son susceptibles a cometer errores.

Es así que en el sistema educativo primario y secundario privado de nuestro país, la emisión de documentos académicos también se realiza de manera semi o completamente manual, lo que implica no tener un control adecuado de la información que se genere, modifique y en especial un control del tiempo que conlleva su elaboración. Por ello, realizar la automatización de este proceso permite que; los documentos sean más seguros, reducir costos en almacenamiento físico, reducir la carga operativa, disminuir la burocracia de los procesos que conlleva en términos de validaciones y garantizar que el proceso sea más transparente y confiable para todas las partes involucradas.

Como siguiente, se identifica los procesos que involucran la intervención de alguna autoridad regulatoria (agente externo), como por ejemplo el Distrito Educativo del Ministerio de Educación del Ecuador, quienes son los responsables principales de la legalización de certificados académicos ministeriales (documentos que evidencian el desempeño académico y comportamental que un estudiante ha desarrollado durante un periodo escolar o año lectivo dentro de una Institución Educativa y son de suma importancia para logros académicos y puerta de entrada hacia otras instituciones)[2]. De tal modo que, se evidencia también problemas de integridad y no repudio de los documentos ya que no se garantizar su precedencia. Sin dejar de lado la gran cantidad de documentos físicos que demandan ser revisados, validados, legalizados, firmados y sellados por las autoridades correspondientes [3].

Ante esta problemática, se procedió con la revisión sistemática literaria de los principales trabajos relevantes sobre el uso de las tecnologías Blockchain dentro del contexto de los sistemas educativos, donde se analizó metodologías de investigaciones usadas con anterioridad [4-6], la situación de los procesos de gestión documental con sus actores y responsables, las posibles tecnologías a ser usadas para una posible implementación. Además, se determinó que la tecnología Blockchain y contratos inteligentes son los adecuados para aportar positivamente a la gestión documental académica; por garantizar la no manipulación, modificación, alteración y seguridad [7]. Así pues, esto permite asegurar un nivel muy alto de seguridad y confidencialidad de la información de los documentos emitidos dentro de una Institución y garantizando su precedencia fuera de ella.

Contrarrestando las soluciones encontradas, se identificaron problemas que pueden limitar la propagación de Blockchain como solución en el sector educativo [5], estos son: la falta de una plataforma nacional de Blockchain, los costos de mantenimiento para infraestructura, el historial de accesos a todos los certificados, almacenamiento seguro de los documentos y la falta de una estructura de administración centralizada que coordine el Blockchain cómo único espacio de información digital.

Posteriormente, se diseñó un modelo basado en Blockchain que permite registrar y legalizar los documentos o certificados académicos sustentado en los lineamientos propuestos por la Norma ISO 15489, donde se identifican los principios y características que un sistema de gestión documental debe tener. Por tanto, se identificó a nivel operativo: los documentos que forman parte del sistema, sus procesos, instrumentos, políticas y responsabilidades que contribuirán y sustentarán en la gestión hasta el diseño arquitectónico en Amazon Web Services (AWS).

Por otro lado, para la validación del modelo se llevó a cabo una encuesta basada en la metodología GQM orientada a las partes interesadas para exaltar su opinión sobre el modelo propuesto [8], ya que este trabajo es totalmente teórico y no incluye una fase de pruebas experimentales. En este caso como parte interesada se identifica al personal de TI de las Instituciones Educativas. Como resultados, se evidenció que esta propuesta tiene una buena tasa de aceptación tanto en los lineamientos propuestos como en la tecnología de AWS, debido a que este proporciona una alta seguridad y disponibilidad en sus servicios. Además de contribuir significativamente para una posible implementación, en el tiempo de sus procesos operativos y reducción de recursos de manera ágil y eficaz. Por tanto, con esta solución se garantiza la disponibilidad, integridad, confiabilidad y seguridad de la información de los documentos, acelerar significativamente los procesos operativos involucrados, reducir

los costos administrativos y llevando un control permanente de todas sus transacciones [9]. Sin embargo, algunos de los comentarios de los participantes recalcaron que era necesario detallar el costo que implicaría implementar esta solución y de la necesidad de requerir un personal técnico.

Finalmente, este trabajo plantea su solución en base a tres enfoques principales para la validación de certificados en las Instituciones Educativas privadas del Ecuador:

- Administración centralizada mediante el uso de la plataforma de Amazon Web Services, que se enfoca en la autenticación, autorización y seguridad de los documentos. Donde, la propuesta será planteada a nivel de arquitectura.
- Ambiente seguro para el almacenamiento y acceso de los documentos digitales.
- Autenticidad de la emisión de los documentos académicos una vez aprobados, para avalar la aprobación de todas las entidades autorizadoras involucradas y su precedencia.

1.1. Pregunta de investigación

Debido a la necesidad de establecer un modelo que permita garantizar la seguridad e integridad de la información y avalar la precedencia documental académica, se plantea la siguiente pregunta de investigación para obtener diferentes enfoques, recomendaciones y métodos de investigaciones realizadas: ¿Es posible diseñar un modelo con la tecnología Blockchain que contribuya de manera segura y eficiente la gestión documental académica en instituciones educativas privadas de Quito? Esta interrogante es utilizada en la revisión de la literatura.

1.2. Objetivo general

Proponer un modelo de gestión documental académica inteligente basado en la tecnología Blockchain.

1.3. Objetivos específicos

- Estudiar y analizar el estado del arte de la tecnología y herramientas Blockchain.
- Identificar el proceso actual de legalización de certificados académicos para las instituciones educativas privadas.

- Identificar los principales actores o entidades que intervienen en el proceso de legalización o aprobación de documentos.
- Diseñar el modelo de gestión académica.
- Presentar resultados del modelo propuesto.

1.4. Alcance

El entorno sin papel aún no se ha convertido en una realidad en Sudáfrica [10] y por ende no en nuestro país. Los documentos físicos todavía se imprimen a diario, lo que los hace susceptibles al fraude, pérdida de integridad y la imposibilidad de validar su precedencia. Esta investigación incluye la revisión de las fuentes bibliográficas [11] en las áreas relacionadas con la tecnología Blockchain y su aplicación en el sistema educativo para salvaguardar la confidencialidad, integridad y autenticidad de los documentos académicos. Así como, la elaboración de la propuesta para registrar, revisar y validar un documento/certificado académico digital en el Blockchain. Para ello, se recurre a la metodología de Pólya [12] para dar solución al problema planteado y al ser este trabajo totalmente teórico, se excluye la fase de implementación. Sin embargo, para garantizar su verosimilitud se apoya de la metodología GMQ [8] para su evaluación en base de una encuesta a partes interesadas.

1.5. Marco Teórico

A continuación, se procede con la descripción de los principales conceptos, términos técnicos y recursos tecnológicos utilizados para dar solución a esta investigación.

1.5.1. Criptografía

Función Hash

Es una función que toma como entrada una cadena de cualquier longitud para obtener una cadena o valor de una longitud fija [13], es decir, la misma entrada de datos obtendrá el mismo resultado. Cualquier cambio que se realice a los datos de entrada produce un resultado totalmente diferente, siendo impredecible. Además, el cálculo directo es fácil pero su inverso es extremadamente difícil, siendo considerado imposible en las condiciones científicas y tecnológicas actuales.

Criptografía de clave pública

El cifrado de clave pública utiliza dos claves relacionadas: una que cifrará el mensaje y otra que es la única con la capacidad de descifrarlo. El remitente solicita al receptor la clave

de cifrado, cifra el mensaje y envía el mensaje cifrado al receptor. Sólo el receptor puede descifrar el mensaje, incluso el mismo no es capaz de leer el mensaje cifrado. Por ejemplo, en las siguientes dos secciones se utilizará a las personas Alice, Bob y Eve. Cuando Alice y Bob desean comunicarse, primero Bob le pide a Alice su clave pública. Luego, Bob usa la clave pública de Alice para cifrar el mensaje. En este tipo de cifrado, sólo la clave privada de Alice puede desbloquear el mensaje cifrado con su clave pública. Bob envía su mensaje a Alice, Alice usa su clave privada para descifrar el mensaje de Bob [14]. Por tanto, cualquier persona puede acceder a una clave pública para cifrar, pero únicamente la persona que tenga la clave privada puede descifrar los datos. Esto se denomina cifrado asimétrico.

Firma digital

Mediante el cifrado asimétrico es posible compartir mensajes cifrados sin tener que compartir una clave secreta común. Aunque Eve no pueda leer los mensajes de Alice y Bob, si es capaz de causar daños. Puede enviar un mensaje a Bob ya que su clave pública está disponible para ella y pretender que el remitente es Alice. Por tanto, Bob no tiene forma de saber si Alice realmente escribió el mensaje. La solución a este problema es el uso de firmas digitales.

El protocolo de firma digital se aplica con la adición de dos funciones. La primera función toma un mensaje, una clave privada y retorna una firma. La segunda función toma un mensaje, una firma, una clave pública y retorna un valor verdadero o falso. Alice quiere enviar un mensaje a Bob y quiere asegurarse de que Bob sepa que lo envió, así que ella toma su mensaje m y su clave privada sk para producir una firma s. El mensaje y la firma se envía por un canal público a Bob. Luego Bob toma el mensaje m, la firma s y la clave pública pk de Alice para verificar que Alice es el remitente del mensaje. Con este ejemplo, el mensaje en sí no es confidencial, su fin es demostrar que Alice sea el remitente del mensaje. Sin embargo, las firmas digitales se pueden usar junto con el cifrado de clave pública para cifrar el mensaje y demostrar quién es el remitente del mensaje.

Nonce

Un nonce es un número que solo se usa una vez, por lo general es un número al azar. Se usa para alterar el valor hash de un mensaje sin cambiar por sí mismo el mensaje. A menudo se agregan al mensaje cuando se calcula el hash, pero el receptor del mensaje lo descarta [15].

SHA

Los algoritmos hash seguros (SHA) son una familia de funciones hash de naturaleza iterativa que cumplen los requisitos de las funciones hash criptográficas [13].

Blockchain utiliza el algoritmo SHA-256 el mismo que utiliza 64 iteraciones de un solo paso para producir un valor hash con una longitud de 256 bits.

1.5.2. Tecnología Blockchain

¿Qué es Blockchain?

La tecnología Blockchain [16] surgió en el año 2008 con la publicación de un documento firmado por Satoshi Nakamoto, en el cual propone un sistema de efectivo electrónico entre redes p2p (peer-to-peer) en internet. Esta red permite a los usuarios realizar y recibir transacciones directamente entre sí en forma de un token, que ahora es conocido como Bitcoin. Primero, las transacciones se agrupan en un bloque, luego se encadena con bloques anteriores utilizando procesos criptográficos y el hash de su contenido. Mediante esta relación se garantiza que el contenido del bloque sea consistente e inmutable. Además, cuando una transacción de Bitcoin es validada, sus comandos integrados de bloqueo y desbloqueo son ejecutados en secuencia para ver si cumple con la condición de gasto. Aunque la funcionalidad de los comandos integrados en la transacción de bitcoin es muy limitada, enciende la noción de contratos inteligentes en la siguiente generación de blockchain.

Fuera del lado de bitcoin, Blockchain es un libro mayor de transacciones conocidas en inglés como ledger que puede registrar movimientos que representan cualquier tipo de valor, siendo esta incapaz de ser eliminada o modificada. Si un actor no autorizado trata de cambiar el contenido de un bloque, su hash cambiaría y por ende su relación con todos los bloques siguientes sería inválida. Por lo tanto, un bloque almacena un número de transacciones de manera inmutable y los mismos están relacionados entre sí, lo que permite una actualización constante que garantiza su trazabilidad.

Características

Las siguientes características hacen que la revolucionaria tecnología de blockchain se destaque [17]:

Descentralizado

Blockchain es de naturaleza descentralizada, lo que significa que ninguna persona o grupo tiene la autoridad de la red en general. Si bien todos en la red tienen la copia del libro mayor distribuido con ellos, nadie puede modificarlo. Esta característica única permite la transparencia y seguridad al tiempo que otorga poder a los usuarios.

Inmutable

Se refiere al hecho de que cualquier dato una vez escrito en la cadena de bloques o Blockchain no se puede cambiar. Una vez que los datos se han procesado, no se pueden modificar ni eliminar. En el caso de la cadena de bloques, si intenta cambiar los datos de un bloque, tendrá que cambiar toda la cadena de bloques siguientes, ya que cada bloque almacena el hash de su bloque anterior. El cambio en un hash conducirá a un cambio en todos los hashes siguientes. Es extremadamente complicado para alguien cambiar todos los valores hash, ya que requiere mucha potencia computacional para hacerlo. Por lo tanto, los datos almacenados en una cadena de bloques no son susceptibles a alteraciones o ataques de piratas informáticos debido a la inmutabilidad.

Con esta propiedad se hace más fácil detectar la manipulación de cualquier dato, ya que cualquier cambio en un solo bloque puede detectarse y abordarse sin problema.

Red peer-to-peer (p2p)

Una red blockchain, es una red p2p en la que un par (nodos) es responsable de validar las transacciones, crear nuevos bloques y verificar la validez de los bloques recién creados. La mayoría de los pares en la red deben estar de acuerdo mediante una regla determinada no solamente para confirmar las transacciones, sino también para obligar a un bloque recién creado a cumplir con el acuerdo predefinido. Es decir, todos los pares deben seguir un algoritmo de consenso conocido para proteger la integridad de los datos sin la necesidad de verificar si un nodo en la red es malicioso o no; anulando así el requisito de un tercero, protegiendo la coherencia de la información [1]. Por consiguiente, si desea realizar cualquier transacción hacia cualquier parte del mundo, con blockchain se lo haría en pocos segundos, sin las interrupciones o cargos adicionales de la transferencia.

1.5.3. Algoritmos de consenso

El consenso de refiere al proceso de lograr un acuerdo entre los participantes de la red sobre el estado correcto de los datos en el sistema, es decir, para que todos los nodos compartan exactamente los mismos datos. Por tanto, se asegura que los datos registrados sean los mismos para todos los nodos de la red, imposibilitando su manipulación. Adicional, existen algoritmos de consenso que varían con las diferentes implementaciones de Blockchain, a continuación se detallan algunas de las existentes [18].

Prueba de trabajo (PoW)

Este algoritmo implica resolver un desafío criptográfico computacional con el fin de crear nuevos bloques en el Blockchain de Bitcoin, este proceso se conoce como “minería” y los nodos de la red que se dedican a la minería se conoce como “mineros”. Este algoritmo requiere de una gran cantidad de energía ya que se requiere de un poder computacional muy pesado, además, tiene una alta latencia de validación de transacciones. El PoW es el resultado de un proceso de minería exitoso que concluye con una recompensa de bitcoins al primer minero en cumplir con el desafío.

Prueba de participación o estaca (PoS)

Es el segundo algoritmo más frecuente en las cadenas de bloques, usado para las criptomonedas luego de la prueba de trabajo. Tiene un funcionamiento similar a PoW pero no genera una competencia entre los nodos, los nodos se conocen como validadores y en lugar de minar bloques, validan las transacciones ganando una tarifa por transacción. No se realiza una extracción, debido a que todas las monedas existen desde el primer día. Los nodos se seleccionan aleatoriamente para validar los bloques y la probabilidad de esta selección aleatoria depende de la cantidad de participación que se tenga.

Prueba de tiempo transcurrido (PoET)

Este algoritmo emula la prueba de trabajo de estilo Bitcoin, la implementación de Sawtooth de Hyperledger es un ejemplo. En lugar de competir para resolver el desafío criptográfico y extraer el próximo bloque, este es un híbrido de una lotería aleatoria y de un orden de llegada. Así también, aprovecha de la informática para imponer tiempos de espera aleatorios para generar nuevos bloques por nodos estocásticamente elegidos. Se elige como líder al validador (nodos especializados para validar transacciones y llevarlas a la cadena a través de un proceso especializado) con el menor tiempo de espera para un bloque de transacción, quién es el que crea el siguiente bloque de la cadena.

Tolerancia práctica de fallas Bizantinas (PBFT)

En este algoritmo es usado en cadenas de cloques privadas como Hyperledger. Todos los nodos o mineros son confiables y conocidos e intervienen en el proceso de votación para agregar el siguiente bloque; el consenso se alcanza cuando más de dos tercios de todos los nodos están de acuerdo con ese bloque. Para cada bloque de transacciones, el algoritmo selecciona al azar un conjunto pequeño de usuarios únicos de manera segura y justa, ocultando la identidad de los mismos hasta confirmar el bloqueo para protegerlos de los

atacantes. Además, posee un alto rendimiento, baja latencia, bajo uso recursos computacionales y brinda seguridad; sin embargo, puede ser vulnerables a ataques cuando la red no posee muchos nodos.

1.5.4. Estructura Blockchain

Cada bloque en blockchain contiene los siguientes elementos [19]:

Datos principales: los datos dependen del tipo de transacción, generalmente es una transferencia entre nodos. Sin embargo, pueden ser de cualquier tipo como transferencia de dinero o transferencia de registros.

Hash del bloque anterior: cuando se ejecuta una transacción, su hash se genera y se transmite a la red.

Raíz de Merkle: es una estructura de datos de árbol que simula un orden jerárquico de arriba hacia abajo. Todas las transacciones en el bloque se unen en un solo hash, que es esta raíz.

Hash del bloque actual: el valor hash final se registra en el encabezado del bloque (hash del bloque actual), mientras que el contenido en sí se almacena en el cuerpo del bloque. Generalmente los bloques están vinculados a un tamaño, lo que permite un número limitado de transacciones por bloque.

Objetivo: es el número de 256 bits que indica a los mineros cuál puede ser el hash correcto.

Marca de tiempo: detalla la hora a la que se generó el bloque.

Nonce: como la firma del bloque, el valor nonce u otros datos que el usuario define.

1.5.5. Tipos de blockchain

Actualmente existen tres tipos de blockchain que difieren en gobernanza y arquitectura [20]:

Blockchain pública: todos los registros son visibles para el público y todos pueden participar en el proceso de consenso. La inmutabilidad es alta en este tipo de blockchain, pero la eficiencia es baja. Se destaca las siguientes ventajas: son totalmente descentralizadas por lo que la información se distribuye a través de todos los nodos que conforman la red, se mantiene en todo momento la anonimidad de los participantes, todos los participantes participan de igual forma y acceden a la misma información. Así también, se identifica las siguientes desventajas: gran consumo de recursos del algoritmo de consenso PoW y existe un número de transacciones limitado que se pueden introducir en un bloque.

Blockchain privada: pertenece a una organización específica y sólo los nodos provenientes de esa organización pueden unirse al proceso de consenso. Tienen mayor eficiencia. Se destaca las siguientes ventajas: el rendimiento de estas redes es mayor ya que existen nodos predefinidos que se encargan exclusivamente de la validación de transacciones, el nivel de privacidad es mayor y no es necesario implementar el algoritmo de consenso PoW.

Blockchain hibrida: combinación de los dos tipos anteriores en los que un grupo preseleccionado de usuarios puede participar en el proceso de consenso y no todos los usuarios pertenecen a la misma organización. La inmutabilidad y la eficiencia son similares a la blockchain privada. A este tipo también se conoce como blockchain autorizado.

1.5.6. Plataformas blockchain principales

Bitcoin

Primera criptomoneda virtual que nació teóricamente junto con el manifiesto del blockchain creado por Satoshi Nakamoto. Muchas de sus características son heredadas o retocadas por posteriores tecnologías como las que se verá a continuación. Fue creado como una alternativa al dinero real, es una moneda que no está controlada por ninguna organización o entidad financiera como las demás monedas. Sin embargo, presenta problemas que han frenado sus expectativas: tiempos de minado cada vez más superiores y confianza de la sociedad en la moneda.

Ethereum[21]

Es una plataforma open-source que proporciona todo lo necesario para poder facilitar la construcción de aplicaciones en tecnología blockchain, así como facilitar las transacciones de divisas de las que se habla en Bitcoin. Cuenta con su propia moneda (ether) y agrega un gran avance ante Bitcoin introduciendo el concepto de contratos inteligentes. Los contratos inteligentes son aplicaciones que permiten definir, por una o más partes, una serie de reglas que se ejecutan automáticamente cuando se cumplen ciertas condiciones, estos a su vez no pueden ser modificados, del mismo modo cuando se ejecutan ya no es posible dar marcha atrás. El leguaje empleado en Ethereum para desarrollas estos contratos inteligentes es Solidity.

En Ethereum, todos los participantes deben llegar a un consenso sobre el orden de todas las transacciones, siendo esta una consistencia para el libro mayor. Si no se puede establecer un orden de transacciones, podría generarse registros dobles o algún tipo de inconsistencia. El Blockchain de Ethereum es público por lo que podría involucrar a partes no confiables y anónimas, por tanto, se debe emplear un mecanismo de consenso que proteja el

libro mayor contra los participantes fraudulentos, este es el algoritmo de prueba de trabajo (PoW).

Por otro lado, se cobra un precio por el procesamiento computacional de las transacciones llamado GAS, cuyas ganancias van destinadas a los mineros de la red quienes deben resolver un puzzle criptográfico para poder generar un nuevo bloque en la cadena. Si bien en uno de los mecanismos más populares y seguros dentro de esta tecnología, sus propias características impactan negativamente en el rendimiento y en los recursos que esta necesita.

Existen maneras de crear redes Ethereum privadas donde solo se permite acceder a determinados nodos, sin embargo, esto hace que la red tenga menos nodos mineros validadores que validen los bloques, lo que los hace ineficientes.

Hyperledger

Proyecto open-source de la Fundación Linux. Nace con un enfoque hacia el mundo empresarial y de las redes privadas, así como, incluye todo lo necesario para realizar contratos inteligentes. Cuenta con un sin número de frameworks, entre uno de ellos está, Hyperledger Fabric que es una cadena de bloques de carácter privado y está orientada al uso empresarial ya que permite realizar transacciones privadas. Como principales diferencias con otras tecnologías se puede destacar que Hyperledger no dispone de una criptomoneda propia. A continuación, se describen los algunos de los frameworks que este alberga:

- **Hyperledger Fabric:** proporciona una arquitectura modular, que permite que los componentes como el consenso y los servicios de membresía sean plug-and-play (permite una reutilización de funciones e integración fácil de varios módulos existentes). Además, permite que las entidades realicen transacciones confidenciales sin pasar información a través de una autoridad central por medio de diferentes canales que se ejecutan dentro de la red, así como la división del trabajo que caracteriza a los diferentes nodos. Finalmente, aprovecha la tecnología de contenedores para alojar contratos inteligentes denominados “chaincode” que concentra la lógica o reglas del negocio, las cuales son fácilmente de modelar.
- **Hyperledger Sawtooth:** inicialmente desarrollada por Intel y que permite su despliegue en modo *permissioned* o *permissionless*. Incluye un algoritmo de consenso llamado Proof of Elapsed Time “PoET”.
- **Hyperledger Iroha:** orientada a su integración en otros proyectos como Fabric y Sawtooth que cuenta con una serie de elementos preconfigurados. Además, está orientada al desarrollo de proyectos móviles y está desarrollado en C++.

1.5.7. Evaluación de plataformas

A continuación, se realiza una comparativa entre las plataformas Ethereum y Hyperledger con el fin de identificar la plataforma más adecuada para utilizarse en contratos inteligentes y privacidad. Para ello, se compararon las principales características identificadas entre Hyperledger y Ethereum.

La comparativa se detalla en la Tabla 1, donde se identificó las siguientes métricas para su comparación: descripción de la plataforma, nombre de la organización que alberga los proyectos, moneda, recompensa minera, forma de almacenamiento de la información, algoritmo de consenso, modo de operación, contratos inteligentes, consenso y los sistemas operativos que soporta.

	Hyperledger	**Ethereum**
Descripción plataforma	Blockchain de propósito general	Blockchain de propósito general
Organización	Fundación Linux	Ethereum
Moneda	Ninguna	Ether
Recompensa minera	N/A	Si
Almacenamiento	Base de datos de valores clave	Datos de la cuenta
Algoritmo de consenso	PBFT (dependiendo de los requisitos específicos de la aplicación)	En su mayoría PoW. En otros PoS (depende de la participación económica de un minero o de la criptomoneda disponible en la red)
Modo de operación	Bajo permisos (privado)	Público o privado
Contratos inteligentes	Varios lenguajes de programación: JAVA, GO, NODEjs	Lenguaje de programación: Solidity
Consenso	Sólo los involucrados llegan a un consenso (mejora la escalabilidad, rendimiento y privacidad)	Todos deben llegar a consenso, aunque no tengan participación (afecta directamente al desempeño de la red)
Sistemas operativos	Linux, MAC y Windows	Linux, MAC y Windows

Tabla 1: Comparativa entre Ethereum y Hyperledger Fabric

Ahora, tomando en cuenta las condiciones del presente trabajo, se considera los siguientes factores que se empleará para el desarrollo del mismo, como: *privacidad*, se debe mantener la privacidad de las operaciones o procesos que se realizan e *identidad*, el acceso a cualquier documento debe ser cuando así lo requieran público o privado, por tanto, se debe permitir realizar restricciones.

Considerando los aspectos anteriores se descarta el uso de Ethereum debido a que no garantiza un adecuado consenso de validación cuando su red es privada, por tanto, se inclina por el uso de Hyperledger por la privacidad que ofrece y la no utilización de la minería como consenso, además de la flexibilidad que presenta y la gran comunidad de soporte que lo respalda.

1.5.8. Contratos inteligentes

Los contratos inteligentes juegan un papel esencial. Estos están integrados con la tecnología blockchain y ejecutan muchas aplicaciones en una infraestructura descentralizada. Son contratos autoejecutables que están diseñados para cumplir con las condiciones de los acuerdos y luego entregar los resultados, también son a prueba de manipulaciones, es decir, nadie puede alterarlos. Además, proporcionan precisión, transparencia, alta velocidad, almacenamiento de datos y confianza [22]. En conclusión, son un procedimiento almacenado que desencadena una transacción, donde, cada entrada, salida y estado de las transacciones se ven afectados por cada nodo que participó en la misma.

1.5.9. Profundizando en Hyperledger

Hyperledger Fabric

Es una tecnología para soluciones contables distribuidas autorizadas de código abierto que por su arquitectura modular ofrece altos grados de confidencialidad, resistencia, flexibilidad y escalabilidad. Es utilizada principalmente para diferentes entornos empresariales a través de blockchain, donde los participantes en la red (red operada bajo una autoridad conforme a los acuerdos o diseño) son conocidos entre sí, pero pueden no confiar el uno con el otro.

Permite la implementación de contratos inteligentes mediante la utilización de algunos lenguajes de programación como; Java, Go y Node.js [22].

Chaincode [23]

Es un programa escrito en Go, Node.js o Java que implementa una interfaz prescrita. Se ejecuta en un contenedor seguro aislado del proceso de homologación e inicializa y gestiona el estado contable a través de transacciones enviadas por las solicitudes.

Normalmente maneja la lógica comercial acordada por los miembros de la red, por lo que puede considerarse como un “contrato inteligente”. Generalmente es usado por los administradores para agrupar los contratos inteligentes relacionados.

Un chaincode dispone de un estado, el cual está limitado exclusivamente a su propio uso y otro no puede acceder directamente a él. Sin embargo, dentro de la misma red, dado el permiso necesario, un chaincode puede invocar a otro chaincode para acceder a su estado.

1.5.10. Serverless

La computación sin servidores o serverless se entiende como un modelo de computación en la nube, cuyo objetivo es abstraer la gestión de servidores y las decisiones de infraestructura a bajo nivel. Es decir, la asignación de recursos y todas las decisiones de infraestructura son gestionadas por el proveedor de la nube en lugar del arquitecto de infraestructura permitiendo aportar grandes beneficios.

1.5.11. Amazon Web Services (AWS)

Amazon Simple Storage Service (S3)

Es el sistema de almacenamiento simple de Amazon. Conceptualmente, es un almacén infinito para objetos de tamaño variable (mínimo 1 Byte, máximo 5 GB). Un objeto es simplemente un contendor de bytes que se identifica por una URI (a la que se tiene acceso desde la interfaz de S3).

Los clientes pueden leer y actualizar objetos en S3 de forma remota utilizando las librerías que proporciona funciones similares a los protocolos SOAP o REST. El cubo (bucket) aparte de almacenar los archivos contiene además las versiones previas de dichos archivos, lo que hace que se pueda llevar un respectivo control de versiones. El cubo también puede ser tratado como una parte fundamental de la seguridad, donde los usuarios pueden conceder autorización de lectura y escritura a otros usuarios para; cubos enteros o bien se pueden conceder privilegios de acceso a objetos individuales. Por tanto, se puede hacer que los cubos sean totalmente públicos y que implica que cualquiera pueda acceder por la URI.

Lambda

AWS Lambda es el servicio que permite implementar arquitecturas de microservicios sin necesidad de gestionar servidores, facilitando la creación de funciones que pueden ser fácilmente desplegadas y escaladas automáticamente. Lo que permite reducir costos de infraestructura y operaciones de computación. En general, este servicio está diseñado para ofrecer una estructura de costes por solicitud.

Permite escribir las funciones en los lenguajes Node.js, Java, Python y C#. Este tipo de arquitectura es adecuada para aplicaciones que requieren de gran computación de datos a altas velocidades o computaciones paralelas. Así, las funciones lambda son invocadas mediante las bibliotecas proporcionadas por AWS.

AWS Secrets Manager [24]

Ayuda a proteger los datos confidenciales necesarios para acceder a sus aplicaciones, servicios y recursos de TI. El servicio le permite alternar, administrar y recuperar fácilmente credenciales de base de datos, claves de API y otros datos confidenciales durante su ciclo de vida. Los usuarios y las aplicaciones recuperan datos confidenciales con una llamada a las API de Secrets Manager, lo que elimina la necesidad de codificar información confidencial en texto sin formato. Además, ofrece la alternación de datos confidenciales con integración incorporada para Amazon RDS, Amazon Redshift y Amazon DocumentDB, también puede extenderse a otros tipos de datos confidenciales, incluidas las claves de API y los tokens de OAuth. Finalmente permite controlar el acceso a los datos confidenciales mediante permisos detallados y auditar la alternación de datos de manera centralizada de los recursos que se encuentran en la nube de AWS, en servicios de terceros o en las instalaciones propias.

Amazon Quantum Ledger Database (QLDB) [25]

Amazon QLDB es una base de datos de contabilidad completamente administrada la cual proporciona un registro de transacciones transparente, inmutable y que se puede ser verificada mediante criptografía. Además, puede utilizarse para registrar cada uno de los cambios que se producen en los datos de las aplicaciones manteniendo un historial completo y verificable.

Los libros mayores generalmente se usan para registrar un historial de la actividad económica y financiera de una organización. Las aplicaciones del libro mayor a menudo se implementan usando tablas de auditoría personalizada o registros de auditoría creadas en base de datos relacionales. Sin embargo, crear la funcionalidad de una auditoría con bases de datos relacionales es lento y propenso al error humano ya que requiere desarrollo personalizado y no son inherentemente inmutables, además cualquier cambio inintencionado en los datos es difícil de rastrear y verificar. De forma alternativa, los marcos de la cadena de bloque como Hyperledger Fabric y Ethereum también se pueden usar como libro mayor, sin embargo, esto agrega complejidad ya que necesita establecer; una red completa de cadena de bloques con nodos múltiples, gestión de su infraestructura y requieren nodos para validar cada transacción antes de que se pueda agregar al libro mayor.

Amazon QLDB es una nueva clase de base de datos que elimina la necesidad del esfuerzo de desarrollo completo en crear sus propias aplicaciones similares al libro mayor. Con QLDB, el historial de cambios de los datos es inmutable, es decir, no se puede modificar ni eliminar y, al usar la criptografía, puede verificar fácilmente que no se hayan producido modificaciones no deseadas en los datos de su aplicación. También es fácil de usar debido a que proporciona a los desarrolladores una API familiar similar a la de SQL, un modelo de datos de documentos flexible y un soporte completo para transacciones. La capacidad de streaming de QLDB ofrece un flujo casi en tiempo real de los datos almacenados en QLDB, lo que le permite desarrollar flujos de trabajo determinados por eventos, realizar análisis en tiempo real y replicar datos en otros servicios de AWS para contribuir al procesamiento de análisis avanzado. Por último, QLDB es sin servidor lo que le permite escalar de forma automática para admitir las demandas de su aplicación. No hay servidores para administrar y no hay límites de lectura o escritura a configurar.

Amazon Managed Blockchain [26]

Amazon Managed Blockchain es un servicio completamente administrado que facilita la creación y administración de redes de blockchain escalables mediante el uso de los marcos de código abierto populares como Hyperledger Fabric y Ethereum. Además, es un servicio completamente administrado que le permite configurar y administrar una red de blockchain escalable. Con Amazon Managed Blockchain se elimina la sobrecarga que implica la creación de la red, además, el servicio ajusta su escala automáticamente para satisfacer las demandas de miles de aplicaciones que ejecutan millones de transacciones.

Por otro lado, también administra sus certificados permitiendo invitar de forma sencilla a nuevos miembros para que se unan a la red y realizar un seguimiento de las métricas operacionales como, por ejemplo, el uso de recursos informáticos, de memoria y almacenamiento. Finalmente, puede replicar una copia inmutable de su actividad de red de cadenas de bloques a QLDB lo que permite analizar fácilmente la actividad de la red de manera externa y obtener información acerca de las tendencias.

1.5.12. Metodología Goal Question Metric (GQM) [8]

Es un enfoque creado para definir y evaluar objetivos para un proyecto en particular y en un entorno particular. Además, es un sistema de preguntas y respuestas simples para la evaluación de propiedades. A continuación, se identifica lo siguiente;

Niveles:

1. **Nivel conceptual (objetivos):** se define un objetivo para un objeto, para una variedad de razones desde varios puntos de vista relativo a un entorno en particular. Los objetos medibles pueden ser productos (documentos), procesos (como el proceso de gestión documental) y recursos (personas, software, etc.).
2. **Nivel operativo (pregunta):** las preguntas intentan caracterizar el objeto de medición.
3. **Nivel cuantitativo (métrico):** se asocia un conjunto de datos con cada pregunta para responderla de forma cuantitativa**.** Estos pueden ser: objetivo si dependen sólo del objeto que se está midiendo y no del punto de vista del que se toma; o subjetivo si depende tanto del objeto que se está midiendo como del punto de vista desde el cual se toma.

Proceso:

Un modelo GQM inicia definiendo diferentes objetivos. Cada objetivo debe cumplir la siguiente estructura:

- Propósito de la medida.
- Objeto a medir.
- Problema a medir.
- Punto de vista desde el cual se toma la medida.

Cada objetivo definido debe enfocarse en un conjunto de preguntas que tienen como propósito la división del problema. Posterior, cada pregunta se relaciona en métricas objetivas o subjetivas.

1.5.13. Norma ISO 15489 [27]

Origen

Se trata de la primera norma internacional en el campo de la gestión de documentos. Su primera edición fue publicada en septiembre de 2001 por el Comité Técnico ISO / TC 46, Información y documentación, Subcomité SC 11, Archivos /Gestión de registros. La norma ISO 15489 se centra en los principios de la gestión de documentos y establece los requisitos básicos para permitir a las organizaciones establecer un marco de buenas prácticas que mejorarán de forma sistemática y efectiva la creación y mantenimiento de los documentos. Por consiguiente, también de apoyar en las políticas y los objetivos de la organización de acuerdo con sus necesidades.

Los objetivos principales de la norma son: 1. Adecuar la gestión de los documentos de la organización, y 2. Garantizar que una organización sea capaz de crear, conservar y utilizar los documentos que necesita. Donde, en términos generales, esta norma regula la gestión de documentos producidos en las organizaciones, ya sean públicos o privados, para clientes externos e internos. De este modo, los documentos deben ser auténticos, confiables, completos, sin alteración y deben permitir su uso y acceso, así también deben poseer metadatos que definan el contexto, contenido y estructura.

A continuación, se identifica las partes que constituye la norma:

a) **UNE-ISO 15489-1: 2006. Información y documentación - Gestión de documentos - Parte 1:** Generalidades, define los conceptos básicos, los principios y los requisitos de la gestión de documentos en las organizaciones, es decir, proporciona una idea de todos los aspectos a contemplar para poner en marcha un plan de gestión de documentos, como:
    - Beneficios de la gestión de documentos.
    - Marco reglamentario (entorno legal y normativo).
    - Política y responsables.
    - Requisitos de la gestión de documentos.
    - Diseño e implementación de un sistema de gestión de documentos.
    - Procesos y controles de la gestión de documentos.
    - Supervisión y auditoría.
    - Formación.

b) **UNE-ISO / TR 15489-2: 2006. Información y documentación - Gestión de documentos - Parte 2**: Directrices, es un informe técnico que proporciona una metodología de implementación de un sistema de gestión de documentos de acuerdo con los principios definidos en la primera parte de la norma. Sobresale las estrategias y la metodología de diseño e implementación y las directrices específicas adicionales para definir los procesos y los instrumentos principales de gestión de documentos.

    La norma dirige la práctica de cualquier persona que cree o utiliza documentos en el curso de sus actividades, lo que incluye:
    - Fijar políticas y normas.
    - Asignar autoridades y autoridades.
    - Establecer y promulgar procedimientos y directivas.
    - Proporcionar una serie de servicios relacionados con la gestión y uso de documentos.

- Diseñar, implementar y administrar sistemas especializados para la gestión de documentos.
- Integrar la gestión de documentos en los sistemas y los procesos de la actividad.

La norma ISO 15489 propone la metodología DIRKS (Diseño e Implementación Sistemas de mantenimiento de registros), para el diseño e implementación de un sistema de gestión de documentos y consta de ocho etapas como se indica en la Figura 1.

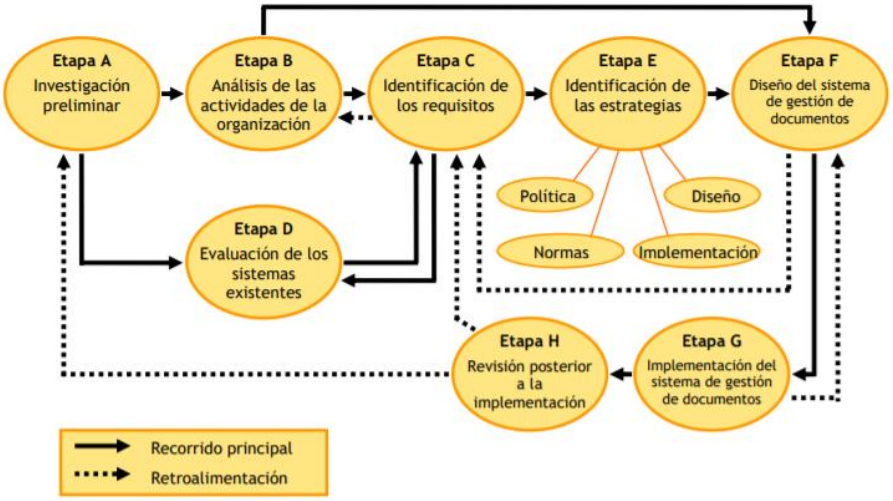


Figura 1: La metodología DIRKS

Etapas	Actividades
A. Investigación preliminar	**Objetivo:** proporcionar la comprensión del contexto en el que la organización desarrolla su actividad. Lo manifestado tiene como la de identificar los factores que influyen en la necesidad de crear y mantener documentos (administrativos, legales, de negocio y sociales), y conocer las fortalezas y debilidades que se presentan dentro de la organización con respecto a la gestión de documentos.
	Resultados: examen de la misión, visión y valores de la organización, de su política y

	estrategia, de sus objetivos, de su estructura organizativa, de las regulaciones específicos a las cuales están algunas veces sus actividades y de los factores de éxito relacionados con la gestión de los documentos dentro de la organización en la cual se aplica.
B. Análisis de las actividades de la organización	**Objetivo:** desarrollar un modelo conceptual de qué hace la organización y de cómo lo hace, examinando cómo interactúan los documentos con los procesos y las actividades de la empresa. Se puede identificar y analizar los procesos y actividades de la organización y examen los circuitos documentales que se siguen para llevar a cabo un cabo estos procesos. Es útil conocer: • Los tipos documentales que producen y utilizan cada unidad. • Las atribuciones de cada unidad sobre cada tipo documental (elaboración, revisión, aprobación, control, archivo, etc.). • Las aplicaciones informáticas utilizadas para crear y gestionar los documentos. • Su soporte y su localización. • Sus valores documentales y sus plazos de conservación.
	Resultados: se puede elaborar una primera versión del cuadro de clasificación con el fin de mostrar las funciones, actividades y operaciones que generan documentos. También es útil utilizar un análisis secuencial que describe mediante diagramas de flujo de

	procesos clave de la empresa (por ejemplo, en el caso de una empresa de edificación y obra civil el proceso que se sigue desde el estudio de la oferta hasta la finalización del período de garantía de la obra, pasando por las fases de elaboración del proyecto constructivo, licitación, contratación y ejecución de la obra). Los diagramas de proceso que permiten visualizar qué documentos se producen en cada parte del proceso, cómo se transmite la información de una unidad a otra y quién es responsable en cada momento del manejo y custodia de los documentos.
C. Identificación de los requisitos	**Objetivo:** determinar los requisitos que tienen que cumplir para crear y mantener documentos que evidencien las actividades de la organización. Estos requisitos se identifican mediante un análisis sistemático de las necesidades de la organización, las obligaciones legales y normativas y la rendición de cuentas, tanto con respecto a partes interesadas internas (dirección, personal) como exteriores (clientes, accionistas, proveedores, contratistas, administración pública).
	Resultados: se puede redactar una primera versión del calendario de conservación (que determina los horarios durante los cuales se tiene que preservar la documentación) y de la tabla de acceso y seguridad (que establece las condiciones de acceso a los documentos).
D. Evaluación de los sistemas existentes	**Objetivo:** paralelamente a la etapa A, B y C, se analiza el sistema de gestión de

	documentos y otros sistemas de información relacionada, con el fin de valorar si incorporan y requieren los documentos necesarios de una manera confiable, íntegra, exhaustiva, sistemática y conforme a los requisitos identificados en la etapa anterior.
	Resultados: como resultado se puede hacer un inventario de los sistemas que evalúan el cumplimiento de los requisitos documentales
E. Identificación de las estrategias para cumplir con los requisitos	**Objetivo**: determinar qué políticas, normas y procedimientos se adoptarán y qué herramientas, tanto informáticas como documentales, hace falta diseñar e implementar con el fin de implementar la creación y el mantenimiento de los documentos que detallan la actividad de la organización. En este sentido, estas estrategias pueden incluir: • El establecimiento de políticas, normas o códigos de buenas prácticas de gestión. • La asignación de responsabilidades y competencias. • La elaboración de procedimientos e instrucciones de trabajo. • El diseño, implementación y administración de nuevos componentes de los sistemas o de nuevos sistemas. • La integración de la gestión de documentos en los procesos y sistemas de la organización.
	Resultados: puede ser conveniente presentar un informe, junto con un resumen

	ejecutivo, dirigido a la dirección en el cual se planteen las posibles estrategias de actuación y los beneficios que se esperan obtener**.**
F. Diseño del sistema de gestión de documentos	**Objetivo:** traducir las estrategias afectadas en la etapa anterior en un plan de actuación que cumpla con los requisitos identificados en la etapa C y que solucione las deficiencias detectadas en la etapa D. Este plan aporta una visión de conjunto en que se integran los diferentes elementos del sistema.
	Resultados: se pueden llevar a cabo las siguientes acciones: • Elaborar los instrumentos del sistema de gestión de documentos: cuadro de clasificación, calendario de conservación, tabla de acceso y seguridad. • Definir los requisitos funcionales o diseñar y desarrollar las posibles aplicaciones informáticas. • Redactar las primeras versiones de la documentación del sistema de gestión de documentos: manual, procedimientos e instrucciones de trabajo. • Establecer una metodología de evaluación del rendimiento del sistema de gestión de documentos y los mecanismos de supervisión y control. • Elaborar un calendario de trabajo en el que se programará las tareas previsto para implementar el sistema.
G. Implementación del sistema de	**Objetivo:** aplicar el conjunto de estrategias

gestión de documentos	poniendo en marcha el plan de actuación diseñada en la etapa anterior con una alteración mínima de las actividades diarias.
	Resultados: se pueden llevar a cabo las siguientes funciones: • Revisión y aprobación de los instrumentos del sistema de gestión de documentos. • Puesta en marcha, en fase de prueba, de las aplicaciones informáticas. • Revisión, aprobación y publicación del manual, los procedimientos y las instrucciones de trabajo. • Formación del personal. • Reorganización del depósito de archivo
H. Revisión posterior a la implementación	**Objetivo:** evaluar y medir la eficacia del sistema de gestión de documentos con el fin de corregir las deficiencias detectadas.
	Resultados: se puede entregar a la dirección un informe de revisión en el que se detallarán las discrepancias observadas y se propondrán las acciones adecuadas para corregir las disconformidades que se han encontrado y adoptar las oportunidades de mejora que no se hayan previsto en las etapas anteriores.

Tabla 2: Etapas metodología DIRKS

1.5.14. Componentes de un Sistema de Gestión

La gestión de documentos es el conjunto de tareas y procedimientos orientados a lograr un control eficaz y sistemático de la creación, recepción, mantenimiento, uso y disposición de los documentos, incluidos los procesos para incorporar y mantener, en forma

de documentos, la información y prueba de las actividades y operaciones de la organización. Además, es necesario recordar que la gestión de documentos deriva de la función archivística, lo que implica, que una estructura común debería estar presente en todo sistema de gestión de documentos, con independencia del tamaño y complejidad de la organización. Por consiguiente, se identifica lo siguiente:

- Los subsistemas: representan el ciclo vital de los documentos desde cuando son creados, usados, conservados, dados de baja o preservados como históricos de acuerdo con un criterio establecido. Por tanto, se determina las siguientes acciones:
  - Creación o adquisición del documento
  - Ubicación del documento en un sistema lógico documentado que contribuye a su clasificación y ordenamiento que facilita su recuperación.
  - Conservación y uso.
- Las herramientas funcionales: desarrollan las funciones específicas de la gestión de documentos, como:
  - Control documental, para gestionar, distribuir y registrar los documentos.
  - Clasificación y ordenación, para agrupar u ordenar los documentos de acuerdo con un criterio establecido.
  - Descripción, para establecer un plan de descripción en donde detalle las características de los mismos.
  - Instalación, ubicación física de los documentos en una unidad de instalación.
  - Mantenimiento, para la valoración, selección y eliminación de un documento de acuerdo con un criterio establecido.
- Las herramientas normativas: prevalecen dos perspectivas reglamentarias y procedimentales.
- Las herramientas operativas: aseguran la funcionalidad desde el punto de vista operativo que involucran desde la formación de los usuarios, responsabilidades y las tecnologías de la información.

Por otro lado, la gestión de documentos debe desarrollarse apoyada en tres pilares:

a) Visión estratégica: alineamiento con el negocio, política y recursos de la organización.
b) Visión operativa: determinación de los procesos, competencias y controles.
c) Enfoque tecnológico: desarrollo e implementación de las aplicaciones de gestión documental.

Finalmente, las organizaciones deben implementar procesos de creación y control de la documentación, tales que les permitan:

- Determinar qué documentos, cuándo y cómo den ser creados y capturados en cada

proceso de negocio.

- Determinar la información sobre el contenido, contexto y control (metadatos) que debe incluirse en los documentos.
- Decidir en qué forma y estructura se deben crear y capturar los documentos.
- Determinar qué información de control (metadatos) debe crearse en los procesos de gestión de documentos, cómo se vincularán con los documentos y cómo se gestionará a lo largo del tiempo.
- Establecer las reglas y condiciones para el uso de los documentos a lo largo del tiempo.
- Mantener la usabilidad de los documentos a lo largo del tiempo.
- Establecer la disposición/eliminación autorizada de los documentos.
- Establecer las condiciones de administración y, mantenimiento de las aplicaciones de gestión de documentos.

1.5.15. Sistema Educativo en Ecuador [28]

Definiciones básicas

Instituciones Educativas (IE): son los establecimientos que imparten servicios educativos en distintos niveles.

Docente: persona oficialmente habilitada en régimen de empleo o parcial para orientar y encauzar la experiencia del aprendizaje de estudiantes, cualquiera que sea su certificación profesional o la modalidad de enseñanza.

Estudiante: es toda persona que demanda servicios educativos y recurre a las aulas dentro de lo programado por las IE.

Estudiante matriculado: es una persona que lleva a cabo, por sí misma o a través de su representante legal, el trámite de inscripción en una determinada IE y, por tanto, está habilitada para cursar un determinado año, grado o curso.

Sostenimiento: las IE se clasifican según la fuente principal de financiamiento que permite su sostenimiento y pueden ser públicas, fiscomisionales y privadas o particulares.

Año/Grado/Curso: etapa específica de instrucción de la educación formal normalmente cubierta durante un año académicos.

Periodo de escolaridad: es una medida que señala el promedio de años que una persona tiene de educación.

Periodo/ año lectivo: comprende el tiempo en que los estudiantes asisten a clases.

Jurisdicción: se refiere a la dirección provincial y cantonal de educación que tiene a cargo lIE.

Estructura

De acuerdo con lo especificado en la Ley Orgánica de Educación Intercultural (LOEI) y el Reglamento a la LOEI, la clasificación de los niveles educativos corresponde a:

- Educación Inicial (EI)
- Educación General Básica (EGB)
- Bachillerato

A su vez, estos niveles educativos presentan los siguientes subniveles (Reglamento General a la LOEI, 2012: art. 27):

Educación Inicial:

- Inicial 1, que no es escolarizado y comprende a infantes de hasta tres (3) años de edad.
- Inicial 2, que comprende a infantes de tres (3) a cinco (5) años de edad.

Educación General Básica:

- Preparatoria, que corresponde a 1° grado de EGB y preferentemente se ofrece a los estudiantes de cinco (5) años de edad;
- Básica Elemental, que corresponde a 2°, 3° y 4° grados de EGB y preferentemente se ofrece a los estudiantes de 6 a 8 años de edad;
- Básica Media, que corresponde a 5°, 6° y 7° grados de EGB y preferentemente se ofrece a los estudiantes de 9 a 11 años de edad; y,
- Básica Superior, que corresponde a 8°, 9° y 10° grados de EGB y preferentemente se ofrece a los estudiantes de 12 a 14 años de edad.

Bachillerato:

El nivel de Bachillerato tiene tres (3) cursos y preferentemente se ofrece a los estudiantes de 15 a 17 años de edad. Como se ha descrito, el rango de edad sugerida de ingreso para el nivel de Educación Inicial corresponde de 3 a 5 años (LOEI, 2011: art. 40), 5 a 14 años para la EGB (LOEI, 2011: art. 42), y 15 a 17 años para el Bachillerato (LOEI, 2011: art. 43). Los niños, niñas, adolescentes y jóvenes que exceden estas edades pueden ingresar al sistema educativo sin discriminación.

Documentos académicos para Instituciones Educativas privadas del Ecuador

Las IE privadas, gestionan concurrentemente durante un año lectivo, documentos académicos que avalan el desempeño de los estudiantes durante un periodo escolar. Por lo general, estos documentos son obtenidos de forma manual, por sistemas informáticos de proveedores externos o de su autoría, hojas de Excel, etc. Con estos documentos, se permiten a los docentes, personal administrativo gestionar todas sus actividades relacionadas con los estudiantes. Sin embargo, las mismas no cuentan con un sistema estándar de gestión académica para la emisión y gestión de documentos académicos, ya que los mismos difieren en cada IE y dependen de la autoridad interna.

Además, existen documentos académicos que necesitan de algún tipo de validación por parte de alguna entidad legal externa a la IE (Ministerio de Educación del Ecuador) para poder avalar la información que estos contienen, estos documentos se identifican como documentos o certificados ministeriales. Por otro lado, también existen documentos que sólo requieren la validación de alguna entidad legal interna como: libretas de calificaciones, currículo de estudiantes, pases de año, etc.

Proceso de emisión de certificados

Se identifica el proceso interno estándar que actualmente las IE llevan a cabo para la emisión de dichos certificados:

Actividad	Responsable
Solicitar a la Secretaría General el/los certificados.	Estudiante, Representante o profesional
Verificar solicitud y tipo de documento	Secretaría General
Verificar, imprimir y sellar el(los) certificado(s) por las respectivas autoridades involucradas.	Secretaria General
Legalización de certificados (se efectúa cuando es un certificado ministerial)	Secretaria General y Ministerio de Educación
Firma de certificados	Secretaria General, Rector y/o Ministerio de Educación
Entrega de certificados	Secretaria General

Tabla 3: Proceso de emisión de certificados

Proceso de legalización de certificados por parte del Ministerio de Educación del Ecuador

De acuerdo con el Ministerio de Educación del Ecuador, se identifica el actual proceso y requisitos para la legación de los certificados ministeriales:

Nombre del trámite	Requisitos	Proceso
LEGALIZACIÓN DE CUADROS DE CALIFICACIONES	• Formato dirigido al Director Distrital. • Cuadros de calificaciones quimestrales, finales y promociones. • Nómina de matriculados • Acuerdos de Funcionamiento	1. Usuario entrega documentación completa para realizar trámite 2. Usuario recibe comprobante de ingreso, indicando plazo de entrega 3. El analista de atención ciudadana debe: Revisar los cuadros de calificaciones conjuntamente con el representante de la Institución Educativa, verificando los requisitos de pase de nivel 4. El analista debe: Validar los estudios del estudiante mediante su firma 5. Entregar la legalización de cuadros en máximo cuatro días laborables

Tabla 4: Proceso de legalización de certificados ministeriales

1.6. Revisión Sistemática de la literatura

Mediante la propuesta metodológica de Kitchenham [29] se realizó la revisión de la literatura para identificar, evaluar e interpretar la información necesaria para diseñar un modelo de gestión documental académica inteligente basado en la tecnología Blockchain.

1.6.1. Fase de búsqueda

Se establece la guía bajo el cual se realiza el estudio y clasificación del material bibliográfico, a partir de la pregunta: ¿Es posible diseñar un modelo con la tecnología Blockchain que contribuya de manera segura y eficiente la gestión documental académica en instituciones educativas privadas de Quito?

Cadenas de búsqueda

Para la búsqueda de la información necesaria para solventar a la pregunta de investigación planteada, se determina las siguientes cadenas de búsqueda:

Population	Private school OR high schools
Intervention	Blockchain for digital certificate OR Blockchain for documents OR Blockchain for students
Outcome	Secure OR verification OR integrity
Context	Education
Search strategy	Population AND Intervention AND Outcome

Tabla 5: Cadenas de búsqueda

Criterios de inclusión y exclusión

Para la obtención de la información relacionada con la pregunta de investigación se identifican los siguientes criterios:

Inclusión	Diplomas/Documentos digitales/ Transcripciones/Contratos inteligentes
Exclusión	Artículos que no se encuentren disponibles libremente. Artículos duplicados. Tesis de pregrado. Otros idiomas diferentes a los establecidos.

Tabla 6: Criterios de inclusión y exclusión

Formas de extracción

Se identifica las siguientes fuentes digitales para el proceso de extracción:

Fuente	Enlace
Springer Link	https://link.springer.com
IEEE Xplore	https://ieeexplore.ieee.org
Researchgate	https://www.researchgate.net/

Tabla 7: Fuentes digitales

Criterios de selección

La selección del material depende principalmente de los términos de búsqueda y las fuentes digitales, adicional se identifica los siguientes criterios:

- **Idioma**: inglés debido a que existe más trabajos en este idioma.
- **Contenido:**
  - Que muestren una metodología y resultados claros.
  - Sean únicos.
  - Aporte a la investigación.
- **Periodo de tiempo:** Publicaciones a partir del año 2018.

1.6.2. Fase de Ejecución

El resultado de la búsqueda se muestra en la Tabla 8, en total se obtuvieron 68 artículos donde se excluyeron 12 artículos que no se relacionan con el tema. Además, se identificaron artículos duplicados y posterior a la depuración se obtuvo 12 artículos relevantes para el estudio.

Cadena de búsqueda	Término asociado	Springer Link	IEEE	Researchgate	Subtotal
Secure Verification Integrity	Blockchain for digital certificate	1 3 0	4 5 1	7 9 4	12 17 5
Secure Verification Integrity	Blockchain for documents	1 0 0	2 3 1	5 3 1	8 6 2
Secure Verification Integrity	Blochchain for student	1 0 0	2 1 1	5 6 2	8 7 3

Número de trabajos encontrados	68

Tabla 8: Trabajos potencialmente relevantes

Recurso	Resultados	Estudios potencialmente relevantes	No relevantes	Repetidos	Incompleto	Estudios relevantes
Springer Link	6	3				1
IEEE	20	12	6	2	1	4
Researchgate	42	18	2	4	3	7
						12

Tabla 9: Trabajos relevantes

Para la revisión sistemática de la literatura de tomaron los siguientes 12 artículos según su relevancia:

	Título	Autores	Año	Relevancia
[4]	Transcript Management Using Blockchain Enabled Smart Contracts	Patel, Kirtan	2019	Alta
[5]	Application of the blockchain technology for digital diplomas: problems and prospects	M. Shamsutdinova, T	2019	Alta
[6]	Blockchain and Smart Contract for Digital Certificate	J. Cheng, N. Lee, C. Chi, Y. Chen	2018	Alta
[10]	Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents	Mthethwa, Sthembile	2018	Alta
[9]	Issuing and Verifying Digital Certificates with Blockchain	Thua Huynh, Trong	2018	Alta
[30]	Cerberus: A Blockchain-Based Accreditation and Degree Verification System	Tariq, Aamna	2019	Alta
[7]	SmartCert BlockChain Imperative for Educational Certificates	T. Kanan	2019	Alta

[19]	Blockchain Based Framework for Educational Certificates Verification	Saleh, Omar	2020	Media
[31]	Blockchain and smart contracts for higher education registry in Brazil	M. Palma, Lucas	2019	Media
[32]	The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling	Gresch, Jerinas	2019	Media
[33]	Blockchain for Student Data Privacy and Consent	Gilda, Shlok	2018	Media
[34]	CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials	R. Arenas	2018	Media

Tabla 10: Información de trabajos relevantes

1.6.3. Fase de Extracción

Se realizó el análisis de los 12 artículos seleccionados anteriormente mediante la herramienta Atlas.ti 8 en donde se procedió a:

- Identificar segmentos de texto importantes para el estudio.
- Clasificar las citas mediante códigos.
- Agrupar códigos mediante familias.

	Título del artículo académico	**Modelo**	**Fase**	**Atributo Seguridad**	**Metodologías**
[9]	Issuing and Verifying Digital Certificates with Blockchain	NO	Implementación		UniCert basado en UniCoin construidos a partir de Blockchain
[30]	Cerberus: A Blockchain-Based Accreditation and Degree Verification System	NO		Integridad	

[7]	SmartCert BlockChain Imperative for Educational Certificates	SI	Diseño	Integridad Autenticidad	SmartCert basado en contratos inteligentes
[4]	Transcript Management Using Blockchain Enabled Smart Contracts	SI	Diseño Implementación		
[5]	Application of the blockchain technology for digital diplomas: problems and prospects	SI	Diseño e implementación	Confidencialidad Integridad	Ethereum Willetera electrónica
[6]	Blockchain and Smart Contract for Digital Certificate	SI	Diseño	Confidencialidad Integridad	Ethereum Smart Contracts
[10]	Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents	SI	Diseño	Integridad	Autenticación, autorización, confidencialidad, propietario y privacidad
[19]	Blockchain Based Framework for Educational Certificates Verification	NO	Implementación	Confidencialidad	
[31]	Blockchain and smart contracts for higher education registry in Brazil	SI	Diseño		

[32]	The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling	NO	Diseño		
[33]	Blockchain for Student Data Privacy and Consent	NO			
[34]	CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials	SI	Implementación	Disponibilidad	CredenceLedge Smart Contract Ethereum Multichain Hyperledger

Tabla 11: Detalle de fase de extracción

Los documentos, en su mayoría, aún son impresos físicamente, esto los hace susceptibles ante posibles fraudes poniendo en peligro la credibilidad tanto del titular del documento como la de la autoridad emisora [19]. Para poder manejar la transparencia y verificabilidad de los documentos sin la intervención de organizaciones intermediarias, quienes son las que implementan una variedad de funciones de supervisión, certificación de soporte y determinación de posibles manipulaciones. Se ha identificado varias técnicas que permiten proteger a los documentos, como; la combinación de códigos de barras, firmas digitales y hash criptográfico, los cuales trabajando en conjunto han demostrado buenos resultados. Para ello, el autor [10] ha propuesto una solución que incorpora la combinación de blockchain con las técnicas anteriormente mencionadas.

Por otro lado, Blockchain se identifica como la tecnología subyacente que impulsa las criptomonedas como Bitcoin y Ethereum, la misma que está ganando mucha atención de diferentes partes de la industria, gobiernos y comunidades de investigación. Esta tecnología puede cambiar conceptualmente el sistema de archivos de datos, aumentar la confiabilidad de la protección de la información contra la falsificación, permitiendo además acelerar significativamente la ejecución de solicitudes de información y procesamiento de datos. Es así, que los autores de los artículos analizados identifican a Blockchain como una tecnología capaz de mantener la integridad de la información, mediante algunos atributos clave como la

descentralización, la inmutabilidad, la seguridad y la transparencia [31], así también, como su autenticidad mediante los contratos inteligentes o smart contracts que permite avalar su precedencia entre dos partes involucradas sin depender de un intermediario legal.

Además, para implementar un sistema de autenticación electrónica que valide los documentos electrónicamente, se puede utilizar blockchain ya que permite implementar un sistema integrado de documentos oficiales de todo tipo y construir un sistema de base de datos robusto que no puede ser manipulado, modificado, destruido o alterado [7]. Esto garantiza la seguridad de los documentos emitidos dentro de una entidad en específico y aquellos exportados fuera del mismo, así como, de un nivel muy alto de seguridad y confidencialidad de los datos e información. Por consiguiente, Blockchain permite emitir documentos a terceros en un tiempo considerable, sin la intervención de muchos recursos y llevar un registro permanente de todas sus transacciones [9].

En el sector educativo, existen varios temas de interés que valen la pena ser analizados para salvaguardar potenciales problemas de seguridad, falsificaciones, integridad y validación de documentos académico [6]. En especial los diplomas o certificados, ya que son los documentos más importantes debido a que son pruebas oficiales de presentación [32]. Donde, se han identificado algunas soluciones basadas en el uso de la tecnología Blockchain; los autores [34] proponen una verificación descentralizada de credenciales académicas denominada CredenceLedger que almacena pruebas de datos compactas de credenciales académicas digitales en el libro mayor, las cuales son fácilmente verificables para los interesados en la educación y las organizaciones de terceros. De manera similar los autores de [32] y [9], identifican una solución holística que incluye la emisión y verificación de diplomas denominado UZHBC (University of ZuricH BlockChain y UniCert respectivamente, lo que permite resolver el problema de la falsificación.

Por otra parte, se identifican las siguientes soluciones con el uso de contratos inteligentes donde; el artículo [33] plantea el uso de Hyperledger Fabric y Hyperledger Composer para un marco de autorización anidada, lo que permite otorgar autorización y derechos de acceso a datos e intervención de terceros. El artículo [31] propone un modelo que permite registrar a los estudiantes y sus créditos académicos, utilizando la infraestructura de clave pública de Brasil. La propuesta de [30] plantea Cerberus para la renovación de credenciales y verificación de transcripciones o certificados que incluyen privacidad y divulgación selectiva de datos. Finalmente, si un estudiante requiere trasladarse de una institución a otra el método tradicional actual es altamente ineficiente, por ello el autor [4]

propone un modelo para compartir y administrar transcripciones en diferentes instituciones basado en la emisión y validación de los mismos.

En su mayoría de las soluciones detalladas anteriormente se identifican posibles problemas que limitan la propagación de Blockchain en el sector educativo [5]; la falta de una plataforma nacional de Blockchain, costos de mantenimiento para infraestructura, historial de accesos a todos los certificados, almacenamiento seguro de los documentos y una falta de una estructura de administración centralizada que coordine el Blockchain cómo único espacio de información digital.

En general, de todos los artículos analizados se ha identificado el siguiente procedimiento para la validación de los certificados [6]: primero, generar el archivo o documento digital, calcular el valor hash del documento digital y finalmente almacenar el valor hash en el bloque en el sistema de la cadena o blockchain. Este último punto, difiere totalmente y depende de la solución del autor, así de cómo almacenar el documento digital, las tecnologías usadas, las partes interesadas y el acuerdo de validación como el uso adicional de códigos QR.

Finalmente, apoyada literalmente los todos los artículos revisados, esta investigación propone tres enfoques principales para la validación de documentos en el Sistema Educativo Privado del Ecuador:

- Administración centralizada mediante el uso de la plataforma de Amazon Web Services, que se enfoca en la autenticación, autorización y seguridad de los documentos. Esta no será implementada, propuesta planteada a nivel de arquitectura.
- Ambiente seguro para el almacenamiento y acceso de los documentos digitales.
- Autenticidad de la emisión de los certificados académicos una vez aprobados, para avalar la aprobación de las dos partes involucradas.

2. METODOLOGÍA

En el presente capítulo se detalla el método de investigación utilizado para este estudio. Se describe la estructura general para el diseño de la propuesta a la problemática planteada basada en la propuesta de Pólya [12] para la solución de problemas, donde, se identifica las siguientes fases:

- Entendimiento del problema
- Creación de un plan.
- Ejecución del plan.
- Revisión de resultados.

La primera fase se logró a través de la revisión sistemática de la literatura ubicada en el capítulo uno para la obtención de la información necesaria sobre el área de conocimiento para este estudio. En esta fase es importante analizar técnicas, modelos y tecnologías previas enfocadas hacia la gestión de certificados académicos en el sector de la educación. Donde, basada en la pregunta de investigación, se analizó un total de doce artículos para obtener información relevante para la aportación de este trabajo, así como determinar sus posibles problemas. Finalmente, se analizó artículos relacionados al ámbito de computación en la nube para determinar la mejor opción para propuesta de un ambiente centralizado.

La fase de creación del plan correspondió con el proceso de creación de la propuesta guiada por los trabajos [4-6] y la norma ISO 15489, en donde se utilizó los lineamientos base que un sistema de gestión documental debe tener, así como Blockchain y contratos inteligentes para garantizar la integridad de la información, la precedencia de los documentos académicos y con el aporte del autor, para el diseño de una arquitectura orientada a la nube de AWS. En primera instancia, se establece los lineamientos base como los requisitos, responsabilidades, políticas, contexto o caso específico de partida y para su posible aplicabilidad en contexto de las IE privadas de la ciudad de Quito se realizó el diseño de una arquitectura basada en la nube. Por último, se definió una encuesta basada en la metodología GQM orientada a un grupo de interesados para validar la propuesta planteada.

La fase de ejecución del plan corresponde a la ejecución de la propuesta en un escenario de caso real, sin embargo, el alcance de este estudio no incluye una fase de pruebas experimentales. Por tanto, por ser un trabajo teórico, para sustentar su validez se realizó una encuesta basada en la metodología GQM orientada a un grupo de interesados para evaluar su opinión de la arquitectura propuesta en los atributos de seguridad, integridad y autenticidad. Donde se evidenció que esta propuesta tiene una buena tasa de aceptación tanto en los lineamientos propuestos como en la tecnología de Amazon Web Services usada. Debido a que esta tecnología proporciona alta seguridad y disponibilidad en sus servicios,

además de contribuir significativamente, con una posible implementación, a la solución de sus necesidades. Sin embargo, algunos de los comentarios de los participantes recalcaron que era necesario detallar el costo que implicaría implementar esta solución.

Para esto, se identificó las tres fases secuenciales de la metodología GQM [8]:

- Fase de preparación
  Identificar diferentes preocupaciones de las partes para traducirlas a objetivos:
  Un objetivo se divide en: propósito, objeto a medir y un problema a tratar.
  Crear un cuestionario para medir cada uno de los diferentes objetivos evaluadas por una métrica
- Fase de ejecución
  Ejecutar la encuesta.
- Fase de evaluación
  Interpretación de los resultados.

Por último, en la fase de revisión de resultados, se procedió con el análisis e interpretación de los resultados obtenidos en la encuesta realizada a las partes interesadas para evaluar el presente plan propuesto.

2.1. Propuesta del modelo

2.1.1. Identificación del contexto

Para el diseño se parte de una población de IE privadas del Ecuador, las cuales por lo general se encuentran distribuidas de la siguiente manera:

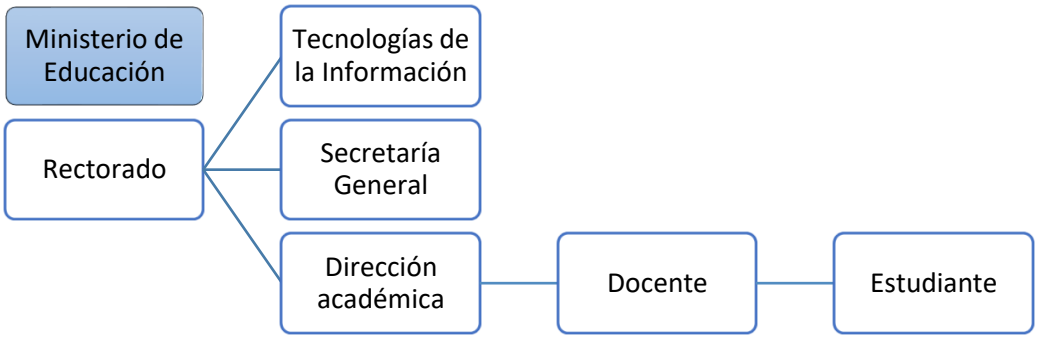


Figura 2: Estructura Institución Educativa

La máxima autoridad académica dentro de la IE es el Rectorado, quien es responsable de certificar o avalar que cualquier documento emitido por Secretaría General sea auténtico y valedero. Por otro lado, la autoridad gubernamental externa a la IE es la que gobierna y regula

las políticas y estatutos académicos. Finalmente, se hace referencia al área de TI de las IE, quienes son responsables de analizar y gestionar cualquier solución tecnológica referente a la misa.

Las IE año tras año llevan a cabo; procesos de emisiones de documentos académicos que detallan un resumen general de informes de desempeño escolar, comportamental e información estudiantil. Se identifica dos tipos; interna, sólo es necesario la intervención de la autoridad interna académica y conjunta, que es necesario la intervención de la autoridad académica y el ministerio de Educación.

2.1.2. Partes interesadas

Para esta propuesta se identifican las siguientes partes interesadas:

ID	Interesado	Descripción
I1	Técnico/ Ingeniero informático de la Institución Educativa	Responsable de analizar y gestionar soluciones informáticas que contribuyan al desarrollo de la IE.
I2	Padres de familia	Beneficiario del documento final.
I3	Secretario	A cargo de la elaboración y gestión de documentos académicos.
I4	Analista Distrital: Ministerio de Educación del Ecuador	A cargo de la acreditación de certificados ministeriales.

Tabla 12: Partes interesadas

Como se puede identificar en la Tabla 12, las necesidades de las partes I2, I3, I4 pueden ser cubiertas en su totalidad cuando se haya implementado la propuesta, es decir, son considerados como usuarios finales y por tanto, centrarse principalmente en el área de TI. Además, al tratarse de una solución informática en fase de diseño se excluyen los desarrolladores y testers, ya que no implica una solución de implementación.

En función de los interesados identificados se identifica sus principales necesidades.

Necesidad	I1	I2	I3	I4
Identificar soluciones informáticas innovadoras y seguras que contribuyan eficientemente en los procesos internos de gestión documental.	X			
Acceder rápida y fácilmente a los documentos académicos	X	X	X	X
Almacenar de forma segura los documentos.	X			
Agilizar el proceso de acreditación y gestión de documentos.	X		X	X

Tabla 13: Necesidades partes interesadas

2.1.3. Diseño de la propuesta

Siguiendo los lineamientos generales de la norma ISO 15489, desde el punto de vista técnico, se establece las siguientes etapas de un sistema de gestión documental académica inteligente SGDAI [27].

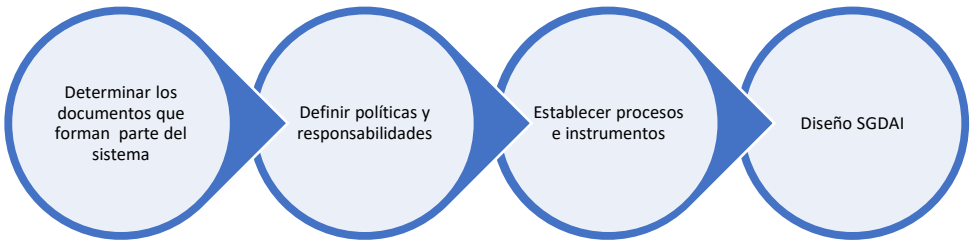


Figura 3: Lineamientos propuesta

- **Determinar los documentos académicos que forman parte del sistema**

Identificar los documentos académicos de la IE que implican una acción, responsabilidad o una evidencia de las actividades realizadas por un estudiante en un periodo escolar. Para ello, es necesario examinar los procesos, actividades y las operaciones que se llevan a cabo para determinar qué tipo de documentación se genera en cada caso.

Cada tipo de documento debería; estar producido por una actividad concreta, ser el resultado de un proceso, tener una estructura, un contenido informativo e identificarse claramente con un nombre.

Para este estudio se determinan los siguientes documentos académicos:

- Libretas o Reportes académicos de los distintos niveles.
- Certificados ministeriales.

- **Definir políticas y responsabilidades**

Establecer, documentar, mantener y distribuir una política de gestión de documentos académicos, con el fin de asegurar su información y evidencia. Estas políticas deben elaborarse a partir del análisis de las actividades académicas que involucran a todos los documentos determinados en el paso anterior de una IE. Así también, definir políticas de asignación de responsabilidades, clasificación, distribución, conservación y eliminación de documentos.

- **Establecer procesos e instrumentos**

Especificar los diferentes procesos que siguen los documentos desde el momento que son producidos hasta su destino final.

Procesos	Instrumentos
Carga o emisión de documento	Metadata
Control de acceso	Reglas de accesos y permisos
Clasificación e indización	Dominio de búsqueda (AWS S3)
Autorización / Aprobación / Verificación	Contratos inteligentes
Almacenamiento	

Tabla 14: Procesos e instrumentos

Carga documento

a) Identificar la necesidad de emitir un documento desde cualquier sistema informático.
b) Revisar el documento para determinar si efectivamente puede ser cargado en el sistema de gestión.
c) Definir un nombre claro para el documento.
d) Identificar la distribución del documento.
e) Cargar el documento, con la respectiva firma digital del creador.
f) Si aplica, notificar a los responsables de autorizar el documento para el proceso de firmas.

Aprobación

a) Con las autorizaciones de las partes interesadas, ubicar las respectivas firmas digitales.
b) Si no hay ninguna observación el documento es aprobado con todas sus firmas, caso contrario el mismo necesita ser revisado.

Almacenamiento

a) Almacenar los documentos en Amazon S3.
b) El documento podrá ser accedido cuando haya sido aprobado por todos los responsables asignados.
c) Cómo mecanismo de control y protección se puede acceder a los servicios adicionales de AWS S3 para respaldar la información y encriptado de los mismos.
d) Los documentos cargados, están limitados a solo lectura.

Control

a) Revisar constantemente los logs generados por Amazon, por parte de un técnico asignado, para le detección de posibles anomalías. Esto debe estar definido en una política.
b) Administrar en la consola de AWS las distribuciones e indización de los documentos.

Estructura Documento.

Estructura	Tipo documento	
	Libretas o Reportes	**Certificados ministeriales**
Cabecera: Información de la IE con sus respetivos logos.	X	X
Cabecera: Información del Distrito Educativo al cual pertenece la IE, con el logo ministerial.		X
Título documento	X	X
Información completa del estudiante con su respectivo curso	X	X
Detalle de calificaciones académicas y comportamentales de acuerdo con el periodo de interés.	X	X
Observaciones	X	X
Firmas	X	X
Pie de página	X	

Tabla 15: Estructura documento

Los tipos de documento no necesitan de algún tipo de código para su identificación, se identifican mediante el título.

- **Sistema de Gestión Documental Académica Inteligente**

  El diseño parte desde la carga o emisión de los certificados (en adelante se denominará documento), su elaboración no se encuentra considerado y se asume que los documentos se encuentran correctamente elaborados. Como siguiente se procede con la autorización del documento, en caso de que aplique, con la aplicación de las firmas digitales por parte de las entidades regulatorias internas y/o externas (Ministerio de Educación) y finalmente, con la verificación del documento.

Previo a la ejecución del flujo anterior, es requerido definir los controles de acceso e indización que tendrán los documentos. Para ello, se identifican los siguientes actores y redes involucradas:

- Secretaria: personal administrativo responsable de cargar o emitir el documento (red institución educativa).
- Rector: máxima autoridad de la IE (red institución educativa).
- Analista Distrital: entidad regulatoria del Ministerio de Educación responsable externo de autorizar el documento (red ministerio).
- Usuario: persona solicitante del documento.

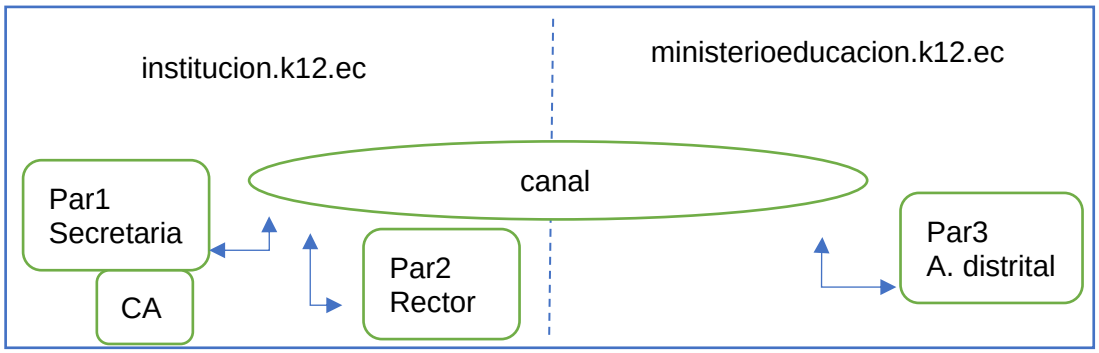


Figura 4: Red - actores

Así, la arquitectura propuesta aprovecha las siguientes características de la tecnología Hyperlegder Fabric:

- **Red transparente:** capacidad de crear canales privados entre los actores para permitir que cierta información fluya libre y transparentemente entre ellos. Es decir, el canal permitirá la comunicación entre las redes de la institución educativa y ministerio de educación establecidas.
- **Certificado digital de identificación única:** el certificado digital se incrustará con un hash de identificación única que es imposible de manipular. La información puede validarse simplemente haciendo coincidir el hash de los datos digitales presentes en la cadena de bloques.
- **Acceso autorizado:** los documentos cargados se pueden acceder por entidades autorizadas.

2.1.4. Protocolos propuestos

Para el proceso se establece los siguientes protocolos: carga del documento en blockchain y verificación del documento.

Protocolo para carga de documento en blockchain

Este protocolo se puede visualizar en la Figura 5, donde se identifica a la secretaria y entidades regulatorias (rector y analista distrital) como actores involucrados en el siguiente proceso:

1. Generar hash del documento: se proceder a codificar el documento usando SHA256 y obtener un código hash de longitud fija.
2. Generar certificado digital: utilizando el algoritmo asimétrico para generar el certificado digital del hash obtenido utilizando la clave privada de la institución educativa.
3. Generar metadatos: corresponde a la creación de un JSON que contendrá la información del documento como; certificado digital, nombre y estado del documento, propietario, marca de tiempo, lista de las respectivas claves públicas de las entidades regulatorias encargadas de autorizar el documento y lista de claves públicas de entidades que hayan autorizado el documento.
4. Cargar documento en blockchain usando contratos inteligentes: posterior a la generación de los metadatos del documento y para garantizar la transparencia en el proceso, se necesita un acuerdo contractual entre las entidades regulatorias. Por tanto, se invocará al contrato denominado *carga*, responsable de guardar los metadatos del documento en blockchain, así como validar que todas las entidades regulatorias detalladas en la lista de claves públicas de los metadatos hayan firmado el documento y, por último, almacenar externamente el documento digital que para esta propuesta se lo realiza en Amazon S3.

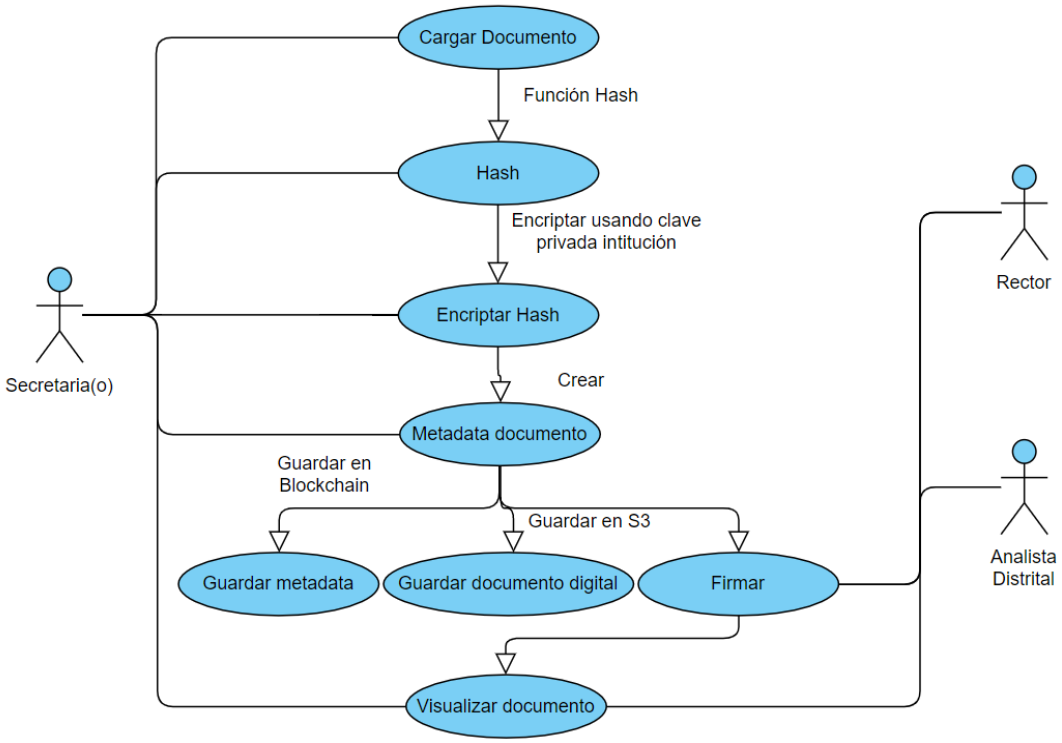


Figura 5: Diagrama caso de uso - Carga documento

Protocolo para verificar el documento en blockchain

Este protocolo se puede visualizar en la Figura 6, donde los actores involucrados son usuario y/o secretaria donde se permite verificar que un documento fue emitido por quien dice haberlo realizado y que su contenido no ha sido alterado, manteniendo así su integridad.

1. Escanear código de barras.
2. Decodificar el código de barras del documento: el código de barras consiste en una clave pública y una clave única utilizada para obtener metadatos (el valor hash firmado) relacionado al documento del blockchain.
3. Validar el hash con el del documento original recuperado del blockchain.

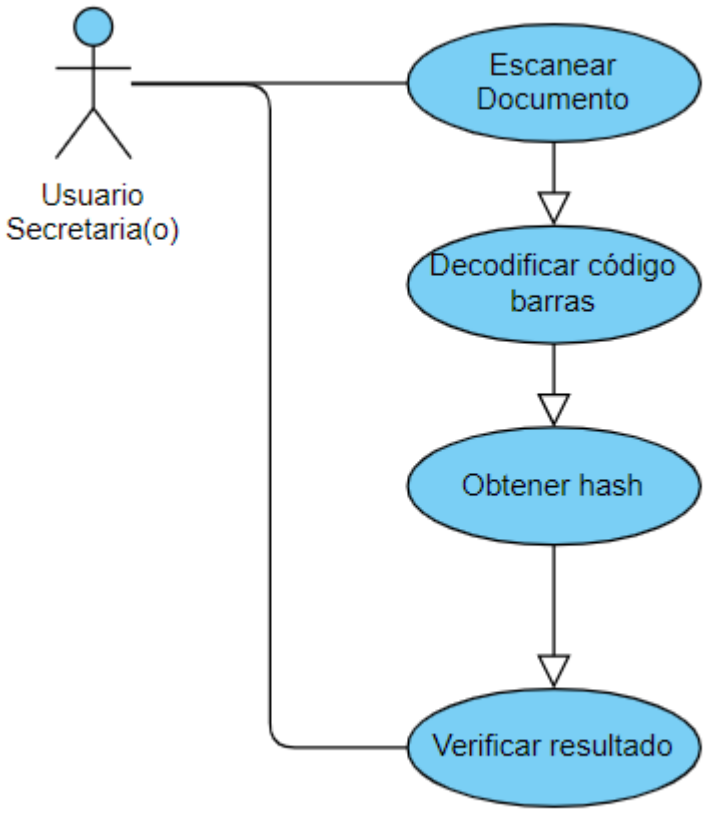


Figura 6: Diagrama caso de uso - Verificar documento

2.1.5. Arquitectura en la nube

La propuesta se basa en el servicio de Amazon Web Services, la cual provee grandes beneficios de seguridad de administración de cuentas y servicios, permitiendo una administración centralizada de servicios.

Los servicios utilizados son:

- Amazon EC2: para la implementación de los servicios del sistema de gestión académica.
- Amazon S3: para el almacenamiento de los documentos digitales
- Amazon Managed Blochchain: para la gestión de la red de Blockchain, la cual integra HyperLedger Fabric para el ledger, contratos inteligentes y CouchDB para una base de datos de estado para mantener el último registro de un bloque.

- Amazon QLDB: base de datos basada en blockchain para mantener un registro inmutable de la red.
- Amazon Secrets Manager: para la gestión segura de credenciales de acceso.

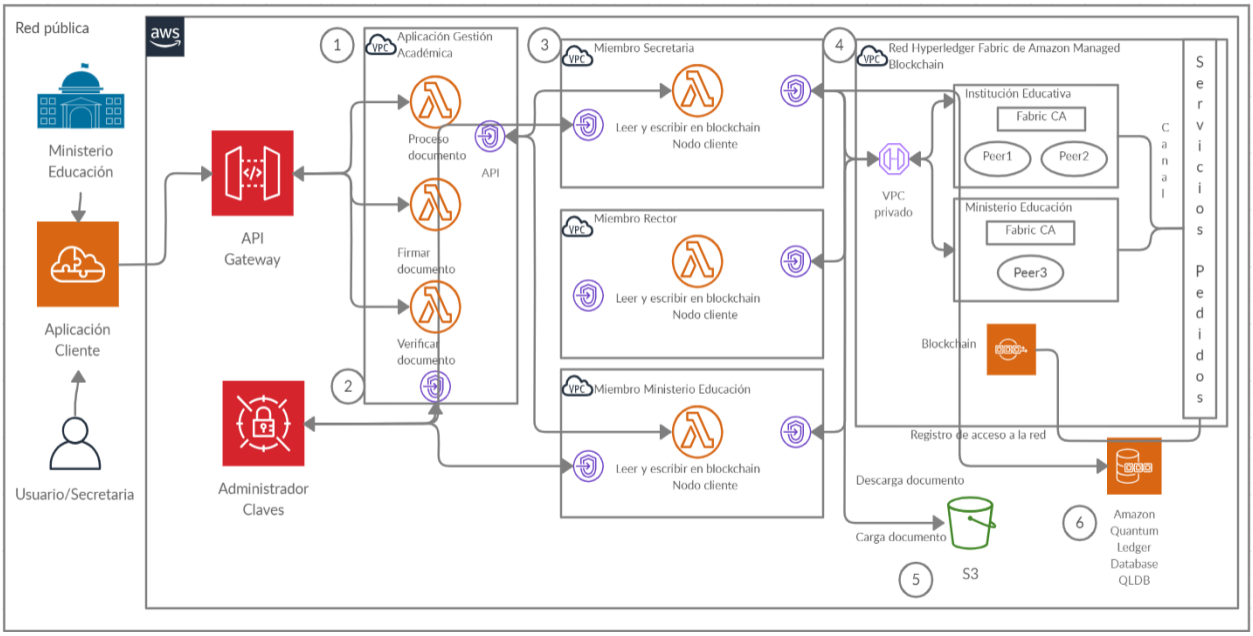


Figura 7: Diagrama de arquitectura (elaborado por el autor)

La Figura 7 representa la arquitectura global de la solución, donde, los usuarios interactúan atreves de un sitio web (client application) hacia la puerta de enlace (API Gateway) para proporcionar rutas API a la aplicación e invocar a funcionalidades de servicios de backend o funciones Lambda, gestionando todas las tareas implicadas. Las funciones Lambda (1) obtienen credenciales de los servicios API de Secrets Manager (2). Y, se dispone de tres servicios: carga, autorización y verificación de un documento, donde carga y verificación invocan a la ejecución de contratos inteligentes para lo cual, los nodos clientes (3) son responsables de comunicarse con la red blockchain, donde, toda la comunicación a la red es a través del nodo cliente y se utiliza AWS privatelink para garantizar que sólo miembros de la red puedan acceder a los recursos necesarios. De esta manera cada miembro tiene una conexión privada de un cliente en su VPC a la red Managed Blockchain.

Por otro lado, para el almacenamiento de los documentos se utiliza Amazon S3 (5) como almacenamiento fuera de Blockchain, mientras que los metadatos de los documentos que pueden acceder a los datos del archivo se mantienen en el Blockchain. Donde, para almacenar los documentos, se utiliza el mecanismo de observación de eventos de un contrato inteligente.

Por último, la red Hyperledger administrada por Amazon Managed Blockchain (4) a pesar de tener muchos componentes como; libro mayor (estado mundial + registro de transacciones) y contratos inteligentes, no se detallan en el diagrama de arquitectura. Además, gracias a Managed Blockchain se puede replicar una copia inmutable de su actividad de red a Amazon Quatum Ledger Database (6), una base de datos de libro mayor completamente administrada, permitiendo analizar fácilmente la actividad de la red y obtener información acerca de las tendencias. Finalmente, se identifica Hyperledger Fabric CA como autoridad de certificación (CA) para Hyperledger Fabric.

Contratos inteligentes

Se identifican los contratos inteligentes para la ejecución automática de eventos de acuerdos contractuales establecidos entre las partes. Para ello, se establecen los siguientes contratos en el chaincode de Hyperledger: ContratoCarga y ContratoVerificar.

ContratoCarga: permite cargar y firmar el documento, donde, posterior a su autorización se registra en Amazon S3 y su metadata en Blockchain. A continuación, en la Tabla 8 se establece el flujo del proceso con el cual se interactúa con el contrato inteligente a fin.

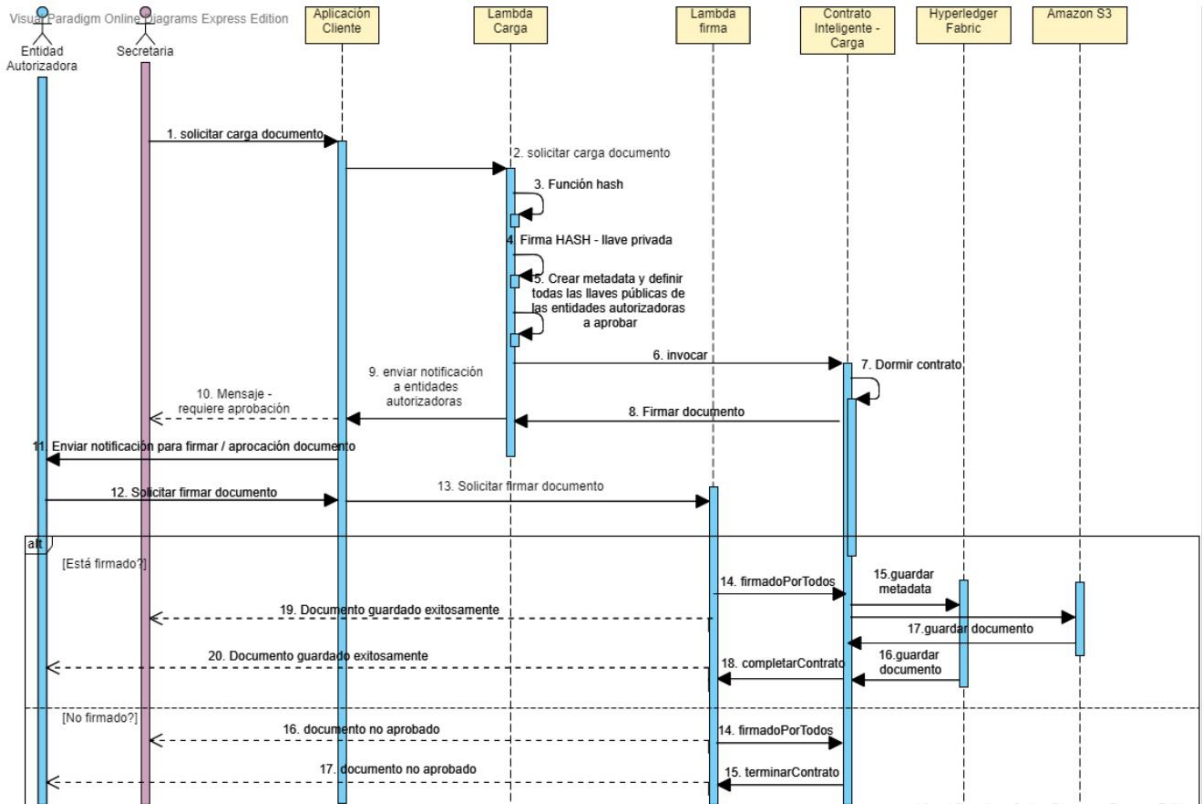


Figura 8: Diagrama de secuencia – Carga del autor (elaborado por el autor)

Estructura del contrato

La Tabla 16 describe la esquematización del contrato inteligente de la propuesta referente al contrato *Carga*.

Parámetros Entrada	Parámetros Salida	Funciones
- Llave pública del solicitante - nombre documento - hash documento - propietario - timestamp - arreglo llaves públicas de entidades autorizadoras - estado	- mensaje	- checkPermission: verifica si el usuario tiene permiso para publicar. - sendNotification: envía un mensaje - generateNotificationToAuthority: mensaje para solicitar a una entidad que firmen el documento - waitContract: pone en espera al contrato inteligente durante un tiempo específico. - signedByAll: verifica si todas las entidades especificadas en el arreglo de llaves públicas hayan firmado. - publishDataOnBlockChain: función API que guarda la metadata en blokchain de Hyperledger - saveDataOnS3: función API que guarda el documento en Amazon S3 - completeContract: completa el contrato - terminateContract: termina el contrato

Tabla 16: Estructura contrato inteligente - Carga

ContratoVerificar: permite validar el hash de un documento.

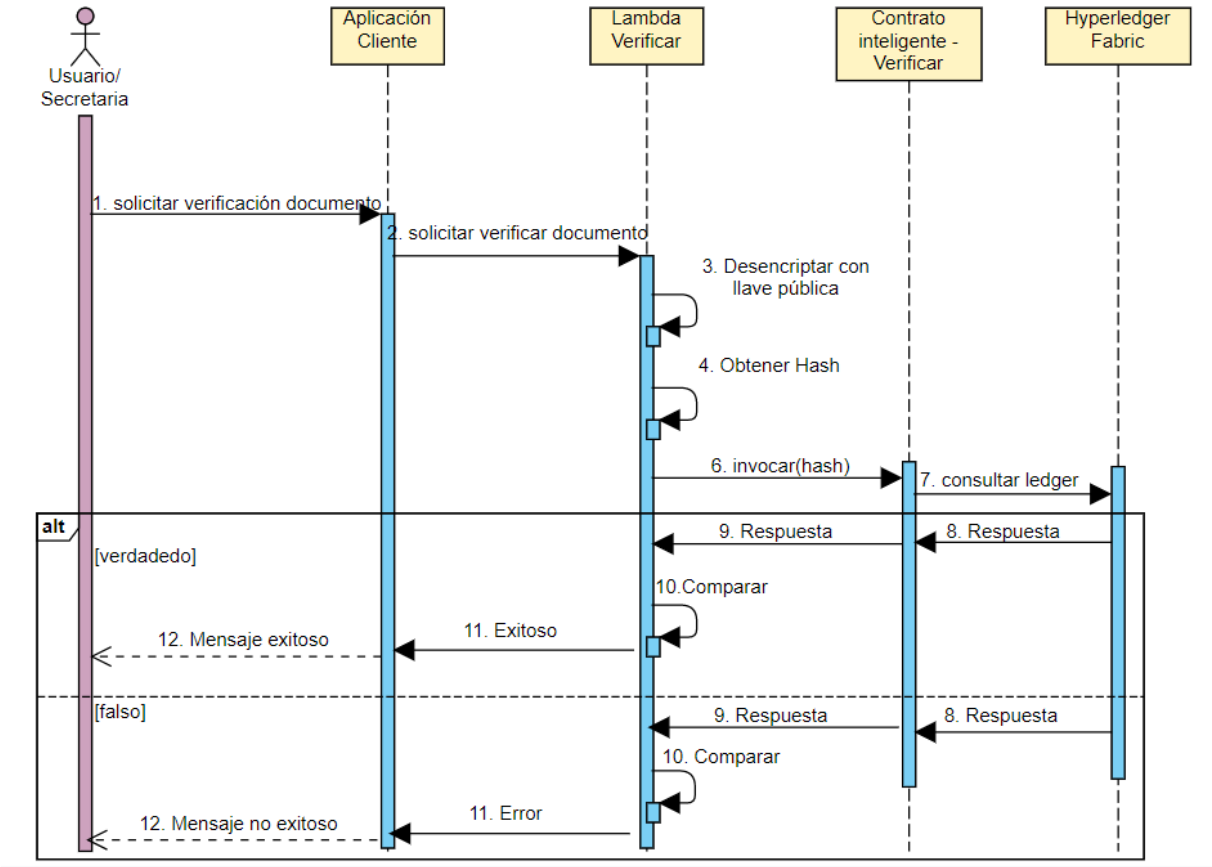


Figura 9: Diagrama de secuencia – Verificar (elaborado por el autor)

Estructura del contrato

Parámetros Entrada	Parámetros Salida	Funciones
- documento digital - llave pública del solicitante	- Documento validado o no validado	- getBlock: función API que devuelve un bloque - completeContract

Tabla 17: Estructura contrato inteligente - Verificar

2.2. Evaluación

La evaluación del modelo propuesto se realizó mediante una encuesta basada en la metodología GQM orientada al grupo de interés del área técnica de las IE. Además, s importante recalcar que esta evaluación no tiene como objetivo obtener información

sobre la implementación de esta propuesta, ya que este se encuentra fuera del alcance de este estudio. Por esta razón, se propone un cuestionario simple para recopilar la opinión de los interesados, así, se proporcionó un resumen como guía del modelo basado en este trabajo expresado a través de una terminología técnica junto con el cuestionario para ayudar a los participantes a comprender y evaluar este proyecto. El proceso de la encuesta consta de tres fases: preparación, ejecución y evaluación.

2.2.1. Preparación

En esta fase, se creó un cuestionario utilizando la metodología GQM descrito anteriormente. Donde, todos los objetivos se enfocaron en las partes interesadas, sin embargo, la encuesta se realizó al personal de TI de las IE, ya que son los responsables de implementar y analizar cualquier solución tecnológica. Por otro lado, las partes interesadas restantes, son usuarios que en cierta parte son beneficiados de la aplicación correcta de esta propuesta para un caso de estudio específico. La Tabla 18 muestra el mapeo de un objetivo de GQM.

Necesidad	**Objetivos**	**Interesados**
Identificar soluciones informáticas innovadoras y seguras que contribuyan eficientemente en los procesos internos de gestión documental.	**Propósito:** Identificar	Persona TI
	Objeto a medir: Software	
	Problema: falta de conocimiento de las tecnologías informáticas	
Acceder rápida y fácilmente a los documentos académicos	**Propósito:** Acceder	Persona TI Padres de familia Secretario Analista distrital
	Objeto a medir: Disponibilidad	
	Problema:	
Almacenar de forma segura los documentos.	**Propósito:** Almacenar	Persona TI
	Objeto a medir: Seguridad	
	Problema:	
	Propósito: Agilizar	

Agilizar el proceso de acreditación y gestión de documentos.	**Objeto a medir:** Procesos	Persona TI Secretario Analista distrital
	Problema: Procesos mal definidos	

Tabla 18: Objetivos GQM

Definición de métricas

Se utilizaron las siguientes métricas (Tabla 19) para evaluar las preguntas planteadas:

Métrica	**Descripción**
Respuesta abierta	Respuesta descriptiva con respecto a un tema en específico.
Respuesta dicotómica	Opción directa de SI o NO.
Calificación	Escala: Muy bueno Bueno Regular Malo

Tabla 19: Métricas

Definición de preguntas

En función de los objetivos definidos en la Tabla 18, se plantearon las siguientes preguntas para cumplir con los objetivos y poder determinar qué posibles mejoras podría agregarse en un futuro. Con las métricas propuestas, la encuesta contribuyó con resultados cualitativos y cuantitativos que permitió la recopilación de opiniones sobre mejoras y métricas de seguridad. Todas las preguntas fueron establecidas con sus respectivas métricas para su posterior análisis en la fase de evaluación de acuerdo con la metodología GQM.

Objetivo	**Pregunta**	**Métrica**
Identificar soluciones informáticas innovadoras y seguras que contribuyan eficientemente en los procesos internos de gestión documental.	¿Considera usted que el modelo propuesto utiliza herramientas tecnológicas seguras e innovadoras?	Respuesta dicotómica
	¿Considera que los contratos inteligentes son	Respuesta dicotómica

	seguros para un sistema de gestión?	
	De modo general, ¿cómo evalúa esta propuesta?	Calificación
Acceder rápida y fácilmente a los documentos académicos	¿Considera usted que el modelo propuesto, facilita el acceso de los documentos?	Respuesta dicotómica
Almacenar de forma segura los documentos.	¿Considera que la tecnología de Amazon Web Services es seguro y confiable?	Respuesta dicotómica
Agilizar el proceso de acreditación y gestión de documentos.	¿Considera usted que el modelo propuesto, facilita en la carga y organización de los documentos?	Respuesta dicotómica
	¿Considera usted que el modelo propuesto, facilita al proceso de aprobación de documentos mediante los contratos inteligentes?	Respuesta dicotómica
	¿Considera usted que el modelo propuesto le facilita lineamientos para una implementación?	Respuesta dicotómica
Pregunta general	Si usted desea expresar algún otro criterio sobre el modelo propuesto, puede ingresarlo aquí	Respuesta abierta

Tabla 20: Cuestionario de evaluación

Aparte de este cuestionario se adicionó preguntas para recopilar información demográfica para determinar ciertas características de los encuestados.

Información	Métrica
Edad	Respuesta abierta
Nivel de educación	Pregunta de selección: - Secundario - Tercer nivel - Cuarto nivel
¿Tiene usted experiencia en gestión documental?	N/A
¿Tiene usted experiencia en Amazon Web Service?	N/A
¿Tiene usted conocimiento sobre la tecnología Blockchain?	N/A

Tabla 21: Información demográfica

2.2.2. Ejecución

El cuestionario fue cargado como una encuesta en línea, donde se envió el enlace a los participantes durante tres días. A continuación, se hace referencia a la encuesta realizada en el Anexo I.

Formulario	Referencia
Encuesta de evaluación de la propuesta de modelo de gestión documental académica inteligente (SGDAI)	Anexo I

Tabla 22: Referencia encuesta

2.2.3. Evaluación

Basada en el trabajo realizado por Nielsen [35], quién afirma que cinco es un tamaño de muestra más que suficiente como práctica estándar para estudios de usabilidad ya que a partir de este número, los resultados comienzan a mostrar los mismos resultados. Por tanto, se envió el formulario a un total de 10 personas pertenecientes al área de TI de 5 Instituciones Educativas y se obtuvo la colaboración de 7 personas.

Información demográfica

Edad

31	**1**
33	**1**
35	**2**
38	**1**
40	**1**
45	**1**

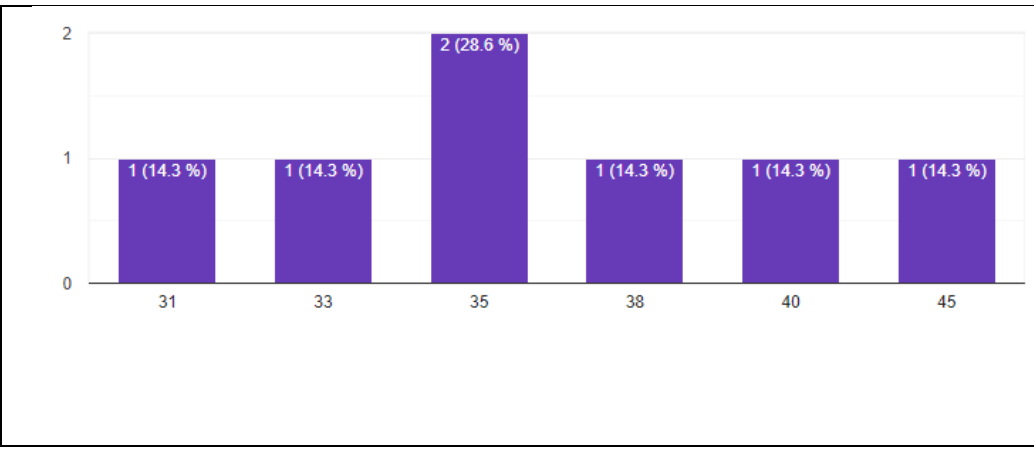


Figura 10: Información demográfica

Nivel de educación

Bachillerato		
Tercer nivel	**7**	
Cuarto nivel		

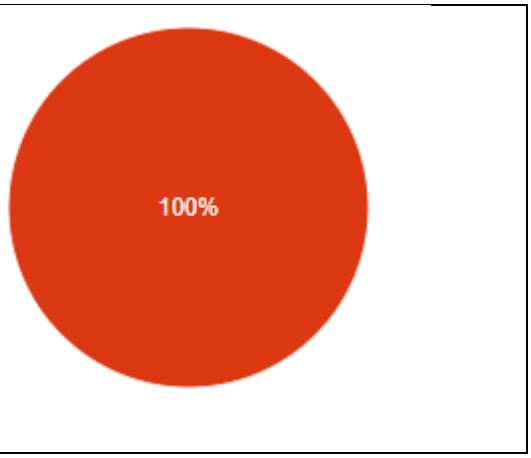


Figura 11: Nivel de educación

¿Tiene usted experiencia en gestión documental?

SI	**6**	
NO	**1**	

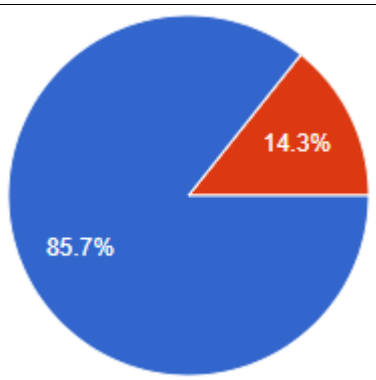


Figura 12: Resultado - Pregunta 1

¿Tiene usted experiencia en Amazon Web Services?

SI	**5**	
NO	**2**	

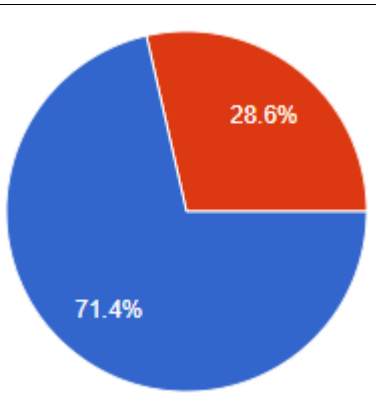


Figura 13: Resultado - Pregunta 2

¿Tiene usted conocimiento sobre la tecnología Blockchain?

SI	**4**	
NO	**3**	

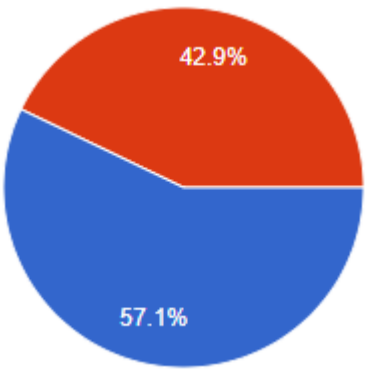


Figura 14: Resultado - Pregunta 3

¿Considera usted que el modelo propuesto utiliza herramientas tecnológicas seguras e innovadoras?

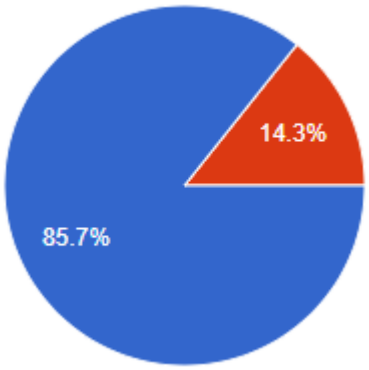
SI	**6**		
NO	**1**		

Figura 15: Resultado - Pregunta 4

¿Considera que los contratos inteligentes son seguros para un sistema de gestión?

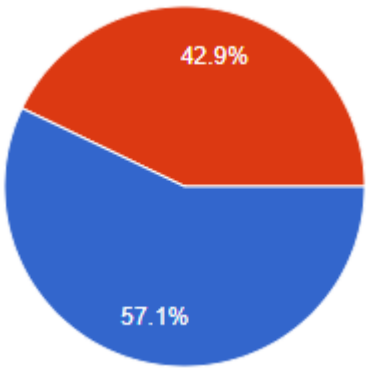
SI	**4**		
NO	**3**		

Figura 16: Resultado - Pregunta 6

¿Considera usted que el modelo propuesto, facilita al acceso de los documentos?

SI	**7**		

NO	0		

Figura 17: Resultado - Pregunta 7

¿Considera que la tecnología de Amazon Web Services es seguro y confiable?

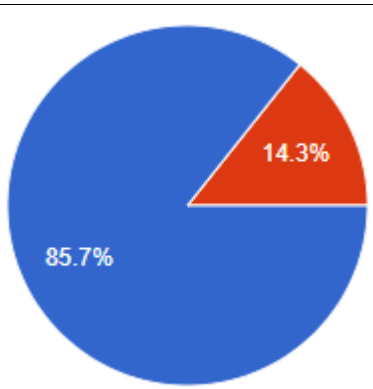
SI	7		
NO	0		

Figura 18: Resultado - Pregunta 8

¿Considera usted que el modelo propuesto, facilita en la carga y organización de los documentos?

SI	7		
NO	0		

Figura 19: Resultado - Pregunta 9

¿Considera usted que el modelo propuesto, facilita al proceso de aprobación de documentos mediante los contratos inteligentes?

SI	**6**	
NO	**1**	

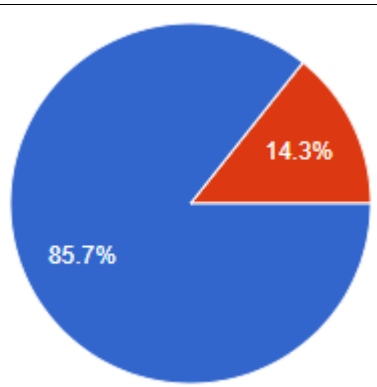


Figura 20: Resultado - Pregunta 10

¿Considera usted que el modelo propuesto le facilita lineamientos para una implementación?

SI	**3**	
NO	**4**	

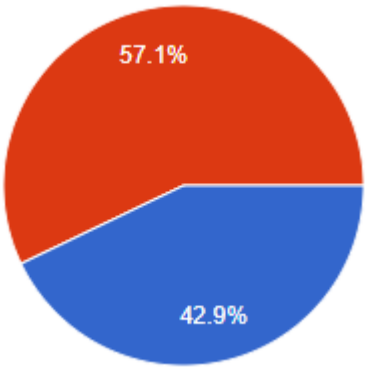


Figura 21: Resultado - Pregunta 11

De modo general, ¿cómo evalúa esta propuesta?

Muy bueno	**2**	
Bueno	**5**	
Regular		

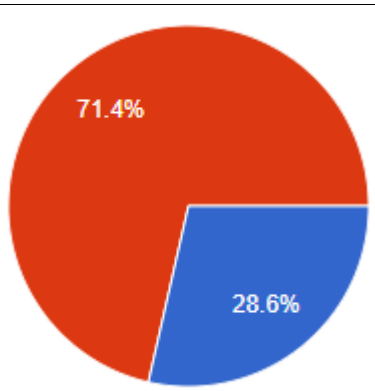
Malo			

Figura 22: Resultado - Pregunta 12

Si usted desea expresar algún otro criterio sobre el modelo propuesto, puede ingresarlo aquí

Me parece muy interesante la solución, sin embargo estas decisiones no dependen al 100% del área de TI para una futura implementación, si no que también de la alta gerencia por el tema de costos

Hubiese sido bueno que el modelo presente detalle de costos

Es necesario evaluar la política de privacidad de los datos almacenados en la nube

Figura 23: Resultado - Pregunta 13

Análisis de resultados

Los resultados de la información demográfica muestran que la edad promedio de los participantes se encuentra entre 30 y 40 años, con un nivel de educación de tercer nivel. Los mismos que aseguran tener experiencia en gestión documental y en las tecnologías planteadas, lo que beneficia el entendimiento de esta propuesta. Con esto, se puede asegurar que sus comentarios se basan en la experiencia y el conocimiento profesional.

Por otro lado, se evidenció que esta propuesta tiene una aceptación considerable tanto en los lineamientos propuestos, así como en la tecnología de Amazon Web Service, aseguran también que este proporciona seguridad en el almacenamiento de sus documentos. Además, para una posible implementación, esta contribuye significativamente a la solución de sus necesidades. Sin embargo, algunos de los comentarios de los participantes recalcaron que era necesario detallar el costo que implicaría implementar esta solución.

3. DISCUSIÓN

Como principal objetivo, se presenta la propuesta de un sistema de gestión académica inteligente basado en Blockchain, donde, se ha podido plantear y obtener como resultado los lineamientos a considerar para su posible implementación. Esto será de mucha ayuda para el manejo de los documentos académicos en una Institución Educativa (IE) privada. Para ello, se identificó la situación en la que se encuentran las IE en la gestión documental académica, cómo contribuiría este modelo en el apoyo de la gestión de los documentos y sobre todo cómo garantiza su integridad, seguridad y autenticidad.

En la propuesta se considera el proceso a seguir de un documento, desde su emisión hasta su almacenamiento en los recursos de la nube. Donde, la Norma ISO 15489 proporciona los principios y características que un sistema de gestión de documentos debe tener, los cuales deben ser fiables y utilizables de acuerdo con las necesidades de la parte interesada. Por tanto, la contribución de esta propuesta se enfoca principalmente en los lineamientos operativos de los procesos de gestión documental, definición de políticas y responsabilidades, partiendo desde la decisión de cuando obtener un documento y cuando cargarlo en el sistema documental. Y, así mantenerlos almacenados sin posibilidad de cambio, permitiendo el acceso al personal o usuario autorizado, garantizando que los mismos se encuentren almacenados en un lugar seguro y sin posibilidad de cambio mediante la aplicabilidad de blockchain.

Las técnicas que aportan en esta solución son: el cifrado de clave pública y privada que aportan en la autenticidad de los documentos, para ello es necesario que los actores involucrados en el proceso de aprobación de los documentos (contratos) cuenten con sus respectivas llaves, y la función hash que genera un número fijo que garantiza que un documento no pueda ser modificado. Por otro lado, la arquitectura de AWS parte de la creación de redes internas para la correcta administración, accesibilidad y seguridad de los usuarios e identificación de recursos, permitiendo revisar posibles anomalías en base a los logs de accesos, también provee el recurso en donde se almacenará físicamente los documentos que permite controlar sus accesos públicos y privados. Además, es necesario considerar que AWS posee grandes aplicaciones e integraciones de soluciones tecnológicas y una de ellas es Hyperledger Fabric que es el indicado para manejar contratos inteligentes. Finalmente, los contratos inteligentes ayudan significativamente en el proceso de aprobación de documentos ministeriales, garantizando su ejecución entre las partes o actores identificados mediante las respetivas llaves públicas.

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Lastimosamente la mayoría de los procesos internos de gestión documental socavan la eficiencia en las instituciones educativas, afectando su desarrollo y especialmente los costos económicos significativos que estos conllevan. Además, el proceso de aprobación o acreditación de los documentos heredados requieren de mucho tiempo y son engorrosos. Por tanto, en este trabajo se identificó los temas de seguridad requeridos para el proceso de aprobación de documentos basado en blockchain y Hyperledger Fabric, permitiendo mejorar los procesos y los documentos en términos de autenticación, autorización. Adicionalmente la usabilidad y eficiencia con una posible implementación en AWS.
- La tecnología AWS proporciona un sin número de herramientas que benefician en gran medida al desempeño de las organizaciones, es por ello que esta propuesta se recurre a esta tecnología ya que beneficia en gran medida el diseño fácil y rápido de la construcción de las redes internas y gestión de claves de las aplicaciones. Esto permite que sea aplicable para cualquier Institución Educativa privada del grupo k12 que desee invertir, acorde a sus necesidades, en una arquitectura en la nube para mejorar su organización documental, principalmente ahora que nos encontramos en la pandemia del Covid-19.
- La solución plantada tiene gran aceptación por las partes involucradas en este trabajo, sin embargo, en cuanto a los costos se plantea comparar la implementación de esta solución con la emisión de los documentos académicos. Por tanto, se espera que los lineamientos detallados como solución contribuyan positivamente a los esfuerzos en curso.

4.2 Recomendaciones

- Se recomienda su futura aplicabilidad en una Institución Educativa, ya que mejorará notablemente su organización documental, brindando agilidad y seguridad en los mismos. Así como también, permitirá mantener una constante comunicación entre las partes operativas y técnicas para determinar posibles mejoras. Para ello, es necesario impartir una cultura en el uso de las tecnologías, por tanto, se recomienda contar con profesionales que posean conocimiento en las tecnologías AWS planteadas en esta solución.
- La solución del diseño de la arquitectura se enfoca en una Institución Educativa privada, donde, el ente regulador (Ministerio de Educación) es quién deberá tener acceso. Por tanto, se recomienda que en un futuro esta solución parta desde el ente regulador para que este sea quién provea acceso a las diferentes instituciones educativas del grupo ministerial correspondiente, es decir, por cada institución educativa deberá crearse una red con su respectivo canal de AWS.

REFERENCIAS BIBLIOGRÁFICAS

[1] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts SoK," presented at the Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204, 2017.

[2] "Ministerio de Educación del Ecuador, Instructivo: Informe Técnico para la fusión de Instituciones Educativas." https://educacion.gob.ec/wp-content/uploads/downloads/2017/03/instructivo_para_la_aplicacion_de_la_evaluacion_estudiantil_febrero-2017-1.pdf (accessed Nov 01,2018).

[3] "Ministerio de Educación del Ecuador, Trámite requisitos procedimiento - Ministerio de Educación." https://educacion.gob.ec/wp-content/uploads/downloads/2014/04/matriz_tramites_proceso_de_atencion_ciudadana.pdf (accessed Nov 01,2018).

[4] K. Patel and M. Das, "Transcript Management Using Blockchain Enabled Smart Contracts," 2019, pp. 392-407.

[5] T. M. Shamsutdinova, *Application of the blockchain technology for digital diplomas: problems and prospects*. 2019, pp. 51-58.

[6] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," *2018 IEEE International Conference on Applied System Invention (ICASI),* pp. 1046-1051, 2018.

[7] T. Kanan, A. T. Obaidat, and M. Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 9-11 April 2019 2019, pp. 629-633, doi: 10.1109/JEEIT.2019.8717505.

[8] R. Solingen and E. Berghout, *The Goal/Question/Metric Method: A Practical Guide for Quality Improvement of Software Development*. 1999.

[9] T. Thua Huynh, T. Tru Huynh, D. Khoa Pham, and A. Khoa Ngo, *Issuing and Verifying Digital Certificates with Blockchain*. 2018, pp. 332-336.

[10] S. Mthethwa, N. Dlamini, and G. Barbour, *Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents*. 2018, pp. 1-5.

[11] B. Kitchenham, "*Systematic review in software engineering: Where we are and where we should be going*," ed: ACM, 2012.

[12] G. Polya, "A Problem Solving Approach to Mathematics for Elementary School Teachers," ed: Benjamin/Cummings Publishing Co., 1945.

[13] Y. Chen, Y. Zhang, and B. Zhou, "Research on the risk of block chain technology in

Internet finance supported by wireless network," *EURASIP Journal on Wireless Communications and Networking,* vol. 2020, no. 1, p. 71, 2020/03/30 2020, doi: 10.1186/s13638-020-01685-6.

[14] H. K. An, "Design of the new efficient decripting machine, that can be applied to the wireless sensor network, based on the GF(2n) field theory and the modified RSA algorithm," *International Journal of Security and its Applications,* Article vol. 8, no. 2, pp. 353-362, 2014, doi: 10.14257/ijsia.2014.8.2.36.

[15] T. P. Adewumi and M. Liwicki, "Inner For-Loop for Speeding up Blockchain Mining," *Open Computer Science,* Article vol. 10, no. 1, pp. 42-47, 2020, doi: 10.1515/comp-2020-0004.

[16] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009.

[17] T. Das, "BLOCKCHAIN TECHNOLOGY," vol. 1, 10/29 2018.

[18] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, *On Security Analysis of Proof-of-Elapsed-Time (PoET)*. 2017, pp. 282-297.

[19] O. Saleh, O. Ghazali, and M. E. Rana, "Blockchain Based Framework for Educational Certificates Verification," vol. 7, pp. 79-84, 03/20 2020, doi: 10.31838/jcr.07.03.13.

[20] T. Arndt and A. Guercio, "Blockchain-Based Transcripts for Mobile Higher-Education," *International Journal of Information and Education Technology,* vol. 10, pp. 84-89, 01/01 2020, doi: 10.18178/ijiet.2020.10.2.1344.

[21] K. Toyoda, K. Machi, Y. Ohtake, and A. N. Zhang, "Function-Level Bottleneck Analysis of Private Proof-of-Authority Ethereum Blockchain," *IEEE Access,* vol. 8, pp. 141611-141621, 2020, doi: 10.1109/ACCESS.2020.3011876.

[22] P. N, P. M, and R. Aantonny, *An Efficient System Framework for Managing Identity in Educational System based on Blockchain Technology*. 2020, pp. 1-5.

[23] Hyperledger. "A Blockchain Platform for the Enterprise." https://hyperledger-fabric.readthedocs.io/en/release-2.0/ (accessed.

[24] AWS. "AWS Secrets Manager." https://aws.amazon.com/es/secrets-manager/ (accessed.

[25] AWS. "Amazon Quantum Ledger Database (QLDB)." https://aws.amazon.com/es/qldb/ (accessed.

[26] AWS. "Amazon Managed Blockchain." https://aws.amazon.com/es/managed-blockchain/ (accessed.

[27] ACIMED. "INFORMACION Y DOCUMENTACION. GESTIÓN DE DOCUMENTOS." https://www.uma.es/media/tinyimages/file/ISO_15489.2.pdf (accessed 2020).

[28] M. d. Educación. "Indicadores Educativos."

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjyxpeUtpjqAhWnTd8KHc4dAfMQFjAAegQIARAB&url=https%3A%2F%2Feducacion.gob.ec%2Fwp-content%2Fuploads%2Fdownloads%2F2013%2F10%2FIndicadores_Educativos_10-2013_DNAIE.pdf&usg=AOvVaw1LbdTyu8dsLSecy8Vb0_Qs (accessed 2020).

[29] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," *Inf. Softw. Technol.,* vol. 51, no. 1, pp. 7-15, 2009, doi: 10.1016/j.infsof.2008.09.009.

[30] A. Tariq, H. Haq, and S. Ali, *Cerberus: A Blockchain-Based Accreditation and Degree Verification System*. 2019.

[31] L. M. Palma, M. Vigil, and F. L. Pereira, *Blockchain and smart contracts for higher education registry in Brazil*. 2019, p. e2061.

[32] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, "The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling: BIS 2018 International Workshops, Berlin, Germany, July 18–20, 2018, Revised Papers," 2019, pp. 185-196.

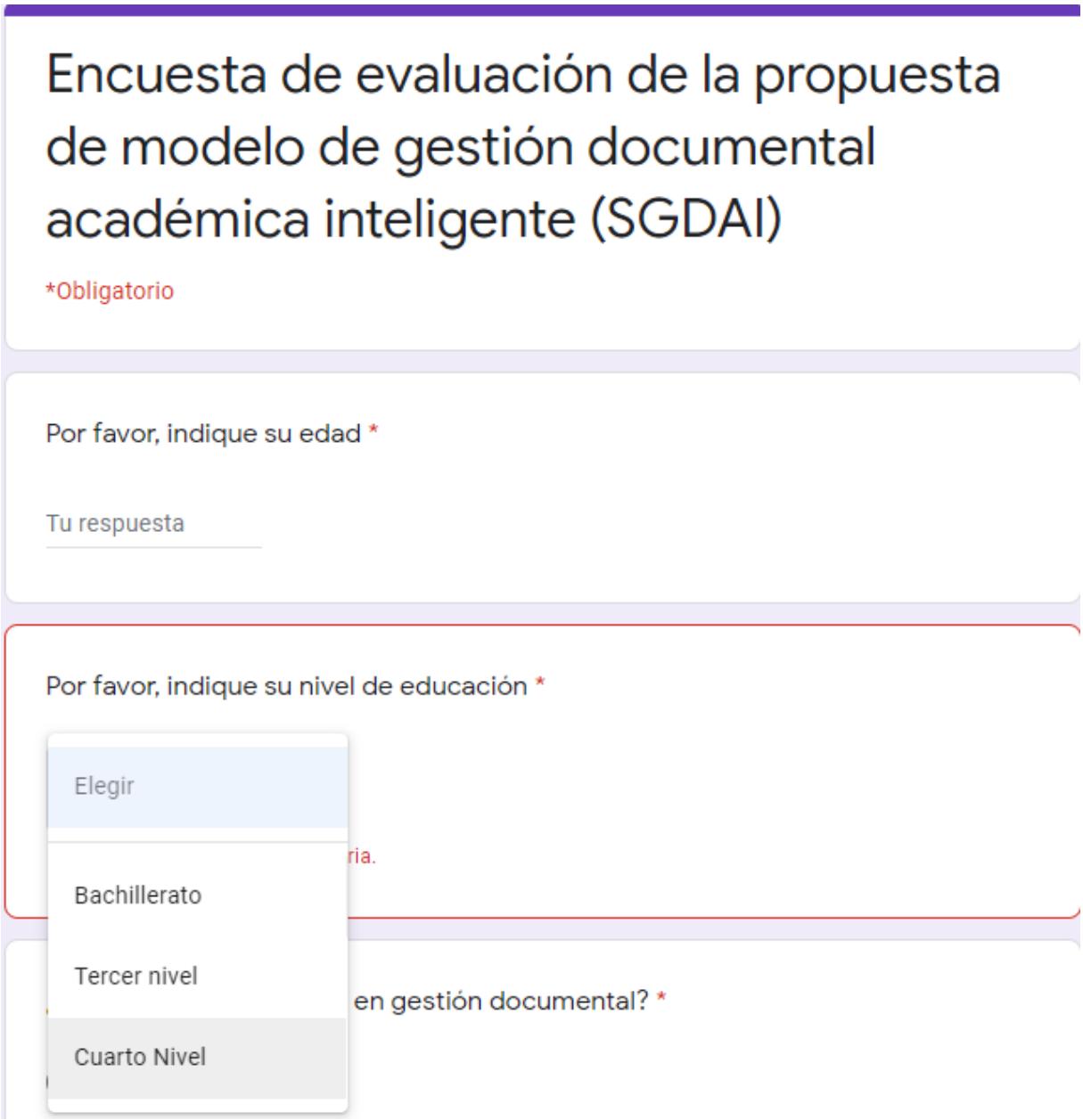
[33] S. Gilda and M. Mehrotra, *Blockchain for Student Data Privacy and Consent*. 2018, pp. 1-5.

[34] R. Arenas and P. Fernandez, "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials," in *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, 17-20 June 2018 2018, pp. 1-6, doi: 10.1109/ICE.2018.8436324.

[35] J. Nielsen. "Why You Only Need to Test With 5 Users." http://www.useit.com/alertbox/20000319.html (accessed 2020).

ANEXOS

Anexo I


Encuesta de evaluación de la propuesta de modelo de gestión documental académica inteligente (SGDAI)
*Obligatorio
Por favor, indique su edad *
Tu respuesta
Por favor, indique su nivel de educación *
Elegir
Bachillerato
Tercer nivel
Cuarto Nivel
en gestión documental? *

¿Tiene usted experiencia en gestión documental? *

- ○ Sí
- ○ No

¿Tiene usted experiencia en Amazon Web Service? *

- ○ Sí
- ○ No

¿Tiene usted conocimiento sobre la tecnología Blockchain? *

- ○ Sí
- ○ No

¿Considera usted que el modelo propuesto utiliza herramientas tecnológicas seguras e innovadoras? *

- ○ Sí
- ○ No

¿Considera que los contratos inteligentes son seguros para un sistema de gestión? *

- ◯ Sí
- ◯ No

¿Considera usted que el modelo propuesto, facilita al acceso de los documentos? *

- ◯ Sí
- ◯ No

¿Considera que la tecnología de Amazon Web Services es seguro y confiable? *

- ◯ Sí
- ◯ No

¿Considera usted que el modelo propuesto, facilita en la carga y organización de los documentos? *

- ◯ Sí
- ◯ No

¿Considera usted que el modelo propuesto, facilita al proceso de aprobación de documentos mediante los contratos inteligentes? *

- ◯ Sí
- ◯ No

¿Considera usted que el modelo propuesto le facilita lineamientos para una implementación?

- ◯ Sí
- ◯ No

De modo general, ¿cómo evalúa esta propuesta? *

- ◯ Muy bueno
- ◯ Bueno
- ◯ Regular
- ◯ Malo

Si usted desea expresar algún otro criterio sobre el modelo propuesto, puede ingresarlo aquí

Tu respuesta