

REPÚBLICA DEL ECUADOR



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO



MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD

INFORMÁTICA

**TEMA: IMPLEMENTACIÓN DE UN SISTEMA AUTOMATIZADO DE
CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES
EN UNA EMPRESA ECUATORIANA DE TELECOMUNICACIONES BAJO EL
MARCO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS
PERSONALES DEL ECUADOR**

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con
Mención en Seguridad Informática

Línea de investigación: "Desarrollo, aplicación de software y cyber security (seguridad cibernética)."

AUTOR: Carlos David Aguirre Benavides

DIRECTOR: Msc. Xavier Mauricio Rea Peñafiel

ASESOR: Msc. Diego Javier Trejo España

IBARRA - ECUADOR

2025

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA

UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	1003770482		
APELLIDOS Y NOMBRES	Carlos David Aguirre Benavides		
DIRECCION	Rio Chimbo 2-18 y Rio Curaray		
EMAIL	cdaguirreb@utn.edu.ec		
TELÉFONO FIJO		TELÉFONO MOVIL	0996716563
DATOS DE LA OBRA			
TÍTULO:	IMPLEMENTACIÓN DE UN SISTEMA AUTOMATIZADO DE CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES EN UNA EMPRESA ECUATORIANA DE TELECOMUNICACIONES BAJO EL MARCO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES DEL ECUADOR		

AUTOR (ES):	Carlos David Aguirre Benavides
FECHA:DD/MM/AAAA	19/11/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	<input type="checkbox"/> PREGRADO <input checked="" type="checkbox"/> POSGRADO
TÍTULO POR EL QUE OPTA:	Magister en Computación con Mención en Seguridad Informática
DIRECTOR:	Msc. Mauricio Rea Peñafiel
ASESOR:	Msc. Diego Trejo España

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que son los titulares de los derechos patrimoniales, por lo que asumen la responsabilidad sobre el contenido de la misma y saldrán en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 19 días del mes de noviembre del año 2025.

AUTOR:



Nombre: Carlos David Aguirre Benavides



CERTIFICACIÓN TUTOR Y ASESOR DEL TRABAJO DE TITULACIÓN

Nos permitimos informar que revisado el Trabajo final de Grado "IMPLEMENTACIÓN DE UN SISTEMA AUTOMATIZADO DE CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES EN UNA EMPRESA ECUATORIANA DE TELECOMUNICACIONES BAJO EL MARCO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES DEL ECUADOR", del Maestrante: Carlos David Aguirre Benavides de la Maestría en Computación con Mención en Seguridad Informática, certificamos que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizamos su presentación para los fines legales pertinentes.

Ibarra, a los 24 días del mes de septiembre de 2025

	Nombres Apellidos	Firma
Director	Msc. Mauricio Rea Peñafiel	 Firmado electrónicamente por: XAVIER MAURICIO REA PEÑAFIEL Validar únicamente con Firma@C
Asesor	Msc. Diego Trejo España	TREJO ESPANA DIEGO JAVIER  Firmado digitalmente por TREJO ESPANA DIEGO JAVIER Fecha: 2025.11.19 12:43:11 -05'00'

DEDICATORIA

Dedico este logro a quien en mi confiaron, mi base y cimientos: mi padre quien ha sido guía, amigo y consejero y de igual manera a mi madre que desde algún lugar del universo su recuerdo y energía me acompañan, mis hijas hermosas María Emilia y Martina Estefanía quien son mi motivación y mi motor para lograr lo que me propongo, mi compañera de vida quien es pilar fundamental en el hogar que decidimos formar, mis hermanos que han sabido acompañarme y quienes han hecho de mí una mejor persona. Les dedico esto y mucho más este logro no es solo mío es de todos. Los Amo

Carlos Aguirre Benavides

AGRADECIMIENTO

A la Universidad Técnica del Norte por acogerme nuevamente en el camino académico ahora como Maestrante, un especial agradecimiento a mi director y asesor quien me acompañaron este proceso su profesionalismo, apoyo y aportes hicieron posible esto.

A mi familia por los ánimos y apoyo incondicional

Carlos Aguirre Benavides

INDICE DE CONTENIDOS

IDENTIFICACIÓN DE LA OBRA	II
CONSTANCIAS	III
CERTIFICACIÓN TUTOR Y ASESOR DEL TRABAJO DE TITULACIÓN.....	IV
DEDICATORIA.....	V
AGRADECIMIENTO	VI
INDICE DE CONTENIDOS.....	VII
INDICE DE TABLAS.....	X
INDICE DE FIGURAS	X
RESUMEN.....	XII
ABSTRACT	XIII
CAPITULO I.....	1
EL PROBLEMA.....	1
1.1 Problema de investigación.....	1
1.2 Interrogantes de la Investigación.....	1
1.3 Objetivos de la investigación.....	2
1.3.1 Objetivo general	2
1.3.2 Objetivos específicos.....	2
1.4 Hipótesis de Trabajo.....	2
1.4.1 Hipótesis Alternativa	2
1.4.2 Hipótesis Nula	2

1.5 Caracterización de Variables	3
1.6 Justificación	3
CAPITULO II.....	4
MARCO REFERENCIAL	4
2.1 Marco Teórico	5
2.1.1 Datos personales y categorías especiales.....	5
2.1.2 Principios rectores del tratamiento de datos	5
2.1.3. Derechos de los titulares: ARCO/ARCT.....	6
2.1.4 Consentimiento para el tratamiento de datos.....	7
2.1.5 Validez del consentimiento	8
2.1.6 Gestión del consentimiento en telecomunicaciones	9
2.1.7 Modelos de plataformas de Consent Management (CMP).....	9
2.1.8 Flujos típicos.....	10
2.1.9 Arquitectura de 3 capas y orientación a servicios	11
2.1.10 Stack tecnológico.....	11
2.2 Marco Legal.....	12
2.2.1. Constitución de la República del Ecuador.....	12
2.2.2 Ley Orgánica de Protección de Datos Personales (2021).....	12
2.2.3 Reglamento a la LOPDP.....	13
2.2.4. Ley Orgánica de Telecomunicaciones (LOT)	13
2.2.5. Decisión 897 de la Comunidad Andina.....	13
CAPITULO III	15

MARCO METODOLÓGICO	15
3.1. Descripción del área de estudio / Descripción del grupo de estudio	15
3.2 Enfoque y tipo de investigación	15
3.3 Tipo de investigación:	16
3.4 Procedimiento de investigación.....	16
3.5 Análisis de requerimientos técnicos	16
3.6 Técnicas de recolección de datos.....	17
3.7 Validación técnica	21
3.8 Técnicas y herramientas	22
3.9.1 Eficiencia operativa	22
3.9.2 Cumplimiento normativo.....	23
3.9.3 Experiencia del usuario	23
CAPÍTULO IV	24
RESULTADOS Y DISCUSIÓN	24
4.1 Criterios técnicos y legales	24
4.3 Porcentaje de consentimientos válidos según LOPDP y tasa de finalización del proceso de consentimiento.....	32
4.4 Encuestas de satisfacción validadas	36
CONCLUSIONES Y RECOMENDACIONES	41
Conclusiones.....	41
Recomendaciones	42
REFERENCIAS	43

ANEXOS	46
--------------	----

INDICE DE TABLAS

Tabla 1 Muestra del grupo de estudio	15
Tabla 2 Cuadro comparativo tiempos	35
Tabla 3 Respuestas obtenidas de la encuesta en una escala del 1 - 5	39

INDICE DE FIGURAS

Figura 1. Parte 1 - Flujo de proceso del Software	18
Figura 2. Parte 2 y Parte 3 - Flujo de proceso del Software.....	19
Figura 3. Procedimiento de tratamiento de consentimiento de datos personales.....	24
Figura 4. Página login de administrador del sistema.....	26
Figura 5. Pantalla Dashboar con información en tiempo real	26
Figura 6. Sección de resultados de reporte de consentimientos	27
Figura 7. Sección de visualización de clientes y envíos de correo individual o masivos	28
Figura 8. Gestión de usuarios	28
Figura 9. Correo recibido para inicio de proceso de consentimiento por parte del cliente	29
Figura 10. Ingreso de datos para la validación de identidad	29
Figura 11. Correo recibido por el cliente con OTP enviado por el sistema	30
Figura 12. Introducción de código OTP	30
Figura 13. Presentación de datos del cliente para su verificación.....	31
Figura 14. Finalización de proceso con éxito.....	31

Figura 15. Correo electrónico con información de acuerdo en formato PDF	32
Figura 16. Porcentaje de consentimientos validados.....	33
Figura 17. Script de la Base de Datos.....	34
Figura 18. Factibilidad de consentimiento	37
Figura 19. Claridad y comprensión del tratamiento de datos.....	37
Figura 20. Sentido de seguridad en brindar información	38
Figura 21. Nivel de satisfacción	38
Figura 22. Matriz de correlacion Pearson.....	39

RESUMEN

El presente trabajo se enfoca en la implantación de un sistema diseñado para la obtención del consentimiento de tratamiento de datos personales en una empresa ecuatoriana de telecomunicaciones proveedor de servicios de internet ISP por sus siglas en inglés, en respuesta a la necesidad de cumplimiento normativo de la Ley Orgánica de Protección de Datos Personales (LOPDP) vigente en el Ecuador desde el año 2021. La problemática que se identifica en la presente investigación radica en que las empresas ecuatorianas aún siguen utilizando métodos manuales para la obtención del consentimiento de tratamiento de datos personales causando ineficiencia operativa e incluso arriesgándose a sanciones tanto administrativas como económicas que pueden llegar a ser hasta del 1% de los ingresos anuales. El proyecto contempla el desarrollo de un sistema web en .NET Core versión 8 con una Base de Datos en SQL server 2022 y desplegado en Microsoft IIS (Internet Information Services), sin dejar de lado aspectos de seguridad incorporando el uso de: OTPs, links únicos, certificados SSL y registrando evidencias como: timestamp, IP pública, agente de navegador, e incluso almacenando el acuerdo del cliente. Los resultados son concluyentes ya que muestran una reducción del 62.26% en el tiempo de procesamiento de 15 a 5.66 minutos en promedio por consentimiento, logrando una mayor productividad al momento de la obtención del consentimiento de tratamiento de datos por parte de sus clientes. El sistema puede garantizar la trazabilidad completa en el proceso, cumpliendo con los principios de licitud, finalidad, proporcionalidad, transparencia y seguridad establecidos en la LOPDP.

Palabras Clave: Consentimiento de datos personales, Ley Orgánica de Protección de Datos Personales (LOPDP), Sistema automatizado, Telecomunicaciones, Gestión del consentimiento (CMP), .NET Core 8, SQL Server 2022, Seguridad informática, Trazabilidad, OTP (One Time Password), Cumplimiento normativo, Eficiencia operativa, Privacidad de datos, Validación de identidad, Auditoría digital

ABSTRACT

This paper focuses on the implementation of a system designed to obtain consent for the processing of personal data in an Ecuadorian telecommunications company (ISP), in response to the need for regulatory compliance with the Ley Organica de Protección de Datos Personales (LOPDP), in force in Ecuador since 2021.

The problem identified in this research is that Ecuadorian companies continue to use manual methods to obtain consent for the processing of personal data, causing operational inefficiency and even risking administrative and financial penalties that can reach up to 1% of annual revenue.

The project involves the development of a web system in .NET Core version 8 with a SQL Server 2022 database deployed on Microsoft IIS (Internet Information Services). It also incorporates security features, including OTPs, unique links, SSL certificates, and recording evidence such as timestamps, public IP addresses, browser agents, and even storing the customer's consent.

The results are conclusive, showing a 62.26% reduction in processing time, from 15 to 5.66 minutes on average per consent, achieving greater productivity when obtaining data processing consent from clients. The system can guarantee complete traceability throughout the process, complying with the principles of legality, purpose, proportionality, transparency, and security established in the LOPDP.

Keywords:

Personal Data Consent, Data Protection Law (LOPDP), Automated System, Telecommunications, Consent Management Platform (CMP), .NET Core 8, SQL Server 2022, Cybersecurity, Traceability, One-Time Password (OTP), Regulatory Compliance, Operational Efficiency, Data Privacy, Identity Validation, Digital Audit

CAPITULO I

EL PROBLEMA

El sector de telecomunicaciones en Ecuador maneja diariamente millones de datos personales de sus usuarios. Con la publicación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en mayo de 2021, las empresas de telecomunicaciones enfrentan un desafío crítico para implementar mecanismos que garanticen el cumplimiento normativo, principalmente para a la obtención y gestión del consentimiento de tratamiento de datos personales.

El principal problema radica en que actualmente muchas empresas del Ecuador en las que se incluyen las de telecomunicaciones continúan utilizando procesos manuales o semiautomatizados para la gestión del consentimiento, lo que genera:

- **Ineficiencia operativa:** Los procesos manuales requieren considerable inversión de tiempo y recursos humanos.
- **Riesgo de incumplimiento normativo:** La falta de trazabilidad y auditoría del proceso de consentimiento de tratamiento de datos personales puede resultar en sanciones económicas y administrativas.
- **Experiencia deficiente del usuario:** Los clientes enfrentan procesos complejos y largos al momento de dar su consentimiento de tratamiento de datos personales cuando se lo hace de forma manual.
- **Vulnerabilidades de seguridad:** La gestión manual aumenta el riesgo de pérdida o alteración no autorizada de registros de consentimiento firmados por los clientes.

1.1 Problema de investigación

¿Cómo se puede implementar un sistema automatizado que garantice la obtención, gestión y trazabilidad del consentimiento para el tratamiento de datos personales en empresas de telecomunicaciones, cumpliendo con los requisitos de la LOPDP y mejorando simultáneamente la eficiencia operativa?

1.2 Interrogantes de la Investigación

¿Cuál es el estado actual de la gestión del consentimiento de tratamiento de datos personales en las empresas de telecomunicaciones ecuatorianas?

¿Qué arquitectura tecnológica sería la más adecuada para garantizar no solo el cumplimiento normativo, sino también la escalabilidad del sistema?

¿Cómo podemos medir objetivamente el impacto de la automatización de consentimiento de tratamiento de datos personales en la eficiencia operativa?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Implementar un sistema web automatizado de obtención y gestión de consentimiento para el tratamiento de datos personales en empresas de telecomunicaciones, cumpliendo con los requerimientos establecidos en la Ley Orgánica de Protección de Datos Personales del Ecuador.

1.3.2 Objetivos específicos

- Identificar los criterios técnicos y legales que debe cumplir un sistema automatizado de consentimiento de tratamiento de datos personales.
- Desarrollar un prototipo funcional del sistema automatizado de consentimiento de tratamiento de datos personales.
- Evaluar el impacto de la implementación del sistema automatizado en términos de eficiencia operativa, cumplimiento normativo y experiencia del usuario.

1.4 Hipótesis de Trabajo

La implementación de un sistema automatizado de consentimiento para el tratamiento de datos personales en una empresa ecuatoriana de telecomunicaciones optimiza el tiempo del proceso de recolección de acuerdos, asegurando un cumplimiento eficiente y efectivo de la Ley Orgánica de Protección de Datos Personales del Ecuador.

1.4.1 Hipótesis Alternativa

La implementación de un sistema web automatizado de obtención y gestión de consentimiento para el tratamiento de datos personales mejorará el tiempo de recolección de acuerdos de tratamiento de datos personales de los clientes de una empresa ecuatoriana de telecomunicaciones

1.4.2 Hipótesis Nula

La implementación de un sistema web automatizado de obtención y gestión de consentimiento para el tratamiento de datos personales no mejorará el tiempo de

recolección de acuerdos de tratamiento de datos personales de los clientes de una empresa ecuatoriana de telecomunicaciones

1.5 Caracterización de Variables

Variable Independiente:

Implementación del sistema automatizado de consentimiento para el tratamiento de datos personales bajo el marco de la LOPDP

Variable Dependiente:

Tiempo de ejecución y experiencia de usuario para la obtención del consentimiento de tratamiento de datos personales para una empresa de telecomunicaciones.

1.6 Justificación

La implementación de un sistema automatizado de consentimiento en el sector de telecomunicaciones se justifica por múltiples razones:

- **Relevancia legal:** La LOPDP establece multas de hasta 1% de los ingresos del ejercicio fiscal anterior para infracciones graves (Asamblea Nacional del Ecuador, 2021, Art. 78). Un sistema automatizado reduce significativamente el riesgo de incumplimiento normativo.
- **Aporte al conocimiento:** Este trabajo contribuirá al desarrollo de un marco metodológico para la implementación de sistemas de consentimiento específicamente adaptados al contexto ecuatoriano.
- **Impacto social:** Según datos del Instituto Nacional de Estadística y Censos (INEC, 2023), el 81.8% de la población ecuatoriana utiliza servicios de telecomunicaciones, por lo que mejorar la gestión de sus datos personales impacta directamente en la privacidad de millones de ciudadanos.

CAPITULO II

MARCO REFERENCIAL

La gestión del consentimiento en el tratamiento de datos personales representa un desafío crítico para el sector de telecomunicaciones a nivel mundial. Según Acurio (2021) identificaron que las empresas de telecomunicaciones procesan volúmenes inmensos de datos personales que requieren mecanismos robustos de gestión del consentimiento para cumplir con las regulaciones emergentes de protección de datos.

En el contexto latinoamericano, diversas investigaciones han explorado la automatización de procesos para el cumplimiento normativo. Mila (2019) menciona que el desarrollo un framework para la automatización del consentimiento en empresas brasileñas de telecomunicaciones bajo la LGPD, documentando una reducción del 65% en el tiempo de procesamiento de solicitudes. De manera complementaria Chávez y Burgos (2025) analizaron la implementación de sistemas de gestión de privacidad en operadores españoles, evidenciando que las empresas con sistemas automatizados experimentaron una reducción del 78% en incidentes relacionados con el manejo inadecuado del consentimiento.

Desde una perspectiva organizacional, Rivera (2020) detectaron factores clave para la puesta en marcha exitosa de sistemas automatizados de protección de datos, subrayando el respaldo directivo, la formación del personal y la compatibilidad con la infraestructura vigente como componentes decisivos. Los resultados son especialmente pertinentes para organizaciones con arquitecturas tecnológicas complejas.

En Ecuador, la literatura específica sobre implementación bajo la LOPDP permanece en desarrollo debido a su reciente promulgación. Sin embargo, Bermeo (2020) registra que el 73% de las compañías de telecomunicaciones en Ecuador señalaron serios inconvenientes en la administración manual del consentimiento durante el primer año de aplicación de la normativa, lo que pone en evidencia la imperiosa necesidad de implementar alternativas automatizadas.

Los antecedentes ponen de manifiesto que la adopción de sistemas automatizados de consentimiento en el sector de telecomunicaciones demanda un abordaje integral, capaz de contemplar aspectos tecnológicos, normativos, organizacionales y centrados en

el usuario. De este modo, se configura la base teórico-práctica que sustenta el desarrollo de la presente investigación.

2.1 Marco Teórico

2.1.1 Datos personales y categorías especiales

Los datos personales constituyen el núcleo de toda normativa de protección de la privacidad, pues se definen como aquella información que identifica o pueden llegar a identificar a una persona natural. Dentro de esta categoría, los datos sensibles requieren un tratamiento reforzado por el riesgo que implican en la dignidad y derechos fundamentales. Un ejemplo de estos es la información relativa a la salud, convicciones religiosas o datos biométricos (Cano & Jaramillo, 2023). Desde una perspectiva crítica, reconocer esta clasificación es esencial porque condiciona las salvaguardas técnicas que deben ofrecer cualquier sistema automatizado. Por lo tanto, no es lo mismo gestionar un correo electrónico que un registro médico.

En el contexto de las telecomunicaciones, la empresa actúa con responsable del tratamiento, pues define finalidades y medios mientras que el encargado ejecuta instrucciones y medidas técnicas de seguridad. En la práctica, el proyecto analizado sitúa a la empresa proveedora como responsable y a los módulos desarrollados .NET Core 8, SQL Server 2022 e IIS como herramientas que permiten a los encargados operar el consentimiento bajo criterios de trazabilidad y confiabilidad (Esginnova Group, 2018).

2.1.2 Principios rectores del tratamiento de datos

El tratamiento de datos personales no puede entenderse únicamente como una operación técnica de almacenamiento o procesamiento, ya que implica más bien un compromiso ético y jurídico orientado a salvaguardar los derechos fundamentales. Por esta razón, la Ley Orgánica de Protección de datos Personales (Asamblea Nacional, 2021) y la doctrina especializada establecen un conjunto de principios que deben guiar toda práctica relacionada con los datos personales. Dichos principios no solo garantizan la legitimidad del tratamiento, sino que también fortalecen la confianza de los titulares al asegurar que la información proporcionada será utilizada con responsabilidad, transparencia y respeto a su dignidad (Ponce, 2021) A continuación, se detalla cada principio (García, 2021):

- **Licitud.** Todo tratamiento debe tener base jurídica válida; en este caso, consentimiento libre, informado, específico e inequívoco, por lo cual implica

registrar evidencias verificables (token, OTP, timestamp, IP) que demuestren la validez del acto.

- **Finalidad.** Los datos solo pueden usarse para propósitos concretos y comunicados al titular como por ejemplo la provisión del servicio, facturación y soporte. Es decir, cualquier desvío constituye uso indebido; por eso, la solución adjunta comprobantes en PDF que acotan el alcance del consentimiento.
- **Proporcionalidad y minimización.** Se recaban solo los datos estrictamente necesarios y se conservan por el tiempo imprescindible. En la práctica: modelos de datos acotados en SQL Server, controles por roles y políticas de retención/eliminación oportuna.
- **Transparencia.** Exige información clara y accesible sobre el tratamiento y sus consecuencias. Se materializa en interfaces comprensibles, notificaciones de aceptación/negación y acceso al acuerdo para consulta y eventual revocatoria.
- **Seguridad.** Obliga a medidas técnicas y organizativas (OTP, control de accesos, cifrado en tránsito, registro de agente e IP, logging y auditoría) para prevenir acceso no autorizado, pérdida o alteración. La arquitectura en .NET Core 8 + IIS + SQL Server incorpora estos controles de forma trazable

2.1.3. Derechos de los titulares: ARCO/ARCT

Según (Asamblea Nacional, 2021) El respeto a los derechos de los titulares de datos personales constituye la base del marco normativo en protección de la información, entre ellos destacan los derechos ARCO/ARCT (acceso, rectificación, cancelación/supresión, oposición y portabilidad) que otorgan a las personas el control efectivo sobre el uso de sus datos. Los derechos de los titulares no solo son garantías jurídicas, sino también herramientas prácticas que fortalecen la confianza en las organizaciones. De esta manera aseguran transparencia, corrección, eliminación, decisión autónoma y movilidad de la información en entornos digitales.

- **Derecho de acceso:** Es aquel que garantiza que el titular pueda conocer que datos suyos son tratados, con que finalidad y bajo qué base legal. El ejercicio de este derecho permite auditar el cumplimiento de la normativa y fortalecer la confianza hacia la organización.
- **Derecho de rectificación:** Es aquel que permite corregir inexactitudes o actualizar información que sea necesaria, asegurando que los datos sean verídicos

y pertinentes, esto evita decisiones equivocadas basadas en información erróneas y refuerzan la calidad del sistema de gestión.

- **Derecho de cancelación o supresión:** Es aquel que autoría al titular a solicitar la eliminación de sus datos cuando no son necesarios para la finalidad inicial o cuando se revoque el consentimiento, representando un mecanismo de control directo frente la retención excesiva o abusiva de información.
- **Derecho de oposición:** Es aquel que digna la facultad de rechazar tratamientos no esenciales o secundarios como usos comerciales o de mercadeo. De esta manera se refuerza la autonomía de la persona y evita que su información sea empleada con fines distintos a los originalmente consentidos.
- **Derecho de portabilidad:** Es aquel que permite recibir los datos en un formato estructurado, común y legible o transferirles directamente a otros responsables. De esta manera se asegura la interoperabilidad entre sistemas y se fortalece la libertad de elección del titular, respecto a los servicios que utiliza.

2.1.4 Consentimiento para el tratamiento de datos

El consentimiento es el pilar central de la protección de datos personales, pues constituye la manifestación de voluntad mediante la cual el titular autoriza o rechaza el uso de información. En el marco de la LOPDP (Asamblea Nacional, 2021), menciona que la obtención, gestión y registro no son actos formales aislados, sino que son procesos que aseguran el respeto a la autonomía y dignidad de las personas. En este contexto, cualquier sistema de gestión manual o automatizado deben diseñarse para garantizar el consentimiento sea válido, trazable y susceptible a una auditoria.

El consentimiento valido se define como la expresión de voluntad libre, específica, informada e inequívoca del titular. Con respecto al concepto de libre se refiere a que no puede estar condicionado ni inducido mediante engaños. Por otro lado, el específico debe referirse a un tratamiento claramente delimitado. En el informado, requiere que el usuario conozca la finalidad, los riesgos y sus derechos (Minguillón, 2019). Finalmente, el inequívoco, es aquel que se refiere a la acción que lo materializa como la aceptación digital, firma y OTP. Debe ser clara y verificable.

2.1.4.1 Modalidades de obtención del consentimiento

El consentimiento puede expresarse de diferentes formas siempre que se respete la libertad y claridad de la decisión del titular. Las modalidades de obtención buscan facilitar

la comprensión del usuario y al mismo tiempo garantizar que la organización cumpla con los requisitos de validez establecidos en la normativa. En la práctica, optar por una u otra modalidad depende de la finalidad del tratamiento y del nivel de riesgo que implique el uso de los datos (Palomino, 2018):

- **Modalidad explícita:** Se otorga mediante una acción afirmativa clara, como afirmar digitalmente o aceptar una casilla en línea, su ventaja es la certeza jurídica que ofrece.
- **Modalidad Granular:** Es aquella que divide el consentimiento en secciones específicas permitiendo que el titular acepte unas finalidades y rechace otras, favoreciendo la autonomía y la personalización del control sobre los datos.
- **Modalidad por categorías de tratamiento:** Es aquella que agrupa usos similares de la información como: facturación, mercadeo y soporte. De esta manera el usuario podrá autorizar bloques de tratamiento sin tener que aceptar cada acción por separado. Por lo tanto, facilita la gestión, aunque requiere explicaciones claras para no generar confusión.

2.1.5 Validez del consentimiento

La validez del consentimiento no solamente debe ser jurídico sino debe tener un respaldo a través de evidencia que lo respalden, como registros de fecha, hora, IP pública, agente de navegador y archivo PDF. Así mismo, debe garantizarse la revocatoria, es decir la posibilidad de que el titular retire su autorización en cualquier momento sin perjuicio alguno. Finalmente, los límites del consentimiento impiden utilizar la información más allá de las finalidades comunicadas y aceptadas (García, 2021). En este sentido, la propuesta técnica asegura validez al permitir notificaciones automáticas y almacenamiento de evidencias digitales que pueden ser auditadas por la empresa o por la autoridad de control.

La trazabilidad implica seguir el ciclo completo del consentimiento desde su emisión hasta su revocatoria o expiración. Por lo tanto, se supone registrar no solamente la aceptación o negación, sino también los contextos técnicos en los que ocurrió: el navegador utilizado, ubicación aproximada, token y OTP empleados. La registrabilidad por su parte demanda conservar estos datos por un tiempo prudente, definido tanto por la finalidad del tratamiento como por los plazos legales aplicables (Brito, 2022). En el sistema automatizado desarrollado, la trazabilidad se logra como un repositorio central

en SQL Server 2022, que almacena evidencias con capacidad de consulta y exportación, garantizando de esta manera un control riguroso y demostrable en auditorías internas y externas.

2.1.6 Gestión del consentimiento en telecomunicaciones

El sector de telecomunicaciones opera sobre volúmenes masivo de datos personales en los que se identifica, realiza un contacto y patrones de consumo, generados de forma continua por millones de interacciones y dispositivos. La escala incrementa la superficie de riesgo, es decir a mayor caudal y variedad de datos mayores exigencias de control, segregación de accesos y monitoreo de acceso legítimo. Además, la multicanalidad de la contratación presencial, portales web, aplicaciones móviles, call center y correos, complejiza la obtención y verificación del consentimiento, pues exige coherencia entre canales y la posibilidad de auditar la validez de cada acto (Mato, 2020). En este contexto, la investigación plantea que la automatización no es opcional, sino una condición para sostener trazabilidad verificable en cumplimiento normativo en tiempo real.

Los esquemas manuales o semiautomatizados de consentimiento suelen derivar en ineficiencias operativas en tiempos de ciclo variables, dependencia de mensajería física o validaciones. Por lo tanto, generan una trazabilidad incompleta que implica una posible pérdida de evidencia, registros heterogéneos, dificultades para reconstruir el flujo. A ello se suman errores humanos, omisiones, transcripciones, versiones desalineadas del texto consentido. Lo cual erosionan la calidad probatoria del consentimiento y elevan el riesgo de sanciones. Frente a esas brechas, la investigación propone una plataforma que consolidan evidencias técnicas como: timestamp, IP publica, gente de navegador, token y OTP. Por lo cual, resguarda el acuerdo en PDF, genera notificaciones automáticas y habilita reportes exportables, reduciendo los tiempos de respuesta a minutos y permitiendo auditoría posterior con garantías de no repudio (Mato, 2020).

2.1.7 Modelos de plataformas de Consent Management (CMP)

Un CMP moderno se organiza, por claridad y resiliencia, en tres capas. La capa de presentación concentra las interfaces donde el titular interactúa (web, móvil, correo con enlaces seguros): aquí se comunican finalidades, se muestran opciones granulares y se recogen acciones afirmativas (aceptar/denegar). El diseño debe ser claro, accesible y coherente entre canales para reducir fricción y errores de interpretación (Blendee, 2025).

La capa de lógica de negocio orquesta reglas, se encarga de validar tokens y OTP, aplica políticas de finalidad/minimización, versiona cláusulas, controla ventanas de vigencia y dispara notificaciones. Por último, la capa de persistencia almacena, de forma íntegra y auditable, evidencias del consentimiento. En la investigación, este patrón se materializa con .NET Core 8 (servicios), IIS (despliegue) y SQL Server 2022 (registro y reportes) para asegurar trazabilidad y no repudio (Blendee, 2025).

2.1.8 Flujos típicos: solicitud, autenticación, entrega de información, consentimiento, registro, auditoría y revocatoria

El flujo estándar inicia con la solicitud: el sistema envía un enlace único con token al correo declarado por el cliente, sigue la autenticación OTP de 6 dígitos para verificar identidad. Luego, la entrega de información expone finalidades, bases jurídicas y derechos en lenguaje claro; solo entonces se recoge la decisión de consentimiento (Yepez, 2019).

Tras la decisión, el CMP realiza el registro probatorio entre metadatos técnicos + PDF del acuerdo, emite notificaciones al titular y habilita la auditoría consultas, exportables, bitácoras. Según Yépez (2019) La revocatoria debe ser tan simple como la aceptación: un canal visible, con la misma robustez técnica y documental. La secuencia implementada en la solución propuesta reduce tiempos de ciclo, homologa canales y eleva la calidad jurídica del consentimiento frente a inspecciones o controversias.

Un CMP se gestiona con indicadores operativos y de cumplimiento. La tasa de finalización muestra qué porcentaje concluye el proceso sin abandonos; su mejora suele depender de claridad textual y simplicidad de pasos. El tiempo de ciclo (desde el envío hasta la decisión) es crítico para operaciones: la tesis reporta reducciones a minutos, frente a procesos manuales que podían tardar días, con impacto directo en costos y riesgo de incumplimiento.

La validez jurídica se evalúa por la completitud y consistencia de la evidencia como la verificabilidad de identidad, integridad del texto aceptado, sellos temporales, IP/UA y logs. Finalmente, la satisfacción del usuario es medida con encuestas breves y valida si el proceso es comprensible y respetuoso. Un buen CMP no solo cumple la ley: genera confianza, reduce retrabajos y facilita auditorías gracias a reportes y dashboards que visibilizan brechas y oportunidades de mejora continua.

2.1.9 Arquitectura de 3 capas y orientación a servicios

La arquitectura de tres capas organiza el sistema en presentación, aplicación, servicios e infraestructura y datos. La capa web muestra finalidades y opciones granulares y captura la decisión del titular; la capa de servicios aplica reglas como la validación de token y OTP, versionado de cláusulas, notificaciones y la capa de datos conserva evidencias auditables, timestamp, IP pública, agente de navegador, hash del texto aceptado, estado y vigencia, habilitando consultas y reportes. La separación reduce acoplamientos, facilita el mantenimiento y sostiene la trazabilidad exigida por la LOPDP (Rodríguez, 2020).

Sobre esta base, el proyecto implementa .NET Core 8 para la lógica, IIS para el despliegue y SQL Server 2022 para el almacenamiento seguro, publicado en un servidor corporativo con IP pública. La orientación a servicios (APIs) integra el envío de enlaces con token, autenticación por OTP, generación del acuerdo en PDF y bitácoras, asegurando no repudio y evidencia verificable del consentimiento; así, el ciclo operativo pasa de días a minutos con control probatorio robusto.

El diseño modular separa el módulo de consentimiento enlace seguro, autenticación, renderizado de cláusulas, registro de evidencias y notificación del gestor de tratamientos, envíos unitarios por filtros, reintentos, dashboard en tiempo real y reportes exportables. La modularidad permite escalar, ajustar políticas sin impactos colaterales y mantener coherencia multicanal, a la vez que facilita auditorías internas y externas al centralizar métricas.

2.1.10 Stack tecnológico

.NET 8 ofrece un entorno maduro y de alto rendimiento para construir APIs REST con Minimal APIs, inyección de dependencias y manejo asíncrono eficiente, lo que reduce latencia y simplifica el código. Su ecosistema facilita aplicar patrones limpios de separación de capas, validaciones, middlewares de seguridad) y encapsular reglas de negocio del consentimiento como: tokens, OTP, versionado de cláusulas) en servicios testeables (López, 2022). Además, integra fácilmente autenticación, logging estructurado y envío de notificaciones, elementos cruciales para la trazabilidad y el no repudio exigidos por la LOPDP.

SQL Server 2022: modelos de datos de consentimiento, auditoría y reporting. SQL Server 2022 permite diseñar modelos de datos que relacionan titulares, finalidades

y decisiones (aceptado/negado/revocado), junto con evidencias técnicas (timestamp, IP pública, user-agent, hash/versión del texto aceptado). Las capacidades de auditoría y retención facilitan políticas de conservación y consultas reproducibles; a la vez, las vistas y procedimientos almacenados agilizan reportes y exportaciones por ejemplo a Excel, para control interno y requerimientos de la autoridad (López, 2022). Con índices adecuados y controles por rol, se garantiza integridad, desempeño y acceso mínimo necesario.

IIS e IIS Manager simplifican el despliegue de la aplicación en Windows Server 2022 con IP pública, gestionando bindings HTTPS (SNI, certificados), application pools aislados y políticas de reciclado que elevan disponibilidad y seguridad. La administración local y remota permite orquestar sitios, reglas de redirección y hardening (TLS, headers), mientras se integran logs de acceso para auditoría. Este entorno encaja con la arquitectura en tres capas del proyecto y asegura publicación confiable, escalable y trazable del flujo de consentimiento a través de canales web y correo.

2.2 Marco Legal

2.2.1. Constitución de la República del Ecuador

La Constitución de la República del Ecuador reconoce la protección de datos personales como derecho fundamental (art. 66, num. 19), vinculándolo con la dignidad y con el ejercicio de otras libertades. Este mandato constitucional exige que todo tratamiento respete principios como licitud, finalidad, minimización, transparencia y seguridad, y habilite el ejercicio efectivo de derechos del titular (acceso, rectificación, oposición, supresión y portabilidad). En el contexto de esta investigación, dicho marco superior legitima la automatización del consentimiento en telecomunicaciones: el sistema propuesto (.NET Core 8 + IIS + SQL Server 2022) materializa la exigencia constitucional al registrar evidencias trazables (timestamp, IP, agente, versión aceptada), habilitar revocatoria y facilitar auditoría, convirtiendo la garantía abstracta en controles técnicos verificables

2.2.2 Ley Orgánica de Protección de Datos Personales (2021)

La protección de datos personales en Ecuador encuentra su piedra angular en la Ley Orgánica de Protección de Datos Personales, vigente desde mayo de 2021. Esta normativa define el consentimiento como la manifestación de voluntad libre, específica, informada e inequívoca por la que el titular acepta el tratamiento de sus datos (Asamblea

Nacional del Ecuador, 2021, art. 4). La definición responde a una necesidad urgente del sector empresarial ecuatoriano, de contar con reglas claras en el manejo de los datos personales de los clientes.

2.2.3 Reglamento a la LOPDP

El Reglamento a la LOPDP (2024) operacionaliza el consentimiento exigiendo trazabilidad, registrabilidad y verificabilidad: demostrar cuándo, cómo y en qué condiciones se otorgó o negó, habilitar revocatoria y conservar evidencias técnicas como: timestamp, IP, agente, versión del texto). En telecomunicaciones, por su volumen y multicanalidad, esta exigencia vuelve indispensable la automatización. La propuesta en .NET Core 8 + IIS + SQL Server 2022 responde a ello al registrar metadatos probatorios, emitir el PDF del acuerdo, notificar por correo y facilitar auditorías mediante reportes exportables con token y OTP, alineando eficiencia operativa con cumplimiento normativo.

2.2.4. Ley Orgánica de Telecomunicaciones (LOT)

La Ley Orgánica de Telecomunicaciones (LOT) regula la prestación de servicios en Ecuador y, tras su reforma, el art. 22 incorpora exigencias sobre protección y gestión responsable de la información de usuarios, elevando los controles que deben cumplir los operadores. Este marco, sumado a la LOPDP y su Reglamento, configura un entorno de alto cumplimiento en el que la gestión manual del consentimiento es insuficiente. Por ello, la investigación propone un sistema automatizado (.NET Core 8 + IIS + SQL Server 2022) que registra evidencias trazables, facilita auditorías y reduce tiempos operativos, ofreciendo una vía técnica para cumplir integralmente con la LOT y la normativa de datos personales en el sector telecomunicaciones.

2.2.5. Decisión 897 de la Comunidad Andina.

La Decisión 897 (Comunidad Andina de Naciones, 2022) establece lineamientos regionales en materia de protección de datos personales, buscando homologar criterios entre los países miembros y garantizar un nivel común de resguardo de la información. El marco supranacional obliga a las empresas ecuatorianas a cumplir no solo con la legislación interna, sino también con estándares compartidos en la región, lo que eleva la complejidad regulatoria en sectores sensibles como el de telecomunicaciones. En relación con la investigación, la implementación de un sistema automatizado de consentimiento responde directamente a estas exigencias, pues asegura trazabilidad, interoperabilidad y

registros probatorios que permiten a las operadoras ecuatorianas alinearse tanto con la LOPDP como con la normativa andina, reforzando la confianza de los usuarios y la seguridad jurídica de la organización.

CAPITULO III

MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

El estudio se realizará en una empresa de telecomunicaciones con 15 años en el mercado como proveedor de servicios de internet ISP con su matriz ubicada en la provincia de Imbabura, Ecuador. La empresa seleccionada cuenta con 14000 clientes aproximadamente y opera en varias provincias del país como: Carchi, Imbabura, Pichincha, Chimborazo, Cotopaxi, Sucumbíos, Azuay y Guayas prestando servicio de proveedor de Internet como su principal servicio.

La empresa procesa algunos datos personales, incluyendo:

- Datos de identificación (nombre, cédula, dirección)
- Datos de contacto (teléfono, correo electrónico)
- Datos de consumo (planes contratados, uso de servicios)

La muestra del grupo de estudio está conformada por 12 empleados de la empresa, quienes fueron seleccionados por la organización debido a su conocimiento del estado actual del proceso y la situación relacionada con la obtención manual del consentimiento para el tratamiento de datos personales.

Tabla 1

Muestra del grupo de estudio

Sexo	Número
Hombres	9
Mujeres	3

3.2 Enfoque y tipo de investigación

La investigación adoptará un enfoque mixto (cuantitativo-cualitativo) por las siguientes razones:

- **Componente cuantitativo:** Se medirán variables como tiempo de procesamiento de consentimientos, tasa de cumplimiento.
- **Componente cualitativo:** Se analizarán las percepciones de usuarios y administradores sobre la usabilidad del sistema.

3.3 Tipo de investigación:

- **Según su alcance:** Aplicada y evaluativa, ya que busca resolver un problema práctico específico y evaluar el impacto de la solución implementada.
- **Según las fuentes:** De campo y documental, combinando análisis de documentos legales y técnicos con implementación práctica en un entorno real.

3.4 Procedimiento de investigación

Fase 1: Identificación de criterios técnicos y legales (Objetivo Específico 1)

Se realizó un análisis exhaustivo de la Ley Orgánica de Protección de Datos Personales del Ecuador, identificando específicamente:

- Materia relacionada al consentimiento en el artículo 8.
- Requisitos del consentimiento según el artículo 11.
- Obligaciones del responsable del tratamiento (artículos 47-48).
- Requisitos de seguridad y notificación de brechas (artículo 43).

3.5 Análisis de requerimientos técnicos

Basándose en el marco arquitectónico propuesto para el proyecto de obtención de consentimiento de tratamiento de datos personales se definió:

- Componentes de arquitectura necesarios

El sistema fue desarrollado en una arquitectura SOA de 3 capas.

Fue necesaria la publicación mediante ISS en un Servidor Windows 2022 provisto por la empresa en el que se instaló software que permitió el correcto funcionamiento y gestión de la información obtenida y generada por el prototipo. Un navegador web por el cual los clientes acceden al mismo.

- Mecanismos de auditoría y trazabilidad

La auditoría se la realiza de forma manual o con cruce de datos obtenidos del gestor de base de datos, los mismo que son almacenados por el prototipo de forma automática en una tabla específica que fue destinada para este propósito.

- **Requisitos de rendimiento**

Para que el sistema funcione correctamente fue necesario un servidor con las siguientes características:

Sistema Operativo: Windows Server 2022

CPU: 2 vCPU

RAM: 10 GB

Disco Duro: 40GB

Y por parte del cliente necesita: una conexión a internet de mínimo 10Mbps, un dispositivo que pueda ejecutar un navegador Web y el acceso al correo electrónico registrado en el contrato de servicio.

3.6 Técnicas de recolección de datos

Los datos fueron proporcionados por la empresa de telecomunicaciones, los mismos que por decisión de esta, fueron de los clientes que ya contaban con un contrato firmado previo a la implementación del sistema de consentimiento de tratamiento de datos personales. Los datos fueron entregados en una hoja de Excel la misma que fue convertida en un script SQL para su inserción en la Base de Datos.

Fase 2: Implementación del prototipo (Objetivo Específico 2)

Para iniciar con la implantación del prototipo se vio la necesidad de generar un diagrama de flujo para el proceso que se llevara a cabo en el software el cual por motivos de una mejor comprensión se lo dividió en 3 partes que son:

Parte 1 - Acciones tomadas por el administrador del sistema.

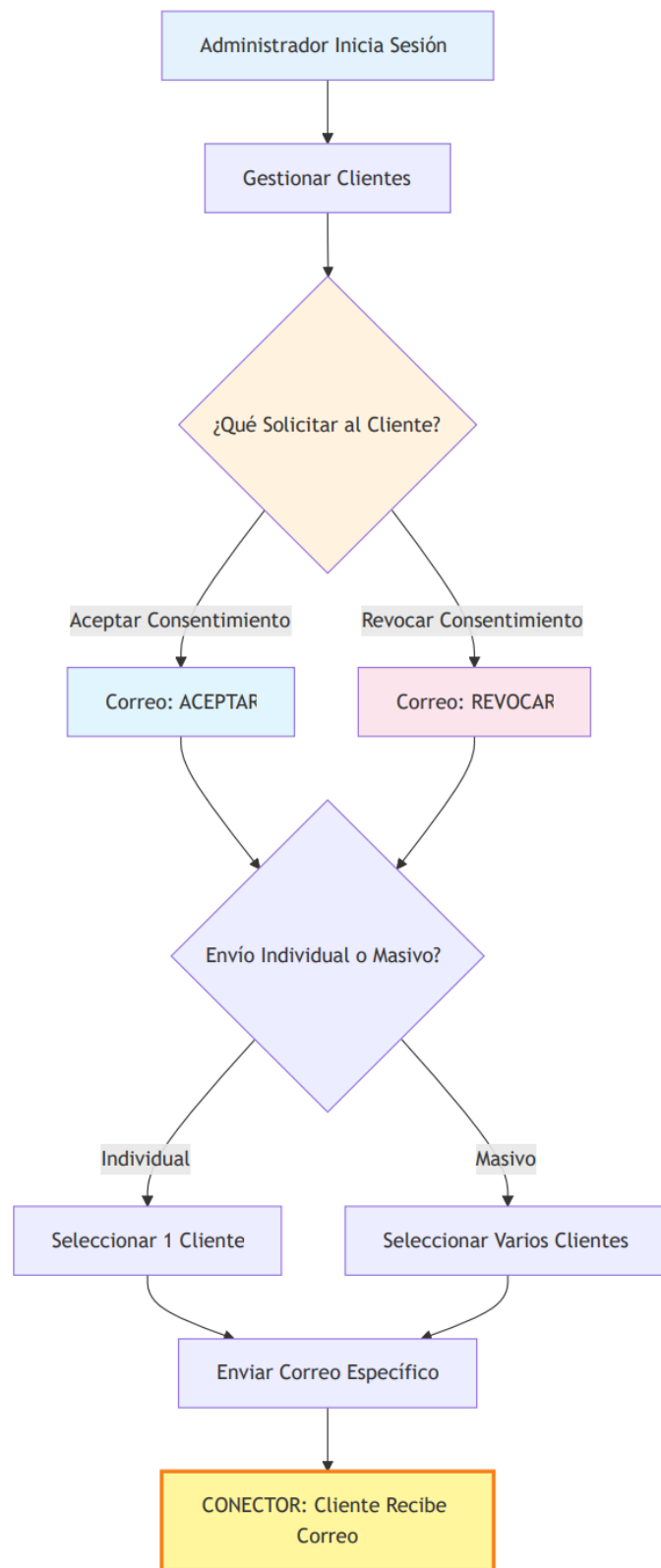


Figura 1. Parte 1 - Flujo de proceso del Software
Fuente: Propia

Parte 2- Cliente recibe el correo electrónico y Parte 3- Continúa proceso de decisión:

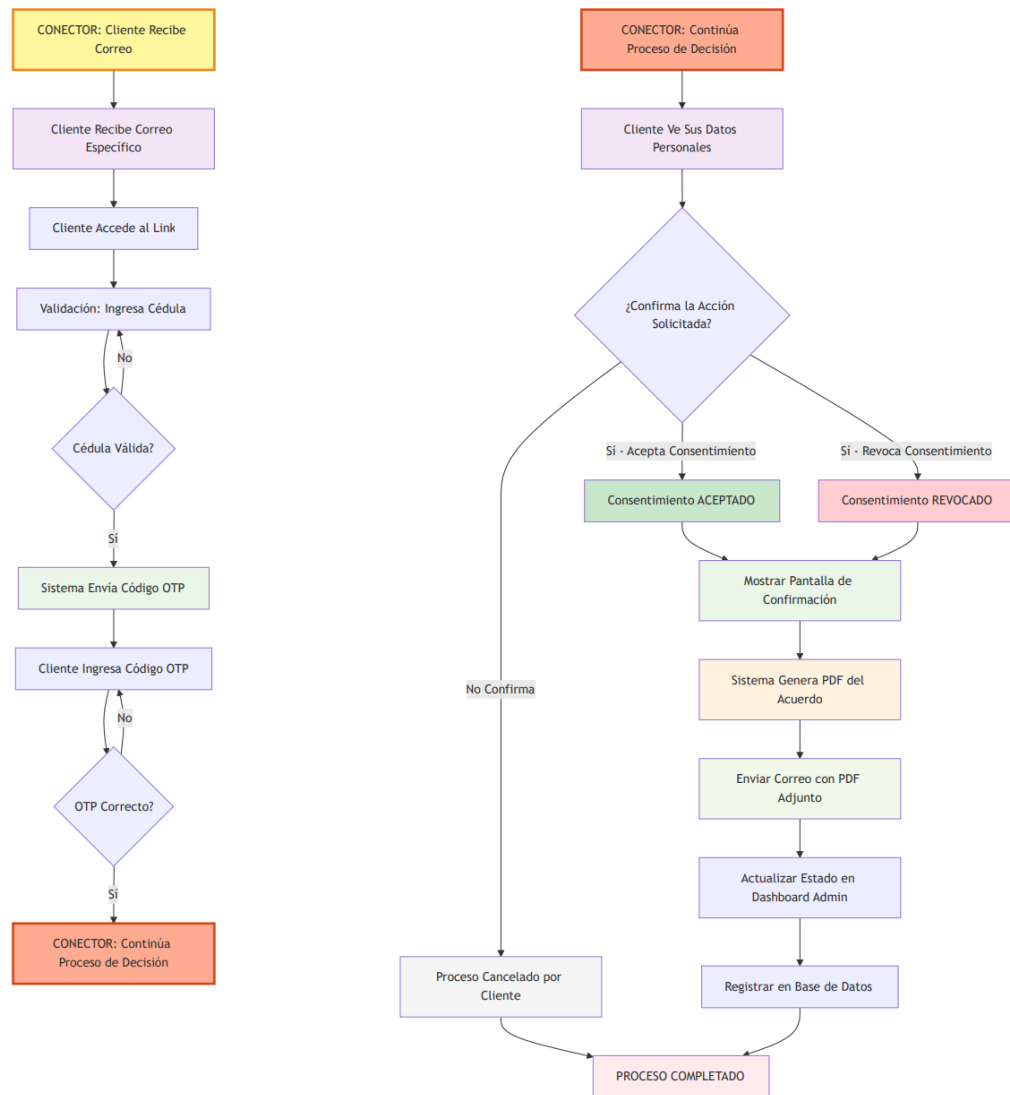


Figura 2. Parte 2 y Parte 3 - Flujo de proceso del Software
Fuente: Propia

El sistema para la obtención del consentimiento de tratamiento de datos personales es un proyecto realizado en Microsoft .NET Core 8 y base de datos de SQL Server 2022. El proyecto se diseñó en una arquitectura orientada a servicios que consta de 3 capas: aplicación, infraestructura y web, cada una de estas capas representan un pilar fundamental del correcto funcionamiento del aplicativo.

El desarrollo siguió una metodología ágil con sprints en un total de 3 meses:

Sprint 1-2: Desarrollo del módulo de consentimiento

- **Método de envío de mecanismo de consentimiento**

Para el envío de la solicitud de consentimiento de tratamiento de datos personales se optó la vía del correo electrónico ya que al momento de la firma del contrato de servicio el ISP solicita al socio una dirección de correo.

- **Seguridad de entrega de datos**

Para garantizar la legitimidad de los datos cada correo enviado tiene un enlace compuesto por la URL del sistema más un token que se valida con la base de datos de los clientes ingresados, es así que para solicitar la aprobación o cancelación del tratamiento el cliente debe conocer su número de cedula y contar con acceso a su correo electrónico registrado en el momento de la firma del contrato, ya que a este se destinaran OTPs para validar las acciones tomadas y las notificaciones de estas.

- **OTP (One Time Password)**

Para incrementar la seguridad del proceso se optó por la utilización de un OTP de 6 dígitos el cual se envía al correo registrado por los socios al momento de la firma de sus contratos.

- **Notificación y fin de proceso**

Una vez aceptado o revocado el tratamiento se notifica al cliente mediante correo electrónico la decisión tomada, en el caso de la aceptación se adjunta a dicho correo el ejemplar de su acuerdo de tratamiento de datos personales y para el caso de la negación u oposición se notifica con un texto de igual manera enviado mediante un correo electrónico.

- **Almacenamiento de evidencias**

Para manejar las evidencias el sistema guarda los documentos de acuerdo de tratamiento de datos personales en formato PDF los mismo que pueden ser visualizados por el administrador del sistema.

- **Trazabilidad**

Para poder validar la trazabilidad de los acuerdos de tratamiento de datos personales se almacenan registros de detalles del momento de la aceptación o rechazo del acuerdo, los datos más relevantes que se guardan son: Navegador, IP Publica, fecha y hora de la aceptación o negación.

- **Sprint 3-4: Implementación del gestor de tratamientos**

Se vio la necesidad de la implementación de un procedimiento para el envío de los acuerdos ya sea de manera unitario o masivo por lo que se desarrolló en el módulo clientes estas opciones permitiendo a la empresa poder gestionar de mejor manera el envío de las solicitudes de acuerdo de tratamiento de datos personales.

De igual manera se desarrolló un Dashboard donde se muestran estadísticas a tiempo real donde se puede apreciar el número de acuerdos aceptados, revocados o pendientes.

- **Sprint 5-6: Pruebas y optimización.**

Para un mejor control y revisión se implementó en esta última fase un módulo de reportes, donde los administradores del sistema pueden obtener información como el listado de los acuerdos aceptados o rechazados en un rango de fechas establecidas por el administrador, dichos datos pueden ser exportados a un Excel.

Para las pruebas se las llevó a cabo en dos ambientes, desarrollo y producción, en desarrollo con datos simulados y utilizando correos electrónicos propios para un mejor control y en producción con datos de los clientes internos que son los colaboradores de la empresa.

3.7 Validación técnica

Las pruebas se las realizó con datos controlados, la muestra con la que se realizaron las pruebas son los clientes internos de la empresa es decir sus colaboradores, para una correcta comparación se obtuvo el consentimiento de tratamiento de datos personales por dos métodos: un método manual el cual consistía en la impresión del acuerdo de tratamiento y firma con rubrica o el estampado de una firma digital en un

documento .PDF (ANEXO 1) y por otra parte el consentimiento obtenido mediante el sistema implementado en la empresa.

3.8 Técnicas y herramientas

Se compararon los tiempos de ejecución manual y automatizado de la obtención de consentimiento de tratamiento de datos personales, en una entrevista realizada a la encargada del procedimiento notifico que los tiempos que toma realizar este proceso es variable ya que existían trabajadores en la ciudad y misma oficina que desde la notificación no les tomo más de 15 minutos realizarlo pero por otra parte se vio un obstáculo ya que al existir oficinas separadas geográficamente los empleados que no contaban con firma electrónica tuvieron que hacerlo de forma manual y enviar estos documentos firmados por valijas que llego a tomar un tiempo de hasta 2 días.

De igual manera se utilizó una encuesta realizada en Microsoft Forms donde se pudo medir la satisfacción del usuario.

Fase 3: Evaluación del impacto (Objetivo Específico 3)

3.9 Definición de métricas de evaluación

3.9.1 Eficiencia operativa

- **Tiempo promedio de procesamiento de consentimientos (antes vs después)**

Antes: de 15 minutos a 2 días.

Después: Se estima <10 minutos.

- **Reducción de recursos humanos dedicados a gestión manual**

La interacción humana se vio reducida a un administrador del sistema que envía las notificaciones mediante correo electrónico mientras que antes se veían involucrados más personal como atención al cliente, miembros del Call Center o secretaria de cada oficina para notificar a los clientes y el encargado del proceso.

- **Tasa de automatización de procesos.**

El proceso se podría definir como semiautomatizado ya que aún es necesario la interacción humana que en este caso es el administrador del sistema que es quien determina a quién y cuándo enviar las notificaciones para la aceptación o negación del acuerdo de tratamiento de datos personales.

3.9.2 Cumplimiento normativo

- **Porcentaje de consentimientos válidos según LOPDP.**

En la prueba que se realizó con los datos entregados por parte de la empresa se esperaba obtener un 100% de respuesta de aceptación de tratamiento de datos personales.

En el caso de no obtener la aceptación de consentimiento de tratamiento de datos personales la empresa no podrá hacer uso de los datos de los clientes y deberá definir políticas para estos casos particulares

3.9.3 Experiencia del usuario

- **Tasa de finalización del proceso de consentimiento**

Se estimo que la finalización del proceso obtendría una tasa del 100%.

- **Tiempo promedio para completar el consentimiento**

Estos datos se obtuvieron aplicando un Script a la Base de Datos y aplicando la fórmula de:

$$\text{Tiempo Promedio (TP)} = \frac{\text{Suma de los tiempos de duración (STD)}}{\text{Número total de miembros (N)}}$$

- **Satisfacción del usuario.**

Mediante una encuesta que se realizó a los usuarios se pretendía obtener que el 100% de los usuarios reconocerían generalmente estar satisfechos con la experiencia de la aceptación de tratamiento de datos personales.

En el ANEXO 2 se muestra la encuesta realizada para la medición de satisfacción del usuario.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 Criterios técnicos y legales

Según el análisis documental referente a la normativa legal vigente en el país en materia de protección de datos personales, el presente trabajo se enfocó en los artículos relevantes de las normativas legales vigentes lo que permitió el desarrollo del proyecto tomando en cuenta que en la LOPDP en el Artículo 8 establece que el consentimiento debe manifestarse de manera libre, específica, informada e inequívoca, estas exigencias implican la toma de decisiones técnicas que deberán ser reflejadas en el desarrollo del proyecto.

Por ejemplo, para la exigencia de una decisión “libre” se implementaron mecanismos de aceptación y revocamiento de consentimiento del tratamiento de datos personales sin implicar sanciones o penalizaciones al rechazo en cuanto al carácter “específico” el sistema se diseñó dos correos con características similares, pero con objetivos totalmente opuestos que claramente muestran e informan el procedimiento a realizarse para que de esta manera no se pueda tomar una decisión inequívoca como se muestra en la siguiente imagen.

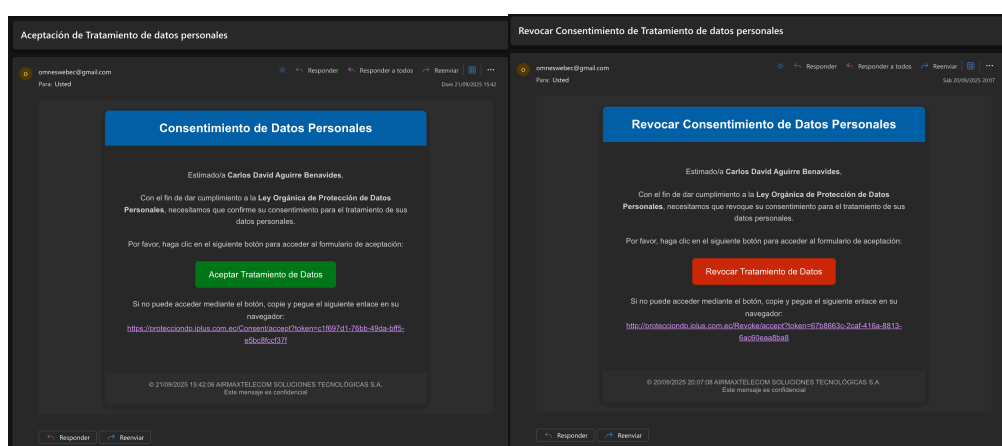


Figura 3. Procedimiento de tratamiento de consentimiento de datos personales

Fuente: Correo electrónico utilizado para pruebas.

Por lo que se determinó la necesidad del desarrollo del sistema que permita la gestión para la obtención del consentimiento de tratamiento de datos personales que

permita a la empresa de telecomunicaciones cumplir con la normativa vigente y evitar sanciones económicas y administrativas.

4.2 El prototipo desarrollado

Para el desarrollo del sistema se optó por una Arquitectura Orientada a Servicios en la que se cuenta con 3 capas:

- **Aplicación:** En esta capa se mapean los modelos de las bases de datos, enums que son las variables definidas o constantes y modelos que son clases para ser usadas en la aplicación.
- **Infraestructura:** Maneja los servicios como correo electrónico, clientes, Generación de Tokens, y generación de OTPs, así como las operaciones de Base de Datos.
- **Web:** Esta capa es la de presentación prácticamente es el FrontEnd del proyecto lo visual que muestra el navegador web tanto al administrador del sistema como los clientes.

El proyecto fue realizado en Microsoft .Net Core 8 y base de datos de SQL Server 2022 su diagrama se presenta en el ANEXO 3, desplegados en un servidor propiedad de la empresa y con salida a internet a través de una IP pública. El despliegue del proyecto se lo realizó mediante el ISS (Internet Information Services Manager) es una herramienta gráfica proporcionada por Microsoft para administrar de forma remota y local los servidores web IIS, como adicional se agregó un certificado SSL al ISS para mantener una navegación segura en el sitio. El proyecto permite cumplir con los requisitos establecidos tanto en la LOPDP y la necesidad de la empresa de telecomunicaciones para el desarrollo de su proceso de obtención de consentimiento de tratamiento de datos personales.

El prototipo desarrollado cuenta con módulos y funciones para el administrador del sistema como:

Pantalla de Login: El administrador del sistema con sus credenciales es capaz de ingresar al sistema para la gestión del consentimiento de tratamiento de datos personales de los clientes de la empresa de telecomunicaciones.



Figura 4. Página login de administrador del sistema

Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto

Dashboard: Pantalla con información general y a tiempo real del estado de la aceptación, negación y procesos pendientes de los acuerdos de tratamiento enviados a los clientes.

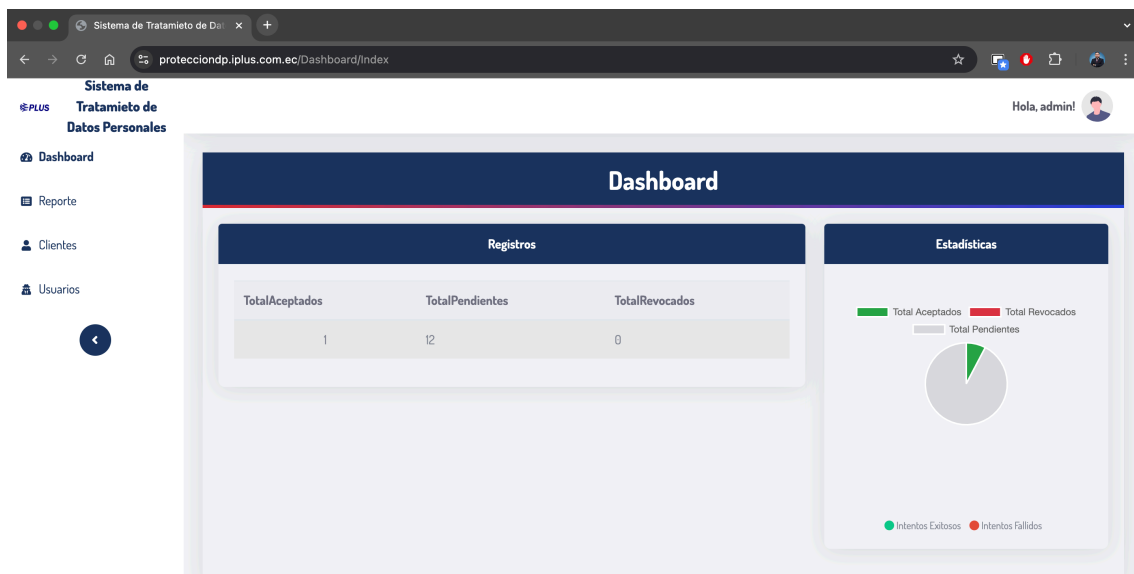


Figura 5. Pantalla Dashboard con información en tiempo real

Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto

Reporte: En este módulo se puede obtener reportes detallados sobre clientes que han aceptado o negado el acuerdo de tratamiento de datos personales, para la generación

de los reportes se debe escoger una fecha de inicio y fin y una vez generada se muestra en pantalla y de igual manera es posible exportar estos datos a una hoja de Excel el cual se muestra en el ANEXO 4.

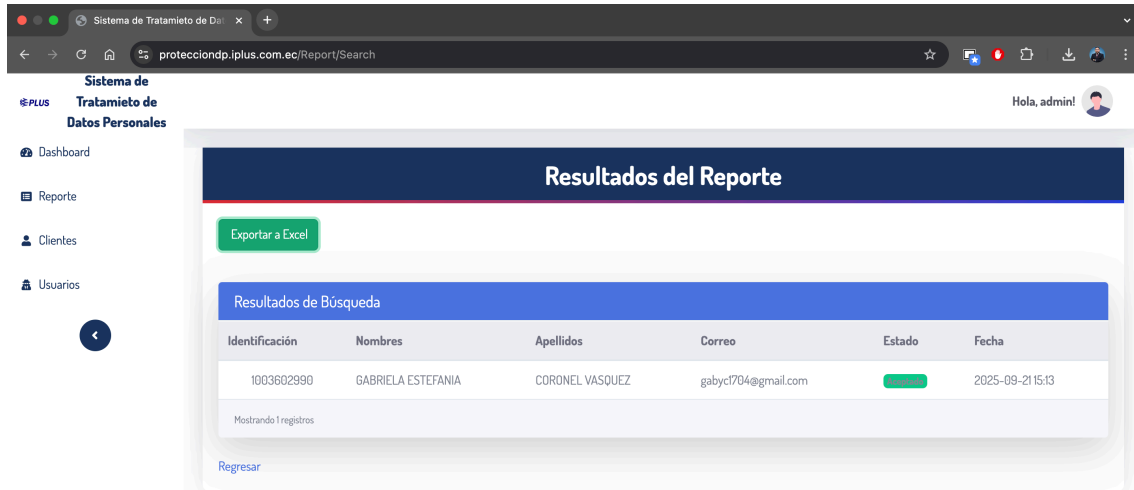


Figura 6. Sección de resultados de reporte de consentimientos

Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto

Cientes: En este módulo se puede observar los clientes registrados listados con campos como identificación, nombres, apellidos, correo electrónico, estado y acciones como “Detalles” que muestra información del cliente y el detalle de su estado actual de consentimiento. “Enviar” que permite realizar el envío del correo electrónico al cliente para que pueda acceder a dar su consentimiento de tratamiento y por último la acción de “Revocar” que de igual manera envía un correo que permite al cliente revocar su autorización.

Para el envío masivo de correos electrónicos de solicitud de consentimiento el tratamiento de datos personales el administrador cuenta con una serie de filtros que permiten seleccionar a varios clientes y un botón de “Enviar a seleccionados”

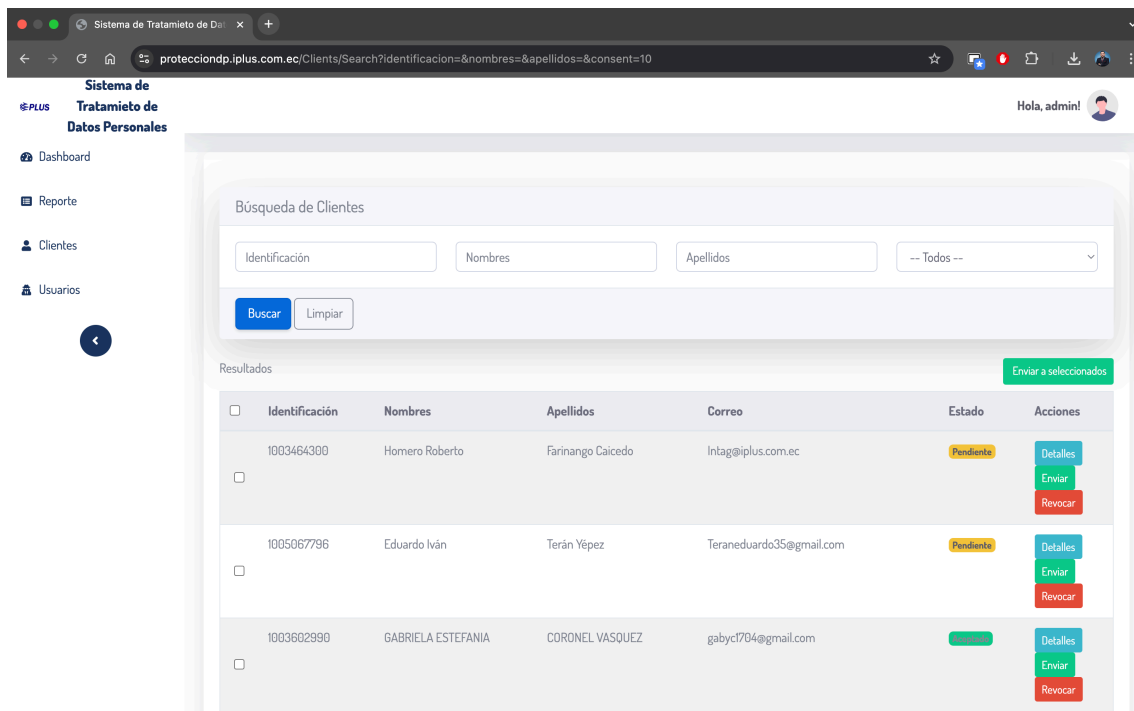


Figura 7. Sección de visualización de clientes y envíos de correo individual o masivos
Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto.

Usuarios: En este módulo se puede gestionar la creación y eliminación de usuarios que pueden acceder al aplicativo, como controles en este módulo se propuso que un usuario no pueda eliminar el acceso a su mismo usuario.

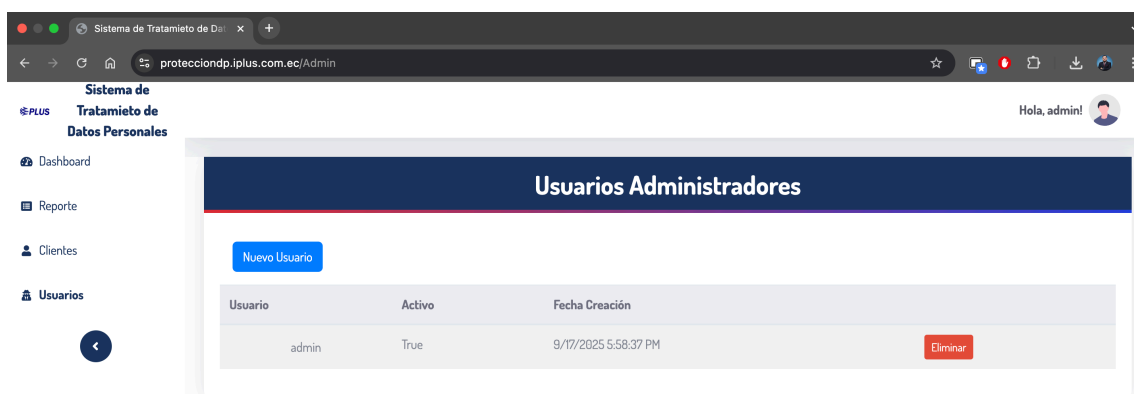


Figura 8. Gestión de usuarios
Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto

Y por otra parte una interfaz para los clientes, donde se puede realizar las acciones de aprobación o revocamiento del consentimiento de tratamiento de datos personales

totalmente intuitivos e informados, en los que se incluye el envío de un correo electrónico el mismo que contiene un link al que el cliente debe acceder para aceptar o revocar el consentimiento de tratamiento de datos personales según la opción que haya sido enviada por el administrador del sistema.

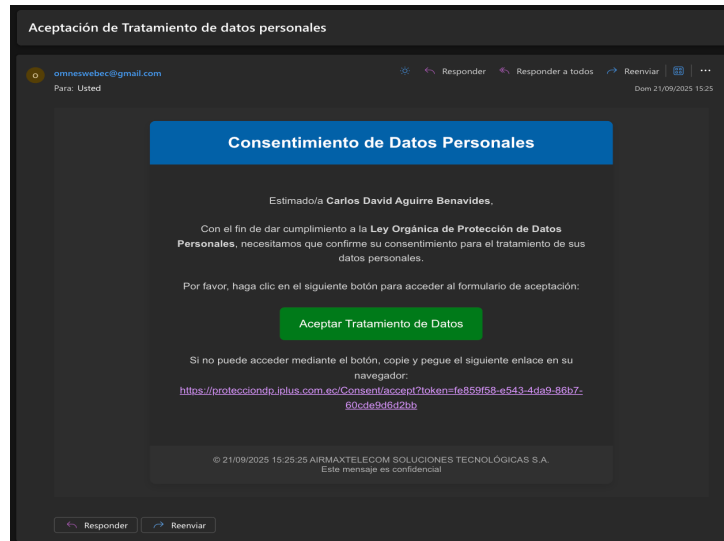


Figura 9. Correo recibido para inicio de proceso de consentimiento por parte del cliente
Fuente: Correo electrónico utilizado para pruebas

Una vez que el cliente haya accedido al link se muestra el proceso en donde se debe ingresar su número de cedula para validar que dicho link pertenece al cliente.

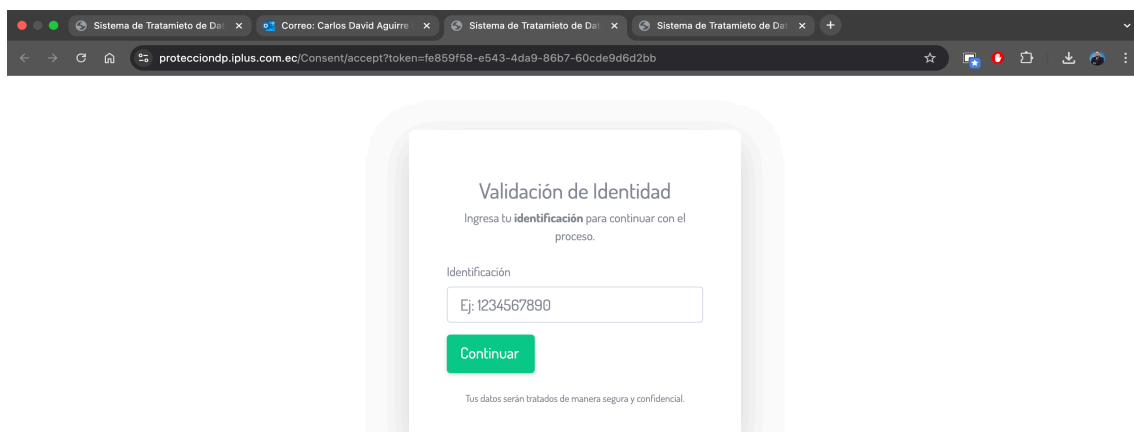


Figura 10. Ingreso de datos para la validación de identidad
Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto

Seguido de esto el sistema genera un código OTP con una validez de 5 minutos, este OTP es enviado por correo electrónico a la dirección registrada por el cliente al momento de la firma de su contrato de servicios con la empresa.

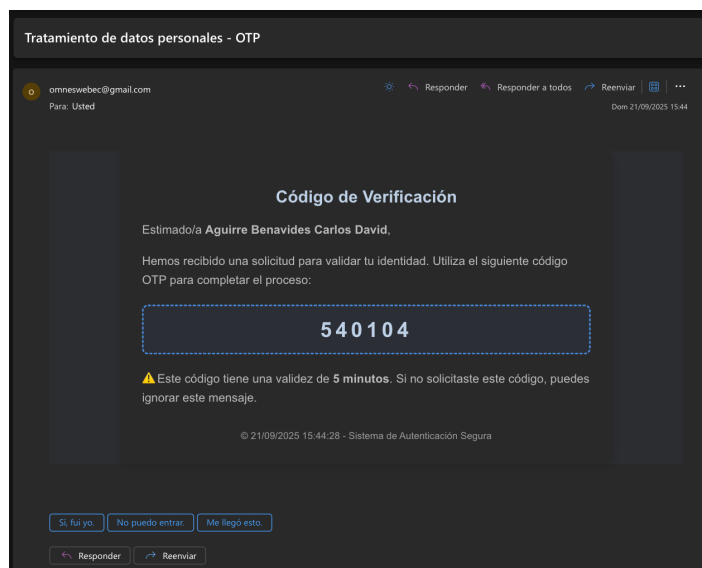


Figura 11. Correo recibido por el cliente con OTP enviado por el sistema
Fuente: Correo electrónico utilizado para pruebas

El cliente deberá introducir el código enviado en la casilla de texto para seguir con el proceso

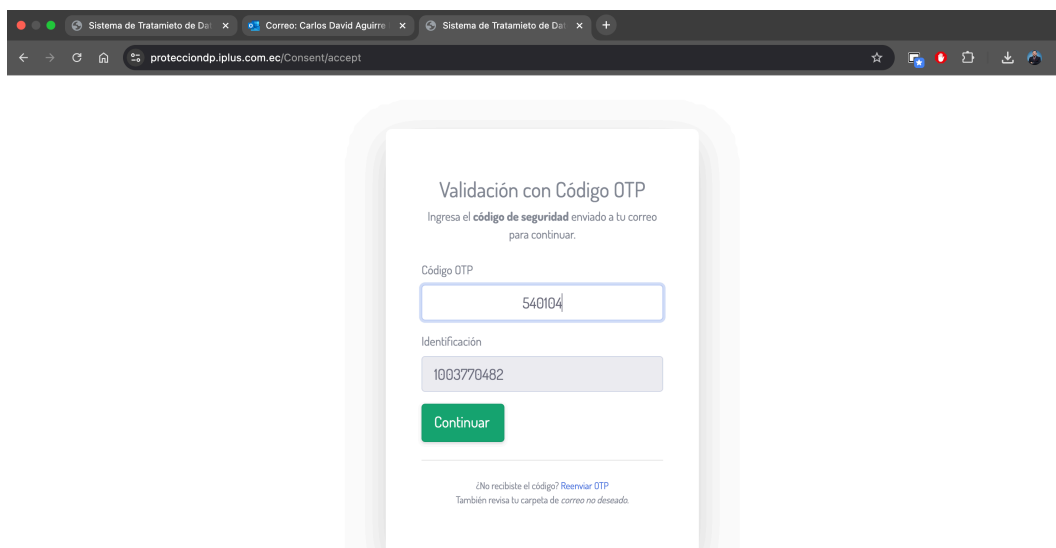


Figura 12.Introducción de código OTP

Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto

A continuación, se presenta una pantalla en la que los datos del cliente están precargados, sin posibilidad de edición, en esta pantalla se debe dar check en la casilla para aceptar el

consentimiento del tratamiento de sus datos personales en el caso que sus datos sean correctos.

Formulario de Consentimiento

Verifica que tus datos sean correctos y marca la casilla si aceptas el tratamiento de tus datos personales.

Identificación
1003770482

Nombres
Carlos David

Apellidos
Aguirre Benavides

Correo
cdaguirreb@hotmail.com

TeléfonoMóvil
099676563

TeléfonoFijo

Acepto el tratamiento de mis datos personales
Al marcar esta casilla, autorizo el uso de mis datos conforme a la Ley Orgánica de Protección de Datos Personales.

Continuar

Tus datos serán tratados conforme a la Ley de Protección de Datos Personales.

Figura 13. Presentación de datos del cliente para su verificación

Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto

Una vez finalizado el proceso, el cliente puede observar una pantalla en el que se muestra que el proceso de su aceptación del consentimiento de tratamiento de datos personales termino.

¡Proceso Exitoso!

Los datos del cliente han sido procesados correctamente.

Identificación	1003770482
Nombres	Carlos David
Apellidos	Aguirre Benavides
Correo	cdaguirreb@hotmail.com
TeléfonoMóvil	099676563
TeléfonoFijo	
Acepto el tratamiento de mis datos personales	<input checked="" type="checkbox"/>

Figura 14. Finalización de proceso con éxito

Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto.

Y para finalizar el proceso, el sistema envía automáticamente un correo electrónico informando al cliente su decisión, en dicho correo adjunta un ejemplar del acuerdo aceptado o revocado ANEXO 5.

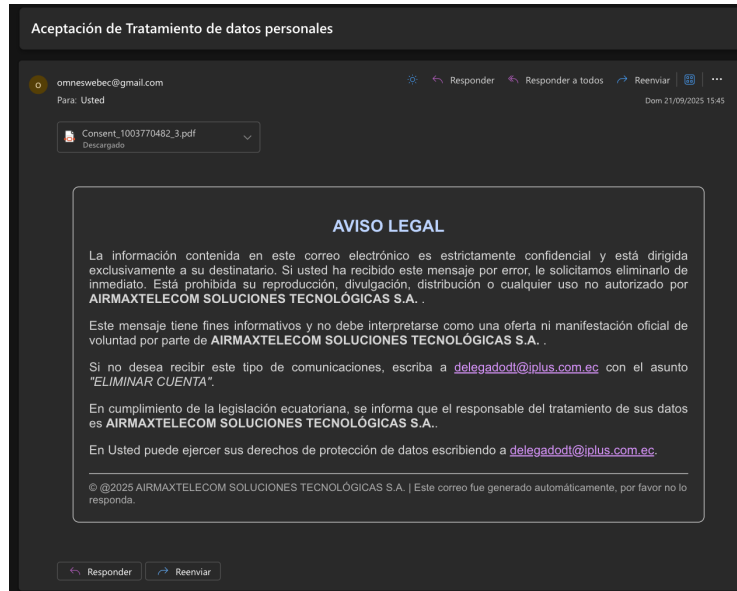


Figura 15. Correo electrónico con información de acuerdo en formato PDF
Fuente: Correo electrónico utilizado para pruebas

Todas las acciones realizadas por parte del titular cuentan con medidas de seguridad que permiten que, el titular de los datos sea el único que pueda aprobar o revocar el consentimiento, esto se logra gracias al envío de códigos OTP al correo registrado al momento de la firma del contrato de servicio.

El prototipo es totalmente funcional y cumple con su propósito.

4.3 Porcentaje de consentimientos válidos según LOPDP y tasa de finalización del proceso de consentimiento.

En la prueba realizada a los colaboradores de la empresa, se obtiene un 100% de respuesta de aceptación de tratamiento de datos personales como se muestra en la siguiente imagen, donde de igual manera se muestra 0 solicitudes pendientes lo que también indica que la tasa de finalización es de un 100%.

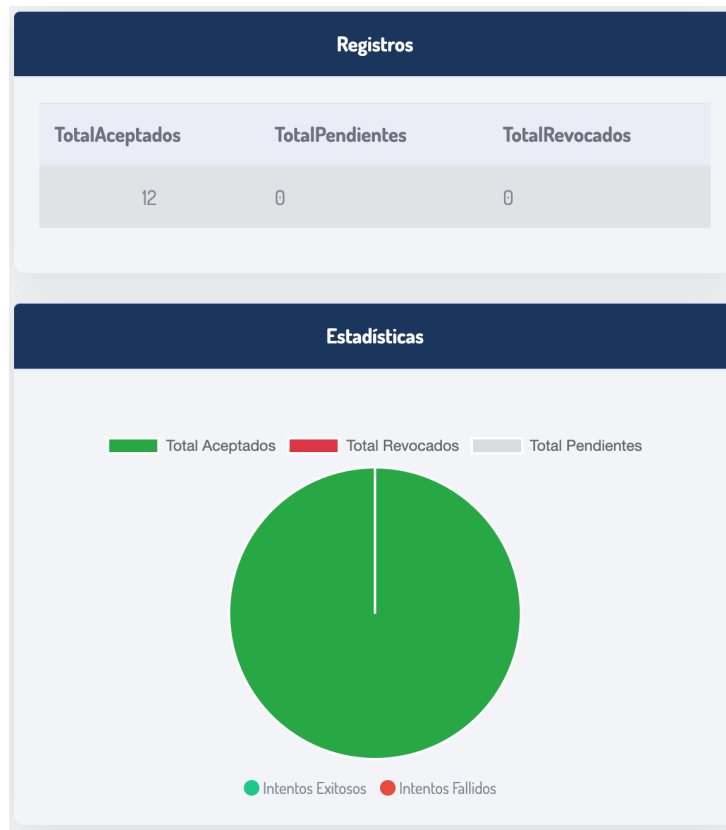


Figura 16. Porcentaje de consentimientos validados

Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto.

Tiempo promedio para completar el consentimiento

Para la obtención de estos datos se ha aplicado un script a la Base de Datos del cual se obtuvo el tiempo que empleó cada miembro de la prueba desde que recibió el correo inicial hasta que consintió el tratamiento de sus datos, los resultados obtenidos son los que se muestran en la siguiente imagen.

```

1 SELECT cli.Nombres , cli.Apellidos, Fecha_Mail =lt.CreatedAtUtc,
2 Fecha_Acepta =con.EffectiveAtUtc,
3 DURACION= DATEDIFF(MINUTE, lt.CreatedAtUtc, con.EffectiveAtUtc)
4 FROM Clients cli inner join
5 LinkTokens lt on cli.Id = lt.ClientId
6 inner join Consents con on con.ClientId= cli.Id
7 where lt.ConsumedAtUtc is not null
8 and lt.Purpose=1
9 AND CON.Status=1

```

	Nombres	Apellidos	Fecha_Mail	Fecha_Acepta	DURACION
1	GABRIELA ESTEFANIA	CORONEL VASQUEZ	2025-09-21 15:11:44.303	2025-09-21 15:13:00.810	2
2	Luis Israel	Cadena Portilla	2025-09-21 15:46:55.143	2025-09-21 16:01:00.880	15
3	Mario Leonado	Silva Garcia	2025-09-21 16:23:59.383	2025-09-21 16:26:03.187	3
4	Eduardo Iván	Terán Yépez	2025-09-21 16:32:28.713	2025-09-21 16:36:45.357	4
5	Carlos Andres	Benavides Sanchez	2025-09-21 16:43:11.847	2025-09-21 16:45:39.423	2
6	JONATHAN JAVIER	CALDERON GRIJALVA	2025-09-21 16:46:04.257	2025-09-21 16:50:27.897	4
7	CRISTIAN VINICIO	ICHAU AREVALO	2025-09-21 18:29:10.800	2025-09-21 18:37:01.680	8
8	Homero Roberto	Farinango Caicedo	2025-09-21 18:58:34.093	2025-09-21 19:06:36.423	8
9	Bryan Amulfo	Ruiz Cruz	2025-09-21 18:58:22.757	2025-09-21 19:11:08.757	13
10	DENIS XAVIER	MEJIA RUIZ	2025-09-21 19:10:03.000	2025-09-21 19:14:39.813	4
11	Lizeth Guadalupe	Maldonado Rosero	2025-09-21 20:35:41.357	2025-09-21 20:37:30.060	2
12	Gabriela Alexandra	Farinango Vinueza	2025-09-21 20:56:30.050	2025-09-21 20:59:30.497	3

Figura 17. Script de la Base de Datos

Fuente: Sistema de consentimiento de tratamiento de datos personales desarrollado en este proyecto.

Los cálculos que realiza el Script es una resta de tiempo entre los datos de la columna Fecha_Mail y la columna Fecha_Acepta dándonos como respuesta la columna DURACION la cual fue expresada en minutos.

Con estos datos y conociendo el número de personas participantes en la prueba se realiza el siguiente calculo:

Tiempo Promedio (TP) = Suma de los tiempos de duración (STD) / Número total de miembros (N)

STD= 68 minutos

N= 12

TP=68/12

TP=5.66 minutos

Instrumentos de evaluación:

Cuadro comparativo tiempos

Para el análisis del cuadro comparativo se obtuvieron datos tanto entregados por la empresa de telecomunicaciones como el promedio del tiempo del proceso manual para la obtención de consentimiento de tratamiento de datos el cual es de 15 minutos

Y por otro lado el tiempo de proceso automatizado que se obtuvo mediante el cálculo de promedio de los tiempos de los consentimientos procesados por el sistema el cual fue de 5.66 minutos.

Tabla 2

Cuadro comparativo tiempos

Proceso/Tarea	Tiempo Manual (tm)	Tiempo Automatizado (ta)	Diferencia Absoluta (Δt)	Diferencia Relativa (%)	Eficiencia (E)
Obtención de acuerdo de tratamiento de datos personales	15 min	5.66 min	$t_m - t_a$	$((t_m - t_a) / t_m) \times 100$	t_m / t_a

Fórmulas Aplicadas:

- **Diferencia Absoluta (Δt):**

$$\Delta t = t_m - t_a$$

Donde:

t_m es el tiempo promedio manual.

t_a es el tiempo promedio automatizado

$$\Delta t = 15 \text{ min} - 5.66 \text{ min}$$

$$\Delta t = 9.34 \text{ min}$$

- **Diferencia Relativa (Porcentaje de mejora):**

$$\% \text{Mejora} = ((t_m - t_a) / t_m) \times 100$$

Donde:

t_m es el tiempo promedio manual.

t_a es el tiempo promedio automatizado

$$\% \text{Mejora} = ((15 \text{ min} - 5.66 \text{ min}) / 15 \text{ min}) \times 100$$

$$\% \text{Mejora} = 62.26\%$$

- **Factor de Eficiencia (E):**

$$E = t_m / t_a$$

$$E = 15 \text{ min} / 5.66 \text{ min}$$

Donde:

t_m es el tiempo promedio manual.

t_a es el tiempo promedio automatizado

$$E = 2.65$$

Donde $E > 1$ indica que la automatización es más eficiente.

○ **Análisis de Productividad**

Capacidad Manual = $60\text{min} \div 15\text{min} = 4$ consentimientos/hora

Capacidad Automatizada = $60\text{min} \div 5.66\text{min} = 11$ consentimientos/hora aprox.

Incremento de Productividad = 175% (2.75x más productivo)

Significancia de los Resultados:

$E = 2,65$: La automatización es 2.65 veces más eficiente indicando una automatización altamente efectiva.

62.26% de mejora: Reducción significativa del tiempo de proceso

ROI temporal: 175% de incremento en productividad

Reducción de 9.34 minutos por proceso

Implicaciones para Ciberseguridad:

Menor tiempo de exposición durante el proceso

Respuesta más rápida a solicitudes de consentimiento

Mayor agilidad en cumplimiento normativo ante LOPDP

El presente análisis respalda la implementación del sistema automatizado de consentimiento de tratamiento de datos personales desde una perspectiva de eficiencia operacional y cumplimiento normativo en ciberseguridad alineado a los requerimientos de la LOPDP.

4.4 Encuestas de satisfacción validadas

Mediante una encuesta realizada a todos los miembros de la muestra seleccionada se obtuvieron resultados muy alentadores que demuestran de manera general que la experiencia de usuario fue muy positiva y en el análisis de cada una de las preguntas que se plantearon se encontraron los siguientes resultados:

Pregunta 1: ¿Cómo califica la facilidad para otorgar su consentimiento a través de nuestro sistema?

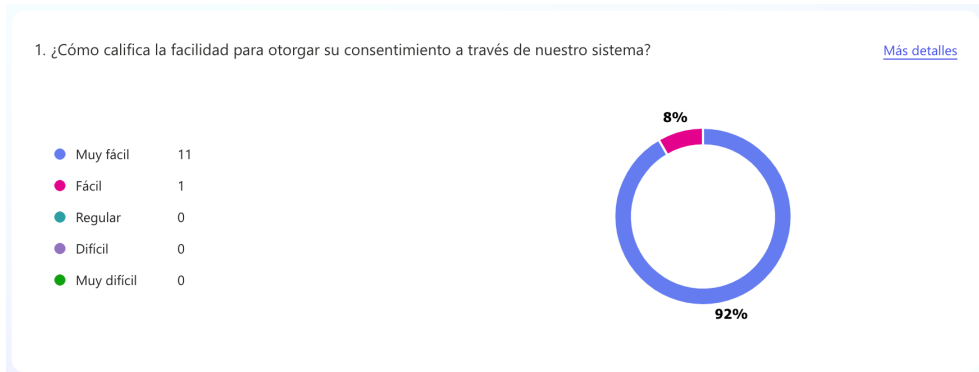


Figura 18.Factibilidad de consentimiento

Fuente: Encuesta de satisfacción de usuarios de la empresa de telecomunicaciones.

Los resultados obtenidos muestran un nivel alto de usabilidad del nuevo sistema tomando en cuenta que solo existen respuestas positivas lo que implica que la experiencia de usuario fue altamente positiva, y se podría inferir que el nivel de abandono del proceso es muy bajo por lo que se asumiría que lograr conseguir consentimientos con este sistema es muy probable y factible.

Pregunta 2: ¿Qué tan clara y comprensible fue la información sobre el tratamiento de sus datos personales?

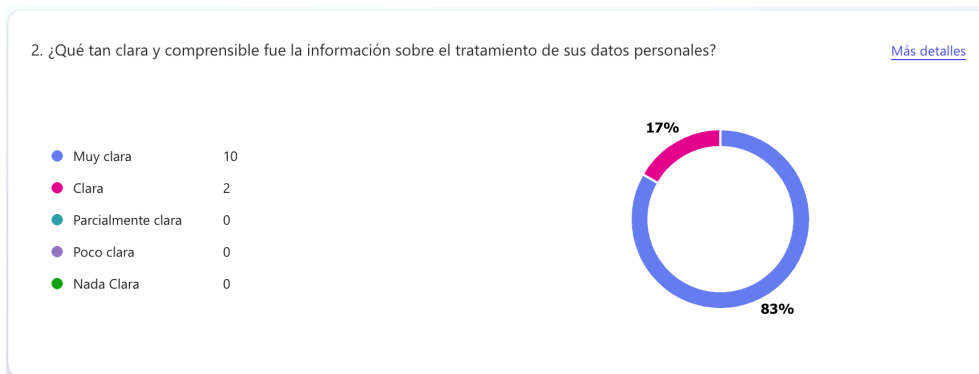


Figura 19.Claridad y comprensión del tratamiento de datos

Fuente: Encuesta de satisfacción de usuarios de la empresa de telecomunicaciones.

Los resultados obtenidos muestran que los usuarios comprendieron la información correctamente lo que hace que el cumplimiento normativo sea satisfactorio porque la claridad de la información es un requisito legal fundamental para la LOPDP y esto conlleva a minimizar los posibles reclamos de los clientes por falta de información o consentimientos no informados.

Pregunta 3: ¿Qué tan seguro se sintió al proporcionar su consentimiento a través de este sistema?

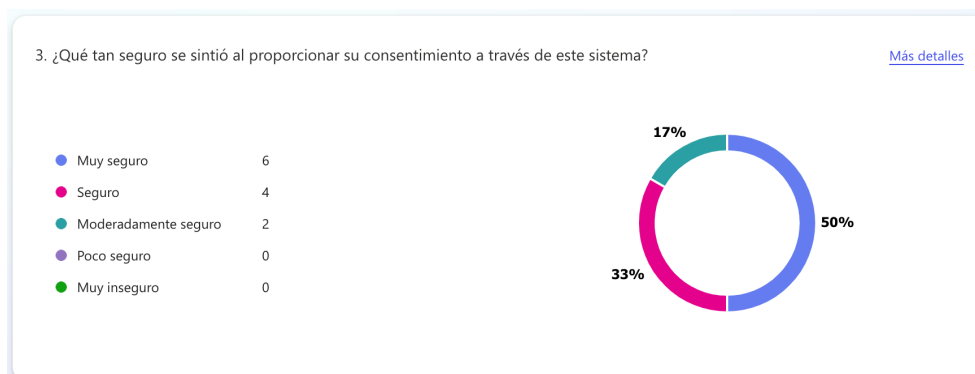


Figura 20. Sentido de seguridad en brindar información
Fuente: Encuesta de satisfacción de usuarios de la empresa de telecomunicaciones.

Con estos resultados se puede decir la confianza es un tema para mejorar al momento de la obtención de consentimientos, aunque ningún encuestado se muestra poco seguro o inseguro es necesario que la empresa genere la confianza a sus clientes de utilizar el nuevo sistema comunicando las medidas de seguridad implementadas.

Pregunta 4: ¿Cuál es su nivel de satisfacción general con el sistema de consentimiento para el tratamiento de datos personales?

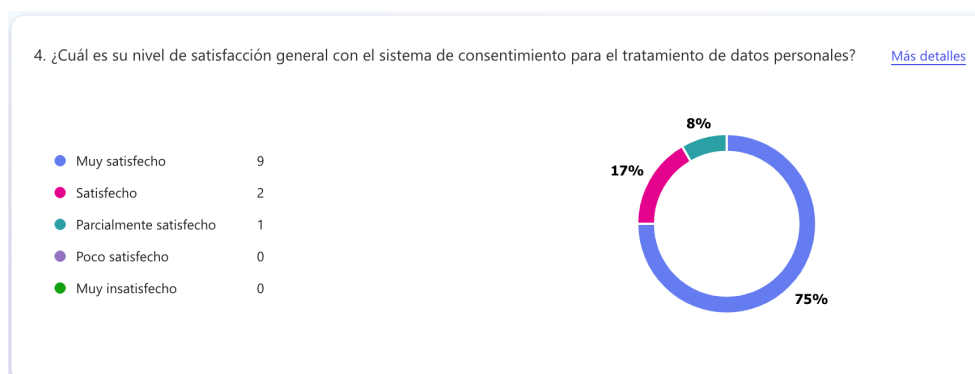


Figura 21. Nivel de satisfacción
Fuente: Encuesta de satisfacción de usuarios de la empresa de telecomunicaciones.

A pesar de la parcial inseguridad percibida se podría decir que la satisfacción general es muy alta indicando la efectividad del cumplimiento del propósito del sistema por lo que se podría afirmar que el desarrollo del sistema está encaminado correctamente.

4.4.1. Validación de la Encuesta

Para tener una evaluación de la validez de la encuesta se optó por aplicar un análisis de correlación Pearson mediante el uso del software Jamovi con una muestra: n = 12 participantes y una escala: 1-5 (5 = máximo).

Tabla 3 Respuestas obtenidas de la encuesta en una escala del 1 - 5

Individuo	Facilidad	Claridad	Seguridad	Satisfacción
1	5	5	5	5
2	5	4	4	4
3	5	5	4	5
4	5	5	5	5
5	5	5	4	5
6	5	5	5	5
7	5	5	5	5
8	4	4	3	3
9	5	5	5	5
10	5	5	5	5
11	5	5	4	4
12	5	5	3	5

La correlación obtenida mediante el software es la siguiente

Matriz de Correlaciones

Matriz de Correlaciones		Facilidad	Claridad	Seguridad	Satisfacción
Facilidad	R de Pearson	—			
	gl	—			
	valor p	—			
Claridad	R de Pearson	0.674 *	—		
	gl	10	—		
	valor p	0.016	—		
Seguridad	R de Pearson	0.539	0.500	—	
	gl	10	10	—	
	valor p	0.070	0.098	—	
Satisfacción	R de Pearson	0.806 **	0.837 ***	0.598 *	—
	gl	10	10	10	—
	valor p	0.002	<.001	0.040	—

Nota. * p < .05, ** p < .01, *** p < .001

Figura 22. Matriz de correlacion Pearson
Fuente: Software Jamovi

Haciendo un análisis de la matriz de correlaciones de Pearson se muestra una validez excelente de la encuesta, con el 66.66% de las correlaciones siendo estadísticamente significativas (4 de 6 pares). Las correlaciones significativas incluyen Facilidad-Claridad ($r=0.674^*$, $p=0.016$), Facilidad-Satisfacción ($r=0.806^{**}$, $p=0.002$), Claridad-Satisfacción ($r=0.837^{***}$, $p<0.001$), y Seguridad-Satisfacción ($r=0.598^*$, $p=0.040$), indicando que todas las variables contribuyen de manera coherente con la de experiencia del usuario con el sistema de consentimiento de tratamiento de datos personales.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Después de un análisis del presente documento se puede concluir que los objetivos planteados para este proyecto se cumplieron de forma satisfactoria y que el documento podría ser utilizado por empresas ecuatorianas para afrontar de mejor manera el cumplimiento de la LOPDP.

El uso de la infraestructura implementada con .NET Core 8, SQL Server 2022 para el desarrollo del proyecto fue una decisión acertada, ya que cumple con el propósito por el que fue elegido, permitiendo a futuro posibles actualizaciones con forme avance el marco normativo de la LOPDP.

El aporte a la seguridad del sistema con el uso de OTPs, links únicos por cliente, certificados SSL ayudaran al sistema a evitar potenciales vulnerabilidades, se debe mencionar que la necesidad de implementar a futuro nuevos canales, a parte del correo electrónico es evidente.

Este tipo de sistemas y análisis deberían ser implementados por las empresas ecuatorianas, eliminando de forma definitiva procesos manuales que pueden presentar riesgos al momento de la gestión de los consentimientos de tratamiento de datos personales.

El sistema actual aporta a un mejor control sobre los consentimientos de tratamiento de datos personales firmados con rubrica, ya que el sistema se encarga de almacenar los documentos y permite visualizarlos, lo que aporta a la disponibilidad de la información de manera eficaz.

Si bien la aceptación del consentimiento de tratamiento de datos personales es un pilar fundamental de la LOPDP, es necesario que las empresas difundan sus políticas de protección y demás requisitos que se estipulan en la ley, para de esta manera obtener un mejor resultado al momento de la recolección de los acuerdos.

Recomendaciones

Una vez concluido el presente proyecto se podrían separar las recomendaciones en inmediatas y a largo plazo sabiendo esto.

Se recomienda brindar capacitaciones al personal en temas enmarcados a la LOPDP, incluyendo temas como implicaciones éticas y legales sobre el tratamiento de datos personales, si bien el sistema automatizado ayudara a la obtención del consentimiento de tratamiento de datos, la responsabilidad del cumplimiento total de la ley recae sobre la empresa y sus trabajadores.

De igual manera se recomienda, no descartar por completo ni de inmediato el sistema de obtención del consentimiento manual, ya que pueden existir casos específicos que no se detectaron en el desarrollo del sistema automatizado, el planteamiento de un periodo de transición será decisión de la empresa, pero se recomienda un lapso de 3 meses.

Por otra parte viendo el futuro que se le puede dar al sistema se recomienda considerar más canales para la obtención del consentimiento, estas podrían ser WhatsApp, SMS, aplicaciones móviles propias etc, esto aportaría a tener un mayor alcance sin limitar al cliente a otorgar su consentimiento por un solo canal.

La vinculación con los sistemas propios de la empresa para manejar una misma base de clientes seria optimo, aunque sistema está diseñado para gestionar una lista concreta de clientes, por escalabilidad y usabilidad se considera importante que dichos clientes sean obtenidos mediante APIs de los sistemas legacy de la empresa.

La auditoría constante de los procesos de obtención de consentimiento de tratamiento de datos podría ayudar al cumplimiento de la LOPDP y a evitar sanciones administrativas y económicas.

Se recomienda que el presente proyecto sea tomado como el inicio de un proceso de mejora continua en materia del cumplimiento normativo, si bien este es un gran avance, no es el punto de llegada, ya que se podrían implementar mejoras como por ejemplo tecnología blockchain que permitirían crear un registro inmutable y aportar con mayor seguridad a preocupaciones relacionadas a la integridad de los acuerdos.

REFERENCIAS

- Acurio, S. (2021). *Introducción a la protección de datos personales*. Obtenido de [file:///C:/Users/HP/Downloads/Diferencias_entre_intimidad_privacidad_y%20\(1\).pdf](file:///C:/Users/HP/Downloads/Diferencias_entre_intimidad_privacidad_y%20(1).pdf)
- Mila, P. (2019). Análisis exploratorio de datos a una base de datos de la biblioteca de la universidad de la salle. *Retos en la formación de ingenieros en la era digital*. Obtenido de <https://acofipapers.org/index.php/eiei/article/download/196/189/376>
- Chávez, D., & Burgos, K. (2025). Gestión de riesgos para el tratamiento de datos personales sensibles en el movimiento de mujeres de El Oro. *Darwin Chávez; Kevin Burgos*, 7(3), 11-19. Obtenido de <https://doi.org/10.59169/pentaciencias.v7i3.1505>
- Cano, N., & Jaramillo, D. (mayo de 2023). *Análisis sobre el consentimiento del titular bajo la ley de protección de datos personales*. Obtenido de <https://www.usfq.edu.ec/sites/default/files/2023-05/legallab-003.pdf>
- Esginova Group. (2018). *Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad*. Obtenido de Esginova group: <https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/>
- Asamblea Nacional. (21 de mayo de 2021). *Ley orgánica de protección de datos personales*. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

- Ponce, L. (mayo de 2021). *Todo lo que debes conocer sobre la Protección de Datos Personales*. Obtenido de <https://www.pwc.ec/es/entrevistas-de-temas-de-interes/todo-lo-que-debes-conocer-sobre-la-proteccion-de-datos-personales.html>
- García, L. (2021). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*. Obtenido de Organización de los Estados Americanos: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf
- Minguillón, J. (2019). Introducción a la visualización de datos. *Universitat Oberta de Catalunya*. Obtenido de https://www.researchgate.net/publication/330684603_La_visualizacion_de_datos_y_el_arte_de_archivo_intersecciones_senderos_y_desvios
- Palomino, Á. (2018). *Análisis de los datos técnicos*. Universidad Carlos III De Madrid, Leganés. Obtenido de <https://core.ac.uk/download/pdf/29404175.pdf>
- Brito, G. (2022). *Tribunal de jsuticia de la comunidad andina*. Obtenido de https://www.comunidadandina.org/DocOficialesFiles/Procesos/230_IP_2020.pdf
- Mato, M. (2020). Privacidad y consentimiento en el entorno digital: aproximación desde la perspectiva de la Unión Europea. *Universidad Carlos III*, 8(3). doi:<https://orcid.org/0000-0003-4194-8802>
- Blendee. (2025). *CMP – Consent Management Platform*. Obtenido de <https://blog.blendee.com/es/glossario-cdp-marketing-automation/cmp-consent-management-platform/>

- Yepez, E. (2019). *La prueba electronica en la legislación ecuatoriana*. Universidad e las Americas. Obtenido de <https://dspace.udla.edu.ec/bitstream/33000/540/1/UDLA-EC-TAB-2009-04.pdf>
- Rivera, B. (2020). La importancia de la protección de datos y la situación actual del Ecuador. *Revista de Estudios Jurídicos*. Quito , 112-122. Obtenido de Facultad de derecho.
- López, H. (2022). *Stack tecnológico del curso aceleración en java*. Obtenido de AceleraTI:
<https://acelerati.co/hubfs/Stack%20Tecnol%C3%B3gico%20del%20Curso%20de%20Aceleraci%C3%B3n%20en%20Java.pdf?hsLang=es-co>
- Bermeo, J. (2020). *Análisis de la regulación de telecomunicaciones en el Ecuador y las nuevas tendencias del sector*. Universidad Politecnica Salesiana. Obtenido de <https://dspace.ups.edu.ec/bitstream/123456789/2739/11/UPS-CT002287.pdf>
- Comunidad Andina de Naciones. (2022). *Decisión 897 CAN*. Peru.

ANEXOS

ANEXO 1: Consentimiento físico del proceso manual.

ACUERDO DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES PARA CLIENTES DE

I. COMPARECEN:

_____ en adelante _____

2. EL CLIENTE

II. OBJETO

El presente acuerdo establece los términos y condiciones para el uso de datos personales del CLIENTE por parte de _____

III. DEFINICIONES

En el presente acuerdo se utilizarán términos como: datos personales, tratamiento, encargo, transferencia, cesión y demás cuya definición estará a lo establecido en el artículo 4 de la Ley Orgánica de Protección de Datos Personales.

IV. CONSENTIMIENTO Y FINALIDAD

EL CLIENTE autoriza expresamente a _____ para el tratamiento y transferencia de sus datos personales para las siguientes finalidades:

- Gestionar la prestación de los servicios de internet contratados, incluyendo la facturación y soporte técnico.
- Mejorar la experiencia del cliente mediante estudios de calidad y encuestas de satisfacción.
- Cumplir con obligaciones legales y regulatorias derivadas de la prestación del servicio.
- Implementar medidas de seguridad para garantizar la protección de la información personal del cliente.
- Responder y proveer respuesta a quejas y reclamos de servicios.
- Enviar información de nuevos servicios, documentos electrónicos, tarifas, recordatorios de pago, promociones, eventos e información de interés para clientes.
- Consultar y registrar la calificación crediticia de los clientes que solicitan créditos.
- Tratar los datos generados por la navegación y uso de la página web de _____
- Mantener una comunicación permanente y abierta con el cliente, utilizando canales y plataformas WhatsApp, Instagram, Telegram, Facebook Messenger, llamadas telefónicas, mensajes de texto, entre otros.

V. DATOS PERSONALES TRATADOS

_____ tratará los siguientes datos personales del CLIENTE:

- Nombre y apellidos.
- Dirección de domicilio o lugar en el cual se recibirá el servicio.
- Teléfonos personales.
- Correo electrónico.
- Número de RUC
- Número de cédula.
- Referencias comerciales

Página 1 de 3

- Número de cuentas bancarias (En caso de débito automático)

VI. TRANSFERENCIA DE DATOS

_____ podrá transferir los datos personales del CLIENTE a:

- Proveedores de software o programas de almacenamiento de datos (nubes)
- Burós de crédito.
- Proveedores de software financiero y contable.
- Instituciones financieras nacionales.
- Jueces y autoridades gubernamentales.

VII. MEDIDAS DE SEGURIDAD

_____ implementará medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales.

Estas medidas incluyen:

- Control de accesos físicos y lógicos.
- Cifrado de datos en tránsito y en reposo.
- Mecanismos de autenticación segura.
- Copias de seguridad periódicas.
- Gestión de incidentes de seguridad.
- Evaluaciones de riesgo y auditorías periódicas.
- Capacitación continua al personal sobre buenas prácticas de seguridad.

VIII. DERECHOS DEL CLIENTE

EL CLIENTE tiene derecho a:

- Acceder a sus datos personales.
- Rectificar o actualizar sus datos.
- Cancelar sus datos.
- Oponerse al tratamiento.
- Solicitar la portabilidad de sus datos.

IX. CONSERVACIÓN DE DATOS

_____ conservará los datos personales durante el periodo necesario para cumplir con las finalidades establecidas y de conformidad a su política de protección de datos.

X. REQUISITOS LEGALES

_____ cumplirá con la Ley Orgánica de Protección de Datos Personales y su Reglamento.

XI. REVOCACIÓN DEL CONSENTIMIENTO

EL CLIENTE puede revocar su consentimiento en cualquier momento.

XII. ACEPTACIÓN

EL CLIENTE declara haber leído y comprendido los términos de este acuerdo

|

Página 2 de 3

EL CLIENTE _____

NOMBRE: _____

REPRESENTANTE LEGAL: _____

CÉDULA: _____

RUC: _____


Fecha, _____

ANEXO 2: Encuesta de satisfacción aplicada a miembros de la prueba

Encuesta de satisfacción usuario final

En la presente encuesta deberá responder su experiencia de uso del sistema de obtención de consentimiento de tratamiento de datos personales.


Cuando envíe este formulario, no recopilaremos automáticamente sus detalles, como el nombre y la dirección de correo electrónico, a menos que lo proporcione usted mismo.

1. ¿Cómo califica la facilidad para otorgar su consentimiento a través de nuestro sistema? 


- Muy fácil
- Fácil
- Regular
- Difícil
- Muy difícil

2. ¿Qué tan clara y comprensible fue la información sobre el tratamiento de sus datos personales? 

- Muy clara
- Clara
- Parcialmente clara
- Poco clara
- Nada Clara

3. ¿Qué tan seguro se sintió al proporcionar su consentimiento a través de este sistema? 

- Muy seguro
- Seguro
- Moderadamente seguro
- Poco seguro
- Muy inseguro

4. ¿Cuál es su nivel de satisfacción general con el sistema de consentimiento para el tratamiento de datos personales? 

- Muy satisfecho
- Satisfecho
- Parcialmente satisfecho
- Poco satisfecho
- Muy insatisfecho



Este contenido lo creó el propietario del formulario. Los datos que envíe se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca de su contraseña.

Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial [Crear mi propio formulario](#)

El propietario de este formulario no ha proporcionado una declaración de privacidad sobre cómo utilizarán los datos de tus respuestas. No proporcionar información personal o confidencial. | [Términos de uso](#)

ANEXO 3: Diagrama de Base de Datos



ANEXO 4: Documento exportado de reportes de consentimientos.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	Identificaci	Nombres	Apellidos	Correo	Estado	Fecha UTC	Dirección IP Navegador													
2	1003602991	GABRIELA E	CORONEL V	gabyc1704	Aceptado	21/9/25 15:13	2803:c420::Mozilla/5.0 (iPhone; CPU iPhone OS 17_6_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/17.6 Mobile/15E148 Safari/604.1													

ANEXO 5: Documento de acuerdo enviado a cliente fin del proceso

SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. 2025

ACUERDO DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES PARA CLIENTES DE AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A

I. COMPARECEN

AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A., en adelante AIRMAXTELECOM, y

EL CLIENTE: Aguirre Benavides Carlos David

II. OBJETO

El presente acuerdo establece los términos y condiciones para el uso de datos personales del CLIENTE por parte de AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A.

III. FINALIDAD

En el presente acuerdo se utilizarán términos como: datos personales, tratamiento, encargado, transferencia, cesión y demás cuya definición estará a lo establecido en el artículo 4 de la Ley Orgánica de Protección de Datos Personales.

IV. CONSENTIMIENTO Y FINALIDAD

EL CLIENTE autoriza expresamente a AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. el tratamiento y transferencia de sus datos personales para las siguientes finalidades:

- Gestionar la prestación de los servicios de internet contratados, incluyendo la facturación y soporte técnico.
- Mejorar la experiencia del cliente mediante estudios de calidad y encuestas de satisfacción.
- Cumplir con obligaciones legales y regulatorias derivadas de la prestación del servicio.
- Implementar medidas de seguridad para garantizar la protección de la información personal del cliente.
- Responder y proveer respuesta a quejas y reclamos de servicios.
- Enviar información de nuevos servicios, documentos electrónicos, tarifas, recordatorios de pago, promociones, eventos e información de interés para clientes.
- Consultar y registrar la calificación crediticia de los clientes que solicitan créditos.
- Tratar los datos generados por la navegación y uso de la página web de Airmaxtelecom Soluciones Tecnológicas S.A.
- Mantener una comunicación permanente y abierta con el cliente, utilizando canales y plataformas WhatsApp, Instagram, Telegram, Facebook Messenger, llamadas telefónicas, mensajes de texto, entre otros.

V. DATOS PERSONALES TRATADOS

AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS tratará los siguientes datos personales del CLIENTE:

- Nombre y apellidos.
- Dirección de domicilio o lugar en el cual se recibirá el servicio.
- Teléfonos personales.
- Correo electrónico.
- Número de RUC
- Número de cédula
- Referencias comerciales

- Número de cuentas bancarias (En caso de débito automático)

VI. TRANSFERENCIA DE DATOS

AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS podrá transferir los datos personales del CLIENTE a:

- Proveedores de software o programas de almacenamiento de datos (nubes)
- Burós de crédito.
- Proveedores de software financiero y contable.
- Instituciones financieras nacionales.
- Jueces y autoridades gubernamentales.

VII. MEDIDAS DE SEGURIDAD

AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS implementará medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales.

Estas medidas incluyen:

- Control de accesos físicos y lógicos.
- Cifrado de datos en tránsito y en reposo.
- Mecanismos de autenticación segura.
- Copias de seguridad periódicas.
- Gestión de incidentes de seguridad.
- Evaluaciones de riesgo y auditorías periódicas.
- Capacitación continua al personal sobre buenas prácticas de seguridad.

VIII. DERECHOS DEL CLIENTE

EL CLIENTE tiene derecho a:

- Acceder a sus datos personales.
- Rectificar o actualizar sus datos.
- Cancelar sus datos.
- Oponerse al tratamiento.
- Solicitar la portabilidad de sus datos.

IX. CONSERVACIÓN DE DATOS

AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. conservará los datos personales durante el tiempo necesario para cumplir con las finalidades establecidas y de conformidad a su política de protección de datos.

X. REQUISITOS LEGALES

AIRMAXTELECOM SOLUCIONES TECNOLÓGICAS S.A. cumplirá con la Ley Orgánica de Protección de Datos Personales y su Reglamento.

XI. REVOCACIÓN DEL CONSENTIMIENTO

EL CLIENTE puede revocar su consentimiento en cualquier momento.

XII. ACEPTACIÓN

EL CLIENTE declara haber leído y comprendido los términos de este acuerdo

Aceptado por OTP - 21/09/2025 15:45:34

EL CLIENTE

NOMBRE: Aguirre Benavides Carlos David

REPRESENTANTE LEGAL:

CÉDULA: 1003770482

RUC: