Institución Universitaria

Metodología para la adaptación y aplicación de blockchain en el proceso de facturación de una Empresa de servicios públicos

María Isabel Cano Cano

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2022

Metodología para la adaptación y aplicación de blockchain en el proceso de facturación de una Empresa de servicios públicos

María Isabel Cano Cano

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director (a):

MSc. Alicia Osorio Builes

Línea de Investigación:

Ciencias computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2022

Si no puedes volar, corre.

Si no puedes correr, camina.

Sino puedes caminar, gatea.

Pero hagas lo que hagas,

Siempre sigue hacia adelante.

Martin Luther King

Agradecimientos

Mi más sincero agradecimiento a mi asesora en esta investigación, MSc. Alicia Osorio, y a Héctor Vargas Montoya por su acompañamiento, su apoyo, su tiempo, y los conocimientos que me han compartido durante el desarrollo de mi tesis.

Igualmente, mi reconocimiento y agradecimiento a cada uno de mis profesores y a quienes participaron en la revisión y aprobación de mi trabajo de grado, porque con cada una de sus contribuciones aportaron a la construcción de éste.

A mis padres por el apoyo incondicional, confiar en mí, motivarme e impulsarme a ser siempre mejor y a luchar por mis sueños.

Finalmente, a Dios por ser mi guía.

Resumen

El presente proyecto de investigación establece una metodología, a través de la adaptación y aplicación de blockchain en los procesos de facturación de las empresas de servicios públicos domiciliarios, que permita mitigar los riesgos de seguridad de la información, hacer seguimientos de principio a fin en línea, disminuir tiempos de ejecución, y asegurar la integridad, disponibilidad y confidencialidad de la información en cada fase que compone dicho proceso. Para lograr los objetivos propuestos se inició con la construcción de un mapa de riesgos general, que puede aplicarse al proceso de facturación de las empresas de servicios públicos domiciliarios. A partir de éste, y de la identificación de amenazas y vulnerabilidades inherentes a dicho proceso, se construyeron controles de seguridad que disminuyen los riesgos. Así mismo, se estudió sobre la tecnología blockchain y sus diversos usos, lo que permitió por medio de la obtención y recopilación de unas mejores prácticas, proponer una metodología de adaptación y aplicación, la cual se validó comparando el método tradicional y aplicando la tecnología ya mencionada.

Paralelamente se estudiaron los procesos de facturación de diferentes empresas, encontrando que independientemente de la industria, tamaño y destinación, éstas incluyen la facturación como requisito legal, enfocándose en la venta o prestación de un producto o servicio, respectivamente, el cual conlleva a un costo y a la solicitud de su pago. Las empresas de servicios públicos domiciliarios segmentan las actividades que se ejecutan en sus procesos de facturación, cumpliendo con la normatividad vigente colombiana, los Contratos de Condiciones Uniformes, y demás directrices expedidas por entidades como: la Superintendencia de Servicios Públicos Domiciliarios (SSPD), la Comisión de Regulación de Energía y Gas (CREG), y la Comisión de Regulación de Agua Potable y Saneamiento (CRA). Esta segmentación surge por las etapas que deben surtirse antes de emitir la factura y por los actores que intervienen, condiciones que, acrecientan los riesgos y brechas de seguridad que pueden comprometer la continuidad del negocio; brechas causadas por amenazas, vulnerabilidades, errores humanos, aspectos legales, falta de comunicación, control y seguimiento, entre otras, las cuales exigen ajustes y correcciones, dadas las afectaciones del curso natural del proceso, su funcionamiento, validez y resultado.

Palabras clave: Blockchain, ciberataque, factura, proceso de facturación, seguridad de la información, vulnerabilidad

Abstract

This research project establishes a methodology, through the adaptation and application of blockchain in the billing processes of home public service companies, which allows mitigating information security risks, monitoring from start to finish online, reduce execution times, and ensure the integrity, availability, and confidentiality of the information in each phase that makes up said process. In order to achieve the proposed objectives, the construction of a general risk map began, which can be applied to the billing process of residential public utility companies. From this, and from the identification of threats and vulnerabilities inherent to said process, security controls were built to reduce risks. Likewise, blockchain technology and its various uses were studied, which allowed, through obtaining and compiling best practices, to propose an adaptation and application methodology, which was validated by comparing the traditional method and applying the technology already used.

At the same time, the billing processes of different companies were studied, finding that regardless of the industry, size, and destination, they include billing as a legal requirement, focusing on the sale or provision of a product or service, respectively, which entails a cost. and upon request for payment. Home public service companies segment the activities that are carried out in their billing processes, complying with current Colombian regulations, the Uniform Conditions Contracts, and other guidelines issued by entities such as: the Superintendence of Home Public Services (SSPD), the Commission for the Regulation of Energy and Gas (CREG), and the Commission for the Regulation of Potable Water and Sanitation (CRA). This segmentation arises from the stages that must be completed before issuing the invoice and from the actors involved, conditions that increase the risks and security gaps that can compromise business continuity; gaps caused by threats, vulnerabilities, human errors, legal aspects, lack of communication, control, and monitoring, among others, which require adjustments and corrections, given the effects of the natural course of the process, its operation, validity and result.

Keywords: Bloc kchain, cyber attack, bill, billing process, information security, vulnerability

Contenido

Lista de figuras

Lista de tablas

Lista de símbolos y abreviaturas

Abreviatura	Término
CRA	Comisión de Regulación de Agua Potable y Saneamiento
CREG	Comisión de Regulación de Energía y Gas
CVE	Common Vulnerabilities and Exponsures
DNS	Domain Name System
DLT	Distributed Ledger Technology
ESP	Empresa de servicios públicos
IBM	International Business Machines Corporation
INCIBE	Instituto Nacional de Ciberseguridad
IRC	Internet Relay Chat
NIST	National Institute of Standards and Technology
NVD	Base de datos nacional de vulnerabilidades
OMS	Organización mundial de la salud
SIC	Superintendencia de Industria y Comercio
SPD	Servicios públicos domiciliarios
SSPD	Superintendencia de Servicios Públicos Domiciliarios
TI	Tecnologías de la información

Introducción

La factura como requisito legal para realizar el cobro por la venta de un producto o servicio incluye una serie de procesos y procedimientos que son ejecutados por diferentes colaboradores en distintos aplicativos, lo que hace necesario asegurar la información del proceso completo desde que se programa la facturación hasta que se entrega el documento al cliente y usuario. Por este motivo, con la presente tesis de maestría, se pretende aportar mayor seguridad a la información de los procesos de facturación de las empresas de servicios públicos domiciliarios, estableciéndose el siguiente objetivo general: "Proponer una metodología para la implementación de blockchain, con el fin de reducir riesgos presentes en el proceso de facturación de las Empresas de Servicios Públicos Domiciliarios". Igualmente, para lograr este objetivo, se propusieron los siguientes objetivos específicos:

- "Identificar las posibles amenazas y vulnerabilidades del proceso de facturación, a partir de la realización de un mapa de riesgos".

- "Caracterizar las diferentes soluciones o controles de seguridad tradicionales del proceso de facturación, para construir uno con las mejores prácticas".

- "Evaluar diferentes usos que se han dado utilizando blockchain, y recopilar de estas experiencias las mejores prácticas que puedan ser aplicadas en la reducción de riesgos del proceso de facturación, con el fin de proponer una metodología de implementación".

- "Validar el diseño de la metodología, a través de la comparación entre un modelo tradicional de protección y la tecnología blockchain".

En Colombia, los servicios públicos domiciliarios se rigen bajo diferentes normas y conceptos que determinan la forma por medio de la cual debe gestionarse su prestación, y que, a su vez, determinan cada proceso y procedimiento desde su solicitud, hasta su posterior facturación.

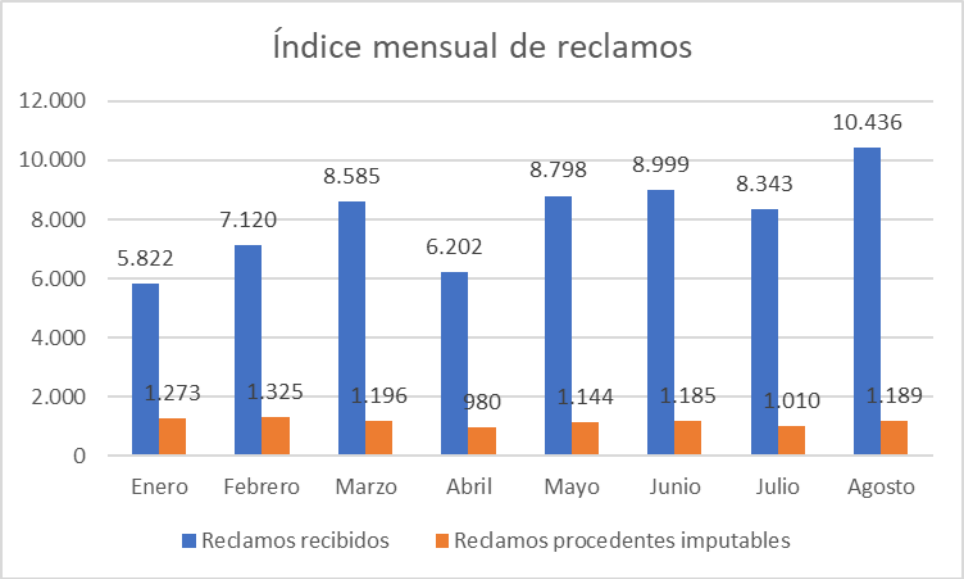
De acuerdo con lo anterior, se considera importante citar el artículo 1 de la Ley 142 de 1994 "Por la cual se establece el régimen de los servicios públicos domiciliarios y se dictan otras disposiciones". “ARTICULO 1. Ámbito de aplicación de la ley. Esta ley se aplica a los servicios públicos domiciliarios de acueducto, alcantarillado, aseo, energía eléctrica, distribución de gas combustible, telefonía fija pública básica conmutada y la telefonía local móvil en el sector rural; a las actividades que realicen las personas prestadoras de servicios públicos de que trata el artículo 15 de la presente ley, y a las actividades complementarias definidas en el Capítulo II del presente título y a los otros servicios previstos en normas especiales de esta ley” [1] .

Actualmente, las Empresas de Servicios Públicos cuentan con la información de sus clientes y usuarios en lo que se refiere a sus datos personales y de sus inmuebles. Aunado a esto, el proceso de facturación está compuesto por diversas actividades que se relacionan entre sí, y son ejecutadas por diferentes colaboradores que desarrollan funciones distintas dentro de la Organización.

Lo anterior representa un verdadero reto para la Organización, toda vez que adicionalmente a garantizar el funcionamiento de su proceso completo de facturación, también debe salvaguardar los datos personales de sus clientes y usuarios, todo basados en el cumplimiento de la normatividad vigente y bajo los parámetros de seguridad y ciberseguridad pertinentes. Igualmente, es importante mencionar que, paralelo al crecimiento de la Organización, también se acrecientan los riesgos y vulnerabilidades.

Igualmente, es pertinente considerar la cantidad de reclamos que presentan los usuarios ante las Empresas de Servicios Públicos Domiciliarios por desacuerdos con sus facturas, los cuales pueden presentarse, entre otras, como resultado de manualidades, la intervención de diferentes colaboradores y las múltiples actividades implícitas en el proceso de facturación. Así las cosas, a continuación, se expone la figura 0-1, en la que se muestra el índice mensual de reclamaciones que una Empresa de Servicios Públicos Domiciliarios atendió entre enero y agosto de 2022:

Figura 0-1: Índice mensual de reclamos



Nota. Índice mensual de reclamos. Grafica construida con información tomada del índice mensual de reclamos por valores, de una Empresa de Servicios Públicos Domiciliarios [2]

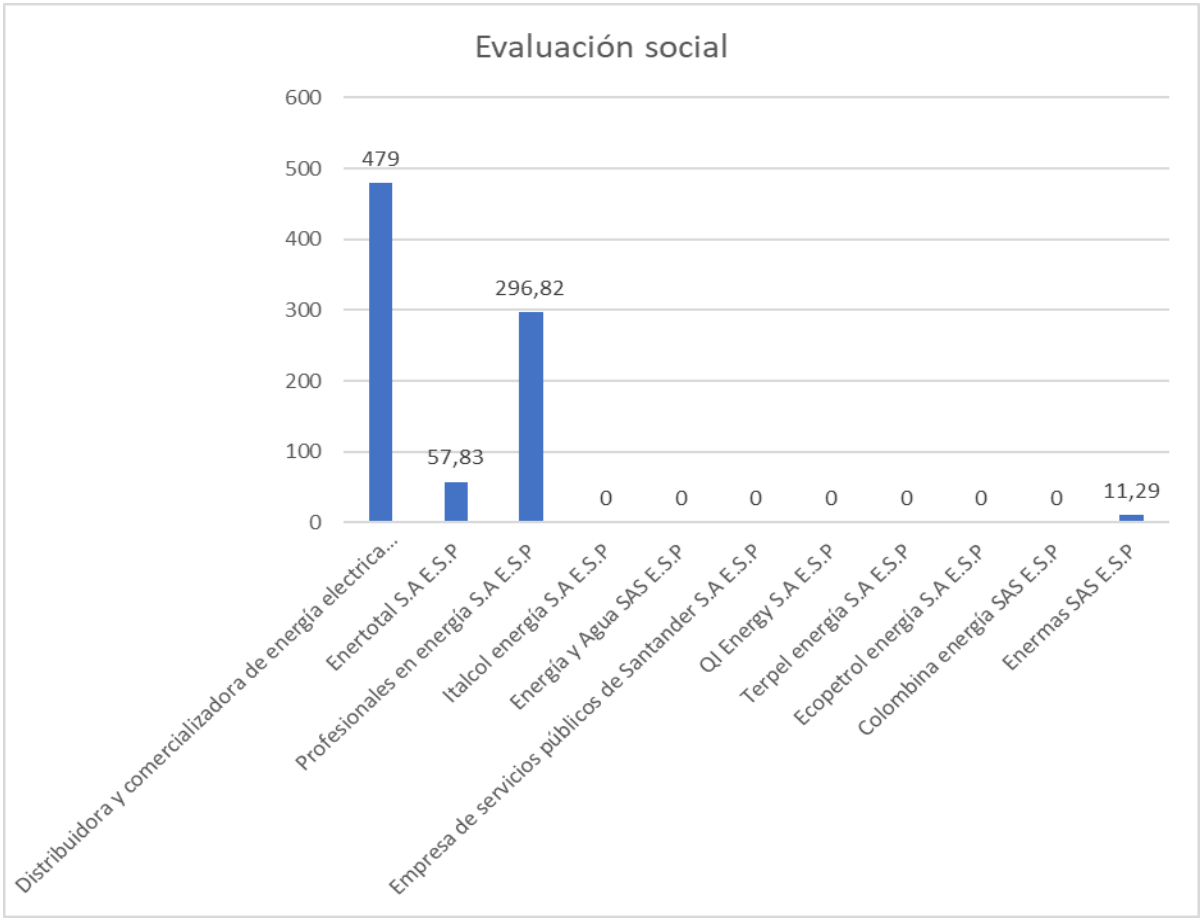
De la gráfica anterior, puede inferirse que, en una de las Empresas de servicios públicos del país, durante los meses de enero, febrero, marzo, abril, mayo, junio, julio y agosto del año 2022, se presentaron 64.305 reclamos, de los cuales, 9.302 fueron imputables a la Empresa. Es decir, el 14,46% de los reclamos sobre la facturación, se resolvió a favor del cliente, lo que significa acceder parcial o completamente a las reclamaciones, perder el derecho al cobro y/o devolver el dinero [3]. Observando esto, se evidencia que el proceso de facturación tiene brechas que deben cerrarse para así minimizar el número de reclamaciones y el porcentaje procedente de las mismas.

Con base en lo anterior, se explica que un reclamo es el "Derecho que tiene toda persona por motivo general o particular, referente a la prestación indebida de un servicio o a la falta de atención de una solicitud, incluidos los actos de corrupción realizados por funcionarios de la entidad, y de los cuales tenga conocimiento, así como sugerencias que permitan realizar modificaciones a la manera como se presta el servicio público" [4]. Los reclamos pueden ser favorables total o parcialmente al cliente y usuario, o también completamente negados.

Así mismo, a la Superintendencia llegan quejas, reclamos, recursos de reposición en subsidio de apelación, y demás acciones que los clientes pretendan interponer en contra de los prestadores de servicios públicos domiciliarios. Al consultar en dicha Superintendencia, se encuentran los Indicadores técnicos y administrativos del año 2021 asociados al servicio de energía, los cuales se determinan con base en un referente calculado, de la siguiente manera: (número reclamos de facturación/facturas expedidas) *10.000, esto de acuerdo con la Resolución CREG 072 de 2002 y su modificatoria. En el resultado de los indicadores se obtienen las etiquetas “CUMPLE” y “NO CUMPLE”, lo que evidencia el nivel de cumplimiento por Empresa [5].

De acuerdo con lo anterior, en la figura 0-2, se muestran los resultados de gestión de reclamaciones por facturación de energía de algunas Empresas de Servicios públicos, teniendo como referencia de cumplimiento: <=182.42. Con base en esto, de 11 empresas 2 incumplen los indicadores:

Figura 0-2: Evaluación social



Nota. Evaluación social. Gráfica construida con información obtenida de la Superintendencia de Servicios públicos Domiciliarios [5].

Las empresas que no cumplieron con los indicadores son: Distribuidora y comercializadora de energía electrica S.A E.S.P y Profesionales en energía S.A E.S.P, toda vez que las facturas reclamadas superaron el índice establecido según las facturas emitidas [5].

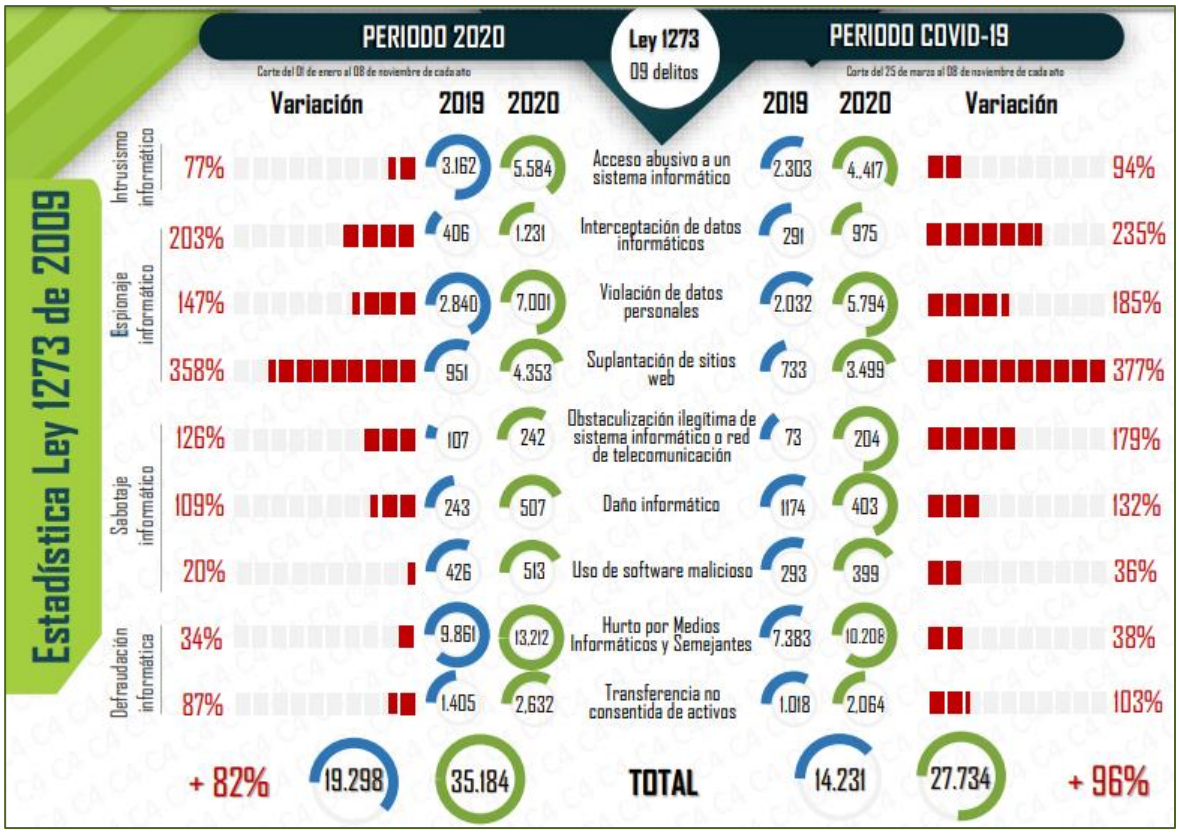
Con base en la cantidad de reclamos asociados a la facturación, los cuales se presentan comúnmente en las empresas de servicios públicos, es pertinente pensar en darle mayor prioridad a las bondades de emplear nuevas tecnologías como blockchain en los procesos de facturación de dichas empresas, en pro de aumentar sus niveles de seguridad, ciberseguridad y rendimiento, mejorar la operación, tener trazabilidad, costo beneficio, y dejando en un nivel de prioridad inferior estudios como el de Capgemini, que menciona que el 92% de las empresas consideran que recuperar la inversión aplicando blockchain puede ser tardío [6].

Por otro lado, sobre los ciberataques, se encuentra que según las Tendencias Cibercrimen Colombia 2019 – 2020, se identificó una modalidad en la que engañan a los clientes para que hagan pagos de sus facturas y el dinero sea abonado a las cuentas de los atacantes. Para retirar los dineros, se usan cuentas bancarias con datos de las empresas afectadas mediante ingeniería social. [7]

Así mismo, de acuerdo con el último balance de Cibercrimen emitido por el Centro Cibernético Policial con base en la ley 1273 de 2009 (delito informático) de la semana 45 del año 2020 [8], ha habido un aumento bastante significativo de los ciberdelitos con respecto al año 2019, y más aun con respecto al periodo de pandemia, en particular, cada uno de los delitos allí destacados, puede afectar directa o indirectamente el proceso de facturación de las Organizaciones, por lo que se resalta la necesidad de revisar el proceso actual en términos de riesgos y controles, y la posibilidad de incluir tecnologías disruptivas.

En la siguiente figura 0-3, se muestra la estadística donde se evidencia que entre los años 2019 y 2020 el ciberdelito incrementó, aún más, durante la pandemia, debido al aumento en el uso de internet y las comunicaciones por la necesidad de realizar las labores académicas y educativas desde la residencia, situación que fue directamente proporcional con las amplias posibilidades que se le presentaron a los ciberdelincuentes de atacar:

Figura 0-3: Denuncias Ley 1273 – 2019/2020



Nota. Comparativo de denuncias en la Policía Nacional de Colombia, bajo la ley 1273 de 2009[8].

Basados en la figura anterior, entre el año 2019 y 2020 comparando desde enero, el incremento en los delitos fue de 82%. Así mismo, en tiempos de pandemia, el incremento fue mucho más alto, del 96%.

Por lo tanto, se pretende diseñar una propuesta metodológica para la adaptación e implementación de la tecnología blockchain, la cual permita mejorar los procesos de facturación, propendiendo por una factura que contenga la información precisa y correspondiente según los consumos reales de los usuarios, registros de datos inmodificables en tiempo real sin recurrir a mediadores, que facilite cada actividad del proceso completo, proporcione eficiencia, rentabilidad, medición permanente, evite fraudes, y que además, permita que los involucrados tengan amplia y plena visibilidad del proceso [6]. Esta se validó a partir de la investigación que se hizo sobre el proceso de facturación, sus riesgos, controles y mejores prácticas, tanto en bases de datos científicas como en las mismas empresas donde ese es su día a día; la creación de un proceso global de facturación y mapa de riesgos aplicables a cualquier empresa del sector, recopilación de riesgos,

controles y mejores prácticas de las empresas encuestadas; el acogerse a nuevas metodologías y metodologías ágiles. Además, del estudio sobre blockchain y ratificar que se ha aplicado en diferentes procesos, en los cuales sus bondades ya fueron identificadas y debidamente medidas, con porcentajes que soportaron los resultados.

En el informe se mostrará el cumplimiento secuencial cada uno de los objetivos planteados, e igualmente se desarrollarán los siguientes apartes: Marco teórico, estado del arte, metodología, resultados, conclusiones, recomendaciones y anexos.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

Con el presente trabajo, se propuso una metodología para la aplicación e implementación de blockchain en el proceso de facturación de las ESP, con el propósito de reducir los riesgos presentes en dicho proceso y mejorar la calidad de este. Por lo tanto, a continuación, se definirán algunos conceptos relacionados:

1.1.1 Proceso de facturación

Es un conjunto de actividades que le permiten a una Empresa de servicios públicos, mantener actualizada la información de los suscriptores que están haciendo uso de los servicios de energía, acueducto, alcantarillado y aseo, con el ánimo de generarles facturas de los servicios prestados, asentar los pagos realizados, las financiaciones solicitadas, generar balances e informes correspondientes a lo facturado y recaudado, informes relacionados con los consumos y vertimientos por estratos y/o categorías ocasionados en el mes, actualizar tarifas y un sin número de informes que pueden apoyar a la Empresa en la implementación de políticas y tareas a realizar con esta información [9].

Es así que, el proceso de facturación de las ESP permite incluir los valores causados y realizar cobros por los servicios prestados a sus clientes y usuarios.

Así mismo, es importante mencionar que cada empresa de servicios públicos diseña su propio proceso de facturación. Por ejemplo, la Empresa Semtec plantea sus actividades buscando calidad en la operación de los servicios de acueducto, alcantarillado y aseo, tiene un sistema que le permite realizar el cobro de estos servicios, hacer la lectura de medidores y entrega de facturas. En la tabla 1-1, se observa que su proceso está compuesto por las siguientes 12 actividades [9]:

Tabla 1-1: Proceso de facturación Semtec

Número de actividad	Descripción
1.	Verificación de suscriptores
2.	Configuración de datos del municipio
3.	Creación de usuarios en la base del municipio
4.	Configuración de usos y categorías usuarios prospecto
5.	Configuración de servicios a facturar
6.	Configuración de tarifas
7.	Configuración de cobros adicionales
8.	Configuración del tipo de factura
9.	Creación de usuarios en la aplicación de los suscriptores
10.	Liquidación de los cobros
11.	Generación de informes
12.	Elaboración de copias de seguridad

Nota. Proceso de facturación Semtec [9]

Otro ejemplo es Empresas Públicas de Medellín, la cual presta los servicios de energía, acueducto, alcantarillado y gas en Antioquia y otros departamentos a través de sus empresas filiales. En la tabla 1-2, se describen las 10 actividades inmersas en su proceso:

Tabla 1-2: Proceso de facturación Empresas públicas de Medellín

Número de actividad	Descripción
1.	Programación de la factura
2.	Lectura y revisión de medidores
3.	Análisis de consumos
4.	Identificación e incorporación de cobros en la factura
5.	Cálculo tarifario e ingreso de tarifas
6.	Aplicación de reglas de liquidación
7.	Verificación de calidad de la factura
8.	Generación de facturas por suscriptor

Número de actividad	Descripción
9.	Distribución de facturas
10.	Generación de información contable y estadística de la facturación

Nota. Proceso de facturación EPM [10]

1.1.2 Factura

La factura contiene el detalle del producto o servicio vendido y es el medio por el cual se solicita el cumplimiento de la obligación, por lo tanto, el documento debe cumplir con los diferentes requisitos que se encuentran descritos en la normatividad vigente. Aunado a lo anterior, se detalla que:

> Una factura es un documento de carácter mercantil que indica una compraventa de un bien o servicio y que, entre otras cosas, debe incluir toda la información de la operación. Podemos decir que es una acreditación de una transferencia de un producto o servicio tras la compra de este. Es así pues que una factura sirve para demostrar la entrega de un producto o servicio tras su compra a modo de justificante [11].

Según el Decreto 358 de 2020 en el artículo 615 del Estatuto Tributario dispone: "Obligación de expedir factura; para efectos tributarios, todas las personas o entidades que tengan la calidad de comerciantes ejerzan profesiones liberales o presten servicios inherentes a éstas, o enajenen bienes producto de la actividad agrícola o ganadera, deberán expedir factura o documento equivalente, y conservar copia de la misma por cada una de las operaciones que realicen, independientemente de su calidad de contribuyentes o no contribuyentes de los impuestos administrados por la Dirección General de Impuestos Nacionales(...)" [12]

Por otro lado, la factura de servicios públicos domiciliarios se define como “la cuenta que una persona prestadora de servicios públicos entrega o remite al usuario, por causa del consumo y demás servicios inherentes en desarrollo de un contrato de prestación de servicios públicos” (Elias et al., 1994, p.9).

Así mismo, estas deben tener controles estrictos que garanticen su correcta emisión en términos de calidad y cantidad, y que se minimicen errores de elaboración, costos innecesarios, cálculos inadecuados, información incorrecta, incumplimiento de la norma, entre otros. Para el caso de

servicios públicos, antes de emitir una factura, la empresa prestadora realiza procedimientos de lectura, medición, análisis y tasación de consumos, para posteriormente liquidarlos. Una vez cuenta con la información, se genera el documento que también debe contener datos que son obligatorios según la normatividad vigente (nombre, número de identificación, dirección, consumos de cada servicio, tarifas, periodo de facturación, fecha de vencimiento, entre otros), para así ser entregado al cliente y usuario, quien al conocer el detalle del servicio que se le prestó, las condiciones como cliente y las condiciones de pago, tiene la potestad de aceptar lo facturado o presentar posibles reclamaciones y/o recursos de ley que considere [1].

Sobre los requisitos que deben cumplir las facturas de servicios públicos domiciliarios, en el artículo 148 de la Ley 142 de 1994 se especifica que estos serán los establecidos en los contratos de condiciones uniformes, los cuales tienen definidas las condiciones mediante las cuales las empresas prestan los servicios. También especifica que la factura debe presentar la información con la que se determinó el consumo y su costo, además evidenciar que se cumplió con la normatividad vigente para su emisión [1]. Con base al cumplimiento de requisitos, es preciso resaltar que la Superintendencia de Servicios Públicos Domiciliarios, es la entidad que inspecciona, vigila y controla las empresas prestadoras de los servicios de energía, acueducto, alcantarillado, gas y aseo [4].

Por otro lado, a partir del año 2015 surge el concepto de facturación electrónica, que según el Decreto 2242 es emitida y almacenada en medios electrónicos, tiene la misma validez legal que una factura física y contiene datos íntegros que permiten verificar el producto o servicio que se le entrega al cliente. Implementarla, redundaría en la mitigación de inconsistencias, mayor control y calidad de los procesos y disminución de costos y tiempos de ejecución. A su vez, la facturación electrónica representa evolución, fiabilidad, integridad, cumplimiento de la normatividad, seguridad, mejoras y confianza en la prestación del servicio, mayor acceso digital, comunicación con entidades gubernamentales, entre otras [11].

1.1.3 Seguridad de la información

"La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información" [13]. A partir de la evolución y transformación tecnológica, las empresas son más vulnerables a la materialización de ataques y ciberataques. Incluso cada vez es más

común que la información de las organizaciones sea menos confidencial, esté expuesta y, por lo tanto, sea conocida y accedida fácilmente con y sin autorización. Motivo por el cual, es imperativo reiterar la necesidad de propender por la seguridad de esta, para lo que se cita lo indicado en la Norma ISO-27000 sobre el propósito de la seguridad de la información: "es proteger y preservar la confidencialidad, integridad y disponibilidad de la información. También puede implicar proteger y preservar la autenticidad y fiabilidad de la información y garantizar que las entidades puedan ser consideradas responsables" [14].

A continuación, se definirán las tres dimensiones de la seguridad de la información:

- **Confidencialidad**: "es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado para acceder a dicha información" [15]. Hace referencia a que solo personal autorizado puede acceder a la información.

- **Integridad**: "es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales" [15]. Garantiza que la información esté libre de modificaciones, errores y no esté adulterada.

- **Disponibilidad**: "capacidad de un servicio, un sistema o una información a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran" [15]. Es decir, se refiere a que la información sea accesible en el momento que se requiera.

Así mismo, existen salvaguardas o medidas de seguridad, que se toman para proteger la información. Previamente a tomar las salvaguardas se debe caracterizar la información según su legalidad, criticidad, daño reputacional, entre otros, y clasificarla en términos de privacidad, como confidencial, interna y pública. Posteriormente, se establece el tipo de medidas a implementar, que para el caso serían técnicas, organizativas y físicas [16].

De acuerdo con INCIBE, en su escrito ¿Sabes qué es el Día Internacional de la Seguridad de la Información? [16], las siguientes son algunas medidas básicas para la seguridad de la información:

- Control de acceso a la información: segregación de funciones y seguir el principio del mínimo privilegio
- Copias de seguridad: preservar la información de hurto o pérdida.
- Cifrado de la información: emplear técnicas criptográficas y utilizar claves robustas.
- Desechado o reutilización de soportes y equipos: borrados seguros que eviten la recuperación de información de equipos desechados y documentos.
- Almacenamiento en la nube: almacenamiento de información en servicios de la nube.

Aunado a lo anterior, es importante tener en cuenta el documento mediante el cual se establecen las directrices asociadas a la seguridad de la información, es decir, las políticas de seguridad, las cuales "son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos" [15].

Debido a las brechas y vulnerabilidades que constantemente están presentes en las Organizaciones y en sus sistemas, sus diferentes procesos y activos se encuentran en constante riesgo, y frente a la posibilidad de no obtener los resultados deseados, se considera importante gestionar dichos riesgos con base en actividades como: Compromiso de la alta y media dirección, conformación de un grupo inter disciplinado que tenga visión completa de la Entidad y la capacitación en la metodología [17].

1.1.3.1 Norma Técnica Colombiana 27001

Otro de los puntos importantes relacionados con la seguridad de la información, son los asociados con los 14 dominios de la Norma Técnica Colombiana 27001. Estos dominios tecnológicos son aplicados sobre los procesos que ya tienen establecidos las Organizaciones en pro de gestionar dicha seguridad de la información. De acuerdo con lo anterior, a continuación, se resaltan aquellos dominios que apuntan a asegurar el presente proyecto de investigación [18]:

Tabla 1-3 Dominios de la Norma Técnica ISO 27001 que apuntan a la seguridad del presente proyecto

DOMINIO	¿PORQUÉ APUNTA A LA SEGURIDAD DEL PRESENTE PROYECTO?
A.5 POLÍTICA DE SEGURIDAD	Porque en la propuesta se consideraron las políticas de seguridad ya establecidas en la Organización, toda vez que, deben cumplirse ya que son acordes al negocio, reglamentos y normatividad.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Porque en la propuesta: *Se contempló la segregación de funciones definida por la Organización. *Se contó con las autorizaciones requeridas para las modificaciones que se presenten con el almacenamiento de la información. *Se contempló cumplir con los acuerdos de confidencialidad establecidos. *Se mencionó la importancia de tener contacto permanente con los grupos de interés *Se identificaron los riesgos y controles de información que tienen los terceros
A.7 GESTIÓN DE ACTIVOS	Porque se identificaron los activos inmersos en el proceso de facturación de las empresas de servicios públicos domiciliarios, con el fin de realizar el mapa de riesgos asociado a la información.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES	Porque con la tecnología blockchain se almacena la información de tal modo que para modificarla se requiere consenso entre los nodos autorizados.
A.11 CONTROL DE ACCESO	Porque con la metodología propuesta se tuvo presente la verificación con los líderes respectivos para la revisión del proceso de facturación, entre lo que se encuentra el control de acceso a la aplicación.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	Porque: *Con la adaptación e implementación de blockchain se tienen medidas se seguridad que protegen la integridad y aseguran la autenticidad de los datos. *Se tiene el manejo de nodos con información cifrada y uso de hashes.

DOMINIO	¿PORQUÉ APUNTA A LA SEGURIDAD DEL PRESENTE PROYECTO?
A.15 CUMPLIMIENTO	Porque: *Al iniciar la metodología propuesta se incluyó el conocimiento del negocio y del proceso de facturación de la Organización, lo que incluye la normatividad que lo rige. *La propuesta cumple con requisitos asociados a la seguridad de la información

Nota. Fuente propia

1.1.3.2 Ley 1581 de 2012

"Artículo 1°. Objeto. La presente ley 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 bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Artículo 2°. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales" [19]

Con base en lo anterior, la SSPD indicó que esta ley resulta exigible para las empresas del sector de los servicios públicos domiciliarios, toda vez que hace tratamiento de los datos personales de sus clientes y usuarios, so pena de recibir sanciones por parte de la Superintendencia de Industria y Comercio, en adelante SIC. En concordancia con ello, estas empresas solo podrán obtener o divulgar información con previa y expresa autorización [20].

De acuerdo con estudio realizado por la SIC, 33.596 empresas públicas, 24.424 Organizaciones públicas y privadas, no tienen mecanismos eficientes para asegurar los datos personales de sus clientes. Adicionalmente, 20.594 no han implementado las medidas requeridas para proteger datos sensibles.

Aunque al comparar estos resultados con los obtenidos en el año 2019, hubo una mejoría del 12.73% en el cumplimiento de medidas de seguridad. Como lo manifestó el Superintendente de Industria y comercio, cumplir con la Ley de Protección de datos personales, otorga mayor seguridad y por ende confianza en los clientes, además, se mitigan las posibilidades de afectar los intereses de las Organizaciones. En la siguiente tabla, se evidencia el porcentaje de cumplimiento asociado a medidas de seguridad [21]:

Tabla 1-4 Comparativo de estudio de seguridad 2019-2020

	2019	2020
Número de organizaciones evaluadas	32.763	33.596
No tienen una política de protección para acceso remoto a la información personal	88%	72.7%
No cuenta con mecanismos de monitoreo de consulta de las bases de datos	84%	69.3%
No ha implementado un procedimiento de auditoria de los sistemas de información	83%	71.3%
No tiene implementado un sistema de gestión de seguridad o un programa integral de gestión de datos	82%	67.5%
No ha implementado medidas especiales para proteger datos sensibles	79%	61.3%
No ha implementado una política de seguridad para el intercambio físico o electrónico de datos	76%	66.1%
No tiene política de auditoria de seguridad de la información	72%	63.6%
No tiene controles de seguridad en la tercerización de servicios para el tratamiento de datos	71%	61%
No implementa medidas apropiadas y efectivas de seguridad	66%	50.7%
No cuenta con herramientas de gestión de datos	63%	49.9%
No tiene políticas y procedimientos de gestión de incidentes de seguridad	62%	52.6%
Promedio de incumplimiento respecto de los ítems evaluados	75.09%	62.36%

Nota. Resultados de los años 2019-2020 del estudio de seguridad [21]

Por otro lado, y en concordancia con el presente proyecto, se hace pertinente informar que adaptando y aplicando blockchain en el sistema de facturación de una empresa de servicios públicos, se posibilita el cumplimiento de la Ley 1581 de 2012, debido a que esta tecnología tiene bondades como el consenso en sus transacciones, inmutabilidad, transparencia ay cifrado, lo que permite mantener la

integridad de los datos y evidenciar si los datos llegan a ser manipulados de forma inadecuada o fraudulenta [22].

Adicionalmente, entre las propiedades de blockchain está la confidencialidad, es decir, la cadena de bloques garantiza que la información confidencial no sea expuesta y solo accedan a ella personas debidamente autorizadas. Otra de sus propiedades es la integridad, que en términos de datos, cuenta con opciones como firma digital y el cifrado a través de hash, de modo que el valor enviado es el mismo recibido, y de encontrarse alguna alteración sería detectada [22]. Así las cosas, blockchain aporta a la protección de información sensible a nivel de la base de datos, de las aplicaciones y el proceso, lo que permitire que el número de sanciones que impone la SIC disminuya.

A continuación, se muestran las estadísticas emitidas por la SIC en diciembre de 2018, asociadas a las sanciones que se han impuesto por el incumplimiento a la norma, en los siguientes términos:

- Fallas en seguridad de la información
- Inadecuadas autorizaciones
- Desinformación sobre la finalidad del tratamiento
- Incumplimientos en la atención de reclamos
- Documentación incompleta de políticas, controles y procedimientos

Figura 1-1 Sanciones por incumplimiento de la Ley 1581 de 2012

Nota. Sanciones emitidas por la SIC debido a incumplimientos con la Ley 1581 de 2012 [23]

Con base en la gráfica anterior, solo por inconsistencias en seguridad de la información, el total de multas impuestas por incumplimiento a la Ley 1581 de 2012, fue de 20.9%.

1.1.4 Vulnerabilidades

Son vacíos que se encuentran en las aplicaciones y que pueden ser aprovechadas por los delincuentes informáticos para tomar control y/o realizar operaciones no autorizadas . Algunas son reconocidas y ya se establecieron métodos de corrección, otras reconocidas y aún no se identifica como corregirlas y otras desconocidas [25].

También conocidas como agujeros de seguridad. Son "Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda la información o lleve a cabo operaciones no permitidas de manera remota. Los agujeros de seguridad pueden ser aprovechados por atacantes mediante exploits, para acceder a los sistemas con fines maliciosos. Las empresas deben ser conscientes de estos riesgos y mantener una actitud preventiva, así como llevar un control de sus sistemas mediante actualizaciones periódicas" [15].

En la base de datos nacional de vulnerabilidad (CNV), las vulnerabilidades tienen asignado un identificador Common Vulnerabilities and Exposures (CVE), el cual las define como: "Una debilidad en la lógica computacional que se encuentra en los componentes de software y hardware que, cuando se explota, tiene como resultado un impacto negativo en la confidencialidad, la integridad o la disponibilidad" [26].

1.1.5 Ciberataque

Responde a “toda operación cibernética, ya sea ofensiva o defensiva, que se espera razonablemente que cause lesiones o la muerte a personas o daños o destrucción de objetos” [27].

Dependiendo del objetivo o el daño que se pretenda provocar, los ciberataques pueden presentarse de diferentes maneras, utilizando diversas técnicas que se aplican de forma individual o combinada. Algunas técnicas son [28]:

- Virus informáticos

- Envío masivo de correos no deseados
- Suplantación de remitentes de mensajes mediante Spoofing
- Envío o instalación de archivos espías o Keyloggers
- Uso de Troyanos para el control remoto de los sistemas o la sustracción de información
- Uso de archivos BOT del IRC
- Rootkits

Según Incibe, "Un ataque es un proceso dirigido con una intención bien definida: conseguir unos efectos sobre un objetivo; por ejemplo, robar datos que están en un servidor web o cifrar los contenidos de una máquina para hacer que el usuario pague un rescate. Pero al tratarse de una secuencia de fases (cadena), una mitigación en cualquiera de ellas romperá la cadena, y, por lo tanto, frustrará el ataque" [29].

Igualmente, Incibe indica que al ciclo de vida de un cibertataque se le conoce como Cyber Kill Chain, que está formada por cada una de las etapas de un ataque, las cuales se describen a continuación [29]:

- **Reconocimiento**: el ciberdelincuente estudia y obtiene información de su víctima, con el propósito de identificar las diversas formas de ataque que pueden ser potencialmente efectivas.
- **Preparación**: el ciberdelincuente identifica su forma de ataque y prepara su ejecución.
- **Distribución**: inserción del ataque en el equipo víctima.
- **Explotación**: Compromiso del equipo víctima.
- **Instalación**: Instalación de malware en el equipo víctima.
- **Comando y control:** el ciberdelincuente tiene control sobre el equipo víctima y puede cumplir el objetivo de su ataque.
- **Acciones sobre los objetivos**: el ciberdelincuente cumple con su objetivo, sustrae la información y puede tener acceso a otros nodos de la red.

"Un ciberataque es un intento malicioso y deliberado por parte de un individuo o una organización para irrumpir en el sistema de información de otro individuo u otra organización. Usualmente, el atacante busca algún tipo de beneficio con la interrupción de la red de la víctima" [30].

Seguidamente, revisando en la literatura, se encuentra que según el estudio trimestral de ciberseguridad informado por CCIT, "En el año 2021 se presentaron 41 billones de intentos de ataques cibernéticos en el mundo y siete billones en Colombia". Además, "en Colombia en el año 2021 el número de ataques cibernéticos aumentó en un 30%, comparado con el año anterior" [31].
Por otro lado, el Ministerio de tecnologías de la información y las comunicaciones, basados en el estudio de Ciberseguridad realizado por la Cámara colombiana de informática y telecomunicaciones, incluye en su escrito que, la suplantación de sitios web para la obtención de datos personales, fue el delito más denunciado en Colombia en el año 2020, con un aumento del 303% con respecto al año 2019 [32].

Sumado a lo anterior, indicó Cisco Annual Cybersecurity Report, algunos tipos de ciberataques más comunes son [30]:

- **Malware**: "es un término que se usa para describir el software malicioso, que incluye spyware, ransomware, virus y gusanos. El malware infringe las redes mediante una vulnerabilidad, usualmente cuando un usuario hace clic en un enlace peligroso o en un archivo adjunto de correo electrónico que, luego, instala un software riesgoso. Una vez dentro del sistema, el malware puede hacer lo siguiente: Bloquear el acceso a los componentes clave de la red (ransomware). Instalar malware o software dañino adicional. Obtener información furtivamente mediante la transmisión de datos del disco duro (spyware). Alterar ciertos componentes y hacer que el equipo sea inoperable".

- **Phishing**: "La suplantación de identidad (phishing) es la práctica de enviar comunicaciones fraudulentas que parecen provenir de fuentes confiables, habitualmente a través del correo electrónico. El objetivo es robar datos sensibles, como información de inicio de sesión y tarjetas de crédito, o instalar malware en la máquina de la víctima".

- **Ataque de denegación de servicio:** "Un ataque de denegación de servicio satura los sistemas, los servidores o las redes con tráfico para agotar los recursos y el ancho de banda. Como resultado, el sistema no puede completar las solicitudes legítimas. Los atacantes además pueden usar múltiples dispositivos comprometidos para lanzar un ataque".

- **Inyección de SQL:** "Una inyección de lenguaje de consulta estructurado (SQL) ocurre cuando un atacante inserta un código malicioso en un servidor que usa el SQL y fuerza al servidor para que revele información que normalmente no revelaría. El atacante puede efectuar la inyección de SQL simplemente enviando un código malicioso a un cuadro de búsqueda de un sitio web vulnerable".

- **Ataques de día cero:** "Un ataque de día cero puede impactar después del anuncio de una vulnerabilidad en la red, pero antes de que se implemente un parche o solución. Los atacantes apuntan a la vulnerabilidad divulgada durante esta ventana de tiempo".

- **Tunelización de DNS:** "La tunelización de DNS usa el protocolo DNS para comunicar tráfico que no pertenece al DNS por el puerto 53. Envía HTTP y otro tráfico del protocolo por el DNS. Hay varias razones legítimas para usar la tunelización de DNS. Sin embargo, también existen motivos maliciosos para usar los servicios de VPN de tunelización de DNS. Pueden usarse para encubrir tráfico saliente del DNS y ocultar datos que típicamente se comparten mediante una conexión a Internet. Para el uso malicioso, se manipulan las solicitudes del DNS a fin de exfiltrar los datos de un sistema comprometido a la infraestructura del atacante".

1.1.6 Posibles amenazas en los procesos de facturación

A continuación, se definen algunas de las posibles amenazas que pueden afectar los sistemas de facturación de las empresas de servicios públicos domiciliarios:

- **Denegación de servicio DOS/DDOS:** El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso. Un método más sofisticado es el ataque de Denegación de Servicio Distribuido (DDoS), mediante el cual las peticiones son enviadas, de forma coordinada entre varios equipos, que pueden estar siendo utilizados para este fin sin el conocimiento de sus legítimos dueños [15].

- **Ingeniería social:** Las técnicas de ingeniería social son tácticas utilizadas para obtener datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima [15].

- **Malware**: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software [15].

- **Phishing**: Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta [15].

- **SQL Injection:** Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso [15].

- **Ransomware**: El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos [15].

- **Fraude**: Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete [33]

- **Fuga de información:** La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros [15].

- **Huelga**: Interrupción colectiva de la actividad laboral por parte de los trabajadores con el fin de reivindicar ciertas condiciones o manifestar una protesta [34]

1.1.7 Blockchain

"Blockchain es un libro mayor compartido e inmutable que facilita el proceso de registro de transacciones y seguimiento de activos en una red empresarial. Un activo puede ser tangible (una casa, automóvil, efectivo, terreno) o intangible (propiedad intelectual, patentes, derechos de autor, marca). Prácticamente cualquier cosa de valor se puede rastrear y comercializar en una red blockchain, lo que reduce el riesgo y los costos para todos los involucrados" [35].

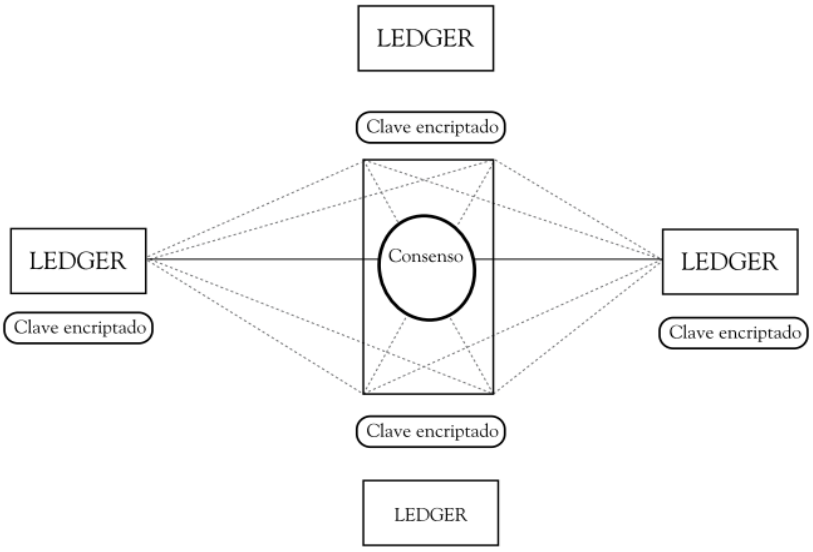
"es una tecnología que permite, a través de técnicas criptográficas, agilización de transacciones complejas"[36].

El activo más importante de las empresas es la información y su seguridad, y por medio de la blockchain, ésta es en línea, compartida, integra, confiable, eficiente y permite monitoreos constantes, además, la almacena en un libro de contabilidad al que ingresa solo personal autorizado [35].

De acuerdo con lo mencionado, y con el propósito de asegurar el proceso de facturación de servicios públicos domiciliarios, se propuso la implementación de la tecnología blockchain, por su base de datos transaccional, descentralizada, transparente, actualizada en línea, compartida, segura y monitoreada por sus partes, en la que las transacciones no requieren intermediarios.

Para el Institute of International Finance, blockchain "es un registro contable distribuido, descentralizado, público y encriptado, en el cual las personas pueden almacenar información y hacer transacciones seguras sin la necesidad de intermediarios. La información de las transacciones no está guardada en un archivo central, está representada por transacciones registradas en una hoja de cálculo global o libro mayor que aprovecha los recursos de una gran red peer-to-peer para verificar y aprobar transacciones" [37], como se muestra en la figura 1-1:

Figura 1-2: Esquema tecnología blockchain



Nota. Tecnología blockchain [37]

Otra definición indica que es una base de datos accedida desde diferentes nodos, que se agrupan en forma de cadena que es protegida por algoritmos ininteligibles seguros, que ejecutan transacciones entre sí [38]. A continuación, se describen los componentes de blockchain, como son transacción, bloque, verificación, hash y ejecución [39]:

- **Transacción**: Acuerdo entre dos personas que deciden intercambiar una unidad de valor e iniciar la transacción, bajo las definiciones de un contrato.
- **Bloque**: Se envía a la red de computadoras participantes en el blockchain.
- **Verificación**: Momento en que las computadoras participantes evalúan y determinan a través de cálculos la validez de las transacciones; alcanzar el consenso entre las computadoras hace que la transacción sea verificada.
- **Hash**: A cada bloque verificado se le estampa temporalmente un hash criptográfico, cada bloque tiene referencia a los previos creando así una cadena de registros infalsificables.
- **Ejecución**: La unidad de valor de la cuenta de A se mueve a la cuenta de B. Es una base de datos distribuida, descentralizada y encriptada dinámicamente, donde cada bloque de información que se une al sistema es validado de forma descentralizada por los anteriores.

En síntesis, blockchain es una tecnología descentralizada y distribuida, que puede interconectarse con dispositivos inteligentes, aumentando la eficacia de los procesos y la confiabilidad en la transmisión de la información, lo que la hace sostenible, compatible y segura [40].

Blockchain permite transacciones donde las partes son autónomas y pueden realizar transacciones entre si independientemente de su ubicación. Además, no existe un punto central de conexión. La confianza que ofrece radica en que tiene procesos de validación, verificación, criptografía y consensos que permiten la adición de un nuevo bloque a la cadena, siempre y cuando no se evidencie ningún tipo de modificación a la estructura.

1.1.6.1 Estructura de Blockchain [41]

Una cadena de bloques, como su nombre lo dice, está compuesta por bloques inmutables, que referencian el bloque anterior, por medio de un hash. Para el caso, "cada referencia en una cadena de bloques está criptográficamente asegurada".
En el hash se considera el contenido y la marca de tiempo. Se pueden usar algoritmos como SHA256, teniendo en cuenta que puede ser:

- **Unidireccional**: "tiene que ser fácil calcular una salida de una entrada dada, pero imposible calcular la entrada de una salida dada".
- **Pseudoaleatorio**: "un cambio en la entrada debe dar como resultado un cambio imprevisible de la salida".
- **Resistente a colisiones**: "debe ser difícil encontrar dos entradas para una función hash que produzca la misma salida".
- **Determinista**: "dada una entrada siempre obtendremos la misma salida".

Los hashes impiden que los bloques sean alterados, y solo permiten adicionar bloques al final de la cadena.

Génesis, es el bloque inicial de toda cadena y se crea automáticamente. Es importante verificar la cadena, garantizando que cada bloque tenga su respectivo hash.

Muchas transacciones forman un bloque y muchos bloques forman una cadena por medio de un enlace digital de datos. Los bloques pasan por un consenso realizado por mineros, el cual al ser admitido permite la adición de un nuevo bloque. Estos mineros son ordenadores que ejecutan los algoritmos previamente definidos en la blockchain.

1.1.6.2 ¿Cómo funciona blockchain?

La tecnología se basa en cuatro fundamentos: "el registro compartido de las transacciones (ledger), el consenso para verificar las transacciones, un contrato que determina las reglas de funcionamiento de las transacciones y finalmente la criptografía, que es el fundamento de todo" [36].

Blockchain se incluye en el proceso como una capa intermedia. Posteriormente, se programa el contrato o las reglas para tener en cuenta. Es así como, las nuevas transacciones se ejecutarán basadas en la manera que fueron programadas.

- A medida que ocurre cada transacción, se registra como un "bloque" de datos: Las transacciones describen la información detallada del activo en cuestión, como: cuándo, dónde, porqué, estado, tiempo, entre otros [35].
- Cada bloque está conectado a los anteriores y posteriores: Cada bloque se entrelaza entre sí de forma segura, para evitar que se altere la integridad de cada uno [35].
- Las transacciones se bloquean juntas en una cadena irreversible, una cadena de bloques: Cada bloque verifica la integridad del bloque anterior, garantizando que no exista algún tipo de acto malintencionado, lo cual otorga mayor confianza en las transacciones [35].

1.1.6.3 Beneficios [35]

- **Mayor confianza:** Debido a que es una red compuesta por miembros, los datos son exactos, confidenciales y compartido solo entre los mismos miembros que estén autorizados.

- **Mayor seguridad:** Los miembros de la red verifican la exactitud de los datos. Además, ninguna transacción es eliminada, siempre se tiene trazabilidad.

"Al crear un registro que no se puede modificar y que cuenta con cifrado end-to-end, blockchain ayuda a prevenir el fraude y la actividad no autorizada. Los problemas de privacidad también se pueden abordar en blockchain mediante el anonimato de los datos personales y el uso de permisos para evitar el acceso. La información se almacena en una red de computadoras en lugar de en un solo servidor, lo que hace más difícil que la información sea visible para los piratas informáticos"[42].

- **Mayor eficiencia:** Se cuenta con un libro mayor compartido entre los miembros, y con una cantidad de reglas almacenadas que se ejecutan automáticamente.

  Aquellos procesos que requieren muchos procesos, manualidades y tiempos, pueden optimizarse con blockchain, en términos de eficiencia y tiempo. Así mismo, "la documentación se puede almacenar en la cadena de bloques junto con los detalles de la transacción, lo que elimina la necesidad de utilizar papel"[42].

- **Mayor transparencia:** "Debido a que blockchain utiliza un registro distribuido, las transacciones y los datos se registran de manera idéntica en múltiples ubicaciones. Todos los participantes de la red con acceso autorizado ven la misma información al mismo tiempo, lo que brinda total transparencia. Todas las transacciones se registran con inmutabilidad y se sellan con la fecha y la hora. Esto permite a los miembros ver el historial completo de una transacción y prácticamente elimina cualquier oportunidad de fraude"[42].

- **Automatización:** Por medio de contratos inteligentes se pueden automatizar las transacciones inmersas en un proceso. Además, permiten evitar la manualidad y la necesidad de comprobación externa del funcionamiento [42].

1.1.6.4 Elementos clave

- **Tecnología de contabilidad distribuida:** "Todos los participantes de la red tienen acceso al libro mayor distribuido y su registro inmutable de transacciones. Con este libro mayor compartido, las transacciones se registran solo una vez, lo que elimina la duplicación de esfuerzos que es típica de las redes comerciales tradicionales" [35].

- **Registros inmutables:** "Ningún participante puede cambiar o alterar una transacción después de que se haya registrado en el libro mayor compartido. Si un registro de transacción incluye un error, se debe agregar una nueva transacción para revertir el error, y ambas transacciones serán visibles" [35].

- **Contratos inteligentes:** "Para acelerar las transacciones, un conjunto de reglas, llamado contrato inteligente , se almacena en la cadena de bloques y se ejecuta automáticamente. Un contrato inteligente puede definir las condiciones para las transferencias de bonos corporativos, incluir términos para el pago del seguro de viaje y mucho más" [35].

  "Los contratos inteligentes son simplemente programas almacenados en una cadena de bloques que se ejecutan cuando se cumplen condiciones predeterminadas. Por lo general, se utilizan para automatizar la ejecución de un acuerdo para que todos los participantes puedan estar seguros de inmediato del resultado, sin la participación de ningún intermediario o pérdida de tiempo. También pueden automatizar un flujo de trabajo, activando la siguiente acción cuando se cumplen las condiciones" [43].

  Es decir, con base en unas determinadas condiciones y en un diseño previo, se crean algoritmos en una cadena de bloques, los cuales realizan tareas automatizadas, lo que a su vez trae eficacia, controles y disminuye la mano de obra. Los contratos inteligentes están programados por sentencias lógicas simples, las cuales están incluidas en la cadena de bloques. En la medida que las respuestas a las sentencias avanzan, se van haciendo las actualizaciones indicadas en el mismo programa.

  Entre los beneficios de los contratos inteligentes, se encuentran [43]:

- **Velocidad, eficiencia y precisión:** En la medida en que se avanza en las condiciones incluidas en el programa, se van cumpliendo las ejecuciones también indicadas. Al ser contratos digitales y automatizados, se disminuyen los posibles errores humanos y los extensos tiempos de ejecución.

- **Seguridad:** Los registros de las transacciones están encriptados. Además, para alterar registros se debería alterar toda la cadena de bloques.

- **Ahorro:** Menos mano de obra humana, menos manualidad, menos errores, y menos terceros involucrados.

1.1.6.5 Tipos de redes blockchain

- **Redes públicas:** Cualquiera puede unirse y verificar las transacciones, por lo que es mínimamente segura [35].

- **Redes privadas:** "Una red blockchain privada, similar a una red blockchain pública, es una red de igual a igual descentralizada. Sin embargo, una organización gobierna la red, controlando quién puede participar, ejecutar un protocolo de consenso y mantener el libro mayor compartido. Dependiendo del caso de uso, esto puede aumentar significativamente la confianza entre los participantes. Una cadena de bloques privada se puede ejecutar detrás de un firewall corporativo e incluso alojarse en las instalaciones" [35].

- **Redes autorizadas:** presentan restricciones y solicitan permisos para unirse y participar en las transacciones [35].

- **Blockchain del consorcio:** "Varias organizaciones pueden compartir las responsabilidades de mantener una cadena de bloques. Estas organizaciones preseleccionadas determinan quién puede enviar transacciones o acceder a los datos. Una cadena de bloques de consorcio es ideal para las empresas cuando todos los participantes deben tener permiso y tener una responsabilidad compartida por la cadena de bloques" [35].

- **Cadenas de bloque sin permisos:** sin ningún tipo de restricción para su participación [44].

Igualmente, es pertinente mencionar que Blockchain tiene diversas ventajas, entre las que se ratifica que no es centralizada, toda vez que se ejecuta en computadoras distribuidas en diferentes lugares del mundo, es pública porque quién lo requiera puede hacer seguimiento y monitoreo constantemente, y es encriptada, lo que hace que sea segura. En la tabla 1-3 se presenta esquema

comparativo, donde se evidencian las ventajas de implementar blockchain con relación a los sistemas centralizados [37]:

Tabla 1-5: Comparativo entre un sistema centralizado y blockchain

Características	Sistema centralizado	Blockchain
Administración de la información	Existe un administrador de la información	La información se encuentra descentralizada
Sistema de seguridad	El administrador debe implementar un sistema de seguridad con la finalizad de proteger la información. La estructura de los mecanismos de seguridad en manos del administrador o de un tercero señalado por este, sin que, por ello, el administrador deje de ser el responsable.	Existe un sistema criptográfico, el cual puede variar a través de los mecanismos de claves públicas y privadas.
Transparencia	El administrador establece los mecanismos por medio de los cuales los participantes acceden a la totalidad de la información dentro de protocolos establecidos para tal fin.	Los participantes del sistema tienen la posibilidad de acceder a la información y verificarla a través de la cadena de bloques.
Costos	Se materializan costos por razón de la infraestructura tecnológica y en materia de la ciberseguridad que requiere el administrador central en el manejo de la información.	Hay una reducción de costos, ya que el manejo de la información es reemplazado por códigos algorítmicos, los cuales, a través de nodos, procesan y verifican la información de forma independiente de cada transacción.

Características	Sistema centralizado	Blockchain
Alterabilidad de la información	Depende de los sistemas tecnológicos de ciberseguridad con que cuenta el administrador, los cuales no son inmunes a ataques cibernéticos.	Al existir una descentralización de la información, la cual está organizada en bloques por medio de procesos algorítmicos, la manipulación y alteración de dicha información es difícil de realizar

Nota. Comparación tecnología blockchain en relación con sistemas centralizados [37]

Aunado a las definiciones anteriores, se informa también que blockchain es un tipo de tecnología de contabilidad distribuida (DLT) que registra transacciones descentralizadas por medio de un protocolo criptográfico distribuido; en el que se manejan muchos nodos que verifican los datos y la información entre sí. La tecnología Blockchain/DLT tiene características de descentralización, persistencia, anonimato, auditabilidad y ofrece una arquitectura que organiza las transacciones [45].

Así mismo, se relacionan términos como Ethereum, que corresponde a "una plataforma informática distribuida de código abierto, pública y basada en blockchain que presenta un contrato inteligente, mientras que Ether es la criptomoneda utilizada en esta plataforma" [46, p. 1]. El propósito de Ethereum se basa en construir un protocolo alternativo para generar aplicaciones descentralizadas. Sobre el concepto de contratos inteligentes, éstos son compromisos digitales donde se acuerda la manera en la cual las partes determinan el cumplimiento de estos. Normalmente, los contratos inteligentes se basan en Ethereum y son programadas por el lenguaje Solidity. Con el uso de estos contratos, ocurre que los errores y brechas de seguridad son visibles para todos los participantes y no tienen soluciones rápidas [46].

Otro termino relacionado es Hyperledger Fabric, que permite código abierto, realiza validaciones de ejecución donde los contratos inteligentes se ejecutan antes de los pedidos, y su estructura es clave-valor versionado, que representa la salida de las transacciones [47].

Hyperledge, fue creado en el 2015 por Linux Foundation [36].

1.1.6.6 Seguridad blockchain

“La seguridad de la cadena de bloques es un sistema integral de gestión de riesgos para una red de cadena de bloques, que utiliza marcos de ciberseguridad, servicios de garantía y mejores prácticas para reducir los riesgos contra ataques y fraudes”[44].

"La tecnología Blockchain produce una estructura de datos con cualidades de seguridad inherentes. Se basa en principios de criptografía, descentralización y consenso, que garantizan la confianza en las transacciones. En la mayoría de las cadenas de bloques o tecnologías de contabilidad distribuida (DLT), los datos se estructuran en bloques y cada bloque contiene una transacción o paquete de transacciones. Cada nuevo bloque se conecta a todos los bloques anteriores en una cadena criptográfica de tal manera que es casi imposible manipularlo. Todas las transacciones dentro de los bloques se validan y acuerdan mediante un mecanismo de consenso, lo que garantiza que cada transacción sea verdadera y correcta. Esta tecnología, permite la descentralización a través de la participación de miembros en una red distribuida. No hay un solo punto de falla y un solo usuario no puede cambiar el registro de transacciones" [44].

De acuerdo con IBM, los siguientes son los ataques más comunes hacia las cadenas de bloque [44]:

- **Phishing**: Se basa en la obtención de las credenciales de los usuarios mediante hipervínculos.
- **Ataques de enrutamiento:** Es la extracción de información y/o monedas mientras se transfieren datos en la cadena.
- **Ataques de Sybil:** Es el uso de identidades falsas para colapsar la red.
- **51% de ataques:** tener más del 50% de la potencia minera de una red permite controlar y manipular el libro mayor. Este tipo de ataque no se materializa en las redes de blockchain privadas.

No obstante, IBM sugiere los siguientes controles para conservar la seguridad en las cadenas de bloque:

- Gestión de identidades y accesos
- Gestión de claves

- Privacidad de datos
- Comunicación segura
- Seguridad de contrato inteligente
- Aprobación de la transacción

1.1.7.7 Principios esenciales implícitos en blockchain

- **Integridad en la red:** "La confianza es intrínseca, no extrínseca. La integridad está cifrada en todas y cada una de las etapas del proceso y distribuida, y no depende de cada miembro individualmente. Los participantes pueden intercambiar valor directamente, confiados en que los demás actuarán con integridad". Es decir, la cadena no podría ser modificada o alterada en ninguno de sus nodos toda vez que es inmutable. No obstante, si llegara a cambiarse la información de algún nodo, sería visible la situación y no se aceptaría la adición del bloque en cuestión.

- **Poder distribuido:** "El sistema distribuye poder por una red de iguales sin que haya ningún punto de control. Las partes no pueden apagar el sistema por sí solas. Si una autoridad central lograra inhabilitar o expulsar a un grupo, el sistema sobreviviría. Si la mitad de la red intentara dominar al conjunto, todo el mundo lo vería". Cada nodo tendrá el mismo poder y cualquier alteración sería fácilmente identificada.

- **El valor como incentivo:** "El sistema hace coincidir los incentivos de todos los participantes. El bitcoin o alguna ficha de valor es parte esencial de esta coincidencia y correlativo a la reputación". La cadena de bloques incluye incentivos que aportan a que esta se mantenga íntegra.

- **Seguridad: "**Las medidas de seguridad están integradas en la red sin puntos flacos y no sólo garantizan la confidencialidad, sino también la autenticidad de todas las actividades y la imposibilidad de que no sean denegadas. Todo el que quiera participar debe usar criptografía – no es posible optar, por lo contrario – y las consecuencias de comportarse mal solo las sufre la persona que se comparta mal". La blockchain asegura los procesos, toda vez que tiene elementos que extreman la seguridad, como llaves privadas, públicas, criptografía, entre otras.

- **Privacidad:** corresponde al control que se tiene sobre los datos propios y la posibilidad de decidir cómo, cuándo y de qué manera compartir la información con el entorno. De acuerdo con la configuración de la blockchain, la seguridad puede tener algunas variaciones.

- **Derechos preservados:** El derecho a la propiedad es legítimo y respetado.

- **Inclusión:** una de las bondades de blockchain es que es descentralizada, lo cual permite que haya distribución entre los nodos e inclusión.

1.2 Estado del arte

Para el desarrollo del presente proyecto de grado, se consultó en las siguientes bases de datos científicas: Scopus, Arxiv, Dialnet, SCielo, EBSCO, ProQuest, IEEE y Nist. Así mismo, proveedores masivos de cursos como Coursera, empresas reconocidas de la industria, entre las que se encuentran IBM, Oracle y Blockchain-Ex Innovation Center y empresas del sector de los servicios públicos ubicadas en Colombia. Para realizar la búsqueda se utilizaron las palabras claves: blockchain, facturación, seguridad de la información, normatividad, Empresas de Servicios públicos domiciliarios, Superintendencia de Servicios públicos domiciliarios y ciberataques. Igualmente, en la Tabla 1-3 se indicaron los criterios de inclusión y exclusión para los artículos encontrados:

Tabla 1-6 Criterios de inclusión y exclusión de artículos, proyectos y empresas

Criterios de inclusión	Criterios de exclusión
Implementaciones de blockchain	Artículos inferiores a 10 años
Artículos o proyectos escritos sólo en inglés o español.	Artículos diferentes a los idiomas inglés o español.
Facturación de servicios públicos domiciliarios	Facturación diferente a servicios públicos domiciliarios
Vulnerabilidades actuales en procesos de facturación	Artículos relacionados solo con temas de facturación de servicios públicos domiciliarios
Amenazas actuales en procesos de facturación	Artículos relacionados solo con temas de facturación de servicios públicos domiciliarios

Criterios de inclusión	Criterios de exclusión
Riesgos actuales en procesos de facturación	Artículos relacionados solo con temas de facturación de servicios públicos domiciliarios

Nota: Fuente propia

Con base en las búsquedas realizadas, se detallaron a continuación los artículos o documentos más relevantes en el estado del arte:

Se evidencia la versatilidad que tiene blockchain en términos de uso, toda vez que puede aplicarse y adaptarse en industrias totalmente diversas. Por ejemplo, autores como Hlaing y Nyaung en su artículo [48], informan que Blockchain permite el uso de contratos inteligentes que disminuyen el consumo de gas, soporta sistemas de facturación de energía eléctrica, permite emplear Ethereum para ejecutar contratos entre pares y Firebase para el almacenamiento de datos en redes descentralizadas, como por ejemplo, los datos del medidor. Afirman además que, al utilizar Firebase con blockchain el costo de cada transacción realizada en Ethereum se reduce un 73%, aproximadamente, que al combinarse Firebase Authentication con Ethereum Blockchain se proporciona una autenticación de dos factores, el contrato inteligente se utiliza para guardar el token de autenticación y configurar la política de uso del medidor.

Así las cosas, el uso de Ethereum y firebase es amplio, por lo que podrían ajustarse también a servicios como el acueducto, utilizando sensores que estén conectados con blockchain, de modo que por medio de contratos inteligentes se pueda registrar también este consumo [48].

En ese mismo orden de ideas, en el artículo [49], mencionan que los medidores inteligentes se han adoptado para facilitar las medidas de uso de energía residencial y que los usuarios y los gobiernos requieren verificar si las facturas están en línea de acuerdo con sus consumos reales. Lo cual es retador, debido a la falta de privacidad causada por la facilidad de acceso al historial de consumos de energía y al requisito de eficiencia para las solicitudes de auditoría masiva sobre las facturas y los consumos de los residentes. Por lo anterior, introdujeron el cifrado homomórfico cooperado con la técnica blockchain para aprovechar la auditoría de datos y requisitos de preservación de la privacidad. El artículo también menciona el uso del framework AuditChain, debido a la importancia de preservar la seguridad de los datos de la factura y del cumplimiento de las auditorías. Lo anterior, será considerado, por la permanente necesidad de asegurar la información de los usuarios y la empresa prestadora de

los servicios, establecer la segregación de funciones y el mínimo privilegio, y cumplir con los estándares requeridos por las auditorías que se realizan, internas y externas.

Sin embargo, con respecto al tema asociado con el uso de medidores inteligentes, se considera importante indicar que, actualmente, las empresas utilizan medidores convencionales, porque con estos se da cumplimiento a lo establecido en la Ley 142 de 1994, donde se informa que los consumos deben ser medidos con instrumentos idóneos, y que estos son el elemento principal para determinar el valor a facturar. [1].

Por lo tanto, en atención a que las facturas estén en línea de acuerdo con los consumos reales, corresponde a un gran salto tecnológico que aportaría tanto a las Empresas como a los usuarios. Actualmente, ocurre que un consumo sea liquidado entre 1 y 2 meses después de tomar la lectura, lo cual es legal, teniendo en cuenta que cada servicio público se rige bajo un contrato de condiciones uniformes, y en los mismos se definen los periodos de facturación que deben contemplarse. A manera de ejemplo, se relaciona del Contrato de Condiciones Uniformes de Energía de una Empresa prestadora, la cláusula 43, en la que se indica que los periodos de facturación pueden ser mensuales, bimensuales, trimestrales o semestrales de acuerdo con la posibilidad de acceso a la zona donde se presta el servicio, casos en los cuales además se permiten pagos intermedios entre periodos, basados en las lecturas tomadas en los elementos de medición [50].

Cabe considerar, por otra parte, la gestión energética cooperativa de una comunidad de edificios inteligentes con enfoque en la tecnología Blockchain, pues se trata de un algoritmo descentralizado de dicha tecnología, que permite un medio de comunicación confiable entre los participantes y refuerza el monitoreo y la facturación autónoma a través de contratos inteligentes. Con un marco de gestión de energía de este tipo, los edificios inteligentes pueden apuntar a un objetivo común, como el uso de recursos libres de carbono o servicios de red agregados, sin depender de un servicio público centralizado. El documento presenta un marco descentralizado para gestionar el consumo eléctrico en una comunidad de edificios inteligentes y energías renovables. Los contratos inteligentes permitieron a los participantes decidir de manera colaborativa un perfil de planificación que minimiza el costo total agregado, a través de una sucesión de procesos de optimización local. Esta planificación puede beneficiar enormemente al operador de la red en su despacho diario, y el seguimiento en línea

reduce la necesidad de reserva de capacidad adicional. Finalmente, el análisis de escalabilidad destacó que se puede aplicar a una comunidad de hasta 100 edificios inteligentes, dado el estado actual de Ethereum. Dado que el futuro exige una electrificación intensa de los edificios y el transporte, estos activos descentralizados deben incorporarse de manera eficiente a la red global teniendo en cuenta su comportamiento agregado [51].

Es decir, el propósito establecido en el documento hace mayor referencia en que la solución basada en Blockchain permite trabajar cooperativamente hacia una red eléctrica descarbonizada en general, y cómo los edificios inteligentes permiten aumentar la eficiencia energética. Contrario al enfoque pretendido en la propuesta, debido a que la necesidad principal radica en asegurar con la utilización de dicha tecnología, el proceso de facturación de las Empresas de servicios públicos. [51]

Ahora bien, en el artículo Colombia estrena 'blockchain' para aparatos médicos, se informa que alrededor de 9 millones de pacientes serían beneficiados con esta implementación de IBM, basada en Hyperledger Fabric, para el seguimiento, control y abastecimiento de dispositivos médicos como catéteres y marcapasos en la Clínica Las Américas de Medellín. El control de disponibilidad e inventarios de dispositivos médicos para pacientes coronarios se redujo a solo 24 horas, mejorando en un 90% el tiempo de facturación y un 60% en las órdenes de compra. El control también entrega datos precisos en tiempo real, sobre el stock, tanto cuando existe exceso o escasez de insumos. La Clínica Las Américas es pionera en América Latina en esta implementación, para soluciones de trazabilidad de dispositivos [52].

En tal sentido, aunque este último artículo se enfoca en el manejo del stock de medicamentos, puede evidenciarse que blockchain, permite gestionar cadenas de suministro, tener trazabilidad, proteger los datos y tener una constante colaboración con los proveedores, lo que, entre otras bondades, se asemeja a la aplicación propuesta en el presente texto. Adicionalmente, se evidencia que esta tecnología puede adaptarse e implementarse para diferentes necesidades. En el caso puntual, puede aportar a los procesos de facturación de servicios públicos domiciliarios, en lo que se refiere a la ejecución de cada una de las fases que lo componen y en paralelo, al fortalecimiento de la seguridad de su información [52].

Igualmente, en el artículo [53] los autores hablan de la forma en la que blockchain puede aplicarse en la liquidación de pagos del comercio transfronterizo, toda vez que el modelo actual pasa por varias instituciones, requiere sincronizar información de los bancos individuales, es poco eficiente, costoso e inseguro. Se menciona esta nueva forma de hacerlo, argumentando que es descentralizada, confiable, colectiva porque los datos son mantenidos por todos los nodos, de programación diseñada en contratos inteligentes, con uso de hash o algoritmos de curva elíptica y uso de consenso que confirma su validez. El ejemplo anterior, enfocado en liquidación de pagos, también tiene aplicación en las diversas transacciones que se realizan en el área de facturación de las Organizaciones, pues es allí donde se determinan los valores a cobrar para posteriormente recibir su pago, y este proceso también se requiere transparencia, verificación y eficiencia.

Por otro lado, la marca RSM-multinacional de firmas de contabilidad, incrementa su facturación global en un 6,9% y alcanza los 5.740 millones de dólares en 2020, la Organización mundial de auditoría y consultoría middle market reportó para el año 2019 una facturación de 5.740 millones de dólares que representa un crecimiento del 6,9%, además, incrementó el número de sus empleados y oficinas, y se evidencia que los servicios que han incrementado su facturación son parafiscales y consultoría con 11,7% y 7,2 %, respectivamente. En España, la firma se asoció con BanQu, plataforma blockchain sin uso de criptomoneda que otorga sostenibilidad y transparencia a los procesos de cadena de suministro. En España, la firma se asoció con BanQu, una plataforma blockchain sin criptomoneda que aporta soluciones de transparencia, sostenibilidad y trazabilidad de la cadena de suministro. Esta alianza permite que las empresas obtengan la trazabilidad de cada eslabón que comprenden las cadenas de suministros, desde el inicio del proceso hasta la entrega al cliente final [54].

El ejemplo anterior, comunica sobre el crecimiento económico y financiero de la Empresa. Además, aduce como se ha favorecido su cadena de suministro y las bondades que ha obtenido a través de blockchain, bondades en términos de transparencia, sostenibilidad, trazabilidad y seguridad. Aunque se hace referencia al proceso de cadenas de suministro, puede ser totalmente aplicable al proceso de facturación, toda vez que éste también está separado por fases que dependen de la anterior, involucra diferentes actores y requiere de las bondades mencionadas [54].

Por su parte, IBM lanzó el Centro Cognitivo de Transformación en Bogotá apostando a la innovación y cuarta revolución industrial. Este Centro busca aportar a los procesos de facturación, contabilidad, compras y servicio al cliente en industrias como la banca, telecomunicaciones, gas y energía; para lo cual se han dictado capacitaciones en temas como inteligencia artificial, blockchain y otras tecnologías disruptivas, lo que hace que se visione un futuro donde la tecnología blockchain tendrá un papel realmente importante [55].

Cabe destacar la publicación anterior, toda vez que puede inferirse la importancia que tienen las nuevas tecnologías, no solo en la academia, también para las Empresas. Estas últimas deben prepararse para estar a la vanguardia y responder a un Mercado demandante, y una de las estrategias para ello es la innovación y la transformación empresarial equilibrada con la transformación tecnológica [55]

A propósito, según el estudio de DHL BlockChain in Logistics, se recomienda utilizar esta tecnología, en aras de dar seguridad y autenticidad a los procesos farmacéuticos. Se cita el ejemplo porque permite evidenciar que la cadena de bloques es de su uso es versátil, pues como se ha evidenciado en párrafos anteriores, no solo es utilizada en la industria farmacéutica, también puede aplicarse en otras industrias, y podría ser utilizada en procesos como: facturación. Para el proceso de facturación, una de las innumerables ventajas, es que con blockchain se produce una serie de códigos cifrados que se registran en sus bloques, haciendo que estos registros sean únicos [6].

Por otra parte, se tienen otras Empresas cuyos manejos de la facturación son diferentes, por ejemplo, las de servicios de gestión inmobiliaria del sector público, consideran lineamientos como los siguientes para su facturación: documentación consistente, los bienes y servicios se facturan si están estipulados en los comprobantes de venta, retención y demás documentos autorizados por el servicio de rentas internas. Así mismo, para la anulación de las facturas se debe justificar la razón, y por último, los comprobantes electrónicos como facturas, notas y demás, se emiten bajo los parámetros estipulados en la norma [56].

Brevemente, es una forma funcional de facturar, los lineamientos se basan sobre todo en que funcione y en el cumplimiento de la normatividad vigente, no se incluye un ítem que se refiera a la secuencia,

confiabilidad, integridad y disponibilidad de la transacción. Por lo tanto, no tiene símil con la propuesta actual. [56]

De la misma forma, según los autores del artículo [57], blockchain podría ser muy útil en todos los procesos de producción, distribución y entrega de la cadena de suministros agroalimentaria. Lo anterior, por presentar nuevas formas de hacer el proceso, certificar la información por su trazabilidad, garantizar los controles, auditorías, tener datos actualizados y disponibles para los interesados, altos niveles de transparencia, seguridad, confianza y rentabilidad. Se relaciona con los procesos de facturación de las empresas de servicios públicos, en la medida que estos están compuestos por fases que pueden ser los eslabones de una cadena, los cuales se entrelazan entre sí, y solo continúan su curso o se pasa al siguiente al finalizar el anterior. Además, se nuevamente, se resaltan beneficios que indiscutiblemente son necesarios para fortalecer dicho proceso.

Así mismo, con la situación que se ha vivido de pandemia, también se vio la oportunidad de implementar blockchain con diferentes robots para combatir el Covid 19 u otras pandemias. Son robots con administración descentralizadas que realizan diversas tareas de limpieza, desinfección, detección y entrega de elementos, lo cual contribuiría a combatir la enfermedad, permitir el distanciamiento físico y aportaría a la labor de los profesionales de la salud [33].

Adicionalmente, cada vez es mayor la necesidad de conectar dispositivos inteligentes, teniendo en cuenta el internet de las cosas (IoT) y blockchain, ya que ésta última, es una solución que podría realizar la transferencia eficiente de datos e información, por medio de algoritmos que van de nodo a nodo [40]. Es así como, el éxito que ha tenido blockchain con las aplicaciones IoT, ha permitido pensar en diversas aplicaciones y usos. Por ejemplo, pensar en un esquema para cámaras de vigilancia en el borde, que propenda por la privacidad de las personas y que puedan detectarse comportamientos inadecuados. Esto sería en plataforma blockchain con contratos inteligentes, equipos de detección y cámaras hacen capturas de video, divisiones, desenfoques, y análisis de video en tiempo real, entre otras [34].

Ya para terminar, se concluye que blockchain es una tecnología disruptiva tan versátil que puede adaptarse y aplicarse en diferentes ámbitos, e indiscutiblemente, su aporte representa múltiples ventajas, mejoras y beneficios para los procesos.

A continuación, en la tabla 1-7 se encuentra el resumen comparativo asociado al estado del arte:

Tabla 1-7: Resumen comparativo - Estado del arte implementación de blockchain en diversos sectores

TRABAJO RELACIONADO	CONTRIBUCIÓN	LIMITANTES	APORTE
Electricity Billing System using Ethereum and Firebase. Kyawt May Hlaing Dim En Nyaung. 2019	Blockchain permite el uso de contratos inteligentes que disminuyen el consumo de gas, soporta sistemas de facturación de energía eléctrica, permite emplear Ethereum para ejecutar contratos entre pares y Firebase para el almacenamiento de datos en redes descentralizadas. Al utilizar Firebase con blockchain el costo de cada transacción realizada en Ethereum se reduce. Combinar Firebase Authentication con Ethereum Blockchain proporciona una autenticación de dos factores.	Se basa solo en la facturación del servicio de energía.	Con la metodología propuesta, se abarcó el proceso de facturación de los servicios de energía, acueducto, alcantarillado y gas. Como se menciona en la metodología, se va a propender porque en dicho proceso se minimicen los riesgos que afectan la confidencialidad, integridad y disponibilidad.
lockchain Enables Your Bill Safer. Qin Wang, Longxia Huang and Yang Xiang. 2020	Se habla de la necesidad de medir los consumos de energía en línea y contar con las debidas auditorías sobre los mismos. Por lo que se propone el uso de cifrado homomórfico con blockchain para aprovechar los requisitos de auditoría de datos y preservación de la privacidad. Se propone el marco pAuditChain, porque acepta solicitudes para verificar el consumo y maneja solicitudes de auditoría masivas. Este marco mejora la seguridad y privacidad de las facturas sin perder la función de auditoría. Igualmente, se enfoca en el uso de medidores inteligentes de IoT.	Se refiere al uso de medidores inteligentes solo para la medición de los consumos del servicio de energía eléctrica.	Se aportará al proceso de medición y facturación de los servicios públicos domiciliarios: energía, acueducto, alcantarillado y gas natural residencial. Como se menciona en la metodología, se va a propender porque en el proceso de facturación se minimicen los

TRABAJO RELACIONADO	CONTRIBUCIÓN	LIMITANTES	APORTE
			riesgos que afectan la confidencialidad, integridad y disponibilidad.
Colombia estrena 'blockchain' para aparatos médicos. Grupo de Diarios América. 2020	Implementación de la tecnología IBM Blockchain basada en Hyperledger Fabric, para el seguimiento, control y abastecimiento de dispositivos médicos. Es decir, la utilización y la licencia de uso de esta tecnología en el sector salud para el control de disponibilidad de insumos e inventarios de dispositivos médicos lo que mejora en gran medida el tiempo de facturación y los errores en las órdenes de compra.	La implementación se enfatiza en la disponibilidad de insumos e inventario de equipos médicos.	La metodología propuesta, podrá aportar al proceso de disponibilidad de insumos e inventarios, el proceso de facturación. La metodología propuesta aporta a la disminución de los riesgos que pueden ocasionar indisponibilidad en la información
Blockchain for Multi-Robot Collaboration to Combat COVID-19 and Future Pandemics. S. H. Alsamhi, Brian Lee, Y Qiao. 2020	Se describe cómo la tecnología blockchain puede combinarse de forma colaborativa con robots para combatir el covid -19 y pandemias en general. Estos robots pueden realizar tareas como rociar, desinfectar, limpiar, tratar, detectar alta temperatura corporal / ausencia de mascarilla y entregar bienes y suministros médicos.	Se hace énfasis en el uso de robots para el manejo de pandemias, de modo que estos suplan necesidades de distanciamiento social.	

TRABAJO RELACIONADO	CONTRIBUCIÓN	LIMITANTES	APORTE
A Lightweight Blockchain-based Privacy Protection for Smart Surveillance at the Edge. Alem Fitwi†, Yu Chen†, Sencun Zhu. 2019	Se propone un esquema de protección de privacidad basado en Blockchain para cámaras de vigilancia en el borde. Hacer vigilancia sin vulnerar la privacidad de las personas. El sistema Lib-Pri transforma el VSS implementado en un sistema que funciona como una red de cadena de bloques federada capaz de realizar comprobaciones de integridad, gestión de claves borrosas, uso compartido de funciones y sanción de acceso a vídeos.	Se basa en la vigilancia realizada a través de cámaras y video cámaras.	La fusión entre cada una de las etapas que tiene el proceso, de forma segura y con monitoreos y revisión en tiempo real. Que el proceso pueda ser monitoreado en tiempo real aporta a garantizar que finalice correctamente.

Nota: Fuente propia

2. Metodología

El enfoque metodológico empleado es de tipo deductivo/inductivo, toda vez que se toman conclusiones generales para llevarlas a situaciones particulares. Además, se utiliza el razonamiento para emitir conclusiones posteriores a hechos válidos.

A partir de caracterizar activos, vulnerabilidades, amenazas, riesgos presentes en los procesos de facturación de las ESP y su plan de tratamiento, también a partir de la conversación con empresas del sector a través de una encuesta para identificar sus riesgos, controles y mejores prácticas, y finalmente, tras la recolección de información sobre las cadenas de bloques, sus usos y sus ventajas, en bases de datos y empresas de la industria, se identificaron patrones y estructuras que permitieron diseñar y proponer una metodología para la adaptación y aplicación de blockchain, con el propósito de optimizar y asegurar la información de dicho proceso y mejorar la calidad del producto final: La factura.

Para el desarrollo de la presente tesis de maestría y el cumplimiento de su objetivo general, se definieron las siguientes cuatro (4) fases, equivalentes a cada uno de los objetivos específicos diseñados, estas a su vez, contienen las tareas que se describen a continuación en la figura 2-1:

Figura 2-1: Metodología de desarrollo de proyecto de grado

Nota. Fuente propia

2.1 Fase 1. Proceso de facturación general y mapa de riesgos

En esta primera fase, correspondiente al objetivo específico número 1, se construyó y se diseñó un proceso de facturación general basado en los procesos de facturación particulares que se han estudiado en el presente proyecto. Por lo tanto, este proceso de facturación general puede ser adoptado por cualquier empresa dedicada a los servicios públicos. Así mismo, también puede ser adoptado por empresas de otros sectores, siempre que en su proceso se haga una distribución por fases y éstas tengan similitud o se puedan adaptar con las definidas.

Adicionalmente, en esta fase también se identificaron activos, amenazas, vulnerabilidades, escenarios de riesgo, agentes generadores y calificación de probabilidad, impacto y riesgo, asociados al proceso de facturación de servicios públicos. Seguidamente, con esta información, se construyó un mapa de riesgo a nivel de información, basado en la norma técnica NTC-ISO/IEC colombiana 27005. Es decir, una vez se recopiló la información, con el mapa de riesgos construido, se realizó la evaluación de los riesgos, se cuantificó su probabilidad de ocurrencia y se definió su aceptabilidad [58]. Esta información es de gran valor, pues conocer los riesgos presentes permite identificar y cerrar brechas que pueden llegar a ser aprovechadas por atacantes, mejorar los

procesos y elevar los niveles de maduración corporativa desde el punto de vista de seguridad de la información.

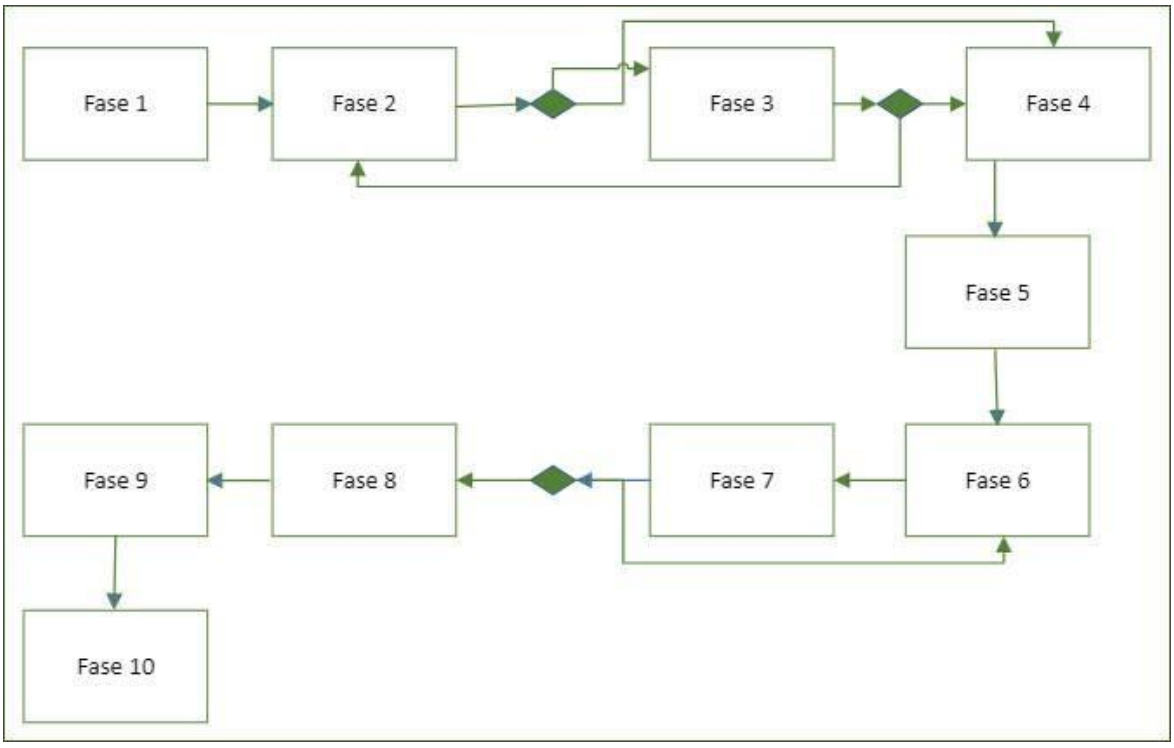
Los entregables de esta fase son:

- Proceso de facturación general construido
- Mapa de riesgos general.

2.1.1 Proceso de facturación general

Corresponde a la creación de un proceso de facturación general que puede ser aplicado a diferentes empresas del sector de los servicios públicos. Este resultó de la observación y análisis de los diferentes procesos de facturación de las empresas investigadas, los cuales fueron mencionados en el marco teórico. El mismo se plasmó en un diagrama de flujo como el de la figura 2-2, en el cual los rectángulos representaron las fases que componen dicho proceso, las líneas de flujo o flechas indicaron el orden de ejecución de las fases, y los rombos permitieron analizar una situación con base en los valores verdadero (SI) y falso (NO):

Figura 2-2 Diagrama del proceso e facturación



Nota. Fuente propia

2.1.2 Mapa de riesgos

Se realizó mapa de riesgos con el fin de identificar los factores y brechas que representan riesgo en el proceso de facturación de las ESP, establecer su magnitud y posteriormente cuantificarlos para planear estrategias de manejo y tomar las acciones pertinentes para mitigar y/o evitar su materialización. De tal forma que se fortalezca la seguridad de la información de la Empresa.

Para realizarlo se llevaron a cabo las siguientes actividades:

- Identificación de activos
- Identificación de amenazas
- Identificación de vulnerabilidades
- Identificación de escenarios de riesgo
- Agentes generadores
- Calificación de probabilidad, impacto y riesgo

2.1.2.1 Identificación de activos

En una tabla como la 2-1, se hizo el inventario de los activos más representativos que se hallaron en las fases informadas para el proceso de facturación construido, con el objetivo de tenerlos identificados, saber su descripción, su tipo, su nivel de criticidad y verificar en cuál de las fases de dicho proceso tienen su acción. La tabla consta de las siguientes columnas [59]:

- **Identificación**: código que identifica el activo
- **Nombre**: nombre que tiene el activo
- **Descripción**: definición del activo
- **Fase del proceso de facturación**: Nombre de la actividad del proceso de facturación de la cual hace parte y/o se relaciona
- **Tipo**: Indicar si es un activo físico o lógico
- **Crítico**: Indica si el activo es fundamental para la Empresa.

Tabla 2-1 Identificación de activos

Identificación	Nombre	Descripción	Fase del proceso de facturación	Tipo	Crítico

Nota: Fuente propia

Adicionalmente, se hace la relación entre los activos definidos y los pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad, con la intensión de reconocer el impacto que tendría cada activo en uno o varios de los principios mencionados, al materializarse un riesgo.

Esta información se recopilará en una tabla como la 2-2, en la cual cada ítem tiene el siguiente significado:

- **Activo**: activo identificado en el inventario de activos y que hace parte del proceso de facturación
- **Principio**: principio que se afecta si llega a materializarse un riesgo en el respectivo activo
- **Motivo**: razón por la cual se afectaría uno o varios principios de la seguridad de la información al materializarse un riesgo.

Tabla 2-2 Relación activos y principios de seguridad de la información

Activo	Principio	Motivo

Nota. Fuente propia

2.1.2.2 Identificación de amenazas

Son algunas de las amenazas que se consideraron más comunes en el proceso de facturación, y de las cuales se identificó cómo puede afectarlo. Para consignar la información, se creó la tabla 2-3 con los siguientes items:

- **Identificación Amenaza**: Código que identifica la amenaza
- **Nombre de la amenaza:** Nombre de la amenaza
- **Posible afectación al proceso de facturación:** detalle donde se identifica la manera en la que cada determinada amenaza en cuestión afecta el proceso de facturación.

Tabla 2-3 Identificación de amenazas

Identificación amenaza	Nombre de la amenaza	Posible afectación al proceso de facturación

Nota: Fuente propia

2.1.2.3 Identificación de vulnerabilidades

Se identificaron algunas de las vulnerabilidades más comunes de los procesos de facturación, de acuerdo con el proceso diseñado previamente y la Norma ISO 27001. Esta información se almacenó en la tabla 2-4, la cual está compuesta por los siguientes campos:

- **Identificación de la vulnerabilidad**: código asignado a la vulnerabilidad
- **Nombre de la vulnerabilidad**: nombre de la vulnerabilidad

Tabla 2-4 Identificación de vulnerabilidades

Identificación de la vulnerabilidad	Nombre de la vulnerabilidad

Nota. Fuente propia

2.1.2.4 Escenarios del riesgo

Corresponde a la relación que se hizo entre las amenazas y los activos. Es decir, con esta evaluación se identificó para cada activo, las amenazas por las que podría sufrir mayor afectación. Esto es importante para tomar las acciones necesarias que permitan mitigar la posibilidad de materialización de los riesgos. Esta información se consigna en la tabla 2-5, en la cual, se listaron las amenazas verticalmente, y los activos horizontalmente. De modo que, resulta un cruce entre ambos, en el que se observa la identificación amenazas vs. activos:

Tabla 2-5: Escenarios de riesgo

AMENAZAS / ACTIVOS					

Nota: ISO 27005 Gestión de riesgos de la seguridad [58]

2.1.2.5 Agentes generadores

Así mismo, para los escenarios de riesgo identificados se creó la tabla 2-6, en la que se incluyeron los posibles agentes generadores de riesgos y los probables efectos y/o consecuencias que resultarían si estos se materializan. La tabla diseñada está compuesta por los siguientes ítems:

- **Nro**.: identificación del escenario de riesgo
- **Escenario del riesgo:** detalle del escenario de riesgo
- **Agente generador:** agente que puede causar el riesgo
- **Efecto o consecuencia:** consecuencia de materializarse un riesgo

Tabla 2-6 Agentes y consecuencias de los escenarios de riesgo

Nro.	Escenario de riesgos	Agente generador	Efecto o consecuencia

Nota: Fuente propia

2.1.2.6 Calificación del control

Para el desarrollo del presente proyecto, se evaluaron los impactos que pueden generarse al materializarse un riesgo, a nivel de indisponibilidad de la información. Por lo tanto, se diseñó la

tabla 2-7, en la cual se detalla la manera en la que se evaluó el impacto, resaltando el nivel, su rango de gravedad y la respectiva descripción:

Tabla 2-7: Tabla de medición de impacto en información

Impacto a nivel de indisponibilidad de la información		
Nivel	**Rangos**	**Rango detallado de la descripción**
1	**Insignificante**	La situación se presentó en un pequeño porcentaje de la Empresa. El apoyo lo brinda mesa de ayuda
2	**Menor**	Pérdida de la confidencialidad por debajo del 10%, los sistemas están comprometidos en ese mismo nivel.
3	**Intermedio**	Pérdida de la confidencialidad por entre el 10% y el 30%, los sistemas están comprometidos en ese mismo nivel.
4	**Mayor**	Pérdida de la confidencialidad entre el 30% y el 60%, los sistemas están comprometidos en ese mismo nivel.
5	**Superior**	Pérdida de la confidencialidad por encima del 60%, los sistemas están comprometidos en ese mismo nivel.

Nota. Tabla de medición de impacto [17]

Es así como, con la información recopilada se logró la calificación de los controles y sus riesgos. Obteniendo información como, el escenario de riesgo, probabilidad de ocurrencia, impacto, riesgo por impacto, clasificación del activo, controles actuales y la efectividad del control. Por lo tanto, en la tabla 2-8 se consignó la siguiente información:

- **Nro**.: Identificación del escenario de riesgo
- **Escenario de riesgo**: descripción del escenario de riesgo
- **Probabilidad**: Probabilidad de ocurrencia del escenario de riesgo
- **Impacto**: Impacto con el cual se hizo el mapa de riesgo, que para el caso fue a nivel de información.
- **Riesgo por impacto**: riesgo por impacto a nivel de información

Tabla 2-8 Calificación de control

Calificación con Controles				
No.	**Escenario de riesgos**	**Probabilidad**	**Impacto Información**	**Riesgo por Impacto de Información**

Nota: Fuente propia

Finalmente, con base en la información conseguida, se comparó la probabilidad de ocurrencia del riesgo con respecto a su impacto, para así obtener la matriz de calificación, evaluación y respuesta a los riesgos, la cual contiene criterios de riesgos como: aceptables, tolerables, inaceptables e inadmisibles. Esto permite visualizar con mayor detalle los riesgos a los cuales se encuentra expuesta la Organización, priorizarlos y tratarlos.

Cada una de estas se refiere a [17]:

- **Riesgo inadmisible:** Riesgo urgente, de tratamiento inmediato por sus consecuencias
- **Riesgo inaceptable:** Requiere ser evitado o eliminado por sus consecuencias
- **Riesgo tolerable:** Riesgo que se puede eliminar o controlar
- **Riesgo aceptable:** Riesgo que puede aceptarse porque no tiene un efecto catastrófico

Esta información se plasmará en una tabla como la 2-9:

Tabla 2-9: Matriz de clasificación de aceptabilidad

Valor	Consecuencia				
	Insignificante	Menor	Intermedio	Mayor	Superior
	1	2	3	4	5
5					
4					
3					
2					
1					

Nota. Matriz de clasificación [17]

En la tabla 2-10 se define el significado de cada una de las zonas: roja, amarilla, anaranjada y verde, siento las zonas roja y anaranjada las de mayor problemática por su gravedad.

Tabla 2-10: Convenciones

Convenciones	
Color	**Definición**
	Inadmisible
	Inaceptable
	Tolerable
	Aceptable

Nota. Fuente propia

Igualmente, el resultado se mostró en un gráfico circular como el siguiente, en el que según el color de la zona se identifica la aceptabilidad del control. Ver figura 2-3:

- **Rojo**: Inadmisible
- **Anaranjado**: Inaceptable
- **Amarillo**: Tolerable
- **Verde**: Aceptable

Figura 2-3 Figura de aceptabilidad del control

Nota. Aceptabilidad del control [17]

2.2 Fase 2. Definición de controles y mejores prácticas

Con el propósito de dar cumplimiento a esta fase, se construyó un plan de tratamiento para gestionar los riesgos inadmisibles e inaceptables descritos en el mapa de riesgo realizado en la fase anterior. Este permite indicar las acciones que se harán para aceptar, evitar, controlar o transferir los riesgos existentes, teniendo en cuenta los criterios de aceptación definidos.

También, se diseñó una encuesta que se realizó a cuatro empresas reconocidas en el sector de los servicios públicos, las cuales están distribuidas en el territorio colombiano: Manizales, Norte de Santander, Santander y Medellín. La encuesta se realizó en modalidad virtual al colaborador designado por cada una de las empresas mencionadas, donde estos fueron denominados profesionales expertos del proceso de facturación. La encuesta se realizó con el propósito de determinar si las empresas seleccionadas conocen los riesgos a los cuales están expuestas, sus controles y si elaboran y ejecutan su respectivo plan de tratamiento. Además, identificar sus prácticas o acciones asertivas en términos de seguridad de la información, y descubrir si están dispuestas a modificar la forma de ejecutar sus labores y si estuvieran dispuestas a innovar con la utilización de nuevas tecnologías.

Por otro lado, se consolidó el resultado obtenido en el mapa de riesgos elaborado y el resultado de las encuestas realizadas a 4 empresas, con el objetivo de recopilar riesgos, controles existentes e identificar algunos nuevos, para a partir de allí, construir mejores prácticas que, finalmente, apunten a salvaguardar la seguridad de la información de los procesos de facturación ante ataques y ciberataques, y a prevenir la materialización de los riegos hallados previamente.

Los entregables de esta fase son:

- Plan de tratamiento para riesgos inadmisibles e inaceptables
- Encuesta sobre el aseguramiento del proceso de facturación, la cual está en la sesión resultados del presente documento (Encuesta sobre el aseguramiento en el proceso de facturación)
- Construcción de controles para mejores prácticas

2.2.1 Plan de tratamiento para riesgos inadmisibles e inaceptables

Con base en los resultados obtenidos en el mapa de riesgo realizado para el impacto a nivel de indisponibilidad de la información, se realizó su respectivo plan de tratamiento, en el cual, a partir de la valoración del riesgo, los costos de implementación y los beneficios obtenidos, se definió si se aceptan, se evitan, se controlan o se transfieren. Igualmente, se estableció una forma de monitoreo periódico, y se asignaron sus respectivos responsables. El esquema propuesto para el plan de tratamiento consta de los siguientes ítems:

Riesgo: Corresponde al escenario de riesgo al cual se le va a realizar el plan de tratamiento. Posteriormente, a realizar el análisis de cada escenario, se puede tratar según las siguientes opciones [58]:

- **Reducir**: la acción se basa en minimizar el riesgo mediante la implementación de controles, de forma que un riesgo residual pueda llegar a ser un riesgo aceptable.
- **Retener**: "Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de los riesgos"
- **Evitar**: la acción se refiere a evitar la situación que origina el riesgo
- **Transferir**: el riesgo puede transferirse hacia donde se le realice una gestión eficaz

El plan de tratamiento contiene la siguiente información y se consolidó en una tabla como la 2-11, en la que cada ítem se explica a continuación:

- **Riesgo**: riesgo al cual se le realizará el tratamiento
- **Tratamiento**: opción por la que se optará en el tratamiento del riesgo, entre las que se encuentra reducir controlar, retener aceptar, evitar y transferir
- **Descripción del plan:** se describe la manera en la cual se va a realizar el tratamiento, cómo se evitaría o se controlaría, a quién se transferiría y porqué se aceptaría.
- **Plan de monitoreo:** es el seguimiento que se hará al plan de monitoreo establecido
- **Responsables**: quien será la persona o colaborador encargado de cumplir con la opción de tratamiento elegida
- **Resultados esperados**: corresponde al objetivo que se quiere lograr con la implementación del plan de tratamiento.

Tabla 2-11 Plan de tratamiento

RIESGOS	TRATAMIENTO				Descripción del plan	Plan de monitoreo	Responsables	Resultados esperados
	Aceptarlo	Evitarlo	Controlarlo	Transferirlo				

Nota. Construcción de esquema. [17]

2.2.2 Encuesta sobre el aseguramiento en el proceso de facturación

En esta segunda fase alineada con el objetivo específico número 2, se consultaron 4 empresas del sector de servicios públicos, ubicadas en distintos departamentos del territorio colombiano, para determinar si de su proceso de facturación, conocen los riesgos, controles actuales y si hacen uso de estos últimos. Además, observar sus mejores prácticas en el manejo de la seguridad de la información, e identificar si consideran la posibilidad de reestructurar la forma de ejecutar sus actividades incluyendo nuevas tecnologías.

Como se mencionó, la encuesta se realizó en 4 Empresas, donde cada una dispuso de un colaborador designado como profesional experto del proceso de facturación, para un total de 4 colaboradores. Debido a que en la encuesta se obtendría información sensible de datos personales y procesos propios, se incluyó un párrafo relacionado con la no divulgación de información como el nombre de la Empresa y del colaborador, y un argumento asociado la Ley 1581 de 2012 de la protección de los datos personales. Así las cosas, la encuesta incluyó las preguntas contenidas en la tabla 2-12:

Tabla 2-12 Preguntas de la encuesta

ENCUESTA DISEÑADA
1. ¿Su Empresa dispone de un respaldo actualizado con la información necesaria para continuar con los procesos de lectura, ingreso de tarifas, liquidación de consumos, impresión, etc. , en caso de presentarse algún fallo inesperado en su sistema facturador?
2. ¿Se tiene implementado el método de segregación de funciones en el aplicativo facturador? La segregación de funciones es un método que permite separar responsabilidades de sus colaboradores con base en las diferentes actividades que ejecutan.
3. ¿Se tienen identificados los riesgos del proceso, inherentes a la seguridad de la información?
4. Si la respuesta anterior es positiva, por favor informe mínimo 5 riesgos que tiene identificados en el proceso de facturación
5. ¿Se tienen controles para los riesgos identificados en el proceso?
6. Si la respuesta anterior es positiva, por favor enuncie mínimo 5 controles, de los identificados en el proceso de facturación
7. ¿Alguno de los controles ya establecidos, valida que la información incluida para la liquidación de los consumos permanece íntegra durante todo el proceso de facturación?
7.1 Describa el o los controles
8. ¿Ha calculado qué impacto podría tener a nivel de información, si se materializara un riesgo?
9. ¿Este cálculo lo ha hecho recientemente (Un año)?
10. ¿Se hacen monitoreos y seguimientos frecuentes sobre la ejecución y el resultado de los controles?
11. ¿Se tienen lineamientos establecidos para la administración de la seguridad de la información en el aplicativo facturador?
12. ¿Se garantiza la completitud de cada una de las fases que componen el proceso de facturación, antes de continuar con la siguiente?. Lo anterior, considerando que dichos procesos constan de fases como: lectura, análisis, liquidación, entre otras.
13. ¿Conoce los riesgos que tienen sus proveedores y contratistas, asociados a la seguridad de su información?
14. ¿Conoce los controles que tienen sus proveedores y contratistas, asociados a la seguridad de la información?
15. ¿Se considera que el proceso de liquidación cuenta con los pilares de seguridad de la información: integridad, disponibilidad y confidencialidad?
Explique
16. Califique de 1 a 10 el grado de satisfacción con el proceso actual de facturación
17. ¿Renunciaría al proceso de facturación actual si tuviera evidencia de obtener mayor seguridad en la información y en el proceso de facturación, a través de la implementación de nuevas tecnologías?
18. ¿Se han explorados nuevas tecnologías como: blockchain, internet de las cosas, entre otras, ¿para reemplazar el proceso de facturación actual?
19. ¿Cuál? o ¿Cuáles?

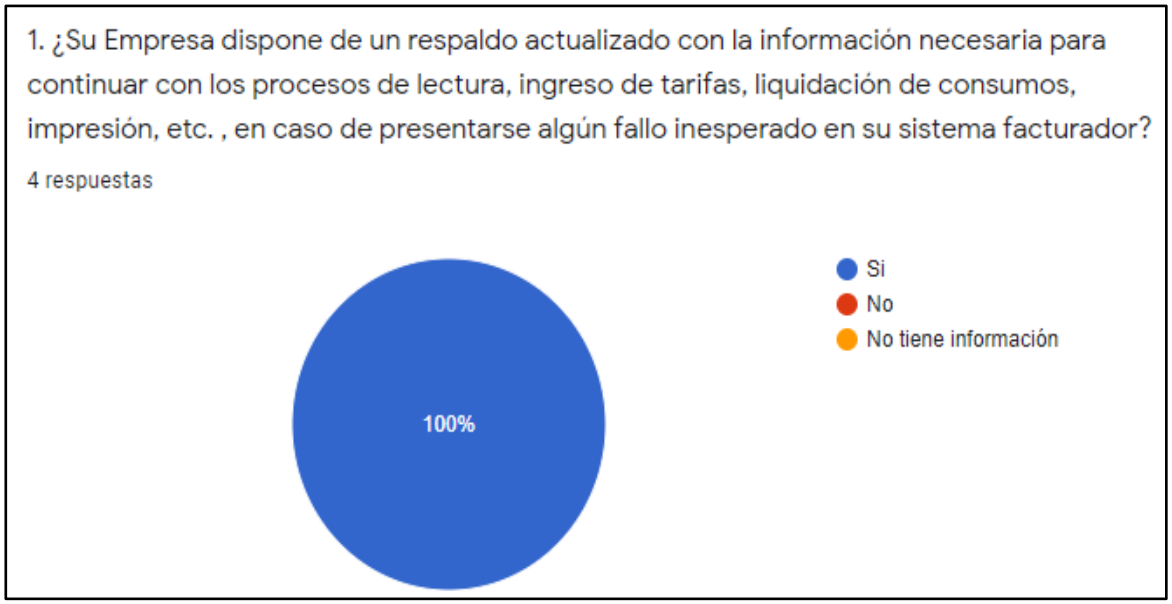
Nota. Fuente propia

La encuesta, que constó de preguntas con respuestas abiertas y cerradas, fue enviada digitalmente a las direcciones de electrónico de los destinatarios que fueron informadas por cada empresa, otorgando un tiempo prudente de respuesta, para que la respondieran concienzudamente.

Posteriormente, cada profesional regresó su respectiva encuesta diligenciada. Una vez recibidas, se consolidó la información recolectada, se analizó y se tabuló en Excel, logrando emitir para cada pregunta, un gráfico circular o una tabla, para facilitar su lectura e interpretación.

Para la algunas de las respuestas se diseñó un diagrama circular como el que se presenta en la figura 2-4. Para otras de ellas se hizo la presentación en tablas. No obstante, en ambos escenarios, para cada pregunta y respuesta, se adicionó su correspondiente análisis y conclusión:

Figura 2-4 Ejemplo de diagrama circular



Nota: Fuente propia

En el ejemplo plasmado en la figura 2-4, se evidencia inicialmente la pregunta realizada, las opciones de respuesta, y con base en ello el diagrama. Por lo tanto, para el ejemplo, las 4 empresas encuestadas respondieron positivamente a la pregunta planteada. Así mismo, en la sesión de los resultados, se detalló la conclusión obtenida a partir de la respuesta dada.

2.2.3 Construcción de controles para mejores prácticas

El resultado obtenido en la fase 1 permitió identificar los riesgos a los que están expuestos los procesos de facturación de las empresas y la cuantificación de su gravedad. Aunado a ello, en la presente fase se construyó un plan de tratamiento para dichos riesgos. Además, se analizó y se

tabuló la información resultante de la encuesta realizada a las diferentes empresas pertenecientes al sector de servicios públicos.

Con base en los resultados obtenidos a través de las actividades ya mencionadas, se obtuvieron insumos valiosos que permitieron identificar, definir y proponer nuevas medidas y controles que constituyen mejores prácticas que apuntan a la disminución de la probabilidad de ocurrencia de los riesgos, y por tanto, apuntar a asegurar la información de los procesos en sus principios fundamentales: confidencialidad, integridad y disponibilidad.

La información de los controles para mejores prácticas se registró en una tabla como la 2-13, para la cual se describen los siguientes campos:

- **Actividad**: Acción que se ejecuta
- **Control actual**: control que existe y fue diseñado para una determinada actividad que se ejecuta
- **Usabilidad**: indica si el control existente es utilizado
- **Efectividad**: indica si el control existente es funcional, es efectivo.
- **Control propuesto**: controles que se proponen ante una determinada actividad
- **Control definitivo**: Seleccionar un control definitivo para una actividad que se ejecuta
- **¿Por qué?:** explicación detallada de la razón por la cual se seleccionó un control.

Tabla 2-13 Encuesta de controles

Actividad	Control actual	Usabilidad	Efectividad	Control propuesto	Control definitivo	¿Porqué?
		SI/NO	SI/NO		SI/NO	

Nota: Fuente propia

2.3 Fase 3. Usos y metodología de adaptación y aplicación de blockchain

Para cumplir con la presente fase asociada al objetivo específico número 3, se investigó sobre los diferentes usos que se le ha dado a la tecnología blockchain, en medios como: bases de datos

científicas, páginas web, conferencias, libros y demás publicaciones. Adicionalmente, se hicieron consultas a empresas que actualmente incluyen dicha tecnología en sus procesos.

Igualmente, con la investigación realizada y al conocer los diferentes usos que tiene la tecnología, también se identificaron sus mejores prácticas, y se analizó como éstas se pueden aplicar en el presente proyecto, con el objetivo de aportarlas para el mejoramiento del proceso de facturación tradicional que tienen las ESP.

Adicionalmente, en la presente fase también se propuso una metodología que plantea y explica la manera de adaptar y aplicar la tecnología blockchain en el proceso de facturación de las Empresas de servicios públicos. Dicha metodología está compuesta por 16 etapas que fueron debidamente definidas, aclaradas y detalladas en la sesión de resultados, especificando cómo se llevarían a cabo, sus actores e indicando sus respectivos entregables. Para la propuesta entregada se tuvo en cuenta la investigación que se ha realizado sobre los procesos de facturación, blockchain, metodologías ágiles, experiencias corporativas y todos los resultados obtenidos en el presente documento.

Los entregables que se obtendrán en esta fase son:

- Evaluación del uso de blockchain en empresas donde se encuentra implementado y otros
- Mejores prácticas investigadas en el uso de blockchain vs los riesgos hallados previamente
- Metodología para la adaptación y aplicación de blockchain

2.3.1 Evaluación del uso de blockchain en empresas donde se ha implementado y otros

La información investigada en cada una de las fuentes consultadas se analizó y se compiló, extrayendo los diferentes usos que se han aplicado a blockchain. Usos que dan mayor claridad y certeza sobre que, es una tecnología disruptiva, versátil que ofrece diferentes bondades en términos de seguridad de la información, trazabilidad en el proceso, permite la información en línea, entre otros. Es importante mencionar que, para la mayoría de las fuentes consultadas, fue posible identificar y relacionar el proceso donde esta tecnología es aplicada.

Esta información se presentó en una tabla como la 2-14, en la que sus columnas se refieren a:

- **Empresa/proyecto:** Empresa, emprendimiento o proyecto donde se utiliza la tecnología blockchain
- **Proceso**: Proceso interno de la Empresa en el cual se aplica blockchain
- **Usabilidad**: Uso o usos que se le da a blockchain
- **Bibliografía**: Fuente de la cual se extrajo la información

Tabla 2-14 Usos de blockchain

Empresa/proyecto	Proceso	Usabilidad	Bibliografía

Nota: Fuente propia

2.3.2 Mejores prácticas investigadas en el uso de blockchain vs los riesgos hallados previamente

Para los diferentes usos que se le ha dado a blockchain se hallaron y se listaron las mejores prácticas. Estas prácticas positivas o mejores prácticas se llevaron a un paralelo, con los riesgos hallados en la primera fase del presente documento. Con esta información, se identificó para cada uno de los riesgos, una buena práctica que ayude a mitigarlo, para así mejorar el proceso y propender porque sea más seguro.

Tener identificados la mayoría de los riesgos presentes en el proceso de facturación es una gran ganancia en términos de seguridad, pero ejercer mejores prácticas que ayuden a minimizar la posibilidad de ocurrencia de estos, es aún más beneficioso para el proceso y en gran medida, aporta para que dicho proceso cumpla con los tres pilares de la seguridad de la información: Disponibilidad, integridad y confidencialidad.

Estas mejores prácticas, se relacionaron en la tabla 2-15 que contiene la siguiente información:

- **Empresa/proyecto:** Empresa, emprendimiento o proyecto donde se evidenció la buena práctica

- **Mejores prácticas:** Acciones que hacen que han dado buenos resultados en los procesos que son aplicadas
- **Riesgo**: Riesgo que se puede evitar con la acción hallada

Tabla 2-15: Comparación entre diferentes empresas que ya implementaron blockchain

Empresa/proyecto	Riesgos identificados en el proceso facturación	Mejores prácticas

Nota: Fuente propia

2.3.3 Metodología para la adaptación y aplicación de blockchain

Corresponde a una propuesta compuesta por diferentes etapas secuenciales, en las cuales se plantea detallada y escalonadamente, la forma o manera de adaptar y aplicar blockchain en el proceso de facturación de una empresa que presta los servicios públicos de acueducto, alcantarillado, energía y gas natural residencial.

La construcción de cada una de las etapas se hizo teniendo en cuenta la necesidad que tienen las Organizaciones de conocer su proceso de facturación, sus riesgos y la normatividad que lo rige, identificar sus actores involucrados y dependencias interesadas, y asegurar su información. Además, del estudio que se realizó sobre diferentes metodologías, cómo las ágiles, y el análisis y estudio sobre la tecnología blockchain. Por lo que, en la tabla 2-16, se nombran las etapas que se incluyeron en la metodología:

Tabla 2-16 Fases de la metodología propuesta

FASES DE LA METODOLOGÍA
Definir el equipo de trabajo
Capacitar al equipo de trabajo sobre la tecnología blockchain
Levantar requerimientos
Conocer el proceso de facturación de la compañía
Costo inicial
Identificar las aplicaciones y herramientas
Hacer mapa de riesgos
Diseñar plan de tratamiento
Construir controles para mejores prácticas
Evaluar la pertinencia de adaptar y aplicar blockchain

FASES DE LA METODOLOGÍA
Justificar la pertinencia de la implementación
Contratar empresa experta en desarrollar blockchain para su adaptación y aplicación
Entrega de resultados
Capacitar a los equipos de trabajo sobre la adaptación y aplicación
Revisión del costo
Gestionar el proyecto

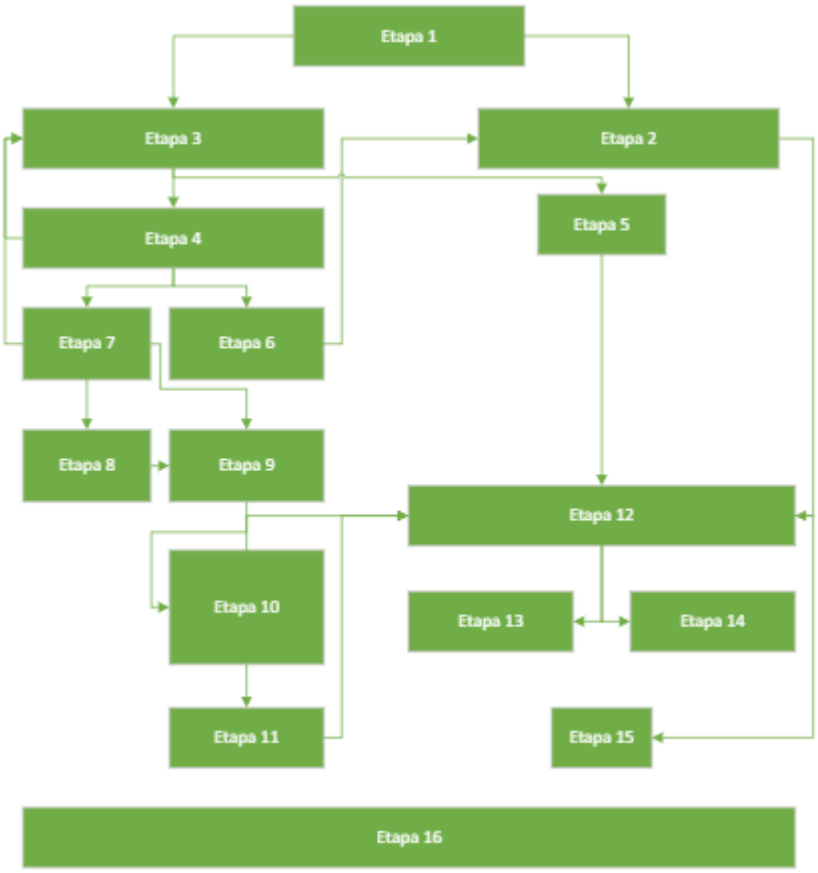
Nota. Fuente propia

Con base en las etapas mencionadas, la metodología propuesta se estructuró en un diagrama como el de la Figura 2-5, en el que se relacionaron cada una de las dieciséis etapas que la integran, con su respectivo orden y/o dirección de ejecución.

Posteriormente, en el apartado de resultados del presente proyecto, se explicó detalladamente cada una de estas etapas, indicando su significado, su forma de ejecución, sus responsables y los entregables definidos.

Con respecto al diagrama, es importante aclarar que, los rectángulos representan cada una de las 16 etapas que componen la metodología, y las líneas de flujo o flechas, muestran la relación, secuencia y dirección existente entre cada una. Igualmente, cuando de una sola etapa nacen varias líneas de flujo, significa que desde esa etapa se tiene dirección a varias etapas. Ver figura 2-5:

Figura 2-5 Diagrama de la metodología para adaptar y aplicar blockchain



Nota. Fuente propia

2.4 Fase 4. Comparativo entre el proceso de facturación actual y utilizando blockchain

El propósito de la presente fase correspondiente al objetivo número 4, fue validar el diseño de la metodología propuesta. Para ello, a lo largo de la ejecución del proyecto, se han realizado diferentes procedimientos que se aportan como pruebas sugeridas, validadas y verificadas, toda vez que nacen de la investigación realizada en bases de datos científicas, en las empresas debidamente constituidas con vasta trayectoria y experiencia en los servicios públicos domiciliarios, y en las empresas donde ya se utiliza blockchain.

Adicionalmente, por medio de la comparación entre el modelo tradicional de protección que se tiene implementado en el proceso de facturación, y el modelo adaptando y aplicando blockchain. Comparación en la que, como se mencionó, se consideraron los resultados obtenidos hasta el momento a lo largo del proyecto, pues estos permitieron identificar riesgos, controles y diversas acciones presentes entre un proceso y otro. Además, de contar con la experiencia de empresas del sector que enriquecieron el contenido del presente documento. Todo en aras de procurar por que el proceso que se eligió sea idóneo y el que realmente apunte a obtener y/o conservarlos principios de la seguridad de la información en la Organización.

Para ello, se seleccionaron 4 grandes criterios que se consideraron clave para concluir cómo es mejor llevar a cabo el proceso de facturación, si con la manera actual o adaptando y aplicando blockchain. A cada uno de estos criterios se les asignó un porcentaje de calificación de 1% a 100%, y entre todos sumaron un 100%.

Los criterios elegidos se hallan valiosos, importantes y estratégicos, toda vez que aportan para que los procesos funcionen óptima y eficazmente, para ofrecer una mejor experiencia al cliente y, sobre todo, para velar por la seguridad de la información. Estos fueron:

- Funcionalidad
- Tempos de respuesta
- Seguridad de la información
- Costos

La calificación obtenida se consideraron los riesgos y su tratamiento, el resultado consolidado de las encuestas, las mejores prácticas recomendadas para la mitigación de los riesgos, las experiencias de otras empresas e implementaciones y los aprendizajes obtenidos sobre el proceso de facturación de las empresas de servicios públicos y sobre blockchain. No obstante, una vez se realice el desarrollo, la empresa contratante puede repetir la evaluación y determinar si hubo alguna variación en los resultados.

2.4.1 Valoración de criterios con el método tradicional vs adaptando y aplicando blockchain

El entregable de esta fase será la calificación de criterios, los cuales son evaluados en una tabla que contendrá los siguientes ítems:

- **Criterio:** Aspecto que se eligió para valorar la metodología diseñada en la fase 3 del presente documento. Los criterios establecidos fueron:

    - **Funcionalidad:** se refiere a la capacidad que tiene el modelo para cumplir constantemente con sus especificaciones. Es decir, independientemente de la opción elegida, el proceso de facturación debe continuar su curso con toda normalidad, sin que sufra alteraciones que puedan afectar el producto final, que es la emisión de la factura. El porcentaje de este criterio en total fue 30%.

    - **Tiempos de respuesta:** el modelo debe disminuir los tiempos que transcurren entre cada tarea incluida en las etapas del proceso de facturación, así mismo, este tiempo debe disminuir entre etapas, de modo que la respuesta al cliente y usuario sea más ágil. El porcentaje de este criterio en total fue 20%.

    - **Seguridad de la información:** El modelo deberá cumplir con los principios fundamentales de seguridad de la información, los cuales son la confidencialidad, la integridad y la disponibilidad. El porcentaje de este criterio en total fue 30%.

    - **Costos:** Hace referencia a que el costo de continuar con el modelo tradicional o implementar blockchain debe recuperarse posteriormente a su implementación. En los costos se validó no solo la implementación, también los costos en los que se puede incurrir por las manualidades y demás ajustes por inconsistencias. El porcentaje de este criterio fue 20%.

- **Porcentaje:** En adelante %, es el porcentaje de calificación que se dió a cada criterio, tanto para el modelo tradicional, como adaptando y aplicando blockchain**.**

De acuerdo con lo informado, la tabla diseñada para plasmar la valoración realizada será la 2-17:

Tabla 2-17: Comparativo método tradicional vs Implementación blockchain

Modelo	Funcionalidad	%	Criterio
Modelo tradicional de protección en el proceso de facturación de una empresa de servicios públicos domiciliarios			
Implementación de blockchain en una empresa de servicios públicos domiciliarios			

Nota. Fuente propia

Igualmente, el resultado final será compilado en una tabla como la siguiente 2-18:

Tabla 2-18 Valoración final

Criterio	Porcentaje	Porcentaje de calificación al modelo tradicional de protección en el proceso de facturación de una empresa de servicios públicos	Porcentaje de calificación a la adaptación y aplicación de blockchain en una empresa de servicios públicos

Nota: Fuente propia

2.5 Marco lógico

En la tabla 2-19 se resume para cada objetivo específico, las actividades que se realizaron, además, sus respectivos indicadores de cumplimiento.

Tabla 2-19 Marco lógico

Objetivo	Actividades	Indicadores
Identificar las posibles amenazas y vulnerabilidades del proceso de facturación, a partir de la realización de un mapa de riesgos	*Realizar proceso de facturación *Realizar mapa de riesgos -Identificar activos -Identificar amenazas -Identificar vulnerabilidades -Establecer escenarios del riesgo -Agentes generadores -Calificación del control	*Diagrama con el proceso de facturación general estructurado *Mapa de riesgos
Caracterizar las diferentes soluciones o controles de seguridad tradicionales del proceso de facturación, para construir uno con las mejores prácticas	*Definición de controles *Encuesta sobre el aseguramiento del proceso de facturación *Definición de mejores prácticas	*Plan de tratamiento *Resultado de encuesta realizada a varias empresas del sector *Construcción de controles para mejores prácticas
Evaluar diferentes usos que se han dado utilizando blockchain, y recopilar de estas experiencias las mejores prácticas que puedan ser aplicadas en la reducción de riesgos del proceso de facturación, con el fin de proponer una metodología de implementación	*Evaluación del uso de blockchain en empresas donde se ha implementado y otros *Mejores prácticas investigadas en el uso de blockchain vs los riesgos hallados previamente *Metodología de adaptación y aplicación de blockchain	*Evaluación de usos que se han dado a blockchain *Recomendar mejores prácticas en el uso de blockchain vs los riesgos previamente hallados *Metodología propuesta para la adaptación y aplicación de blockchain
Validar el diseño de la metodología, a través de la comparación entre un modelo tradicional de protección y la tecnología blockchain	*Comparativo entre el proceso de facturación actual y utilizando blockchain	*Valoración de criterios con el método tradicional vs implementando blockchain

Nota: Fuente propia

3. Resultados

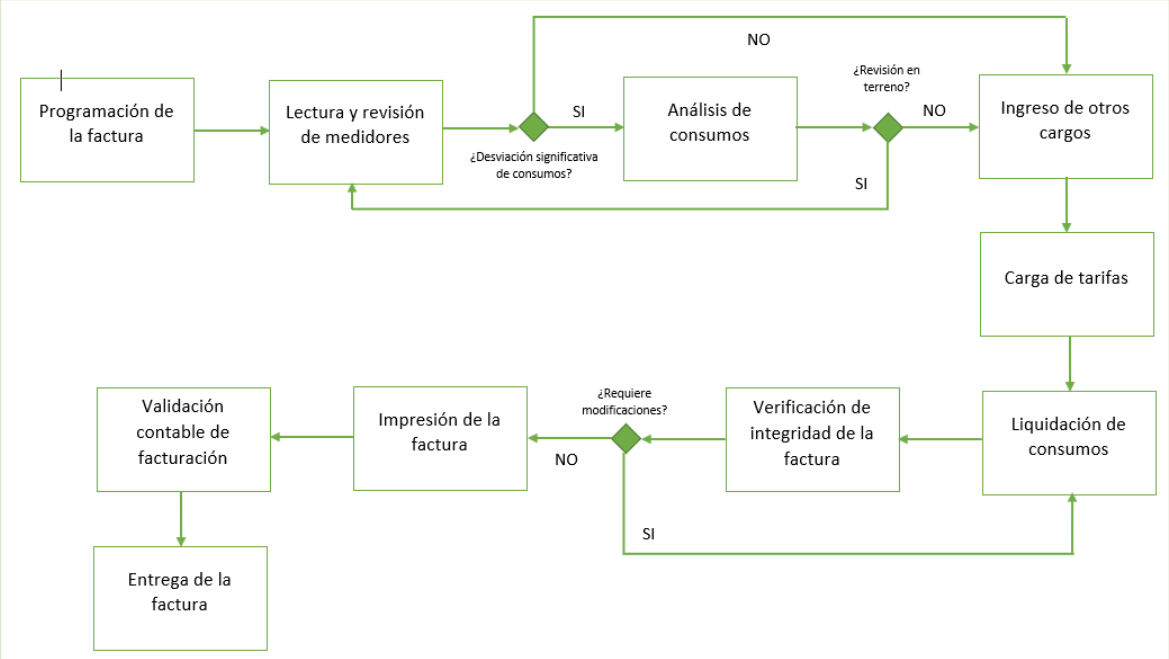
A continuación, se presentarán los resultados obtenidos en cada una de las fases incluidas en la metodología, para el cumplimiento de los objetivos.

3.1 Fase 1. Proceso de facturación general y mapa de riesgos

3.1.1 Proceso de facturación general

Con base en los procesos de facturación estudiados de diferentes empresas y que fueron incluidos en el marco teórico, se construyó el siguiente proceso de facturación general, el cual consta de 10 grandes fases, las cuales son secuenciales, y en las que se garantiza que antes de pasar a la siguiente se debe surtir la anterior. Este podrá ser implementado en cualquier empresa de servicios públicos, cumpliendo con la normatividad vigente y a la luz de las tecnologías de hoy, como blockchain. En la figura 3-1 se encuentra el proceso estructurado:

Figura 3-1: Proceso de facturación general



Nota: Fuente propia

Las actividades que componen el proceso mencionado integran el proceso de principio a fin. Iniciando desde la lectura de los medidores hasta la entrega de la factura física o por correo electrónico. A continuación, se describe a qué se refiere cada actividad:

- **Programación de la factura:** La población a la cual se le facturará por concepto de servicios públicos domiciliarios es dividida por zonas, y una vez esto ocurre, se hace la programación, lo cual se refiere al cronograma que se crea para detallar las fechas en las cuales se realizarán las fases descritas en el proceso de facturación diseñado. Por ejemplo, si la Empresa presta el servicio en un departamento específico del país, este se distribuye en zonas, a las cuales les asignan fechas en las que debe garantizarse la ejecución de cada una de las fases que se incluyeron en el proceso construido. Es decir, las 10 fases diseñadas, deben ejecutarse para cada una de las zonas establecidas.

  Esta actividad se puede planear anualmente, aunque con posibilidades de sufrir modificaciones. Y es realizada por el equipo de trabajo encargado de hacer la distribución de la población por zonas y por lectores. Una vez se realiza la programación de la factura, se continúa con la fase Nro. 2: Lectura y revisión de medidores.

- **Lectura y revisión de medidores**: es la acción que realiza el colaborador con el rol de lector, en la cual se dirige a cada inmueble y registra la lectura que halla en cada medidor de energía, acueducto y gas. Una vez toma las lecturas, el lector se desplaza hasta su lugar de trabajo y descarga la información en el aplicativo de lecturas.

  Esta actividad la pueden hacer contratistas de la Empresa con el cargo de lector en campo, a través de la terminal de lectura que se le asigne.

  En esta fase, también se puede hacer una segunda revisión al inmueble si es necesaria, dada alguna desviación significativa. O igualmente, si se requiere, puede retirarse alguno de los medidores que deba ser revisado e instalar uno provisional.

  A partir de la lectura tomada pueden presentarse dos escenarios. Si se presenta desviación significativa en el consumo, se debe pasar a la fase Nro. 3: Análisis de consumo. Si, por el

contrario, el consumo está dentro del promedio normal del inmueble, pasa a la fase Nro. 4: Ingreso de otros cargos.

- **Análisis de consumos**: se refiere a revisar aquellas instalaciones cuyos consumos presentaron desviaciones significativas a partir de su lectura. Esta revisión puede hacerse con la información de los sistemas, o si es del caso, debe solicitarse la revisión al inmueble o directamente llevar el medidor en el laboratorio.

  Esta actividad es realizada por un equipo de trabajo que se encarga de revisar minuciosamente los consumos y todo el contexto de facturación en los inmuebles específicos, porque posterior a la revisión se toma la decisión de confirmarse o ajustarse el cobro generado inicialmente, y cualquiera de estas decisiones debe estar debidamente soportada.

  Si realizado el análisis no se tiene claridad y/o soportes requeridos para ratificar el cobro, puede enviarse nuevamente la instalación a la fase Nro. 2: Lectura y revisión de medidores. Si, por el contrario, el consumo no presentó ningún tipo de anormalidad, se continúa con la fase Nro. 4: Ingreso de otros cargos.

- **Ingresos de otros cargos**: son los valores adicionales que deben incluirse en la factura, como los cobros de terceros: alumbrado público, aseo, mínimo vital, entro otros que la norma permita o exija.

  Esta tarea es realizada por el equipo de trabajo que tenga relación con las empresas que prestan los servicios mencionados. Estas empresas deberán compartir la información de sus cobros para que dicho equipo la incorpore posteriormente al aplicativo facturador.

  Una vez se ingresa la información en el facturador, se puede continuar con la fase Nro. 5: Carga de tarifas.

- **Carga de tarifas:** son los archivos que contienen los valores correspondientes a cada metro cúbico o kilovatio hora, para los servicios de acueducto, alcantarillado, gas y energía. Estos

valores resultan de acuerdo con la categoría, el estrato, el servicio, el departamento, la localidad, entre otros.

Esta actividad la desarrolla un equipo de trabajo que constantemente debe actualizarse sobre las tarifas de los servicios públicos domiciliarios, para que ante algún cambio se hagan las modificaciones a lugar. Siempre que se tenga la información de las tarifas deberá ingresarse al aplicativo facturador.

- **Liquidación de consumos:** proceso en el cual se liquidan los consumos de cada servicio, con base en las tarifas cargadas. Es decir, se hacen los respectivos cálculos entre los consumos, tarifas y demás componentes del costo para emitir los valores incluidos en la factura.

  Este proceso debe realizarlo el equipo encargado de liquidar por medio del aplicativo facturador, todos los consumos y demás cargos necesarios para la obtención de los valores a cobrar.

  Posteriormente, se continúa con la fase Nro. 7: Verificación de la integridad de la factura.

- **Verificación de la integridad de la factura:** revisión que se hace post liquidación de la factura y antes de imprimirla, para garantizar su calidad. En esta revisión se hacen análisis estadísticos donde se evidencien variaciones que requieren ser revisadas.

  Corresponde a un equipo de trabajo que se encarga de forma aleatoria de revisar diferentes facturas de los servicios de acueducto, alcantarillado, gas y energía. Esto lo hacen por medio del facturador.

  Si revisada la facturación se encuentra alguna inconsistencia, es necesario regresar a la fase Nro. 6: Liquidación de consumos, para que allí se hagan las correcciones necesarias. No obstante, sino se presentó ninguna inconsistencia, se continúa con la fase Nro. 8: Impresión de la factura.

- **Impresión de la factura**: proceso en el que la Empresa prestadora de servicios envía los paquetes de impresión a la empresa encargada de imprimir los documentos. Una vez esta empresa los imprime, los regresa para su repartición a los clientes y usuarios.

  Esta actividad es tercerizada, ya que la ejecuta una empresa contratista encargada de la impresión masiva de facturas. Dicha empresa debe cumplir con las cláusulas incluidas en los contratos.

  Al dejar en firme la facturación, se continúa con la fase Nro. 9: Validación contable de la factura.

- **Validación contable de facturación:** revisión que se hace de los valores facturados para garantizar que la información de los estados financieros es la que corresponde.

  Este equipo de trabajo revisa a través del aplicativo facturador que los reportes contables coincidan con la facturación. Si se encuentra alguna inconsistencia, en esta misma fase deben gestionare las correcciones a lugar.

  Posteriormente, se continúa con la fase Nro. 10: Entrega de la factura.

- **Entrega de la factura:** repartición de las facturas a los clientes en su dirección de domicilio o vía correo electrónico, de acuerdo con su elección. La repartición de las facturas físicas es planificada previamente según las zonas asignadas, y es realizada por personal contratista.

  Igualmente, las facturas que se envían por correo electrónico son enviadas por correo certificado.

3.1.2 Mapa de riesgos

3.1.2.1 Identificación de activos

Con base en las fases incluidas en el proceso de facturación general que se construyó, se identificaron los activos más relevantes que las integran. Esto es importante porque permitió

identificarlos, clasificarlos según su tipo: lógico o físico, identificar su criticidad, y reconocer claramente con cuál o cuáles de las fases del proceso de facturación se relacionan, para el evento en que ocurra algún tipo de situación o que simplemente se requiera. Por tanto, a continuación, en la tabla 3-1 se observa el inventario de activos:

Tabla 3-1: Resultado de la identificación de activos

Identificación	Nombre	Descripción	Fase del proceso de facturación	Tipo	Crítico
1	Bases de datos	"Una base de datos es una colección organizada de información estructurada, o datos, típicamente almacenados electrónicamente en un sistema de computadora. Una base de datos es usualmente controlada por un sistema de gestión de base de datos (DBMS). En conjunto, los datos y el DBMS, junto con las aplicaciones que están asociados con ellos, se conocen como un sistema de base de datos, que a menudo se reducen a solo base de datos" [47].	° Lectura y revisión de medidores ° Análisis de consumos ° Ingresos de otros cargos ° Carga de tarifas ° Liquidación de consumos ° Validación contable de facturación	Lógico	Si
2	Cliente	"Persona que compra en una tienda, o que utiliza con asiduidad los servicios de un profesional o empresa" [48]	° Lectura y revisión de medidores ° Entrega de la factura	Físico	Si
3	Contratista	"Que realiza una obra o presta un servicio por contrato" [48]	° Lectura y revisión de medidores ° Impresión de la factura ° Entrega de la factura	Físico	Si

Identificación	Nombre	Descripción	Fase del proceso de facturación	Tipo	Crítico
4	Empleado	“"Persona que por un salario o sueldo desempeña los trabajos domésticos o ayuda en ellos" [48].	° Programación de la factura ° Lectura y revisión de medidores ° Análisis de consumos ° Ingresos de otros cargos ° Carga de tarifas ° Liquidación de consumos ° Verificación de integridad de la factura ° Impresión de la factura ° Validación contable de facturación ° Entrega de la factura	Físico	Si
5	Factura	“Cuenta en que se detallan con su precio los artículos vendidos o los servicios realizados y que se entrega al cliente para exigir su pago” [48].	° Verificación de integridad de la factura ° Impresión de la factura ° Validación contable de facturación ° Entrega de la factura	Físico	Si
6	Herramienta ofimática	“Automatización, mediante sistemas electrónicos, de las comunicaciones y procesos administrativos en las oficinas” [48].	° Programación de la factura ° Carga de tarifas ° Verificación integridad de la factura ° Validación contable de facturación	Lógico	Si

Identificación	Nombre	Descripción	Fase del proceso de facturación	Tipo	Crítico
7	Información	"La información es un conjunto de datos con significado que estructura el pensamiento de los seres vivos, especialmente, del ser humano "[51].	° Programación de la factura ° Lectura y revisión de medidores ° Análisis de consumos ° Ingresos de otros cargos ° Carga de tarifas ° Liquidación de consumos ° Verificación de integridad de la factura ° Impresión de la factura ° Validación contable de facturación ° Entrega de la factura	Lógico	Si
		"Para la informática, para el caso, la información es el conjunto de datos organizados y procesados que constituyen mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que tenga lugar en relación con un ordenador" [51].			
8	Proveedor de impresión	"Dicho de una persona o de una empresa: Que provee o abastece de todo lo necesario para un fin a grandes grupos, asociaciones, comunidades" [48].	° Impresión de la factura	Físico	Si

Identificación	Nombre	Descripción	Fase del proceso de facturación	Tipo	Crítico
9	Servidor	"Puede entenderse como servidor tanto el software que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él. Así, se entiende por servidor tanto el equipo que almacena una determinada información como el programa de software encargado de gestionar dicha información y ofrecerla" [14].	° Lectura y revisión de medidores ° Análisis de consumos ° Ingresos de otros cargos ° Carga de tarifas ° Liquidación de consumos ° Verificación de integridad de la factura ° Validación contable de facturación	Físico	Si
10	Sistema o aplicación de gestión de direcciones	"Un sistema es un conjunto de funciones que operan en armonía o con un mismo propósito, y que puede ser ideal o real. Por su propia naturaleza, un sistema posee reglas o normas que regulan su funcionamiento y, como tal, puede ser entendido, aprendido y enseñado" [52].	° Lectura y revisión de medidores	Lógico	Si
		"Una aplicación es un programa de computadora que se utiliza como herramienta para una operación o tarea específica" [53].			

Identificación	Nombre	Descripción	Fase del proceso de facturación	Tipo	Crítico
		Para el caso, el sistema y/o aplicación, estarían diseñados para la administración las direcciones asociadas a los inmuebles a los cuales se les presta el servicio.			
11	Sistema o aplicación facturador	"Un sistema es un conjunto de funciones que operan en armonía o con un mismo propósito, y que puede ser ideal o real. Por su propia naturaleza, un sistema posee reglas o normas que regulan su funcionamiento y, como tal, puede ser entendido, aprendido y enseñado" [52].	° Programación de la factura ° Análisis de consumos ° Ingreso de otros cargos ° Carga de tarifas ° Liquidación de consumos ° Validación contable de facturación	Lógico	Si
		"Una aplicación es un programa de computadora que se utiliza como herramienta para una operación o tarea específica" [53].			
		Para el caso, el sistema y/o aplicación, estarían diseñados para la administración de la facturación de los servicios públicos domiciliarios.			

Identificación	Nombre	Descripción	Fase del proceso de facturación	Tipo	Crítico
12	Software o aplicación de lectura	"Un sistema es un conjunto de funciones que operan en armonía o con un mismo propósito, y que puede ser ideal o real. Por su propia naturaleza, un sistema posee reglas o normas que regulan su funcionamiento y, como tal, puede ser entendido, aprendido y enseñado" [52].	° Lectura y revisión de medidores	Lógico	Si
		"Una aplicación es un programa de computadora que se utiliza como herramienta para una operación o tarea específica" [53].			
		Para el caso, el sistema y/o aplicación, estarían diseñados para la administración de las lecturas tomadas en los medidores de cada inmueble en el que se presta el servicio.			
13	Terminal de lectura	Máquina con teclado y pantalla mediante la cual se proporcionan datos a una computadora central o se obtiene información de ella.	° Lectura y revisión de medidores	Físico	Si

Nota. Fuente propia

Adicionalmente, al inventario de activos anterior, en la tabla 3-2 se relacionó el impacto que tendrían los activos en los principios de seguridad de la información: confidencialidad, integridad y disponibilidad, en el evento de materializarse un riesgo en alguno de ellos:

Tabla 3-2 Relación activos y principios de seguridad de la información

Activo	Principio	Motivo de afectación
Bases de datos	Confidencialidad Integridad Disponibilidad	*Si la base de datos es atacada, dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad. *Al presentarse un ataque en la base de datos, personas malintencionadas y atacantes podrían acceder a la información confidencial. *Si no se realiza una debida segregación de funciones, personal no autorizado puede acceder a información que no corresponde
Cliente	Integridad	*Si la base de datos es atacada, dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad. *Al cliente ser atacado, puede afectar la información de la cuenta de facturación que tenga en la Organización. *Si el cliente recibe un ataque puede perder las credenciales de la cuenta que tenga para acceder a la información de su facturación, y a partir de allí el atacante puede realizar las transacciones que considere y que la página permita al loguearse
Contratista	Confidencialidad Integridad Disponibilidad	*Si el contratista es atacado puede ser utilizado como vector de ataque para acceder a la información confidencial de las bases de datos y aplicativos de la Organización, y dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad.
Empleado	Confidencialidad Integridad Disponibilidad	*Si el empleado es atacado puede ser utilizado como vector de ataque para acceder a la información confidencial de las bases de datos y aplicativos de la Organización, y dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad.
Factura	Confidencialidad	*En el evento que por algún motivo la Organización pierda las facturas de los clientes y usuarios, y con esta los atacantes hagan mal uso de los datos personales (Ley 1581 de 2012).

Activo	Principio	Motivo de afectación
Herramienta ofimática	Confidencialidad	*Al materializarse algún tipo de ataque en las herramientas ofimáticas, dependiendo de este, puede verse afectado uno a varios principios de la seguridad de la información.
	Integridad	
	Disponibilidad	
Información	Confidencialidad	*Al materializarse algún tipo de ataque en la información, dependiendo de este, puede verse afectado uno a varios principios de la seguridad de la información.
	Integridad	
	Disponibilidad	
Proveedor de impresión	Confidencialidad	*Si el proveedor es atacado, puede ser utilizado como vector de ataque para acceder a la información confidencial de las bases de datos y aplicativos de la Organización, y dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad.
	Integridad	
	Disponibilidad	
Servidor	Confidencialidad	*Si el servidor es atacado, dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad.
	Integridad	
	Disponibilidad	
Sistema o aplicación de gestión de direcciones	Confidencialidad	*Si el sistema o aplicación de gestión de direcciones es atacado, dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad.
	Integridad	
	Disponibilidad	
Sistema o aplicación del facturador	Confidencialidad	*Si el sistema o aplicación del facturador es atacado, dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad.
	Integridad	
	Disponibilidad	
	Confidencialidad	

Activo	Principio	Motivo de afectación
Software o aplicación de lectura	Integridad	*Si el sistema o aplicación de lectura es atacado, dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad.
	Disponibilidad	
Terminal de lectura	Confidencialidad	*Si el sistema o aplicación de lectura es atacado, dependiendo del ataque que se materialice, puede llegar a afectar uno o varios de los principios: confidencialidad, integridad y disponibilidad.
	Integridad	
	Disponibilidad	

Nota. Fuente propia

3.1.2.2 Identificación de amenazas

A continuación, en la tabla 3-3, se relacionaron algunas amenazas y la manera cómo pueden llegar a afectar las 10 fases incluidas en el proceso de facturación general que se construyó. Identificarlas y tenerlas presentes en el mapa de riesgos, puede aportar a que se minimice la materialización posterior de estos:

Tabla 3-3: Resultado clasificación de amenazas

Identificación Amenaza	Nombre de la amenaza	Posible afectación al proceso de facturación
1	Denegación de servicio DOS/DDOS	Esta amenaza puede afectar el proceso de facturación, en el evento que se presente una inundación de peticiones sobre los servidores en los cuales se alojan el aplicativo facturador, de lectura y de direcciones, hasta el punto de colapsarlos.

Identificación Amenaza	Nombre de la amenaza	Posible afectación al proceso de facturación
2	Ingeniería social	Por medio de las técnicas de ingeniería social, el atacante puede obtener datos sensibles de los clientes. Además, datos de los colaboradorescon los que se pueden realizar transacciones que conlleven a fraudes.
3	Malware	Al infiltrarse un malware en la base de datos, aplicaciones, herramientas ofimáticas y/o el servidor que componen el proceso de facturación, puede afectar los tres pilares de la seguridad de la información. Por ejemplo, pueden modificarse y/o perderse los datos. Además, afectar la confidencialidad.
4	Phishing	Por medio de un Phishing se puede caer en algún tipo de estafa accediendo a la entrega de datos sensibles de clientes y colaboradores. O también, accediendo a realizar transacciones o ajustes monetarios inadecuados sobre la facturación de los clientes.
5	SQL Injection	Al materializase un ataque SQL Injection, el atacante puede obtener la información sensible de los clientes que está alojada en la base de datos. Además, obtener las contraseñas del facturador, sistema de lecturas y de direcciones, con las cuales se puede incurrir en acciones indebidas.

Identificación Amenaza	Nombre de la amenaza	Posible afectación al proceso de facturación
6	Ransomware	Con este tipo de ataques, un atacante podría cifrar la información del facturador, sistema de lecturas y de direcciones, lo cual afectaría la prestación del servicio, se podría incurrir en inconvenientes legales y financieros, en términos del pago que se solicita por el rescate de la información.
7	Errores o imprecisiones en la elaboración de los contratos	Las imprecisiones en los contratos ocasionan que el cumplimiento de estos no sean los exactos y se afecte el proceso de facturación. Por ejemplo, al cargar la información de servicios como aseo o alumbrado público, se halla un malware que infecta las aplicaciones. No obstante, en el contrato no se incluyeron las pautas ante estos eventos, lo que sería un bache que afectaría el proceso y multiplique los trámites.
8	Fraude	Podrían presentarse situaciones en las que las lecturas y la liquidación sean manipuladas, a favor de un interesado, el cual posteriormente realizaría pagos por dichas manipulaciones.
9	Fuga de información	Al presentarse fuga de información, la confidencialidad del proceso de facturación se vería altamente perjudicada. Además, con el mal uso de esta, se podría afectar normativamente la Entidad y su prestación del servicio.

Identificación Amenaza	Nombre de la amenaza	Posible afectación al proceso de facturación
10	Huelga	Se interrumpiría la prestación del servicio, atención al cliente, toma de lecturas, análisis de consumos, liquidación y facturación, entrega al contratista para su impresión, porque los colaboradores de la Entidad estarían en manifestaciones y protestas.
11	Inadecuada segregación de funciones	No tener segregación de funciones posibilita la materialización de fraudes e irregularidades en el proceso. Por ejemplo: realizar transacciones que no corresponden según la labor para la cual fue contratado, ajustes monetarios. Entre otras.
12	Inadecuado control de la ejecución	Al no tener controles establecidos y ejecutarlos, se puede presentar la no ejecución de las fases asociadas al proceso de facturación, además, la ausencia de controles impide la medición asertiva y puede posibilitar los fraudes.
13	Incumplimiento de normas, leyes y requisitos	Incumplir con algún requerimiento normativo en el proceso de facturación, conlleva a multas emitidas por entes como la SSPD. Por ejemplo, por un error en la segregación de funciones se hizo una rebaja de valores inadecuada, al ser revisado por la SSPD puede emitir sus multas respectivas.

Identificación Amenaza	Nombre de la amenaza	Posible afectación al proceso de facturación
14	Selección de contratistas o personal no idóneo	El personal contratado debe ser idóneo, esto disminuye la probabilidad de materialización de fraudes.

Nota: Fuente propia

3.1.2.3 Identificación de vulnerabilidades

De acuerdo con el listado de vulnerabilidades de ISO 27001 indicado por la Escuela europea de excelencia, se seleccionaron las siguientes vulnerabilidades [60], la cuales se consideró que pueden afectar el proceso de facturación general construido. En la tabla 3-4 se relacionan las vulnerabilidades seleccionadas:

Tabla 3-4: Resultado de identificación de vulnerabilidades

Identificación de la vulnerabilidad	Nombre de la vulnerabilidad
1	Contraseñas predeterminadas no modificadas
2	Gestión inadecuada del cambio
3	Clasificación inadecuada de la información
4	Respaldo inapropiado o irregular
5	Inadecuada gestión y protección de contraseñas
6	Falta de formación y conciencia sobre seguridad
7	Inadecuada segregación de funciones
8	Insuficiente supervisión de los empleados y vendedores
9	Especificación incompleta para el desarrollo de software
10	Pruebas de software insuficientes
11	Falta de control sobre los datos de entrada y salida
12	Falta de documentación interna
13	Carencia o mala implementación de la auditoría interna
14	Copia no controlada de datos
15	Descarga no controlada de Internet
16	Software no documentado
17	Empleados desmotivados
18	Falta de capacitación para los empleados
19	Conexiones a red pública desprotegidas

Nota. Fuente propia

3.1.2.4 Escenarios del riesgo

Con base en los activos definidos y las amenazas relacionadas, se identificaron posibles escenarios de riesgo que pueden presentarse, los cuales se detallan en la tabla 3-5:

Tabla 3-5: Resultado de los escenarios de riesgo

ACTIVOS / AMENAZAS	Bases de datos	Clientes	Contratistas	Empleados	Facturas	Herramientas ofimáticas	Información	Proveedor de impresión	Servidor	Sistema facturador	Sistema o aplicación de gestión de direcciones	Software de lectura	Terminal de lectura
Denegación de servicio DOS/DDOS	x		x				x	x	x	x	x	x	
Ingeniería social		x	x	x				x					
Malware	x		x			x	x	x	x	x	x	x	
Phishing			x	x			x	x					
SQL Injection	x		x					x					
Ransomware	x		x			x	x	x	x	x	x	x	
Ausentismo			x					x					
Errores o imprecisiones en la elaboración de los contratos			x	x	x			x					
Fraude	x	x	x	x		x	x	x	x	x	x	x	x
Fuga de información	x		x	x	x	x	x	x	x	x	x	x	x
Huelga			x	x				x					
Inadecuada segregación de funciones	x						x		x	x	x	x	
Inadecuado control de la ejecución				x		x							x
Incumplimiento de normas, leyes y requisitos		x	x	x	x		x	x		x			
Selección de contratistas o personal no idóneo		x	x	x				x		x			

3.1.2.5 Agentes generadores

Con base en los escenarios de riesgo identificados, se definieron 91 posibles agentes generadores y los probables efectos o consecuencias, en caso de materializarse. En la tabla 3-6 se muestran 10 escenarios, la tabla completa se encuentra en la sección de anexos (Anexo A: Escenario del riesgo, agente generador y efecto).

Tabla 3-6: Escenario del riesgo, agente generador y efecto

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(1)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Bases de datos	Error humano Personal interno Delincuente informático	° Caída del servicio
(2)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Contratistas	Error humano Personal interno Delincuente informático	° Caída del servicio

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(3)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Información	Error humano Personal interno Delincuente informático	° Caída del servicio
(4)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Proveedor de impresión	Error humano Personal interno Delincuente informático	° Caída del servicio
(5)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Servidor	Error humano Personal interno Delincuente informático	° Caída del servicio
(6)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Sistema facturador	Error humano Personal interno Delincuente informático	° Caída del servicio
(7)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Sistema o aplicación de gestión de direcciones	Error humano Personal interno Delincuente informático	° Caída del servicio
(8)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Software de lectura	Error humano Personal interno Delincuente informático	° Caída del servicio
(9)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Clientes	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(10)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Contratistas	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información

Nota: Fuente propia

3.1.2.6 Calificación de probabilidad, impacto y riesgo:

Con el desarrollo de la presente fase se definió para cada escenario de riesgo la probabilidad de ocurrencia, el impacto y el riesgo por impacto. Esta definición se desarrolló para el impacto de indisponibilidad de la información.

En la tabla 3-7 se presentan 10 de los registros obtenidos. La tabla completa se encuentra en los anexos (Anexo B: Calificación de probabilidad, impacto y riesgo):

Tabla 3-7: Calificación de probabilidad, impacto y riesgo

Calificación con Controles

No.	Escenario de riesgos	Probabilidad		Impacto Información		Riesgo por Impacto de Información
(1)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Bases de datos	Improbable	2	Superior	5	10
(2)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Contratistas	Improbable	2	Superior	5	10
(3)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Información	Improbable	2	Superior	5	10
(4)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Proveedor de impresión	Improbable	2	Superior	5	10
(5)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Servidor	Improbable	2	Superior	5	10
(6)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Sistema facturador	Improbable	2	Superior	5	10
(7)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Sistema o aplicación de gestión de direcciones	Improbable	2	Superior	5	10
(8)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Software de lectura	Improbable	2	Superior	5	10
(9)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Clientes	Improbable	2	Insignificante	1	2
(10)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Contratistas	Improbable	2	Superior	5	10

Nota: Fuente propia

Al comparar la probabilidad de ocurrencia del riesgo con su impacto, se obtuvo la matriz de calificación, evaluación y respuesta a los riesgos, la cual contiene los criterios: aceptables, tolerables, inaceptables e inadmisibles. Con base en ello, a continuación, se muestra el resultado:

- **Impacto de indisponibilidad de la información:** puede presentarse fuga de información, interrupciones en el procesamiento de los datos, interrupción en la prestación del servicio, pérdidas monetarias y afectaciones negativas en la reputación de la Empresa. En la tabla 3-8 se ubican los riesgos según su probabilidad de ocurrencia y consecuencia:

Tabla 3-8: Matriz de clasificación de aceptabilidad

Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4					
Posible	3		(33) - (39) -	(31) - (38) - (60) - (75) - (76) -	(27) - (68) - (70) - (71) - (73) - (74) -	(13) - (14) - (15) - (16) - (17) - (18) - (19) - (20) - (21) - (22) - (23) - (24) - (25) - (26) - (28) - (29) - (30) - (32) - (34) - (35) - (36) - (37) - (40) - (41) - (42) - (43) - (44) - (45) - (46) - (47) - (48) - (49) - (50) - (51) - (52) - (53) - (54) - (55) - (56) - (57) - (58) - (59) - (61) - (62) - (63) - (64) - (65) - (66) - (67) - (72) -
Improbable	2	(9) -			(69) - (77) - (78) - (81) - (82) - (85) - (87) - (88) - (89) - (90) - (91) -	(1) - (2) - (3) - (4) - (5) - (6) - (7) - (8) - (10) - (11) - (12) - (79) - (80) - (83) - (84) - (86) -
Raro	1					

Nota. Matriz de clasificación [17]

Así mismo, en la tabla 3-9 se muestra la distribución porcentual, según el total de riesgos:

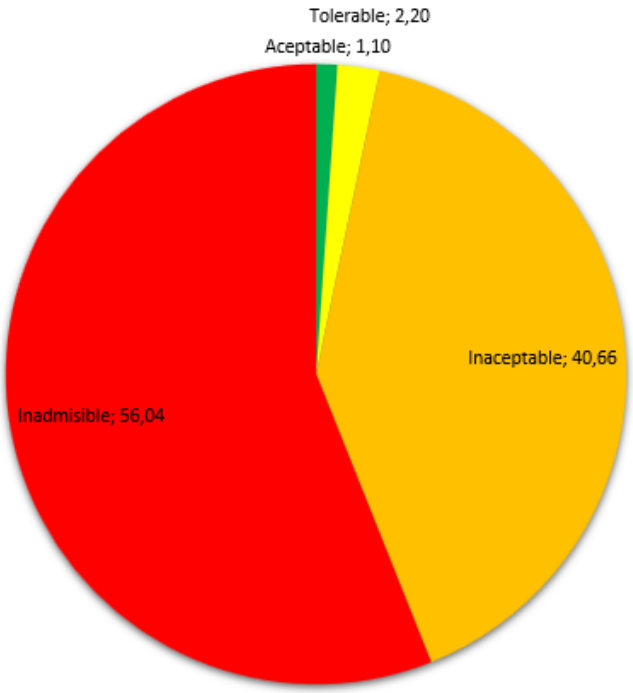
Tabla 3-9 Distribución porcentual

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Aceptable	1,10	1
Tolerable	2,20	2
Inaceptable	40,66	37
Inadmisible	56,04	51

Nota. Distribución porcentual [17]

En la figura 3-2 se encuentra la distribución del número de riesgos, de acuerdo con su respectiva zona:

Figura 3-2 Gráfico de distribución de riesgos por zona



Nota. Fuente propia

Con base en los anterior, se concluyó que se hallaron 51 riesgos inadmisibles, 37 inaceptables, 2 tolerables y 1 aceptable. A partir del resultado de este mapa, la Organización puede tomar acciones para el manejo y tratamiento de los riesgos, en pro de lograr y mantener los principios fundamentales de la seguridad de la información. Además, de adoptar mayor madurez y posibilidad de defensa, en términos, igualmente de, seguridad.

Seguidamente, con este resultado se hizo el respectivo plan de tratamiento, sobre los riesgos inadmisibles e inaceptables.

De estos resultados, se puede inferir que el hecho de materializarse un riesgo ocasionaría impactos importantes a nivel de información, y a partir de allí otros que pueden afectar el proceso, su ejecución y hasta la continuidad del negocio. Su nivel de criticidad exigió que se realizara un plan de tratamiento, donde se especificaron las acciones a realizar, el cumplimiento, monitoreo y responsables, para así proporcionar mayor manejo y control a nivel de los riesgos, además de fortalecer la seguridad e la información.

3.2 Fase 2. Definición de controles y mejores prácticas

3.2.1 Plan de tratamiento para riesgos inadmisibles e inaceptables

Con el plan de tratamiento realizado, se evaluaron y se asignaron las acciones que van a tomarse para gestionar los riesgos inadmisibles e inaceptables hallados, teniendo en cuenta los criterios definidos para ello. De esta manera, puede mitigarse la probabilidad de materialización de los riesgos y lo que esto representa.

Al realizar el plan de tratamiento, se encontró que para ninguno de los riesgos se tomó la acción de retener.

De los 88 riesgos, se propusieron 66 acciones para que fueran evitados. En cada una de estas acciones se detalló el plan a realizar y de monitoreo, los responsables y los resultados esperados.

Solo se decidió reducir uno de los riesgos, toda vez que se refiere a realizar diferentes actividades que permitan concientizar a los empleados para no ser víctimas de un ataque por ingeniería social.

El plan de acción de 19 de los riesgos se basó en transferir, debido a que estos deberían ser gestionados y tramitados por una dependencia o equipo de trabajo diferente.

En la tabla 3-10 se relacionó el plan de tratamiento establecido para 3 riesgos. El plan de tratamiento completo se puede observar en la sección de anexos (Anexo C: Plan de tratamiento):

Tabla 3-10 Plan de tratamiento

Riesgos altos considerando los controles actuales	TRATAMIENTO				Descripción del plan: * Controlar o evitar: ¿cómo? * Transferir: ¿A quién?	Plan de monitoreo	Responsable	Resultado Esperado
	Retener	Evitar	Reducir	Transferir				
(15) -Posibilidad que la amenaza: Malware, afecte el activo: Herramientas ofimáticas		X			1. Contar con un software antivirus licenciado y actualizado, en todos los equipos corporativos que utilicen herramientas ofimáticas. 2. Ejecutar escaneo semanal con la herramienta antivirus, a todos los equipos que posean herramientas ofimáticas. 3. Configurar las herramienta ofimáticas, para que tenga inhabilitadas por defecto las macros.	1. Resumen semanal de los eventos y alertas emitidos por el antivirus. 2. Informe semanal, que contenga los resultados de los escaneo realizados a todos los equipos que posean alguna herramienta ofimática. 3. Plantilla que evidencia, que todo equipo que posea herramientas ofimáticas, tienen por defecto inhabilitado el uso de macros.	1. Oficial de seguridad de la información. 2. Oficial de seguridad de la información. 3. Gerente de Tecnologías de la información	1. Informe semanal que contenga los eventos y alertas emitidos por el antivirus 2. Informe semanal, con los resultados obtenidos en los escaneos realizados con el antivirus, a los equipos que posean alguna herramienta ofimática instalada. 3. Plantilla que contenga la revisión realizada a todos equipo que contenga herramientas ofimáticas, en la cual se evidencia que las macros están por defectos inhabilitadas.
(16) -Posibilidad que la amenaza: Malware, afecte el activo: Información		X			1. Contar con un software antivirus licenciado y actualizado, en todos los equipos corporativos. 2. Verificar que todos los usuarios corporativos tienen perfil restringidos en el Dominio (Directorio Activo) 3. Configurar en el antivirus, una tarea semanal para que analice todos los equipos corporativos. 4. Realizar monitoreo activo al trafico del trafico entrante y saliente de la red corporativa	1. Monitorear de manera proactiva, las alertas emitidas por la herramienta antivirus. 2. Solicitar de manera mensual, un informe de los usuarios existente en el dominio, incluyendo el perfil que poseen. 3. Realizar informe semanal, sobre los hallazgos identificados en los análisis realizados por el antivirus. 4. Realizar informe semanal, del monitoreo realizado al trafico entrante y saliente de la red corporativa.	1. Oficial de seguridad de la información. 2. Gerente de Tecnologías de la información 3. Oficial de seguridad de la información. 4. Gerente de Tecnologías de la información	1. Informe semanal, del monitoreo proactivo realizado sobre las alertas emitidas por la herramienta antivirus. 2. Informe mensual, de los usuarios y su respectivo perfil, existente en el dominio corporativo. 3. Informe semanal, sobre los hallazgos identificados por el escaneo realizado por el antivirus. 4. Informe semanal, del análisis realizado al trafico entrante y saliente de la red corporativa.
(21) -Posibilidad que la amenaza: Malware, afecte el activo: Software de lectura		X			1. Solicitar que los dispositivos que posean el Software de Lectura, cuenten con un antivirus, licenciado y actualizado. 2. Aplicar línea base (hardening) a los dispositivos que posean instalado el Software de lectura. 3. Actualizar de manera proactiva, el sistema operativo que contengan los dispositivos que cuenten con el Software de lectura	1. Solicitar informe semanal sobre las alertas emitidas por el Servidor que soporta el Sistema o aplicación de gestión de direcciones. 2. Solicitar plantilla que constante la aplicación de Hardening al servidor que soporta el Sistema o aplicación de gestión de direcciones. 3. Solicitar informe mensual, de las actualizaciones aplicadas, y las que tenga pendiente por aplicarse, en el servidor que soporta el Sistema o aplicación de gestión de direcciones.	1. Gerente de Tecnologías de la información 2. Oficial de Seguridad de la Información. 3. Gerente de Tecnologías de la información	1. Informe semanal, que permite identificar y analizar las alertas emitidas por el antivirus instalado en el servidor que soporta el Sistema o aplicación de gestión de direcciones. 2. Documento que contenga el procedimiento de hardening aplicado al servidor que soporta el Sistema o aplicación de gestión de direcciones. 3. Informe mensual, sobre las actualizaciones aplicadas, y las que están pendiente por aplicar, en el servidor que soporta el Sistema o aplicación de gestión de direcciones.

Nota. Plan de tratamiento [17]

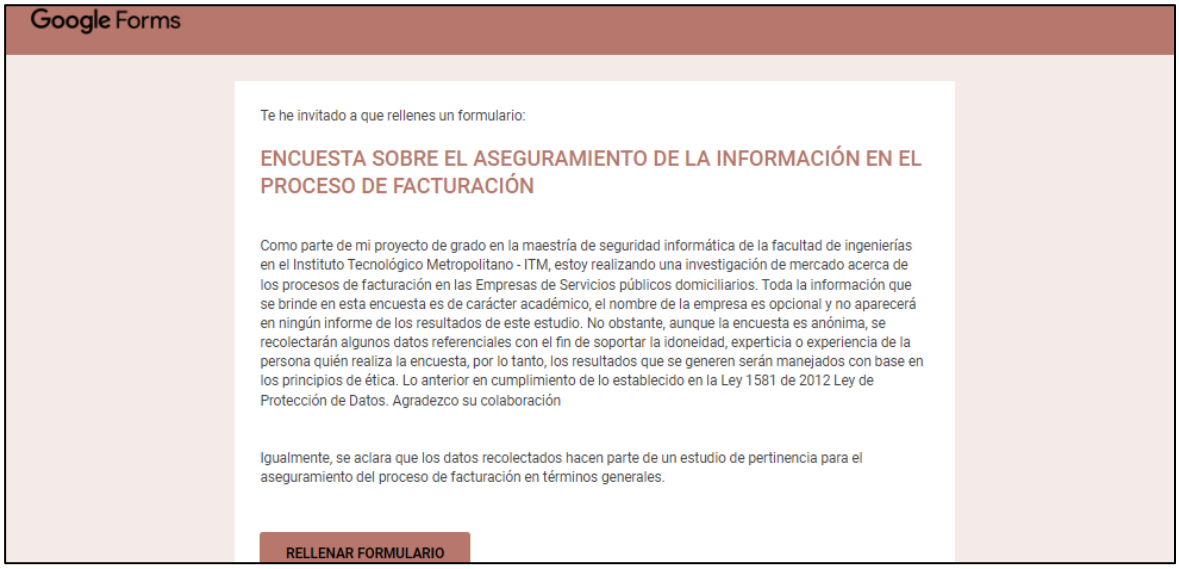
3.2.2 Encuesta sobre el aseguramiento en el proceso de facturación

En atención a la Ley 1581 de 2012 de Protección de Datos Personales, y toda vez que, la información incluida en las respuestas dadas a la encuesta es sensible a algún ciberataque, la razón social de las empresas y los nombres de los colaboradores, no fueron revelados en el presente documento.

Como se indicó en la metodología, se realizó encuesta a 4 diferentes Empresas de servicios públicos ubicadas en el territorio colombiano. Cada una de estas designó a un profesional experto del proceso de facturación, para un total de 4 expertos. La encuesta se hizo con el fin de identificar el estado actual de las organizaciones frente a los riesgos inmersos en su proceso de facturación, al tratamiento que se les aplica, las prácticas que puedan ser replicadas y la posibilidad de incursionar o adoptar nuevas maneras para ejecutar sus labores.

Los pasados meses de octubre y noviembre de 2021, se realizó la encuesta a 4 empresas de servicios públicos, ubicadas en Manizales, Santander, Norte de Santander y Medellín. Estas se realizaron virtualmente, debido a que como se mencionó, son empresas ubicadas en distintas zonas del país. Adicionalmente, por las restricciones de aforo a causa del COVID 19 (Coronavirus), que fue reconocido por la Organización Mundial de la Salud (OMS) como una pandemia global el 11 de marzo de 2020. La encuesta se desarrolló en Google Forms y tuvo la siguiente presentación:

Figura 3-3 Presentación inicial de la encuesta

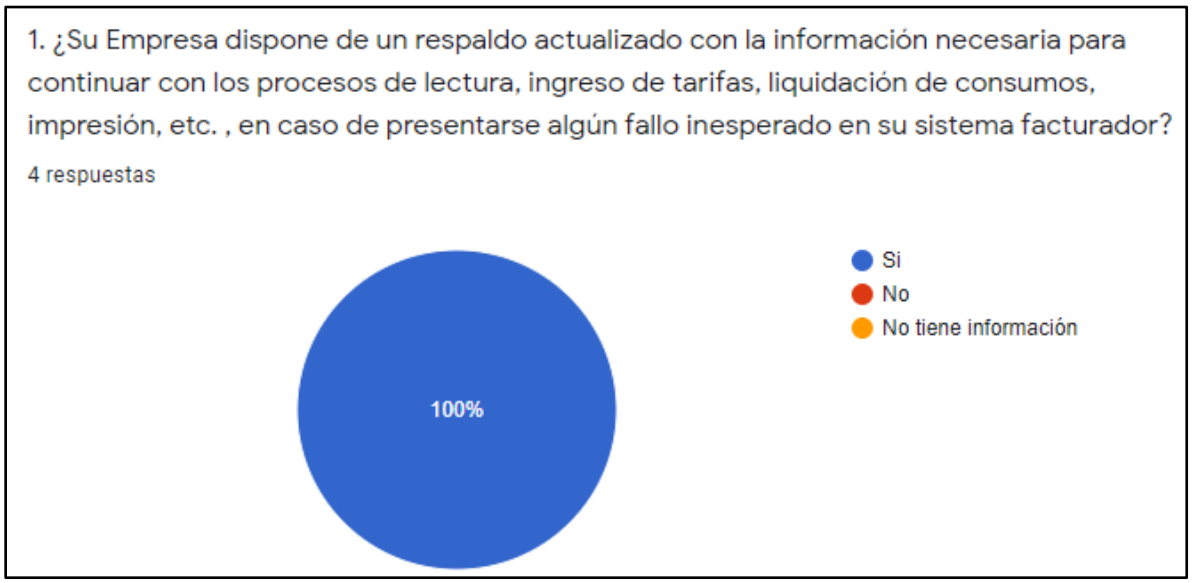


Nota. Fuente propia

Para ver el detalle de las respuestas, ir a la sección de anexos (Anexo D: Resultado de la encuesta)
A continuación, se expone el análisis de los resultados obtenidos para cada una de las preguntas incluidas en la encuesta:

Para la pregunta: ¿Su Empresa dispone de un respaldo actualizado con la información necesaria para continuar con los procesos de lectura, ingreso de tarifas, liquidación de consumos, impresión, etc., en caso de presentarse algún fallo inesperado en su sistema facturador?, las respuestas de los entrevistados se pueden observar en la Figura 3-4, en la cual, se identifica que las 4 Empresas tienen respaldo de su información en caso de presentarse algún incidente. Lo anterior, es importante, porque les permite rapidez al recuperar datos, continuidad en los procesos, conservación de la información, entre otros.

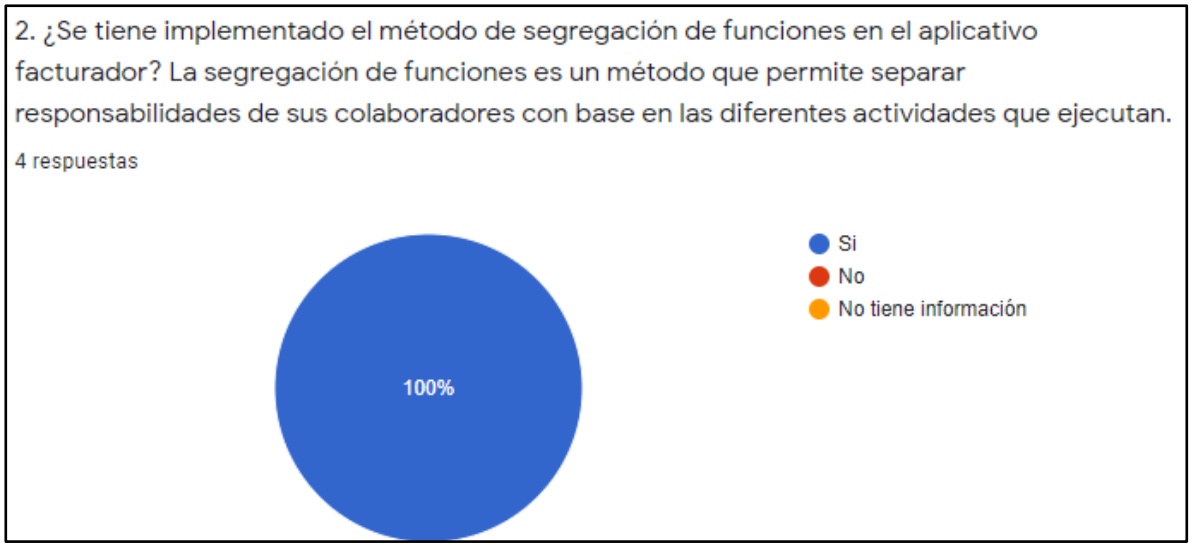
Figura 3-4: Resultado de la pregunta Nro. 1



Nota: Fuente propia

Frente a la inquietud: ¿Se tiene implementado el método de segregación de funciones en el aplicativo facturador? La segregación de funciones es un método que permite separar responsabilidades de sus colaboradores con base en las diferentes actividades que ejecutan. Se encontró que las 4 Empresas encuestadas tienen segregadas sus funciones, de modo que cada colaborador tiene definidos y asignados sus roles con base en su labor, para mayor detalle ver la Figura 3-5:

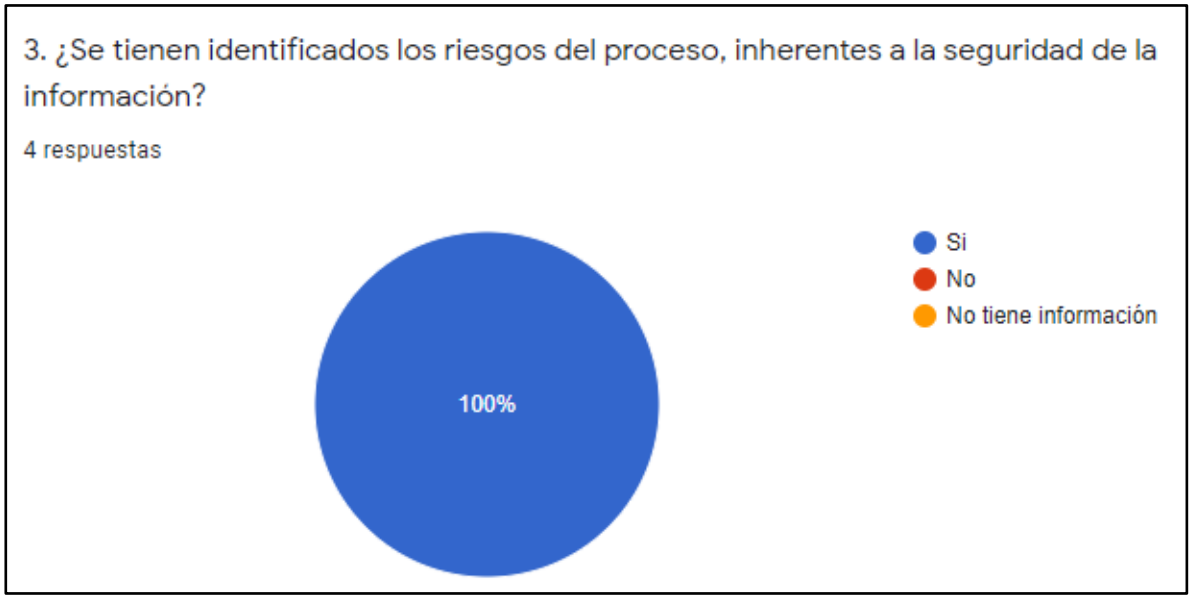
Figura 3-5: Resultado de la pregunta Nro. 2



Nota: Fuente propia

En la consulta: ¿Se tienen identificados los riesgos del proceso, inherentes a la seguridad de la información?, se encontró que las 4 Empresas tienen identificados sus riesgos, en lo que a la seguridad de la información se refiere, lo cual es positivo, debido a que al presentarse algún tipo de incidente que esté previamente identificado, su atención sería rápida y contendría un alto porcentaje de eficacia. Esta información se observa en la Figura 3-6:

Figura 3-6: Resultado de la pregunta Nro. 3



Nota: Fuente propia

Con base en la pregunta anterior, se indicó: Si la respuesta anterior es positiva, por favor informe mínimo 5 riesgos que tiene identificados en el proceso de facturación. En la Figura 3-7, se relacionaron los riesgos informados por cada una de las Empresas, nombrándolas Empresa Nro. 1, Empresa Nro. 2, Empresa Nro. 3 y Empresa Nro. 4. Algunos de los riesgos que se evidencian más comúnmente entre las Empresas encuestadas, son: la pérdida, indisponibilidad o alteración de la información, inconsistencias en la información entregada por terceros y daños en la infraestructura y equipos. Es importante que se reconoció que los riesgos a nivel de información son relevantes, pues esto puede permitirles engrosar sus métodos de seguridad y enfocarse en mejorar los procesos que involucran la información susceptible que se maneja.

Figura 3-7: Resultado de la pregunta Nro. 4

Empresa Nro. 1

- No disponibilidad del Sistema Comercial y de comunicaciones.
- Inconsistencia de la información entregada por terceros y convenios de alumbrado publico.
- Debilidad en los atributos de la información. Perdida de la información por hurto o daño de los dispositivos móviles.

Empresa Nro. 2

- Deficiencia en la disponibilidad y/o integridad de la información
- Alteración de información de cobros en la factura
- Falta de oportunidad y/o inconsistencias en la información entregada por terceros

Empresa Nro. 3

- Caída de la base de datos
- Pérdida de terminales portátiles
- Acceso no permitidos a la base de datos
- Ataques informáticos
- Errores en los web servicio

Empresa Nro. 4

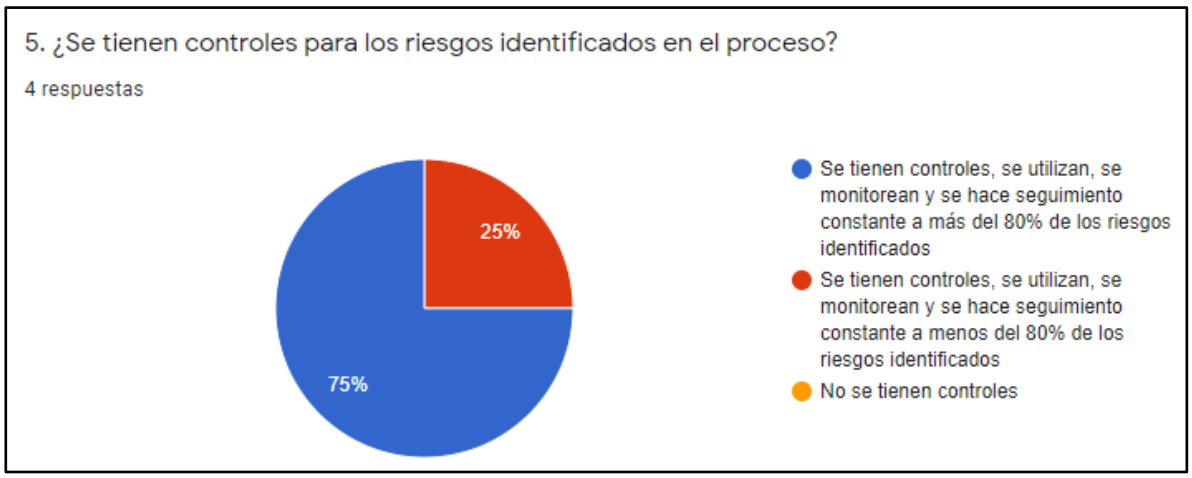
- Inadecuada liquidación del consumo real de energía al cliente: Problemas en la descarga de las lecturas en el sistema de información SAC.
- Deficiencias de disponibilidad de información o del sistema de información para realizar las actividades de liquidación: No contar con acceso al SAC; Demoras en las interfases de los sistemas.
- Daños masivos de la infraestructura (TPL): Uso indebido de los equipos (Caidas, rayones); Suministrar voltaje indebido a los equipos; Obsolescencia y pérdida de la vida útil.

Nota: Fuente propia

Con respecto a la pregunta: ¿Se tienen controles para los riesgos identificados en el proceso?, según la Figura 3-8, todas las empresas tienen controlados los riesgos. No obstante, 3 de ellas que corresponden al 75%, dicen que utilizan, monitorean y hacen seguimiento a menos del 80% de sus

riegos. Y una de ellas, que es el 25%, utiliza, monitorea y hace seguimiento a más del 80%. Lo anterior, corresponde a una alerta importante, debido a que las empresas quedan susceptibles a eventos como ciberataques, porque, aunque conocen sus riesgos, no los tratan.

Figura 3-8: Resultado de la pregunta Nro. 5

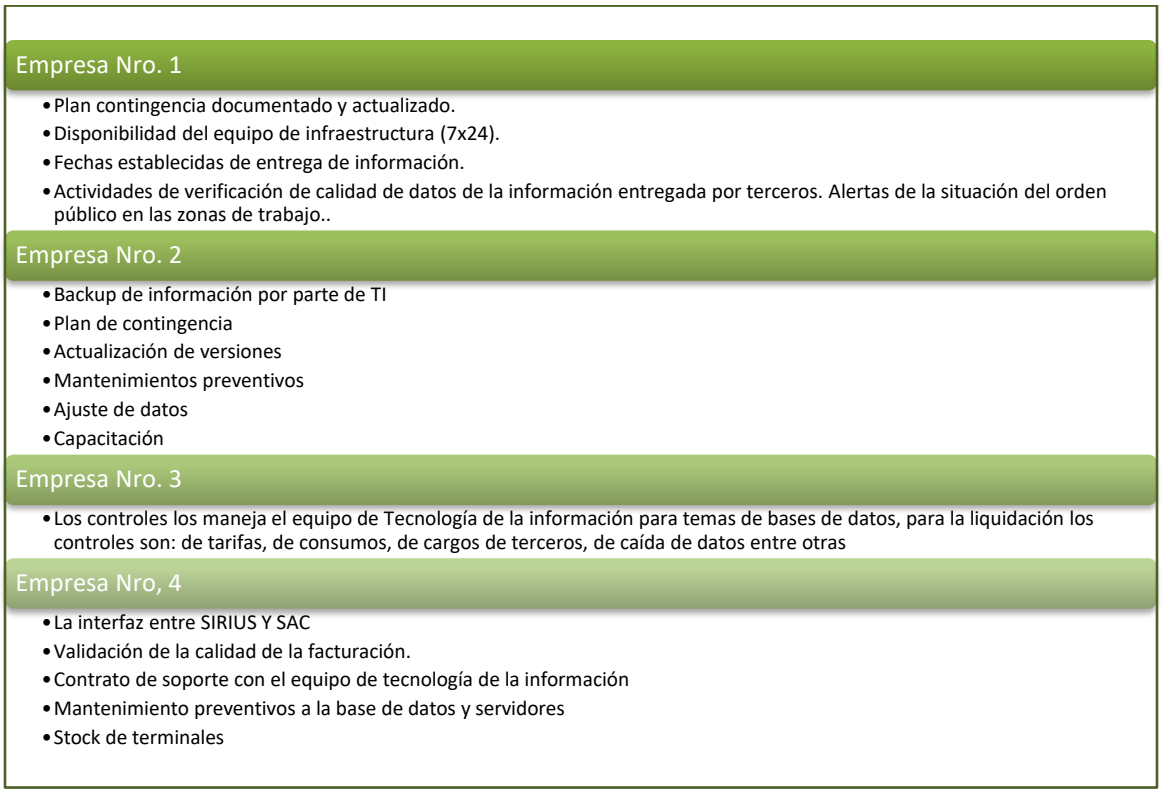


Nota: Fuente propia

Frente al planteamiento: Si la respuesta anterior es positiva, por favor enuncie mínimo 5 controles, de los identificados en el proceso de facturación, en la Figura 3-9, se plasman las respuestas recibidas por cada empresa, nombradas Empresa Nro. 1, Empresa Nro. 2, Empresa Nro. 3 y Empresa Nro.4. En dichas respuestas, se observa que las empresas encuestadas tienen mecanismos para afrontar el riesgo que se evidenció sobre la información, tales como: backups, documentación, tiempos para recibirla, mantenimientos preventivos a las bases de datos y a los servidores, y revisiones en la calidad de la información.

Entre los controles que se implementan, se hallan ajustes o modificaciones manuales a los datos, los cuales, aunque sean necesarios, ya que se presentan por diferentes inconsistencias en los mismos, conllevan a que la factura que se entrega al usuario final pierda su integridad, pues es modificada y/o alterada.

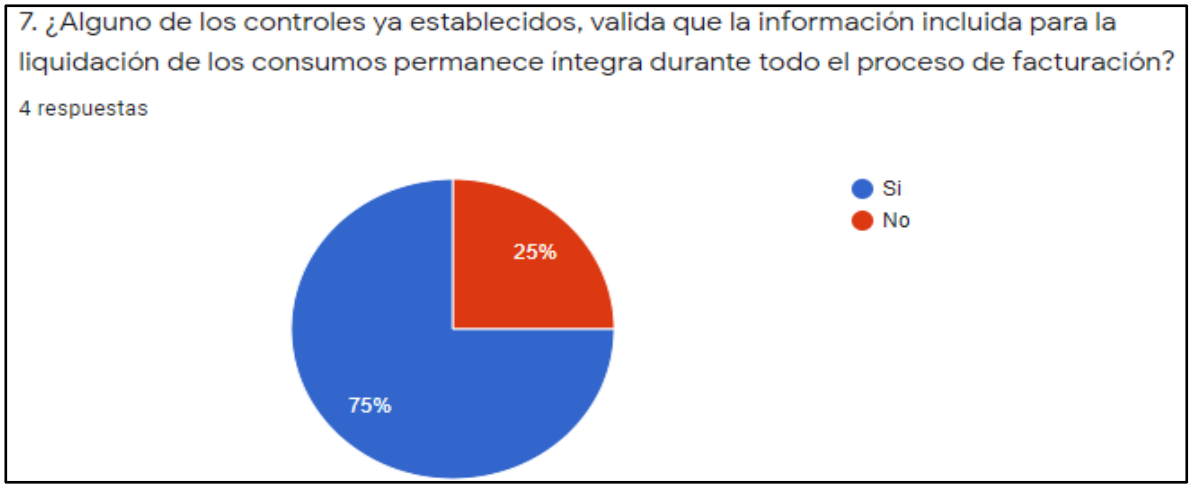
Figura 3-9 Resultado de la pregunta Nro. 6



Nota. Fuente propia

Para la pregunta: ¿Alguno de los controles ya establecidos, valida que la información incluida para la liquidación de los consumos permanece íntegra durante todo el proceso de facturación?, se encontró que según la Figura 3-10, 3 empresas que representan el 75%, consideraron que, durante el proceso de facturación, la liquidación permanece íntegra. Es delicado que una de ellas, que es el 25% restante no realiza esa validación, pues puede presentarse que esta tenga algún tipo de manipulación que le reste integridad y represente una vulnerabilidad que pueda ser aprovechada por un atacante, y, a su vez, se le entregue al usuario final un resultado incorrecto de su factura.

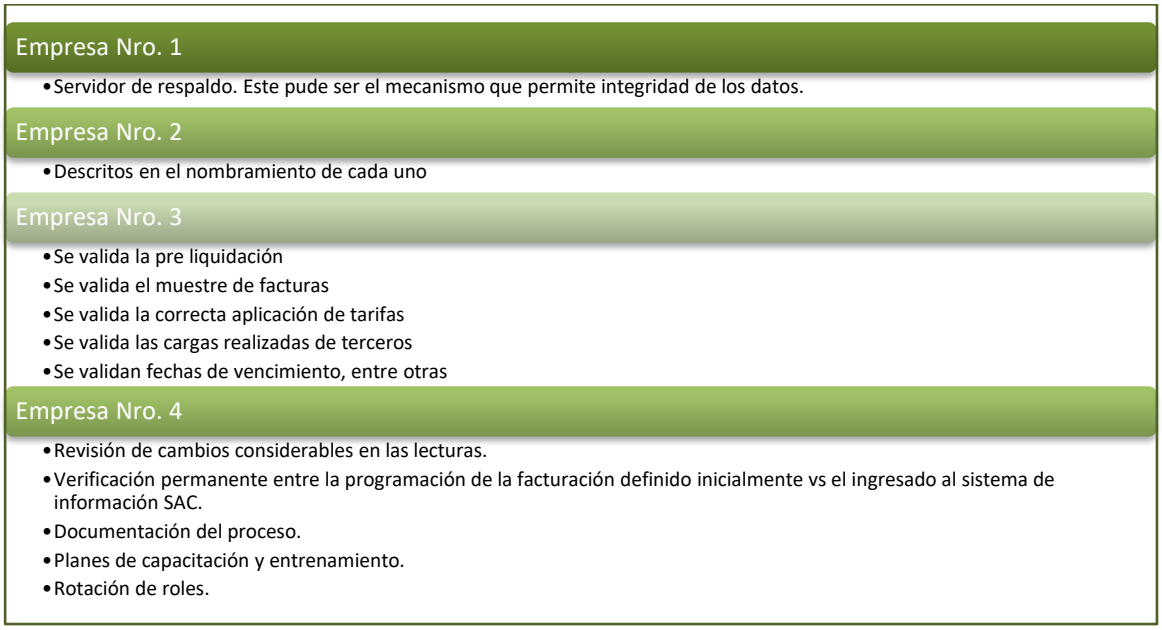
Figura 3-10: Resultado de la pregunta Nro. 7



Nota: Fuente propia

Con respecto a la solicitud: Describa el o los controles. En la Figura 3-11 se detallaron los controles que fueron reportados, donde, se resaltaron las empresas 3 y 4, debido a que se infiere que hacen una validación detallada de la liquidación. Con respecto a la Empresa 1, los controles están enfocados en los backups. Finalmente, la Empresa 2, aunque tiene controles, presenta vacíos en la revisión de los procesos de la liquidación, y que se requieren para que esta sea íntegra. En conclusión, falta solidez en los controles que se tienen al interior del proceso de facturación.

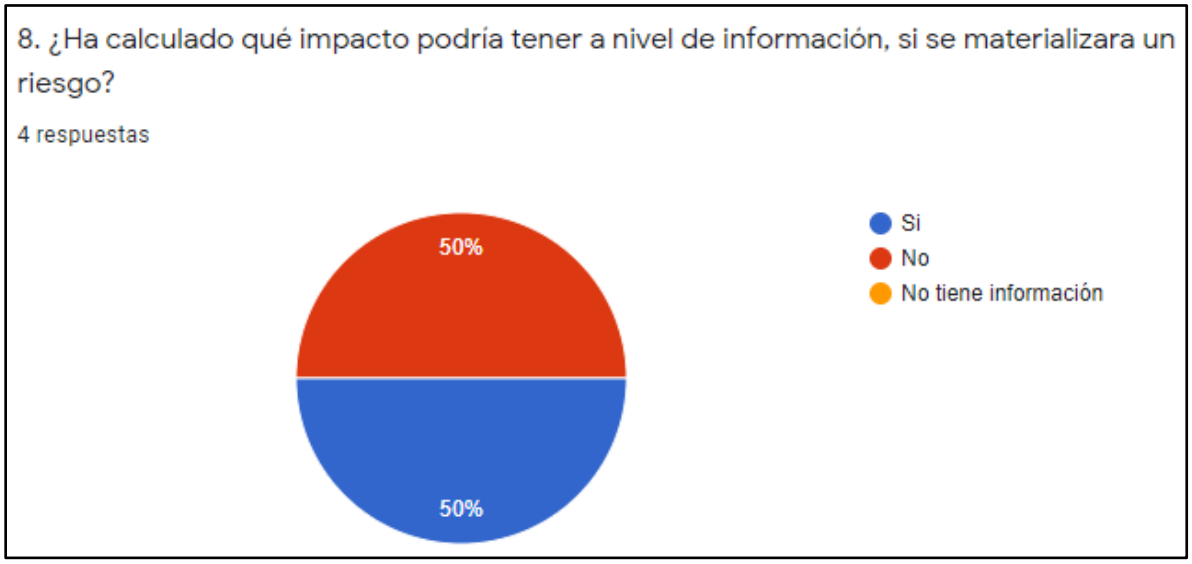
Figura 3-11: Resultado de la pregunta Nro. 7.1



Nota: Fuente propia

En la consulta: ¿Ha calculado qué impacto podría tener a nivel de información, si se materializara un riesgo? Como se muestra en la Figura 3-12, 2 de las empresas, que son el 50%, ha calculado el impacto de materializarse un riesgo mientras que, las otras 2, el otro 50% no lo ha hecho. Es importante hacer este cálculo, porque permite tener un horizonte de posibles consecuencias que se tendrían al materializarse un riesgo, y, en dicho horizonte, se pueden establecer medidas contingentes que aminoren el impacto de la situación.

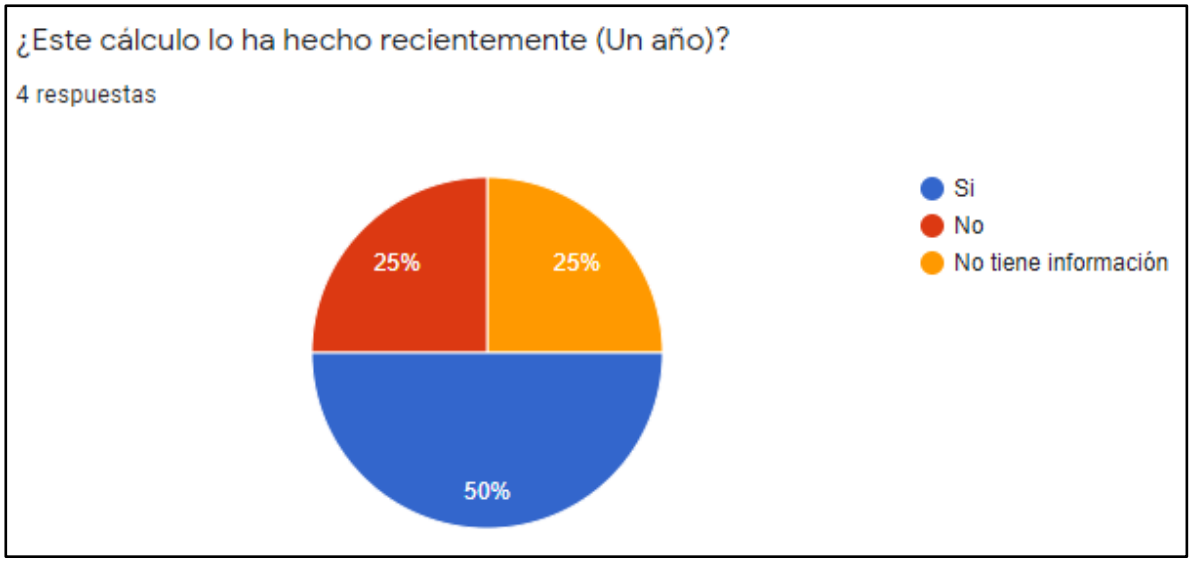
Figura 3-12: Resultado de la pregunta Nro. 8



Nota: Fuente propia

Para la pregunta: ¿Este cálculo lo ha hecho recientemente (Un año)? De acuerdo con la Figura 3-13, 2 de las empresas (el 50%) ha calculado el impacto que puede tener en caso de que se materialice un riesgo, a nivel de información, una de ellas (25%) no lo ha hecho y la otra (25%) no tiene información. Con respecto a las Empresas que lo han hecho recientemente, se resalta la labor ya que, el mapa de riesgos debe ser constantemente actualizado, pues con los avances tecnológicos también avanzan las posibilidades de ejecutar ciberataques. Hacer este cálculo aporta al soporte de decisiones preventivas que pueden aminorar la gravedad de los impactos al materializarse un ataque. El no hacer estos cálculos o no tener información es una alerta importante, porque, las personas entrevistadas son los expertos del proceso de facturación, por lo tanto, son los llamados a proteger dicho proceso, y una de las formas de hacerlo es calcular los impactos y conservar el mapa de riesgos actualizado.

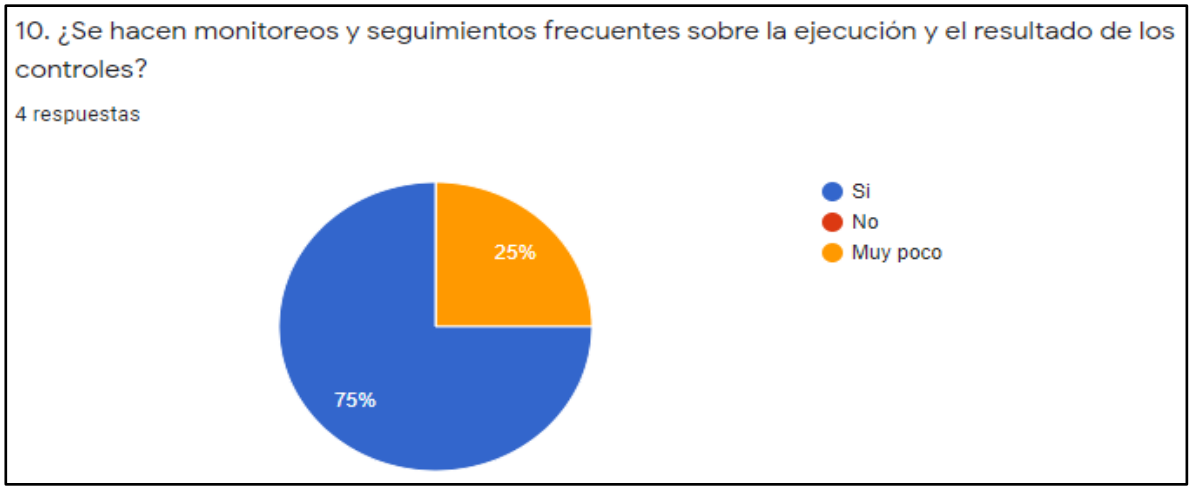
Figura 3-13: Resultado de la pregunta Nro. 9



Nota: Fuente propia

Frente a la pregunta: 10. ¿Se hacen monitoreos y seguimientos frecuentes sobre la ejecución y el resultado de los controles? De acuerdo con la Figura 3-14, 3 de las empresas afirmaron que, sí se realizan monitoreos y seguimientos regularmente, y una de ellas indica que realiza este proceso muy pocas veces. Hacer monitoreo y seguimiento sobre el resultado de los controles, ayuda a garantizar que se está llevando a cabo el plan de tratamiento diseñado para gestionar los riesgos. Adicionalmente, previene y puede evitar que se materialice un riesgo o se presente algún incidente.

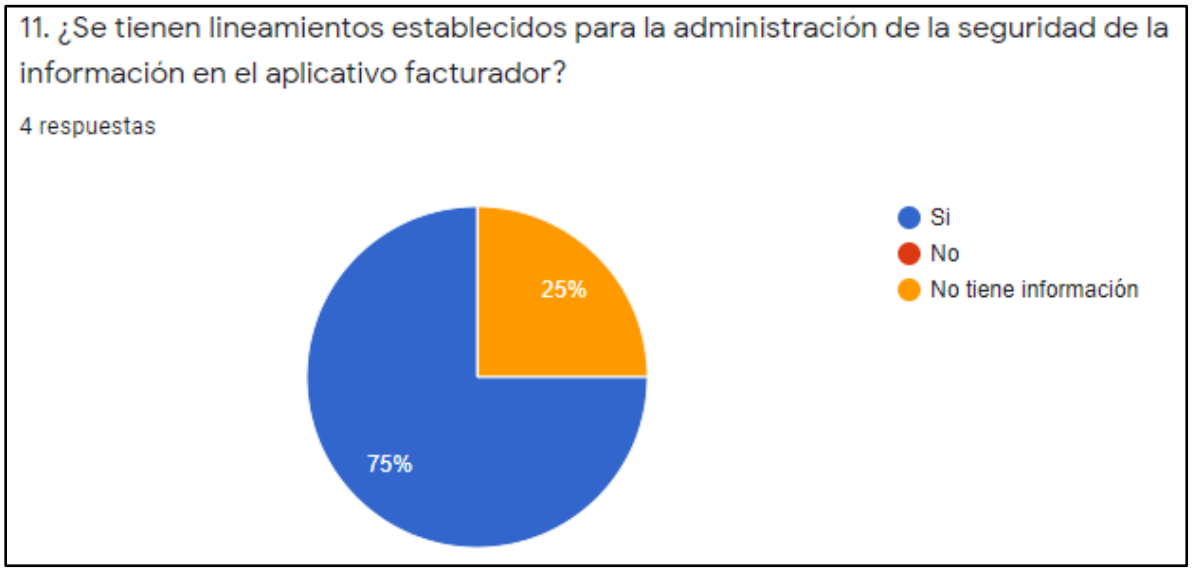
Figura 3-14: Resultado de la pregunta Nro. 10



Nota: Fuente propia

Con respecto a la inquietud: ¿Se tienen lineamientos establecidos para la administración de la seguridad de la información en el aplicativo facturador?, Como aparece en los resultados arrojados en la Figura 3-15, 3 empresas si lo tienen, y una de ellas desconoce la información. Conocer, aplicar, documentar y especificar los parámetros requeridos para administrar el aplicativo facturador, permite un mejor uso y que su manejo y gestión sean óptimos. Cumplir con los lineamientos y políticas definidos, fortalece la seguridad de la información.

Figura 3-15: Resultado de la pregunta Nro. 11

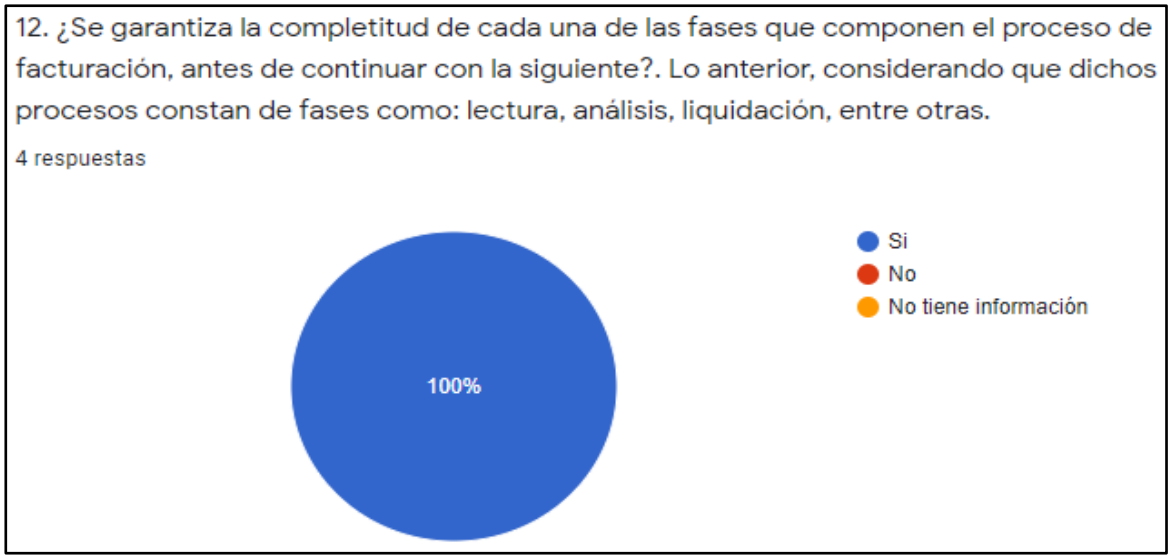


Nota: Fuente propia

Para la pregunta: ¿Se garantiza la completitud de cada una de las fases que componen el proceso de facturación, antes de continuar con la siguiente? Lo anterior, considerando que dichos procesos constan de fases como: lectura, análisis, liquidación, entre otras. Según la Figura 3-16, todas las empresas encuestadas indicaron que el proceso de facturación se cumple en cada una de sus fases.

Que se cumpla cada fase del proceso garantiza que la facturación pasó por todas las etapas requeridas para llegar al producto final. Es decir, si falta una de estas fases, la factura presentaría inconsistencias. No obstante, también es necesario que dichas etapas internamente se lleven a cabo totalmente, de modo que no queden requisitos pendientes de ejecución.

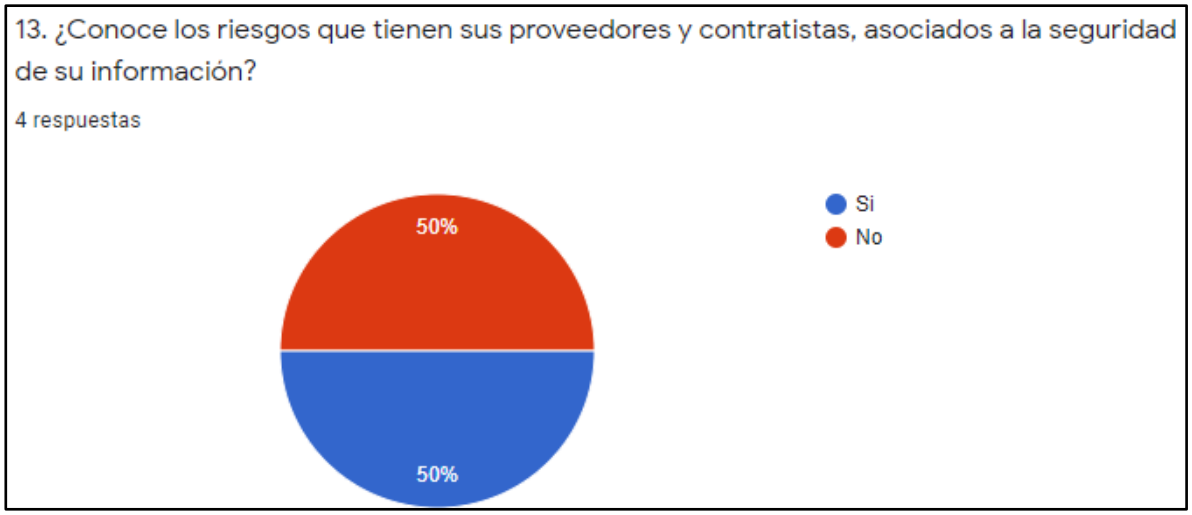
Figura 3-16: Resultado de la pregunta Nro. 12



Nota: Fuente propia

En la consulta: ¿Conoce los riesgos que tienen sus proveedores y contratistas, asociados a la seguridad de su información?, como se muestra en la Figura 3-17, solo 2 empresas encuestadas indicaron conocer los riegos de sus proveedores y contratistas mientras que, las otras dos los desconoce. Desconocer los riesgos de proveedores y contratistas, se convierte en un riesgo para la empresa contratante, pues al presentarse un incidente o materializarse un riesgo de estos actores, puede repercutir en el servicio prestado a la Empresa contratante y en la afectación de sus procesos e información.

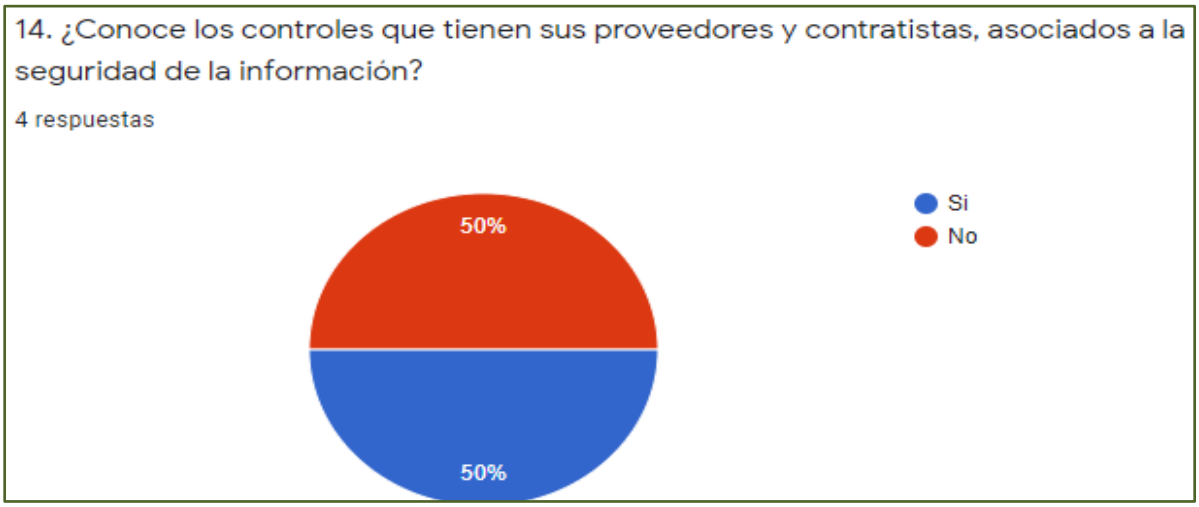
Figura 3-17: Resultado de la pregunta Nro. 13



Nota: Fuente propia

Frente a la pregunta: ¿Conoce los controles que tienen sus proveedores y contratistas, asociados a la seguridad de la información? Se puede observar en la Figura 3-18, que solo 2 de las empresas encuestadas conocen los controles de sus proveedores. Desconocer los controles que tienen los proveedores y contratistas, traslada un riesgo a la empresa contratante, pues puede existir algún vacío en términos de seguridad, que, en caso de presentarse algún incidente, va a repercutir en la empresa mencionada.

Figura 3-18: Resultado de la pregunta Nro. 14

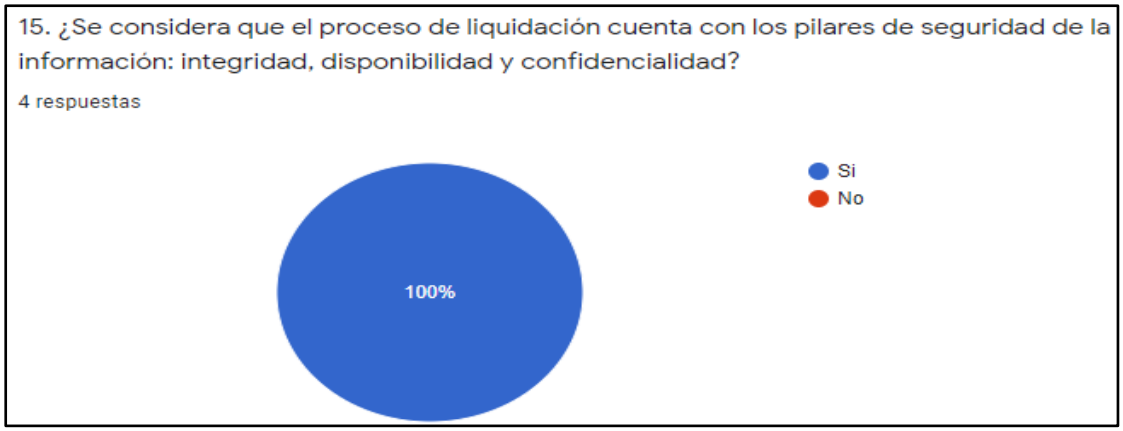


Nota: Fuente propia

Para la pregunta: ¿Se considera que el proceso de liquidación cuenta con los pilares de seguridad de la información: integridad, disponibilidad y confidencialidad? De acuerdo con la Figura 3-19, todas las empresas encuestadas señalan que el proceso de la liquidación es íntegro, disponible y confidencial.

Que el proceso cumpla con estas dimensiones lo hace altamente seguro. No obstante, cada una de ellas tiene una definición tan amplia que sería importante profundizar y soportar esta repuesta con personal técnico.

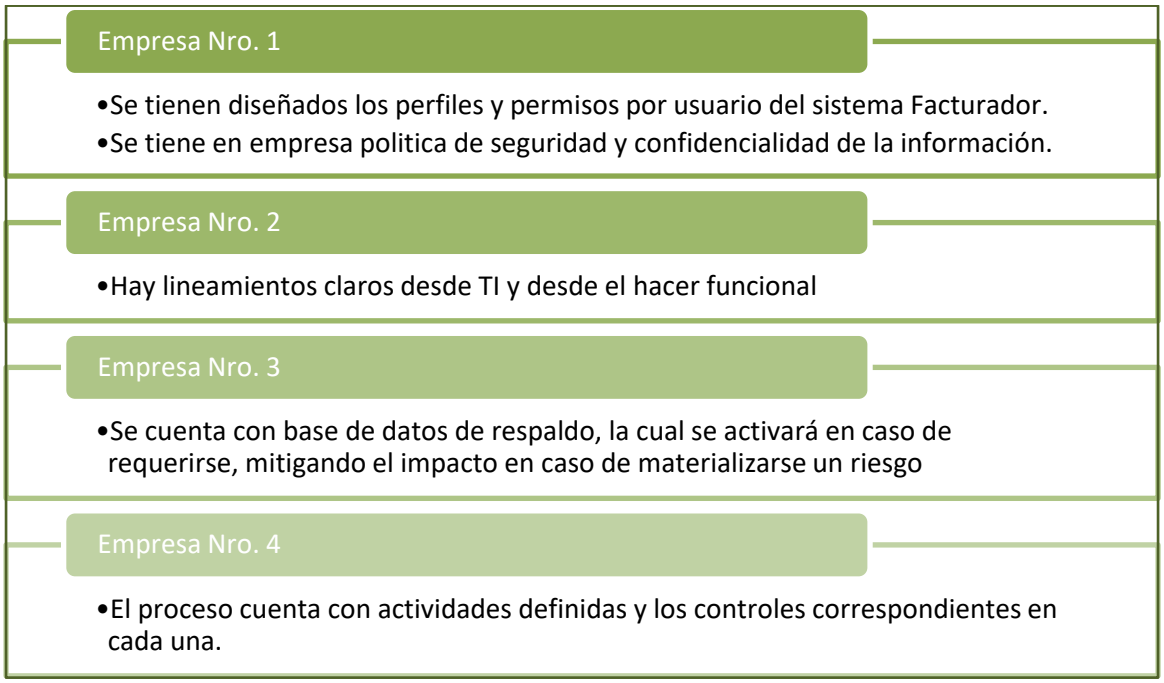
Figura 3-19: Resultado de la pregunta Nro. 15



Nota: Fuente propia

Con base en la respuesta dada a la pregunta anterior, se solicitó explicar, presentando los comentarios de cada una de las empresas, en la imagen 3-20. Cada empresa se identificó Empresa Nro. 1, Empresa Nro. 2, Empresa Nro. 3 y Empresa Nro. 4. En las explicaciones se evidenció que, aunque cuentan con mecanismos que pueden conservar los pilares de la seguridad de la información en el proceso de la liquidación, son pocos para cubrir el proceso en toda su magnitud.

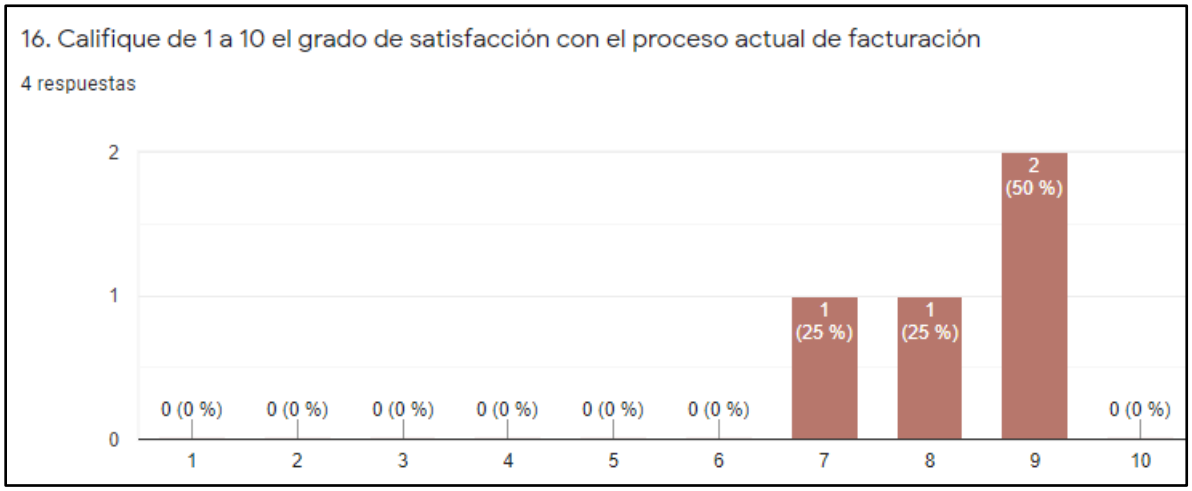
Figura 3-20 Resultado de la pregunta Nro. 15.1



Nota: Fuente propia

Con respecto a la solicitud: Califique de 1 a 10 el grado de satisfacción con el proceso actual de facturación. Se plasma en la figura 3-21 que una Empresa respondió 7, otra empresa 8 y dos de ellas 9. Por lo anterior, se estima que puede trabajarse en el nivel de satisfacción del proceso de facturación, implementando mejoras y nuevas formas de ejecutar las labores, implementando nuevos procesos y hasta nuevas tecnologías.

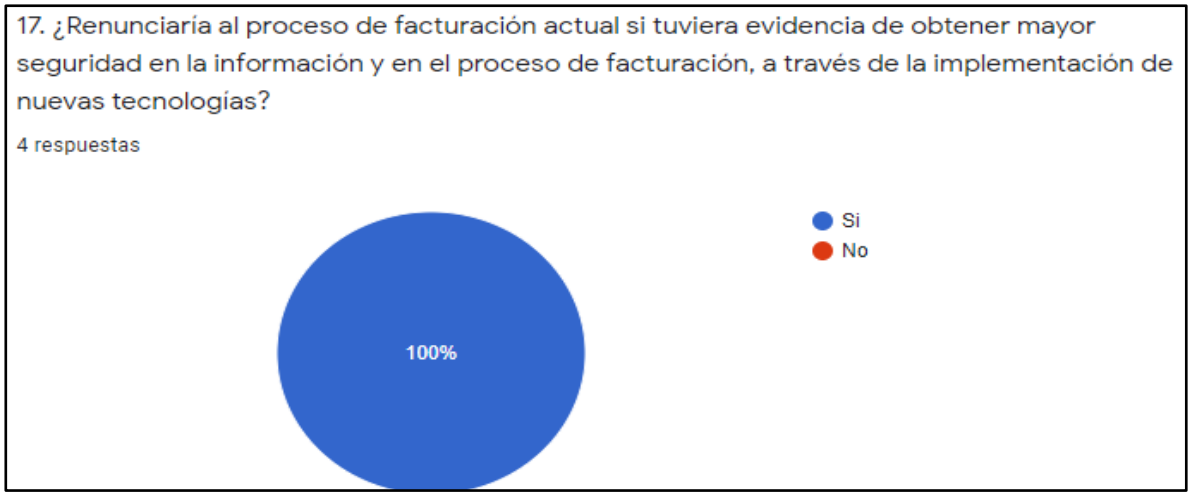
Figura 3-21: Resultado de la pregunta Nro. 16



Nota: Fuente propia

Sobre la pregunta ¿Renunciaría al proceso de facturación actual si tuviera evidencia de obtener mayor seguridad en la información y en el proceso de facturación, a través de la implementación de nuevas tecnologías?, según la figura 3-22, se evidencia disposición al cambio, toda vez que el 100% de las empresas, indicó que renunciaría a la forma actual de trabajar y aprendería otra. Esto es importante, porque el dinamismo del mercado, el crecimiento en tecnología, nuevos procedimientos y clientes es exponencial, lo que es directamente proporcional con la necesidad y/o urgencia que tienen las empresas de reinventarse, en pro de mejorar la calidad de su servicio, conservar los clientes y asegurar sus procesos.

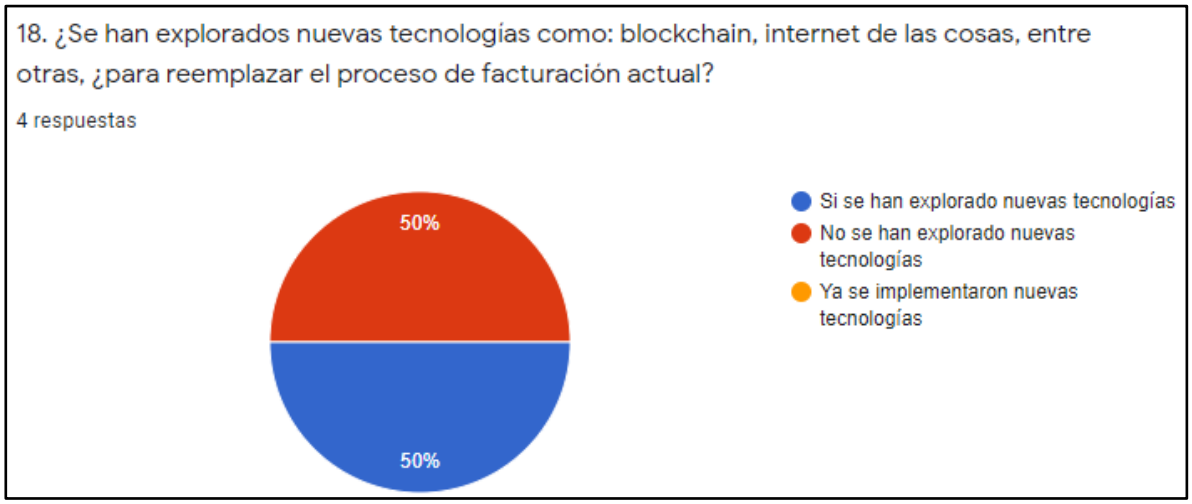
Figura 3-22: Resultado de la pregunta Nro. 17



Nota: Fuente propia

En atención a la pregunta ¿Se han explorados nuevas tecnologías como: blockchain, internet de las cosas, entre otras, ¿para reemplazar el proceso de facturación actual?, se halló que 2 de las empresas encuestadas han explorado nuevas tecnologías para actualizar los procesos de facturación. Las otras 2, no lo han hecho. Ver figura 3-23:

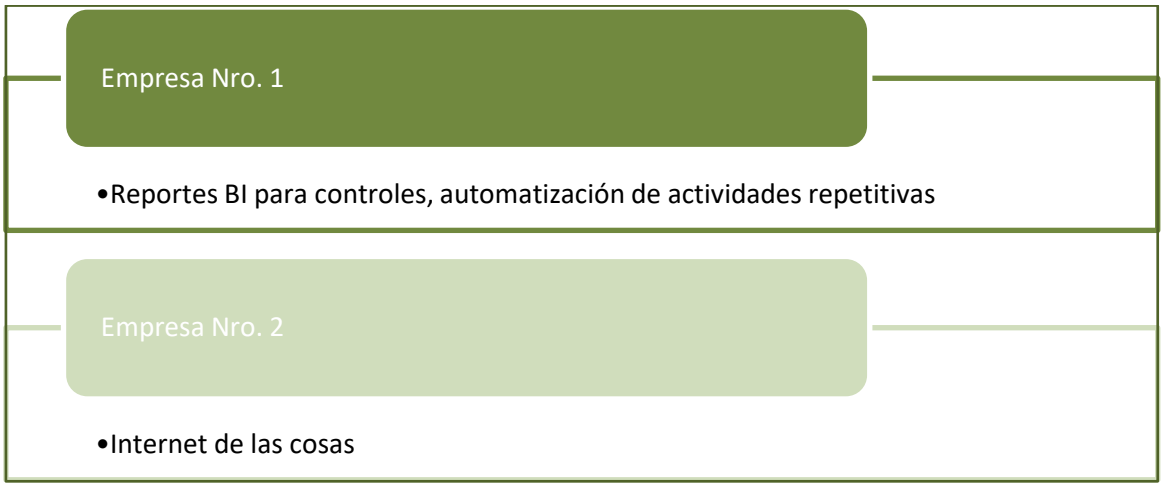
Figura 3-23: Resultado de la pregunta Nro. 18



Nota: Fuente propia

Con base en la pregunta anterior, en la figura 3-24 se detallan las nuevas tecnologías que han sido exploradas por algunas de las empresas encuestadas. Esto permite pensar que las Empresas están interesadas en innovar sus procesos y encontrar nuevas formas de hacer las cosas, por medio de la implementación de nuevas tecnologías.

Figura 3-24: Resultado de la pregunta Nro. 19



Nota: Fuente propia

Con las respuestas obtenidas, se puede inferir que las empresas comprenden la importancia de su proceso de facturación y disponen de controles. No obstante, no siempre se hace el seguimiento correspondiente a dichos controles, y en ocasiones incluso no cubren la totalidad del proceso, lo cual las deja vulnerables ante posibles ataques. A su vez, se evidenció que están conscientes sobre la necesidad permanente de buscar otras opciones y formas de hacer las cosas, dando cabida a la adaptación y aplicación de procedimientos y nuevas tecnologías como blockchain

3.2.3 construcción de controles para mejores prácticas

Con el propósito de comparar los riesgos identificados en el mapa de riesgos de la fase Nro. 1, y los mencionados en la encuesta, éstos fueron clasificados en los siguientes grandes grupos, teniendo en cuenta su similitud:

- Indisponibilidad de los aplicativos
- Errores en la información
- Ciberataques o ataques informáticos
- Inadecuada segregación de funciones

En la tabla 3-11 se encuentran un paralelo con la similitud de riesgos hallados:

Tabla 3-11 Paralelo de riesgos entre la encuesta y el mapa de riesgos

ENCUESTA	MAPA DE RIESGO
Indisponibilidad de los aplicativos	
*Errores en los servicios web	*Denegación de servicio DOS/DDO: bases de datos, contratistas, información, proveedor de impresión, servidor, sistema facturador, sistema o aplicación de gestión de direcciones, software de lectura
*Deficiencias de disponibilidad de información o del sistema de información para realizar las actividades de liquidación: No contar con acceso al SAC;	*Ataque informático o saboteo interno
*No disponibilidad del Sistema Comercial y de comunicaciones.	*Malware (Por ejemplo: Infectar el motor de la base de datos)
*Demoras en las interfases de los sistemas	*Ataque externo por medio de ingeniería social
*Caída de la base de datos	*Ramsonware
Errores en la información	
*Inconsistencia de la información entregada por terceros y convenios de alumbrado público.	*Fraude: bases de datos, contratistas, empleados, herramientas informáticas, información, proveedor de impresión, servidor, sistema facturador, sistema o aplicación de gestión de direcciones, software de lectura, terminal de lectura
*Debilidad en los atributos de la información.	*Errores humanos
*Deficiencia en la disponibilidad y/o integridad de la información	*Manualidad
*Alteración de información de cobros en la factura, falta de oportunidad y/o inconsistencias en la información entregada por terceros	*Ataques externos o internos por medio de ingeniería social
*Inadecuada liquidación del consumo real de energía al cliente: Problemas en la descarga de las lecturas en el sistema de información SAC.	*Errores en los ajustes que se realizan sobre consumos, tarifas y diferentes valores
Ciberataques o ataques informáticos	
*Ataques informáticos	*Malware: bases de datos, contratistas, herramientas ofimáticas, información, proveedor de impresión, servidor, sistema facturador, sistema o aplicación de gestión de direcciones, software de lectura
*Pérdida de la información	*Phishing: contratistas, empleados, información, proveedor de impresión

*Pérdida o hurto de la información:	*SQL Injection: Bases de datos, contratistas, proveedor de impresión
*Perdida de la información por hurto o daño de los dispositivos móviles.	*Ransomware: Bases de datos, contratistas, herramienteas ofimáticas, información, servidor, sistema facturador, sistema o aplicación de gestión de direcciones, software de lectura
*Pérdida de terminales portátiles	
*Daños masivos de la infraestructura (TPL): Uso indebido de los equipos (Caidas, rayones); Suministrar voltaje indebido a los equipos	
*Obsolescencia y pérdida de la vida útil."	
Inadecuada segregación de funciones	
*Accesos no permitidos a la base de datos	*Inadecuada segregación de funciones: bases de datos, información, servidor, sistema facturador, sistema o aplicación de gestión de direcciones, software de lectura, empleados, herramientas ofimáticas, terminal de lectura

Nota: Fuente propia

Por otro lado, se comparó el resultado de la encuesta y el mapa de riesgos realizados, evidenciándose que existen algunos riesgos que no han sido considerados por las empresas encuestadas. Por lo anterior, y al ser importantes, en la tabla 3-12 se relacionan dichos riesgos:

Tabla 3-12: Riesgos no identificados por las empresas encuestadas

RIESGOS NO IDENTIFICADOS POR LAS EMPRESAS ENCUESTADAS
Ingeniería social, afecte el activo: contratistas, empleados, proveedor de impresión
Ausentismo, afecte el activo: Contratistas
Errores o imprecisiones en la elaboración de los contratos, afecte el activo: Contratistas, empleados, facturas, proveedor de impresión
Fraude, afecte el activo: Clientes, contratistas, empleados, proveedores
Fuga de información, afecte el activo: Bases de datos, contratistas, empleados, facturas, herramientas ofimáticas, información, proveedor de impresión, servidor, sistema facturador, sistema o aplicación de gestión de direcciones, software de lectura, terminal de lectura.
Huelga, afecte el activo: Contratistas, empleados, proveedor de impresión
Inadecuado control de la ejecución afecte el activo: Empleados, herramientas ofimáticas, terminal de lectura
Incumplimiento de normas, leyes y requisitos, afecte el activo: Clientes, contratistas, empleados, facturas, información, proveedor de impresión, sistema facturador

RIESGOS NO IDENTIFICADOS POR LAS EMPRESAS ENCUESTADAS
Selección de contratistas o personal no idóneo, afecte el activo: Clientes, contratistas, empleados, proveedor de impresión, sistema facturador

Nota: Fuente propia

Con la información que suministra la tabla anterior, se encontró que las empresas encuestadas no tienen contemplados riegos como los de ingeniería social, y la manera cómo a través de esta práctica, un atacante puede obtener información sensible y confidencial al manipular a los usuarios, los cuales pueden ser contratistas, empleados, proveedores, entre otros.

Otros riesgos que no se contemplaron son los asociados a los colaboradores y procesos contratados, a nivel de ausentismos y huelgas. Toda vez que estas situaciones pueden presentar altos retrasos en las actividades.

Un riesgo adicional es el relacionado con los errores o imprecisiones en la elaboración de los contratos, lo cual puede afectar a contratistas, empleados, facturas y, proveedores de impresión. Los vacíos que tengan lugar en las cláusulas de los contratos pueden ocasionar daños y pérdidas de información, lo cual también puede ser utilizado de forma malintencionada.

El fraude también es un riesgo que puede materializarse en las empresas, con actores como los clientes, colaboradores, proveedores, entre otros. Este riesgo puede conllevar a un delito cibernético, alteración de los datos, fuga de información, etc.

El riesgo fuga de información, puede materializarse en la base de datos, contratistas, empleados, facturas, herramientas ofimáticas, información, proveedor de impresión, servidor, sistema facturador, sistema o aplicación de gestión de direcciones, software de lectura, terminal de lectura, ocasionando una salida incorrecta y sin control de la información hacia personas inescrupulosas.

El inadecuado control de la ejecución afecta los empleados, las herramientas ofimáticas y las terminales de lectura, entre otros. El no tener control sobre los procesos propios de la liquidación puede representar baches de seguridad en la información, toda vez que puede perder su confidencialidad, integridad y disponibilidad.

El incumplimiento de normas, leyes y requisitos afecta el activo clientes, contratistas, empleados, facturas, información, proveedor de impresión, sistema facturador.

La selección de contratistas o personal no idóneo afecta el activo clientes, contratistas, empleados, proveedor de impresión y, el sistema facturador. El desconocimiento de los riesgos y controles de los contratistas y proveedores, la inadecuada segregación de funciones para los colaboradores y la ejecución de procesos inadecuados de selección, dejan vulnerable el proceso de facturación de las empresas, ante ataques y ciberataques.

Adicionalmente, en la tabla 3-13 se recopilaron los controles que las empresas encuestadas utilizan en su operación y con los cuales las protegen:

Tabla 3-13: Controles enunciados por las empresas encuestadas

CONTROLES ENUNCIADOS POR LAS EMPRESAS ENCUESTADAS
*Plan contingencia documentado y actualizado. *Disponibilidad del equipo de infraestructura (7x24). *Fechas establecidas de entrega de información. *Actividades de verificación de calidad de datos de la información entregada por terceros. *Alertas de la situación del orden público en las zonas de trabajo.
*Backup de información por parte de TI *Plan de contingencia *Actualización de versiones *Mantenimientos preventivos, ajuste de datos, capacitación
*Los controles los maneja el equipo de tecnología de la información para temas de bases de datos. *Para la liquidación los controles son: de tarifas, de consumos, de cargos de terceros, de caída de datos entre otras
* La interfaz entre SIRIUS Y SAC * Validación de la calidad de la facturación. * Contrato de soporte con el equipo de tecnología de la información * Mantenimiento preventivos a la base de datos y servidores * Stock de terminales

Nota: Fuente propia

Finalmente, con base en los resultados obtenidos en la encuesta sobre los riesgos y controles, y tras analizar el mapa de riesgos construido en la fase 1 del presente documento, se planteó el

siguiente consolidado del uso mejores prácticas, con las cuales se fortalece el proceso de facturación, se aporta al cierre de brechas y se robustece la seguridad de la información.

En la tabla 3-14 se recopilaron las mejores prácticas que deben aplicarse para mitigar los riesgos identificados en el mapa de riesgos realizado sobre el proceso general de facturación, y en los resultados de la encuesta realizada a empresas del sector de los servicios públicos. Con cada una de estas, se veló por la conservación y el fortalecimiento de los pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad:

Tabla 3-14: Recopilación de mejores prácticas

MEJORES PRÁCTICAS PARA MITIGAR LOS RIESGOS OBTENIDOS	
1	Establecer un procedimiento de Backup que tenga pruebas de restauración
2	Aplicar WAF y customizar reglas que permitan minimizar el impacto o la probabilidad de ocurrencia de un ataque de negación de servicio (DOS) o de un ataque de denegación distribuido (DDOS)
3	Crear reglas de flujo en correos corporativos que restrinjan los correos empresariales tipo fishing
4	Aplicar una Solución EDR (Endpoint Detection and Response) para monitorear y analizar el endpoint y la red.
5	Validar y depurar los campos de entrada de información de las aplicaciones, para evitar sql injection
6	Tener backups cifrados
7	Tener backups diferenciales e incrementales.
8	Tener herramientas de prevención de pérdida de datos DLP (Data Loss Prevention) y GPO a nivel del dominio
9	Diseñar un plan de recuperación ante desastres (DRP)
10	Incluir acuerdos de nivel de servicio a nivel contractual con los proveedores.
11	Realizar seguimiento y monitoreo, a la prestación de servicios de los proveedores.
12	Realizar auditorías a los proveedores.
13	Aplicar línea base (hardening) a los servidores y equipos de cómputo
14	Realizar análisis de vulnerabilidades al servidor
15	Realizar monitoreo sobre la disponibilidad del Sistema Facturador
16	Instalar y configurar Firewall local en el servidor que soporta el Sistema facturador
17	Solicitar análisis estático y dinámico de código sobre el sistema facturador
18	Verificar que el contrato firmado con los contratistas y proveedores contenga una cláusula que mencione los controles que tienen y mitiguen la posibilidad de materialización de un ciberataque
19	Verificar que, en el contrato firmado con los contratistas y proveedores, estos se comprometan a realizar pruebas de ingeniera social sobre sus colaboradores.
20	Realizar encuestas a los colaboradores, asociadas a la calidad de vida laboral

MEJORES PRÁCTICAS PARA MITIGAR LOS RIESGOS OBTENIDOS	
21	Capacitar a los colaboradores en contenidos asociados a seguridad de la información
22	Hacer pruebas aleatorias de ingeniería social a los colaboradores
23	Contar con un software antivirus licenciado y actualizado
24	Implementar la segregación de funciones y el principio del mínimo privilegio en la base de datos y aplicaciones
25	Verificar que el contrato firmado con los contratistas y proveedores contenga un numeral donde se comprometa a implementar controles anti-Malware.
26	Verificar que, en el contrato firmado con los contratistas y proveedores, se exija la implementación de una herramienta antivirus, licenciada y actualizada.
27	Verificar que en el contrato firmado con los contratistas y proveedores proveedor, contenga un numeral donde se mencione que debe alinear su política de seguridad de la información, con la del cliente
28	Ejecutar escaneo semanal con la herramienta antivirus, a todos los equipos que posean herramientas ofimáticas.
29	Configurar las herramientas ofimáticas, para que tenga inhabilitadas por defecto las macros.
30	Solicitar apoyo de las áreas de Seguridad de la Información, Gerencia de TI y Jurídica, para la revisión de los contratos.
31	Verificar y leer detalladamente, los contratos con los con los contratistas y proveedores, antes de proceder con la firma del contrato.
32	Contar con un plan de capacitación para la prevención del fraude.
33	Contar con un plan de capacitación para la prevención de fuga de información. Incluyendo a todos los colaboradores que administren o manipulen las bases de datos.
34	Verificar que se aplica el principio de mínimo privilegio, para el acceso a la base de datos
35	Contar con manuales de procedimientos y funciones, asociados a los cargos de la empresa que deban tener acceso a las bases de datos.
36	Contar con una matriz de roles y permisos, asociados a los cargos de la empresa que tengan acceso al facturador y bases de datos
37	Desarrollar modelos de factura que garanticen el cumplimiento de toda la normativa legal vigente en Colombia, y que sea aplicable al proceso de facturación.
38	Contar con una Política de Seguridad de la Información, que contenga las normas, leyes y requerimientos vigentes en Colombia, asociadas a la protección de la información.
39	Contar con un manual de procedimientos, para la selección y contratación de personal, contratistas y proveedores.
40	Aplicar estudios de seguridad, en la contratación de personal.
41	Poseer Políticas de Seguridad de la Información, las cuales deban ser cumplidas por empleados, proveedores, contratistas y clientes.

MEJORES PRÁCTICAS PARA MITIGAR LOS RIESGOS OBTENIDOS	
42	Realizar reuniones de seguimiento (auditorias), con proveedores, contratistas y clientes, donde se logra evidenciar el cumplimiento de las políticas de seguridad de la información.

Nota: Fuente propia

3.3 Fase 3. Usos y metodología de adaptación y aplicación de blockchain

Para cumplir con la fase número 3 se investigó en diferentes páginas web sobre los usos que se le han dado a blockchain y se evaluaron un par de empresas que ya hacen uso de esta tecnología. La investigación se hizo para reconocer usos y mejores prácticas, que sirvieron como sugerencia en la disminución de la posibilidad de ocurrencia de los riesgos hallados en los procesos de facturación, previamente descritos.

Igualmente, a partir del desarrollo de las fases 1 y 2, y del estudio que se ha realizado a lo largo de la tesis, se diseñó la propuesta de una metodología en la que se describe el paso a paso para adaptar y aplicar blockchain en el proceso de facturación de las Empresa de servicios públicos domiciliarios.

3.3.1 Evaluación del uso de blockchain en empresas donde se ha implementado y otros

A continuación, se presentan los resultados que se obtuvieron de evaluar algunas empresas y consultar información en diferentes páginas web. Se abordaron distintos sectores donde se ha aplicado blockchan con el propósito de analizar experiencias diversas. La evaluación y las consultas realizadas estuvieron enfocadas en conocer en qué áreas tienen implementado blockchain, la forma de implementación, bondades, ventajas, desventajas y mejores prácticas.

Con los usos hallados puede comprobarse que esta tecnología de hoy es versátil y en cada proceso que se aplique suma a las empresas, aporta seguridad, trazabilidad, inmutabilidad, observación en línea y mucha confianza. Además de la cantidad de actividades que puede cubrir en un único proceso y en procesos diferentes.

A continuación, se muestra el resultado detallado de algunas de las consultas realizadas, donde se evidencia que independientemente del proceso donde se aplique blockchain tiene usos específicos y que representan múltiples mejoras a los procesos:

- **Evaluación Blockchain Logistic**

Función: Emprendimiento diseñado para manejar cadenas de suministros de productos de manufactura y de café, por medio de blockchain.
Entrevistado: Gerente

Experiencia: la idea surgió de una combinación entre pasión y la necesidad de encontrar datos sobre diferentes productos que eran para el consumo propio. El entrevistado considera que actualmente, las especificaciones que se conocen de los productos de consumo son deficientes, incluso si se indaga en las páginas web. Por este motivo, con su emprendimiento desea que los empresarios cambien su forma de comunicarse con los clientes y les permitan consultar y conocer el detalle de la información que hay alrededor de sus productos.

Proceso: Los empaques de los productos tienen un código QR, el cual al ser escaneado se dirigirá a una landing page donde se podrá observar toda la información de la cadena de suministro, como, por ejemplo, granjas de cultivo, momento de cosecha, proceso de empacado, transporte, proveedores, puntos de almacenamiento, unión de ingredientes, proceso de entrega, imágenes, certificados, entre otros.

Para el caso de esta empresa, la implementación la va a contratar con un tercero, el cual, mediante una plataforma en la nube soportada por blockchain, mostrará la cadena de suministro de sus productos específicos desde su origen y procedencia, hasta su entrega final.

La plataforma utilizada es Amazon Web Service y el código se desarrollará en Hyperleger fabric.

Ventajas:

- Rastreo y trazabilidad de los productos en tiempo real

- Digitalización de la cadena de suministro
- Seguridad de los datos porque blockchain es descentralizada. Es decir, no está en un único repositorio fácilmente hackeable.
- La información está en la nube
- En la cadena de bloques se tiene hashes y criptografía
- Programación teniendo en cuenta la normatividad que se debe cumplir

Desventajas:
La implementación de blockchain la solicitó con un tercero porque en su emprendimiento no tiene desarrolladores expertos.

- **Evaluación Blockchain Ex Innovation center**

Función: la empresa ayuda a empresarios, emprendedores y profesionales independientes a desarrollar una mentalidad ágil que comprenda los retos que trae la cuarta revolución industrial, y así crear valor o generar nuevas capacidades digitales para sus proyectos o empresas.

Experiencia: Han asesorado a muchos emprendedores y empresarios sobre blockchain y, además, los han acompañado en el proceso de implementación.

Proceso: Inicialmente hablan con el cliente y le hacen preguntas como: ¿cuál es la situación para resolver?, ¿qué ocurre si no se soluciona?, ¿cuántas auditorías hacen en sus procesos y los costos?, validan si tienen presupuesto para la atención de fraudes, preguntan la cantidad de registros que se incluirán, si el proceso es uno solo o está fraccionado, y el detalle de este. Posteriormente, realizan una hipótesis y analizan si al agregar blockchain en el proceso pueden asegurar la inmutabilidad de los datos y mejorarlo.

Dependiendo del tipo de negocio, proponen diversas alternativas de solución. Por ejemplo, si son muchos registros, proponen generar paquetes de datos con funciones criptográficas y luego almacenarlos en blockchain, toda vez que el almacenamiento por dato es costoso. Cada bloque es un conjunto de filas con una marca de tiempo, y la huella digital del último bloque, es el registro del siguiente.

Por otro lado, si no son tantos datos, puede realizarse la cadena con un manejo diferente a empaquetar los registros, e igualmente teniendo en cuenta el manejo de los hashes.

Ventajas:

- Reducción de costos de auditorías de contratos
- Reducir costos futuros en disputas legales
- Disminución de tiempos de consolidación de pruebas
- Adicionar un método probatorio para posibles disputas
- Aumentar la integridad a los datos
- Mayor trazabilidad de la alteración y los cambios en los datos del sistema
- Fortalecer los niveles de confianza entre las partes

Desventajas

No se indicó ninguna

- **https://www.provenance.io/**

Función: "Provenance Blockchain es una cadena de bloques pública de código abierto diseñada y desarrollada para brindar beneficios comerciales materiales a los participantes y desarrolladores de servicios financieros a través de sus capacidades de registro, registro e intercambio en múltiples activos y mercados financieros" [61]. En otras palabras, brindan posibilidades comerciales asociadas a servicios financieros, utilizando blockchain.

Experiencia: Provenance Blockchain ofrece una plataforma tecnológica para realizar transacciones financieras [61].

Ventajas [61]**:**

- Proporciona un libro mayor, un registro y un intercambio entre activos y mercados financieros
- El hash se utiliza para pagar las tarifas de la transacción, comunidad y contratos inteligentes.
- Mercados descentralizados
- La cadena de bloques es el registrador, los valores están en las billeteras de los propietarios, por ello estos los controlan.
- Autenticidad

- Precisión
- Líder para servicios financieros
- Validadores de calidad

Desventajas:

No se observa ninguna

- **https://www.ibm.com/co-es/blockchain/solutions/food-trust** [62]

Función: Por medio de blockchain muestran a sus clientes el proceso completo de la cadena de suministro. Es decir, pueden rastrear sus productos en todo momento, ver ubicación, estado, tiempo desde la cosecha, tiempo de permanencia, entre otros. Igualmente, blockchain es segura y permite cargar, administrar, editar y compartir documentos asociados.

Experiencia: Es un ecosistema conformado por productores y proveedores, que están trascendiendo en un sistema alimentario inteligente, seguro, rastreable, y sostenible.

Ventajas:

- Integridad
- Eficiencia
- Confianza
- Brinda visibilidad de extremo a extremo
- Innovación
- Seguridad

Desventajas:

No se halló ninguna en la página consultada

Aparte de estos resultados expuestos anteriormente, a en la tabla 3-15 se relaciona un mayor detalle del resultado obtenido en la investigación:

Tabla 3-15 Usos de blockchain

Empresa/ proyecto	Proceso	Usabilidad	Bibliografía
Blockchain Logistic	Cadenas de suministro de productos de manufactura y producción de café	Manejo y rastreo de la cadena de suministro	Evaluación de empresa
Blockchain Ex Innovation center	Asesoría a empresarios, emprendedores y estudiantes, sobre blockchain y su implementación	*Formación a estudiantes sobre blockchain y su implementación *Acompañamiento en instalación de blockchain en soluciones financieras *Formación y acompañamiento a emprendimientos	Evaluación de empresa
Provenance blockchain	Transacciones financieras	*Realización de transacciones financieras	[61]
IBM Food Trust blockchain	Cadena de suministros	*Rastreo de café *Rastreo de comida de mar *Rastreo de lechugas	[62]
Unergy	Energías renovables	Aseguramiento de los movimientos de la plataforma, imposibilitando su modificación.	[63]
Walmart	Cadena de suministros de productos cárnicos y avícolas	*Mejoramiento del proceso de gestión y seguimiento de datos. *Rastrear la información desde el agricultor hasta el corredor	[64]
Aerolínea British Airways	Vuelos	Administración e información de los vuelos entre aeropuertos	[64]
Compañía naviera Maerks	Carga	*Rastreo de envíos desde un puerto a otro. *Registro de los detalles de envío de carga desde su inicio hasta su destino final	[64]
FedEx	Envíos	Resolución de disputas entre clientes	[64]

Empresa/ proyecto	Proceso	Usabilidad	Bibliografía
BHP Billiton	Minería	Manejo de las cadenas de suministro, registrando y rastreando los movimientos de las muestras de rocas y fluidos de los pozos	[64]
Alibaba: comercio electrónico	Cadena de suministros de bienes de lujos y alimentos	*Seguimiento de bienes de lujo en sus sitios de comercio *Rastreo del movimiento de alimentos con sus socios	[64]
Tencent	Facturación legal e impuestos	*Combatir facturas falsas *Verificar autenticidad de las facturas *Reducción de negocios que aprovechan los vacíos fiscales	[64]
Metlife	Salud	*Conexión de registros médicos electrónicos en tiempo real y emisión de pólizas en minutos *Emisión de pagos automáticos sin necesidad de reclamaciones	[64]
Facebook	Datos personales	Almacenamiento de datos personales	[64]
Walt Disney	Inventarios	*Seguimiento de inventarios, ventas y envíos en los parques	[64]
Ford	Industria automotriz	*Permitir que las tecnologías de movilidad sean compatibles con sus soluciones Smart Mobility *Comunicación entre autos para reducir el tráfico	[64]
Prudential	Seguros	*Búsqueda de socios y distribuidores. Realizar pagos y rastrear bienes.	[64]
Nestlé	Cadena de suministro de alimentos para niños	*Seguimiento de productos alimenticios	[64]
Toyota	Industria automotriz	*Acelerar la tecnología de conducción autónoma.	[64]
Samsung	Tecnología	Administrar su cadena de suministro de dispositivos electrónicos de todos los tamaños	[64]

Nota. Fuente: propia

3.3.2 Mejores prácticas investigadas en el uso de blockchain vs los riesgos hallados previamente

Igualmente, con base en la investigación, el estudio que se ha realizado y las empresas evaluadas, en la tabla 3-16 se relacionan las mejores prácticas que se hallaron en los diferentes usos, procesos y sectores donde se ha aplicado blockchain. Con estas mejores prácticas halladas, se hará un paralelo con los riesgos identificados en los procesos de facturación y plasmados en la fase 1 de este documento, con el propósito de proponer acciones que ayuden a disminuir la posibilidad de que un riesgo sea materializado:

Tabla 3-16 Mejores prácticas

Riesgos	Mejores prácticas
Denegación de servicio DOS/DDOS en bases de datos, contratistas, información, proveedores, servidores, sistema facturador, sistema de direcciones, software de lectura	Blockchain ayuda a mejorar la defensa cibernética, asegurando y previniendo fraudes, toda vez que tiene mecanismos de consenso, uso de hasches, detecta si hubo manipulación de información, por sus características de inmutabilidad, transparencia, auditabilidad, ofuscación de datos y resiliencia operacional
Ingeniería social que afecte clientes, contratistas, empleados, proveedores.	Debido a que es un sistema distribuido se pueden realizar transacciones sin intermediarios. Adicionalmente, cada uno de los nodos tiene su propio hash, su propia seguridad, por lo que cada bloque es validado de forma descentralizada por los anteriores. Así las cosas, si llega a modificarse la información de un bloque, esto sería identificado fácilmente por los demás, por el cambio de su hash. En otras palabras, se hace un consenso entre nodos. Así, al almacenarse la transacción en la blockchain y llegar al consenso, se asegura criptográficamente, lo que dificulta ampliamente que la información sea manipulada.

Riesgos	Mejores prácticas
Malware, afecte bases de datos, contratistas, herramientas ofimáticas, información, proveedores, servidores, sistema facturador, contratistas, sistema de gestión de direcciones, software de lectura	Blockchain ayuda a mejorar la defensa cibernética, asegurando y previniendo fraudes, toda vez que tiene mecanismos de consenso, uso de hasches, detecta si hubo manipulación de información, por sus características de inmutabilidad, transparencia, auditabilidad, cifrado de datos y resiliencia operacional
Phishing, afecte contratistas, empleados, información, impresión	Blockchain ayuda a mejorar la defensa cibernética, asegurando y previniendo fraudes, toda vez que tiene mecanismos de consenso, uso de hasches, detecta si hubo manipulación de información, por sus características de inmutabilidad, transparencia, auditabilidad, cifrado de datos y resiliencia operacional
SQL Injection, afecte bases de datos, contratistas, proveedores	Blockchain ayuda a mejorar la defensa cibernética, asegurando y previniendo fraudes, toda vez que tiene mecanismos de consenso, uso de hasches, detecta si hubo manipulación de información, por sus características de inmutabilidad, transparencia, auditabilidad, cifrado de datos y resiliencia operacional
Ransomware, afecte bases de datos, contratistas, herramientas ofimáticas, información, proveedores, servidor, sistema facturador, sistema gestor de direcciones, software de lectura	Blockchain ayuda a mejorar la defensa cibernética, asegurando y previniendo fraudes, toda vez que tiene mecanismos de consenso, uso de hasches, detecta si hubo manipulación de información, por sus características de inmutabilidad, transparencia, auditabilidad, cifrado de datos y resiliencia operacional
Ausentismo afecte contratistas, proveedores	
Errores o imprecisiones en la elaboración de los contratos, afecte contratistas, empleados, facturas, proveedores	A nivel técnico, cada contrato inteligente, tendrá programado en su interior el código especificado inicialmente, con las garantías de seguridad que brinda blockchain

Riesgos	Mejores prácticas
Fraude afecte bases de datos, clientes, contratistas, emleados, herramientas ofimáticas, infomración, proveedores, servidores, sistema facturador, sistema gestor de direcciones, software de lectura, terminal de lectura	Blockchain ayuda a mejorar la defensa cibernética, asegurando y previniendo fraudes, toda vez que tiene mecanismos de consenso, uso de hasches, detecta si hubo manipulación de información, por sus características de inmutabilidad, transparencia, auditabilidad, cifrado de datos y resiliencia operacional
Fuga de información afecte el activo bases de datos, contratistas, empleados, facturas, herramientas ofimáticas, información, proveedor de impresión, servidores, sistema facturador, sistema gestor de direcciones, software de lectura, terminal de lectura	Blockchain tiene mecanismos de cifrado de datos. Adicionalmente, tiene hasches y llaves privadas y públicas.
Huelga afecte contratistas, proveedores, empleados	
Inadecuada segregación de funciones afecte bases de datos, información, servidor, sistema facturador, sistema gestor de direcciones, software de lectura, empleados, herramientas ofimáticas, terminal de lectura	Durante el desarrollo de los contratos inteligentes de la blockchain, se pueden evidenciar errores asociados a la segregación de funciones y a su vez se pueden corregir. Las funciones y/o actividades críticas se pueden separar dentro de la cadena de bloques, de modo que cada colaborador ejecute el procedimiento que le corresponde de acuerdo con su cargo.
Inadecuado control de la ejecución que afecte empleados, herramientas ofimáticas, terminal de lectura	Los algoritmos incluidos en los contratos inteligentes validan los datos que se ingresan. Por ejemplo: validación del tipo de datos. Igualmente, la blockchain contiene los controles propios del proceso de facturación.
Incumplimiento de normas, leyes y requisitos, afecte clientes, contratistas, empleados, facturas, información, proveedores, sistema facturador.	La facturación de los servicios públicos está sujeta a la normatividad que se emita en el país y la cual es de obligatorio cumplimiento. Por lo tanto, la blockchain debe tener la capacidad de adoptar en sus algoritmos los nuevos procedimientos, conceptos de facturación y hasta las nuevas formas de facturar.
Selección de contratistas o personal no idóneo, afecte clientes, contratistas, empleados, proveedores, sistema facturador	Blockchain tiene mecanismos de cifrado de datos. Adicionalmente, tiene hasches y llaves privadas y públicas.

Nota. Fuente: propia

3.3.3 Metodología para la adaptación y aplicación de blockchain

Se propuso la metodología para la adaptación y aplicación de blockchain, con el propósito de asegurar el proceso de facturación de las empresas de servicios públicos, toda vez que esta apunta a los principios de la seguridad de la información, con blockchain “cada evento o modificación de los datos se escriben como un nuevo bloque de una cadena y de esta manera queda un registro asentado, certificado y se garantiza su integridad y disponibilidad”. Si además ese contenido está cifrado, garantiza confidencialidad” [65].

Lo anterior, es avalado por la dependencia de ciber-riesgo de Deloitte, debido a que afirman:

Sobre integridad “aunque todavía es incipiente, existe una innovación prometedora en blockchain encaminada a ayudar a las empresas a enfrentar desafíos inmutables de riesgo cibernético como lo son la identidad digital y mantener la integridad de los datos.” Por tanto, con esta tecnología se pueden prevenir ciberataques e identificar alteración de datos, todo debido a sus mecanismos de consenso, transparencia, auditabilidad y validación en línea [22].

Sobre disponibilidad indican “asegurar el acceso y uso oportuno y confiable de la información”, lo cual es una fortaleza de blockchain, dado que es descentralizada y por sus características peer to peer o red entre pares [22].

Igualmente, sobre confidencialidad indican “El cifrado completo de los datos de la cadena de bloques garantiza que las partes no autorizadas no puedan acceder a los datos mientras estos datos se encuentren en tránsito”, por lo tanto, que en blockchain la información sea cifrada, eleva su nivel de confidencialidad [22].

Así las cosas, se confirma que el modelo de la tecnología mencionada permite tener datos exactos, confidenciales y cifrados, compartidos solo entre quienes tienen autorización de gestionarlos, lo cual, a su vez, conlleva a mitigar y a eliminar la materialización de los riesgos, los cuales, en muchas oportunidades corresponden a puertas abiertas para los ciberdelincuentes.

Por lo anterior, y al ser una tecnología altamente versátil y aplicable, a continuación, en la Figura 3-25 se presenta la metodología propuesta, en la que se explica el paso a paso que se puede llevar

a cabo para adaptar y aplicar blockchain en el proceso de facturación de una empresa de servicios públicos.

Con la certeza de que será de gran ayuda, toda vez que la metodología está dividida en 16 etapas y muchas de estas ya fueron explicadas y desarrolladas a lo largo del presente documento. Las etapas diseñadas para llevarse a cabo en la presente metodología son:

Figura 3-25 Metodología diseñada para adoptar y aplicar blockchain

Nota: Fuente propia

3.3.3.1 Definir el equipo de trabajo

Es importante definir el equipo de trabajo con el cual se realizará el proceso de aplicación e implementación de blockchain, el cual está compuesto por personal inmerso en el proceso de facturación y personal contratista, para ello se puede revisar la fase uno de este escrito (Proceso

de facturación general). Allí se informa por cada etapa que compone el proceso, quienes realizan las actividades, si son colaboradores individualmente, equipos o empresas contratadas.

Lo anterior porque, adicional a requerirse personal experto en facturación, también se requiere personal experto en blockchain, personal directivo para la toma de decisiones, personal operativo, personal de tecnologías de la información (TI) y de presupuesto, un líder técnico y uno funcional.

La participación de cada uno de estos roles sería:

- **Personal experto de facturación:** con sus amplios conocimientos en el proceso de facturar, desde su inicio hasta su fin, los expertos guiarían sobre la estructura establecida para ejecutar todas las actividades inmersas en el proceso. Además, son los conocedores de la normatividad que se debe cumplir.

- **Personal directivo:** son los colaboradores que, por su cargo directivo, a lo largo del proyecto tienen la posibilidad de tomar decisiones sobre el proceso de facturación.

- **Personal operativo:** son las personas que saben cómo realizar sus actividades y tareas, esta información es crucial para el personal experto en blockchain, pues son quienes crearán los algoritmos y programación requerida para la implementación.

- **Personal de tecnologías de la información (TI):** es preciso contar con TI porque es la dependencia que conocen la estructura tecnológica con la que se cuenta, a nivel de servidores, bases de datos, permisos de instalación y aplicaciones. Información necesaria para revisar la posibilidad de implementar blockchain en el proceso y para su posterior implementación.

- **Personal de presupuesto:** son quienes se encargan de analizar y revisar si es viable destinar el presupuesto requerido para la implementación de blockchain.

- **Líder técnico:** se encarga de liderar y planificar el proyecto de implementación de blockchain a nivel técnico. Es decir, define roles, herramientas, hace seguimientos y reporta avances.

- **Líder funcional:** se encarga de engranar todos los equipos de trabajo, hacer cronogramas, revisar periódicamente el estado del proyecto, programar reuniones diarias, solicitar presupuestos, entregar reportes e informes periódicos, evaluar la pertinencia de la implementación de blockchain.

El entregable es:

- Documento de roles por equipo de trabajo: Documento que contenga para cada uno de los roles incluidos en el proceso y la descripción de sus actividades. Debe incluir nombres, cargos, herramientas y aplicaciones que utilizan en su labor, e indicar si se tienen colaboradores espejo

A partir de la definición del equipo de trabajo, se continúa con las etapas: Levantar requerimientos y Capacitar al equipo de trabajo en blockchain.

3.3.3.2 Capacitar al equipo de trabajo sobre la tecnología blockchain

La metodología que se está proponiendo, pretende ilustrar e informar la manera como se puede adoptar y aplicar la tecnología blockchain en una empresa del sector de los servicios públicos domiciliarios, toda vez que, esta permitirá innovar, optimizar, agilizar, y asegurar el proceso de facturación según los pilares de seguridad de la información (integridad, disponibilidad y confidencialidad).

Para cumplir con lo anterior, es necesario inicialmente, hacer una capacitación de cambio, cultura y concientización. Además, una capacitación propia de blockchain para que el equipo de trabajo adquiera los conocimientos necesarios y puedan aplicarlos en el proyecto a realizar.

Entre los posibles temas que se pueden incluir en la capacitación están los siguientes, los cuales se encuentran en el marco teórico del presente escrito (Blockchain):

- Definición de blockchain
- Estructura

- Funcionamiento
- Beneficios
- Elementos clave
- Tipos de redes blockchain
- Seguridad
- Principios esenciales

Igualmente, se pueden contar experiencias de otras empresas, y cómo por medio de su implementación se han transformado otros procesos. En este documento se encuentran algunos ejemplos (Evaluación del uso de blockchain en empresas donde se ha implementado y otros).

Los entregables son:

- Plan de asimilación: este plan deberá contener los multiplicadores, temas que se incluirán en la capacitación, espacios y tiempos.
- Instructivos: documentos que incluyan los temas tratados
- Registro de asistencia: nombres, identificación, equipo de trabajo y firma.
- Información de aplicaciones y herramientas que se utilizan en el proceso.

A partir del conocimiento adquirido en esta etapa, se puede continuar con la etapa: Contratar Empresa experta en el desarrollo de blockchain para su adaptación y aplicación.

3.3.3.3 Levantar requerimientos

Este inicio de la metodología permite conocer las necesidades del negocio, e identificar su naturaleza. Es decir, entender la necesidad y sus razones, si corresponde a falencias en la ejecución de los procesos, obsolescencia y/o cambios tecnológicos, auditorías, seguridad, normatividad, tendencias del mercado, el dinamismo de la empresa por política administrativa, entre otras.

Para hacer el levantamiento de requerimientos se pueden tener en cuenta las siguientes técnicas de ingeniería de requisitos en metodologías ágiles con sus respectivos entregables [66]:

- La entrevista: es la manera más idónea de acercarse al cliente, porque conversando se puede obtener la información suficiente que permita identificar su necesidad, aclarar sus ideas, y entender detalladamente el requerimiento. Adicionalmente, reducir en un alto porcentaje las interpretaciones erradas.

  Estas entrevistas pueden tener preguntas cerradas y preguntas abiertas, éstas últimas facilitan el entendimiento, toda vez que contienen información ampliada.
  El entregable de las entrevistas es un documento donde se plasmen fechas, entrevistador y entrevistado, y por supuesto, las preguntas y respuestas entregadas.

- Reuniones de análisis: las reuniones son transversales a todas las actividades que se ejecutan y deben ser constantes, aportan al análisis de elementos que surgen, entregan retroalimentación sobre el proceso y une a los interesados.

  El entregable es un documento con el registro de la fecha de realización, participantes, temas tratados y compromisos.

- Documentación: Con el fin de ampliar el conocimiento sobre el negocio, es recomendable obtener instructivos, definiciones, normatividad asociada y demás información que pueda ser relevante.

- Validación: Son encuentros donde se valida el cumplimento de los objetivos, esto con respecto a lo definido inicialmente y al cronograma.

- Historias de usuario: corresponde al detalle de las actuaciones que conllevarán al logro de los objetivos definidos previamente. Tienen un rol importante, toda vez que son construidas por el cliente, quien finalmente es quien conoce su necesidad.

  El entregable sería un documento donde se incluyan las historias de usuario, el rol y el resultado esperado.

Al final de la o las técnicas planteadas, se obtendrá como entregable:

- Documento de especificación en el cual se informe la solicitud ampliamente explicada, clara, concisa y detallada, el propósito, las historias de usuario e interesados.

A partir del levantamiento de requisitos o de requerimientos, se desprenden las etapas de: Conocer el proceso de facturación de la compañía y costo inicial.

3.3.3.4 Conocer el proceso de facturación de la compañía

Una vez se tenga claridad sobre la necesidad del cliente y el equipo de trabajo, continúa conocer el proceso que se lleva a cabo para facturar, a nivel operacional y de negocio. Por lo que se sugiere dirigirse hasta el desarrollo de la fase 1 de este documento (Proceso de facturación general), toda vez que allí se estructuró un proceso de facturación global, que se puede aplicar a cualquier empresa de servicios públicos domiciliarios. Adicionalmente, se definió y se explicó detalladamente en qué consiste cada una de sus partes y los colaboradores o equipos de trabajo que deben ejecutarlas.

Igualmente, el conocimiento del proceso de facturación de la compañía se puede obtener por medio de entrevistas enfocadas a líderes y expertos, terceros, y consultas a la página web de la empresa y de los Entes reguladores. Así mismo, con la documentación que el cliente brinde, como: instructivos, reportes e informes, y demás documentación que facilita la profundización en la información y la obtención de mayores detalles sobre el proceso.

Una vez se conozca el proceso es preciso documentarlo, y se recomienda llevarlo a un diagrama de flujo en el que se visualicen sus partes, pues esto facilitará su comprensión.

Para esta etapa el entregable es:

- Proceso de facturación estructurado en el que se evidencie cada una de sus partes y como se conectan unas con otras. Además, la definición de cada una de cada una de ellas con la respectiva identificación de sus actores.

El hecho de conocer el proceso de facturación de la compañía permite conectarse conectarse con la etapa: Levantar requerimientos. Toda vez que, al conocer más a fondo el negocio y su operación, se pueden evidenciar nuevos requisitos y necesidades. Igualmente, se puede continuar con las etapas: Hacer mapa de riesgos e Identificar aplicaciones y herramientas.

3.3.3.5 Costo inicial

Hace referencia al análisis que se realiza para determinar que el proyecto no se desborde financieramente, de modo que se cumpla con que el valor retornado sea superior al costo del proyecto.

En este análisis, la Empresa debe revisar los siguientes costos:

- Fijos
- Variables
- Mano de obra directa e indirecta
- Software

Así mismo, es importante revisar aspectos como:

- Costos por materialización de los riesgos
- Costos promedios en el último año ocasionados por actividades manuales
- Costos por hallazgos en auditorías
- Costos por remuneración de personal

Al recibir la propuesta de la empresa que se contratará para el desarrollo de blockchain, podrá compararse el costo beneficio que traería la implementación.

El entregable es un documento donde se aclaren todos los costos y donde se evidencie el valor proyectado de pérdidas y ganancias.

Con base en el análisis obtenido en esta etapa Costo inicial, se puede continuar con la etapa Contratar Empresa experta en el desarrollo de blockchain para su implementación.

3.3.3.6 Identificar las aplicaciones y herramientas

Se debe hacer el reconocimiento de las aplicaciones y herramientas que hacen parte del proceso de facturación actual, para ello se recomienda dirigirse a la fase 1 de este documento en la sección identificación de activos (Identificación de activos), allí se relacionan los activos inmersos en los procesos de facturación.

Igualmente, la manera de identificar los activos del proceso de facturación es analizar cada una de las partes que lo integran, allí se observan herramientas, aplicaciones, equipos y demás activos.

Los entregables de esta etapa son:

- Inventario de los activos hallados con su descripción. Además, asociarlos con cada determinada parte del proceso de facturación.

A partir de identificar las aplicaciones y herramientas, se continúa con la etapa: Capacitación del equipo de trabajo en blockchain.

3.3.3.7 Hacer mapa de riesgos

Realizar un mapa de riesgos en el que se identifiquen los riesgos inmersos en el proceso de facturación, midiendo el impacto a nivel de indisponibilidad de la información, cómo activo más importante del negocio. Con dicho mapa de riesgos construir una matriz de calificación del riesgo, con las clasificaciones de aceptables, tolerables, inaceptables e inadmisibles.
Para realizar el mapa de riesgos se recomienda revisar la fase 1 del presente documento, pues se elaboró un mapa de riesgos sobre un proceso de facturación global, enfocado en el impacto indisponibilidad de la información (Mapa de riesgos).

Se aclara que el enfoque se hizo con el impacto a nivel de indisponibilidad de la información, porque, entre otras, es el activo que pretende blindarse con la implementación de blockchain.

Así mismo, es importante tener en cuenta que para llegar al mapa de riesgos se debe hacer la identificación de los siguientes elementos, para finalmente llegar a la calificación del control:

- Activos
- Amenazas
- Vulnerabilidades
- Escenarios del riesgo
- Agentes generadores

El entregable es:

- Mapa de riesgos: Documento con la construcción de un mapa de riesgos enfocado en indisponibilidad de la información. Así las cosas, se evidencian los riesgos latentes en el proceso y su clasificación en términos de gravedad. Este debe contener: activos, amenazas, vulnerabilidades, escenarios del riesgo y calificación del control. El documento debe contener graficas donde se plasmen los hallazgos.

Con base a la información recopilada en el mapa de riesgos, se puede nutrir nuevamente la etapa Levantar requerimientos, pues pueden surgir nuevas necesidades que deban ser incluidas. Igualmente, dicho mapa da continuidad a las etapas: Diseño del plan de tratamiento y la Construcción de mejores prácticas en el proceso de facturación.

3.3.3.8 Diseñar plan de tratamiento

En esta fase, se deberá diseñar un plan de tratamiento para gestionar los riesgos de seguridad inadmisibles e inaceptables, incluidos y analizados en el mapa de riesgos previamente construido. El plan de tratamiento deberá incluir las acciones de reducir, retener, evitar y transferir los riesgos. Igualmente, se recomienda revisar el plan de tratamiento desarrollado en la fase 2 de este documento Plan de tratamiento para riesgos inadmisibles e inaceptables, toda vez que cumple con las condiciones necesarias para evitar que se materialice un riesgo y facilitar la reacción oportuna y eficaz en caso de que ocurra. Debido a las ventajas en términos de automatización y de seguridad

que brinda blockchain, con su implementación muchos de los riesgos incluidos en el plan de tratamiento pueden evitarse y reducirse.

El plan de tratamiento se hace sobre los riesgos inadmisibles e inaceptables, identificando su tratamiento en términos de retención, evitación, reducción y transferencia. Igualmente, se deben describir las acciones que se realizarán para dicho tratamiento, el plan de monitoreo, los responsables y el resultado esperado.
El entregable es:

- Plan de tratamiento: Documento donde se plasme por cada riesgo inadmisible e inaceptable, si se va a reducir, retener, evitar o transferir; el plan que se va a ejecutar para su gestión, el plan de monitoreo y los responsables.

Esta información debe estar incluida en una tabla diseñada para tal fin y en la que se visualice para todos los riesgos, el detalle ya mencionado.

Con los resultados obtenidos a partir del plan de tratamiento, se puede continuar con la siguiente etapa de la metodología propuesta: Construir controles para mejores prácticas.

3.3.3.9 Construir controles para mejores prácticas

Con base en los riesgos identificados en el mapa de riesgo construido y en posibles encuestas realizadas al cliente, se deben plasmar y establecer las mejores prácticas y acciones que proactivamente ayuden a disminuir errores y a mitigar la posibilidad de materialización de los riesgos. Para esto, se propone desplazarse hasta la fase Nro. 2 de los resultados de este documento, allí se encontrarán las mejores prácticas diseñadas a partir de los riesgos identificados (construcción de controles para mejores prácticas).

Para definir las mejores prácticas se sugiere agrupar los riesgos hallados según su similitud. Posteriormente, establecerle a cada grupo acciones que disminuyan su posibilidad de ocurrencia, aporten al cierre de brechas e incrementen la seguridad de la información.

Los entregables son:

- Tabla donde se recopile por grupos todos los riesgos identificados, y a cada grupo asignarle un grupo de acciones o mejores prácticas.

Posteriormente a esta etapa de Construir controles para mejores prácticas, se continúa con la etapa Evaluar la pertinencia de implementar blockchain.

3.3.3.10 Evaluar la pertinencia de adaptar y aplicar blockchain

En esta etapa se deben realizar varias mesas de trabajo individuales, con los líderes funcional y técnico, además, con cada equipo de trabajo: personal operativo, personal experto y personal de TI. En dichas mesas de trabajo, consultar la eficacia de la solución, en términos de uso, funcionalidad, seguridad, proceso, ejecución y optimización. Igualmente, con el apoyo del personal directivo, se deben gestionar los ajustes que se consideren necesarios y resulten de estas mesas de trabajo.

Adicionalmente, con los expertos del proceso de facturación y quienes lo operan, se hará una revisión a nivel de proceso, se revisará si cada fase asociada al proceso de facturación está funcionando correctamente y si el producto final cumple con las especificaciones requeridas.
Por otro lado, se encuestará a los colaboradores involucrados en el proceso, con preguntas enfocadas a validar si la solución desarrollada y entregada es eficaz y cumple con sus requerimientos.

Los entregables son:

- Actas de reunión: De cada una de las mesas de trabajo registrar los resultados. Este documento deberá tener: asistentes, responsables, consultas sobre la eficiencia y seguridad de la solución entregada. Revisión de ajustes pendientes y realizados. Las actas deben incluir fecha y lugar, asistentes, propósito del encuentro, avances, preguntas y respuestas, revisión de ajustes, registro de nuevos ajustes y acciones a tomar, y si aplica, fecha de un futuro encuentro.

- Documento de revisión de la solución entregada: Documento donde se incluya la revisión realizada en cada parte del proceso de facturación, de principio a fin. Revisión a nivel de efectividad del algoritmo y el resultado final.

- Encuesta a colaboradores: Documento donde se incluyan preguntas y respuestas de los colaboradores, asociadas a la efectividad del proceso con la implementación de blockchain. Estas respuestas deben ser compilada y analizadas, para determinar si se está cumpliendo con los requisitos inicialmente levantados.

A partir de la etapa: Evaluación de la pertinencia de adaptar y aplicar blockchain se desglosan las etapas: Justificar la pertinencia de la implementación y Contratar Empresa experta en el desarrollo de blockchain para su implementación.

3.3.3.11 Justificar la pertinencia de la implementación

Con base en los resultados obtenidos en la evaluación realizada, se deberá justificar detalladamente, los motivos por los cuales, la implementación de la tecnología blockchain es la mejor opción para realizar el proceso de facturación de una empresa de servicios públicos. Estos motivos pueden ser en términos de seguridad, mitigación de riesgos, optimización de tiempos, funcionalidad y automatización.

Esta justificación debe incluir estadísticas, porcentajes de avance, valoración de tiempos, comparaciones, y demás información que permita determinar que definitivamente blockchain es la mejor opción.

El entregable es:

- Justificación: Documento donde se argumente y se detallen las razones por las cuales, aplicar e implementar blockchain es la mejor opción para el proceso de facturación de una empresa de servicios públicos. Dicha argumentación detallada, debe estar acompañada de estadísticas de tiempos, ejecución del proceso y eficacia.

Esta etapa de Justificar la pertinencia de la implementación también da apertura a la siguiente etapa: Contratar Empresa experta en el desarrollo de blockchain para su adaptación y aplicación.

3.3.3.12 Contratar empresa experta en desarrollar blockchain para su adaptación y aplicación

Al elegir la Empresa experta para realizar el desarrollo de blockchain, se debe analizar que su propuesta apalanque todas las condiciones de la prestación actual del servicio, porque a la postre, el proceso deberá continuarse y ser funcional hasta obtener el producto final, es decir, la factura.

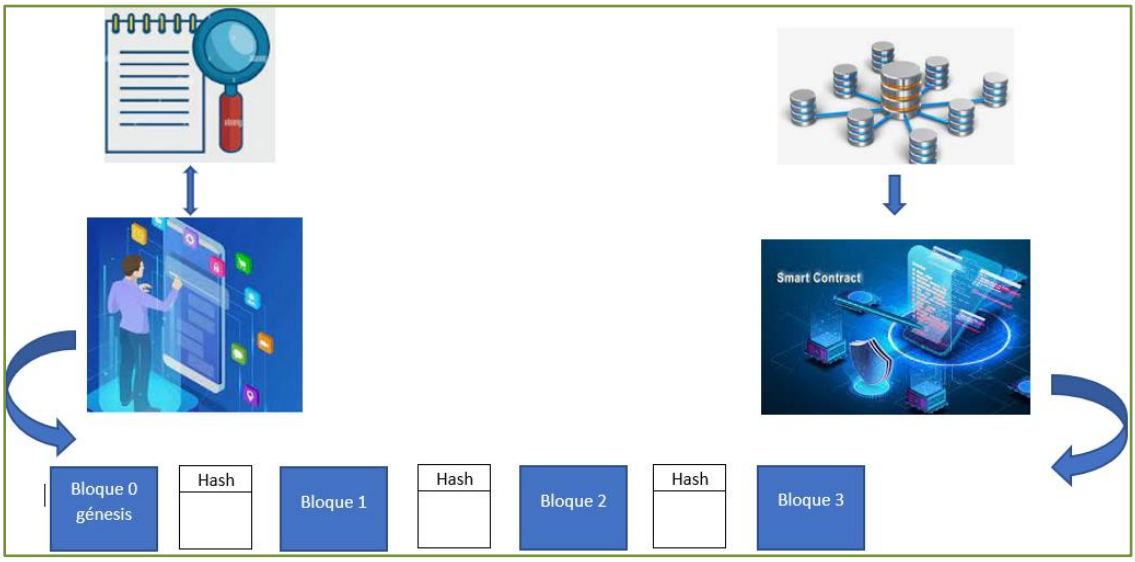
Al contratar la empresa desarrolladora deben considerarse características como: trayectoria, conocimientos de desarrollo en blockchain, manejo de los riesgos y del control de cambios, costos, metodología que utilizan (por ejemplo: metodologías ágiles), cronogramas, horas de soporte posteriormente al paso a producción, plataforma de desarrollo de software, recursos y capacidad que solicitan, como colaboradores, servidores, motor de base de datos, entre otros.

Con la empresa se deberán firmar acuerdos de confianza, toda vez que hay que entregarles la base de datos con los datos de los clientes, códigos de los servicios que se prestan, direcciones, lecturas tomadas para cada servicio de energía, gas, acueducto y alcantarillado con sus respectivas tarifas, los cargos de terceros, y demás información adicional que hace parte de la liquidación de la factura.

La empresa de desarrollo contratada deberá crear una interfaz con el desarrollo de los respectivos contratos inteligentes. La interfaz obtendrá y entregará información desde y hacia la red distribuida de blockchain, la cual será alimentada con los datos entregados por la empresa contratante que estarán alojados en el servidor. Igualmente, el o los contratos inteligentes serán incluidos en bloques, los cuales se interconectarán por medio de hashes.

El esquema podría asemejarse al relacionado en la figura 3-26:

Figura 3-26 Estructura de blockchain



Nota: Fuente propia

La empresa desarrolladora deberá construir un escrito claro y detallado, donde se documenten las ayudas del desarrollo por cada una de las fases de la implementación realizada, de modo que, en el evento de requerir algún tipo de información o modificación, se tenga una base de información completa.

El entregable es:

- Contrato: Contrato con una empresa desarrolladora que implemente blockchain en el proceso de facturación de una empresa de servicios públicos domiciliarios.

Esta etapa surge a partir de las etapas: Evaluar la pertinencia de implementar blockchain, Justificar la pertinencia de la implementación y Costo inicial. Y de ella se desprenden las etapas: Entrega de resultados, Capacitar a los equipos de trabajo sobre la adaptación y aplicación y Revisión del costo.

3.3.3.13 Entrega de resultados

Al revisar el proceso de implementación y aplicación de blockchain, se deberán entregar resultados por cada fase incluida en el proceso de facturación, discriminando los siguientes ítems:

- Disminución de tiempos de ejecución
- Disminución de tareas manuales
- Disminución de los riesgos identificados en la fase No. 1 del presente documento
- Aplicación de mejores prácticas identificadas en la fase Nro. 2 del presente documento
- Crecimiento del proceso en términos de seguridad: confiabilidad, integridad y disponibilidad.

El entregable es:

- Resultados: Informe donde se relacionen los resultados obtenidos con la aplicación e implementación de blockchain, incluyendo el resultado de los ítems mencionados en porcentaje.

3.3.3.14 Capacitar a los equipos de trabajo sobre la adaptación y aplicación

Se debe realizar un plan de asimilación para los colaboradores que intervienen en el proceso de facturación y que no participaron en el proceso de aplicación e implementación de blockchain, de modo que se les transmita el conocimiento sobre la nueva forma de ejecutar sus labores.

Los entregables son:

- Plan de asimilación
- Instructivo: documento donde por cada una de las partes del proceso de facturación, se defina y se explique su funcionamiento, y la nueva manera de ejecutar las actividades asignadas.
- Presentación: Presentación gráfica con el contenido del instructivo realizado, para mayor entendimiento y multiplicación más amena.

3.3.3.15 Revisión del costo

En esta etapa es crucial comparar el costo inicial con el costo final, corroborando que se haya cumplido con los costos previstos y que la inversión realizada no sea superior al valor retornado por la aplicación e implementación de blockchain.

Los beneficios obtenidos con dicha aplicación e implementación deben ser superiores a todo nivel en comparación con los costos de inversión. Es decir, deben ser superiores a la inversión, los beneficios de seguridad de la información y el proceso de facturación, disminución y mitigación de los riesgos, disminución de actividades manuales, mayor automatización y calidad del proceso y del producto final: la factura.

El entregable de esta etapa es:

Documento que incluya los costos iniciales y la proyección de costos finales, con el comparativo de los costos en los que realmente se incurrió y proyectados según las mejoras realizadas sobre el proceso con la aplicación e implementación de blockchain.

3.3.3.16 Gestionar el proyecto

Esta etapa es constante a lo largo de la aplicación e implementación de blockchain en el proceso de facturación. Se refiere a coordinar el proceso planeado y los recursos humanos y técnicos desde el principio hasta si final, pautar reuniones, hacer seguimiento a cada una de las etapas de la metodología propuesta, evitar que se presenten excesos en los costos, garantizar que se cumpla con el cronograma establecido previamente, disponer de holgura para la atención de los imprevistos que se presenten, aportar en la comunicación efectiva entre los integrantes del equipo de trabajo, hacer seguimientos permanentes y el respectivo cierre, todo en pro de lograr los objetivos propuestos.

El entregable de esta etapa es:

Reunión de finalización: Reunión entre las partes incluidas en la etapa Definir el equipo de trabajo, donde se determine el cumplimiento del proyecto y su efectividad. Sobre esta reunión, deberá crearse un acta con fecha del encuentro, el contenido de la reunión, los asistentes, descripción de ajustes pendientes y la aceptación de los involucrados a través de sus firmas.

3.4 Fase 4. Comparativo entre el proceso de facturación actual y utilizando blockchain

Debido a que en la presente investigación se propone una metodología distribuida en etapas para adaptar, aplicar y/o implementar blockchain en el proceso de facturación de una empresa del sector de los servicios públicos domiciliarios, se realizó una valoración que permite definir entre el método tradicional y con la blockchain cuál es más eficiente según criterios previamente identificados: funcionalidad, tiempos de respuesta, seguridad de la información y costos, esto teniendo en consideración los riesgos que se hallaron en la fase 1 del presente documento, las respuestas otorgadas por las empresas encuestadas en la fase 2, la experiencia de implementar en otros sectores en la fase 3, el análisis que se ha hecho de blockchain, y como tal toda la información investigada en el presente documento.

3.4.1 Valoración de criterios con el método tradicional vs adaptando y aplicando blockchain

A continuación, en la tabla 3-17 se detalla los criterios definidos, el porcentaje de calificación otorgado a cada uno de los métodos aplicados al proceso de facturación, tanto el tradicional como adaptando, aplicando y/o implementado con blockchain:

Tabla 3-17 Valoración de criterios con el método tradicional vs adaptando y aplicando blockchain

Criterio	Funcionalidad	%	Tiempos de respuesta	%
Modelo tradicional de protección en el proceso de facturación de una empresa de servicios públicos domiciliarios	El proceso de facturación con el modelo tradicional cumple con lo requerido, aunque deben realizarse controles y actividades de transformación semiautomáticas de información. El proceso tiene brechas de optimización importantes por cerrar, y para las cuales se requieren cambios costosos o transiciones muy complejas dado lo ofrecido por el proveedor y por la forma como se ha customizado la operación. Por ejemplo: el análisis de consumos telemedidos, no es posible realizarlo en el aplicativo porque no lo soporta, igual que la agrupación por ciclos.	60	Los tiempos de respuesta ya están dados y pueden variar dependiendo de situaciones como: *Errores en la carga de consumos *Errores en la carga de tarifas *Errores en la carga de archivos *Retrasos en ciclos anteriores En lo que se refiere a nuevos desarrollos e implementaciones ajenos a la normatividad, la respuesta es lenta y puede tardarse meses debido a las diferentes mejoras que se tengan pendientes. Cuando son requerimientos normativos, aunque se priorizan, en ocasiones tampoco alcanzan el horizonte en el tiempo establecido.	45
	Costos	**%**	**Seguridad de la información**	**%**

	Corresponden a los costos propios del proceso y a los que se incurre por los diferentes contratos de lectura, terceros e impresión. Así mismo, en términos de actualización de versión del facturador, representan costos considerables, teniendo en cuenta que el beneficio no es realmente significativo en lo que se refiere a nuevas posibilidades. En términos de reclamaciones, cuando son revocados, la Empresa pierde el derecho al cobro y debe realizar reintegros y devoluciones a los clientes.	55	Al existir segregación de funciones, se garantizaría que solo quienes realicen determinadas actividades, tengan los privilegios necesarios para observar esa determinada información. En otras palabras, la seguridad se ha fortalecido dejando claros los roles, perfiles y estableciendo el modo de acceder a ellos. El ingreso de datos manualmente permite su alteración, y conlleva a reprocesos y ajustes de facturación. Los ajustes y arreglos a la factura ocasionan reclamos, los cuales al ser manuales también pueden presentar datos errados. Adicionalmente, las auditorías internas y externas permanentes permiten detectar constantemente oportunidades de mejora.	45
Criterio	**Funcionalidad**	**%**	**Tiempos de respuesta**	**%**
Adaptando y aplicando blockchain en una empresa de servicios públicos domiciliarios	Con la implementación de blockchain en el proceso de facturación, éste continúa su curso según el proceso definido en la fase número 1. Desde el levantamiento de requerimientos se hace un reconocimiento de la necesidad del negocio, de modo que los contratos inteligentes desarrollados cumplen con lo especificado inicialmente, y su ejecución es automática. Realizar automáticamente las tareas aumenta las probabilidades de una correcta ejecución y disminuye los errores por manualidades.	95	Los tiempos de respuesta estarán basados según el desarrollo realizado. Es decir, cada nodo ejecutará su actividad y tareas internamente de forma automática. En esta implementación la carga de consumos, tarifas y archivos habrá tenido un proceso de consenso que validará que sea la información correcta. Con blockchain se podrá tener información precisa sobre los tiempos reales de ejecución en cada proceso, y dada la automatización estos disminuyen con respecto al proceso actual.	90

	Los costos varían dependiendo de la cantidad de datos, la forma de almacenamiento y los desarrollos. No obstante, esta inversión sería retornada dados los múltiples beneficios que tiene blockchain. Adicionalmente, el disminuir los errores de facturación, es directamente proporcional con la disminución de los costos por devoluciones y ajustes a la factura.	70	Blockchain tiene la propiedad de la confidencialidad, es decir, que solo el personal autorizado puede acceder a la información. También tiene la propiedad de la integridad. Cada nodo tiene una copia de la base de datos sincronizada, entre los cuales se establece el consenso criptográfico. Es decir, la información no es modificada, cada bloque tiene su respectivo hash que no permite alteraciones en la información, y si llegara a presentarse sería identificado. La misma estructura de blockchain permite que la información siempre esté disponible. Facilita la trazabilidad en línea.	99

Nota. Fuente propia

Finalmente, al hacer el cálculo del total generado por cada forma estudiada para ejecutar el proceso de facturación en cada uno de los criterios previamente definidos, se obtuvieron los resultados que se muestran en la siguiente tabla 3-18:

Tabla 3-18 Valoración final

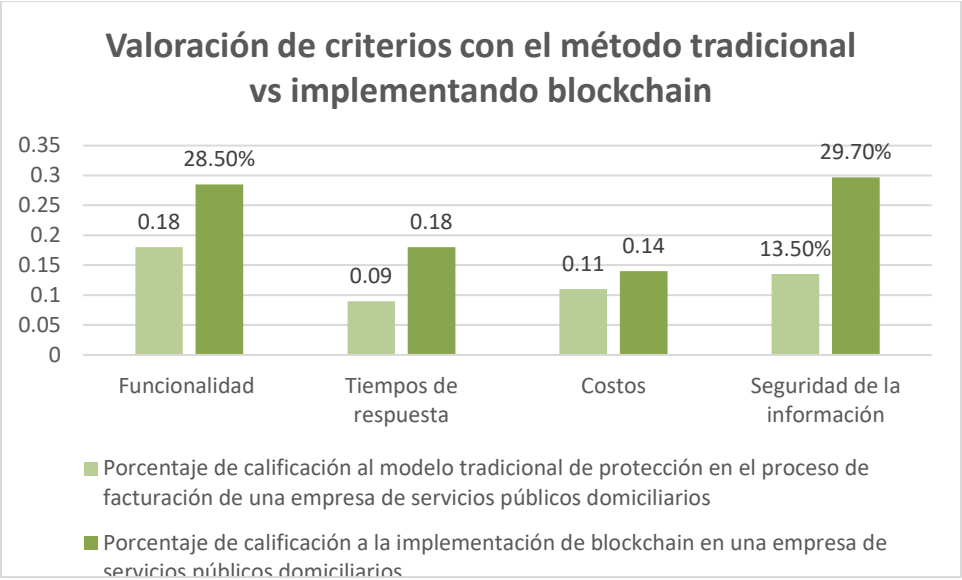
Modelo	Porcentaje	Porcentaje de calificación al modelo tradicional de protección en el proceso de facturación de una empresa de servicios públicos	Porcentaje de calificación a la adaptación y aplicación de blockchain en una empresa de servicios públicos
Funcionalidad	30%	18%	28.5%
Tiempos de respuesta	20%	9%	18%
Costos	20%	11%	14%
Seguridad de la información	30%	13.5%	29.7%
Total	100%	51.5	90.2%

Nota: Fuente propia

En la tabla 3-18 y en la Figura 3-27, se resume el resultado obtenido de la valoración realizada teniendo en cuenta las definiciones halladas en cada una de las formas de realizar el proceso. Igualmente, puede deducirte que, en cada uno de los criterios de funcionalidad, tiempos de

respuesta, costos y seguridad de la información, el mayor porcentaje de logro se obtiene trascendiendo del proceso actual, y adoptando y aplicando blockchain.

Figura 3-27 Resumen gráfico de la valoración de criterios



Nota: Fuente propia

3.5 Resultado consolidado

En el objetivo número 1 se construyó un proceso de facturación que cumple con las etapas requeridas, por lo tanto, es aplicable a cualquier empresa que se dedica a la facturación de servicios públicos. Así mismo, se construyó un mapa de riesgos general con el cual se identificaron activos, amenazas, vulnerabilidades y diferentes escenarios que pueden conllevar a la materialización de diversos riesgos a nivel financiero. Tanto el proceso de facturación como el mapa de riesgos permiten evidenciar la importancia de crear nuevos controles y la necesidad de cambiar la manera de hacer las cosas, incluso implementando nuevas tecnologías.

Con el objetivo 2 se realizó un plan de tratamiento para el mapa de riesgos construido, plasmando las acciones a ejecutar sobre dicho mapa de riesgos. Igualmente, a través de la encuesta realizada a 4 empresas pertenecientes al sector de los servicios públicos, se identificó que existen muchos riesgos y controles que no están siendo considerados, aunque sean latentes. Así mismo, con la información general construida y la obtenida con la encuesta realizada, fue posible determinar controles para mejores prácticas en el desarrollo completo del proceso de facturación.

En el objetivo número 3 se investigó sobre los diferentes usos que se ha dado a blockchain en varias empresas del sector. Además, se investigaron mejores prácticas que se obtienen al implementar blockchain y cómo pueden aplicarse sobre los riesgos incluidos en el mapa de riesgos previamente construido. Adicionalmente, con toda la información investigada y recopilada en las tres primeras fases del desarrollo del presente documento, se logró proponer una metodología para la adaptación y aplicación de blockchain en el proceso de facturación de una empresa de servicios públicos domiciliarios, la cual consta de 16 etapas.

Para el objetivo número 4 con la investigación realizada a lo largo del presente documento, se comparó el proceso de facturación con su funcionamiento tradicional y utilizando la tecnología blockchain, en términos de funcionalidad, tiempos de respuesta, costos y seguridad de la información, encontrándose que, aunque el proceso funciona actualmente, podría optimizarse y asegurarse hasta en un 90.2% implementando la tecnología mencionada. Es decir, con la metodología propuesta, se puede adoptar e implementar blockchain con la certeza que el proceso mejorará casi en un 100%.

4. Conclusiones y recomendaciones

4.1 Conclusiones

- Con base en los hallazgos encontrados en el objetivo 1: "Identificar las posibles amenazas y vulnerabilidades del proceso de facturación, a partir de la realización de un mapa de riesgos", el cual consistió en construir un proceso de facturación global y un mapa de riesgos en el que se identificaron amenazas, vulnerabilidades, escenarios de riesgo, agentes generadores y se calificó el control; se sustenta la necesidad definida a lo largo del presente proyecto de grado, donde se identificaron los diferentes riesgos existentes en cada etapa que se desarrolla en los procesos de facturación de las empresas de servicios públicos domiciliarios. Riesgos en términos de manualidad en los procesos, independencia para ejecutar modificaciones y ajustes a los datos, vacíos en los contratos con terceros, manualidades que pueden favorecer los fraudes y la fuga de información, segregación de funciones débil, carencia de controles

antimalware; brechas que a posteriori pueden facilitar la pérdida funcional del proceso y el acceso a los atacantes que deliberadamente puedan irrumpir en cualquiera de los principios de la seguridad de la información, afectando la Organización a todo nivel, financiero, legal y reputacional.

- Para dar cumplimiento al objetivo 2 “Caracterizar las diferentes soluciones o controles de seguridad tradicionales del proceso de facturación, para construir uno con las mejores prácticas”, se construyó un plan de tratamiento para los riesgos inadmisibles e inaceptables, se realizó una encuesta sobre aseguramiento del proceso de facturación a distintas empresas del sector de los servicios públicos domiciliarios y se construyeron controles para mejores prácticas. Así las cosas, con el plan de tratamiento diseñado se propendió por cerrar en gran medida diferentes brechas que vuelven vulnerable el proceso de facturación, y se presentaron diferentes formas de tratar los riesgos. Igualmente, con la encuesta realizada, se pudieron identificar riesgos y controles presenten en las empresas, además de evidenciar e identificar aquellos que existen y ni siquiera están incluidos en el mapa. Finalmente, con el mapa de riesgos el plan de tratamiento y la encuesta realizada, se construyeron acciones que se consideran mejores prácticas para aportar al engrosamiento de la seguridad de la información en el proceso de facturación. Con el desarrollo de este objetivo tras conocer lo vulnerable que puede estar el proceso de facturación, se aporta a la optimización de cada etapa que lo compone y a que se tomen medidas que lo protejan de la materialización de los riesgos.

- Para dar cumplimiento al objetivo Nro. 3, “Evaluar diferentes usos que se han dado utilizando blockchain, y recopilar de estas experiencias las mejores prácticas que puedan ser aplicadas en la reducción de riesgos del proceso de facturación, con el fin de proponer una metodología de implementación”, se realizaron búsquedas en fuentes de información confiables, en las cuales se confirmó la versatilidad de blockchain, pues se encontraron varios usos que se le ha dado en diferentes sectores y se evidenció cómo haciendo uso de esta tecnología se mejora la forma de almacenar los datos y se aseguran los procesos. Esta información fue muy valiosa para el presente proyecto de grado, pues también se identificaron prácticas que tiene la tecnología blockchain y que disminuyen o eliminan los riesgos identificados previamente en el proceso de facturación. Así mismo, con base en la literatura, las encuestas y toda la investigación que se realizó, se propuso una metodología que consta de 14 pasos, con los que se considera se puede

llegar a la implementación de dicha tecnología, cómo valor agregado e importante para trascender e innovar en la manera de prestar el servicio de facturación en las Empresas de servicios públicos domiciliarios.

- De acuerdo con los resultados obtenidos para el objetivo 4: "Validar el diseño de la metodología, a través de la comparación entre un modelo tradicional de protección y la tecnología blockchain", se pudo concluir que implementar blockchain en el proceso de facturación es la mejor opción, toda vez que en términos de funcionalidad permite realizar el proceso de facturación correctamente y llega al resultado final: la factura. Igualmente, en términos de tiempos de respuesta, esos se disminuyen debido a que el proceso se realiza automáticamente, por medio de los contratos inteligentes previamente desarrollados. Adicionalmente, también brinda seguridad de la información a cada etapa del proceso, toda vez que ayuda a cerrar brechas, disminuir riesgos, minimizar la manualidad y por ende la probabilidad de ocurrencia de errores humanos, evitar la alteración o hurto de la información porque cada uno de sus bloques está vinculado criptográficamente y solo accede a sumar un bloque al final de la cadena, impide modificar datos registrados en el bloque, la confianza es distribuida, permite realizar seguimientos en línea y verificaciones de integridad.

4.2 Recomendaciones

- Profundizar en el estudio de blockchain en aras de mejorar los procesos, pues dicha tecnología es versátil y permite aplicarse en varios sectores: salud, educativo, financiero, logístico, alimentario, entre otros.

- Continuar la metodología propuesta, llegando a su desarrollo e implementación en una empresa del sector de los servicios públicos domiciliarios.

- Como trabajo futuro se puede plantear una metodología que sugiera la implementación de blockchain en una o varias etapas del proceso de facturación, esto permitiría que se cubran partes específicas y consideradas más sensibles de dicho proceso.

- Con el fin de facilitar el trabajo a los colaboradores de la empresa contratante, generar conciencia sobre la importancia de conocer e incursionar en nuevas tecnologías, nuevas tendencias que están aporten al mayor desarrollo y automatización de los procesos, y al mejoramiento de la calidad de vida.

- En un trabajo futuro donde se llegue a la implementación de blockchain en un proceso de facturación, realizar una comparación real con el proceso ejecutado de forma tradicional, calificando cuantitativamente, según los criterios de funcionalidad, tiempos de respuesta y seguridad de la información. nexos

4.3 Anexos

Anexo A: Escenario del riesgo, agente generador y efecto

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(1)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Bases de datos	Error humano Personal interno Delincuente informático	° Caída del servicio
(2)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Contratistas	Error humano Personal interno Delincuente informático	° Caída del servicio
(3)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Información	Error humano Personal interno Delincuente informático	° Caída del servicio
(4)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Proveedor de impresión	Error humano Personal interno Delincuente informático	° Caída del servicio
(5)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Servidor	Error humano Personal interno Delincuente informático	° Caída del servicio
(6)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Sistema facturador	Error humano Personal interno Delincuente informático	° Caída del servicio

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(7)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Sistema o aplicación de gestión de direcciones	Error humano Personal interno Delincuente informático	° Caída del servicio
(8)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Software de lectura	Error humano Personal interno Delincuente informático	° Caída del servicio
(9)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Clientes	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(10)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Contratistas	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(11)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Empleados	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(12)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Proveedor de impresión	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(13)	Posibilidad que la amenaza: Malware, afecte el activo: Bases de datos	Error humano Personal interno Delincuente informático	° Robo de información ° Pérdida de información ° caída del servicio
(14)	Posibilidad que la amenaza: Malware, afecte el activo: Contratistas	Error humano Personal interno Delincuente informático	° Robo de información ° Pérdida de información ° caída del servicio
(15)	Posibilidad que la amenaza: Malware, afecte el activo: Herramientas ofimáticas	Error humano Personal interno Delincuente informático	° Robo de información ° Pérdida de información ° caída del servicio
(16)	Posibilidad que la amenaza: Malware, afecte el activo: Información	Error humano Personal interno Delincuente informático	° Robo de información ° Pérdida de información ° caída del servicio
(17)	Posibilidad que la amenaza: Malware, afecte el activo: Proveedor de impresión	Error humano Personal interno Delincuente informático	° Robo de información ° Pérdida de información ° caída del servicio
(18)	Posibilidad que la amenaza: Malware, afecte el activo: Servidor	Error humano Personal interno Delincuente informático	° Robo de información ° Pérdida de información ° caída del servicio

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(19)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema facturador	Error humano Personal interno Delincuente informático	° Robo de información ° Pérdida de información ° caída del servicio
(20)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema o aplicación de gestión de direcciones	Error humano Personal interno Delincuente informático	° Robo de información ° Pérdida de información ° caída del servicio
(21)	Posibilidad que la amenaza: Malware, afecte el activo: Software de lectura	Error humano Personal interno Delincuente informático	° Robo de información ° Pérdida de información ° caída del servicio
(22)	Posibilidad que la amenaza: Phishing, afecte el activo: Contratistas	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(23)	Posibilidad que la amenaza: Phishing, afecte el activo: Empleados	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(24)	Posibilidad que la amenaza: Phishing, afecte el activo: Información	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(25)	Posibilidad que la amenaza: Phishing, afecte el activo: Proveedor de impresión	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(26)	Posibilidad que la amenaza: SQL Injection, afecte el activo: Bases de datos	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(27)	Posibilidad que la amenaza: SQL Injection, afecte el activo: Contratistas	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(28)	Posibilidad que la amenaza: SQL Injection, afecte el activo: Proveedor de impresión	Personal interno Delincuente informático	° Incidente de seguridad ° Pérdida de información
(29)	Posibilidad que la amenaza: Ransomware, afecte el activo: Bases de datos	Personal interno Delincuente informático	° Secuestro de información ° Retrasos en el proceso
(30)	Posibilidad que la amenaza: Ransomware, afecte el activo: Contratistas	Personal interno Delincuente informático	° Secuestro de información ° Retrasos en el proceso
(31)	Posibilidad que la amenaza: Ransomware, afecte el activo: Herramientas ofimáticas	Personal interno Delincuente informático	° Secuestro de información ° Retrasos en el proceso
(32)	Posibilidad que la amenaza: Ransomware, afecte el activo: Información	Personal interno Delincuente informático	° Secuestro de información ° Retrasos en el proceso

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(33)	Posibilidad que la amenaza: Ransomware, afecte el activo: Proveedor de impresión	Personal interno Delincuente informático	° Secuestro de información ° Retrasos en el proceso
(34)	Posibilidad que la amenaza: Ransomware, afecte el activo: Servidor	Personal interno Delincuente informático	° Secuestro de información ° Retrasos en el proceso
(35)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema facturador	Personal interno Delincuente informático	° Secuestro de información ° Retrasos en el proceso
(36)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema o aplicación de gestión de direcciones	Personal interno Delincuente informático	° Secuestro de información ° Retrasos en el proceso
(37)	Posibilidad que la amenaza: Ransomware, afecte el activo: Software de lectura	Personal interno Delincuente informático	° Secuestro de información ° Retrasos en el proceso
(38)	Posibilidad que la amenaza: Ausentismo, afecte el activo: Contratistas	Personal contratista	° Retrasos del proceso
(39)	Posibilidad que la amenaza: Ausentismo, afecte el activo: Proveedor de impresión	Personal contratista	° Retrasos del proceso
(40)	Posibilidad que la amenaza: Errores o imprecisiones en la elaboración de los contratos, afecte el activo: Contratistas	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(41)	Posibilidad que la amenaza: Errores o imprecisiones en la elaboración de los contratos, afecte el activo: Empleados	Personal interno	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(42)	Posibilidad que la amenaza: Errores o imprecisiones en la elaboración de los contratos, afecte el activo: Facturas	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(43)	Posibilidad que la amenaza: Errores o imprecisiones en la elaboración de los contratos, afecte el activo: Proveedor de impresión	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(44)	Posibilidad que la amenaza: Fraude, afecte el activo: Bases de datos	Personal interno Personal contratista	° Pérdida de información
(45)	Posibilidad que la amenaza: Fraude, afecte el activo: Clientes	Personal interno Personal contratista	° Pérdida de información

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(46)	Posibilidad que la amenaza: Fraude, afecte el activo: Contratistas	Personal interno Personal contratista	° Pérdida de información
(47)	Posibilidad que la amenaza: Fraude, afecte el activo: Empleados	Personal interno Personal contratista	° Pérdida de información
(48)	Posibilidad que la amenaza: Fraude, afecte el activo: Herramientas ofimáticas	Personal interno Personal contratista	° Pérdida de información
(49)	Posibilidad que la amenaza: Fraude, afecte el activo: Información	Personal interno Personal contratista	° Pérdida de información
(50)	Posibilidad que la amenaza: Fraude, afecte el activo: Proveedor de impresión	Personal interno Personal contratista	° Pérdida de información
(51)	Posibilidad que la amenaza: Fraude, afecte el activo: Servidor	Personal interno Personal contratista	° Pérdida de información
(52)	Posibilidad que la amenaza: Fraude, afecte el activo: Sistema facturador	Personal interno Personal contratista	° Pérdida de información
(53)	Posibilidad que la amenaza: Fraude, afecte el activo: Sistema o aplicación de gestión de direcciones	Personal interno Personal contratista	° Pérdida de información
(54)	Posibilidad que la amenaza: Fraude, afecte el activo: Software de lectura	Personal interno Personal contratista	° Pérdida de información
(55)	Posibilidad que la amenaza: Fraude, afecte el activo: Terminal de lectura	Personal interno Personal contratista	° Pérdida de información
(56)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Bases de datos	Personal interno Personal contratista	° Pérdida de información
(57)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Contratistas	Personal contratista	° Pérdida de información
(58)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Empleados	Personal interno	° Pérdida de información
(59)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Facturas	Personal interno Personal contratista	° Pérdida de información
(60)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Herramientas ofimáticas	Personal interno Personal contratista	° Pérdida de información
(61)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Información	Personal interno Personal contratista	° Pérdida de información

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(62)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Proveedor de impresión	Personal contratista	° Pérdida de información
(63)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Servidor	Personal interno Personal contratista	° Pérdida de información
(64)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Sistema facturador	Personal interno Personal contratista	° Pérdida de información
(65)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Sistema o aplicación de gestión de direcciones	Personal interno Personal contratista	° Pérdida de información
(66)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Software de lectura	Personal interno Personal contratista	° Pérdida de información
(67)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Terminal de lectura	Personal interno Personal contratista	° Pérdida de información
(68)	Posibilidad que la amenaza: Huelga, afecte el activo: Contratistas	Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados
(69)	Posibilidad que la amenaza: Huelga, afecte el activo: Empleados	Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados
(70)	Posibilidad que la amenaza: Huelga, afecte el activo: Proveedor de impresión	Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados
(71)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Bases de datos	Personal interno Personal contratista	° Pérdida de información
(72)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Información	Personal interno Personal contratista	° Pérdida de información
(73)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Servidor	Personal interno Personal contratista	° Pérdida de información
(74)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Sistema facturador	Personal interno Personal contratista	° Pérdida de información

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(75)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Sistema o aplicación de gestión de direcciones	Personal interno Personal contratista	° Pérdida de información
(76)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Software de lectura	Personal interno Personal contratista	° Pérdida de información
(77)	Posibilidad que la amenaza: Inadecuado control de la ejecución afecte el activo: Empleados	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(78)	Posibilidad que la amenaza: Inadecuado control de la ejecución afecte el activo: Herramientas ofimáticas	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(79)	Posibilidad que la amenaza: Inadecuado control de la ejecución afecte el activo: Terminal de lectura	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(80)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Clientes	Personal interno Personal contratista	° Retrasos en los procesos ° Pérdida de información ° Multas
(81)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Contratistas	Personal interno Personal contratista	° Retrasos en los procesos ° Pérdida de información ° Multas
(82)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Empleados	Personal interno Personal contratista	° Retrasos en los procesos ° Pérdida de información ° Multas
(83)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Facturas	Personal interno Personal contratista	° Retrasos en los procesos ° Pérdida de información ° Multas
(84)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Información	Personal interno Personal contratista	° Retrasos en los procesos ° Pérdida de información ° Multas
(85)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Proveedor de impresión	Personal interno Personal contratista	° Retrasos en los procesos ° Pérdida de información ° Multas

No.	Escenario del riesgo	Agente Generador	Efecto o consecuencia
(86)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Sistema facturador	Personal interno Personal contratista	° Retrasos en los procesos ° Pérdida de información ° Multas
(87)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Clientes	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(88)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Contratistas	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(89)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Empleados	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(90)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Proveedor de impresión	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información
(91)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Sistema facturador	Personal interno Personal contratista	° Retrasos en los procesos ° Disminución en la calidad de los resultados deseados ° Pérdida de información

Anexo B: Calificación de probabilidad, impacto y riesgo

Calificación con Controles						
No.	**Escenario de riesgos**	**Probabilidad**		**Impacto Información**		**Riesgo por Impacto de Información**
(1)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Bases de datos	Improbable	2	Superior	5	10
(2)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Contratistas	Improbable	2	Superior	5	10
(3)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Información	Improbable	2	Superior	5	10

Calificación con Controles						
No.	**Escenario de riesgos**	**Probabilidad**		**Impacto Información**		**Riesgo por Impacto de Información**
(4)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Proveedor de impresión	Improbable	2	Superior	5	10
(5)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Servidor	Improbable	2	Superior	5	10
(6)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Sistema facturador	Improbable	2	Superior	5	10
(7)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Sistema o aplicación de gestión de direcciones	Improbable	2	Superior	5	10
(8)	Posibilidad que la amenaza: Denegación de servicio DOS/DDOS, afecte el activo: Software de lectura	Improbable	2	Superior	5	10
(9)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Clientes	Improbable	2	Insignificante	1	2
(10)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Contratistas	Improbable	2	Superior	5	10
(11)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Empleados	Improbable	2	Superior	5	10
(12)	Posibilidad que la amenaza: Ingeniería social, afecte el activo: Proveedor de impresión	Improbable	2	Superior	5	10
(13)	Posibilidad que la amenaza: Malware, afecte el activo: Bases de datos	Posible	3	Superior	5	15
(14)	Posibilidad que la amenaza: Malware, afecte el activo: Contratistas	Posible	3	Superior	5	15
(15)	Posibilidad que la amenaza: Malware, afecte el activo: Herramientas ofimáticas	Posible	3	Superior	5	15
(16)	Posibilidad que la amenaza: Malware, afecte el activo: Información	Posible	3	Superior	5	15
(17)	Posibilidad que la amenaza: Malware, afecte el activo: Proveedor de impresión	Posible	3	Superior	5	15
(18)	Posibilidad que la amenaza: Malware, afecte el activo: Servidor	Posible	3	Superior	5	15
(19)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema facturador	Posible	3	Superior	5	15
(20)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema o aplicación de gestión de direcciones	Posible	3	Superior	5	15
(21)	Posibilidad que la amenaza: Malware, afecte el activo: Software de lectura	Posible	3	Superior	5	15

Calificación con Controles						
No.	**Escenario de riesgos**	**Probabilidad**		**Impacto Información**		**Riesgo por Impacto de Información**
(22)	Posibilidad que la amenaza: Phishing, afecte el activo: Contratistas	Posible	3	Superior	5	15
(23)	Posibilidad que la amenaza: Phishing, afecte el activo: Empleados	Posible	3	Superior	5	15
(24)	Posibilidad que la amenaza: Phishing, afecte el activo: Información	Posible	3	Superior	5	15
(25)	Posibilidad que la amenaza: Phishing, afecte el activo: Proveedor de impresión	Posible	3	Superior	5	15
(26)	Posibilidad que la amenaza: SQL Injection, afecte el activo: Bases de datos	Posible	3	Superior	5	15
(27)	Posibilidad que la amenaza: SQL Injection, afecte el activo: Contratistas	Posible	3	Mayor	4	12
(28)	Posibilidad que la amenaza: SQL Injection, afecte el activo: Proveedor de impresión	Posible	3	Superior	5	15
(29)	Posibilidad que la amenaza: Ransomware, afecte el activo: Bases de datos	Posible	3	Superior	5	15
(30)	Posibilidad que la amenaza: Ransomware, afecte el activo: Contratistas	Posible	3	Superior	5	15
(31)	Posibilidad que la amenaza: Ransomware, afecte el activo: Herramientas ofimáticas	Posible	3	Intermedio	3	9
(32)	Posibilidad que la amenaza: Ransomware, afecte el activo: Información	Posible	3	Superior	5	15
(33)	Posibilidad que la amenaza: Ransomware, afecte el activo: Proveedor de impresión	Posible	3	Menor	2	6
(34)	Posibilidad que la amenaza: Ransomware, afecte el activo: Servidor	Posible	3	Superior	5	15
(35)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema facturador	Posible	3	Superior	5	15
(36)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema o aplicación de gestión de direcciones	Posible	3	Superior	5	15
(37)	Posibilidad que la amenaza: Ransomware, afecte el activo: Software de lectura	Posible	3	Superior	5	15
(38)	Posibilidad que la amenaza: Ausentismo, afecte el activo: Contratistas	Posible	3	Intermedio	3	9
(39)	Posibilidad que la amenaza: Ausentismo, afecte el activo: Proveedor de impresión	Posible	3	Menor	2	6
(40)	Posibilidad que la amenaza: Errores o imprecisiones en la elaboración de los contratos, afecte el activo: Contratistas	Posible	3	Superior	5	15
(41)	Posibilidad que la amenaza: Errores o imprecisiones en la elaboración de los contratos, afecte el activo: Empleados	Posible	3	Superior	5	15

Calificación con Controles						
No.	**Escenario de riesgos**	**Probabilidad**		**Impacto Información**		**Riesgo por Impacto de Información**
(42)	Posibilidad que la amenaza: Errores o imprecisiones en la elaboración de los contratos, afecte el activo: Facturas	Posible	3	Superior	5	15
(43)	Posibilidad que la amenaza: Errores o imprecisiones en la elaboración de los contratos, afecte el activo: Proveedor de impresión	Posible	3	Superior	5	15
(44)	Posibilidad que la amenaza: Fraude, afecte el activo: Bases de datos	Posible	3	Superior	5	15
(45)	Posibilidad que la amenaza: Fraude, afecte el activo: Clientes	Posible	3	Superior	5	15
(46)	Posibilidad que la amenaza: Fraude, afecte el activo: Contratistas	Posible	3	Superior	5	15
(47)	Posibilidad que la amenaza: Fraude, afecte el activo: Empleados	Posible	3	Superior	5	15
(48)	Posibilidad que la amenaza: Fraude, afecte el activo: Herramientas ofimáticas	Posible	3	Superior	5	15
(49)	Posibilidad que la amenaza: Fraude, afecte el activo: Información	Posible	3	Superior	5	15
(50)	Posibilidad que la amenaza: Fraude, afecte el activo: Proveedor de impresión	Posible	3	Superior	5	15
(51)	Posibilidad que la amenaza: Fraude, afecte el activo: Servidor	Posible	3	Superior	5	15
(52)	Posibilidad que la amenaza: Fraude, afecte el activo: Sistema facturador	Posible	3	Superior	5	15
(53)	Posibilidad que la amenaza: Fraude, afecte el activo: Sistema o aplicación de gestión de direcciones	Posible	3	Superior	5	15
(54)	Posibilidad que la amenaza: Fraude, afecte el activo: Software de lectura	Posible	3	Superior	5	15
(55)	Posibilidad que la amenaza: Fraude, afecte el activo: Terminal de lectura	Posible	3	Superior	5	15
(56)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Bases de datos	Posible	3	Superior	5	15
(57)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Contratistas	Posible	3	Superior	5	15
(58)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Empleados	Posible	3	Superior	5	15
(59)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Facturas	Posible	3	Superior	5	15
(60)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Herramientas ofimáticas	Posible	3	Intermedio	3	9

Calificación con Controles						
No.	**Escenario de riesgos**	**Probabilidad**		**Impacto Información**		**Riesgo por Impacto de Información**
(61)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Información	Posible	3	Superior	5	15
(62)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Proveedor de impresión	Posible	3	Superior	5	15
(63)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Servidor	Posible	3	Superior	5	15
(64)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Sistema facturador	Posible	3	Superior	5	15
(65)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Sistema o aplicación de gestión de direcciones	Posible	3	Superior	5	15
(66)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Software de lectura	Posible	3	Superior	5	15
(67)	Posibilidad que la amenaza: Fuga de información, afecte el activo: Terminal de lectura	Posible	3	Superior	5	15
(68)	Posibilidad que la amenaza: Huelga, afecte el activo: Contratistas	Posible	3	Mayor	4	12
(69)	Posibilidad que la amenaza: Huelga, afecte el activo: Empleados	Improbable	2	Mayor	4	8
(70)	Posibilidad que la amenaza: Huelga, afecte el activo: Proveedor de impresión	Posible	3	Mayor	4	12
(71)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Bases de datos	Posible	3	Mayor	4	12
(72)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Información	Posible	3	Superior	5	15
(73)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Servidor	Posible	3	Mayor	4	12
(74)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Sistema facturador	Posible	3	Mayor	4	12
(75)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Sistema o aplicación de gestión de direcciones	Posible	3	Intermedio	3	9

Calificación con Controles						
No.	**Escenario de riesgos**	**Probabilidad**		**Impacto Información**		**Riesgo por Impacto de Información**
(76)	Posibilidad que la amenaza: Inadecuada segregación de funciones afecte el activo: Software de lectura	Posible	3	Intermedio	3	9
(77)	Posibilidad que la amenaza: Inadecuado control de la ejecución afecte el activo: Empleados	Improbable	2	Mayor	4	8
(78)	Posibilidad que la amenaza: Inadecuado control de la ejecución afecte el activo: Herramientas ofimáticas	Improbable	2	Mayor	4	8
(79)	Posibilidad que la amenaza: Inadecuado control de la ejecución afecte el activo: Terminal de lectura	Improbable	2	Superior	5	10
(80)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Clientes	Improbable	2	Superior	5	10
(81)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Contratistas	Improbable	2	Mayor	4	8
(82)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Empleados	Improbable	2	Mayor	4	8
(83)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Facturas	Improbable	2	Superior	5	10
(84)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Información	Improbable	2	Superior	5	10
(85)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Proveedor de impresión	Improbable	2	Mayor	4	8
(86)	Posibilidad que la amenaza: Incumplimiento de normas, leyes y requisitos, afecte el activo: Sistema facturador	Improbable	2	Superior	5	10
(87)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Clientes	Improbable	2	Mayor	4	8
(88)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Contratistas	Improbable	2	Mayor	4	8
(89)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Empleados	Improbable	2	Mayor	4	8

Calificación con Controles						
No.	**Escenario de riesgos**	**Probabilidad**		**Impacto Información**		**Riesgo por Impacto de Información**
(90)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Proveedor de impresión	Improbable	2	Mayor	4	8
(91)	Posibilidad que la amenaza: Selección de contratistas o personal no idóneo, afecte el activo: Sistema facturador	Improbable	2	Mayor	4	8

Anexo C: Plan de tratamiento

PLAN DE TRATAMIENTO.xlsx

Anexo D: Resultado de la encuesta

ENCUESTA SOBRE EL ASEGURAMIENTC

Bibliografía

[1] N. J. R. Elias, V. P. Pumarejo, S. F. J. Jattin, and T. D. Vivas, “Ley de servicios públicos Ley 142 de julio 11 de 1994,” 1994, [Online]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0142_1994.html.

[2] Empresas Públicas de Medellín E.S.P., “Estadísticas de atención,” 2020. https://www.epm.com.co/site/clientes_usuarios/clientes-y-usuarios/estadisticas-de-atencion#undefined.

[3] EPM, “Estadísticas de atención,” 2022, [Online]. Available: https://cu.epm.com.co/clientesyusuarios/servicio-al-cliente/estadisticas-de-atencion#ndice-de-reclamos-129.

[4] G. N. Avendaño *et al.*, “Portafolio de Servicios,” 2019, [Online]. Available: https://www.superservicios.gov.co/.

[5] I. Operacionales *et al.*, “Evaluacion de la gestión año 2021 servicio de energía eléctrica,” pp. 1–13, 2021.

[6] I. De, C. E. Nafta, and C. Llc, “Blockchain para una cadena colaborativa,” pp. 2–5, 2019.

[7] M. L. Ceballos A, García F, “Tendencias cibercrimen Colombia 2019-2020,” p. 36, 2020, [Online]. Available: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf.

[8] Centro Cibernetico Policia Nacional, “Balance Cibercrimen 2020,” pp. 2020–2021, 2020.

[9] Semtec, “SEMTEC S.A.S Servicios Empresariales y técnicos S.A.S,” 2019, [Online]. Available: https://semtec.com.co/productos-y-servicios/comercializacion/procesos-de-facturacion/.

[10] Empresas Públicas de Medellín E.S.P., “PQR-7746683-L7N5 Anexo (1 Folio) - Proceso de Facturación.,” 2020.

[11] C. S. C. Calderon, C. G. N. Delgado, M. J. E. Sarmiento, T. J. P. Cuenca, and P. B. Lozada, *Cartilla sober facturación electrónica: aplicación de la facturación electrónica en Colombia*. Bogotá - Colombia: Universidad Manuela Beltrán, 2018.

[12] Función pública Colombia, “Decreto 358 de 2000,” pp. 1–20, 2020, [Online]. Available: http://www.mincultura.gov.co/areas/cinematografia/noticias/Paginas/2006-04-04_6458.aspx.

[13] INCIBE, “Seguridad de la Información,” [Online]. Available: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/seguridad-informacion-1.

[14] Y. J. R. Altamirano and S. Bayona Oré, “Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento,” *RISTI - Rev. Iber. Sist. e Tecnol. Inf.*, vol. 2017, no. 25, pp. 112–134, 2017, doi: 10.17013/risti.25.112-134.

[15] Instituto Nacional de Ciberseguridad, “Glosario de Términos de Ciberseguridad,” *Una guia aproximación para el Empres.*, pp. 1–41, 2017.

[16] INCIBE, “¿Sabes qué es el Día Internacional de la Seguridad de la Información?,” *28-11-2019*, 2019, [Online]. Available: https://www.incibe.es/protege-tu-empresa/blog/sabes-el-dia-internacional-seguridad-informacion.

[17] Mintic, V. digital Colombia, and T. por un nuevo País, “Guía de gestión de riesgos Seguridad y privacidad de la información,” *Mintic*, no. 7, p. 39, 2016, [Online]. Available: http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.

[18] N. Técnica, “Norma Técnica Ntc-Iso/Iec Colombiana 27001,” 2006, [Online]. Available: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma. NTC-ISO-IEC 27001.pdf.

[19] C. de la R. Colombia, “Ley 1581 de Octubre de 2012,” pp. 1–15, 2012.

[20] L. ámbito Jurídico, “Normas sobre tratamiento de datos personales aplican a los prestadores de servicios públicos domiciliarios,” 2021.

[21] S. de I. y Comercio, “Más de 24 mil empresas no tienen mecanismos eficientes para proteger los datos de sus usuarios de accesos no autorizados,” 2021, [Online]. Available: https://www.sic.gov.co/slider/más-de-24-mil-empresas-no-tienen-mecanismos-eficientes-para-proteger-los-datos-de-sus-usuarios-de-accesos-no-autorizados.

[22] E. Piscini, D. Dalton, and L. Kehoe, “Blockchain & Ciberseguridad,” pp. 1–16, 2018.

[23] S. de I. y Comercio, “Empresas sancionadas por incumplimiento a protección de datos personales,” 2018, [Online]. Available: https://www.itechsas.com/blog/proteccion-de-datos/empresas-sancionadas-por-incumplimiento-a-ley-1581/.

[24] J. M. Ramos Saky, *Introducción a la seguridad*. 2006.

[25] B. J. F. Roa, *Seguridad informática - Ciclo formativo grado medio*. 2015.

[26] NIST, “Base de datos nacional de vulnerabilidad,” [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss.

[27] barrio N. C. Linares, “Los ciberataques en el derecho internacional público,” 2019.

[28] C. F. J. Urueña, “Ciberataques, la mayor amenaza actual,” *Inst. Español Estud. Estratégicos*,

pp. 8–45, 2014, [Online]. Available: https://aurelioherrero.blogs.upv.es/files/2015/02/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf%0Ahttp://www.ieee.es/publicaciones-new/documentos-de-opinion/2015/DIEEEO09-2015.html.

[29] INCIBE, “Las 7 fases de un ciberataque. ¿Las conoces?,” 2020, [Online]. Available: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces.

[30] CISCO, “¿Cuáles son los ciberataques más comunes?,” 2022, [Online]. Available: https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html.

[31] C. colombiana de informátca y Telecomunicaciones, “Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno,” 2022, [Online]. Available: https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/.

[32] Ministerio de tecnologías de la información y las telecomunicaciones, “Ministerio TIC capacitará a empresas en protección de ataques informáticos,” 2021, [Online]. Available: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/175743:Ministerio-TIC-capacitara-a-empresas-en-proteccion-de-ataques-informaticos.

[33] S. H. Alsamhi, B. Lee, and Y. Qiao, “Blockchain for Multi-Robot Collaboration to Combat COVID-19 and Future Pandemics,” *IEEE Access*, vol. XX, pp. 1–1, 2020, doi: 10.1109/access.2020.3032450.

[34] A. Fitwi, Y. Chen, and S. Zhu, “A lightweight blockchain-based privacy protection for smart surveillance at the edge,” *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 552–555, 2019, doi: 10.1109/Blockchain.2019.00080.

[35] IBM, “¿Qué es la tecnología blockchain?”

[36] IBM, “¿Qué es blockchain y cómo funciona?,” 2022, [Online]. Available: https://www.ibm.com/blogs/systems/mx-es/2017/03/que-es-blockchain-y-como-funciona/.

[37] J. A. Corredor Higuera and D. Días Guzmán, *Blockchain y mercados financieros: aspectos generales del impacto regulatorio de la aplicación de la tecnología blockchain en los mercados de crédito de América Latina*, vol. 81. 2018.

[38] J. G. Arévalo Ascanio, R. A. Bayona Trillos, and D. W. Rico Bautista, “Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información,” *Rev. Tecnura*, vol. 19, no. 46, p. 123, 2015, doi:

10.14483/udistrital.jour.tecnura.2015.4.a10.

[39] M. Mural and H. Ford, “Consumidor inteligente / ¿ Cómo funciona el blockchain ?,” pp. 3–5, 2017.

[40] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou, and B. Zhang, “A High Performance Blockchain Platform for Intelligent Devices,” *Proc. 2018 1st IEEE Int. Conf. Hot Information-Centric Networking, HotICN 2018*, no. HotICN, pp. 260–261, 2019, doi: 10.1109/HOTICN.2018.8606017.

[41] O. Code, “Estructura de Datos Blockchain,” 2017, [Online]. Available: https://othercode.es/blog/estructura-de-datos-blockchain.

[42] IBM, “Beneficios de blockchain,” [Online]. Available: https://www.ibm.com/es-es/topics/benefits-of-blockchain.

[43] IBM, “¿Qué son los contratos inteligentes en blockchain?,” [Online]. Available: https://www.ibm.com/es-es/topics/smart-contracts.

[44] IBM, “¿Qué es la seguridad blockchain?,” 2021, [Online]. Available: https://www.ibm.com/topics/blockchain-security.

[45] Q. He, N. Guan, M. Lv, and W. Yi, “On the Consensus Mechanisms of Blockchain/DLT for Internet of Things,” *2018 IEEE 13th Int. Symp. Ind. Embed. Syst. SIES 2018 - Proc.*, 2018, doi: 10.1109/SIES.2018.8442076.

[46] X. Liu, R. Chen, Y. W. Chen, and S. M. Yuan, “Off-chain Data Fetching Architecture for Ethereum Smart Contract,” *Int. Conf. Cloud Comput. Big Data Blockchain, ICCBB 2018*, 2018, doi: 10.1109/ICCBB.2018.8756348.

[47] E. Androulaki, A. De Caro, M. Neugschwandtner, and A. Sorniotti, “Endorsement in hyperledger fabric,” *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 510–519, 2019, doi: 10.1109/Blockchain.2019.00077.

[48] K. M. Hlaing and D. E. Nyaung, “Electricity Billing System using Ethereum and Firebase,” *2019 Int. Conf. Adv. Inf. Technol. ICAIT 2019*, pp. 217–221, 2019, doi: 10.1109/AITC.2019.8920931.

[49] Q. Wang, L. Huang, S. Chen, and Y. Xiang, “Blockchain Enables Your Bill Safer,” *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2020, doi: 10.1109/jiot.2020.3016721.

[50] Empresas Públicas de Medellín E.S.P., “Condiciones uniformes para la prestación del servicio público domiciliario de energía eléctrica,” p. 55, 2014, [Online]. Available: http://www.epm.com.co/site/Portals/0/centro_de_documentos/normatividad_y_legislaci

on/energia/CCU Energía Eléctrica Modificado 11 de Diciembre 2014.pdf.

[51] O. Van Cutsem, D. Ho Dac, P. Boudou, and M. Kayal, “Cooperative energy management of a community of smart-buildings: A Blockchain approach,” *Int. J. Electr. Power Energy Syst.*, vol. 117, no. November 2019, p. 105643, 2020, doi: 10.1016/j.ijepes.2019.105643.

[52] G. de D. América, “Colombia estrena ‘blockchain’ para aparatos médicos: La Clínica Las Américas de Medellín dio el primer paso,” pp. 1–2, 2020, [Online]. Available: ento: https://search.proquest.com/docview/2412119884?accountid=30687.

[53] X. Wang, “Research on Payment Settlement Mode in Cross-Border Business Trade Based on Blockchain Technology,” *SAIEE Africa Res. J.*, vol. 113, no. 3, pp. 129–132, 2022, doi: 10.23919/SAIEE.2022.9853022.

[54] W. Kluwer, “RSM incrementa su facturación global un 6,9% y alcanza los 5.740 millones de dólares,” pp. 7–8, 2020.

[55] Portafolio, “IBM lanza el Centro Cognitivo de Transformación en Bogotá,” pp. 1–2, 2020.

[56] P. González, C. Armas, H. Torres, S. Martínez, Á. Caisapanta, and F. Larrea, “Manual del subproceos de facturación,” pp. 0–7, 2015, [Online]. Available: https://www.inmobiliar.gob.ec/wp-content/uploads/2015/09/MANUAL-DEL-SUBPROCESO-DE-FACTURACIÓN.pdf.

[57] I. González-Puetate, C. Marín-Tello, and H. Reyes Pineda, “Agri-food safety optimized by blockchain technology: review Seguridad agroalimentaria optimizada por medio de la tecnología blockchain: revisión,” *Rev. Fac. Nac. Agron. Medellín*, vol. 75, no. 1, pp. 9839–9851, 2022, [Online]. Available: https://revistas.unal.edu.co/index.php/refame.

[58] N. Técnica, “Norma Técnica Colombiana 27005 Ntc-Iso / Iec,” no. 571, 2009.

[59] Incibe, “Inventario de activos,” [Online]. Available: https://bit.ly/3BuJCAx.

[60] E. europea de Excelencia, “Listado de amenezas y vulnerabilidades en ISO 27001,” *2020*, [Online]. Available: https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/.

[61] P. B. F. Inc, “PROVENANCE BLOCKCHAIN,” 2022, [Online]. Available: https://www.provenance.io/.

[62] IBM, “Segmentos de mercado de IBM Food Trust,” [Online]. Available: https://www.ibm.com/blockchain/solutions/food-trust/market-segments.

[63] Unergy, “Haz parte de proyectos de energía solar y obtén la mejor rentabilidad,” [Online]. Available: https://unergy.io/inversion-energia-solar.

[64] 101 Blockchains, “20 Empresas Que Están Implementando La Tecnología Blockchain,” 2022, [Online]. Available: https://101blockchains.com/es/empresas-implementando-blockchain/.

[65] WeliveSecurity by eset, “Blockchain: qué es y cómo funciona esta tecnología,” 2018, [Online]. Available: https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/#Ataques-a-la-blockchain.

[66] J. A. G. L. y D. A. A. Rivera, “La Ingeniería de requisitos en metodologías ágiles,” vol. 7, no. 2, pp. 57–77, 2012.