APLICABILIDAD DE BLOCKCHAIN PARA EL PROCESO DE NEGOCIO "DIGITALIZACIÓN DE DOCUMENTOS" EN UNA EMPRESA DE GESTIÓN DOCUMENTAL

BLOCKCHAIN APPLICABILITY FOR THE BUSINESS PROCESS "DOCUMENT´S DIGITALIZATION" IN A DOCUMENT MANAGEMENT COMPANY

Ing. Rocío Andrea Acevedo Rodríguez[1]
Ing. Fredi Alezander Ospina González[2]
Ing. Giovanni Tapiero Velásquez[3]
Ing. Yenny Isabel Serrato Rodríguez[4]

RESUMEN

El cambio acelerado de la tecnología hace que las empresas que proporcionan servicios de gestión documental, busquen continuamente implementar nuevas formas de gestionar la información de manera segura y eficiente, muchas veces intentan solventar problemas en las cadenas de suministro con soluciones provisionales que en algunas ocasiones resultan ineficientes e inoperantes, algunas de estos problemas pueden atribuirse a fallas o ausencia de controles de seguridad e integridad de la información, fallas en la infraestructura tecnológica o su administración entre otros.

Los modelos de operación actualmente no permiten controlar si los documentos han sido duplicados, accedidos, manipulados, firmados, por personal no autorizado, ante la

ausencia de estos controles se pueden materializar riesgos de seguridad que afectan la disponibilidad, confidencialidad e integridad de la información suministrada por los clientes de la compañía, generando impactos reputacionales, contractuales y legales que pueden poner en riesgo la continuidad de la operación.

La finalidad del presente documento es realizar un análisis de implementación de blockchain en una empresa de gestión documental aplicable para el proceso de digitalización de documentos, por lo cual es necesario hacer un estudio de los principios básicos del funcionamiento de esta tecnología, la clasificación de los sistemas blockchain que se pueden aplicar al proceso, las ventajas a nivel de seguridad de la información de su implementación y las limitaciones que pueden afectar la implementación a futuro y de esta manera concluir la viabilidad del proyecto.

Palabras clave: Blockchain, Criptografía

ABSTRACT

The accelerated change in technology makes companies that provide document management services continuously seek to implement new ways to manage information in a secure and efficient manner. Often, these companies try to solve problems in supply chains with temporary solutions that sometimes turn out to be inefficient and inoperative. Some of these problems can be attributed to failures or lack of security and information integrity controls, failures in the technological infrastructure or its administration, among others.

The current operating models do not allow controlling whether documents have been duplicated, accessed, manipulated or signed by unauthorized staff. In the absence of these controls, security risks could emerge and affect the availability, confidentiality and integrity of the information provided by customers. Consequently; reputational,

contractual and legal impacts may jeopardize the continuity of the operation.

The main purpose of this document is to analyze the implementation of blockchain in a document management company, accurate to the process of digitization of documents, so it is necessary to study the basic principles of the operation of this technology, the classification of blockchain systems that can be applied to the process, the advantages in terms of information security of its implementation and the limitations that may affect the implementation in the future and thus conclude the feasibility of the project.

Keywords: Blockchain, Cryptography

1. INTRODUCCIÓN

Las empresas que suministran servicios de digitalización de documentos, deben constantemente evolucionar y reinventar el negocio hacia un modelo cien por ciento digital que genere valor a los clientes actuales, la documentación electrónica generada a partir de este proceso se vuelve muy sensible para todos los interesados, allí es donde toma relevancia la seguridad de la información.

Este documento se enfoca en realizar un análisis sobre la aplicabilidad de Blockchain buscando fortalecer la seguridad de la información del proceso de negocio de digitalización de documentos.

Esta tecnología introduce el uso de redes descentralizadas a través de nodos interconectados en tiempo real, que brindan mayor seguridad a la información, aplica también el principio de la autenticidad de los documentos y disminuyen el riesgo de alteraciones y fraudes debido a los altos niveles de trazabilidad soportados por algoritmos criptográficos.

De acuerdo al modelo de negocio actual de la organización se analizarán los riesgos de aplicar Blockchain al proceso de digitalización de documentos y se presentará un modelo tecnológico acorde a sus necesidades operacionales.

2. REFERENTES TEÓRICOS

2.1. Blockchain

Se define como una cadena de bloques que contiene información encriptada de una o varias transacciones, generando un valor correspondiente a la secuencia de datos correlacionados protegidos a través del uso de la criptografía. La cadena de bloques opera mediante nodos interconectados y descentralizados que comprueban las transacciones de la red, esta tecnología inicialmente se creó para la operación de criptomonedas, pero ha ido extendiendo su aplicabilidad a otros procesos como cadena de suministros, gestión documental entre otros.

En relación al proceso de gestión documental permite con facilidad que los archivos a procesar generen y registren sus propios hash (estructuras que se usan para validar la integridad de la información) en la cadena de bloques, lo que permite verificar su autenticidad y hacer seguimiento a los documentos digitalizados en la organización.

2.2. Tipos de Blockchain

2.2.1. Blockchain públicos.

Se conoce como el pionero en este tipo de tecnologías que se encuentran utilizables en la web, este tipo de blockchain, es de uso público en referencia a sus datos, programas y código fuente, lo que permite revisar, auditar y modificar todos sus componentes y su código fuente.

2.2.2. Blockchain privados.

Con base en la transformación digital, muchas organizaciones se interesaron por implementar esta tecnología en sus procesos internos, estas cadenas de bloques son cadenas autorizadas, que operan bajo los mecanismos de control de acceso para autorizar la incorporación de los participantes de la red mediante un administrador que también inspecciona y asigna las funciones y permisos dentro de la blockchain. Por lo general son opciones de desarrollo de tipo software restrictivo.

2.2.3. Blockchain o híbrido.

Se define esta tecnología, como la integración entre las blockchain públicas y privadas, optimizan los recursos de cada una, la asistencia a la red es de carácter privada, haciendo esto, que el consumo de sus elementos sea controlado por una o varias organizaciones. Los objetivos primordiales de este modelo de blockchain, son la sostenibilidad en el tiempo y la integralidad de los datos almacenados.

2.3. Almacenamiento de cadena de bloques

Se entiende que una cadena está conformada por varios bloques y en cada uno de estos, se almacena información como: registros, transacciones, información del mismo bloque y sus dependencias a nivel interno, cada uno de estos bloques, ocupa un lugar inamovible dentro de la cadena, creando así una correlación entre todos y cada uno de los bloques existentes (antiguos y recientes).

2.4. Gestión Documental

Se describe como las actividades relacionadas con el manejo de los documentos de una organización o empresa, de manera que estos puedan ser fácilmente ubicados, siendo esto, una dinámica recurrente, que requiere y exige ser realizada de forma ágil y precisa para optimizar los procesos de negocio.

2.5. Digitalización de Documentos

Este proceso convierte la documentación física a un formato digital, lo que permite abordar la problemática de la consulta de altos volúmenes de información, disminuyendo los tiempos de ejecución de los procesos de negocio y optimizando su operación generando un valor agregado y una respuesta más eficiente a los clientes y usuarios internos de la organización.

Para toda esta puesta en marcha, se debe tener claro el procedimiento a ejecutar en referencia al escaneo de múltiples documentos, optimizando el volumen de páginas por minuto y definiendo que se van utilizar recursos propios, ya que se cuenta con la disponibilidad, el recurso humano, técnico y de infraestructura.

Por último, no menos importante, es determinar, una vez implantado y puesto en marcha el esquema de digitalización documental en la organización, se deben generar políticas de copias de seguridad (Back-up), para reducir la pérdida del documento, ante situaciones de borrado del archivo digital en la unidad de almacenamiento.

2.6. Seguridad de la Información en Gestión Documental

Inicialmente, en términos de seguridad se deben tener en cuenta las siguientes premisas:

2.6.1. La seguridad de la infraestructura

Se encarga del acceso a los documentos, a través del software de gestión documental implementado.

2.6.2. La autenticación

Permite comprobar la integridad de los usuarios que van a acceder al software de gestión documental.

2.6.3. La Autorización

Se encarga de verificar qué, quien desea realizar alguna maniobra en el ambiente implementado, esté autorizado para hacerlo.

En referencia a la seguridad de la infraestructura, se tendrá en cuenta, el uso de elementos tecnológicos como: comunicaciones seguras, encriptación de la data, acceso al módulo de almacenamiento (storage) y restauración de back-ups.

Todo esto con el fin de prevenir circunstancias que impliquen riesgo a nivel de conectividad de la red o de acceso a las unidades de almacenamiento donde se encuentra la información de la organización, bajo la figura comercial “por demanda”.

En referencia a la autenticación, podemos decir, que se requiere de un método de acceso (usuario y clave), pero, se pueden alternar con sistemas biométricos (tarjetas y huellas), es potestad del área de control de acceso definir con base al rol del usuario, el tipo de autenticación requerida.

En referencia a la autorización, es quizá, la parte “menos técnica” de todas, ya que, esta se establece mediante un listado de control de acceso, definido por el área de seguridad de la información y la gerencia operativa del área. Determinando así, que permisos de consulta y/o edición, tendrían cada uno de los usuarios que se encuentran en dicha lista, y sus dependencias entre lotes y sus respectivos elementos.

3. METODOLOGÍA

En este capítulo se describe el método de investigación para el desarrollo del presente artículo, el diseño propuesto busca identificar los factores clave que permitirán generar una solución a la problemática de la organización.

Figura 1. Desarrollo de la metodología

3.1. Análisis de la situación actual

Durante esta fase se analiza y documenta: el contexto de la organización, la problemática, la normativa vigente aplicable y buenas prácticas en seguridad de la información.

3.2. Análisis de la tecnología blockchain

Durante esta fase se analiza y documenta: las principales ventajas de la tecnología blockchain, el análisis de riesgos y controles - Tecnología blockchain y normas ISO 27001:2013 e ISO 27002:2022 y las recomendaciones en base a su identificación.

3.3. Análisis de viabilidad blockchain

Durante esta fase se documenta: el análisis de la viabilidad de un modelo basado en blockchain.

3.4. Modelo de la solución tecnológica propuesta

Durante esta fase se analiza y documenta: el modelo tecnológico propuesto.

3.5. Resultado de la investigación

Durante esta fase se documenta: el resultado de la investigación y las conclusiones.

4. DESARROLLO METODOLÓGICO

De acuerdo a la metodología planteada se describen cada una de las fases para el desarrollo del análisis de viabilidad:

4.1. Glosario

- **Algoritmos Criptográficos.** Es un algoritmo que puede encriptar texto en lenguaje natural para hacerlo ilegible, y para que sea desencriptado con el fin de recuperar el texto original. (1)

- **Criptografía Asimétrica.** (*o criptografía de llave pública*) permite establecer una conexión segura entre dos partes, autentificando mutuamente a las partes y permitiendo el traspaso de información entre los dos. El sistema utiliza dos llaves para cifrar un mensaje: una llave pública y otra privada. (2)

- **DAG de Merkle.** Es una estructura que relaciona todas las transacciones y las agrupa entre pares para obtener un Root Hash o "dirección raíz". Este Root Hash, está relacionado con todos los hashes del árbol. (3)

- **Framework.** Es un esquema o marco de trabajo que ofrece una estructura base para elaborar un proyecto con objetivos específicos, una especie de plantilla que sirve como punto de partida para la organización y desarrollo de software. (4)

- **Función Hash.** En inglés hash function, también conocida con el híbrido función hash, convierte uno o varios elementos de entrada a una función en otro elemento. Como su nombre lo indica, una función matemática utilizada en criptografía donde las más comunes agarran entradas de longitudes versátiles para restituir salidas de una longitud permanente. A su vez, combina las capacidades de paso de mensajes hash con propiedades de ciberseguridad. (5)

- **GED.** es un conjunto de tecnologías (*hardware y software específico*) que permite la gestión inteligente de cualquier documento o archivo de una organización, originalmente electrónica o convertidos a formato digital. (6)
- **Gestión de Identidades (*IAM*).** Un sistema de administración de accesos e identidades, es un marco para los procesos de negocio que facilita la gestión de las identidades electrónicas. El marco incluye la tecnología necesaria para apoyar la gestión de identidad. (7)

- **OCR.** (*Optical Character Recognition*) o Reconocimiento Óptico de Caracteres en español, es una tecnología que permite convertir documentos (en varios formatos) en datos que pueden ser buscados y editados por un dispositivo como un teléfono móvil o un ordenador. (8)

- **PHP.** (*Hypertext Preprocessor*) es un lenguaje de código abierto para el desarrollo web y que puede ser incrustado en HTML. (9)

- **Protocolo IPFS.** o (*InterPlanetary File System, IPFS*), que en español se traduce como Sistema de Archivos Interplanetario. Más allá de su nombre, esta tecnología se puede describir como un protocolo de almacenamiento descentralizado que permite interacción directa entre sus usuarios por medio de una red P2P global. (10)

- **JSON.** (*JavaScript Object Notation*), es un formato basado en texto estándar para representar datos estructurados en la sintaxis de objetos de JavaScript. (11)

- **XML.** Es un lenguaje de marcado similar a HTML. Significa Extensible Markup Language (*Lenguaje de Marcado Extensible*) y es una especificación de W3C como lenguaje de marcado de propósito general. (12)

- **Red P2P.** es un modelo de red descentralizado que consta de un grupo de dispositivos (nodos) que almacenan y comparten archivos, cada nodo actúa como un par individual. En esta red, la comunicación P2P se realiza sin ninguna administración centralizada, lo que significa que todos los nodos pueden realizar las mismas tareas. (13)

- **Tolerancia a Fallas Bizantinas.** o (*Byzantine Fault Tolerance BFT),* es la fiabilidad de un sistema informático tolerante a fallos, en particular sistemas informáticos distribuidos, donde los componentes pueden fallar y hay información imperfecta sobre si un componente ha fallado. En un “fallo bizantino”, un componente como un servidor puede aparecer de forma inconsistente tanto en el fallo como en el funcionamiento de los sistemas

de detección de fallos, presentando diferentes síntomas a diferentes observadores. (14)

4.2. Análisis de la Situación Actual

En esta fase se realizaron sesiones de trabajo con el personal de la organización que opera el proceso de gestión documental y el personal del área de tecnología con el fin de comprender la operación de negocio, la ejecución del proceso de digitalización de documentos, la arquitectura tecnológica que lo soporta y la problemática base de la investigación.

4.2.1. Contexto de la organización.

La compañía ofrece a sus clientes servicios como digitalización de documentos, custodia de archivos físicos, destrucción de documentos, organización de archivos y outsourcing de gestión documental.

Esta investigación se centra en el proceso de digitalización de documentos, el cual es el más importante para el negocio, ya que representa el treinta y dos por ciento (32%) de sus ingresos anuales y la compañía en los últimos tres años ha invertido en el mejoramiento del mismo con la adquisición de hardware especializado para digitalizar (escáneres con tecnología OCR) y el desarrollo de una aplicación WEB en PHP para la gestión estandarizada de documentos denominado “GED”, con personal especializado en esta área.

A continuación, se muestra el diagrama de arquitectura de la aplicación GED, la cual en sus capas

presenta alta disponibilidad en los componentes de hardware (Clústeres de aplicación y Bases de Datos).

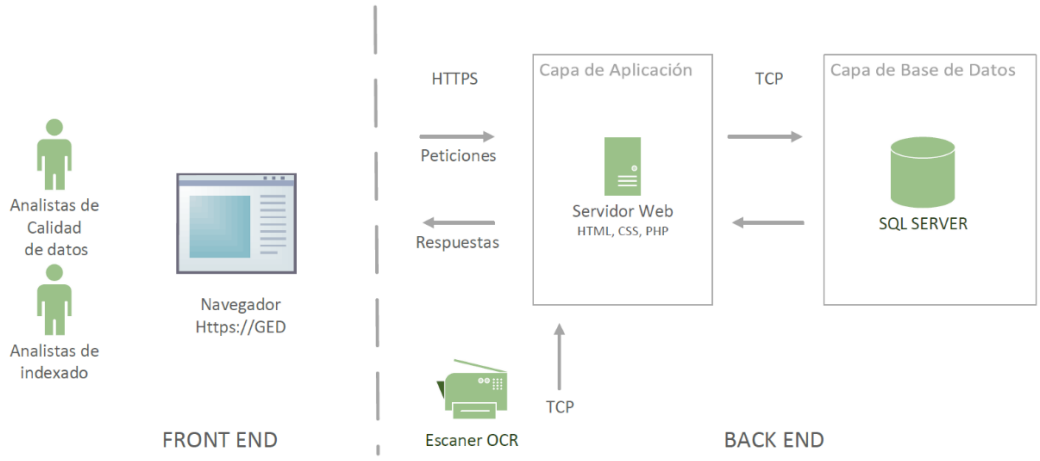

Figura 2. Diagrama de Arquitectura del sistema de gestión GED

El proceso de digitalización presenta las fases que se indican a continuación:

- **Estructura documental:** define los campos de indexación.
- **Prueba de concepto:** una vez se definen los campos, se crean en el sistema de gestión (GED) y se realiza una prueba preliminar para verificar la estructura documental.
- **Preparación de los documentos físicos:** se realiza la limpieza de los documentos en papel y se retiran elementos tales como clips, ganchos, cintas, etc.
- **Clasificación de los documentos físicos:** se realiza una demarcación de los documentos o expedientes, para una carga sencilla en los escáneres profesionales.
- **Escaneo de los documentos:** esta fase se realiza la digitalización de los documentos por medio de los escáneres profesionales.
- **Indexación de la información:** en base a la estructura documental, se realiza la captura

de los valores de cada campo, este paso se hace de forma manual por los analistas de indexado, pero se puede realizar de forma automática por medio de OCR (Reconocimiento Óptico de Caracteres) que presentan los escáneres profesionales y posteriormente la información indexada es almacenada en una Base de Datos.

- **Exportación al sistema de gestión de documental (GED)** en esta fase se realizan las siguientes actividades:
    - Cargue de los documentos o expedientes y su metadata en el sistema de gestión documental.

- **Consulta de los documentos o expedientes en el sistema de gestión documental (GED):**
    - Verificación de la información almacenada por los analistas de calidad.

El siguiente es el diagrama general del proceso de digitalización:

Figura 3. Diagrama del proceso de digitalización

Las fases antes descritas se muestran en el siguiente diagrama de flujo de los documentos, en el proceso de digitalización:

Figura 4. Diagrama de flujo del proceso de digitalización de documentos

4.2.2. Problemática.

La empresa manifiesta la necesidad de mitigar los incidentes que se ha presentado con algunos de sus clientes por errores en la entrega de la información procesada, fase en la que se presentan situaciones como:

- Información entregada a los clientes sin ningún tipo de seguridad; al terminar de digitalizar los documentos la información resultante (documentos en PDF y la información indexada en una copia de la Base de Datos) se envía por correo electrónico o se almacena en un dispositivo externo: memorias, discos USB o CD/DVD para ser entregado.
- En ocasiones se pierde la trazabilidad de la entrega de la información al cliente.
- Información entregada de manera errónea a los clientes, en ocasiones se presenta que la

documentación resultante (documentos en PDF y la información indexada) se entrega al cliente incorrecto.

- Pérdida de tiempo en la búsqueda de documentos, algunas veces se debe realizar la comparación del documento físico con los documentos digitalizados para garantizar su correlación, aumentando los tiempos de entrega del producto final a los clientes.
- Diferentes versiones de un mismo documento, ya que no se tiene trazabilidad del mismo.
- Si se necesita eliminar algún documento digitalizado, no se tiene control y se pueden eliminar documentos que ya pasaron por control de calidad.
- En cuanto a la infraestructura tecnología, se debe almacenar grandes volúmenes de información de los clientes por el tiempo acordado, lo cual consume gran cantidad de recursos en el dispositivo de almacenamiento de la empresa.

4.2.3. Normativa vigente aplicable y buenas prácticas en seguridad de la información

La organización contempla la normativa de gestión documental y la ley de protección de datos personales, aplicable en su interior y hacia los clientes como entidades públicas, privadas, instituciones educativas y del sector salud, entre otras.

- **Ley 1581 / 2012**: define los principios y disposiciones para la protección de datos personales y el tratamiento por parte de entidades de naturaleza pública o privada. (15).
- **Decreto 1377/ 2013** tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. (15).
- **Ley 1266 /2008** Habeas Data tiene por objeto desarrollar el derecho constitucional que

tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos. (16).

- **Ley 872 de 2003 y el Decreto reglamentario 4110 de 2004 y 4297 de 2007**: obligan a las entidades públicas a implementar sistemas de gestión de la calidad e involucran un proceso de gestión documental. Conforme a la Ley 87 de 1993 y su Decreto reglamentario 1537 de 2001, las entidades públicas deben implementar sistemas de control interno por procesos y el componente información a la gestión documental. (16).

  Es importante asegurar el cumplimiento de la normatividad en el modelo propuesto de solución y contar con la aprobación de los asesores expertos legales.

En el mismo sentido acogiendo buenas prácticas, la organización acoge el estándar ISO 15489:2016 Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios para la definición de los lineamientos y procedimientos que soportan la operación de los procesos de gestión documental. De acuerdo a lo anterior expuesto en el artículo se relaciona el estándar, más no se profundiza en su aplicación al interior de la organización.

El análisis de riesgose identificación de controles se orientó bajo las directrices de las normas:

- ISO/CEI 27001:2013 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. (19)
- ISO/CEI 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información. (20)

Así mismo, se utilizan las directrices del documento de ISACA “Blockchain Framework and Guidance (16), para la investigación de la viabilidad en la aplicación de la tecnología blockchain al proceso de gestión documental “digitalización de documentos”.

4.3. Análisis de la tecnología blockchain

4.3.1. Principales ventajas de la tecnología blockchain.

Esta tecnología permite que la digitalización de los documentos durante las diferentes etapas del ciclo de vida sea seguras, confiables e irreversibles generando una relación de confianza en el proceso, además proporciona altos niveles de integridad de la información a través del uso de algoritmos criptográficos que reducen la probabilidad modificación, falsificación y borrado de la información soportado en el principio de inmutabilidad.

Así mismo, al ser una tecnología que opera de manera descentralizada, elimina los puntos únicos de falla, fortaleciendo la continuidad de negocio debido a que ante la afectación de uno de los nodos en la red no se impacta la disponibilidad del servicio.

Otras de las ventajas de esta tecnología es la velocidad en la trasmisión de datos lo cual optimiza la gestión del proceso, los bajo costos ya que reduce el proceso de sobrecarga de información elimina los intermediarios y agiliza las comunicaciones en las diferentes etapas del proceso.

Mediante los nodos de la red, genera copias únicas de los registros, lo cual no permite generar diferentes versiones que cumplan con los criterios de validación de toda la red de nodos, la información que transita y se almacena por los diferentes nodos se encuentra encriptada y se genera históricos de la cadena de información contenida en un bloque apoyando el principio de no repudio en seguridad de la información.

La tecnología de blockchain casi siempre es de código abierto. Eso significa que otros usuarios o desarrolladores tienen la oportunidad de auditarlo, modificarlo y mejorarlo con total libertad para crear nuevas aplicaciones.

4.3.2 Análisis de riesgos y controles - Tecnología blockchain y normas ISO 27001:2013 y 27002:2022

La información es el activo más importantes que tiene cualquier empresa en la actualidad, las organizaciones dependen de su información para operar los procesos de negocio, por lo tanto, es necesario identificar las consecuencias adversas de la pérdida de confidencialidad, integridad y disponibilidad de la información; el análisis y la gestión de riesgos, son procesos esenciales para asegurar que los controles y las inversiones que se derivan de su implementación estén acordes con los niveles de riesgo aceptables, teniendo en cuenta que el riesgo no es posible eliminarlo por completo, “las organizaciones deben evaluar su perfil de riesgo dinámico y determinar qué nivel y qué tipos de ciber-riesgos son aceptables”. Gil, A. (2018) Blockchain & Ciberseguridad P.5.

Como parte de las fortalezas identificadas en la organización, es la definición de la política de seguridad de información y ciberseguridad la cual está orientada a la prevención, protección y

detección de los riesgos vulnerabilidades y amenazas a los que se pueden ver expuestos en materia de seguridad de la información, para abordar estas amenazas es importante establecer los controles y estrategias de seguridad y ciberseguridad, la organización ha adoptado la norma ISO 27001: 2013 como buena práctica para la implementación y mantenimiento de su sistema de gestión de seguridad de la información, sin intención de certificarse, buscando optimizar el grado de madurez del sistema.

La infraestructura actual de la compañía es On-premise y han establecido algunos controles de seguridad física y lógica para la protección de los activos críticos de la organización.

La tecnología blockchain le va a permitir a la organización mitigar en mayor medida los riesgos asociados a la afectación de la confidencialidad, integridad y disponibilidad de la información. A continuación, se presenta la matriz de los principales riesgos identificados, las posibles causas que los pueden materializar, los controles aplicables en blockchain (17) y en las normas ISO 27001:2013 (19) e ISO 27002:2022 (20), así como las recomendaciones generadas de acuerdo a la investigación.

4.3.2.1. Riesgo: Falla en la implementación del blockchain

Causa	Controles Blockchain	Controles ISO 27001:2022	Controles ISO 27002:2022	Recomendaciones
1. Protocolos y/o formatos de programación incompatibles. 2. Inadecuada gestión de la implementación. 3. Ausencia de personal capacitado para realizar la implementación. 4. Incumplimientos normativos.	1. Compatibilidad con los formatos JSON, PHP y XML para el intercambio de información. 2. Mecanismo de autodestrucción de Smart contracts. 3. Comunicación entre nodos a través del Border Gateway Protocol (BGP).	A.18.1 Evitar el incumplimiento de las obligaciones legales, estatutarias de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad. A.14.2 Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	5.3.1 Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados. 5.8 La seguridad de la información debe integrarse en la gestión de proyectos. 8.4 El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software debe administrarse adecuadamente. 8.25 Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas. 8.26 Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones. 8.28 Garantizar que el software se escriba de forma segura, reduciendo así el número de posibles problemas de seguridad de la información. 8.29 Los procesos de prueba de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.	Incluir a las partes interesadas internas y externas necesarias para abordar los riesgos de: • Seguridad de la información y ciberseguridad • Operativos • Normativos Con el fin de tener una visión holística de los riesgos, lo anterior abarca el control 5.8 que hace referencia a la inclusión de la seguridad de la información en la gestión de proyectos. Con la validación de las áreas de riesgos, se debe presentar el proyecto a la Alta Dirección para la aprobación y asignación de recursos. La organización cuenta con un área de desarrollo de sistemas de información, con personal con la competencia, el conocimiento y las habilidades para realizar la integración entre la plataforma de storage blockchain y la aplicación de gestión documental la cual es un desarrollo interno. Así mismo, la compañía aplica prácticas de desarrollo seguro, se recomienda el uso de herramientas de verificación de código dinámico. Otro aspecto que se debe considerar es realizar pruebas previas en un ambiente controlado y establecer los mecanismos adecuados de gestión del cambio. En relación al cumplimiento normativo con la ley 1581 de 2012 de protección de datos personales la cual tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que hayan recogido sobre ellas en bases de datos o archivos; y establece los derechos de: • Integridad y confidencialidad de los datos • Derecho al olvido • Derecho de rectificación

Causa	Controles Blockchain	Controles ISO 27001:2022	Controles ISO 27002:2022	Recomendaciones
				En cuanto al primer derecho, podemos concluir que de acuerdo a la naturaleza de la tecnología blockchain la cual hace uso de técnicas de criptografía asimétrica y mecanismos de gestión de identidad, la integridad y la confidencialidad de los datos se garantiza. Dado que los hashes se almacenan en blockchain y los datos personales permanecen almacenados en una base de datos fuera de la red, los nodos solo tendrán acceso a los hashes –números aleatorios sin significado para ellos–, cumpliendo así los principios de integridad y confidencialidad. (20). Por otra parte, en relación al derecho al olvido se identificó que las soluciones de blockchain de última generación como los Smart contracts cuentan con una opción de autodestrucción, lo cual permite la eliminación de la información. Así mismo, se recomienda que la organización pacte con sus clientes el periodo de tiempo para realizar la verificación y descarga de la información en la plataforma blockchain para que posteriormente se proceda a eliminarse por parte del responsable del tratamiento, al eliminará los datos de la base de datos externa, mientras que el hash correspondiente permanecerá en blockchain, pero éste se convierte en un número aleatorio sin correspondencia, de modo que la información almacenada en blockchain pasa a ser ininteligible y, por tanto, irrelevante.(20). Por otra parte, el derecho a la rectificación si se requiere realizar la modificación a la información en la base de datos externa. El registro actualizado sustituirá al anterior registro de la base de datos externa y recibiendo un nuevo hash, que se almacenará en blockchain. El hash de los datos personales antiguos pasará a ser, nuevamente un número aleatorio carente de significado por no tener correspondencia con ningún dato de la base de datos externa. (20).

Tabla 1. Falla en la implementación del blockchain

4.3.2.2.Riesgo: Duplicidad y errores en la entrega de la información

Causa	Controles Blockchain	Controles ISO 27001:2022	Controles ISO 27002:2022	Recomendaciones
1. Ausencia de controles que impidan la creación de diferentes versiones de los documentos. 2. Ausencia de mecanismos de identificación de documentos.	1. Inmutabilidad, los datos agregados a la cadena de bloques no se pueden modificar, por lo cual son aprueba de manipulaciones. Identificador único asignado a los documentos a través del uso de funciones DAG de Merkle, esta estructura asegura que todos los intercambios en la red peer to peer (P2P) son correctos, no están dañados ni han sido alterados. Esta verificación se realiza organizando los bloques de datos utilizando funciones criptográficas de hash.	A.8.2. Asegurar que la información recibe un nivel apropiado de protección de acuerdo a su importancia para la organización. A.13.2 Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. A.14.1.3 La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la trasmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada de mensajes, la divulgación no autorizada, y la duplicidad o reproducción de mensajes no autorizada,	5.14 Transferencia de información Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes. 5.33 Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	Una de las grandes ventajas de implementar soluciones de blockchain es la inmutabilidad, propiedad que no permite la modificación de los documentos lo cual disminuye en un 100% la generación de diferentes versiones de un documento. A través de funciones como el árbol de Merkle el cual se basa en un algoritmo que toma como datos de entrada el conjunto de transacciones almacenadas en un bloque con el fin de verificar que las mismas no hayan sido alteradas. El bloque no se procesa como un todo, sino que cada transacción es evaluada por separado, mientras el algoritmo las agrupa en segmentos vinculados, produciendo al final un hash del bloque completo, es decir que se asigna a cada nodo un identificador único (hash) y la sumatoria de cada hash es la identificación del nodo principal o padre así, si se altera un documento el hash se modifica lo que permite evidenciar que el documento fue manipulado. (24). Con el uso de esta tecnología se garantiza que al cliente final se le entrega la información en su versión única y final correlacionando el hash del documento almacenado en el storage blockchain con la identificación del cliente, fortaleciendo la integridad de la información.

Tabla 2. Duplicidad y errores en la entrega de la información

4.3.2.3.Riesgo: Modificación no autorizada de la información en el sistema

Causa	Controles Blockchain	Controles ISO 27001:2022	Controles ISO 27002:2022	Recomendaciones
1. Falla o inexistencia de mecanismos de protección de información. 2. Fallas o ausencia de controles de acceso (asignación de Roles, Perfiles y Atribuciones en el sistema). 3. Falta de conocimiento y formación en la gestión de las claves privadas	1. Aplicación de sistema de Gestión de identidades (IAM). 2. Uso de clave privadas y privadas a través de un sistema de criptografía asimétrica. 3. Identificador único asignado a los documentos a través del uso de funciones DAG de Merkle, esta estructura asegura que todos los intercambios en la red P2P son correctos, no están dañados ni han sido alterados. Esta verificación se realiza organizando los bloques de datos utilizando funciones criptográficas de hash.	A.9.2 Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. A.9.4 Evitar el acceso no autorizado a sistemas y aplicaciones. A.10.1 Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad del a información. A.14.1 Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida, esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.	5.15 Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos comerciales y de seguridad de la información. 5.16 Permitir la identificación única de personas y sistemas que acceden a la información de la organización y otros activos asociados y permitir la asignación adecuada de derechos de acceso. 5.33 Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada. 8.24 Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas. 8.5 Las tecnologías y los procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.	El acceso al storage blockchain se realiza a través de la asignación de un usuario y una contraseña, así mismo recordemos que esta tecnología hace uso de la criptografía asimétrica basada en algoritmos, cada participante en la red blockchain administra una clave privada y una clave pública. La clave publica es conocida por los participantes en la red mientras que la privada no. Los datos almacenados en storage blockchain son cifrados y al operar con protocolos de consenso todos los nodos de la red tiene la misma información, lo cual se minimiza el riesgo de modificación de la información. A continuación, se relaciona algunos de los mecanismos de consenso: • Prueba de trabajo (PoW): se utiliza para confirmar transacciones y producir nuevos bloques que se agregan a la cadena. • Prueba de participación (PoS): algoritmo mediante el cual se apunta una red blockchain para lograr un consenso distribuido. • Tolerancia a fallas bizantinas (pBFT): mecanismo de consenso en el que todos los nodos se ordenan en secuencia, siendo un nodo el nodo principal o líder, y todos los demás se denominan nodos de respaldo. (16). Algunas de las API de storage blockchain cuenta con cuentan con mecanismos para la gestión de autorizaciones y una concesión de acceso lo cual es un sobre de seguridad que contiene una dirección satelital, una clave de API restringida y una clave de encriptación basada en una ruta restringida: todo lo que una aplicación necesita para ubicar un objeto en la red, acceder a ese objeto y descifrarlo.

Tabla 3. Modificación no autorizada de la información en el sistema

4.3.2.4.Riesgo: Acceso no autorizado al Sistema y/o datos

Causa	Controles Blockchain	Controles ISO 27001:2022	Controles ISO 27002:2022	Recomendaciones
1. Falla o inexistencia de mecanismos de protección de información. 2. Inexistencia o configuración deficiente de los mecanismos de protección del tráfico de red. 3. Fallas en el proceso de asignación de Roles, Perfiles y Atribuciones en el sistema	1. canales cifrados privados de transmisión de información entre dos o más nodos para asegurar confidencialidad. 2. Uso de protocolos IPFS - al ser un protocolo descentralizado permite interacción directa con los usuarios autorizados por medio de una red P2P de esta manera los usuarios pueden rastrear su ubicación en la red y monitorear modificaciones en los archivos. 3. Los archivos se descargan de forma fragmentada y utilizan funciones hash para garantizar su integridad. 4. Acceso a la información a través del uso de clave privadas y públicas mediante un sistema de criptografía asimétrica. 5. Aplicación de sistema de Gestión de identidades (IAM).	A.9.2 Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. A.9.4 Evitar el acceso no autorizado a sistemas y aplicaciones. A.10.1 Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad del a información. A.13.2 Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa A.14.1 Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida, esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas. .	5.15 Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados deben establecerse e implementarse en función de los requisitos comerciales y de seguridad de la información. 5.16 Permitir la identificación única de personas y sistemas que acceden a la información de la organización y otros activos asociados y permitir la asignación adecuada de derechos de acceso. 5.17 La asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación. - El cifrado y el hashing de contraseñas deben realizarse de acuerdo con las técnicas criptográficas aprobadas para contraseñas. 5.33 Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada. 8.3 El acceso a la información y otros activos asociados debe estar restringido de acuerdo con la política específica del tema establecida sobre control de acceso. 8.15 Para registrar eventos, generar evidencia, garantizar la integridad de la información de registro, prevenir el acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y respaldar investigaciones	Como se mencionó en el numeral anterior, el acceso al storage blockchain se realiza mediante usuario y una contraseña, y con la aplicación de criptografía asimétrica basada en algoritmos lo cual reduce la probabilidad de ocurrencia de accesos no autorizados. Sin embargo, se recomienda sensibilizar a los clientes en relación al uso adecuados de los usuarios y claves asignados para acceder a la plataforma de blockchain, destacando la importancia de no compartir las claves y asignar contraseñas complejas, lo anterior, debido a que pueden llegar a ser víctimas de ataques como phishing para obtener sus credenciales de acceso, no obstante, el atacante también deberá haber conseguido obtener las claves privadas para lograr un acceso no autorizado. Por otra parte, la organización deberá también incluir en su política de gestión de identidad, un procedimiento de autorización y seguimiento de las altas y bajas de usuarios con permisos de acceso a la plataforma blockchain. La organización hará uso del servidor de aplicación el cual cuenta con medidas de seguridad como antivirus, antimalware, sistemas operativos actualizados en el cual se realizará la integración y configuración del nodo en el storage blockchain, este servidor cuenta con las capacidades técnicas requeridas, y es monitoreado de manera permanente a nivel de capacidad y disponibilidad. Se recomienda el uso de canales cifrados de comunicación para minimizar los accesos no autorizados e instalar herramientas como cryptoprevent o una extensión de navegador para Chrome, Firefox y Opera, como NoCoin y minerblock, los cuales impiden que se pueda instalar un software minero y las demás recomendaciones generadas en el anterior numeral con relación a los controles de identidad.

Tabla 4. Acceso no autorizado al Sistema y/o datos

4.3.2.5.Riesgo: Indisponibilidad de la información

Causa	Controles Blockchain	Controles ISO 27001:2022	Controles ISO 27002:2022	Recomendaciones
1. Falla de los nodos de la red 2. Recursos tecnológicos insuficientes 3. Errores humanos en la administración de la base de datos. 4. Ataques de DDoS	1. Red descentralizada P2P, la falla de un nodo no afecta la funcionalidad de la red. 2. Resistencia a fallas bizantinas – BFT 3. Respaldo selectivo o protocolos de consenso, donde los usuarios conocidos verifican las transacciones. 4. Fragmentación de los archivos de los usuarios y distribución en varios nodos de la red - protocolo IPFS 5. La tecnología blockchain es escalable, permite agregar nodos pares y reemplazar el bajo rendimiento de otros nodos. 6. Elimina la necesidad de hardware y la administración sobre la Base de datos disminuyendo la generación de errores humanos.	A.12.1.3. Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. A.13.1.2 se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red ya sean que los servicios se presten internamente o se contraten externamente. A.17 La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización	5.30 La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC. 8.6 El uso de los recursos debe monitorearse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados. 8.14 Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.	La tecnología blockchain divide, distribuye y almacena la información en diferentes nodos de la red, mitigando de esta manera los puntos únicos de falla que se presentan en la infraestructura on-premise y nubes centralizadas. El protocolo de comunicación peer-to-peer permite que los nodos logren lo siguiente: ● Proporcionar disponibilidad a la red manteniendo las conexiones vivo. ● Establecer nuevas conexiones para mejorar la seguridad de la red. ● Distribuir nueva información a otros compañeros para apoyar consenso. (16). Lo anterior debido a que las redes peer to peer no tiene una conexión central, lo cual aumenta el nivel de disponibilidad de la información ante ataques de DDos. Otro aspecto relevante en esta tecnología son los algoritmos de consenso, en los cuales todos los nodos se ordenan en secuencia, existe un nodo principal y los demás se denominan nodos de respaldo los cuales se comunican entre sí y establecen un acuerdo sobre el estado del sistema utilizando una regla mayoritaria, todos los nodos tiene una copia completa del nodo principal.

Tabla 5. Indisponibilidad de la información

4.3.2.6.Riesgo: Exposición a Ciberataques

Causa	Controles Blockchain	Controles ISO 27001:2022	Controles ISO 27002:2022	Recomendaciones
1. Filtración de datos personales 2. filtración de o revelación de datos confidenciales para obtener ventaja económica o causar daño a una organización	1. canales cifrados de transmisión de información entre dos o más nodos para asegurar confidencialidad. 2. Acceso a la información a través del uso de clave privadas y públicas mediante un sistema de criptografía asimétrica. 3. monitorear y garantizar que la tasa de hash de la red se maximice y se distribuya geográficamente y de forma no centralizada, de modo que ninguna entidad o entidades individuales puedan coludirse y tomar el control de al menos el 51 % del hash de la red.	A.12.2,1 Se debe implementar controles de detección, de prevención y de recuperación combinados con la toma de conciencia apropiada de los usuarios para proteger contra código malicioso,	8.10 Para evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información. 8.12 Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.	Si Bien la tecnología blockchain mitiga muchos de los riesgos de disponibilidad, integridad y confidencialidad de la información no es inmune a posibles ciberataques. (21). Los usuarios en la red blockchain son el eslabón más débil por medio del cual un sistema puede ser vulnerado, de ahí la importancia de asegurar la implementación de controles de seguridad para proporcionar autenticación, autorización y cifrado de datos con el fin de proteger adecuadamente el acceso a la información. (17). Los principales vectores de ataque: Phishing y malware: los atacantes mediante el envío de emails con malware buscan obtener las credenciales de acceso de los participantes en la red blockchain e insertar virus y gusanos informáticos. . Otros posibles ataques particulares sobre blockchain son: Ataque de Sybil: Los atacantes crean muchas identidades de red falsas para inundarla bloquear el sistema. Ataques del 51%: Los atacantes buscan obtener el control de la red a través del control del 51% de los nodos. Por lo tanto, es necesario aplicar los controles descritos en el presente articulo para disminuir la probabilidad de ocurrencia de este ataque, destacando los siguientes: • Gestión de identidad y acceso • Gestión de claves • Privacidad de datos • Comunicación segura • Monitoreo de recursos y redes

Tabla 6. Exposición a Ciberataques

4.4. Análisis de viabilidad blockchain

Una vez analizada la operación del proceso de negocio, la tecnología que la soporta, la problemática, con respecto a la digitalización de documentos, se concluyó que la tecnología de Storage blockchain da cubrimiento a las necesidades de la empresa, que permite mejorar la operación del proceso de negocio y fortalecer la seguridad de la información mediante los controles inmersos en esta tecnología identificados en el numeral 4.2.3.

A través de la solución de Storage blockchain, los clientes de la compañía podrán descargar su información de forma segura, ya que los documentos se cargan en la plataforma por la organización (Emisor) y se cifran con la clave publica, el cliente (receptor) ingresa con el usuario y clave asignado descarga el documento y la lee por medio de su clave privada.

Una vez el documento es cifrado, el hash pasa a ser el identificador único, lo que permite reconocer cualquier alteración del documento ya que el hash se modifica, así mismo el documento se cifra al subirlo por el emisor y de esta manera así un atacante logre interceptarlo no podrá ver su contenido ya que para su lectura debería conocer la clave privada del receptor.

Además, los documentos ingresados al Blockchain Storage son divididos, distribuidos y almacenados en varios nodos haciendo uso de los discos de la cadena de bloques disponibles, lo que reduce los puntos únicos de falla que se pueden presentar en la infraestructura On-Premise (en sitio) e incluso en la infraestructura de nube si no existe replicación en diferentes zonas de disponibilidad solución que suele generar mayores costos, la organización puede acordar la

cantidad de nodos a los que se requiere replicar la información de acuerdo a la membresía adquirida, esta tecnología realiza la comprobación de los nodos si algunos no están activos los datos se recuperan desde otro nodo al cual este replicando.

4.5. Modelo de la solución tecnológica propuesta

De acuerdo al proceso de negocio y las viabilidades expuestas anteriormente, la compañía puede utilizar blockchain público de almacenamiento de cadenas de bloques (Blockchain Storage), adicionalmente no necesitaría infraestructura en sitio (On-Premise), con lo cual la empresa ahorraría recursos de infraestructura (servidores, red, almacenamiento, etc.), pero tendrían que adquirir suscripciones para realizar las operaciones sobre los documentos que compartan con los clientes (esto depende de la cantidad de información).

Actualmente existen varios proyectos de empresas destacadas que ofrecen almacenamiento en cadenas de bloques como lo son: Sia, Inter Planetary File System (IPFS), MaidSafe y Storj.

También la compañía tendría que generar algunas mejoras en su sistema de gestión documental actual (GED), para que un documento integre en sus metadatos la información resultante del proceso de indexación, en la actualidad existen marcos de trabajo (Frameworks) desarrollados en código abierto y API’s con lo cual es posible en muy corto plazo realizar esta integración, pero esto debe ir de la mano de un riguroso control de calidad para que la información incrustada en el documento electrónico sea confiable.

El siguiente es un diagrama de arquitectura sobre la solución propuesta, que incluye a la arquitectura actual el componente de Blockchain y al usuario final (clientes de la compañía)

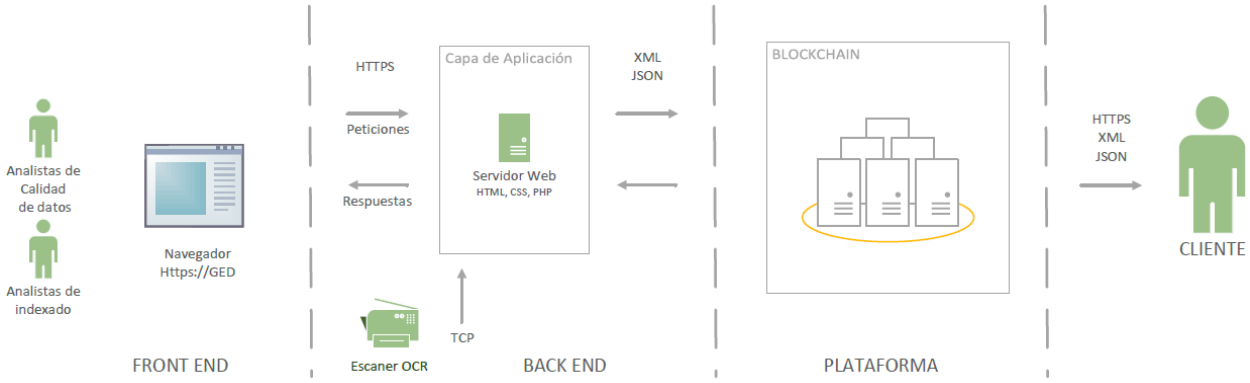

Figura 5. Diagrama de arquitectura integrando Blockchain

4.6. Resultado de la Investigación

Al integrar Blockchain al proceso de digitalización de documentos esta investigación le permite a la empresa:

- Mejorar en la seguridad en la información, ya que desde la carga de los documentos a Blockchain, este incorpora la identidad digital descentralizada o identidad soberana personal. Este sistema busca que el usuario sea el propietario de su identidad digital y no terceros, con este método, el usuario tiene pleno control de sus datos para decidir y permitir quién puede acceder a ellos y en qué términos y condiciones.
- Le permite a la compañía tener una trazabilidad del documento desde el inicio, porque cada vez que se modifica un documento, se crea una pista de auditoría y se logra saber exactamente cómo, cuándo y quién lo ha modificado.

- También se precisa una mejora en el proceso de la entrega de la información a los clientes, la cual actualmente como se indica en la problemática en el numeral 4.2.2, presenta falencias de seguridad, este beneficio permite a la compañía ahorrar recursos económicos (ya que no se debe hacer adquisición de dispositivos o realizar desplazamientos por el personal de la empresa) y aumentar la confidencialidad, ya que se garantiza que las personas autorizadas puedan obtenerla.
- Como se mencionó con anterioridad, si se persigue un modelo de blockchain público, la compañía no haría ninguna inversión en infraestructura tecnológica ni en contratación de personal adicional y al integrar su sistema de gestión documental - GED con alguna de las plataformas anteriormente descritas en el modelo de la solución tecnológica numeral 4.4, aumenta la disponibilidad de la información entregada a sus clientes.
- Como se indica en el numeral 4.5 en el modelo tecnológico propuesto en esta investigación, la empresa debe integrar su infraestructura actual con Blockchain para automatizar la carga de la información, para implementarlo debe adicionar en su aplicación denominada GED varios marcos de trabajo y API’s creados en código abierto para este propósito especifico.

5. CONCLUSIONES

Con este proyecto de investigación se logra establecer que, con la implementación de la solución se garantiza, la disponibilidad, confidencialidad e integridad de la información porque el modelo tecnológico propuesto permite aumentar la seguridad en el proceso de digitalización de documentos de acuerdo a las problemáticas identificada.

Se concluye también que la compañía a un corto plazo puede integrar Blockchain en su proceso de digitalización de documentos, este acoplamiento a su infraestructura tecnológica requiere de la implementación de varios marcos de trabajo (Ethereum, HyperLedger, etc.) o API´s que ya se encuentran desarrollados y son de código abierto.

Todo el proceso de análisis de riesgos realizado, permite fortalecer los niveles de la seguridad de los activos de información críticos y la protección de la información mediante la implementación de controles de acceso, mecanismos de cifrado que proporcionen ambientes seguros, estos controles, deben ser impulsados por políticas de seguridad de la información.

A partir de los documentos revisados y el análisis de la organización se concluye que la implementación de la tecnología blockchain representa una oportunidad para mejorar la gestión del proceso de negocio de digitalización de documentos reduciendo costos en la inversión de infraestructura tecnológica para el almacenamiento de datos y fortaleciendo los controles de seguridad durante la entrega de la información a los clientes, gracias a las características propias de la tecnología que abordan el no repudio, la protección ante modificaciones no autorizadas

soportadas en la característica principal de blockchain que es la inmutabilidad.

Por otra parte, la organización debe considerar las recomendaciones generadas en el numeral 4.3.2. Análisis de riesgos y controles - Tecnología blockchain y normas ISO 27001:2013 y 27002:2022 relacionadas con la adecuada gestión de los riesgos derivada de implementar una solución de almacenamiento basada en blockchain público, para lo cual se hace énfasis en la importancia de realizar un tratamiento adecuado de riesgos de la compañía e identificar el nivel aceptable de los riesgos con el cambio de tecnología.

La investigación nos permite identificar que la tecnología fortalece los controles de seguridad del proceso, no obstante, desde la gestión de proyectos y la gestión de riesgos se debe confrontar el análisis costo beneficio de acuerdo a la premisa de que el riesgo no se elimina por completo.

De acuerdo a lo anterior expuesto, es necesario incluir los riesgos y controles de esta investigación en la evaluación de riesgos tecnológicos de la compañía, lo cual le va a permitir proyectar la implementación de la solución ante la Alta Dirección de la organización y actualizar los elementos clave del Sistema de Gestión de Seguridad de la Información:

- Capacitación o sensibilización de las partes interesadas incluyendo a los clientes debido a que son quienes van a acceder a la plataforma blockchain y son generalmente los puntos clave para generar ataques.
- Prácticas de desarrollo seguro y verificación de código durante el proceso de integración de las aplicaciones.
- Adecuada gestión de cambios y pruebas previas al paso a producción.

- Actualización de la política y procedimientos de gestión de identidades para el seguimiento de las altas y bajas de los usuarios en la plataforma.
- Evaluación periódica de los riesgos de seguridad de la información y ciberseguridad y presentación a la Alta Dirección.

6. REFERENCIAS BIBLIOGRÁFICAS

1. MDN web docs. (febrero 2011). Glosario. recuperado de: https://developer.mozilla.org/es/docs/Glossary/Cipher

2. Altavoz. (octubre 2017). Que es la Criptografía Asimétrica y por qué es Importante. recuperado de: https://www.altavoz.net/altavoz/blog/desarrollo/que-es-la-criptografia-asimetrica-y-por-que-es-importante

3. Bit2me Academy. (marzo 2022). ¿Qué es un Árbol Merkle? recuperado de: https://academy.bit2me.com/que-es-un-arbol-merkle/

4. Edix. (agosto 2021). Framework. recuperado de: https://www.edix.com/es/instituto/framework/#:~:text=Un%20framework%20es%20un%20esquema,organizaci%C3%B3n%20y%20desarrollo%20de%20software

5. Wikipedia. (enero 2022). Función hash. recuperado de: https://es.wikipedia.org/wiki/Funci%C3%B3n_hash

6. Prado Chaves. (octubre 2011). Gestión de Documentos Electrónicos solución para la gestión de archivo y documentos electrónicos. recuperado de: https://pradochaves.com.py/gestao-eletronica-de-documentos-ged.asp

7. OnTek. (diciembre 2021). ¿Qué es… la Gestión de Accesos e Identidades? recuperado de: https://www.ontek.net/que-es-la-gestion-de-accesos-e-identidades/

8. Sydle. (abril 2022). ¿Qué es el OCR? ¿Para qué sirve? recuperado de: https://www.sydle.com/es/blog/ocr600b8be3009fd702f0761f43/#:~:text=El%20OCR%20(Optical%20Character%20Recognition,tel%C3%A9fono%20m%C3%B3vil%20o%20un%20ordenador.

9. Especialistas Hosting. Alojamos tus ideas. (julio 2016). ¿Qué es PHP? y ¿Para qué sirve? recuperado de: https://www.especialistashosting.com/blog/index.php/2016/07/que-es-php-y-para-que-sirve/

10. CriptoNoticias. (abril 2021). IPFS: el protocolo de almacenamiento descentralizado que sustituiría a los HTTP. recuperado de: https://www.criptonoticias.com/tecnologia/ipfs-protocolo-almacenamiento-descentralizado-sustituiria-http/#:~:text=IPFS%20son%20las%20siglas%20de,de%20una%20red%20P2P%20global.

11. MDN web docs. (diciembre 2020). Trabajando con JSON. recuperado de:

https://developer.mozilla.org/es/docs/Learn/JavaScript/Objects/JSON

12. MDN web docs. (diciembre 2020). XML: Extensible Markup Language. recuperado de: https://developer.mozilla.org/es/docs/Web/XML

13. Andalucía de Digital. (julio 1999). Educar para Proteger. recuperado de: https://www.andaluciaesdigital.es/educarparaproteger/adolescentes/capitulos/perfilestics/red es-p2p.html#:~:text=P2P%20(Peer%20to%20Peer)%20significa,en%20la%20generaci%C3%B3n%20m%C3%A1s%20avanzada.

14. Diario Bitcoin. (marzo 2021). Tolerancia a Fallas Bizantinas. recuperado de: https://www.diariobitcoin.com/glossary/byzantine-fault-tolerance-bft-tolerancia-a-fallas-bizantinas/

15. Alcaldiabogota.gov.co. (2022). Documentos para datos personales. Recuperado de: https://www.alcaldiabogota.gov.co/sisjur/listados/tematica2.jsp?subtema=27077

16. ISACA. (2020). Blockchain Framework and Guidance.

17. Deloitte EMEA. (2018). Blockchain & Ciberseguridad. Risk Advisory.

18. Instituto Colombiano de Normas Técnicas. (2013, diciembre). NORMA TÉCNICA

COLOMBIANA NTC-ISO.IEC 27001 (Primera actualización). ICONTEC.

19. ISO. (2022, febrero). INTERNATIONAL STANDARD ISO/IEC 27002 (Tercera edición). ISO/IEC 2022.

20. Grantthornton.es. (2018). RGPD Y Blockchain. recuperado de https://www.grantthornton.es/globalassets/1.-member-firms/spain/folletos/rgpd-y-blockchain-final.pdf

21. *¿Qué es la seguridad de blockchain? | IBM*. (s. f.). IBM. Recuperado 2022, de https://www.ibm.com/es-es/topics/blockchain-security

22. StorJ. (s. f.). *DCS*. (2022). Storj Docs. Recuperado de https://docs.storj.io/dcs/

23. Sia - Decentralized data storage. (2022). (s. f.). SIA. Recuperado de https://sia.tech/

24. docs.ipfs.io. (2022). Recuperado de https://docs.ipfs.io/

7. SOBRE LOS AUTORES

R.A. Acevedo Rodríguez. Nació en Bogotá, Colombia. Candidata a especialista de la Fundación Universitarias Los Libertadores. Es ingeniera de sistemas de la Universidad Incca de Colombia. Email: aacevedor@libertadores.edu.co Certificada como Auditor líder e interno en ISO 27001:2013 e ISO 22301:2013 así como en ITIL fundamentos y Cisco Certified Network Associate (CCNA) introducción y fundamentos en conmutación y enrutamiento. Con conocimiento y experiencia en la implementación y operación de sistemas de gestión de seguridad de la información, sistemas de gestión de continuidad de negocio y administración de plataformas de seguridad informática en empresas del sector público y privado.

F. Ospina González Nació en Bogotá Colombia. Candidato a especialista de la Fundación Universitarias Los Libertadores. Email: faospinag@libertadores.edu.co. Es Ingeniero de Sistemas de la Universitaria de Colombia con orientación profesional a la gestión de recursos y proyectos en áreas de tecnología según lineamientos de ITIL, experiencia en implementación y administración de equipos con plataforma Microsoft, Linux y VmWare, con capacidad de liderazgo, planeación y direccionamiento estratégico, toma de decisiones, desarrollo de ideas que permitan hallar soluciones óptimas e integrales y que le ayudan al mejoramiento continuo de las organizaciones.

G. Tapiero Velasquez. Nació en Bogotá D.C. Colombia. Candidato a especialista de la Fundación Universitarias Los Libertadores. Email: gtapierov@libertadores.edu.co. Es Especialista en Informática para el Aprendizaje en Red de la Fundación Universitaria Los Libertadores e Ingeniero

de Sistemas de la Fundación Universitaria Los Libertadores. Cursó un Diplomado en Administración de S.O. y Redes LINUX: LPIC – 1 en la Fundación de Egresados U. Distrital y otro Especializado en Gerencia y Programación de Proyectos PMI en la Fundación Universitaria CAFAM. Es administrador de la Herramienta de Monitoreo Dynatrace, perteneciente a la Vicepresidencia de Tecnología en el Banco Itaú.

Y.I. Serrato Rodríguez. Nació en Bogotá, Colombia. Especialista en Seguridad de la Información de la Universidad Sergio Arboleda e Ingeniero en Telemática de la Universidad Distrital Francisco José de Caldas. Email: yiserrator@libertadores.edu.co. Es certificada como: CEH, Auditor Líder e interno ISO 27001:2013, Auditor interno ISO 22301:2019, ITIL, Cobit, Scrum Foundations, entre otros. Adicional, posee conocimientos en informática forense, ciberseguridad, auditoría interna y manejo de proyectos. Se ha desempeñado como Oficial de seguridad de la información para empresas multinacionales, consultor para empresas públicas y privadas liderando equipos de trabajo multidisciplinarios además docente universitario en varias universidades.