UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE SISTEMAS DE INFORMACIÓN

PROPUESTA DE UN PLAN DE IMPLEMENTACIÓN PARA EL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LA EMPRESA CABLETEL.

TRABAJO DE TITULACIÓN O PROYECTO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN.

AUTOR: JOHN BYRON YUNGANAULA YUNGANAULA

DIRECTOR: ING. CESAR ALVARITO CORONEL GONZÁLEZ

AZOGUES - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca	DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD	CÓDIGO: F – DB – 34 VERSION: 01 FECHA: 2021-04-15 Página 1 de 1

Declaratoria de Autoría y Responsabilidad

John Byron Yunganaula Yunganaula portador(a) de la cédula de ciudadanía Nº **0302677729**. Declaro ser el autor de la obra: "**PROPUESTA DE UN PLAN DE IMPLEMENTACIÓN PARA EL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LA EMPRESA CABLETEL"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Azogues, **04 de enero de 2024**

F.....

John Byron Yunganaula Yunganaula

C.I. 0302677729

CERTIFICACIÓN DEL DIRECTOR DE TESIS

César Alvarito Coronel González

DOCENTE DE LA CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

De mi consideración:

Certifico que el presente trabajo de titulación denominado: **"Propuesta de un plan de implementación para el cumplimiento de la Ley Orgánica de Protección de Datos Personales en la empresa Cabletel"**, realizado por: **John Byon Yunganaula Yunganaula**, con documentos de identidad: **0302677729,** previo a la obtención del título de **Ingeniero en Sistemas de Información** ha sido asesorado, orientado, revisado y supervisado durante su ejecución, bajo mi tutoría en todo el proceso, por lo que certifico que el presente documento, fue desarrollado siguiendo los parámetros del método científico, se sujeta a las normas éticas de investigación que exige la Universidad Católica de Cuenca, por lo que está expedito para su presentación y sustentación ante el respectivo tribunal.

Azogues, 22 de enero de 2024

César Alvarito Coronel González

C.I. 0301141206

DIRECTOR

AGRADECIMIENTO

Quiero comenzar expresando mi profundo agradecimiento a mi madre, Mami Nati, quien ha sido y continúa siendo el pilar fundamental de mi vida. Su apoyo inquebrantable, sus enseñanzas y los sólidos valores que me ha inculcado han sido la luz que ha guiado cada paso de mi trayectoria. Agradezco de corazón su presencia constante y su amor incondicional.

También extiendo mi gratitud a mis padres por brindarme la valiosa oportunidad de continuar en el camino del estudio. Su sacrificio y respaldo han sido motores clave en mi travesía académica. A cada uno de mis demás familiares, quienes han estado presentes en cada faceta de mi vida, tanto académica como personal les expreso mi sincero agradecimiento. Sus palabras de ánimo, gestos de cariño y respaldo han significado mucho para mí.

De igual forma, quiero expresar mi profundo agradecimiento a mis compañeros de clase, quienes a lo largo de este periodo académico se han convertido en verdaderos amigos. Su inquebrantable compañerismo, las risas compartidas y los momentos gratos que hemos experimentado juntos han enriquecido mi experiencia educativa. Quiero destacar especialmente a Gabriela y Santiago, quienes han demostrado un apoyo continuo hacia mí. Sus palabras alentadoras, su apoyo constante y lo más valioso su amistad, han sido fundamentales. Podríamos decir que durante este tiempo hemos sido los tres mosqueteros, comprometidos con el lema “Uno para todos y todos para uno”.

Que Dios, en su infinita bondad, les retribuya por todo el amor y el apoyo que me han brindado. Gracias a cada uno por ser parte fundamental de mi camino y por contribuir a mi crecimiento y bienestar.

DEDICATORIA

Este trabajo de titulación es un triunfo sincero a mis padres, quienes me guiaron con sabiduría y me enseñaron desde temprana edad a que el estudio, el esfuerzo y la dedicación son las columnas fundamentales para alcanzar cualquier meta. A ellos, agradezco la paciencia y el incondicional respaldo que siempre me brindaron.

Asimismo, quiero dedicar este proyecto a toda mi familia. Su apoyo constante fue mi motor durante este arduo proceso. Sin su aliento, comprensión y cariño no habría culminado esta etapa de mi vida. Este logro es también de ellos, quienes compartieron cada desafío y triunfo en este viaje académico.

PROPUESTA DE UN PLAN DE IMPLEMENTACIÓN PARA EL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LA EMPRESA CABLETEL

John Byron Yunganaula Yunganaula – Ing. César Alvarito Coronel González

Universidad Católica de Cuenca – john.yunganaula.29@est.ucacue.edu.ec

RESUMEN

Es fundamental que Cabletel se alinee a la nueva ley sobre protección de datos personales, debido a que desde el año 2023 se obliga a todas las empresas que manejan datos de usuarios a regirse a esta regulación. Por ende, este trabajo se centra en la evaluación de los niveles de seguridad de Cabletel en relación con la protección de información personal. El trabajo responde la pregunta; ¿Cómo fortalecer la seguridad de la información en Cabletel y asegurar su cumplimiento con los requisitos legales establecidos por la normativa vigente? A través del análisis de la LOPDP y la norma ISO 27002, identificación e implementación de los objetivos de control por parte de la empresa y elaboración de recomendaciones para fortalecer los procesos de seguridad.

La metodología se basó en el enfoque cualitativo, descriptivo y se empleó el modelo de madurez CMMI. Se hizo una revisión de la literatura relacionada con la LOPDP y la norma ISO 27002. Además, se aplicó encuestas al responsable del departamento de TIC's para evaluar la integración de los objetivos de control. Los resultados indican que Cabletel cumple con un 79% en relación con los controles específicos identificados en la norma ISO 27002; a su vez, guardan relación con los requisitos establecidos por la LOPDP. También se determinó el nivel de madurez de cada control identificado, dando un 72% de estabilidad y consistencia. Con base a estos resultados, se sugirieron recomendaciones para garantizar el acatamiento de dichos requerimientos y evitar las sanciones establecidas por la ley.

*Palabra clave***:** Protección de datos personales, Cumplimiento, Normativa, Sanciones, Norma ISO/IEC 27002:2013

PROPOSAL OF AN IMPLEMENTATION PLAN FOR COMPLIANCE WITH THE ORGANIC LAW FOR THE PROTECTION OF PERSONAL DATA AT CABLETEL COMPANY

John Byron Yunganaula Yunganaula - Cesar Alvarito Coronel Gonzalez. Eng.

Catholic University of Cuenca - john.yunganaula.29@est.ucacue.edu.ec

ABSTRACT

Cabletel must be aligned with the new law on personal data protection because, since 2023, all companies that handle user data are obliged to comply with this regulation. Therefore, this work focuses on evaluating Cabletel's security levels concerning protecting personal information. The study answers the question: How can Cabletel strengthen its information security and ensure compliance with the legal requirements established by the current regulations? Through the analysis of the LOPDP and ISO 27002, plan to identify and implement control objectives by the company and development of recommendations to strengthen security processes.

The methodology was based on the qualitative, descriptive approach, and the Capability Maturity Model Integration (CMMI) model was used. A literature review related to the LOPDP and ISO 27002 was conducted. In addition, surveys were applied to the person in charge of the ICT department to evaluate the integration of the control objectives. The results indicate that Cabletel complies with 79% of the specific controls identified in ISO 27002; in turn, they are linked to the requirements established by the LOPDP. The maturity level of each identified control was also determined, representing 72% of stability and consistency. Based on these results, recommendations were suggested to ensure compliance with these requirements and avoid the sanctions established by law.

Keyword: Personal data protection, Compliance, Regulations, Sanctions, ISO/IEC 27002:2013 Standard

INDICE DE CONTENIDO

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

INTRODUCCION

INTERNACIONALES

El trabajo de Manuel y Franklyn titulada “Aplicación de la Norma internacional ISO/IEC 27002:2013 para la Seguridad informática de la Unidad de Gestión Educativa Local ‘Utcubamba’, 2022” tiene como objetivo mejorar la seguridad informática mediante la aplicación de la norma ISO/IEC 27002:2013. Utilizaron una metodología de investigación aplicada y de diseño preexperimental, y se aplicó un cuestionario a una muestra de 18 empleados que laboran en la institución. Se desarrolló una solución tecnológica propuesta basada en la norma ISO/IEC 27002:2013. Los resultados mostraron que se logró mejorar la seguridad informática de la entidad en estudio, específicamente en el grado de confidencialidad, integridad y disponibilidad de la información. La aplicación de la solución propuesta permitió una mayor concienciación sobre la seguridad de la información, un mayor control de activos e información sensible, y una adecuada implementación de políticas de control. En general, la aplicación de la norma ISO/IEC 27002:2013 demostró ser efectiva en la mejora de la seguridad informática de la Unidad de Gestión Educativa Local ‘Utcubamba’ [1].

NACIONALES

La autora Diana Murillo en su tesis titulada “POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN NORMAS ISO 27002 PARA EL DEPARTAMENTO INFORMÁTICO DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ” con el propósito de desarrollar políticas de seguridad de la información basado en la norma ISO 27002 para el departamento informático de la Universidad Estatal del Sur de Manabí, asegurando la integridad, fidelidad y la confidencialidad de la información que resguarda esta institución. Para cumplir con este objetivo utilizo una metodología analítico – descriptivo, de igual manera el uso de técnicas de observación y entrevistas que ayudaron a la recolección de datos y con ello

el desarrollo de la propuesta de las políticas de seguridad de la información para el fortalecimiento de la seguridad [2].

La evolución del ser humano ha estado estrechamente vinculada al avance de la tecnología, siendo esta no solo un reflejo, sino también un impulsor fundamental del crecimiento humano. De acuerdo con las Naciones Unidas “Las tecnologías pueden ayudar a que nuestro mundo sea más justo, más pacífico y más equitativo. Los avances digitales pueden apoyar y acelerar el logro de cada uno de los 17 Objetivos de Desarrollo Sostenible, desde el fin de la pobreza extrema hasta la reducción de la mortalidad materna e infantil, la promoción de la agricultura sostenible y el trabajo decente, y el logro de la alfabetización universal. Sin embargo, las tecnologías también pueden amenazar la privacidad, comprometer la seguridad y alimentar la desigualdad” [3].

Es así que con el progreso de la tecnología se ha tenido grandes cantidades de productos o servicios para ofrecer a las personas, como las redes sociales, acceso a internet, entre otros [4], además, para poder acceder a estos servicios que ofrecen varias empresas es necesario facilitar un poco de nuestra información personal, a partir de esto se establece una conexión entre el cliente y la empresa. De acuerdo con Garzón y Olmos “la aparición del Internet y su uso globalizado a nivel personal y en el entorno empresarial el cual nos permite “estar conectados”, sin embargo, al mismo tiempo estos avances tecnológicos también se transforman en una amenaza toda vez que trae consigo la aparición de nuevas vulnerabilidades y riesgos de seguridad dado la fácil accesibilidad y exposición de información vital o sensible para la Compañías (por ejemplo, los datos personales) gracias a esa conectividad” [5].

En base a lo antes mencionado, la seguridad de la información se ha transformado en un aspecto crítico para las empresas que manejan datos de sus clientes, como es el caso de la Empresa Cabletel, que analizaremos en el presente trabajo, que se enfrenta a desafíos para

garantizar la integridad de la información y su confidencialidad; por lo tanto, es necesario gestionar de manera efectiva la seguridad de la información. En este contexto, la Ley Orgánica de Protección de Datos Personales se centra en esa privacidad, seguridad y protección de los datos, por lo que establece los principios y requisitos que deben seguir las empresas. Sin embargo, para poder dar cumplimiento con lo que expone la ley, se requiere de un enfoque claro en el análisis de políticas, derechos, obligaciones y medidas de seguridad para las empresas.

En este documento, se investigará la situación actual de la empresa Cabletel en relación con la Ley Orgánica de Protección de Datos Personales. Para contextualizar adecuadamente este estudio, se procederá, en primer lugar, a abordar el marco teórico con el tema de la empresa Cabletel. Este enfoque comprenderá un análisis detallado de aspectos como su historia, organigrama, misión, visión y ubicación. La intención es proporciona al lector una comprensión integral de la entidad en cuestión. A continuación, se revisará la documentación de la ley en cuestión, analizando la estructura, principios, requisitos, integrantes que lo conforman, alcance, sus respectivas sanciones; además se destacará el valor de tener una ley para la protección de datos. Posteriormente, se analizará la norma ISO/IEC 27002:2013 y se describirán los beneficios de su uso, sus dominios y se responderá el porqué de su aplicación en este trabajo.

Los apartados del capítulo II exploran las interrelaciones entre la ley actual de protección de datos personales y otras normativas, que permitirán evaluar tanto en cumplimiento de la ley como en la gestión de la seguridad de la información. Finalmente se harán recomendaciones, basadas en los resultados de las evaluaciones.

CAPITULO I

MARCO REFERENCIAL

1.1 PLANTEAMIENTO DEL PROBLEMA

Actualmente, la recopilación de datos se efectúa mediante canales digitales, tales como internet, redes sociales, y al utilizar servicios o adquirir productos. Un ejemplo de este contexto lo constituyen las encuestas en línea, donde los participantes al comprometerse en este proceso brindan información demográficos y opiniones. Todo esto supone alto riesgo en la integridad y privacidad del dueño de los datos personales. Entre los riesgos inherentes a este proceso se encuentran la posibilidad de acceso no autorizado, la vulnerabilidad a brechas de seguridad, la exposición a actividades de ciberdelincuencia, además de violentar los derechos ciudadanos. Por lo tanto, resulta preciso enfocar la recolección, análisis, uso y procesamiento de datos personales que hacen las empresas con el fin de proteger el derecho a la protección de datos [6].

También se debe de tomar en cuenta el inadecuado manejo de los datos personales por parte de las empresas, ya que pueden exponer a sus clientes a varios riesgos como el robo de identidad, la divulgación de su información, la confidencialidad y el mal uso de sus datos por parte de terceras personas.

Particularmente, en la empresa Cabletel desde sus inicios, se ha venido recabando información de todos sus clientes; por lo tanto, es imperativo resguardarla de cualquier vulnerabilidad. En este contexto, es responsabilidad implementar con anticipación medidas apropiadas para garantizar la protección de los datos personales de sus clientes o usuarios, estas acciones deberían estar fundamentadas en normativas preexistentes a la Ley Orgánica de Protección de Datos Personales [7]. Actualmente es la ley vigente para el manejo y tratamiento

de los datos personales en Ecuador; además, de establecer otros requisitos u obligaciones de cumplimiento para las empresas que tienen y manejan la información de sus clientes.

La presente investigación consiste en determinar si la empresa ha realizado un levantamiento de información o implementación de acciones basada en normas anteriores en estudio, cumpliendo con las normativas que permiten la protección de datos personales de sus clientes. De no ser el caso, se realizará un diagnóstico que conduzca a la elaboración de recomendaciones que permitan cumplir con las nuevas disposiciones de la Ley Orgánica de Protección de Datos Personales y evitar las posibles sanciones.

Además, se definirán las acciones basadas en la evaluación de la gestión de la seguridad de la información. Para ello, se hará uso de la norma ISO/IEC 27002:2013. Esta es una herramienta utilizada por las organizaciones con el objetivo de garantizar la disponibilidad, confidencialidad e integridad de la información. Esta normativa ofrece pautas orientadas sobre las practicas optimas en materia de seguridad de la información. Su implementación conlleva a una defensa ante posibles amenazas, la preservación de la integridad y el cumplimiento de las obligaciones de la organización. Por lo tanto, se contempla la adopción de dicha normativa en la empresa Cabletel, dado que sus objetivos de control pueden alinearse con las especificaciones establecidas por la LOPDP. Este enfoque garantizará una gestión coherente y eficaz de la seguridad de la información, en contraste con los requerimientos legales vigentes en materia de protección de datos.

1.2 OBJETIVOS

1.2.1 Objetivo General

Evaluar la gestión de la protección de datos personales en la empresa Cabletel, basándose en la normativa vigente de la Ley Orgánica de Protección de Datos Personales y la norma ISO/IEC 27002:2013, para proponer recomendaciones necesarias que fortalezcan la seguridad de la información.

1.2.2 Objetivos Específicos

- Identificar los requisitos y sanciones que establece la Ley Orgánica de Protección de Datos Personales.
- Identificar los dominios y objetivos de control de la norma ISO/IEC 27002 que se adapten con los requisitos de la ley.
- Recolectar información de la situación actual de la empresa con respecto a la Ley y los objetivos de control identificados.
- Sugerir recomendaciones para la adecuación de Cabletel a la Ley Orgánica de Protección de Datos Personales.

1.3 JUSTIFICACIÓN

La información es el activo más valioso con el que cuentan las organizaciones, quienes deben asegurar esa información y los procesos que se utilizan para su tratamiento o procesamiento [8].

Las empresas gestionan la información personal de sus clientes mediante diversos métodos con el fin de llevar a cabo sus operaciones. Diariamente, se recopilan datos personales de manera verbal, escrita, a través de plataformas web, correos electrónicos, así como mediante formularios físico y digitales. No obstante, es importante señalar que el tratamiento de dicha información debe ejecutarse a las prácticas legales correspondientes en lo que respecta a su manejo, procesamiento, almacenamiento y utilización en bases de datos. Este enfoque garantiza

el cumplimiento normativo y la preservación de la integridad de los datos personales recopilados por las empresas [9].

La protección de los datos es fundamental y más cuando existe un riesgo, una amenaza o una ausencia de la seguridad. Por esto, es importante recalcar que las organizaciones cuenten con herramientas necesarias para proteger esa información personal de sus clientes, empleados, proveedores o también de terceras personas durante su tratamiento o manejo [5].

Si bien la Ley Orgánica de Protección de Datos Personales establece el marco regulatorio para el tratamiento de los datos, las empresas deben de asegurarse no solo de cumplir con esta ley, sino de implementar las mejores prácticas posibles en materia de seguridad de la información. La norma ISO/IEC 27002:2013 surge como una herramienta esencial en este contexto, porque provee las directrices y las prácticas recomendadas para garantizar la seguridad de la información. La unión de esta norma con las regulaciones de la ley puede ofrecer a la empresa un marco de trabajo adaptado a sus necesidades.

El análisis de la situación actual de la empresa Cabletel en relación con la ley vigente y la norma ISO 27002 es esencial para identificar posibles mejoras y obtener un manejo correcto de los datos personales; por lo tanto, el proponer un plan de implementación con recomendaciones permitirá a Cabletel abordar los desafíos relacionados con la protección de datos, minimizar los riesgos, las medidas de seguridad, obviamente dar cumplimiento con las estipulaciones legales de la ley y evitar las posibles sanciones, especialmente considerando que las empresas tienen que cumplir con esta ley a partir del 22 de mayo de 2023.

1.4 ALCANCE

La delimitación de este trabajo se centra de manera específica en la empresa Cabletel. Con la intención de identificar las acciones implementadas y evaluar los niveles de seguridad de la empresa con respecto a la protección de información personal.

Para alcanzar con este objetivo, se procederá inicialmente a llevar a cabo un análisis de la Ley Orgánica de Protección de Datos Personales. Este enfoque tiene como propósito comprender las obligaciones legales que Cabletel debe cumplir. Posteriormente, se llevará a cabo un estudio de la norma ISO/IEC 27002:2013, identificando así sus beneficios y los objetivos de control que esta norma establece. Además, se determinará cuáles de esos objetivos son los más apropiados con respecto a la protección de datos personales y analizar si la empresa cuenta con estos objetivos.

Tras la conclusión de dicho análisis, se procederá a la elaboración de un plan que contendrá recomendaciones y acciones específicas destinadas a fortalecer los procesos de seguridad de Cabletel y asegurar su cumplimiento con los requisitos legales establecidos por la normativa vigente.

1.5 METODOLOGÍA

Para llevar a cabo esta investigación, se empleará una metodología cualitativa y descriptiva. Inicialmente, se realizará una exhaustiva revisión de la literatura vinculada a la privacidad de datos personales, la Ley Orgánica de Protección de Datos Personales de la República del Ecuador y la norma ISO/IEC 27002:2013. Este proceso facilitará la recopilación de información y conocimientos relativos a conceptos, principios, requisitos, así como a las estrategias para salvaguardar la seguridad de la información y proteger los datos.

Posteriormente, se realizarán análisis comparativo entre diversas leyes y normativas, con el propósito de identificar el grado de alineación de la LOPDP con estándares

internacionales. Asimismo, se examinará leyes anteriores que incluyen disposiciones o medidas relacionadas con la seguridad de la información. Por último, se abordará la relación entre la norma ISO 27002 y la LOPDP, con el fin de conocer los objetivos de control pertinentes para la posterior recopilación de información a través de las encuetas.

En la fase final de la investigación, se procederá a la recopilación de información mediante dos encuestas. La primera se desarrollará a partir de la normativa previa a la LOPDP, abordando las acciones de seguridad de la información que la empresa debería haber implementado antes de la promulgación de la ley vigente. La segunda encuesta estará basada en la norma ISO/IEC 27002:2013 y proporcionará información detallada sobre la situación actual de la empresa con respecto a los objetivos de control necesarios para la protección de datos. Además, se identificarán las dificultades, necesidades u obstáculos presentes. Con la información recopilada, se procederá al desarrollo de recomendaciones necesarias para que Cabletel se alinee de manera efectiva con la LOPDP.

CAPITULO II

MARCO TEÓRICO

2.1 EMPRESA

Cabletel es una empresa de telecomunicaciones conocida en la ciudad de Azogues. Actualmente tiene más de 21 años de trayectoria en el mercado de las telecomunicaciones, buscando brindar a sus clientes servicios de calidad, basándose en la excelencia del servicio al cliente.

La empresa ofrece servicios de televisión por cable e internet con tecnología de fibra óptica, abarcando los cantones de Azogues, Biblián y Cuenca. En el servicio de televisión por cable, se dispone de una extensa selección de canales, mientras que en el servicio de internet con fibra óptica se presenta una variada gama de paquetes, con el objetivo de brindar opciones que se adecuen de manera óptima a las necesidades individuales de los clientes finales.

A lo largo del tiempo, Cabletel ha demostrado su capacidad de adaptación a las nuevas tecnologías y a los dinámicos cambios del mercado. En este sentido, la empresa ha realizado inversiones con el propósito de garantizar la entrega eficiente y de calidad de sus servicios a los clientes. Asimismo, en el ámbito de la seguridad y privacidad de los datos, Cabletel ha implementado medidas para salvaguardar la información personal de sus clientes, tomando como referencias normativas previas de la Ley Orgánica de Protección de Datos Personales.

No obstante, en consonancia con las disposiciones actuales, se establece la necesidad de que todas las empresas se ajusten rigurosamente a esta ley y cumplan con los nuevos lineamientos. Esto buscará garantizar la seguridad integral de los datos, reforzando así el compromiso de Cabletel con la protección y privacidad de la información personal de sus clientes en conformidad con los estándares más recientes.

2.1.1 Organigrama

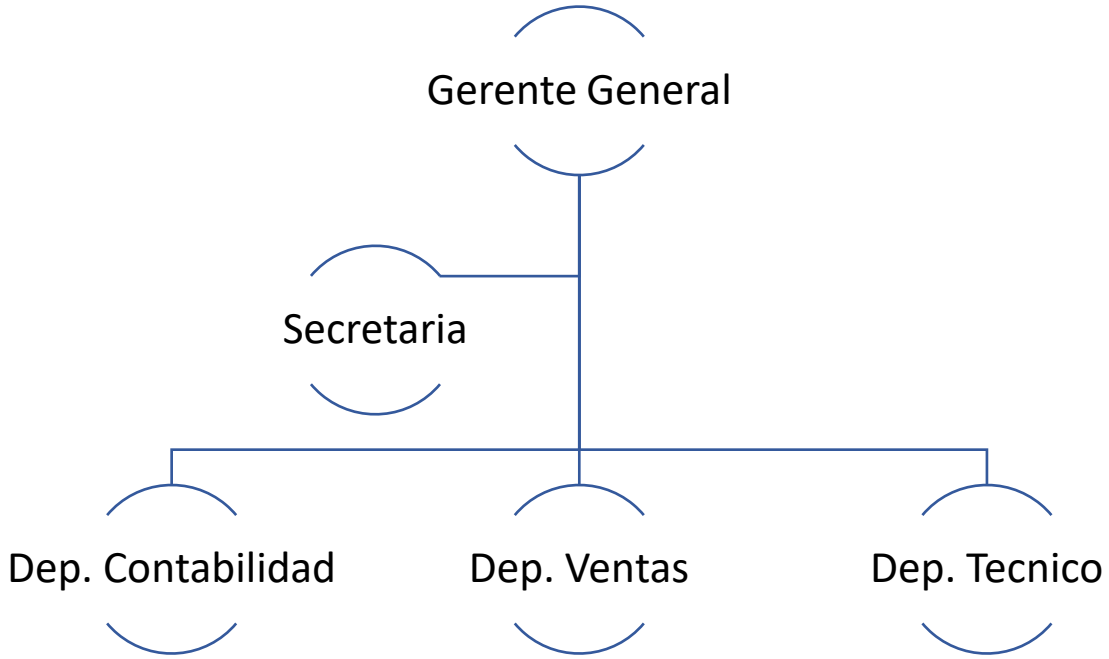

Ilustración 1: Organigrama de Cabletel

2.1.2 Misión

"Ofrecer a las familias ecuatorianas de todos los sectores una experiencia única al alcance de sus manos en contenido, comunicación y tecnología."

2.1.3 Visión

"Mantener el liderazgo en la cobertura más amplia del mercado en sectores urbanos y rurales para formar una red de abonados unidos y comprometidos a la empresa."

2.1.4 Ubicación

La empresa Cabletel tiene sus oficinas en la ciudad de Azogues y se encuentra ubicada en la calle Vintimilla entre Bolívar y Ayacucho.

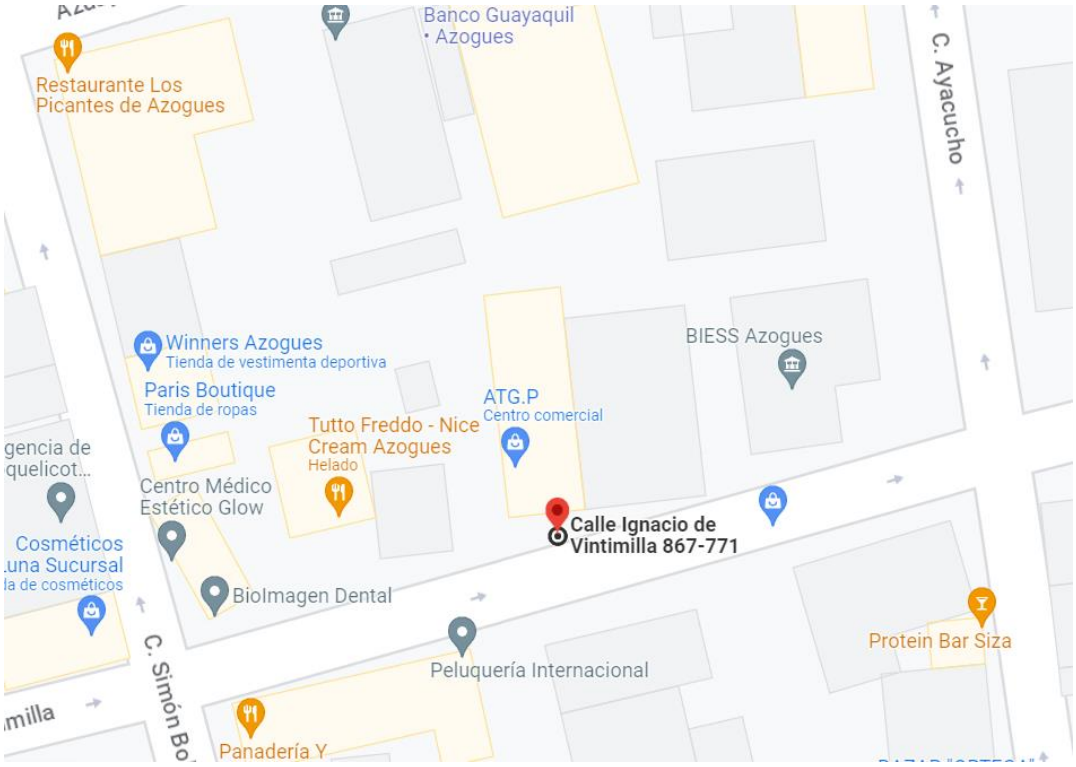

Ilustración 2: Ubicación de la empresa Cabletel

Fuente: https://www.google.com/maps/dir//-2.7370344,-78.8464229/@-2.7368374,-78.8465062,20.87z?entry=ttu

2.2 LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP)

Para abordar este capítulo, es importante conocer la trayectoria que ha tenido la ley orgánica de protección de datos personales (LOPDP). En la constitución de Ecuador de 2008, se reconoce el derecho de las personas con respecto a la protección de sus datos personales, este derecho está instituido en el artículo 66 numeral 19 “El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución

o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley" [10].

A partir de este artículo, se establece la base para la construcción de la ley que ahora está vigente. Por otra parte, en el año 2016 se planteó un anteproyecto de la ley titulado "Ley Orgánica de la Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales", sin embargo, no tuvo la suficiente aceptación por el contenido confuso y algunos lineamientos que generaron controversia, de igual forma se tuvo otra oferta de anteproyecto en el año 2012 titulado "Ley sobre la Protección a la Intimidad y los Datos Personales", el cual tampoco fue aprobado. Se tuvo que esperar hasta el año 2017, para que la Dinardap (Dirección Nacional de Registro de Datos Públicos) realizara su anteproyecto, conocido como "Ley de Protección de Datos Personales" [11].

Para la creación de esta regulación se tuvo la participación de varios sectores públicos y privados, se desarrollaron 80 mesas de trabajo con instituciones públicas tales como "sector de las telecomunicaciones, tales como Agencia de Regulación y Control de las Telecomunicaciones (Arcotel), Agencia de Regulación y Control Postal (ARCPostal), Correos del Ecuador EP, Corporación Nacional de Telecomunicaciones (CNT), Registro Civil y Ministerio de Telecomunicaciones y de la Sociedad de la Información, Mintel" [12]. Además se contó con el apoyo de expertos nacionales e internacionales, como el Comité de Propiedad Intelectual de la Cámara de Comercio Ecuatoriano Americana (Amcham), Asociación Ecuatoriana de Ciberseguridad (AECI), GMS Seguridad, Usuarios Digitales, Asociación para el Progreso de las Comunicaciones (APC), Fundación Ciudadanía y Desarrollo, Consejo de Regulación y Desarrollo de la Información y Comunicación (Cordicom), Observatorio Legislativo, Asociación de la Banca Privada (Asobanca), ONG Access Now para América Latina, Organización de Estados Americanos (OEA), Comisión Europea, Asociación Ecuatoriana de Protección de Datos Personales (Aepdp), Red Iberoamericana de Protección de

Datos, Instituto Nacional de Acceso a la Información Pública (INAI) de México, Consejo de Transparencia de Chile, Organización de Derechos Digitales para América Latina, Citec y la Agencia Latinoamericana de Información (ALAI), para que analizaran el contenido legal y dieran nuevas ideas [12].

El 19 de septiembre de 2019 se realizó la entrega del anteproyecto a la Asamblea Nacional y el 10 de mayo de 2021 se aprobaría la LOPDP con ciento dieciocho (118) votos a favor, de esta forma el 26 de mayo del mismo año se publicó en el Registro Oficial y a partir de esa fecha las empresas tendrían dos años para adaptarse a esta nueva ley [12].

2.2.1 Estructura de la LOPDP

La LOPDP está estructurada por 12 capítulos y 77 artículos, cada capítulo contine diversos artículos y está organizada de la siguiente manera:

Tabla 1: Estructura de la LOPDP

CAPITULO	NOMBRE	NUMERO DE ARTÍCULOS
1	ÁMBITO DE APLICACIÓN INTEGRAL	9
2	PRINCIPIOS	1
3	DERECHOS	14
4	CATEGORÍAS ESPECIALES DE DATOS	8
5	TRANSFERENCIA O COMUNICACIÓN Y ACCESO A DATOS PERSONALES POR TERCEROS	4
6	SEGURIDAD DE DATOS PERSONALES	10
7	RESPONSABLE, ENCARGO Y DELEGADO DE PROTECCIÓN DE DATOS PERSONALES	5

8	DE LA RESPONSABILIDAD PROACTIVA	3
9	TRANSFERENCIA O COMUNICACIÓN INTERNACIONAL DE DATOS PERSONALES	7
10	DE LOS REQUERIMIENTOS DIRECTOS Y DE LA GESTIÓN DEL PROCEDIMIENTO ADMINISTRATIVO	3
11	MEDIDAS CORRECTIVAS, INFRACCIONES Y RÉGIMEN SANCIONATORIO	10
12	AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES	3

2.2.2 ¿Porque una ley para la protección de datos personales?

En estos últimos años, la tecnología ha experimentado una evolución y un incremento masivo en la sociedad, esto ha implicado que la mayoría de las personas estén más ligadas al ámbito tecnológico, tanto en el uso de aplicaciones como en el consumo de servicios empresariales; por lo tanto, para poder acceder a estos productos es necesario el proveer un poco de información de nuestros datos personales. Además, estos datos son recolectados, almacenados y en varias ocasiones analizados como estrategias de negocio. Sin embargo, no sabemos a ciencia cierta si las empresas proporcionan la suficiente seguridad a nuestros datos personales, es por eso que nace la idea o la iniciativa de establecer una ley y según Lorena Naranjo Godoy, directora de la Dinardap “contar con una ley de protección de datos personales permitirá que las instituciones y las empresas privadas, cuyo giro de negocios son los datos,

tengan los criterios para saber qué medidas tecnológicas y organizativas deben implementar, con la finalidad de que los datos que poseen estén adecuadamente resguardados y usados" [13].

Es así que, la LOPDP estable en su artículo 1, "El objeto y finalidad de la presente Ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela" [14].

Otras razones más para tener una ley es el mal manejo de la información por parte de las empresas, como en el caso de los correos electrónicos de sus clientes, ya que se puede dar un ataque de un phishing o tener correos maliciosos, es probable también que los usuarios no puedan acceder a los productos o servicios que tiene la empresa, debido a datos erróneos de sus clientes en su repositorio de bases de dato [13], pero con la presente ley este problema de información errónea se disminuye, ya que en el artículo 14 de la LOPDP establece "El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos. Para tal efecto, el titular deberá presentar los justificativos del caso, cuando sea pertinente. El responsable de tratamiento deberá atender el requerimiento en un plazo de quince (15) días y en este mismo plazo, deberá informar al destinatario de los datos, de ser el caso, sobre la rectificación, a fin de que lo actualice" [14].

2.2.3 Alcance de la LOPDP

Al momento de desarrollar los diferentes artículos para la ley, se establecieron los ámbitos de aplicación a los que estaría enfocado y con ello determinando su alcance. Por lo tanto, el artículo que está orientado al ámbito de aplicación material es el artículo 2 de la LOPDP y establece "La presente ley se aplicará al tratamiento de datos personales contenidos en

cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior" [14], pero este articulo no será aplicable en los diferentes puntos que se mencionan a continuación:

- El uso de datos en actividades familiares o domesticas por parte de personas naturales.
- Personas fallecidas.
- Datos anonimizados, pero si en algún momento los datos dejan de serlo, entonces se dará cumplimiento a lo que dispone la ley.
- Actividades como el periodismo u otros campos editoriales.
- Datos personales regulados por una normativa especializada en el contexto de la gestión de incidentes por desastres naturales, seguridad y defensa del Estado.
- Bases de datos que son utilizados para la investigación, detección, prevención, proceso de las infracciones penales o elaboración de las sanciones penales realizadas por los competentes organismos estatales.
- Datos que identifican a personas jurídicas.

De igual forma se instituye el espacio de aplicación territorial en el artículo 3 de la LOPDP y este establece "Sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia, se aplicará la presente Ley cuando" [14]:

- "El tratamiento de datos personales se realice en cualquier parte del territorio nacional"
- "El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional"

- "Se realice tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador, cuando las actividades del tratamiento estén relacionadas con:
    a) La oferta de bienes o servicios a dichos titulares, independientemente de si a estos se les requiere su pago
    b) Control de su comportamiento, en la medida en que este tenga lugar en el Ecuador"
- "Al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, le resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público" [14].

2.2.4 Integrantes de la LOPDP

Para poner en marcha la ley, es necesario instituir los integrantes que intervendrán y cuáles serían sus roles y responsabilidades, por lo que, en el artículo 5 de la LOPDP se mencionan a los componentes del sistema encargado de salvaguardar la integridad de los datos personales, que incluyen a los siguientes miembros: [14]

- "**Titular:** Persona natural cuyos datos son objeto de tratamiento"
- "Responsable de tratamiento de datos personales: persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales"
- "**Encargado del tratamiento de datos personales:** Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales"

- "**Destinatario:** Persona natural o jurídica que ha sido comunicada con datos personales"
- "**Autoridad de Protección de Datos Personales:** Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales"
- "**Delegado de protección de datos personales:** Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos" [14]

2.2.5 Principios de la LOPDP

Estos principios, establecen las bases para que el tratamiento de datos personales sea responsable y adecuado, garantizando la triada de la seguridad de la información como la disponibilidad, confidencialidad e integridad. Por lo tanto, de acuerdo con el artículo 10 de la LOPDP "Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de" [15]:

- "**Juridicidad:** El tratamiento de datos personales debe efectuarse con estricto apego y cumplimiento a los principios, derechos y obligaciones a la constitución, instrumentos internacionales y la normativa de protección de datos personales"

- "**Lealtad:** Debe ser claro para los titulares que se están tratando sus datos personales y las formas en que dichos datos son o serán tratados. En ningún caso los datos personales pueden ser tratados a través de medios o para fines, ilícitos o desleales"
- "**Transparencia:** Toda información o comunicación relativa al tratamiento debe ser de fácil acceso y comprensión, utilizando lenguaje sencillo y claro. Las relaciones derivadas del tratamiento de datos personales deben ser transparentes"
- "**Finalidad:** Las finalidades del tratamiento deben ser determinadas, explicitas, legitimas y comunicadas al titular. No puede tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legitimo señalados en la LOPDP"
- "**Pertinencia y minimización de datos personales**: Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento"
- "**Proporcionalidad del tratamiento:** El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o la naturaleza misma de las categorías especiales de datos"
- "**Confidencialidad:** El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto. No debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos"

- "**Calidad y exactitud:** Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad"
- "**Conservación:** Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento"
- "**Seguridad de datos personales**: Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias"
- "**Responsabilidad proactiva y demostrada**: Para la protección de datos personales además de lo establecido en la normativa aplicable, el responsable puede valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento"
- "**Aplicación favorable al titular:** En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las deben interpretar y aplicar en el sentido más favorable al titular de dichos datos"
- "**Independencia del control**: La Autoridad de Protección de Datos debe ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción" [15].

2.2.6 Requisitos de la LOPDP

La LOPDP dispone de algunas medidas o requisitos que deben de cumplir las empresas con respecto al tratamiento de los datos personales. Estos requisitos son primordiales para garantizar la seguridad, privacidad y el correcto uso de la información. Por lo tanto, en el art. 47 de la Ley se estipula de manera precisa las obligaciones que tiene el responsable y el encargado del tratamiento de los datos personales con 15 puntos en concreto. A continuación, se muestra la tabla 2 que desglosa esos 15 puntos [14] y posteriormente procederé a relacionarlos con otros artículos presentes en la Ley que hablan de forma más detalla de los requisitos o medidas a tomar en cuenta.

Tabla 2: Requisitos del encargado y responsable del tratamiento de datos personales

ART. 47 (OBLIGACIONES DEL RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES)	ARTICULOS RELACIONADOS
Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia	Art. 8, 10, 12 – 17, 19 – 21, 27
Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia	Art. 37, 39 – 41
Aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, Técnicas, físicas, organizativas y jurídicas implementadas	

Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular	Art. 12 – 17, 19 – 21, 26
Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas	Art. 40
Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales	Art. 42
Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas	Art. 44, 45
Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto	Art. 43, 46
Implementar la protección de datos personales desde el diseño y por defecto	Art. 39
Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales	Art. 10, 34, 35
Asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional	Art. 34
Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales	Art. 51
Designar al delegado de Protección de Datos Personales, en los casos que corresponda	Art. 48

Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales	Art. 68, 69
Los demás establecidos en la presente Ley en su reglamento, en directrices, lineamientos, regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia	Otros artículos

2.2.7 Sanciones de la LOPDP

Las sanciones que contiene la ley son un componente importante para garantizar el cumplimiento de la misma y la adecuada protección de los datos personales, promoviendo así el entorno seguro en las empresas con respecto al tratamiento de la información, derechos y la privacidad que tiene los clientes. A continuación, se centrará solo en detallar las infracciones que puede cometer el responsable de la protección de datos y también cuales serían las sanciones contempladas en la LOPDP.

Este puede incurrir en dos tipos de infracciones, tanto leves como graves, en el artículo 67 de la LOPDP se especifica las infracciones leves y en el artículo 68 las infracciones graves. Entre las infracciones leves se puede encontrar las siguientes [14]:

- "No tramitar, tramitar fuera del término previsto o negar injustificadamente las peticiones o quejas realizadas por el titular"
- "No implementar protección de datos desde el diseño y por defecto"
- "No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales"
- "Elegir un encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales"

- “Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales” [14].

Por otro lado, se consideran infracciones graves a las siguientes [14]:

- “No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia”
- “Utilizar información o datos para fines distintos a los declarados”
- “Ceder o comunicar datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente Ley y su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia”
- “No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales las particularidades del tratamiento y de las partes involucradas”
- “No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarlas”
- “No implementar medidas técnicas organizativas o de cualquier índole, necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones a la seguridad de datos personales que hayan sido identificadas”

- "No notificar a la Autoridad de Protección de Datos Personales y al titular, de vulnerabilidades a la seguridad y protección de datos personales, cuando afecte los derechos fundamentales y libertades individuales de los titulares"
- "No notificar a la Autoridad de Protección de Datos Personales del titular las vulneraciones de seguridad y protección de datos personales, cuando exista afectación a los derechos fundamentales y libertades individuales de los titulares"
- "No subscribir contratos que incluyan cláusulas de confidencialidad y tratamiento adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales"
- "No mantener actualizado el Registro Nacional de protección de datos personales de conformidad a los dispuesto en la presente Ley su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia"
- "No consignar en el Registro Nacional de Protección de Datos Personales lo dispuesto en la presente Ley y su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia"
- "No designar al delegado de protección de datos personales cuando corresponda"
- "No permitir y no contribuir a la realización de auditorías o inspecciones por parte del auditor acreditado por la Autoridad de Protección de Datos Personales"
- "Incumplir las medidas correctivas o cumplir de forma tardía, parcial o defectuosa, siempre y cuando hubiese precedido por dicha causa la aplicación

de una sanción por infracción leve, e incurrir de forma reiterada en faltas leves" [14].

Si se comete una o varias de las infracciones mencionadas, la Autoridad de Protección de Datos Personales podrá imponer las sanciones respectivas, en el caso de que esta verifique el acto de cualquier infracción. En el artículo 71 se especifica las sanciones para el tema de las infracciones leves y son las siguientes [14]:

- "Servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente Ley, serán sancionados con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente"
- "Si el responsable o el encargado del tratamiento de datos personales o de ser el caso un tercero es una entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa" [14].

De igual forma en el artículo 72 se establece las sanciones para las infracciones graves y son las siguientes [14]:

- "Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente Ley serán sancionados con una multa de entre 10 a 20 salarios básicos unificados

del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente"

- "Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa" [14].

2.3 ISO/IEC 27002:2013

En el año de 2007, se realiza la incorporación de la nueva ISO/IEC 27002, la cual contiene componentes como los objetivos de control y los controles que pueden ser aplicados al tema de seguridad de la información [8]. Por otra parte, en 2013 se publica una nueva versión de esta norma con varias recomendaciones de buenas prácticas para mantener el nivel óptimo de seguridad en cualquier organización. Con esta nueva versión pretendieron tener un alcance más amplio en las organizaciones, ya que evita la restricción de su uso con respecto a las recomendaciones que proporciona la norma, es decir, su aplicación podía ser de forma completa o parcial, pero dependiendo de las cláusulas y los controles necesarios según lo requerido al nivel de seguridad de la organización. [16]

La ISO/IEC 27002:2013 es una guía de buenas prácticas que se puede implementar en una organización, como modelo de control de la privacidad de la información. Estos controles están enfocados en la seguridad que se debe de tener dentro de las empresas, ayudando en si a minimizar los riesgos, amenazas y vulnerabilidades que se podrían tener, por lo tanto, la norma establece directrices y recomendaciones de buenas prácticas al momento de tener un suceso de

riesgo y como debemos de actuar para minimizarlo y asegurar la continuación de nuestros procesos. [17]

Esta versión se centra en proporcionar servicios para asegurar el activo esencial de la organización como es en este caso la información, teniendo como objetivo mantener y cumplir con la triada de la seguridad de la información. Por lo tanto, la norma permite definir, monitorear, implementar y evaluar la seguridad de la información que se maneja en las organizaciones, todo esto se lo hace a través de un análisis basado en los niéveles de riesgo y también en la medición del impacto que se tendría. [18]

Ilustración 3: Triada de la Seguridad

Fuente: http://b-one-informatica.blogspot.com/2016/02/la-triada-cid-seguridad-informatica.html

Como ya se había dicho, la norma ISO/IEC 27002:2013 es el código de buenas prácticas, pero para garantizar los activos de la organización la norma debe de tener en cuenta la triada de la seguridad de la información. A continuación, se describe cada componente de la misma:

- **Confidencialidad:** garantizar que el acceso a la información solo debe de ser únicamente para las personas autorizadas y con ello evitar la propagación de información sensible.
- **Integridad:** se refiere a la precisión, completitud y exactitud de la información, buscando asegurar que la información no haya sido modificada.
- **Disponibilidad:** esto implica a que cualquier servicio o en este caso la información este siempre accesible cuando se lo requiera, evitando así las interrupciones. [19]

2.3.1 Beneficios de la norma

La regulación en cuestión abarca un total de 14 áreas temáticas, entre todas se suman 35 metas de control y a su vez se tiene un conjunto de 114 controles, permitiendo tener una mejor orientación en el monitoreo de los niveles de seguridad, analizar los riesgos que se pueden presentar y con ello mantener, establecer e implementar un sistema de gestión de seguridad de la información. [18]

A continuación, se presenta algunos beneficios que nos provee la norma:

- Mayor conciencia sobre el tema de la seguridad de la información.
- Mayor exploración sobre los activos de la organización.
- Mejor orientación en la implementación de las políticas de control de seguridad.
- La oportunidad de identificar y corregir las debilidades.
- Se reduce el riesgo de responsabilidad por la falta de implementación de un SGSI.
- Atrae clientes que valoran la certificación de seguridad, por lo tanto, es un diferenciador competitivo.

- Mejora la organización o gestión con los procesos o mecanismos diseñados.
- La reducción de los costos al prevenir los incidentes.
- Cumplimiento de requisitos legales y otras regulaciones aplicables. [20]

2.3.2 Estructura de la norma ISO

La norma ISO/IEC 27002:2013 contiene una estructura amplia de niveles de seguridad que las empresas pueden llegar a implementar para proteger sus activos más importantes, como puede ser la información. Estos controles proporcionan diferentes dominios con respecto a la seguridad, se dividen en diversos objetivos de control y que a su vez cada uno contiene varios aspectos de control, por lo tanto, la norma establece 14 dominios, 35 objetivos de control y 114 controles. A continuación, se presenta la tabla 3 con todos los parámetros que se mencionaron: [21]

Tabla 3: Estructura de la norma ISO/IEC 27002:2013

DOMINIOS	OBJETIVOS DE CONTROL	CONTROLES
Políticas de seguridad	Directrices de la dirección en seguridad	Conjunto de políticas para la seguridad de la información.
		Revisión de las políticas para la seguridad de la información.
Aspectos organizativos de la seguridad de la información.	Organización interna	Asignación de responsabilidades para la seguridad de la información.
		Segregación de tareas.
		Contacto con las autoridades.
		Contacto con grupos de interés especial.
		Seguridad de la información en la gestión de proyectos.

	Dispositivos para movilidad y teletrabajo	Política de uso de dispositivos para movilidad.
		Teletrabajo.
Seguridad ligada a los recursos humanos	Antes de la contratación	Investigación de antecedentes.
		Términos y condiciones de contratación.
	Durante la contratación	Responsabilidades de gestión.
		Concienciación, educación y capacitación en seguridad de la información.
		Proceso disciplinario.
	Cese o cambio de puesto de trabajo	Cese o cambio de puesto de trabajo.
Gestión de activos	Responsabilidad sobre los activos	Inventario de activos.
		Propiedad de los activos.
		Uso aceptable de los activos.
		Devolución de activos.
	Clasificación de la información	Directrices de clasificación.
		Etiquetado y manipulación de soportes.
		Manipulación de activos.
	Manejo de los soportes de almacenamiento	Gestión de soportes extraíbles.
		Eliminación de soportes.
		Soportes físicos en tránsito.
Control de accesos	Requisitos de negocio para el control de accesos	Política de control de accesos.
		Control de acceso a las redes y servicios asociados.
	Gestión de acceso de usuario	Gestión de altas/bajas en el registro de usuarios.
		Gestión de los derechos de acceso asignados a usuarios.
		Gestión de los derechos de acceso con privilegios especiales.
		Gestión de información confidencial de autenticación de usuarios.
		Revisión de los derechos de acceso de los usuarios.

		Retirada o adaptación de los derechos de acceso.
	Responsabilidad del usuario	Uso de información confidencial para la autenticación.
	Control de acceso a sistemas y aplicaciones	Restricción del acceso a la información.
		Procedimientos seguros de inicio de sesión.
		Gestión de contraseñas de usuario.
		Uso de herramientas de administración de sistemas.
		Control de acceso al código fuente de los programas.
Cifrado	Controles criptográficos	Política de uso de los controles criptográficos.
		Gestión de claves.
Seguridad física y ambiental	Áreas seguras	Perímetro de seguridad física.
		Controles físicos de entrada.
		Seguridad de oficinas, despachos y recursos.
		Protección contra amenazas externas y ambientales.
		El trabajo en áreas seguras.
		Áreas de acceso público, carga y descarga.
	Seguridad de los equipos	Emplazamiento y protección de equipos.
		Instalaciones de suministro.
		Seguridad del cableado.
		Mantenimiento de los equipos.
		Salida de activos fuera de las dependencias de la empresa.
		Seguridad de los equipos y activos fuera de las instalaciones.
		Reutilización o retirada segura de dispositivos de almacenamiento.
		Equipo informático de usuario desatendido.

		Política de puesto de trabajo despejado y bloqueo de pantalla.
Seguridad en la operativa	Responsabilidades y procedimientos de operación	Documentación de procedimientos de operación.
		Gestión de cambios.
		Gestión de capacidades.
		Separación de entornos de desarrollo, prueba y producción.
	Protección contra código malicioso	Controles contra el código malicioso.
	Copias de seguridad	Copias de seguridad de la información.
	Registro de actividad y supervisión	Registro y gestión de eventos de actividad.
		Protección de los registros de información.
		Registros de actividad del administrador y operador del sistema.
		Sincronización de relojes.
	Control del software en explotación	Instalación del software en sistemas en producción.
	Gestión de la vulnerabilidad técnica	Gestión de las vulnerabilidades técnicas.
		Restricciones en la instalación de software.
	Consideraciones de las auditorias de los sistemas de información	Controles de auditoría de los sistemas de información.
Seguridad en las telecomunicaciones	Gestión de la seguridad en las redes	Controles de red
		Mecanismos de seguridad asociados a servicios de red.
		Segregación de redes.
	Intercambio de información con partes externas	Políticas y procedimientos de intercambio de información.
		Acuerdos de intercambio.
		Mensajería electrónica.
		Acuerdos de confidencialidad y secreto.

Adquisición, desarrollo y mantenimiento de los sistemas de información	Requisitos de seguridad de los sistemas de información	Análisis y especificaciones de los requisitos de seguridad.
		Seguridad de las comunicaciones en servicios accesibles por redes públicas.
		Protección de las transacciones por redes telemáticas.
	Seguridad en los procesos de desarrollo y soporte	Política de desarrollo seguro de software.
		Procedimientos de control de cambios en los sistemas.
		Revisión técnica de las aplicaciones tras efectuar cabios en el sistema operativo.
		Restricciones a los cambios en los paquetes de software.
		Uso de principios de ingeniería en protección de sistemas.
		Seguridad en entornos de desarrollo.
		Externalización del desarrollo de software.
		Pruebas de funcionalidad durante el desarrollo de los sistemas.
		Pruebas de aceptación.
	Datos de prueba	Protección de los datos utilizados en pruebas.
Relaciones con suministradores	Seguridad de la información en las relaciones con suministradores	Política de seguridad de la información para suministradores.
		Tratamiento del riesgo dentro de acuerdos de suministradores.
		Cadena de suministro en tecnologías de la información y comunicaciones.
	Gestión de la prestación del servicio por suministradores	Supervisión y revisión de los servicios prestados por terceros.
		Gestión de cambios en los prestados por terceros.
		Responsabilidades y procedimientos.

Gestión de incidentes en la seguridad de la información	Gestión de incidentes de seguridad de la información y mejoras	Notificación de los eventos de seguridad de la información.
		Notificación de puntos débiles de la seguridad.
		Valoración de eventos de seguridad de la información y toma de decisiones.
		Respuesta a los incidentes de seguridad.
		Aprendizaje de los incidentes de seguridad de la información.
		Recopilación de evidencias.
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Continuidad de la seguridad de la información	Planificación de la continuidad de la seguridad de la información.
		Implantación de la continuidad de la seguridad de la información.
		Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	Redundancias	Disponibilidad de instalaciones para el procesamiento de la información.
Cumplimiento	Cumplimiento de los requisitos legales y contractuales	Identificación de la legislación aplicable.
		Derechos de propiedad intelectual (DPI).
		Protección de los registros de la organización.
		Protección de datos y privacidad de la información personal.
		Regulación de los controles criptográficos.
	Revisiones de la seguridad de la información	Revisión independiente de la seguridad de la información.
		Cumplimiento de las políticas y normas de seguridad.
		Comprobación del cumplimiento.

2.3.2.1 Políticas de Seguridad

Este dominio se adapta a la empresa con sus distintos controles, ayudando a orientar las directrices que están relacionadas con la seguridad y la privacidad de la información a la normativa, legislación y controles con los que cuenta la empresa [8]. Por lo tanto, su objetivo es establecer un soporte de seguridad de información basándose en las leyes y sus requerimientos, es así que cada organización debe de redactar su documento y dar a conocer a sus empleados los términos a los que llegaron. Estas políticas no pueden estar siempre estáticas y con el mismo reglamento, deben de tener un cambio constante de acuerdo a las necesidades que vaya presentando la empresa [20].

2.3.2.2 Aspectos organizativos de la seguridad de la información

Toda empresa debe de tener una organización interna y debe de estar gestionada adecuadamente por los representantes organizativos, mismos que tendrán sus roles y responsabilidades bien definidas [22].

2.3.2.3 Seguridad ligada a los recursos humanos

Las obligaciones que tiene el personal de la organización con respecto al tema de la seguridad debe de estar claramente documentada y definida, de igual forma un responsable debe de dar a conocer a todo el personal las normas de seguridad que se tiene en la empresa, para disminuir las consecuencias que pudieran tener en el desarrollo de sus funciones [8].

2.3.2.4 Gestión de activos

Se considera activo a un elemento que genere valor a una organización, por lo que dentro de una organización se puede tener varios activos que necesitan ser protegidos, para ello se necesita a un responsable que los gestione, ya sea en la identificación, clasificación o en el tipo de uso que se requiera, al final se tendrá una lista actualizada de los activos con los que cuenta la empresa [22].

2.3.2.5 Control de accesos

Este dominio trata del permiso al acceso de la información, ya sea en términos de aplicaciones, contraseñas, documentación o cualquier otro privilegio. Para poder garantizar este acceso se tiene que contar con políticas y establecer controles de seguridad de usuarios, con esto facilitara a los usuarios autorizados a acceder a los distintos servicios y con ello tener un mejor control en el registro de acceso [8].

2.3.2.6 Cifrado

En este dominio se establece los controles de criptografía que permitirán garantizar la confidencialidad, integridad y la protección de la información [22].

2.3.2.7 Seguridad física y ambiental

El tema de seguridad no solo abarca la protección interna de los equipos tecnológicos contra cualquier vulnerabilidad, también se debe de tomar cuenta el entorno físico o externo donde se encuentra el equipo, para establecer criterios de seguridad que garanticen la protección contra desastres naturales o un acceso no autorizado [20].

2.3.2.8 Seguridad en la operativa

Este dominio se basa en controles que deben ser consideradas para garantizar que las responsabilidades y procesos operativos sean coherentes con los requisitos de la seguridad, también la protección contra amenazas en la operación diaria [20].

2.3.2.9 Seguridad en las telecomunicaciones

Con respecto a este dominio, trata de proteger y garantizar la seguridad de la información antes de su desarrollo, durante su implementación y después cuando se utiliza en algún medio de comunicación, como puede ser el caso de las redes sociales [22].

2.3.2.10 Adquisición, desarrollo y mantenimiento de los sistemas de información

El presente dominio tiene como objetivo integrar el tema de la seguridad de la información en cada componente del ciclo de vida de un sistema de información [20].

2.3.2.11 Relaciones con suministradores

Al momento de relacionarnos con terceras personas, debemos de establecer las respectivas medidas de seguridad y a través de este dominio lo podemos garantizar [20].

2.3.2.12 Gestión de incidentes en la seguridad de la información

Con este se tendrá procedimientos para establecer en todo la organización, con ello se podrá determinar cuál es el incidente y como debemos de actuar para reducir el riesgo identificado [22].

2.3.2.13 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Este determina controles para mantener y recuperar las operaciones del negocio en caso de identificar incidentes más graves [20].

2.3.2.14 Cumplimiento

Por último, este dominio establece controles que nos permitirá dar cumplimiento a las leyes, regulaciones y contratos establecidos, de igual forma podremos gestionar si existe algún incumplimiento [22].

2.3.3 ¿Por qué el uso de la ISO/IEC 27002?

La incorporación de la norma ISO/IEC 27002 es primordial en el desarrollo de este proyecto, porque no solo sirve como una herramienta para garantizar que la empresa este en conformidad con las regulaciones actuales de la LOPDP, también se establece como un marco sólido y reconocido internacionalmente para abordar la gestión de la seguridad de la información. Después de exponer todo lo relacionado a la ISO/IEC 27002 en los puntos anteriores, se puede decir que esta norma proporciona un conjunto de dominios y objetivos de control diseñados para asegurar la integridad, disponibilidad y confidencialidad de la información.

Entonces la utilización de la norma ofrecerá una guía para desarrollar una conexión entre los dominios de la norma ISO y los requerimientos que impone la ley a las empresas. Una vez establecida esta relación, será posible identificar los objetivos de control pertinentes para garantizar que Cabletel no solo cumpla con las disposiciones de la LOPDP, sino que tenga una adecuada gestión en la seguridad de la información. Con esta estructura definida, se podrá aplicar una encuesta fundamentada en la norma ISO, a través de este instrumento de recolección de información, se hará visible las áreas donde Cabletel ya ha implementado controles adecuados y también se destacarán las áreas que requieren mayor atención. Con este enfoque se busca asegurar la integridad, seguridad y confidencialidad de la información que maneja la empresa, garantizando también el cumplimiento de las regulaciones en vigor.

CAPITULO III

MARCO METODOLÓGICO

La protección de datos personales es un componente esencial para asegurar la privacidad, el uso adecuado y la seguridad de la información, en este contexto la LOPDP regula los procesos y las políticas de las organizaciones mediante la normativa vigente. En este capítulo se aborda el análisis de la gestión de la protección de información personal en la empresa Cabletel. Este análisis se centra en el cumplimiento de los establecido por la LOPDP y la norma ISO/IEC 27002:2013.

Empezamos analizando la relación entre el GDPR (Reglamento General de Protección de Datos) y la LOPDP, esto permite establecer las coincidencias entre ambas normativas, de igual manera se desarrolla una comparativa con la Ley Orgánica de Telecomunicaciones (LOT), para evidenciar su vínculo con la LOPDP.

Después de establecer la relación entre la GDPR, LOPDP y la LOT, se procede a detallar la conexión entre los dominios de la norma ISO/IEC 27002 y la LOPD. Esto permite identificar los objetivos de control que mejor se adaptan a las disposiciones que menciona la ley, proporcionando una estructura sobre la cual se puede basar la gestión de la seguridad de los datos.

El siguiente punto corresponde al análisis de la situación actual de Cabletel, este será un componente crucial en este estudio. Se realizará una revisión de las medidas que la empresa tenía que cumplir previas a la implementación de la LOPDP y de la misma forma se identifican los controles que contiene la empresa que se detallan más adelante, esto permite tener una visión clara de las áreas que requieren atención y de las que ya cumplen con los estándares establecidos.

Finalmente, con los resultados obtenidos se sugiere recomendaciones, estas medidas tienen como propósito fortalecer la gestión de la seguridad de datos personales en Cabletel, lo que no solo garantiza el cumplimiento de la normativa vigente, sino que también la integridad y protección de la información.

Cabe recalcar que, hasta la fecha de investigación para este proyecto la autoridad o superintendencia de protección de datos no se ha conformado, esta superintendencia será la encargada de controlar el cumplimiento de la LOPDP y sancionar a las empresas que no estén alineados a lo estipulado en la ley. A pesar de no contar con dicha autoridad, el presidente Guillermo Lasso envió la terna al Consejo de Participación Ciudadana y Control Social (CPCCS) para la designación de esta [23]. De igual forma, estaría en desarrollo el proyecto de reglamento a la Ley de Protección de Datos Personales [24].

3.1 RELACIÓN ENTRE LA GDPR Y LA LOPDP

El GDPR (Reglamento General de Protección de Datos), es un reglamento de la Unión Europea que establece normas sobre el manejo de los datos personales para proteger los derechos de sus titulares [25]. El GDPR se ha convertido en un estándar para el tema de la protección de datos personales, por lo que varios países lo han tomado como referencia para desarrollar sus propias leyes [26]. Este es el caso de Ecuador, que lo ha tomado como base para la creación de su normativa interna de protección de datos personales, la cual se encuentra actualmente en vigencia [27]. Ambas normativas comparten objetivos similares, aunque particularidades distintas según las necesidades y contextos de cada país. El propósito de esta comparación consiste en discernir las concordancias existentes entre los artículos de cada normativa. Para ello, se ha llevado a cabo una selección de artículos vinculados a los requisitos

estipulados por la LOPDP, los cuales se presentan de manera visual en la tabla 2. A continuación, se muestra la tabla 4 con los artículos de cada normativa y la similitud [14] [25]:

Tabla 4: Relación de artículos GDPR y LOPDP

ARTÍCULOS DE LA LOPDP	ARTÍCULOS DE LA GDPR
Art. 8 (Consentimiento)	Art. 6 (Licitud del tratamiento)
Art. 10 (Principios)	Art. 5 (Principios relativos al tratamiento)
Art. 12 (Derecho a la información)	Art. 12 (Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado) Art. 13 (Información que deberá facilitarse cuando los datos personales se obtengan del interesado)
Art. 13 (Derecho de acceso)	Art. 15 (Derecho de acceso del interesado)
Art. 14 (Derecho de rectificación y actualización)	Art. 16 (Derecho de rectificación)
Art. 15 (Derecho de eliminación)	Art. 17 (Derecho de supresión)
Art. 16 (Derecho de oposición)	Art. 21 (Derecho de oposición)
Art. 17 (Derecho a la portabilidad)	Art. 20 (Derecho a la portabilidad de los datos)
Art. 19 (Derecho a la suspensión del tratamiento)	Art. 18 (Derecho a la limitación del tratamiento)
Art. 20 (Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas)	Art. 22 (Decisiones individuales automatizadas, incluida la elaboración de perfiles)
Art. 21 (Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas)	
Art. 26 (Tratamiento de datos sensibles)	Art. 9 (Tratamiento de categorías especiales de datos personales)

Art. 27 (Datos personales de personas fallecidas)	No identificado
Art. 34 (Acceso a datos personales por parte del encargado)	No identificado
Art. 35 (Acceso a datos personales por parte de terceros)	No identificado
Art. 37 (Seguridad de datos personales)	Art. 32 (Seguridad del tratamiento)
Art. 39 (Protección de datos personales desde el diseño y por defecto)	Art. 25 (Protección de datos desde el diseño y por defecto)
Art. 40 (Análisis de riesgo, amenazas y vulnerabilidades)	No identificado
Art. 41 (Determinación de medidas de seguridad aplicables)	No identificado
Art. 42 (Evaluación de impacto del tratamiento de datos personales)	Art. 35 (Evaluación de impacto relativa a la protección de datos)
Art. 43 (Notificación de vulneración de seguridad)	Art. 33 (Notificación de una violación de la seguridad de los datos personales a la autoridad de control)
Art. 44 (Acceso a datos personales para atención a emergencias e incidentes informáticos)	No identificado
Art. 45 (Garantía del secreto de las comunicaciones y seguridad de datos personales)	No identificado
Art. 46 (Notificación de vulneración de seguridad al titular)	Art. 34 (Comunicación de una violación de la seguridad de los datos personales al interesado)
Art. 48 (delegado de protección de datos personales)	Art. 37 (Designación del delegado de protección de datos)
Art. 51 (Registro Nacional de protección de datos personales)	Art. 30 (Registro de las actividades de tratamiento)

La tabla 4 refleja una coincidencia significativa entre ambas normativas. Por lo cual, de los 26 artículos más relevantes de la LOPDP en el ámbito de los requisitos, 19 tienen una relación con la GDPR. Esto refleja una alineación de la ley de Ecuador con las prácticas y estándares internacionales en materia de protección de datos. Sin embargo, hay 7 artículos que no encuentran un equivalente en la GDPR, por lo tanto, Ecuador a pesar de tomarla como referencia, ha visto la necesidad de añadir sus propias clausulas o tomar de otras normativas y leyes.

3.2 RELACION ENTRE LA LOT Y LA LOPDP

Dentro del marco regulatorio ecuatoriano, la Ley Orgánica de Telecomunicaciones o por sus siglas LOT, surge como un instrumento legal que regula todo lo referente al sector de las telecomunicaciones; como garantizar los derechos de los ciudadanos, establecer principios, medidas de seguridad y obligaciones que deben de cumplir las empresas. Si bien su enfoque recae sobre las telecomunicaciones, la LOT contempla algunos puntos que se relacionan con la protección de datos personales, situándola como una normativa anterior o preexistente a la LOPDP. Por ende, es importante analizar y entender la relación entre los artículos de la LOT y la LOPDP. Esta relación permitirá hacer una evaluación a la empresa Cabletel, determinando si antes de la instauración de la LOPDP la empresa ya cumplía con las disposiciones establecidas en la LOT sobre la protección de datos personales. A continuación, en la tabla 5 se muestra el análisis comparativo entre la LOT y la LOPDP [28]:

Tabla 5: Relación de artículos LOT y LOPDP

ARTICULOS DE LA LOT	ARTICULOS DE LA LOPDP

Artículo 24.- Obligaciones de los prestadores de servicios de telecomunicaciones (4. Respetar los derechos de los usuarios establecidos en esta Ley y en el ordenamiento jurídico vigente. 14. Adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados, de conformidad con esta Ley, su Reglamento General y las normas técnicas y regulaciones respectivas.)	Art. 10, 37, 39, 47
Artículo 78.- Derecho a la intimidad (1. Solo el personal autorizado tendrá acceso a los datos personales. 3. Aplicación de una política de seguridad con respecto al tratamiento de datos personales.)	Art. 37, 41, 47
Artículo 79.- Deber de información (Notificación de violación de los datos al titular)	Art. 46
Artículo 82.- Uso comercial de datos personales (Consentimiento necesario)	Art. 8

El análisis de la tabla 5 evidencia una notable relación entre ambas normativas. En más detalle, se identificaron 7 artículos de la LOPDP que tienen una similitud con las disposiciones de la LOT. Esta relación sugiere que las empresas que previamente habían adoptado con los artículos de la LOT, tal como se detallan en la tabla estarían cumpliendo con los de la LOPDP. Por lo tanto, aquellas empresas que ya hubieran integrado a sus prácticas las estipulaciones de la LOT contarían con una base hacia el cumplimiento de los requisitos establecidos en la LOPDP.

3.3 RELACIÓN ENTRE LA LOPDP Y LOS DOMINIOS DE LA NORMA ISO/IEC 27002

Como ya se había descrito en capítulos anteriores, la LOPDP es una normativa que establece los derechos, requisitos y obligaciones que regulan el manejo adecuado de los datos personales. Por otra parte, la ISO/IEC 27002 es una norma reconocida en cuanto a las mejores prácticas para la gestión de la seguridad de la información.

La información se está convirtiendo en otro activo valioso para las organizaciones, por lo que es fundamental emplear medidas de protección y darles un manejo adecuado. En este punto, se hace necesario que la LOPDP y la ISO/IEC 27002 converjan para establecer una sólida relación entre los controles y las medidas de seguridad que salvaguarden la información personal.

La ISO/IEC 27002 contiene un conjunto de objetivos de control que podrían ayudar a las organizaciones a cumplir con los requisitos de la LOPDP; es así que, la relación entre ambas normativas es importante para poder alinear las políticas legales con las mejores prácticas de la gestión de la seguridad de la información. Por lo tanto, la identificación y aplicación adecuada de los objetivos de control de la norma ISO/IEC 27002 va a facilitar el cumplimiento de la LOPDP.

A continuación, se mostrará la ilustración 4 que contrasta los requisitos del artículo 47 de la LOPDP con los dominios de la ISO/IEC 27002, con el propósito de identificar qué dominios de la norma ISO pueden asegurar el acatamiento de los requisitos estipulados en la Ley.

	Dominio Identificado
	Todos podrían ser relevantes

Requisitos de la LOPDP (Art. 47)	Políticas de seguridad	Aspectos organizativos de la seguridad de la información	Seguridad ligada a los recursos humanos	Gestión de activos	Control de accesos	Cifrado	Seguridad física y ambiental	Seguridad en la operativa	Seguridad en las telecomunicaciones	Adquisicion, desarrollo y mantenimiento de los sistemas de informacion	Relaciones con suministradores	Gestion de incidentes en la seguridad de la informacion	Aspectos de seguridad de la informacion en la gestion de la continuidad del negocio	Cumplimiento
Punto 1														
Punto 2														
Punto 3														
Punto 4														
Punto 5														
Punto 6														
Punto 7														
Punto 8														
Punto 9														
Punto 10														
Punto 11														
Punto 12														
Punto 13														
Punto 14														
Punto 15														

Ilustración 4: Relación LOPDP y los dominios de la norma ISO/IEC 27002

La ilustración 4 evidencia la interconexión entre los requisitos estipulados por la ley y los dominios de la norma ISO/IEC 27002. En la ilustración no solo refleja la conexión, sino que también destaca la viabilidad de utilizar los dominios de la norma ISO para asegurar el cumplimiento de las disposiciones legales vigentes. Es decir, la norma ISO no solo sirve como un estándar de gestión de la seguridad de la información, si no como un medio estratégico para alinear las operaciones, practicas o procesos empresariales con los mandatos de la ley vigente, reforzando así la integridad y confiabilidad de las gestiones en cuestión de la protección de datos.

3.4 IDENTIFICACIÓN DE LOS OBJETIVOS DE CONTROL DE LA NORMA ISO/IEC 27002

La norma ISO/IEC 27002 emerge como una herramienta vital para la implementación efectiva de controles de seguridad, siendo esencial en las organizaciones para que alineen sus objetivos de control con las demandas regulatorias. Es aquí donde el documento "Guía de controles de ciberseguridad para la protección integral de la PYME" se vuelve relevante, porque es su sección 6.2 establece la relación entre la GDPR y la norma ISO/IEC 27002:2013, e identifica de forma detallada los objetivos de control con los artículos de la GDPR [29].

Teniendo en cuenta la sección 6.2 y luego de haber establecido la relación entre la GDPR y la LOPDP en la tabla 4, se puede determinar los objetivos de control necesarios para los artículos relacionados con los requisitos de la LOPDP. Ver tabla 6.

Tabla 6: Artículos de la LOPDP con sus respectivos objetivos de control

ARTÍCULOS DE LA LOPDP	OBJETIVOS DE CONTROL DE LA NORMA ISO 27002:2013
Art. 8	5.1 – 14.1 – 18.1
Art. 10	5.1 – 6.1 – 8.1 – 8.2 – 9.2 – 9.3 – 9.4 – 10.1 – 14.3 – 17.1
Art. 12	5.1 – 8.2 – 8.3 – 12.1 – 14.1
Art. 13	5.1 – 8.1 – 8.2 – 12.1 – 13.2 – 14.1 – 15.1
Art. 14	5.1 – 8.1 – 8.2 – 12.1 – 12.3 – 13.2 – 14.1 – 15.1
Art. 15	5.1 – 8.1 – 8.2 – 8.3 – 12.1 – 12.3 – 13.2 – 14.1
Art. 16	5.1 – 8.1 – 8.2 – 12.1 – 12.3 – 13.2 – 14.1 – 15.1
Art. 17	5.1 – 8.3 – 13.1 – 13.2 – 14.1 – 15.1
Art. 19	5.1 – 8.1 – 8.2 – 12.1 – 12.3 – 13.2 – 14.1 – 15.1
Art. 20, 21	5.1 – 8.2 – 12.1 – 13.2 – 14.1 – 15.1
Art. 26	5.1 – 8.2 – 8.3 – 12.1 – 13.2 – 14.3 – 15.1

Art. 37	Todos los objetivos de control podían ser relevantes
Art. 39	Todos los objetivos de control podrían ser relevantes
Art. 42	5.1 – 6.1 – 8.2 – 12.1 – 13.1 – 14.1 – 15.1
Art. 43	5.1 – 16.1 – 18.1
Art. 46	5.1 – 16.1 – 18.1
Art. 48	5.1 – 6.1 – 18.1
Art. 51	5.1 – 6.1 – 12.1 – 12.4

Luego de elaborar la tabla 6, se hace evidente que existen objetivos de control que se mencionan reiteradamente en diversos artículos. Con el propósito de proporcionar una perspectiva más clara y estructurada, se presenta en la tabla siguiente un resumen:

Tabla 7: Resumen de los objetivos de control

NUMERACIÓN DEL OBJETIVO DE CONTROL	NOMBRE DEL OBJETIVO DE CONTROL
5.1	Directrices de la Dirección en seguridad de la información
6.1	Organización interna
7.1	Antes de la contratación
8.1	Responsabilidad sobre los activos
8.2	Clasificación de la información
8.3	Manejo de los soportes de almacenamiento
9.2	Gestión de acceso de usuario
9.3	Responsabilidades del usuario
9.4	Control de acceso a sistemas y aplicaciones
10.1	Controles criptográficos
12.1	Responsabilidades y procedimientos de operación

12.3	Copias de seguridad
12.7	Consideraciones de las auditorias de los sistemas de información
13.1	Gestión de la seguridad en las redes
13.2	Intercambio de información con partes externas
14.1	Requisitos de seguridad de los sistemas de información
14.3	Datos de prueba
15.1	Seguridad de la información en las relaciones con suministradores
16.1	Gestión de incidentes de seguridad de la información y mejoras
17.1	Continuidad de la seguridad de la información
18.1	Cumplimiento de los requisitos legales y contractuales

Mediante la identificación de estos objetivos de control, se encuentra la base para estructurar la encuesta dirigida a Cabletel. Este instrumento permitirá discernir no solo si la empresa ha integrado en su totalidad dichos objetivos, sino también evidenciar áreas de mejora o aspectos pendientes para garantizar el pleno cumplimento. Es primordial recalcar que cada uno de estos objetivos de control puede estar compuesto por uno o varios controles específicos. Por ello, tanto la estructura de la encuesta como las preguntas que la conforman están basadas en la ISO/IEC 27002, garantizando así un análisis completo y alineado con los estándares internacionales de seguridad de la información.

3.5 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA EMPRESA CABLETEL

El uso de la tecnología en la sociedad requiere que las empresas, como Cabletel almacenen, procesen y utilicen cantidades de datos de sus usuarios. Esto ha planteado desafíos en lo que respecta a la seguridad y resguardo de la información personal, que evite violaciones de seguridad que pueden tener graves consecuencias tanto para las empresas como para sus clientes. El análisis de las prácticas, procesos y protocolos actuales son importantes. En esta sección se llevará a cabo una revisión de la situación actual de Cabletel con respecto a las medidas previamente adoptadas por la empresa antes de la implementación de la LOPDP y la gestión de la seguridad de la información en relación con los objetivos de control de la norma ISO/IEC 27002:2013. Dicha norma proporciona directrices sobre controles que pueden ser implementados en las organizaciones. El propósito de este análisis es identificar tanto las áreas de fortaleza como las debilidades en las operaciones actuales de Cabletel, estableciendo así un punto de partida que orientará las recomendaciones futuras.

3.5.1 ANÁLISIS DE LAS MEDIDAS PREVIAS A LA LOPDP

Como ya se dijo anteriormente, la empresa Cabletel tendría que haber adoptado medidas para cumplir con las normativas preexistentes a la LOPDP, siendo la LOT la principal normativa de referencia en este contexto. Antes, ARCOTEL era el organismo encargado de establecer, reglamentar los mecanismos y controlar el cumplimiento de las empresas en correspondencia a las obligaciones de seguridad y privacidad de los datos personales. Sin embargo, con la promulgación de la LOPDP se introdujeron nuevas disposiciones reformatorias, desplazando las responsabilidades de ARCOTEL. Estas reformas excluyeron la supervisión de la seguridad de los datos personales de su ámbito de competencia, centrándose su función exclusivamente en el sector de las telecomunicaciones.

Realizada la relación entre la LOT y la LOPDP, se diseñaron preguntas destinadas al encargado del Departamento de TIC's de Cabletel en base a las disposiciones de protección de datos de la LOT, con el objetivo de obtener un panorama claro sobre la adaptación y cumplimiento de la empresa frente a la normativa, lo que se puede observar en el anexo 1. A continuación, se presenta la ilustración 5 con las respuestas obtenidas después de haber realizado la encuesta de manera presencial para garantizar la veracidad de la información.

UNIVERSIDAD CATOLICA DE CUENCA SEDE AZOGUES

ENCUESTA A LA EMPRESA CABLETEL SOBRE LAS ACCIONES PREVIAS A LA LOPDP

	SI	NO
1. ¿Ha adoptado o implementado medidas esenciales para la protección de los datos personales de sus clientes?	x	
2. ¿Dispone de un sistema o responsable designado para garantizar el acceso a los datos únicamente a individuos autorizados?	x	
3. ¿Ha establecido políticas de seguridad relacionadas con el tratamiento de datos personales?	x	
4. ¿Posee un mecanismo para alertar al titular de los datos en caso de que se detecte una vulnerabilidad en sus datos personales?		x
5. ¿Solicita el consentimiento de clientes antes de proceder al tratamiento de sus datos personales?	x	

Ilustración 5: Primera encuesta respondida

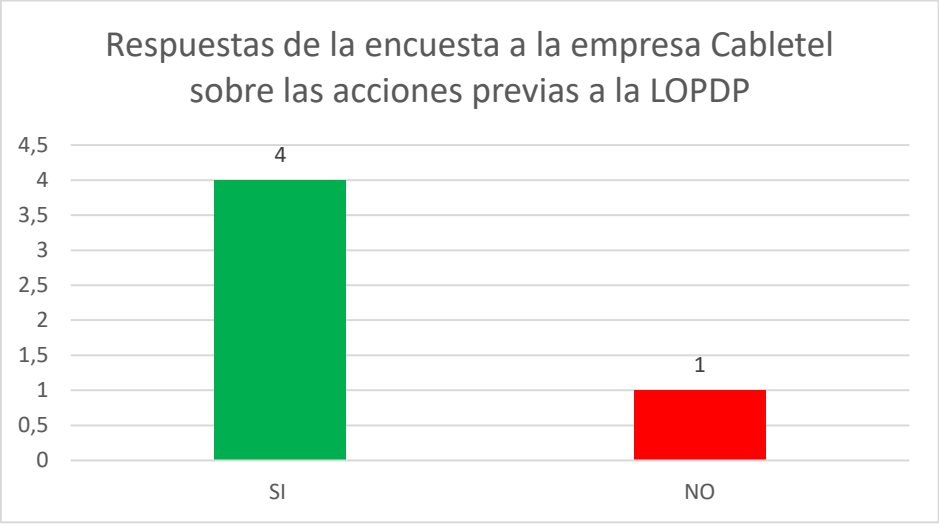

Ilustración 6: Cantidad de acciones implementadas previas a la LOPDP

La ilustración 5 muestra las respuestas obtenidas, se observa que la empresa ha acatado con las disposiciones de la normativa LOT. Tanto en las medidas implementadas para proteger los datos personales, garantizar el acceso solo a individuos autorizados, establecer las políticas

de seguridad en relación con el tratamiento de datos y solicitar el consentimiento de los clientes previo a tratar sus datos. Sin embargo, hay una carencia en cuanto a la alerta al titular de los datos en caso de detección o vulnerabilidad. A partir de la encuesta realizada, se puede determinar que Cabletel ha logrado adaptarse en un 80% a las disposiciones estipuladas por la normativa LOT. Esta cifra no solo refleja el compromiso y esfuerzo de la empresa en alinearse a los estándares establecidos, sino que también indica que tiene una base en lo que respecta a la protección de datos personales. De igual manera, se identifica que la empresa está en concordancia con algunos puntos establecidos por la LOPDP. Es decir que la empresa no solo se ha alineado con una normativa, sino que está encaminado hacia el cumplimiento de las disposiciones más recientes en protección de datos.

3.5.2 ANÁLISIS DE LOS CONTROLES DE LA NORMA ISO/IEC 27002

En el contexto de gestión y seguridad de la información, la norma ISO/IEC 27002 emerge como una de las referencias más destacadas. Esta norma no solo establece las directrices, sino que también proporciona varios controles, objetivos de control y dominios que las organizaciones pueden adoptar para asegurar la integridad, confidencialidad y disponibilidad de la información. En esta sección, el análisis y enfoque estarán orientados hacia la evaluación de los controles que tendría Cabletel, esto debido a que en la tabla 7 se identificaron los objetivos de control. Esta evaluación permitió identificar en qué medida la empresa esta alineada con estos estándares internacionales y como estos pueden reforzar las medidas tomadas bajo la LOPDP.

Para la realización de este análisis, se recurrió al documento “Aplicación de la norma ISO 27002 para mejorar la seguridad de la información de la empresa COMPURED SAC”. Este trabajo es importante dado que proporciona una estructura diseñada con preguntas, estas

están contenidas dentro de una guía de observación que abarca todos los dominios y controles de la norma ISO/IEC 27002. El autor de dicho estudio empleó esta estructura para conducir su investigación y llegar a sus conclusiones [30].

Después de una revisión se seleccionó ciertas preguntas de dicha guía que se alineaban con los objetivos de control que están detallados en la tabla 7. Estas preguntas fueron primordiales para estructurar la segunda encuesta que va a ser dirigida al encargado del Departamento de TIC's de Cabletel. El diseño completo de la encuesta está disponible y se la puede observar en el anexo 2. A continuación, se muestra la ilustración 7 con los resultados obtenidos después de haber realizado la encuesta.

UNIVERSIDAD CATOLICA DE CUENCA SEDE AZOGUES

ENCUESTA A LA EMPRESA CABLETEL SOBRE LOS CONTROLES DE LA NORMA ISO/IEC 27002

	CUMPLE	PARCIALMENTE	NO CUMPLE
5. POLITICAS DE SEGURIDAD			
1. ¿La empresa cuenta con políticas de la seguridad de la información definidas, aprobadas, publicadas y comunicadas a los empleados?	x		
2. ¿Las políticas de seguridad de la información de la empresa se planifican y revisan con regularidad para verificar su efectividad?	x		
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
1. ¿Las responsabilidades para la seguridad de la información en la empresa están definidas y asignadas?			X
2. ¿Las tareas y las áreas de responsabilidad de la empresa se encuentran segregadas?	x		
3. ¿Se mantiene contacto apropiado con las autoridades pertinentes?	x		
4. ¿Se mantiene contacto con grupos o foros de seguridad especializados y asociaciones profesionales?			X
5. ¿Se revisa la seguridad de la información cuando la empresa desarrolla un proyecto?	x		
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
1. ¿Se realizan revisiones de verificación de antecedentes de los candidatos a un empleo de acuerdo con las políticas de la empresa?	x		
2. ¿Los empleados, contratistas y terceros aceptan y firman los términos y condiciones de contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de la información?	x		
8. GESTIÓN DE ACTIVOS			
1. ¿Todos los activos de información de la empresa se encuentran identificados, confeccionando y manteniendo un inventario de los más importantes?	x		
2. ¿Toda la informacion y activos del inventario pertenecen a un área designado de la organización?			X
3. ¿Se ha identificado, documentado e implantado regulaciones para el uso adecuado de los activos de información?	x		
4. ¿Se devuelven todos los activos de la empresa que estén en posesión/responsabilidad de los empleados y usuarios una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo?	x		
5. ¿La información se encuentra clasificada en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización?	x		
6. ¿Se ha desarrollado e implementado un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información de acuerdo con un esquema de clasificación adoptado por la empresa?	x		

7. ¿Se ha desarrollado e implantado procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la empresa?			x
8. ¿Existen procedimientos establecidos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización?			x
9. ¿Se elimina los medios de forma segura y sin riesgo cuando ya no son requeridos usando procedimientos formales?	x		
10. ¿Se encuentran protegidos los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la empresa?	x		
9. CONTROL DE ACCESO			
1. ¿Existe un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso?	x		
2. ¿La empresa cuenta con la implementación de un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios?	x		
3. ¿La asignación y uso de derechos de acceso con privilegios especiales en la empresa está restringido y controlado?	x		
4. ¿Existe un proceso de gestión controlado en la asignación de información confidencial para autenticación?	x		
5. ¿Los propietarios de los activos revisan con regularidad los derechos de accesos de los usuarios?	x		
6. ¿Se retiran o revisan en caso de cambio los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo?	x		
7. ¿Se exige a los trabajadores de la empresa el uso de buenas practicas de seguridad en el uso de información confidencial para la autenticación?	x		
8. ¿Se restringe el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida?	x		
9. ¿La empresa controla el acceso a los sistemas y aplicaciones mediante un procedimiento de log-on?	x		
10. ¿Los sistemas de gestión de contraseñas de la empresa aseguran contraseñas de calidad?			x
11. ¿Se encuentra restringido y controlado el uso de utilidades de software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas de la empresa?	x		
12. ¿Se restringe el acceso al código fuente de las aplicaciones software de la empresa?	x		
10. CIFRADO			
1. ¿La empresa ha desarrollado e implementado una política que regule el uso de controles criptográficos para la protección de la información?	x		
2. ¿La empresa ha desarrollado e implementado una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida?			x
12. SEGURIDAD EN LA OPERATIVA			
1. ¿Se documentan y se dejan a disposición los procedimientos operativos a todos los usuarios que lo necesiten?			x

2. ¿Se controlan los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información?	x		
3. ¿Se monitorea y ajusta el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas?	x		
4. ¿Los entornos de desarrollo, pruebas y operacionales de la empresa permanecen separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional?	x		
5. ¿La empresa realiza copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida?	x		
6. ¿Se planifican y acuerdan los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio?	x		
13. SEGURIDAD EN LAS TELECOMUNICACIONES			
1. ¿Se administra y controlan las redes para proteger la información en sistemas y aplicaciones?	x		
2. ¿Se identifican e incluyen en los acuerdos de servicio, los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados?			x
3. ¿Se encuentran segregadas las redes en función a los grupos de servicios, usuarios y sistemas de información?	x		
4. ¿Existen políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación?			x
5. ¿Los acuerdos de la empresa abordan la transferencia segura de información comercial entre la organización y las partes externas?	x		
6. ¿Se protege adecuadamente la información referida en la mensajería electrónica?			x
7. ¿Se identifican, revisan y documentan de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información?	x		
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN			
1. ¿La empresa incluye los requisitos relacionados con la seguridad de la información en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes?	x		
2. ¿La empresa protege la información de los servicios de aplicación que pasan a través de redes publicas contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada?	x		
3. ¿La empresa protege la información en transacciones de servicios de aplicación para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción?	x		
4. ¿Se seleccionan cuidadosamente, protegen y controlan los datos de prueba?	x		
15. RELACIONES CON SUMINISTRADORES			
1. ¿Se acuerdan y documentan adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas?	x		

2. ¿Se establecen y acuerdan todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización?	x		
3. ¿Los acuerdos con los proveedores incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones?	x		
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN			
1. ¿La empresa establece las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?	x		
2. ¿Se informan los eventos de seguridad de la información lo antes posible utilizando los canales de administración adecuados?	x		
3. ¿Se anota e informa sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización?			x
4. ¿Se evalúan los eventos de seguridad de la información y se deciden su clasificación como incidentes?	x		
5. ¿La empresa responde ante los incidentes de seguridad de la información en atención a los procedimientos documentados?	x		
6. ¿La empresa utiliza el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la portabilidad y/o impacto de incidentes en el futuro?	x		
7. ¿La empresa define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia?	x		
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			
1. ¿La empresa determina los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre?	x		
2. ¿La empresa establece, documenta, implementa y mantiene los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas?	x		
3. ¿Se verifican regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas?			x
18. CUMPLIMIENTO			
1. ¿La empresa identifica, documenta y mantiene al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatuarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos?	x		
2. ¿La empresa implementa procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original?	x		
3. ¿La empresa protege sus registros contra perdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales?	x		
4. ¿La empresa garantiza la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan?	x		
5. ¿La empresa utiliza controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes?			x

Ilustración 7: Segunda encuesta respondida

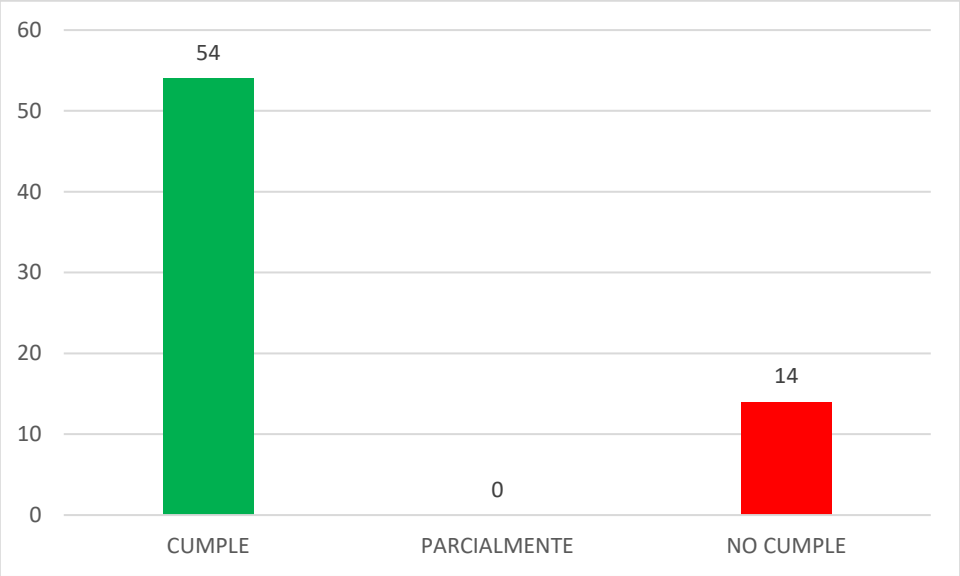

Ilustración 8: Cantidad de controles que cumple la empresa Cabletel

Es esencial destacar que, aunque la organización presenta un nivel de cumplimiento del 79% con respecto a las 54 respuestas de las áreas identificadas de la seguridad de la información, aún existe un 21% con respecto a las 14 respuestas en los cuales se identifican carencias o aspectos de mejora. A continuación, se presenta una descripción de los resultados obtenidos para cada dominio:

- **Políticas de seguridad**

  Cabletel tiene políticas de seguridad definidas, aprobadas y comunicadas. Además, estas políticas son revisadas con regularidad para asegurar su efectividad.

- **Aspectos organizativos de la seguridad de la información**

  Aunque Cabletel mantiene contacto con autoridades pertinentes y considera la seguridad de la información en proyectos, aún no ha definido responsabilidades

específicas para la seguridad de la información ni mantiene contacto con grupos especializados.

- **Seguridad ligada a los recursos humanos**

  La empresa verifica antecedentes de los candidatos, asegura que las condiciones y términos de los contratos estipulen obligaciones de seguridad.

- **Gestión de activos**

  Cabletel tiene un inventario de activos robusto de información importantes y tiene regulaciones sobre su uso. No obstante, hay aspectos como la segregación de información y el manejo de activos según la clasificación que se realizan de manera informal o bajo trabajo.

- **Control de acceso**

  Cabletel tiene procesos robustos en cuanto al control de acceso, pero aún hay oportunidades para mejorar y particularmente en la gestión de contraseñas.

- **Cifrado**

  La empresa utiliza controles criptográficos, pero no tiene una política específica sobre el ciclo de vida de las claves criptográficas.

- **Seguridad en la operativa**

  Hay buenas prácticas en cuanto a la operativa, pero aún no se documentan todos los procedimientos operativos para el acceso universal.

- **Seguridad en las telecomunicaciones**

  Aunque se controlan y segregan las redes, no hay políticas para proteger la transferencia de información ni se garantizan la protección en mensajería electrónica.

- **Adquisición, desarrollo y mantenimiento de los sistemas de información**

Se toman en cuenta las necesidades de seguridad en el desarrollo y mantenimiento, pero hay un área donde la protección de datos se realiza de forma temporal. Por ende, Cabletel debe establecer protocolos permanentes para garantizar la seguridad en todos los aspectos del desarrollo y mantenimiento.

- **Relaciones con suministradores**

  La empresa trabaja activamente para garantizar que los proveedores cumplan con sus requisitos de seguridad.

- **Gestión de incidentes en la seguridad de la información**

  Hay un sólido proceso de gestión de incidentes, pero la empresa no informa debilidades sospechosas a todos los usuarios y contratistas.

- **Aspectos de seguridad de la información en la gestión de la continuidad del negocio**

  La empresa tiene planes para situaciones adversas, pero no revisa regularmente sus controles de continuidad.

- **Cumplimiento**

  Cabletel tiene un enfoque riguroso hacia el cumplimiento, aunque no utiliza controles de cifrado que establecen los acuerdos, la legislación y las normativas pertinentes.

3.5.3 NIVEL DE MADUREZ DE LOS CONTROLES IDENTIFICADOS

En este apartado se realiza una valoración del nivel de madurez actual de la empresa Cabletel con respecto a los objetivos de control que se determinaron previamente; sin embargo, hay que tomar en cuenta que de esos objetivos de control se extienden controles y de los cuales

tenemos 68 identificados. Para llevar a cabo la evaluación se empleará el Modelo de Madurez de Capacidades Integrado (CMMI) y cuya tabla se presenta a continuación:

Tabla 8: CMMI (Niveles, Descripción, Calificación)

NIVEL DE MADUREZ	DESCRIPCION	CALIFICACION
Nivel 0 (Incompleto)	El proceso no se realiza o no se consiguen sus objetivos.	0
Nivel 1 (Ejecutado)	El proceso se ejecuta y se logra su objetivo.	1
Nivel 2 (Gestionado)	El proceso se planifica, se revisa y se evalúa.	2
Nivel 3 (Definido)	Proceso gestionado que se ajusta a la política de procesos.	3
Nivel 4 (Cuantitativamente gestionado)	Proceso definido y se controla utilizando técnicas cuantitativas.	4
Nivel 5 (En Optimización)	El proceso se revisa, se modifica o cambia para adaptarlo a los objetivos del negocio. Mejora continua.	5

Tabla 9: Valoración Políticas de seguridad

POLITICAS DE SEGURIDAD	Situación Inicial	Situación deseada	Valor medio
Conjunto de políticas para la seguridad de la información.	5	5	5
Revisión de las políticas para la seguridad de la información.	5	5	5

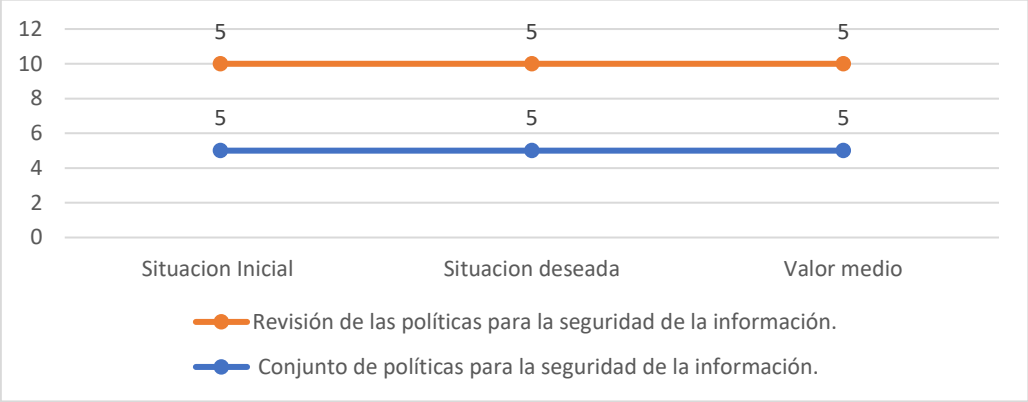

Ilustración 9: Grafica Valoración Políticas de seguridad

En el marco de evaluación de políticas de seguridad de información, se obtuvo la puntuación máxima de 5 indicando que la situación inicial fue considerada altamente efectiva y adecuada para su propósito. Este resultado destaca la robustez y estabilidad del conjunto de políticas de seguridad de la información, teniendo un alto grado de madurez en este aspecto según el CMMI.

Tabla 10: Valoración Aspectos organizativos de la seguridad de la información

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	Situación inicial	Situación deseada	Valor medio
Asignación de responsabilidades para la seguridad de la información	2	4	3
Segregación de tareas.	5	5	5
Contacto con las autoridades	5	5	5
Contacto con grupos de interés especial	1	3	2
Seguridad de la información en la gestión de proyectos.	4	5	4,5

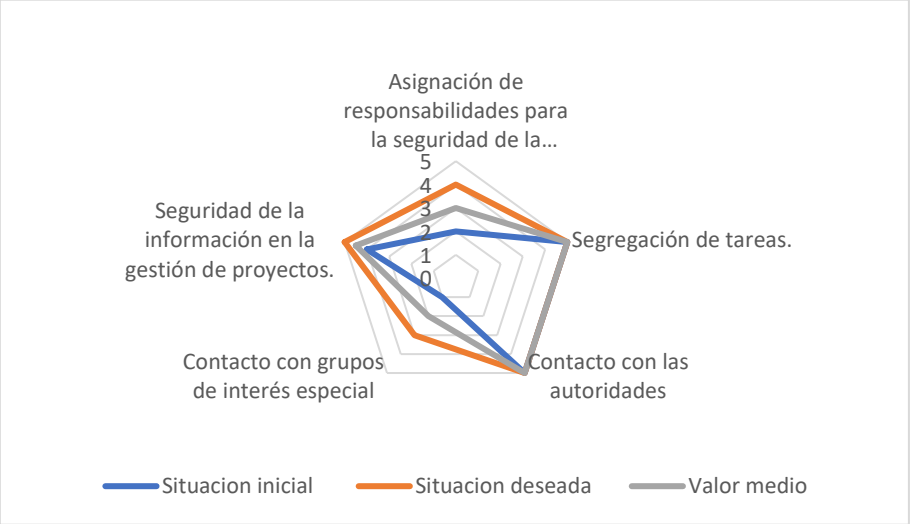

Ilustración 10: Grafica Valoración Aspectos organizativos de la seguridad de la información

En cuanto a la asignación de responsabilidades para la seguridad de la información con una situación inicial de 2, se revelo una mejora significativa en la claridad y eficacia de las responsabilidades asignadas en materia de seguridad de la información. En el caso del contacto con grupos de interés especial, se evidencia un puntaje de 1 que refleja la falta de esfuerzos en fortalecer la relación con otros grupos.

Tabla 11: Valoración Seguridad ligada a los recursos humanos

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	Situación inicial	Situación Deseada	Valor medio
Investigación de antecedentes.	5	5	5
Términos y condiciones de contratación.	3	5	4

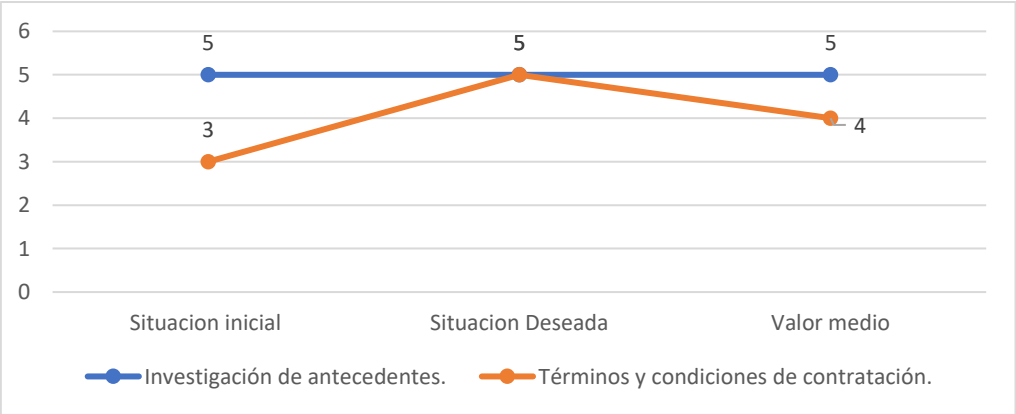

Ilustración 11: Grafica Valoración Seguridad ligada a los recursos humanos

En la definición de antecedentes, la organización mantuvo una posición fuerte desde la situación inicial con una puntuación de 5, indicando un enfoque consistente y exhaustivo en la evaluación de los antecedentes de los recursos humanos. Por otro lado, los términos y condiciones de contratación experimentan y sugieren una atención, lo que contribuye a una gestión más efectiva de los recursos humanos en términos de seguridad.

Tabla 12: Valoración Gestión de activos

GESTIÓN DE ACTIVOS	Situación inicial	Situación Deseada	Valor medio
Inventario de activos.	5	5	5
Propiedad de los activos.	1	3	2
Uso aceptable de los activos.	4	5	4,5
Devolución de activos.	5	5	5
Directrices de clasificación.	5	5	5
Etiquetado y manipulado de la información.	3	5	4
Manipulación de activos	2	4	3
Gestión de soportes extraíbles	1	3	2
Eliminación de soportes.	4	5	4,5
Soportes físicos en tránsito.	4	5	4,5

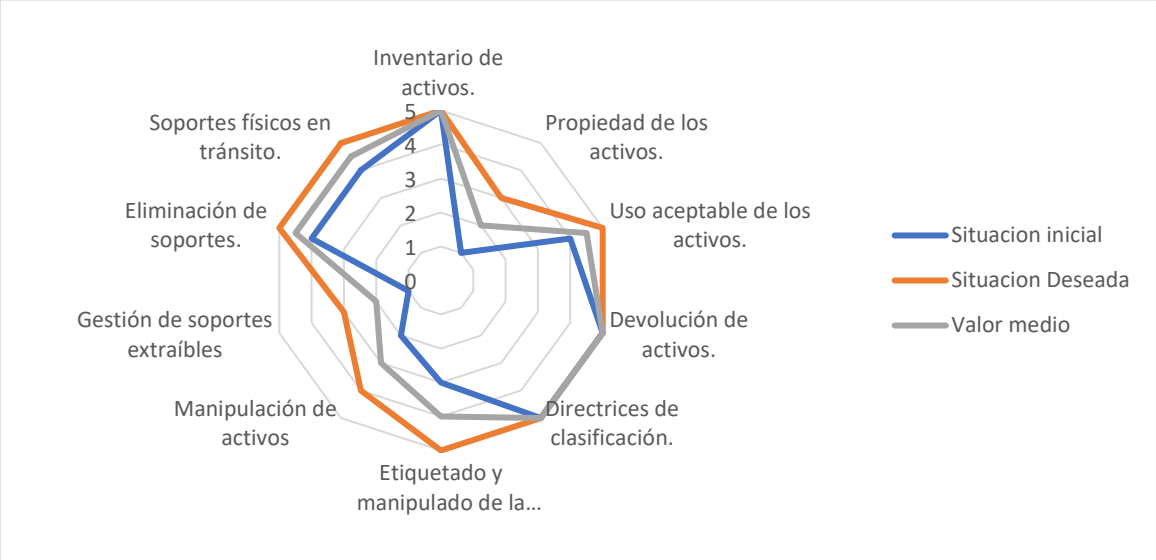

Ilustración 12: Grafica Valoración Gestión de activos

La gestión de activos muestra un buen desempeño general, con áreas destacadas en el inventario y aspectos a mejorar en la propiedad de los activos, manipulación de activos, gestión de soportes

extraíbles y eliminación de soportes. Estos resultados proporcionan una base para fortalecer aún más la seguridad y eficiencia en la gestión de los activos dentro de la empresa.

Tabla 13: Valoración Control de acceso

CONTROL DE ACCESO	Situación inicial	Situación Deseada	Valor medio
Gestión de altas/bajas en el registro de usuarios.	5	5	5
Gestión de los derechos de acceso asignados a usuarios.	3	5	4
Gestión de los derechos de acceso con privilegios especiales.	4	5	4,5
Gestión de información confidencial de autenticación de usuarios.	4	5	4,5
Revisión de los derechos de acceso de los usuarios	5	5	5
Retirada o adaptación de los derechos de acceso	5	5	5
Uso de información confidencial para la autenticación.	4	5	4,5
Restricción del acceso a la información.	4	5	4,5
Procedimientos seguros de inicio de sesión.	5	5	5
Gestión de contraseñas de usuario.	2	4	3
Uso de herramientas de administración de sistemas.	5	5	5
Control de acceso al código fuente de los programas.	5	5	5

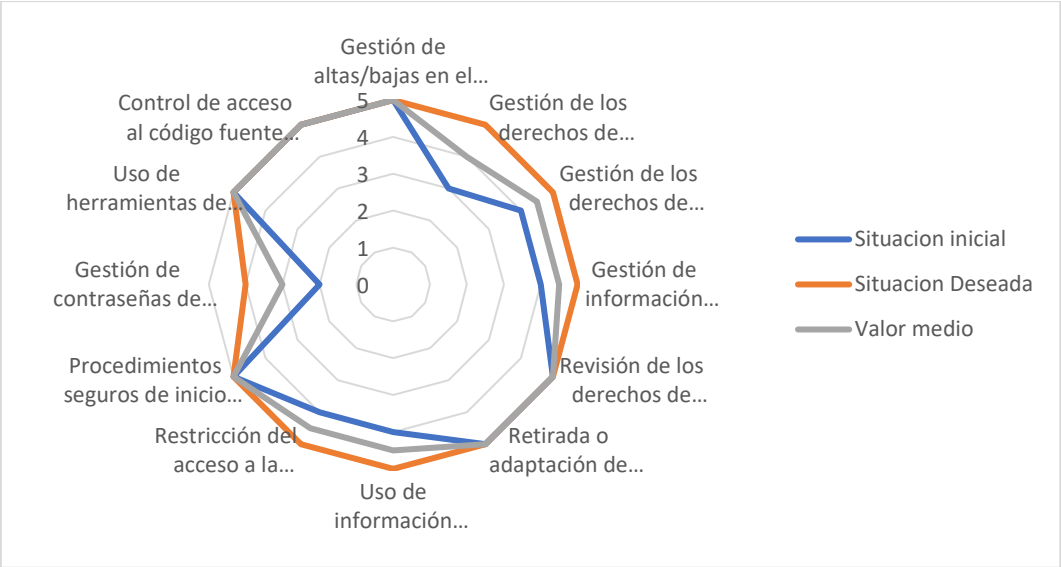

Ilustración 13: Grafica Valoración Control de acceso

El control de accesos exhibe áreas de fortaleza en la gestión de altas/bajas, revisión de derechos de acceso, retirada o adaptación de derechos de acceso y en el uso de las herramientas de administración de sistemas. Al mismo tiempo, se identifican controles de mejora en la asignación de derechos de acceso y la gestión de contraseñas de usuario para crear oportunidades de mejora.

Tabla 14: Valoración Cifrado

CIFRADO	Situación inicial	Situación Deseada	Valor medio
Política de uso de los controles criptográficos.	4	5	4,5
Gestión de claves.	2	4	3

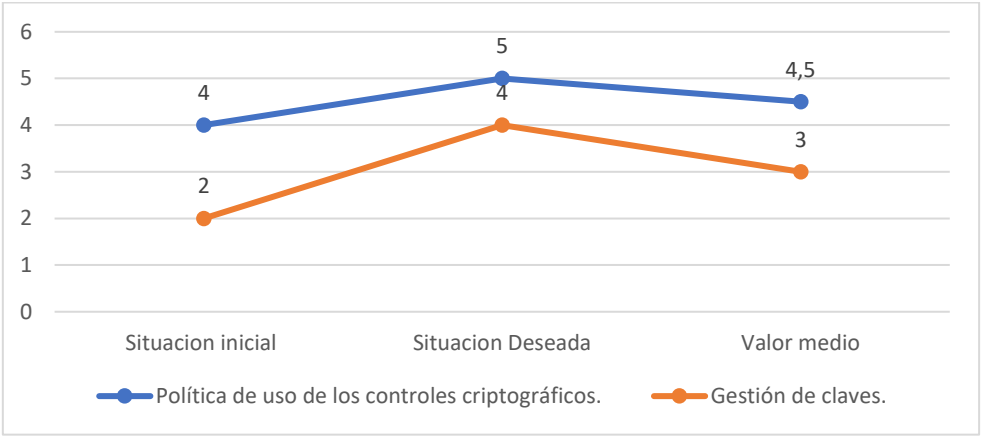

Ilustración 14: Grafica Valoración Cifrado

La empresa ha establecido una política de uso de controles criptográficos con una base sólida, la gestión de claves presenta un área critica que requiere atención y mejora.

Tabla 15: Valoración Seguridad en la operativa

SEGURIDAD EN LA OPERATIVA	Situación inicial	Situación Deseada	Valor medio
Documentación de procedimientos de operación.	2	4	3
Gestión de cambios.	5	5	5
Gestión de capacidades.	4	5	4,5
Separación de entornos de desarrollo, prueba y producción.	5	5	5
Copias de seguridad de la información.	5	5	5
Controles de auditoría de los sistemas de información.	5	5	5

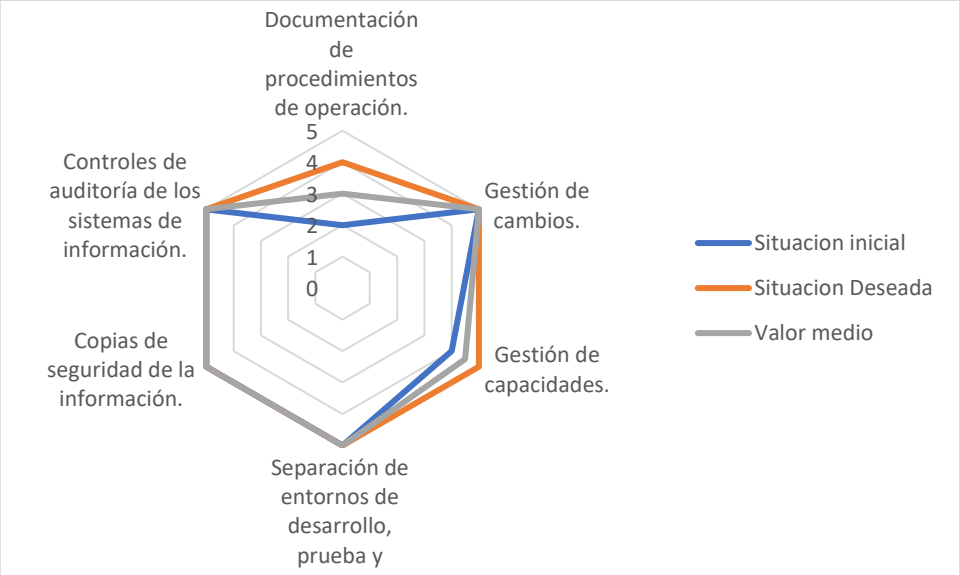

Ilustración 15: Grafica Valoración Seguridad en la operativa

Hay un control que se puede mejorar, como la documentación de procedimientos de operación, pero en si la empresa demuestra un fuerte enfoque en los demás puntos con un alto nivel de madurez.

Tabla 16: Valoración Seguridad en las telecomunicaciones

SEGURIDAD EN LAS TELECOMUNICACIONES	Situación inicial	Situación Deseada	Valor medio

Controles de red.	5	5	5
Mecanismos de seguridad asociados a servicios en red.	2	4	3
Segregación de redes.	3	5	4
Políticas y procedimientos de intercambio de información.	2	4	3
Acuerdos de intercambio.	5	5	5
Mensajería electrónica.	2	4	3
Acuerdos de confidencialidad y secreto	4	5	4,5

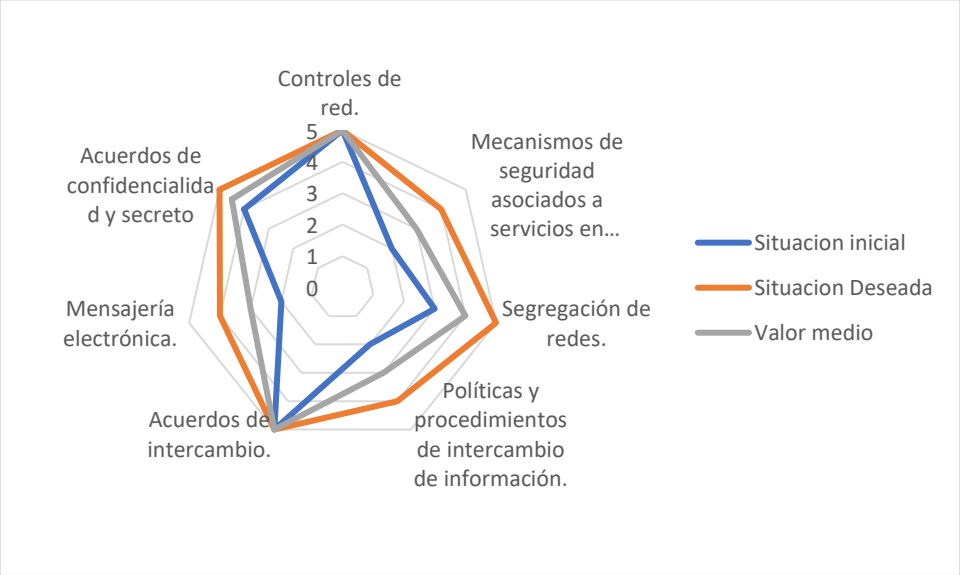

Ilustración 16: Grafica Valoración Seguridad en las telecomunicaciones

La empresa ha trabajado en fortalecer áreas como controles de red, acuerdos de intercambio y acuerdos de confidencialidad, pero aún existen oportunidades para mejorar en otros aspectos como en los mecanismos de seguridad asociados a servicios de red, segregación de redes, políticas y procedimientos de intercambio y mensajería electrónica.

Tabla 17: Valoración Adquisición, desarrollo y mantenimiento de los sistemas de información

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	Situación inicial	Situación Deseada	Valor medio
Análisis y especificación de los requisitos de seguridad.	5	5	5

Seguridad de las comunicaciones en servicios accesibles por redes públicas.	4	5	4,5
Protección de las transacciones por redes telemáticas.	5	5	5
Protección de los datos utilizados en pruebas.	3	5	4

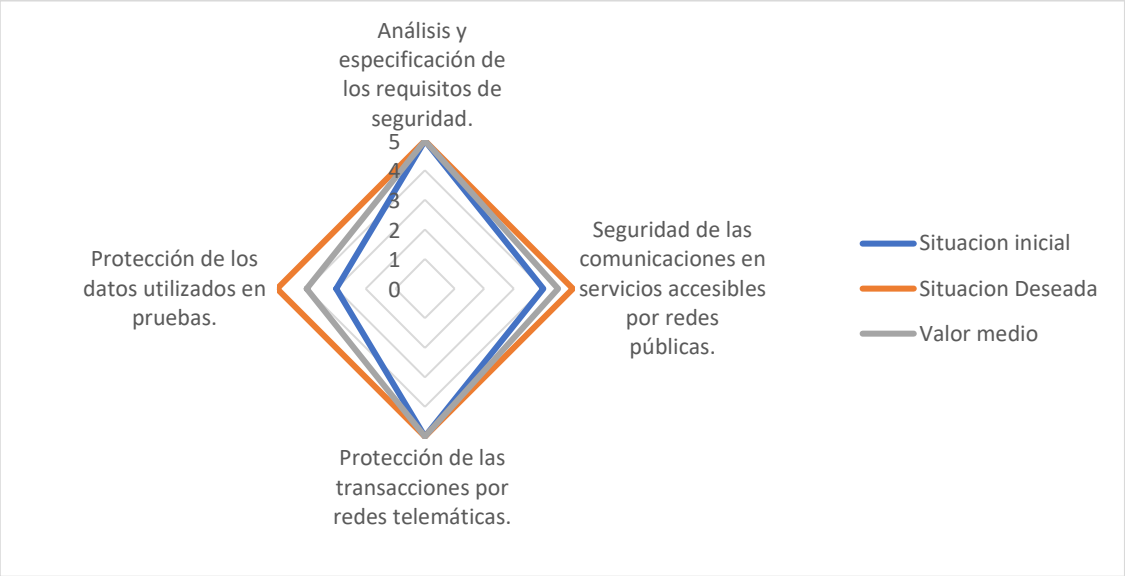

Ilustración 17: Grafica Valoración Adquisición, desarrollo y mantenimiento de los sistemas de información

Existe solo un área de mejora identificada en la protección de los datos utilizados en pruebas, dando como resultado una base para continuar fortaleciendo la seguridad y mantener un buen nivel en este apartado.

Tabla 18: Valoración Relaciones con suministradores

RELACIONES CON SUMINISTRADORES	Situación inicial	Situación Deseada	Valor medio
Política de seguridad de la información para suministradores.	4	5	4,5
Tratamiento del riesgo dentro de acuerdos de suministradores.	4	5	4,5
Cadena de suministro en tecnologías de la información y comunicaciones.	4	5	4,5

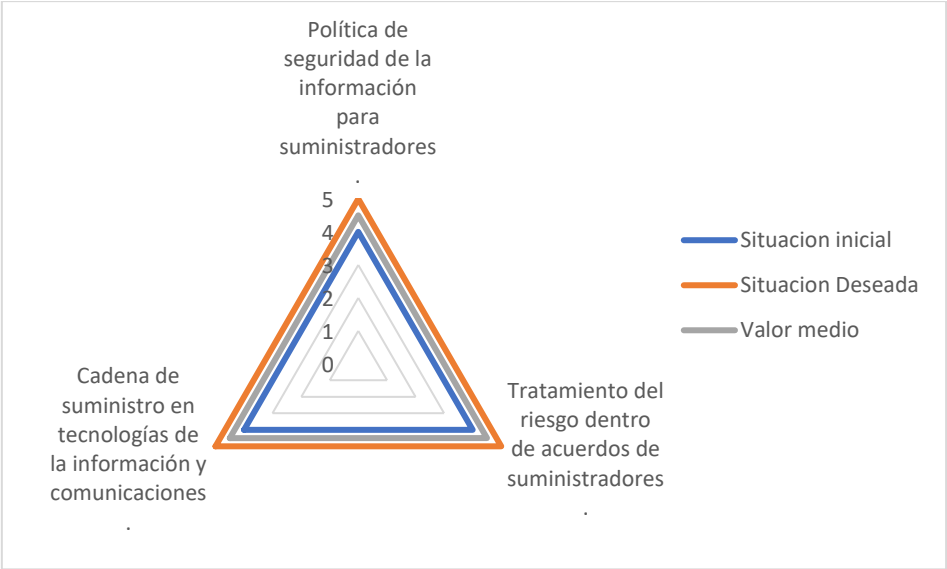

Ilustración 18: Grafica Valoración Relaciones con suministradores

La empresa presenta un desempeño positivo en la formulación de políticas de seguridad para suministradores y en el tratamiento del riesgo. Además, la gestión de la cadena de suministro en tecnologías de la información muestra un buen equilibrio.

Tabla 19: Valoración Gestión de incidentes en la seguridad de la información

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	Situación inicial	Situación Deseada	Valor medio
Responsabilidades y procedimientos.	5	5	5
Notificación de los eventos de seguridad de la información.	5	5	5
Notificación de puntos débiles de la seguridad.	2	4	3
Valoración de eventos de seguridad de la información y toma de decisiones.	5	5	5
Respuesta a los incidentes de seguridad.	5	5	5
Aprendizaje de los incidentes de seguridad de la información.	5	5	5
Recopilación de evidencias.	4	5	4,5

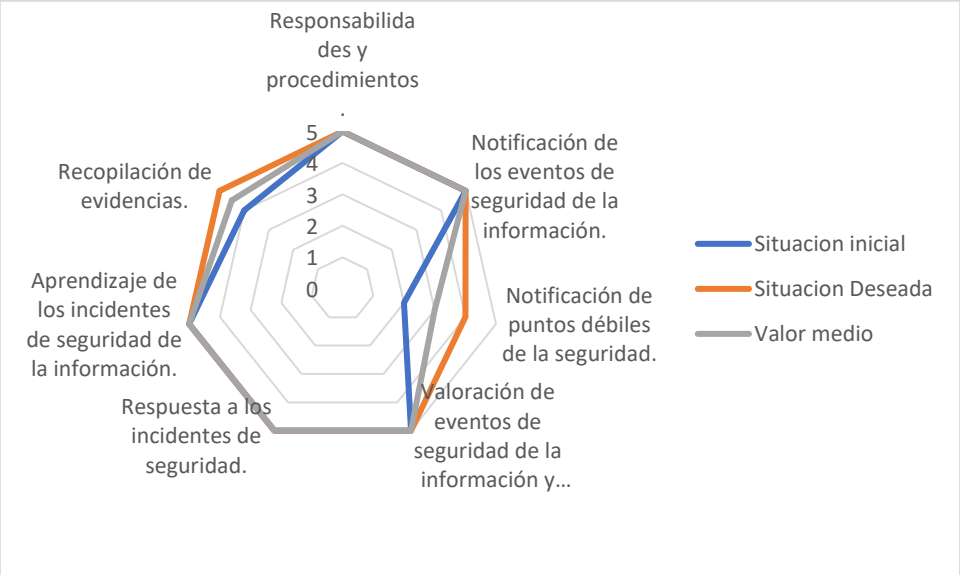

Ilustración 19: Grafica Valoración Gestión de incidentes en la seguridad de la información

La empresa demuestra una gestión robusta de incidentes en la seguridad de la información, pero con áreas específicas de mejora identificadas en la notificación de puntos débiles de la seguridad.

Tabla 20: Valoración Aspectos de seguridad de la información de la gestión de la continuidad del negocio

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Situación inicial	Situación Deseada	Valor medio
Planificación de la continuidad de la seguridad de la información.	5	5	5
Implantación de la continuidad de la seguridad de la información.	5	5	5
Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	2	4	3

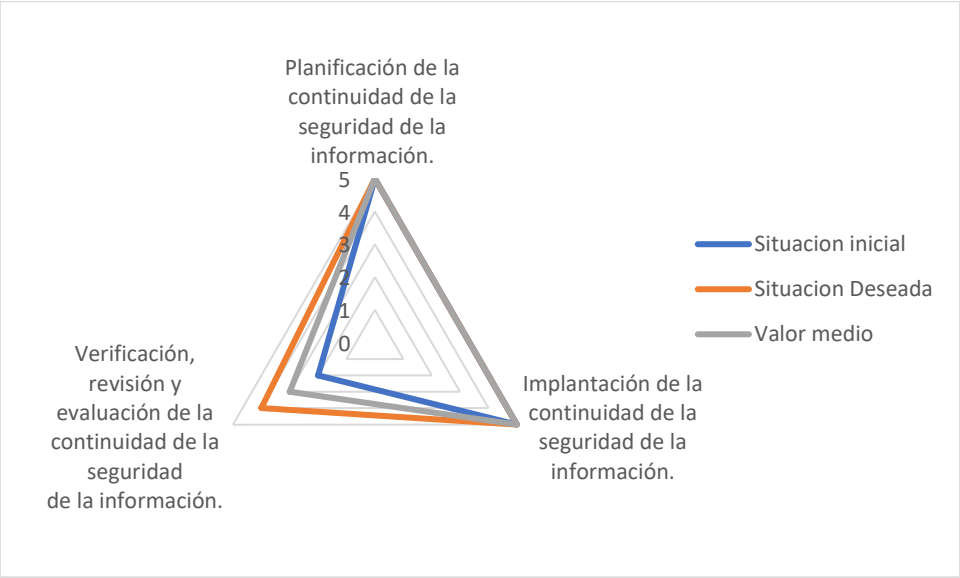

Ilustración 20: Grafica Valoración Aspectos de seguridad de la información de la gestión de la continuidad del negocio

Se tiene un buen nivel de madurez en ciertos controles, pero en contraste con la verificación, revisión y evaluación de la continuidad de la seguridad de la información se obtiene un puntaje de 2. Esto sugiere considerara la implementación de mejoras en los procedimientos de la revisión para garantizar la efectividad continua del plan.

Tabla 21: Valoración Cumplimiento

CUMPLIMIENTO	Situación inicial	Situación Deseada	Valor medio
Identificación de la legislación aplicable.	5	5	5
Derechos de propiedad intelectual (DPI)	5	5	5
Protección de los registros de la organización.	4	5	4,5
Protección de datos y privacidad de la información personal.	4	5	4,5
Regulación de los controles criptográficos.	2	4	3

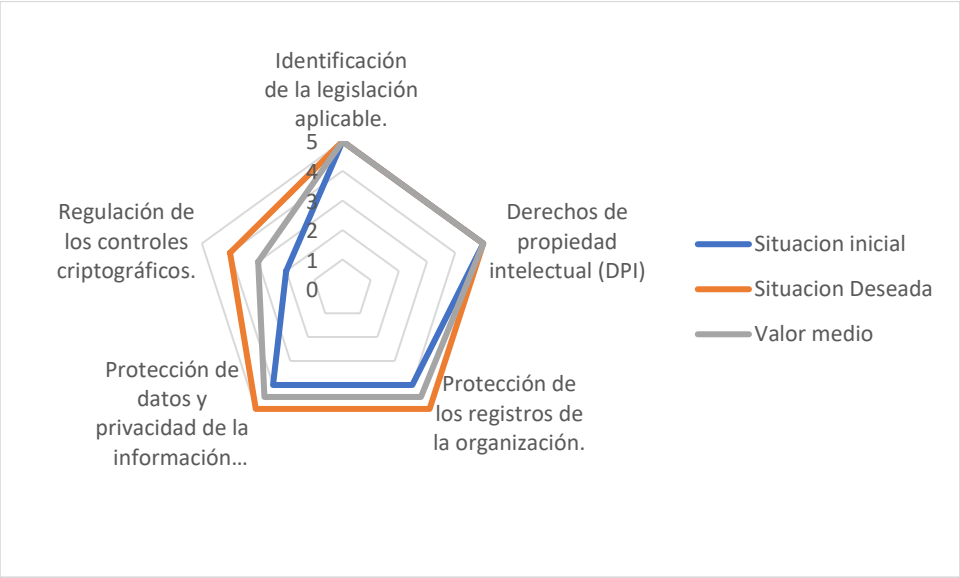

Ilustración 21: Grafica Valoración Cumplimiento

Se percibe un gran compromiso con el tema del cumplimiento, pero se identifican oportunidades de mejora en la regulación de los controles criptográficos, esto indica que la empresa puede adecuarse a prácticas para cumplir con las regulaciones pertinentes.

3.6 RECOMENDACIONES PARA LA ADECUACIÓN DE CABLETEL A LA LOPDP.

El manejo inadecuado de los datos personales o la falta de consideraciones legales puede abarcar sanciones de las leyes y normativas en vigor, multas, daño reputacional o incluso una pérdida de confianza por parte de los clientes y las afectaciones a largo plazo en las operaciones de la empresa. Por ello, es fundamental que las organizaciones y en este caso específico la empresa Cabletel, cuenten con un plan de recomendaciones que sirva de apoyo para el adecuado manejo de los datos personales y la gestión de la seguridad de la información.

Dentro de esta sección, se planteará las recomendaciones que están basadas en el análisis previo realizado en la empresa Cabletel. Esto servirá como soporte para que Cabletel no solo cumpla con la LOPDP y la norma ISO/IEC 27002:2013, sino que vaya un paso más allá y tenga las bases para posibles normativas futuras o establezca un sistema de seguridad de la

información robusta. Las recomendaciones que se presentarán a continuación se dividen en dos categorías. La primera categoría se fundamenta en los resultados obtenidos de la inicial encuesta, mientras que la segunda categoría se enfoca en los resultados derivados de la encuesta subsiguiente.

3.6.1 RECOMENDACIONES BASADAS EN LA LOT

Estas recomendaciones se fundamentan en el análisis, la cual examinó las medidas que Cabletel ya había implementado antes de la entrada en vigor de la LOPDP. En esta parte se hizo visible la carencia de un punto en concreto y que puede ser optimizado o reforzado, también se dará opiniones de los demás puntos.

- **Implementación de un mecanismo de alerta:** Cabletel deberá desarrollar e implementar un sistema que notifique automáticamente a los titulares de los datos en caso de que exista una brecha de seguridad o una vulnerabilidad detectada. Esto no solo ayudara a cumplir con las regulaciones, sino que también a construir confianza con los clientes.
- **Auditorias regulares:** La empresa deberá realizar auditorías externas e internas periódicamente para asegurarse de que las medidas de seguridad son efectivas y se están cumpliendo las políticas y regulaciones.
- **Continua formación:** Realizar capacitaciones para todos los empleados sobre la importancia de la protección de los datos y como asegurar la información de los clientes.
- **Actualización de las políticas:** Revisar y asegurarse de que las políticas de seguridad estén siempre actualizadas con las ultimas regulaciones y prácticas recomendadas.

3.6.2 RECOMENDACIONES BASADAS EN LA NORMA ISO 27002

Este segmento se centra en el análisis sobre los controles existentes dentro de Cabletel. Específicamente se pondrá énfasis en los puntos que indican áreas donde Cabletel aún no ha implementado medidas adecuadas, siendo en total 14 controles faltantes y de los cuales se darán a continuación las siguientes recomendaciones para poder dar cumplimiento y así completar con todos los controles que se requieren para que la empresa se logre alinear a la LOPDP.

- **Aspectos organizativos de la seguridad de la información**

  En este dominio existe la carencia de 2 controles, específicamente el numeral 6.1.1 que hace referencia a la asignación de responsabilidades para la seguridad de la información y el numeral 6.1.4 sobre el contacto con grupos de interés especial. A continuación, se presenta las recomendaciones para poder dar cumplimiento a estos controles.

  1. Definir claramente las responsabilidades relacionadas con la seguridad de la información para cada rol en la empresa.
  2. Proporcionar capacitación especifica basada en esas responsabilidades.
  3. Revisar regularmente estas responsabilidades y ajustarlas según las necesidades de la empresa.
  4. Establecer conexiones con organizaciones o grupos especializados en seguridad de la información.
  5. Participar en conferencias, talleres y seminarios para mantenerse actualizado.

- **Gestión de activos**

  Para la gestión de activos se tiene la ausencia de 3 controles, siendo el numeral 8.1.2 sobre propiedad de los activos, el numeral 8.2.3 sobre la manipulación de activos y el numeral 8.3.1 que hace referencia a la gestión de soportes extraíbles. De igual manera se realiza las siguientes recomendaciones para su cumplimiento.

  1. Identificar y etiquetar todos los activos de información, especificando un propietario o responsable directo para cada uno.
  2. El propietario del activo debería ser responsable de la clasificación, manejo y revisión del mismo.
  3. Establecer procedimientos claros sobre cómo se deben manejar los activos según su clasificación.
  4. Realizar auditorías periódicas para garantizar que los activos se manejen correctamente.
  5. Implementar políticas claras sobre el uso de medios removibles.
  6. Utilizar soluciones tecnológicas para restringir o controlar el uso de medios removibles cuando sea necesario.
  7. Proporcionar capacitación sobre los riesgos asociados con el uso inapropiado de estos medios.

- **Control de acceso**

  Con respecto al control de acceso hay la ausencia de un control, siendo el numeral 9.4.3 sobre la gestión de contraseñas de usuario. A continuación, las respectivas recomendaciones.

  1. Establecer políticas para la creación de contraseñas robustas.

2. Implementar soluciones tecnológicas que obliguen a los usuarios a cambiar las contraseñas regularmente y a seguir las políticas de creación.

- **Cifrado**

  En este dominio existe la falta de un control, siendo el numeral 10.1.2 sobre la gestión de claves, de la misma manera se dejan sus respectivas recomendaciones.

  1. Implementar una política de ciclo de vida de las claves criptográficas.
  2. Considerar soluciones de almacenamiento seguro para las claves, como módulos de hardware de seguridad.

- **Seguridad en la operativa**

  En este apartado hay el incumplimiento de un control, este hace referencia al numeral 12.1.1 sobre la documentación de procedimientos de operación. Siguiendo el mismo orden se dejan las siguientes recomendaciones.

  1. Documentar todos los procedimientos operativos y mantenerlos accesibles para el personal relevante.
  2. Realizar revisiones periódicas de estos documentos y actualizarlos según los cambios en la operativa.

- **Seguridad en las telecomunicaciones**

  Aquí se puede encontrar la ausencia de 3 controles, como el numeral 13.1.2 sobre los mecanismos de seguridad asociados a servicios en red, el numeral 13.2.1 sobre las políticas y procedimientos de intercambio de información y el

numeral 13.2.3 sobre la mensajería electrónica. A continuación, sus recomendaciones.

1. Revisar y documentar los mecanismos de seguridad en los servicios de red.
2. Establecer controles para garantizar que solo se utilicen servicios de red seguros y aprobados.
3. Implementar políticas claras sobre cómo debe transferirse la información.
4. Proporcionar herramientas seguras para la transferencia, como soluciones de cifrado.
5. Implementar soluciones o herramientas para cifrar correos electrónicos que tengan información sensible.
6. Capacitar al personal sobre los riesgos asociados con la mensajería electrónica y como usarlo de manera segura.

- **Gestión de incidentes en la seguridad de la información**

  En este dominio se detecta la falta de implementación de un control, el numeral 16.1.3 que aborda la notificación de puntos débiles de la seguridad de la información. Seguidamente se ofrecen las recomendaciones pertinentes.

  1. Establecer un canal claro y accesible para que el personal informe sobre cualquier debilidad o irregularidad que detecten.
  2. Incentivar al personal a reportar estos hallazgos.

- **Aspectos de seguridad de la información en la gestión de la continuidad del negocio**

En este apartado se ha hecho evidente la ausencia de un control, siendo el numeral 17.1.3 sobre verificación, revisión y evaluación de la continuidad de la seguridad de la información. A continuación, se presentan las recomendaciones pertinentes.

1. Realizar simulacros y pruebas periódicas para verificar los planes de continuidad.
2. Incorporará lecciones aprendidas y actualizar los planes según sea necesario.

- **Cumplimiento**

  Por último, tenemos la falta de implementación de un control, el numeral 18.1.5 sobre la regulación de controles criptográficos. De la misma forma, aquí sus recomendaciones.

  1. Mantenerse al día con la reglamentación sobre controles criptográficos.
  2. Revisar y ajustar las políticas y soluciones de cifrado según las reglamentaciones.

En resumen, es fundamental que Cabletel asuma un enfoque proactivo hacia el acatamiento de los controles de la norma ISO/IEC 27002. Esto incluiría en la revisión regular de las políticas, procedimientos, capacitación del personal y la implementación de soluciones tecnológicas adecuadas para garantizar y reforzar la seguridad de la información.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

En este apartado se llevará a cabo un análisis reflexivo sobre los hallazgos y resultados obtenidos a lo largo de esta investigación realizada. Las conclusiones que a continuación se describen no son observaciones superficiales, estas están basadas en los objetivos específicos que guiaron este estudio desde sus inicios. Estas reflexiones representan la síntesis y la culminación de un esfuerzo investigativo.

- En primer lugar, se llevó a cabo una exploración e investigación de la LOPDP, logrando identificar no solo las sanciones y los requisitos, sino que también sus integrantes y los principios en los que está basado la ley. Esta información resulto esencial para comprender cómo las organizaciones deben operar bajo este marco legal y evitar los posibles contratiempos.
- Se realizó un estudio detallado de los dominios y objetivos de control de la norma ISO/IEC 27002. De esta manera, se pudo establecer un puente entre los requerimientos que tiene la norma y las estipulaciones por parte de la LOPDP, cuya correlación facilita la comprensión y la aplicación de ambas regulaciones en el contexto de esta investigación.
- Para el tercer objetivo, se procedió a recolectar información sobre la situación actual de la empresa en cuanto a la adherencia de leyes preexistentes a la LOPDP y a los objetivos de control identificados. Para entender la realidad interna de la empresa se dió a través de dos encuestas realizadas, que no solo se pudo identificar el nivel de concordancia de la empresa con los estándares y

regulaciones, sino también descubrir áreas de mejora y posibles vulnerabilidades.

- Finalmente, para el ultimo objetivo se tuvo como base los resultados de las encuestas y con ello se sugieren las recomendaciones para garantizar que la empresa cumpla cabalmente con la LOPDP. Este plan proporciona recomendaciones concretas para mejorar áreas específicas y fortalecer la gestión de seguridad de datos personales en toda la empresa.

En resumen, esta investigación no solo proporciono un panorama claro sobe el marco legal y normativo en el espacio de la protección de los datos personales, sino que también ofreció recomendaciones y directrices para que la empresa pueda mejorar y asegura su gestión en este ámbito a través del plan que se está recomendado.

4.2 RECOMENDACIONES

A continuación, se presentarán sugerencias derivadas de los hallazgos de este trabajo. Las recomendaciones tienen como objetivo guiar acciones futuras, proponer mejoras o indicar posibles rutas de investigación.

- Se recomienda que investigaciones futuras se centren en realizar una evaluación del nivel de madurez o eficiencia aún más profunda de los controles identificados en este trabajo. Esto permitirá a la empresa no solo conocer su estado actual en relación con las buenas prácticas, sino también entender que controles requieren mayor atención o fortalecimiento.
- Dado el plan de acción propuesto, un análisis siguiente podría enfocarse en mejorar y optimizar dicho plan. Específicamente en la identificación y

descripción de posibles herramientas tecnológicas o metodologías que se pudiera implementar para hacer realidad cada una de las recomendaciones.

- Dado el cambio dinámico de las leyes o normativas, sería beneficioso realizar una revisión periódica de las mismas, identificando cambios o nuevas disposiciones y como estas afectan o se alinean con las operaciones y políticas internas de la empresa. También se recomienda optar por utilizar metodologías o normativas más actualizadas.

BIBLIOGRAFIA

[1] M. A. Chavez and F. C. Calderon, *Aplicación de la Norma internacional ISO/IEC 27002:2013 para la Seguridad informática de la Unidad de Gestión Educativa Local 'Utcubamba.'* 2022.

[2] D. Murillo, "POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN NORMAS ISO 27002 PARA EL DEPARTAMENTO INFORMÁTICO DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ," pp. 1–84, 2021.

[3] "Influencia de las tecnologías digitales | Naciones Unidas." [Online]. Available: https://www.un.org/es/un75/impact-digital-technologies. [Accessed: 21-Jun-2023].

[4] M. R. Aguilar *et al.*, "Estudios del Desarrollo Social: Cuba y América Latina Protection of Personal Data in Ecuador," *Estud. del Desarro. Soc. Cuba y América Lat. RPNS*, vol. 2346, p. 2022, 2022.

[5] M. Patricia, R. Garzón, D. Paola, and A. Olmos, "SEGURIDAD INFORMÁTICA: RELACIÓN E IMPACTO FRENTE A LA LEY DE PROTECCIÓN DE DATOS PERSONALES (LEY 1581 DE 2012)."

[6] V. N. Pont, D. Ospina-Celis, and J. C. Upegui, "Empresas y datos personales en América Latina."

[7] D. N. de R. P. DINARP, "Beneficios tras la aprobación de la Ley de Protección de Datos Personales." [Online]. Available: https://www.registrospublicos.gob.ec/beneficios-tras-la-aprobacion-de-la-ley-de-proteccion-de-datos-personales/. [Accessed: 26-Aug-2023].

[8] Y. Ramos, O. Urrutia, D. Ordoñez, and A. Bravo, "Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO / IEC 27002 : 2013 para la Cooperativa Codelcauca Adopt an information security policy based on an NTC ISO / IEC 27002 : 2013 standard for the Codelcauca Cooper," *Memorias Congr. UTP*, vol. 1, no. 1, pp. 88–95, 2017.

[9] J. J. RUIZ CONCHA, "MODELO PARA LA IMPLEMENTACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES BASADO EN EL SGSI DE LA NORMA ISO 27001."

[10] "CONSTITUCION DE LA REPUBLICA DEL ECUADOR 2008 Decreto Legislativo 0 Registro Oficial."

[11] "Una vez aprobada, las empresas públicas y privadas deben empezar a aplicar la Ley de Protección de Datos Personales - Dirección Nacional de Registros Públicos." [Online]. Available: https://www.registrospublicos.gob.ec/una-vez-aprobada-las-empresas-publicas-y-privadas-deben-empezar-a-aplicar-la-ley-de-proteccion-de-datos-personales/. [Accessed: 15-Jun-2023].

[12] "Ley de Protección de Datos Personales - Dirección Nacional de Registros Públicos." [Online]. Available: https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/. [Accessed: 15-Jun-2023].

[13] "Dos años tienen las entidades públicas y empresas privadas para adaptar sus procesos, a la Ley de Protección de Datos Personales - Dirección Nacional de Registros Públicos." [Online]. Available: https://www.registrospublicos.gob.ec/dos-anos-tienen-las-entidades-publicas-y-empresas-privadas-para-adaptar-sus-procesos-a-la-ley-de-proteccion-de-datos-personales/. [Accessed: 16-Jun-2023].

[14] Q. Suplemento, "Año II-Nº 459-70 páginas Quito, miércoles 26 de mayo de 2021 ASAMBLEA NACIONAL LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES."

[15] P. Arteaga and M. B. & A. Cia Ltda, *Diseñando el futuro: protección de datos personales*. .

[16] D. G. H. García, "DISEÑO E IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD DE NIVEL 0 A NIVEL1 BASADO EN LAS NORMAS ISO 27002 :2013."

[17] G. A. A. ARÉVALO, "DISEÑO DE UN MODELO PARA LA GESTIÓN DE INCIDENTES EN CIBERSEGURIDAD BASADO EN LA NORMA ISO27002:2013 PARA LA EMPRESA PROYECTOS DE INVERSIÓN VIAL ANDINO S.A.S," 2022.

[18] L. I. Gabriela Álvarez-Lozano and M. I. Santiago Andrade-López, "Políticas de Seguridad de la Información bajo la Norma ISO 27002:2013 para el Gobierno Autónomo Descentralizado del Cantón Biblián," *Polo del Conoc.*, vol. 5, no. 11, pp. 591–621, Nov. 2020.

[19] P. J. Gómez, "Implantación del Reglamento General de Protección de Datos y adaptación al Esquema Nacional de Seguridad de manera integrada en el Sistema de Gestión de Seguridad de la información basado en la ISO 27001," p. 71, 2018.

[20] T. K. S. CHOEZ, "ANÁLISIS DE LA NORMA ISO/IEC 27002:2013 PARA MEJORAR LOS CONTROLES DE LA SEGURIDAD DE LA INFORMACIÓN EN LA SALA DE CÓMPUTO # 14 DE LA CARRERA DE INGENIERÍA EN COMPUTACIÓN Y REDES."

[21] M. Legorreta, "Controles iso 27002." [Online]. Available: https://www.academia.edu/9354293/Controles_iso_27002. [Accessed: 09-Jul-2023].

[22] P. S. P. ORTIZ, "APLICACIÓN DE CONTROLES DEL ESTÁNDAR ISO 27002 PARA LA PREVENCIÓN DE VULNERABILIDADES EN LA PRIVACIDAD DE DATOS EN SERVICIOS WEB DEL FRAMEWORK LARAVEL," 2021.

[23] P. Gonzalez, "Presidente Lasso envió la terna para la Superintendencia de Datos." [Online]. Available: https://www.primicias.ec/noticias/economia/presidente-lasso-terna-superintendencia-datos/. [Accessed: 02-Sep-2023].

[24] D. N. de R. P. DINARP, "Proyecto de Reglamento a la Ley de Protección de Datos Personales es presentado al Ejecutivo." [Online]. Available: https://www.registrospublicos.gob.ec/proyecto-de-reglamento-a-la-ley-de-proteccion-de-datos-personales-es-presentado-al-ejecutivo/. [Accessed: 02-Sep-2023].

[25] "REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO."

[26] A. G. Marcén, "EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS COMO MODELO DE LAS RECIENTES PROPUESTAS DE LEGISLACIÓN DIGITAL EUROPEA," *Cuad.*

Derecho Transnacional, vol. 13, no. 2, pp. 209–232, 2021.

[27] "Ley de Protección de Datos Personales recoge recomendaciones de la OEA y UE, adaptadas a la realidad ecuatoriana - Dirección Nacional de Registros Públicos," 2021. [Online]. Available: https://www.registrospublicos.gob.ec/ley-de-proteccion-de-datos-personales-recoge-recomendaciones-de-la-oea-y-ue-adaptadas-a-la-realidad-ecuatoriana/. [Accessed: 21-Aug-2023].

[28] "LEY ORGANICA DE TELECOMUNICACIONES."

[29] A. O. Huerva, "GUÍA DE CONTROLES DE CIBERSEGURIDAD PARA LA PROTECCIÓN INTEGRAL DE LA PYME," 2017.

[30] E. I. G. Ruiz and R. T. V. Vasquez, "Aplicación de la norma ISO 27002 para mejorar la seguridad de la información de la empresa COMPURED SAC," 2019.

ANEXOS

ANEXO #1

UNIVERSIDAD CATOLICA DE CUENCA SEDE AZOGUES

ENCUESTA A LA EMPRESA CABLETEL SOBRE LAS ACCIONES PREVIAS A LA LOPDP

1. ¿Ha adoptado o implementado medidas esenciales para la protección de los datos personales de sus clientes?

2. ¿Dispone de un sistema o responsable designado para garantizar el acceso a los datos únicamente a individuos autorizados?

3. ¿Ha establecido políticas de seguridad relacionadas con el tratamiento de datos personales?

4. ¿Posee un mecanismo para alertar al titular de los datos en caso de que se detecte una vulnerabilidad en sus datos personales?

5. ¿Solicita el consentimiento de clientes antes de proceder al tratamiento de sus datos personales?

ANEXO #2

UNIVERSIDAD CATOLICA DE CUENCA
SEDE AZOGUES

ENCUESTA A LA EMPRESA CABLETEL SOBRE LOS CONTROLES DE LA NORMA ISO/IEC 27002

5. POLITICAS DE SEGURIDAD

1. ¿La empresa cuenta con políticas de la seguridad de la información definidas, aprobadas, publicadas y comunicadas a los empleados?
2. ¿Las políticas de seguridad de la información de la empresa se planifican y revisan con regularidad para verificar su efectividad?

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

1. ¿Las responsabilidades para la seguridad de la información en la empresa están definidas y asignadas?
2. ¿Las tareas y las áreas de responsabilidad de la empresa se encuentran segregadas?
3. ¿Se mantiene contacto apropiado con las autoridades pertinentes?
4. ¿Se mantiene contacto con grupos o foros de seguridad especializados y asociaciones profesionales?
5. ¿Se revisa la seguridad de la información cuando la empresa desarrolla un proyecto?

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

1. ¿Se realizan revisiones de verificación de antecedentes de los candidatos a un empleo de acuerdo con las políticas de la empresa?

2. ¿Los empleados, contratistas y terceros aceptan y firman los términos y condiciones de contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de la información?

8. GESTIÓN DE ACTIVOS

1. ¿Todos los activos de información de la empresa se encuentran identificados, confeccionando y manteniendo un inventario de los más importantes?
2. ¿Toda la información y activos del inventario pertenecen a un área designado de la organización?
3. ¿Se ha identificado, documentado e implantado regulaciones para el uso adecuado de los activos de información?
4. ¿Se devuelven todos los activos de la empresa que estén en posesión/responsabilidad de los empleados y usuarios una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo?
5. ¿La información se encuentra clasificada en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización?
6. ¿Se ha desarrollado e implementado un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información de acuerdo con un esquema de clasificación adoptado por la empresa?
7. ¿Se ha desarrollado e implantado procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la empresa?
8. ¿Existen procedimientos establecidos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización?
9. ¿Se elimina los medios de forma segura y sin riesgo cuando ya no son requeridos usando procedimientos formales?

10. ¿Se encuentran protegidos los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la empresa?

9. CONTROL DE ACCESO

1. ¿Existe un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso?
2. ¿La empresa cuenta con la implementación de un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios?
3. ¿La asignación y uso de derechos de acceso con privilegios especiales en la empresa está restringido y controlado?
4. ¿Existe un proceso de gestión controlado en la asignación de información confidencial para autenticación?
5. ¿Los propietarios de los activos revisan con regularidad los derechos de accesos de los usuarios?
6. ¿Se retiran o revisan en caso de cambio los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo?
7. ¿Se exige a los trabajadores de la empresa el uso de buenas prácticas de seguridad en el uso de información confidencial para la autenticación?
8. ¿Se restringe el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida?
9. ¿La empresa controla el acceso a los sistemas y aplicaciones mediante un procedimiento de log-on?

10. ¿Los sistemas de gestión de contraseñas de la empresa aseguran contraseñas de calidad?
11. ¿Se encuentra restringido y controlado el uso de utilidades de software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas de la empresa?
12. ¿Se restringe el acceso al código fuente de las aplicaciones software de la empresa?

10. CIFRADO

1. ¿La empresa ha desarrollado e implementado una política que regule el uso de controles criptográficos para la protección de la información?
2. ¿La empresa ha desarrollado e implementado una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida?

12. SEGURIDAD EN LA OPERATIVA

1. ¿Se documentan y se dejan a disposición los procedimientos operativos a todos los usuarios que lo necesiten?
2. ¿Se controlan los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información?
3. ¿Se monitorea y ajusta el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas?
4. ¿Los entornos de desarrollo, pruebas y operacionales de la empresa permanecen separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional?
5. ¿La empresa realiza copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida?

6. ¿Se planifican y acuerdan los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio?

13. SEGURIDAD EN LAS TELECOMUNICACIONES

1. ¿Se administran y controlan las redes para proteger la información en sistemas y aplicaciones?
2. ¿Se identifican e incluyen en los acuerdos de servicio, los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados?
3. ¿Se encuentran segregadas las redes en función a los grupos de servicios, usuarios y sistemas de información?
4. ¿Existen políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación?
5. ¿Los acuerdos de la empresa abordan la transferencia segura de información comercial entre la organización y las partes externas?
6. ¿Se protege adecuadamente la información referida en la mensajería electrónica?
7. ¿Se identifican, revisan y documentan de manera regular los requisitos para los acuerdos de confidencialidad y “no divulgación” que reflejan las necesidades de la organización para la protección de información?

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

1. ¿La empresa incluye los requisitos relacionados con la seguridad de la información en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes?
2. ¿La empresa protege la información de los servicios de aplicación que pasan a través de redes públicas contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada?
3. ¿La empresa protege la información en transacciones de servicios de aplicación para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción?
4. ¿Se seleccionan cuidadosamente, protegen y controlan los datos de prueba?

15. RELACIONES CON SUMINISTRADORES

1. ¿Se acuerdan y documentan adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas?
2. ¿Se establecen y acuerdan todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización?
3. ¿Los acuerdos con los proveedores incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones?

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

1. ¿La empresa establece las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?
2. ¿Se informan los eventos de seguridad de la información lo antes posible utilizando los canales de administración adecuados?
3. ¿Se anota e informa sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización?
4. ¿Se evalúan los eventos de seguridad de la información y se deciden su clasificación como incidentes?
5. ¿La empresa responde ante los incidentes de seguridad de la información en atención a los procedimientos documentados?
6. ¿La empresa utiliza el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la portabilidad y/o impacto de incidentes en el futuro?
7. ¿La empresa define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia?

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

1. ¿La empresa determina los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre?
2. ¿La empresa establece, documenta, implementa y mantiene los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas?

3. ¿Se verifican regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas?

18. CUMPLIMIENTO

1. ¿La empresa identifica, documenta y mantiene al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatuarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos?
2. ¿La empresa implementa procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original?
3. ¿La empresa protege sus registros contra perdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales?
4. ¿La empresa garantiza la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan?
5. ¿la empresa utiliza controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes?

Universidad Católica de Cuenca	AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL	CÓDIGO: F – DB – 30 VERSION: 01 FECHA: 2021-04-15 Página 1 de 1

John Byron Yunganaula Yunganaula portador(a) de la cédula de ciudadanía Nº **030267729**. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación **"PROPUESTA DE UN PLAN DE IMPLEMENTACIÓN PARA EL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LA EMPRESA CABLETEL"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Azogues, **04 de enero de 2024**

F: .....

John Byron Yunganaula Yunganaula

C.I. 0302677729