UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

TRABAJO DE INTEGRACIÓN CURRICULAR

TEMA:

"DESARROLLO DE UNA GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LA EMPRESA BOREALPLAST"

Trabajo de titulación previo a la obtención del título en Ingeniera en Tecnologías de la Información

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

AUTOR:

Martha Cecilia Tiviano Gancino

DIRECTOR:

MSc. Xavier Mauricio Rea Peñafiel

Ibarra – Ecuador 2026

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. 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:	1805144241		
APELLIDOS Y NOMBRES:	Tiviano Gancino Martha Cecilia		
DIRECCIÓN:	La Ecuatoriana, barrio San Marcelo, pasaje 0E9H y pasaje 35 - Quito		
EMAIL:	mctivianog@utn.edu.ec		
TELÉFONO FIJO:	02-3041389	**TELÉFONO MÓVIL:**	0967888595

DATOS DE LA OBRA	
TÍTULO:	DESARROLLO DE UNA GUÍA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LA EMPRESA BOREALPLAST
AUTOR (ES):	Tiviano Gancino Martha Cecilia
FECHA: DD/MM/AAAA	02/03/2026
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	**Ingeniera en Tecnologías de la Información**
ASESOR /DIRECTOR:	MSc. Marco Remigio Pusdá Chulde, PhD./ MSc. Xavier Mauricio Rea Peñafiel

2. CONSTANCIAS

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

Ibarra, a los 04 días del mes de marzo de 2026

EL AUTOR:

Firmado electrónicamente por:
MARTHA CECILIA TIVIANO GANCINO
Validar únicamente con FirmaEC

(Firma)……
Nombre: Tiviano Gancino Martha Cecilia

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 04 de marzo de 2026.

MSc. Xavier Mauricio Rea Peñafiel
DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR
CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

MSc. Xavier Mauricio Rea Peñafiel

C.C: 1002485744

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificado del trabajo de Integración Curricular “ Desarrollo de una guía metodológica para la implementación de la Ley Orgánica de protección de datos personales en la empresa Borealplast ” elaborado por Martha Cecilia Tiviano Gancino , previo a la obtención del título del Ingeniera en Tecnologías de la Información , aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

Firmado electrónicamente por:
XAVIER MAURICIO REA PEÑAFIEL
Validar únicamente con FirmaEC

MSc. Xavier Mauricio Rea Peñafiel

C.C: 1002485744

Firmado electrónicamente por:
MARCO REMIGIO PUSDA CHULDE
Validar únicamente con FirmaEC

MSc. Marco Remigio Pusdá Chulde, PhD.

C.C: 0401200951

DEDICATORIA

Este sueño no habría sido posible sin el amor, la paciencia y el apoyo de quienes caminaron conmigo.

En primer lugar, dedico este trabajo a mi hijo Dylan, por su fuerza emocional y admirable madurez. Gracias por comprender mis ausencias, por animarme cuando me sentía rendida, me di cuenta que, a pesar de todo he criado un excelente hombre. Tu apoyo fue un pilar fundamental que me guio en los momentos más complejos de este recorrido. Como olvidar a mi pequeño Liam, quien con tanto amor entendió mi ausencia mientras cumplía con mis deberes académicos, a él y a Dylan dedico este trabajo, pues son el pilar fundamental que impulsa mi vida.

A mi esposo, arquitecto silencioso de este logro, mi compañero de vida, quien aprendió conmigo a pesar de que el mérito me lo llevaría yo, por convertir cada rincón de nuestra casa en un estudio, biblioteca y refugio según la demanda de mis estudios. Gracias por convertir cada "no voy a poder" en un "tú sí puedes, no te rindas, ya no falta mucho, yo estoy aquí para ti, ahora me tienes a mi" gracias por sostenerme con esas palabras firmes y llenas de amor, gracias por recordarme, siempre, que soy capaz de todo lo que me propongo, aunque el cansancio pesara. Tu compañía, esfuerzo y amor se convirtió en el impulso que necesitaba para no rendirme.

A mi amiga Victoria, por apoyarme en los días más difíciles. Gracias por tu compañía sincera, por cada consejo y cada esfuerzo compartido. Gracias por enseñarme lo bonito de una amistad limpia y pura. Tu amistad fue fundamental en ese recorrido.

También dedico este trabajo a mi hermanita Dayana, que por circunstancias de la vida no pudo estar acompañándome personalmente; sin embargo, se que ella siempre fue el ángel que necesite para no darme por vencida, desde el cielo con una sonrisa dulce también celebra el cumplimiento de mi sueño.

Asimismo, quiero agradecer a todas aquellas personas que, con una palabra o ayuda desinteresada, aportaron un granito de arena para hoy cumplir mi sueño. Gracias por su ayuda, Lesly, por sus palabras, Mishel, y por su infinita y desinteresada ayuda Gaby, porque muchas veces renuncio a sus descansos para acompañarme en esas madrugadas a cumplir con mis obligaciones, todos ustedes han dejado una maravillosa huella en mi corazón.

Este logro no es solo mío, es de todos quienes me acompañaron con paciencia y amor.

Martha Cecilia Tiviano Gancino

AGRADECIMIENTO

Quiero agradecer, en primer lugar, a Dios por haberme brindado la sabiduría y la fortaleza necesarias para estudiar una carrera que muchas veces consideré un reto para mí, pero gracias a él hoy ha sido posible este éxito.

A la Universidad Técnica del Norte, y en especial a la Facultad de Ingeniería en Ciencias Aplicadas, quiero expresar mi más profundo agradecimiento por abrirme las puertas para crecer académica y profesionalmente y por brindarme los medios necesarios para realizar esta investigación, a todos los docentes que me compartieron sus conocimientos con sabiduría y paciencia. Aun recuerdo cuando cree mi primer "Hola mundo" y cuantas horas me tomo crearlo, creo que agote la paciencia de mi profesor, y después me sorprendí del potencial que tuve al crear mi primera plataforma en Moodle, como cree mi primera app y primera página web, todo esto fue posible gracias a mis docentes.

A mi director de tesis, MSc. Xavier Mauricio Rea Peñafiel, por su paciencia, dedicación y orientación durante este proyecto. Gracias por cada una de sus observaciones que permitieron fortalecer este trabajo; su conocimiento, apoyo y ayuda fueron fundamentales para alcanzar este logro.

A mi asesor de tesis, MSc. Marco Pusdá, agradezco su orientación, recomendaciones oportunas, su apoyo y ayuda durante el proceso de esta investigación.

A mis compañeros de estudio, que lamentablemente no llegaron conmigo a la meta final, gracias por enseñarme que el aprendizaje también se construye en equipo.

Finalmente, a mi esposo Milton Caiza, mi pilar más firme, gracias por levantarte cada día a pesar del cansancio acumulado, para proveer de todo lo necesario a nuestro hogar y ayudarme con todo lo que necesité económicamente en esta etapa de formación, por creer en mi incluso cuando parecía que no iba a lograrlo, gracias por sostenerme con paciencia, amor y por tus palabras de aliento. Este logro, en la medida más grande, es también tuyo. A mi esposo y a mis hijos gracias por soportar ese "no me digan nada, ahorita estoy programando", pero en realidad estaba luchando con mi incapacidad, gracias porque a pesar de mis crisis existenciales no me abandonaron, gracias por aceptar mi ausencia, cuando sé, que muchas veces en verdad me necesitaron.

A todos, mi eterna gratitud por ser parte de este logro que hoy culmino con mucho orgullo y gratitud.

Martha Cecilia Tiviano Gancino

ÍNDICE DE CONTENIDOS

CAPÍTULO III

CAPÍTULO IV

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El manejo inadecuado de los datos personales en organizaciones medianas y pequeñas (PYMES) ha incrementado el incumplimiento de normas y sanciones relacionadas con la Ley Orgánica de Protección de Datos Personales (LOPDP), válida desde mayo de 2021. Borealplast, una empresa mediana con una trayectoria significativa en Quito, no cuenta con políticas que garanticen la seguridad y privacidad de los datos que gestionan, lo que la expone a grandes riesgos legales. El presente proyecto desarrolló una guía metodológica orientada a la implementación de la LOPDP. Si bien existen varias guías sobre el manejo de la LOPDP, ninguna contempla la realidad operativa y los recursos financieros limitados respecto a la implementación de esta normativa en las pymes de Ecuador. Por lo tanto, se planteó como objetivo principal el desarrollo de una guía metodológica para la implementación de la LOPDP en la empresa Borealplast, considerando estándares internacionales como la ISO 27001/27701. Metodológicamente, la investigación adoptó un enfoque mixto (Cualitativo-Cuantitativo), complementado con el método Delphi para la validación de la guía mediante una consulta estructurada a expertos en protección y seguridad de datos. Como resultado, se elaboró una guía estructurada y aplicable que incluye: diagnóstico inicial de la empresa respecto a la LOPDP, procedimiento para derechos ARCO (acceso, rectificación, cancelación y oposición), definición de roles como el delegado de protección de datos (DPD) y el responsable de tratamiento de datos (RTDP), recomendaciones legales y un cronograma de capacitación sobre la LOPDP. La validación evidenció un consenso entre los expertos respecto a la utilidad, pertinencia y aplicabilidad de la guía para facilitar el cumplimiento normativo. Se concluye que la propuesta constituye una herramienta práctica y escalable que fortalecerá la protección, seguridad y privacidad de los datos personales en Borealplast y a la vez puede servir de referencia para otras pymes ecuatorianas que busquen alinearse con la LOPDP.

Palabras clave: DPD, Guía metodológica, ISO 27001, ISO 27701, Ley Orgánica de Protección de Datos Personales, Normativa, PYMES, RTDP.

ABSTRACT

The inadequate management of personal data in small and medium-sized enterprises (SMEs) has increased non-compliance with regulations and penalties related to the Organic Law on Personal Data Protection (LOPDP), in force since May 2021. Borealplast, a medium-sized company with a significant trajectory in Quito, lacks policies that ensure the security and privacy of the data it processes, exposing the organisation to substantial legal risks. This project developed a methodological guide aimed at supporting the implementation of the LOPDP. Although various guides exist regarding the application of the LOPDP, none address the operational realities and limited financial resources faced by Ecuadorian SMEs when adopting this regulation. Therefore, the main objective was to design a methodological guide for the implementation of the LOPDP within Borealplast, considering international standards such as ISO 27001 and ISO 27701.

Methodologically, the research adopted a mixed approach (qualitative–quantitative), complemented by the Delphi method to validate the guide through a structured consultation with experts in data protection and security. As a result, a structured and applicable guide was developed, including: an initial diagnosis of the company's compliance with the LOPDP, procedures for ARCO rights (access, rectification, erasure and objection), the definition of roles such as the Data Protection Officer (DPO) and the Personal Data Processing Manager (RTDP), legal recommendations, and a training schedule on the LOPDP. The validation process showed consensus among experts regarding the usefulness, relevance, and applicability of the guide in facilitating regulatory compliance. It is concluded that the proposal constitutes a practical and scalable tool that will strengthen the protection, security, and privacy of personal data within Borealplast, while also serving as a reference for other Ecuadorian SMEs seeking to align with the LOPDP.

Keywords: DPO, methodological guide, ISO 27001, ISO 27701, Organic Law on Personal Data Protection, regulation, SMEs, RTDP.

CAPÍTULO I
INTRODUCCIÓN

1.1 Planteamiento del Problema

En Ecuador, desde el 2008 la protección de datos personales es un derecho constitucional; sin embargo, su regulación específica solo se concretó con la Ley Orgánica de Protección de Datos Personales (LOPDP) en mayo del 2021[1]. Investigaciones anteriores identificaron que varias empresas, como Borealplast, fabricante de empaques para alimentos, aún incumplen esta normativa, lo que las expone a sanciones que pueden ir desde el 0.1 % hasta el 0.7 % del ingreso bruto de la empresa, e incluso puede conllevar al cierre de la organización.[2]

Borealplast maneja datos sensibles de clientes, socios y empleados a través de su software contable, pero no implementa protocolos adecuados de protección. Esta situación la hace vulnerable a sanciones por incumplimiento de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

Como solución, se propone desarrollar una guía metodológica para implementar la LOPDP. Esta guía no solo ayudará a Borealplast a alinearse con estándares internacionales como ISO 27701, que se refiere a gestionar específicamente la privacidad de datos personales, sino que servirá como modelo para otras PYMES manufactureras, mejorando su competitividad y garantizando la sostenibilidad legal del negocio.[3]

En la figura **??** se presenta un análisis estructurado de la problemática de protección de datos en Borealplast, organizado en tres ejes clave. En primer lugar, se identifican los problemas actuales: vulnerabilidades en el software contable, ausencia de políticas de protección de datos e incumplimiento de la LOPDP. Estos generan graves consecuencias, como sanciones legales y económicas, además de pérdida de confianza por parte de clientes y proveedores. Finalmente, se proponen soluciones concretas como: capacitación del personal, creación del rol de Delegado de Protección de Datos (DPO) y desarrollo de una guía metodológica alineada con los estándares ISO 27001 e 27701. Este esquema visual sintetiza de manera clara la relación entre los riesgos, sus impactos y las acciones correctivas necesarias para garantizar el cumplimiento normativo y la seguridad de la información en la empresa.

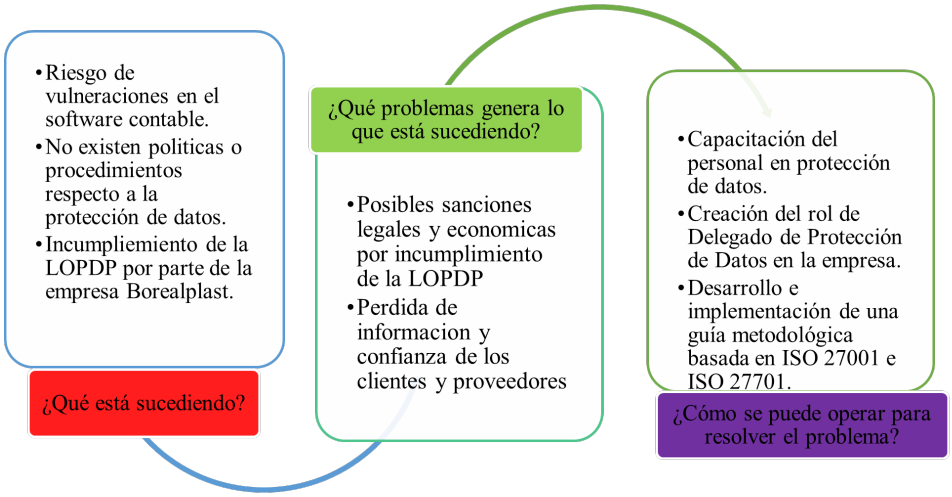


Fig. 1.
Diagrama de Proceso. Fuente: Elaboración propia

1.2 Objetivos

1.2.1 Objetivo General

Desarrollar una Guía metodológica para la implementación de la Ley Orgánica de protección de datos personales en la empresa Borealplast, considerando los estándares ISO 27001 e ISO 27701

1.2.2 Objetivos Específicos

- Diagnosticar el estado actual de la protección de datos en la empresa BOREALPLAST respecto al cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) y las normas ISO 27001 e ISO 27701.

- Establecer los criterios técnicos y legales basados en los estándares ISO 27001, ISO 27701 y la LOPDP, para identificar y priorizar los riesgos de seguridad y privacidad en el software contable de Borealplast, con el fin de desarrollar una guía de implementación adaptada a su contexto operativo.

- Evaluar la propuesta del modelo de cumplimiento mediante expertos para garantizar la efectividad de las medidas descritas en él.

1.3 Alcance y delimitación

Esta investigación se enfocó en la elaboración de la guía metodológica específicamente para implementar la LOPDP en Borealplast, sin incluir su implementación total dentro de la empresa; sin embargo, se proporcionaron las directrices necesarias para su ejecución futura.

Para lograr nuestro objetivo inicialmente realizamos un análisis de la Ley Orgánica de Protección de Datos Personales, para comprender las obligaciones legales que la empresa Borealplast debe cumplir, luego realizaremos un estudio de las normas ISO 27001 e ISO 27701 para identificar los beneficios y los objetivos de control que estas establecen en relación con la protección de datos personales.

Tras la conclusión de los análisis, se procedió a la elaboración de la guía metodológica que contendrá recomendaciones específicas que debería seguir Borealplast para asegurar el cumplimiento de los requisitos legales establecidos en la ley.

La estructura de la guía metodológica estará compuesta por:

- Planificación.
- Recolección de información.
- Marco Teórico
- Análisis de los problemas hallados.
- Desarrollo de la propuesta.
- Validación de la guía metodológica.

1.4 Justificación

La selección de este tema se fundamenta en la creciente relevancia de la protección de datos personales en el entorno empresarial ecuatoriano. El desarrollo de esta guía ayudará a la implementación efectiva de la LOPDP y servirá como referencia para futuras investigaciones, ya que

Borealplast maneja datos sensibles en sus operaciones diarias y por eso necesita preservar la confianza de sus clientes y proveedores.

La implementación de la Ley Orgánica de Protección de Datos Personales dentro de la empresa Borealplast exige herramientas prácticas y adaptadas a su realidad y es fundamental para garantizar la seguridad de la información de todo el personal, como ya se mencionó anteriormente. Actualmente la empresa no cuenta con un sistema de protección de datos, motivo por el cual se encuentra expuesta a riesgos legales y operativos.

El desarrollo de la presente guía metodológica estableció un marco de referencia preciso para implementar las medidas organizativas y técnicas indispensables que se alineen con la LOPDP y las normas ISO 27001/ 27701. Estos estándares ofrecen la armadura fundamental que garantiza la seguridad de la información y la privacidad de los datos personales, asegurando la prevención de riesgos y aumentando la confianza de clientes, proveedores y demás stakeholders de la empresa. Además, la adopción de estas buenas prácticas brindara a la empresa Borealplast, confianza y competitividad en el mercado, puesto que hoy en día, la seguridad de datos se ha vuelto un requisito esencial para la sostenibilidad y el crecimiento empresarial. Así como también es crucial para garantizar los derechos de los titulares de datos, respecto a las solicitudes ARCO.

Desde el punto de vista formativo, este proyecto fomentará el desarrollo de habilidades orientadas al diseño de guías metodológicas y en la aplicación de normativas de seguridad informática. Finalmente, su mayor impacto se reflejará en la transformación de la cultura organizacional, instaurando prácticas sostenibles para la protección de datos, que beneficiarán tanto a la empresa como a los titulares de la información.

CAPÍTULO II
MARCO TEÓRICO

2.1 Empresa

BOREALPLAST Cía. Ltda., se constituyó en la República del Ecuador el veintiséis de junio de dos mil nueve, fecha en la cual fue oficialmente fundada y debidamente legalizada en el Distrito Metropolitano de Quito bajo la supervisión de la Superintendencia de Compañías. Esta entidad establece su origen mediante una estructura centralizada que consta de tres socios de nacionalidad ecuatoriana y un socio de nacionalidad colombiana. Fue creada con el fin de fabricar y comercializar todo tipo de artículos de plástico.

En la actualidad, es una Empresa líder en la fabricación y comercialización de todo clase de fundas, rollos y láminas de plástico en todo tipo de medidas, elaboradas con polietileno de alta y baja densidad, y con polipropileno cast-bio.

Desde sus inicios hasta la actualidad, se mantiene en constante mejora de sus procesos basados en la calidad, cumpliendo sus objetivos de producción y puntualidad con sus clientes, lo que la ubica con gran ventaja frente a la competencia.

2.1.1 Misión

Boreaplast tiene como misión diseñar, producir y suministrar empaques de plástico de alta calidad que satisfagan las necesidades de nuestros clientes, garantizando durabilidad, funcionalidad y personalización. Nos comprometemos a incorporar prácticas sostenibles en nuestros procesos, fomentando el reciclaje, el uso responsable de recursos y la innovación para contribuir al cuidado del medio ambiente.

2.1.2 Visión

Visión de Borealplast al 2030: Ser líderes en la fabricación de soluciones de empaques plásticos sostenibles, ofreciendo productos innovadores y de alta calidad que satisfagan las necesidades de nuestros clientes, mientras reducimos nuestro impacto ambiental y promovemos prácticas responsables en toda nuestra cadena de valor.

2.1.3 Organigrama

En la figura 2 se muestra cómo es la estructura organizacional de la empresa Borealplast, en el nivel superior se ecnuentra la junta de socios, presidente ejecutivo, gerente general, en el nivel intermedio se localizan los departamentos por los cuales están integrados la empresa, terminando en la parte inferior con el nivel operativo.

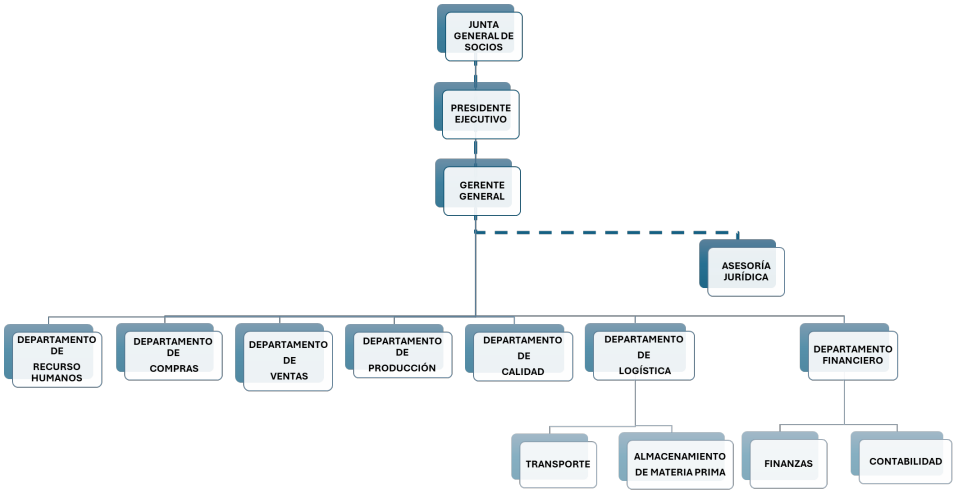


Fig. 2.
Organigrama estructural de la Empresa Borealplast. **Fuente:** Borealplast

2.1.4 Ubicación

Desde sus inicios hasta la actualidad, la empresa está ubicada al norte de la ciudad de Quito, en la Sebastián Moreno E1-25 y Av. Galo Plaza Lasso esquina.

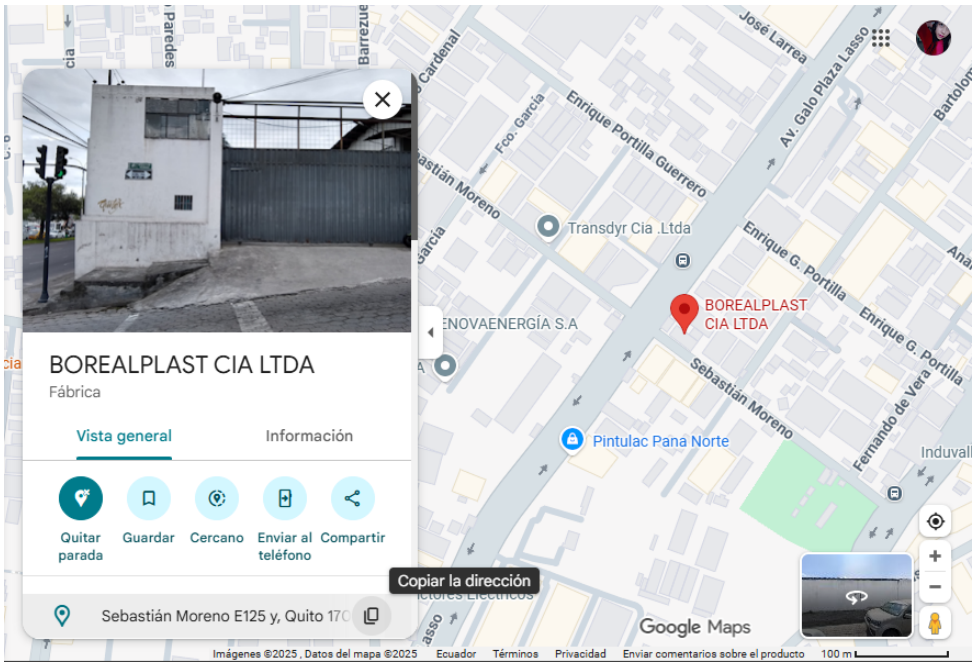


Fig. 3.
Ubicación de BOREALPLAST CÍA. LTDA. en Sebastián Moreno, Quito.

Fuente:(https://maps.app.goo.gl/5Xii6DGhGhasY5cL6)

2.2 Bases Teóricas

2.2.1 Ley Orgánica de Protección de Datos Personales(LOPDP)

Para una mejor comprensión de este capítulo, es importante conocer la trayectoria que ha tenido la ley orgánica de protección de datos personales (LOPDP), en Ecuador en el año 2008, se implementó el derecho a la protección de los datos personales, este derecho está representado en el artículo 66 numeral 19, el cual establece "el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección" [4]. "La recolección, archivación, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley"[5].

A partir de este artículo, se estableció las bases para la edificación de la ley que hoy en día está vigente, en el año 2016, se presentó un anteproyecto donde el objetivo era, proteger los derechos a la intimidad y privacidad de los datos personales, sin embargo este anteproyecto fue rechazado porque presento un contenido difuso, de igual manera en el año 2012 se presentó un anteproyecto similar, titulado "Ley sobre la Protección a la Intimidad y los Datos Personales", que igual fue rechazado, no fue hasta el año 2017 que la Dinardap (Dirección Nacional de Registro de Datos

Públicos) realizó su anteproyecto, conocido como “Ley de Protección de Datos Personales” [6], el cual fue tomado en cuenta y analizado con profundidad.

Para el análisis y aprobación de esta regulación se tuvo la participación de sectores públicos y privados, entre ellos las participaciones del sector de las telecomunicaciones, tales como Agencia de Regulación y Control de las Telecomunicaciones (Arcotel), la Agencia de Regulación y Control Postal (ARCPostal), Correos del Ecuador EP, la Corporación Nacional de Telecomunicaciones (CNT), el Registro Civil y el Ministerio de Telecomunicaciones y de la Sociedad de la Información, Mintel [5].

Se contó con el apoyo de expertos nacionales e internacionales, como el Comité de Propiedad Intelectual de la Cámara de Comercio Ecuatoriano Americana (Amcham), Asociación Ecuatoriana de Ciberseguridad (AECI), GMS Seguridad, Usuarios Digitales, Asociación para el Progreso de las Comunicaciones (APC), Fundación Ciudadanía y Desarrollo, Consejo de Regulación y Desarrollo de la Información y Comunicación (Cordicom), Observatorio Legislativo, Asociación de la Banca Privada (Asobanca), ONG Access Now para América Latina, Organización de Estados Americanos (OEA), Comisión Europea, Asociación Ecuatoriana de Protección de Datos Personales (Aepdp), Red Iberoamericana de Protección de Datos, Instituto Nacional de Acceso a la Información Pública (INAI) de México, Consejo de Transparencia de Chile, Organización de Derechos Digitales para América Latina, Citec y la Agencia Latinoamericana de Información (ALAI), para que analizaran el contenido legal y dieran su punto de vista [5].

En septiembre de 2019 se presenta el anteproyecto a la Asamblea Nacional, la cual el 10 mayo del 2021 es aprobada con ciento dieciocho (118) votos a favor [5], de igual manera el 26 del mismo mes y año es publicada la LOPDP en su registro oficial y desde esa fecha las empresas tendrían dos años para implementar esta nueva ley, esta ley fue aprobada ya que su objetivo es garantizar el derecho fundamental a la protección de datos de los ciudadanos ecuatorianos y el contenido de su anteproyecto fue claro y conciso.

2.2.2 Estructura de la LOPDP

En la tabla 1 se detalla la estructura de la LOPDP según el análisis de Yunganaula, la Ley Orgánica de Protección de Datos Personales posee una estructura jurídica detallada, conformada por 12 capítulos y 77 artículos que establecen los parámetros para el manejo adecuado de datos personales [7]. Como podemos apreciar en la tabla 1, cada capítulo contiene los artículos que garantizan el correcto uso y manipulación de los datos dentro de su marco normativo.

Tabla 1.
ESTRUCTURA DE LA LOPDP. **ADAPTADO DE:** [7, P. 25]

Cap.	**Nombre**	**Art. Artículos**
1	Ámbito de Aplicación Integral	9
2	Principios	1
3	Derechos	14
4	Categorías Especiales de Datos	8
5	Transferencia o Comunicación y Acceso a Datos Personales por Terceros	4
6	Seguridad de Datos Personales	10
7	Responsable, encargado y delegado de protección de datos personales	5
8	De las Responsabilidades Proactivas	3
9	Transferencia o Comunicación Internacional de Datos personales	7
10	De los Requerimientos Directos y de la Gestión del Procedimiento Administrativo	3
11	Medidas Correctivas, Infracciones y Régimen Sancionatorio	10
12	Autoridad de Protección de Datos Personales	3

2.2.3 Alcance de la LOPDP

La LOPDP protege los datos personales como son: nombre, teléfono. correo, cédula, dirección, datos bancarios, etc., que se refieran a una persona natural identificada o identificable. Según el artículo 2 referente al ámbito de aplicación material [1], esta ley no aplica en estos casos:

- Cuando se utilizan datos de familiares o amigos para fines personales (como una agenda de contactos).
- Información de personas fallecidas (a menos que otra ley lo permita).
- Los datos anónimos que no identifiquen a nadie (pero estos dejan de ser anónimos cuando se aplica la ley).
- Para los periodistas que realicen publicaciones editoriales.
- Datos usados en emergencias o seguridad nacional (pero deben respetar derechos humanos).

- Información para investigaciones policiales o judiciales (con las mismas condiciones).
- Datos de empresas (no de personas naturales).
- Datos que identifican a personas jurídicas.

Sin embargo, de acuerdo con el Artículo 3 que se refiere al ámbito de aplicación territorial[1], sí regula el acceso a datos profesionales públicos e información patrimonial de funcionarios. Su alcance territorial incluye[8]:

- Todo procesamiento de datos dentro de Ecuador.
- El responsable del tratamiento de datos personales, cuyo domicilio se encuentre registrado en territorio nacional.
- El aplique tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable no establecido en el territorio ecuatoriano, cuando las actividades estén relacionadas con: 1) La oferta de bienes o servicios a dichos titulares, independientemente de si a LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) - Página 5 FINDER LOYAL - www.lexis.com.ec a estos se les requiere su pago, o, 2) del control de su comportamiento, en la medida en que este tenga lugar en el territorio ecuatoriano.
- Al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, le resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público.

La norma impone exigencias en materia de legalidad y proporcionalidad, en especial en ámbitos sensibles como la seguridad nacional.

2.2.4 Principios de la LOPDP

Con el avance tecnológico que se ha tenido, el tema de la protección de datos es crucial, ya que la privacidad de las personas enfrentan desafíos constantes debido a este avance tecnológico. De acuerdo con el capítulo 2, artículo 10, de la Ley Orgánica de Protección de Datos Personales (LOPDP), se establece una serie de principios que deben ser cumplidos por todo tipo de persona, natural o jurídica. Entre ellos, los principios que se destacan en base al artículo 10 de la LOPDP son[8]:

- **Principio de Juridicidad:** Todo procedimiento de recolección y tratamiento de datos personales debe fundamentarse siguiendo las leyes y regulaciones aplicables. Es decir, el objetivo de este principio es asegurar que el procesamiento de datos se realice mediante un consentimiento libre, informado y expreso del titular, o por el cumplimiento de obligaciones contractuales, todo esto con una justificación legítima.

- **Principio de Lealtad:** La obtención de datos debe realizarse bajo criterios de transparencia y veracidad, no se puede recoger o utilizar de manera engañosa. Asimismo, es obligación del responsable garantizar que los titulares reciban información clara y accesible acerca de las finalidades, métodos y alcances del tratamiento al que serán sometidos sus datos.

- **Principio de Transparencia:** Toda información sobre el uso de datos personales debe ser clara, fácil de entender y accesible para los titulares, es decir tienen derecho a ser informados sobre los objetivos específicos de la recolección, las modalidades de procesamiento aplicables y cualquier eventual transferencia o cesión de sus datos a terceros, ya sea en el ámbito nacional o internacional.

- **Principio de Finalidad:** Los datos solo se pueden usar para el propósito que se fue informado a los titulares al recogerlos. Si estos se usan para otra cosa, deben ser acciones que estén permitidos por la ley.

- **Principio de Proporcionalidad:** El tratamiento de datos debe ser adecuado y limitado estrictamente a los fines para lo que fueron recaudados. Esto implica la implementación de medidas técnicas y organizativas que minimicen el volumen de datos procesados, garantizando así el respeto a la privacidad de los titulares.

- **Principio de Confidencialidad:** Los datos deben ser procesados con seguridad y no deben ser divulgados sin la autorización del titular, a excepción de los casos previstos por la ley.

- **Principio de Calidad y Exactitud:** Los datos deben ser exactos, completos y actualizados. Si hay errores, deben corregirse rápidamente, de manera que no altere su veracidad

2.2.5 Derechos de la LOPDP que respaldan al titular

La Ley Orgánica de protección de datos personales en Ecuador otorga a los titulares de datos un conjunto de derechos que les brindan control y transparencia sobre cómo se manejan sus datos personales durante procesos de recolección y procesamiento de datos personales. Entre ellos los derechos que se destacan son[9]:

- **Derecho a la Información**: Los titulares deben estar informados sobre quién maneja sus datos, qué tipos de datos son guardados y cuál será la finalidad de la recolección de ellos.
- **Derecho de acceso:** Las personas tienen el derecho de acceder a sus datos y conocer cómo están siendo tratados y si se está cumpliendo con la finalidad específica para la que fueron recolectados.
- **Derecho de rectificación y actualización:** Los titulares de los datos personales poseen el derecho de solicitar la corrección y actualización de los datos personales cuando estos sean inexactos o parciales, garantizando de este modo la exactitud e integridad de la información sujeta a tratamiento.
- **Derecho de eliminación:** las personas tienen el derecho a solicitar la eliminación de sus datos personales cuando ya no los estén usando con la finalidad con la que fueron receptados, o en caso de ser separados de la institución o empresa a la que pertenecían.
- **Derecho a la limitación del tratamiento:** En determinadas circunstancias las personas tienen el derecho de solicitar un límite de usos en sus datos personales, como por ejemplo cuanto el tratamiento de estos datos ha sido de manera ilícita.
- **Derecho de oposición:** las personas tienen el derecho de oponerse al uso de sus datos en ciertas circunstancias, por ejemplo, cuando los datos han sido utilizados con fines publicitarios o cuando se utilizada para una decisión automatizada.
- **Derecho a la portabilidad:** las personas tienen el derecho de obtener sus datos personales en un formato estructurado que pueda ser utilizado en otro servicio.

De acuerdo con la Asamblea Nacional de la RepÚblica del Ecuador[1], existen algunas excepciones para ejercer los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad, estos casos están redactados en el artículo 18 del capítulo 3, entre las excepciones tenemos:

- Si el que solicita alguna solicitud ARCO no es el dueño de los datos o no acredita ser su representante legal.
- Si los datos están sujetos a obligaciones legales o contractuales, es decir, son obligatorios por ley o por un contrato.
- Si una autoridad competente (juez o institución pública) lo exige.
- Cuando se necesita un ejercicio o defensa de derechos procesales o recursos legales.
- Cuando el ejercicio de los derechos de los titulares pueda afectar derechos o intereses legítimos de terceros, debidamente justificados por el responsable del tratamiento.
- Si obstaculiza con procesos judiciales, investigaciones o trámites administrativos que se encuentren en curso.
- Si son usados para libertad de expresión e información pública (p.ej., periodismo, opinión pública).
- Si protegen la vida del titular o de una tercera persona, particularmente en casos de emergencia.
- Si es de interés público (cumpliendo estándares de derechos humanos).
- Si son para archivos estatales, investigación científica o estadística.

2.2.6 Requisitos de la LOPDP

La LOPDP establece algunos requisitos que deben cumplir las empresas referente a la protección de datos personales, estos requisitos son primordiales ya que garantizan el correcto uso de la información, así como la privacidad y la seguridad. En la tabla 2 se identifican las obligaciones y responsabilidades que deben tener el encargado y responsable sobre el tratamiento de los datos personales, específicamente, este artículo está compuesto por 15 puntos [7], que deben ser un requisito primordial para los encargados del manejo de datos personales. A continuación, se presenta la tabla 2, en donde según Yunganaula se detallan los 15 puntos estratégicos y se los relaciona con otros artículos que hablan de manera más detallada de las medidas que se debe tener en cuenta, estos puntos se encuentran registrados en el registro oficial de la Asamblea Nacional

de la Republica del ecuador, específicamente en el Capítulo VII, Del Responsable, Encargo y Delegado de Protección de datos personales, artículo 47 [8, p.23].

Tabla 2.
REQUISITOS PARA EL TRATAMIENTO DE DATOS PERSONALES. **ADAPTADO DE:** [8], P. 23)

#	**Requisitos**	**Arts.**
1	Tratar los datos según la normativa vigente emitida por la Autoridad de Protección de Datos Personales.	8,10,12-17
2	Implementar herramientas de cumplimiento para garantizar el tratamiento conforme a la Ley.	37,39,41
3	Verificación periódica de medidas.	37,39,41
4	Implementar políticas de protección de datos personales acordes a cada caso.	12-17,19-21,26
5	Utilizar metodologías de análisis de riesgos.	40
6	Evaluaciones de seguridad previas al tratamiento.	42
7	Medidas preventivas contra riesgos identificados.	44,45
8	Notificación de incidentes a la Autoridad y al titular.	43,46
9	Protección de datos desde el diseño y por defecto.	39
10	Suscribir contratos de confidencialidad.	10,34,35
11	Garantizar mecanismos para la protección de datos según ley y reglamento.	34
12	Actualizar el Registro Nacional de Protección de Datos.	51
13	Designación del delegado.	48
14	Auditorías periódicas.	68,69
15	Cumplimiento normativo.	Varios

2.2.7 Sanciones de la LOPDP

Ante el incumplimiento de la LOPDP existen algunas sanciones y más aún cuando se han vulnerado los derechos y principios de las personas titulares de los datos personales, estas sanciones pueden conllevar a multas, la clausura temporal o definitiva de las actividades relacionas con el tratamiento de los datos personales. Las multas pueden variar dependiendo de la gravedad del caso y pueden oscilar entre 1 y 20 salarios básicos unificados del trabajador en general. En el artículo 67 del capítulo 11 de las Medidas Correctivas, Infracciones y Régimen Sancionatorio de la LOPDP se especifican las siguientes infracciones Leves[8]:

- Se considera una infracción leve si el encargado de protección de datos no responde a tiempo o sin justificación las solicitudes o reclamos de los titulares de los datos.

- No incluye sistemas de protección desde el principio en los sistemas.
- No establecer políticas claras de protección de datos acordes a lo que se está procesando.
- Elegir un encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales.
- Ignorar las correcciones que ha realizado la Autoridad de Protección de Datos Personales.

Infracciones Graves: En el artículo 68 de la LOPDPD se presenta las siguientes infracciones graves del Responsable de protección de datos[8].

- No aplicar técnicas de seguridad robustas legales, necesarias para la protección de datos personales, de acuerdo con lo que exige la ley.
- Utilizar los datos personales para fines ajenos a los establecidos en el principio de finalidad.
- Distribuir la información personal sin seguir los procedimientos legales establecidos.
- No realizar evaluaciones de impacto cuando la ley lo requiere, por ejemplo, cuando se ha manejado datos sensibles.
- Excluir medidas de seguridad para prevenir alguna violación de seguridad que se haya identificado.
- No informar a la Autoridad de Protección de Datos Personales como a los titulares afectados cuando ocurren violaciones de seguridad que afecten los derechos fundamentales de los titulares de los datos.
- La falta de celebración de contratos que establezcan cláusulas específicas sobre confidencialidad y tratamiento adecuado de datos personales con los encargados del procesamiento y el personal involucrado.
- No suscribir contratos que incluyan cláusulas de confidencialidad y tratamiento adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales[8].
- Es un incumplimiento grave no realizar la designación de un Delegado de Protección de Datos cuando sea requerido por la ley.

- Negarse a cooperar en auditorías o investigaciones realizadas por auditores acreditados por la autoridad correspondiente.
- El incumplimiento reiterado de medidas correctivas, después de que el responsable ya ha sido notificado y sancionado por infracciones leves.

De esta forma el Registro Oficial de la Asamblea Nacional de la República del Ecuador, establece las sanciones que deben ser impuestas por la Autoridad de Protección de Datos Personales, de acuerdo con el artículo 71 las sanciones leves serán sancionadas con las siguientes[1]:

- Los servidores o funcionarios públicos que por alguna razón hayan cometido alguna infracción leve establecidas en la ley deberán ser sancionados con una multa de uno a diez salarios básicos unificados del trabajador en general.
- En las empresas privadas, en caso de cometer una infracción leve, su multa será del 0.1 % al 0.7 % de sus ingresos del año pasado, la Autoridad Protectora de Datos debe realizar un análisis para identificar si el daño fue intencional, la infracción es reincidente y si hubo filtración de datos sensibles o afecciones graves, de acuerdo con el análisis que se obtenga se aplicara las sanciones de forma proporcional a la gravedad de la falta.
- Para los DPD de empresas públicas y privadas, al cometer infracciones leves, la multa va desde 1 a 10 salarios básicos unificados de su ingreso al mes anterior en que se impuso la multa.

En las infracciones graves, según el artículo 72 de la ley tenemos[1]:

- Para funcionarios públicos, al cometer una infracción grave pueden obtener una multa de 10 a 20 salarios básicos, además el Estado también podrá ser responsable por los daños causados.
- Para empresas privadas y públicas, al cometer infracciones graves, la multa es del 0.7 % al 1 % de sus ingresos del año anterior. La Autoridad decidirá el monto según la Intención, historial, daño causado, Reincidencia
- Para empresas públicas, al igual que los funcionarios públicos, al cometer infracciones graves, la multa va desde 10 a 20 salarios básicos unificados de su ingreso al mes anterior en que se impuso la multa. La Autoridad decidirá el monto según la Intención, historial, daño causado o Reincidencia

- Para empresas extranjeras sin sede en Ecuador que realicen infracciones graves, se notificará la sanción a la autoridad de protección de datos del país donde esté su sede principal, para que aplique las medidas correspondientes.

2.2.8 Roles definidos en la LOPDP

Según la LOPDPD y la ISO 27701 cláusulas 5.2[10], en la tabla 17 se presentan los integrantes principales que mencionan que son necesarios para el funcionamiento de la ley, dentro de ellos tenemos los siguientes roles presentados en la tabla 17[2, p.3]:

Tabla 4.
ROLES DEFINIDOS EN LA LOPDP (ADAPTADO DE [2, P.3])

ROL	DESCRIPCIÓN	LOPDP/ISO
Titular	Persona natural quien proporciona los datos para que sean objeto de tratamiento.	LOPDP Art. 4
Responsable del tratamiento	Persona natural o jurídica, del sector privado o público, quien decide la finalidad del uso de los datos.	LOPDP Art. 47 / ISO 27701 §5.2.1 / ISO 27001-5.3
Encargado del tratamiento	Persona que trata los datos personales a cuenta de un responsable del tratamiento de datos.	LOPDP Art. 4, 47 / ISO 27701 §5.2.3
Tercero	Autoridad de protección de datos.	-
Destinatario	Persona natural o jurídica que recibe una comunicación de los datos personales.	-
Autoridad de protección de datos	Entidad con autonomía administrativa y financiera.	-
Entidades certificadoras	ISO/IEC.	-
Delegado de protección de datos personales	Es el encargado de controlar permanentemente la protección de los datos personales, especialmente cuando la empresa maneja información sensible con grandes volúmenes de datos.	LOPDP Art. 48-49 / ISO 27701 §6.3.3

De acuerdo con el análisis en la tabla 17, la empresa Borealplast debe implementar un Delegado de protección de datos personales y un Responsable del tratamiento, ya que no cuentan con

este puesto en su organización, esto ayudara al manejo correcto de los datos personales de los stakeholders que maneja la empresa, adquiriendo la confianza y seguridad de estos.

2.3 Estándares internacionales de Protección de Datos-ISO 27001/27701

2.3.1 Norma ISO 27001:2022

Esta norma es la más conocida dentro del mundo para sistemas de gestión de la seguridad de la información (SGSI). En particular, la norma ISO/IEC 27001 sirve de base doctrinal para la implantación de sistemas que ayudan a la seguridad de la información, además esta norma presenta los requisitos esenciales para el mantenimiento, implementación y mejoramiento de un Sistema de Gestión de Seguridad de la información[11]. Con el aumento significativo de la ciberdelincuencia y el desarrollo de amenazas nuevas, puede parecer difícil de combatirlas, es por ello por lo que la ISO 27001 ayuda a concientizar a las organizaciones de los riesgos a los que están expuestos si no se identifica a tiempo estos puntos débiles. Alexander Enoc Bono y Luis Antonio Tinocoro, en su trabajo de posgrado titulado, "Diseño de sistemas de gestión de seguridad de la información, basado en norma ISO27001:2022", demuestran que para tener un reconocimiento alto no es necesarios ser una empresa grande, para adoptar estándares internaciones, con su análisis realizado en 4 empresas, trata de concientizar sobre las utilidades que les puede brindar la ISO 27001, así como su aplicabilidad para cada uno de los servicios que proveen a sus clientes[12]. En la figura 4 , se destacan los principios fundamentales y adiciones de la seguridad de la información.

Fig. 4.
Seguridad de la información. Los principios fundamentales y adiciones de la seguridad de la información,
Adaptado de: [12]

En la figura 4, se detalla los principios básicos como son la confidencialidad que se refiere al acceso solo de personas autorizadas pueden acceder a la información. La integridad para mantener los datos exactos y sin modificaciones no autorizadas, la disponibilidad para que la información esté disponible cuando se necesite. Los autores[12], señalan que son principios adicionales pero que también aporta a la seguridad de la información como es el "no repudio", que garantiza que nadie pueda negar haber enviado o recibido información con alguna firma digital, la autenticidad para verificar que la información sea confiable y la rendición de cuentas que es la encargada de rastrear acciones hasta su responsable para detectar y solucionar fallos.

2.3.2 Norma ISO 27701:2019

La norma ISO 27701, es un estándar internacional derivado de la serie 27000, se concentra en la gestión de la información de privacidad (PIMS), esta norma fue aprobada y adapta en 2019, y es la encargada de prevenir la violación de los datos personales, ya que establece las métricas necesarias que deben adoptar las organizaciones[3]. Si una empresa desea certificarse conforme a la ISO/IEC 27701, es necesario que la organización ya cuente con la certificación ISO/IEC 27001, ya que es una norma de carácter subsidiario a la ISO/IEC 27001, esta norma puede ser utilizada por cualquier organización sin importar su tamaño, complejidad o el país donde opera. La norma ISO/IEC 27701, fue aprobada debido a la necesidad de mantener una protección más fuerte de los datos personales, e incluso ahora se maneja datos sensibles, y esta información

es manejada en varios departamentos, por ello esta norma ayuda a tener una protección más rigurosa de los datos personales[3].

2.3.3 Beneficios de la norma ISO 27001 e ISO 27701

En la figura 5 se detallan los beneficios que obtienen las organizaciones al trabajar con estándares internacionales y certificados. Aunque estas certificaciones no son obligatorias, proporcionan un importante prestigio empresarial, ya que no solo previenen violaciones de seguridad sino que también reducen costos, además, facilitan a organizaciones de todos los tamaños el cumplimiento de normativas con altos estándares de calidad.

Fig. 5.
Beneficios de la implementación de la Norma ISO 27001. **Tomado de:** [13].

En la figura 5 se puede apreciar los beneficios que obtiene una organización al implementar esta norma, se destaca la reducción de riesgos y violaciones de seguridad, la administración sistemática de vulnerabilidades, la disminución de costos operativos y el cumplimiento de normativas reconocidas globalmente. Además, estas prácticas fortalecen la confidencialidad de los datos, mejoran la confianza con clientes y socios, y proporcionan una ventaja competitiva al alinearse con referentes internacionales. Por último, ofrecen un marco estructurado para garantizar el cumplimiento regulatorio.

2.3.4 Beneficios de la ISO/IEC 27701:2019

Según el autor Erick Lachaud, los beneficios de adquirir este estándar internacional son [14]:

- Seguridad y privacidad integradas al combinar la gestión de seguridad (ISO 27001) y protección de datos en un solo marco.
- Reconocimiento global, ya que es una norma aceptada internacionalmente, con auditores disponibles en todo el mundo y por ello genera confianza con los stakeholders.
- Cumplimiento regulatorio simplificado porque ayuda a empresas multinacionales a alinear sus prácticas con diversas leyes de privacidad.
- Genera oportunidades comerciales ya que la certificación es valorada positivamente por el mercado, sin embargo no sustituye el cumplimiento directo del GDPR.

2.3.5 Estructura de la norma ISO 27001:2022 e ISO 27701:2019

La estructura de la Norma ISO 27001 se ha basado en el anexo SL, está compuesta por 10 clausulas, en donde se describen los requisitos generales para la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI)[13].

Fig. 6.
Estructura de la Norma ISO 27001:2022. **Fuente:** Elaboración propia.

La estructura de la norma ISO 27001, detallada en la figura 6, demuestra la importancia de esta herramienta, la cual está diseñada para salvaguardar los principios de confidencialidad, integridad y disponibilidad de la información, cumpliendo con los requisitos legales y protegiendo la información contra riesgos potenciales. Su adopción fortalece la confianza institucional ante empleados, clientes, colaboradores y socios comerciales, posicionando a la empresa en un estándar de excelencia internacionalmente reconocido.

Estructura 27701:2019

La norma ISO 27701 amplia los requisitos de la ISO 27001, es decir esta norma se enfoca más en la protección de la privacidad, es una norma relevante cuando se maneja información personal. En la Tabla 5 se detalla la estructura de la ISO 27701:2019 de acuerdo con la perspectiva de Eric Lachaud en su artículo "ISO/IEC 27701 standard: Threats and Opportunities for GDPR Certification"[14].

Tabla 5.
ESTRUCTURA NORMA ISO 27701:2019 **ADAPTADO DE:** [14]

Componente	Descripción
Extensión de ISO 27001	▪ Es una ampliación de la norma ISO 27001 (seguridad de la información) para incluir gestión de privacidad. ▪ Requiere tener primero un Sistema de Gestión de Seguridad (ISMS) implementado.
Sistema de Gestión de Información Personal (PIMS)	▪ Añade controles específicos para proteger datos personales dentro del ISMS existente.
Certificación conjunta	▪ No se puede certificar por separado: debe evaluarse junto con ISO 27001.
Relación con otras normas	▪ Algunas secciones repiten requisitos de ISO 27001/27002. ▪ Otras agregan o adaptan requisitos para enfoques de privacidad.

De acuerdo con la tabla 5 se puede evidenciar que la ISO 27701 no reemplaza a ISO 27001, sino que la complementa con reglas específicas para privacidad.

2.4 Comparativa con el GDPR vs LOPDP

La Ley Orgánica de Protección de Datos Personales (LOPDP) se relaciona con más marcos regulatorios internacionales que han influido en su estructura y aplicación dentro del Ecuador. A continuación, en la tabla 6 se realiza una comparativa entre la LOPDP y el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

Tabla 6.
COMPARATIVA ENTRE LA LOPDP (ECUADOR) Y EL GDPR (UE). **ADAPTADO DE:** [1] Y [15]

Criterio	**LOPDP (Ecuador)**	**GDPR (Unión Europea)**
Entrada en vigencia	2021	2018
Consentimiento	Requiere consentimiento explícito y verificable.	Requiere consentimiento libre, informado y específico.
Principios	Consentimiento, finalidad, proporcionalidad, seguridad, transparencia.	Legalidad, minimización, integridad, rendición de cuentas.
Derechos del titular	Acceso, rectificación, cancelación, oposición, portabilidad.	Idénticos derechos ARCO + derecho al olvido y a la limitación.
Delegado de Protección de Datos (DPD)	Recomendado para responsables y encargados que traten datos sensibles.	Obligatorio en organismos públicos y empresas con tratamientos sistemáticos.
Multas	Desde el 0.7 % Hasta 1 % de la facturación anual.	Hasta 4 % del volumen de negocio global o 20 000 millones.
Ámbito de aplicación	Ámbito Nacional: aplica a responsables ubicados en Ecuador.	Extraterritorial: aplica a organizaciones que esten fuera de la UE, si tratan datos de ciudadanos europeos.

En la tabla 6, se analizan aspectos claves como son los principios, derechos, roles, las sanciones e incluso el alcance que ambos reglamentos mantienen, esta comparativa permite evidenciar que, aunque la LOPDP se ha inspirado en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, existen diferencias claves en cuanto a las sanciones y la obligatoriedad del Delegado de Protección de Datos (DPO). No obstante, ambas leyes comparten la responsabilidad proactiva en el tratamiento adecuado de los datos personales.

2.5 Relación entre la LOT y LA LOPDP

Dentro del marco regulatorio ecuatoriano, ya existía una normativa anterior a la LOPDP, esta normativa regula todo lo relacionado con las telecomunicaciones como: establecer medidas de protección y seguridad para garantizar los derechos de los ciudadanos dentro de una empresa, la Ley Orgánica de Telecomunicaciones o por sus siglas LOT contempla alguno puntos que se relacionan con la LOPDP. Por esta razón, es importante analizar la relación que mantienen algunos artículos de la LOT y la LOPDP, y así realizar una evaluación a la empresa Borealplast para determinar si antes de la implementación de la LOPDPD ya cumplía con las disposiciones de la LOT referente a la protección de datos. En la tabla 7, se realiza un análisis comparativo entre la LOT[16] y la LOPDP[1]:

Tabla 7.
COMPARACIÓN LOT VS LOPDP. **ADAPTADO DE:** [1] Y [16]

LOT		**LOPDP**	
Artículo	**Concepto**	**Artículo**	**Concepto**
Art. 24	▪ Garantiza acceso no discriminatorio ▪ Protección datos personales ▪ Medidas seguridad redes	Art. 10, 37, 39, 47	▪ Bases legales tratamiento ▪ Seguridad sistemas ▪ Sanciones incumplimiento
Art. 78	▪ Intimidad: acceso restringido ▪ No uso comercial no autorizado	Art. 26, 37, 41, 47	▪ Confidencialidad ▪ Limitación transferencias ▪ Derecho de oposición
Art. 79	▪ Informar violaciones datos	Art. 46	▪ Notificación violaciones
Art. 82	▪ Consentimiento uso comercial ▪ Alineación parámetros legales	Art. 8	▪ Consentimiento informado

En el análisis de la tabla 7, se puede apreciar una relación notable entre ambas leyes, esta relación menciona que las organizaciones que ya implementaban la LOT también estarían cumpliendo con la LOPDP, es decía aquellas empresas que ya han integrado la LOT tiene una base fundamental para la implementación de la LODPD.

2.6 Relación de la ISO 27001 y la LOPDP.

La ISO 27001 es la herramienta que garantiza la confidencialidad, integridad y disponibilidad de los datos que debe cumplir la LOPDP. Como se presentó en los apartados anteriores, la LOPDP es la que garantiza la protección de todos los datos personales de una persona identificada o identificable, mientras que la ISO 27001 es el estándar que garantiza la seguridad de la información. De este modo, la ISO 27001 permite que los principio de la LOPDP presenten un SGSI para garantizar un cumplimiento formal , en la tabla 8 se evidencia la relación intrínseca que mantienen la normativa legal y con el estándar internacional.

Tabla 8.
COMPARATIVA ENTRE LA LOPDP E ISO 27001 EN PROTECCIÓN DE DATOS PERSONALES.
ADAPTADO DE: [1] Y [17]

Aspecto	**LOPDP (Ecuador)**	**ISO 27001 (Internacional)**
1. Protección técnica de datos personales	Garantiza la seguridad de los datos con medidas técnicas y organizativas.	Anexo A: Control de acceso (A.9), Criptografía (A.12), Seguridad en comunicaciones (A.13), Seguridad en adquisiciones (A.14).
2. Gestión de riesgos específica para datos personales	Evaluación de riesgos que puedan afectar los derechos de los interesados.	Cláusula 6.1 y A.6.1.2: Identificar activos de información que contengan datos personales y evaluar amenazas.
3. Responsabilidad proactiva y demostración	Obligación de demostrar cumplimiento (accountability).	Generación de evidencias: políticas de seguridad, inventarios, informes de evaluaciones de impacto, auditorías internas.
4. Gestión de incidentes y notificaciones	Notificación obligatoria de brechas en menos de 72 horas.	A.16.1: Gestión integral de incidentes desde la detección hasta el análisis post-incidente para evitar reincidencia.
5. Seguridad en cadena de suministro	Responsabilidades específicas del RTDP y DPD en contratos.	A.15: Acuerdos de confidencialidad y monitoreo contractual con proveedores.
6. Mejora continua	Establece parámetros fijos de cumplimiento.	Sistema adaptable a las características de cada organización y auditorías externas periódicas.

Al implementar la LOPDP con la ISO 27001es una forma práctica de obtener un prestigio más alto de la organización, en la tabla 8 se evidencio como la 27001 presenta el material necesario para ayudar al cumplimiento de la LOPDP.

2.7 Comparativa LOPDP vs NIST Privacy Framework(EE. UU)

NIST Privacy Framework (National Institute of Standards and Technology, EE.UU), no es considerado una ley, pero contiene un conjunto de guías técnicas y estándares orientadas a la gestión de la seguridad de la información, uno de sus documentos mas destacados es el NIST Privacy Framework[18], el cual es un modelo de ayuda para las organizaciones al momento de gestionar riesgos de privacidad.

Tabla 9.
COMPARATIVA ENTRE LA LOPDP Y EL NIST PRIVACY FRAMEWORK. **ADAPTADO DE:** [1] Y [18]

Criterio	**LOPDP (Ecuador)**	**NIST Privacy Framework (EE.UU.)**
Naturaleza	Ley de cumplimiento obligatorio.	Marco voluntario para organizaciones.
Enfoque	Jurídico, sancionador, basado en derechos y deberes.	Técnico-organizacional, enfocado en gestión de riesgos de privacidad.
Consentimiento	Requiere consentimiento informado para el tratamiento de datos.	Promueve la transparencia, no exige consentimiento legalmente.
Derechos de los titulares	Establece derechos como acceso, rectificación, eliminación, oposición, portabilidad.	Promueve el control individual, sin definir derechos jurídicos obligatorios.
Evaluación de impacto	Obligatoria para tratamientos de alto riesgo.	Recomendado como parte de la evaluación de riesgos.
Multas o sanciones	Establece sanciones de hasta el 1 % de la facturación anual.	No contempla sanciones, sirve como guía preventiva.

En la tabla 9 se realiza una comparación entre los enfoques de la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP) con el Privacy Framework del NIST de los Estados Unidos. La diferencia se basa más en la obligatoriedad, la LOPDP es una ley centrada en obligaciones, sanciones y derechos mientras que el NIST es una guía voluntaria para gestionar riesgos de privacidad, con énfasis técnico y organizacional. Esta comparativa permite comprender la dualidad entre ambos marcos legales, útil para que empresas como Borealplast adopten un enfoque integral de protección de datos.

2.8 Datos Personales

Según el Tribunal de Justicia de la Unión Europea (TJUE), el concepto de dato personal es muy extenso, cuando hablamos de datos personales, nos referimos a cualquier información que se refiere a una persona natural como: nombre, correo, cédula, huella dactilar, historial médico, datos bancarios, teléfono, perfiles de usuarios de las redes sociales, etc[15].

2.8.1 Derecho a la intimidad

El derecho a la intimidad no es algo reciente; sin embargo, en un mundo cada vez más tecnológico y vigilado, protegerlo se torna más complicado. El termino intimidad viene del latín intus que significa, "dentro", es decir se refiere a algo que está muy al interior de una persona. Este derecho está protegido por la Constitución en el artículo 66, numeral 20, el cual garantiza la privacidad humana y la protección de los datos privados[1]. Lo íntimo es una parte sustancial que compone al ser humano y no necesariamente tiene que ser un secreto para la sociedad. Esto se evidencia también en la norma ISO 27001 A.10[19].

No obstante, es necesario recalcar que las personas son libres de decidir si dan o no a conocer su información y hasta qué punto lo hacen. En contraste, en la teoría del mosaico, postulada por Madrid Conesa en 1984, expresa que la intimidad está constituida por pequeños detalles íntimos, que si son analizados individualmente no son importantes ni especiales, sin embargo, estos pequeños detalles en conjunto pueden revelar datos importantes sobre la intimidad de una persona[20].

El derecho a la intimidad personal es un derecho irrenunciable, este derecho es reconocido por el Pacto Internacional de Derechos Civiles y Políticos de 1976, en su artículo 17, donde menciona el derecho y la protección a la privacidad, consecuentemente las autoridades públicas en este contexto no deben ser invasivas. Respecto a este derecho, en el 2015, la ONU publico una resolución llamada, "El derecho a la privacidad en la era digital", con ella busco incentivar a los Estados para salvaguardar este derecho en una era digital, si este derecho no se cumplía, los Estados tienen la obligación de brindar las herramientas necesarias para que la persona afectada por esta injerencia pueda recuperar su derecho, con el propósito de abarcar también la protección de los datos personales[20].

2.8.2 Datos personales sensibles

Según el artículo 4, de la Ley Orgánica de Protección de Datos Personales (LOPDP), los datos sensibles son aquellos que si no son tratados de manera segura puedes dar origen a discriminación y a la violación de los derechos humanos, los datos sensibles se refiere a los aspectos más íntimos de las personas como: la religión, orientación sexual, salud, condición migratoria, pasado judicial, etc[8]. El artículo 26 de la LOPDP menciona que el tratamiento de datos sensibles está prohibido a menos que atraviese algunas de estas circunstancias:

- Haber recibido el consentimiento del titular de los datos, especificándose claramente las finalidades de uso.
- En caso de ser necesario para cumplir con las leyes de trabajo o para que el titular o la empresa pueda ejercer algún derecho relacionado con el tema del dato sensible.
- El tratamiento es necesario si está en peligro la protección del titular y este no pueda dar su consentimiento por falta de capacidad física o jurídica.
- El tratamiento de datos sensibles que el titular haya hecho públicos.
- Realizar alguna petición por orden de autoridad judicial.
- Se permite el tratamiento de los datos sensibles solo si serán utilizados para fines estadísticos, investigaciones científicas o históricas y solo deben proporcionarse los que sean necesarios.
- El tratamiento de los datos de salud deben estar sujetos a las disposiciones establecidas en la presente ley.

2.8.3 Protecciones de datos personales

Las protecciones de datos personales combinan técnicas legales, organizativas y jurídicas que garantizan la integridad, seguridad, confidencialidad y disponibilidad de la información de las personas, estas medidas previenen la alteración, perdida, acceso no autorizado o divulgación ilícita. En el caso de Borealplast, pese a no contar con un delegado de protección de datos personales (DPO), ha implementado prácticas efectivas para salvaguardar la información de sus clientes, proveedores, socios y empleados. La LOPDP exige a las organizaciones cuenten con

un encargado de la protección de datos y exige a los encargados adoptar medidas necesarias para cumplir con el artículo 6 de la LOPDP, referente a la accesibilidad y confidencialidad, esto incluye controles de accesos, creación de sistemas cifrados e incluso la capacitación al personal y la elaboración de políticas y normas internas rigurosas[8].

2.9 Delegado de Protección de Datos (DPD)

El delegado de protección de datos es una figura clave dentro de una organización ya que es el encargado de asegurar el cumplimiento de la LOPDP [8]y de actuar como intermediario entre la empresa, los titulares de los datos y la Autoridad de Protección de datos personales, no se ha establecido un reglamento donde obligue 100 % a las PYMES a tener un DPD, pero su existencia ayuda al prestigio y buena práctica de la empresa, además que previene sanciones a las que son sometidas las organizaciones que no cumplen con la LOPDP. El DPD también es un rol importante presentado dentro de la ISO 27701 cláusula 5.2[10]

2.9.1 Principios generales de protección de datos

El DPD es un puesto primordial dentro de una organización y este debe cumplir con algunos principios generales para la protección de los datos personales. Según Berroa en la figura 6 se presenta los principios de Licitud, Calidad, Lealtad, Finalidad y Seguridad los cuales garantizan la correcta protección de los datos[21],

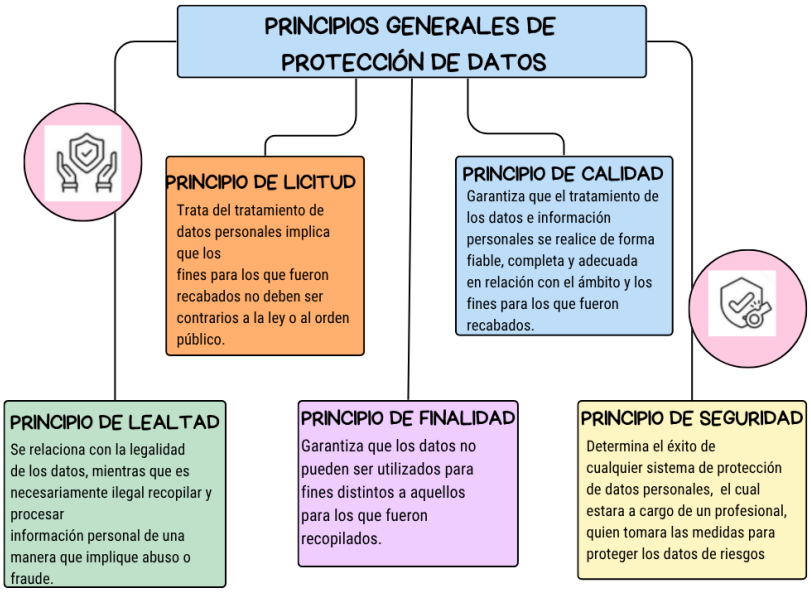


Fig. 7.
Principios generales de protección de datos. **Adaptado de:** [21]

La figura 7 presenta un resumen estructurado de los principios fundamentales de protección de datos personales establecidos en la normativa de protección de datos (LOPDP). Cada principio está destacado en negrita seguido de una breve explicación.

2.9.2 Identificación de la necesidad del DPD en la empresa

En la actualidad Borealplast, es una empresa líder en la fabricación y comercialización de todo tipo de fundas, rollos y láminas de plástico en todo tipo de medidas, elaboradas con polietileno de alta, baja densidad y con polipropileno cast-bio. Debido a su operación, la empresa maneja datos personales de proveedores, socios, clientes y empleados, esto hace que sea necesario garantizar la protección de los datos que han proporcionado los titulares. Esta medida se toma no solo por seguridad, sino que también fortalece el cumplimiento normativo y las buenas prácticas en el manejo de la información. La implementación de un DPD en Borealplast, brindara a la empresa confianza, transparencia y seguridad, tanto internamente como ante clientes, empleados y socios comerciales que exigen el cumplimiento de este derecho. Es necesario que Borealplast implemente este puesto, para prevenir sanciones derivadas del incumplimiento de la Ley orgánica de protección de Datos Personales (LOPDP), el DPD es el responsable de supervisar la adhesión a las disposiciones contenidas en esta ley, asegurando que la empresa obtenga altos estándares de privacidad y competitividad en el sector.

2.9.3 Evaluación del impacto y beneficios para la empresa.

La decisión de designar un DPD, ya sea por responsabilidad o buena práctica, conlleva un impacto positivo con beneficios para la empresa, un Delegado de Protección de Datos eficaz siempre aporta valores estratégicos y operativos a la imagen de la empresa como:

- Mitigación de Riesgos
- Generación de Confianza
- Asesoramiento Experto
- Punto de Contacto Oficial
- Mejora de Procesos Internos
- Cultura de Protección de Datos

2.10 Responsable de protección de datos personales

EL Responsable del Tratamiento de Datos Personales, será la figura clave de una empresa, esta persona puede ser natural o jurídica, privada o pública, y es el responsable del tratamiento de los datos personales recolectados por la empresa, en consecuencia, en este caso Borealplast es la entidad que decide cómo y para qué se recolectan la información de sus clientes, socios y empleados.

Obligaciones del Responsable del Tratamiento

Dentro de las principales obligaciones del responsable del tratamiento de datos tenemos los siguientes[8]:

- Asegurar el cumplimiento normativo de la LOPDP.
- Establecer el alcance y la finalidad de la recolección de datos personales.
- Elaborar y aprobar políticas internas, políticas de privacidad y avisos de tratamientos de datos.
- Garantizar la seguridad y confidencialidad de los datos personales de la empresa.

- Supervisar que terceros cumplan con las normativas de confidencialidad de los datos obtenidos de la empresa; en el caso de Borealplast, debe asegurar que Contífico, bancos y aseguradoras firmen contratos de confidencialidad y manejo de protección de datos.
- Implementar protocolos de respuesta a incidentes.
- Designar un Delegado de protección de datos personales (DPD) quien asesore y supervise el cumplimiento normativo de la LOPDP juntamente con el Responsable de Protección de datos personales (RTDP).

Por ejemplo:

Si un cliente, que ha dejado de pertenecer a la empresa, solicita la eliminación de sus datos personales. ¿Sabe el equipo de la empresa cómo proceder legalmente? Si la empresa no está preparada para realizar este proceso puede enfrentar una demanda por vulneración de derechos ARCO. Si este incidente llega a ser conocido por el sector empresarial, puede ocasionar una pérdida de contratos con clientes que exijan que se cumpla con la protección de datos personales y la seguridad de la información.

Otro ejemplo práctico adicional puede ser, cuando un empleado solicita la rectificación de su dirección en el sistema, el responsable debe garantizar que se cumpla con su requerimiento, en el tiempo establecido a 7 días, si el responsable no da respuesta al requerimiento, el titular puede presentar su reclamo ante la autoridad de protección de datos, estas acciones podrán ser penales, civiles o constitucionales de acuerdo a lo establecido en el capítulo IX, artículo 64 de la Ley orgánica de protección de datos personales del Ecuador[1].

Las obligaciones del Responsable del tratamiento de datos personales, no son solo legales, también deben ser estratégicas, ya que su principal objetivo es reducir el riesgo y proteger la información y la reputación de la empresa para generar confianza con los clientes y empleados.

Perfil del Responsable del Tratamiento de datos

El responsable del tratamiento de datos personales en esta ocasión es Borealplast, y la responsabilidad recae en el gerente general, debido a que tiene la potestad de tomar decisiones, asignar recurso y garantizar que las actividades a realizar estén dentro del cumplimiento normativo, los requisitos que debe cumplir el responsable del tratamiento de datos (RTDP) son:

- Responsabilidad del tratamiento de datos de la empresa.

- Conocimiento legal de la LOPDP ecuatoriana, así como un abogado conoce el código del trabajo.
- Conocimientos técnicos como buenas prácticas, seguridad de la información y ciberseguridad básica.
- Habilidades para coordinar equipos, liderazgo y capacidad para el manejo de registros.
- Mantener contacto con todas las áreas de la empresa (Administración, TI, Contabilidad, RRHH.).

Por ejemplo, si el RTDP identifica una brecha de información, debe actuar con la audacia de un bombero para proteger a los afectados, calmar el fuego y prevenir futuros incidentes, eso lo lograría, si mantiene un contacto con áreas claves de la empresa, coordina equipos para actuar inmediatamente al identificar el fluido de la información y realiza actividades de acuerdo con la normativa vigente para evitar futuras sanciones.

La seguridad de la información y la protección de datos no es exclusiva de las grandes organizaciones, también es un ejemplo de buenas prácticas para las PYMES como Borealplast, tratar la información de sus clientes, empleados y algunos socios con la misma confidencialidad que lo haría una entidad bancaria, con la diferencia de su realidad operativa.

2.11 Definición del perfil y Obligaciones del DPD

El perfil de un Delegado de Protección de Datos Personales debe poseer una combinación de conocimientos jurídicos, técnicos y de gestión. La LOPDP establece responsabilidades para el DPD estas deben conllevar a grandes resultados. El reglamento UE del Parlamento Europeo relativo a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, ha sido tomado y adaptado a la necesidad de cada país, según el artículo 38, apartado 3, pagina 56 de la RGDP, el DPD no recibirá instrucciones sobre el desempeño de sus funciones y no será destituido ni sancionado por ello, sino que rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado. El DPD está obligado a mantener el secreto profesional o la confidencialidad y puede desempeñar otras funciones siempre que no generen conflicto de intereses[22].

2.11.1 Designación del puesto Delegado de Protección de Datos

La designación del DPD viene directamente del responsable del tratamiento de datos (RTDP), en este caso es el Gerente General quien es la autoridad con mayor potestad de tomar decisiones en nombre de la empresa Borealplast, la designación de este puesto constituye un pilar fundamental para la empresa, debido a que no solo supervisa aspectos técnicos referente a la LOPDP, también integra funciones, consultivas, organizativas, de supervisión, información y sensibilización, además de servir como enlace entre las autoridades competentes y la empresa, para la designación de este puesto es recomendable tomar en cuenta los siguientes aspectos:

Perfil del DPD

El nivel de conocimiento de un Delegado de Protección de Datos (DPD) debe determinarse en función de la complejidad de operaciones de datos que maneja, para evaluar a un candidato para DPD, estas son algunos de los requisitos que se debe tomar en cuenta[23]:

- Experiencia sólida en temas de protección de datos, especialmente que mantenga un conocimiento profundo de la LOPDP y tenga la capacidad de redactar políticas de privacidad de acuerdo con el estudio realizado a la empresa perteneciente.
- Experiencia con respaldados, ciberseguridad o programación y certificaciones en seguridad de la información,
- Experiencia en protección de datos y auditorías informáticas.
- Habilidades para coordinar proyectos y equipos, liderazgo y coordinación para manejar varios proyectos al mismo tiempo.
- Habilidades para comunicarse con todo tipo de público, desde gerentes y directivos hasta personal técnico y legal.
- Experiencia técnica, legal y jurídica para el análisis e implementación de leyes.

En el caso de que la empresa opte por contratar un Delegado de Protección de datos Personales con un marcado perfil junior, esta también deberá asumir el compromiso institucional de ayudar a esta nueva incorporación a mantenerse en constante capacitación. Esto se acompañará del establecimiento de mecanismos de seguimiento y control lo cual se verifique tanto su ascenso profesional como técnico.

Existen Delegados de Protección de Datos (DPD) junior que han adquirido formación especializada en la protección de datos incluso antes de la obtención de su título, estas personas pueden ser contratadas por contar con certificaciones que avalúen sus conocimientos en la protección de datos, lo cual garantiza una ventaja e impacto positivo en la empresa al contratar un profesional con conocimientos y experiencias iniciales en el área.

Funciones del DPD

En la figura 8, se establecen las funciones de un delegado de Protección de Datos.

Fig. 8.
Funciones del Delegado de Protección de Datos. **Adaptado de:** [24, p. 111]

Estas funciones garantizan el trabajo del DPD, están orientadas a construir una cultura de protección de los datos personales y seguridad de la información, a continuación, se describe las funciones presentadas en la figura 8 con ejemplos prácticos en el contexto de la empresa.

- **Funciones organizativas:** el DPD lleva registros detallados y actualizados de las operaciones relacionadas con el tratamiento de datos personales, para la realización de este proceso se puede utilizar herramientas como Excel o softwares especializados.

  Por ejemplo, es el encargado de verificar que el departamento de contabilidad utilice los datos de los empleados solo para el fin solicitado, como puede ser la nómina y pago de salarios.

- **Funciones de supervisión:** el DPD, debe vigilar que no existan brechas de seguridad de la información, en caso de robo o mal uso de los datos, debe notificar inmediatamente a la autoridad competente, tomar acciones correctivas para prevenir que el daño se expanda y evitar riesgos de sanciones.

  Por ejemplo, si un empleado pierde su computador o USB con la base de datos de los empleados y clientes de la empresa, debe investigar el suceso, notificar a la autoridad competente y a los afectados lo más pronto posible, sin embargo, el equipo informático asignado al DPD debe ser cifrado de manera robusta desde el momento de su asignación.

- **Funciones consultivas:** el DPD tiene la obligación de revisar contratos y procesos que manejan las diferentes áreas de la empresa y proponer mejoras para cumplir con la LOPDP.

  A modo de ejemplo, el DPD debe revisar que el contrato con el software contable incluya cláusulas de protección de datos y confidencialidad.

- **Funciones de información y sensibilización:** el DPD es el encargado de capacitar a todo el personal sobre las buenas prácticas respecto al manejo de los datos personales en su vida diaria, para lograr este objetivo se debe mantener una formación y comunicación constante.

  Por ejemplo, se debe realizar charlas impartidas por el DPD de la LOPDP e instruir sobre la importancia de verificar la información enviada por correos o la importancia de la protección y actualización periódica de sus contraseñas.

- **Nexo de Contacto:** el DPD es el encargado de mantener una comunicación entre la autoridad de protección de datos y la empresa; debe facilitar el acceso a la información cuando la autoridad lo solicite.

  Por ejemplo, si la empresa cancela el contrato con Contífico, software contable de la organización, el DPD debe coordinar con el área de contabilidad y solicitar la eliminación inmediata de los datos de la empresa en el software contable (Contífico).

Responsabilidades del DPD En la figura 9, se presentan las responsabilidades de un Delegado de Protección de datos personales, las cuales son esenciales para garantizar el correcto manejo de los datos personales que la empresa procesa.

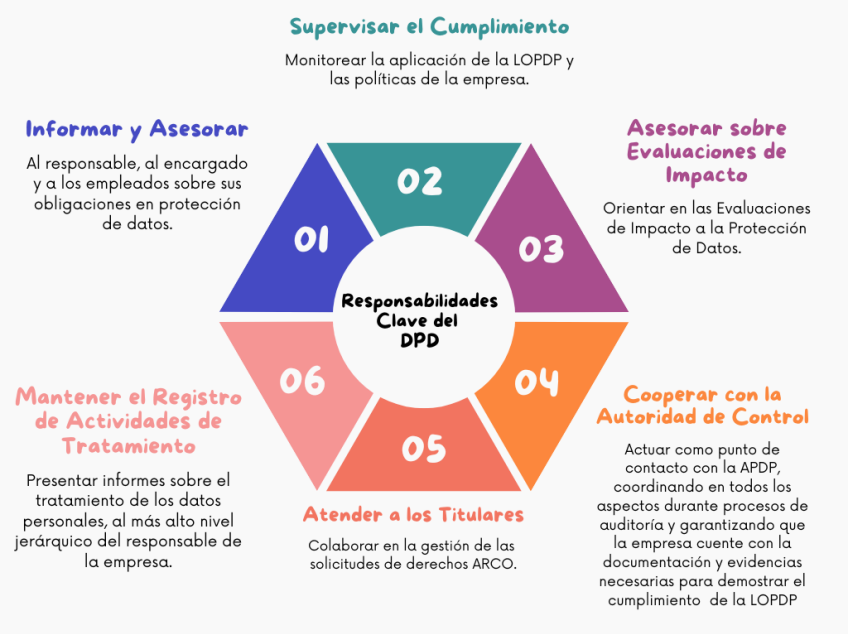


Fig. 9.
Responsabilidades del Delegado de Protección de Datos. **Fuente:** Elaboración propia

El DPD debe orientar a todos los encargados y empleados sobre las responsabilidades que tienen a la hora del manejo de los datos personales, de las responsabilidades presentadas en la figura 9, se describirán las siguientes:

Informar y Asesorar: Es responsabilidad de DPD, guiar y educar a todo el personal de la empresa sobre como cumplir con la normativa ecuatoriana vigente, desde los directivos hasta los empleados.

Supervisar el Cumplimiento: El DPD es el encargado de inspeccionar que la empresa cumpla con la LOPDP y las políticas internas de la empresa.

Asesorar sobre Evaluaciones de Impacto: En caso de que la empresa implemente alguna herramienta que implique el uso de los datos personales, es responsabilidad del DPD identificar y mitigar que el software no presente ningún tipo de riego para la información de la empresa.

Cooperar con la Autoridad de Control: El DPD es el enlace entre la autoridad de protección de datos y la empresa en caso de auditorías o incidentes. Además de ser el encargado de demostrar el cumplimiento de la LOPDP por parte de la empresa.

Atender a los Titulares: Existen derechos y solicitudes de los titulares que el DPD debe velar por el cumplimiento, para una mejor comprensión tomaremos el ejemplo de un cliente.

- **Acceso:** Solicitar información sobre los datos que mantiene la empresa

- **Rectificación:** El cliente solicita la corrección de su correo; debe ser corregido inmediatamente.
- **Cancelación:** El cliente decide cancelar las actividades con la empresa y solicitar que sus datos sean eliminados de la base de la empresa.
- **Oposición:** el cliente tiene derecho a oponerse al uso de sus datos, especialmente cuando sus datos son utilizados para fines no autorizados.

Mantener el Registro de Actividades de Tratamiento: Es recomendable que el DPD documente todas las actividades o elabore un inventario de las operaciones que realiza la empresa referente al manejo de los datos personales. Por ejemplo, en una clínica se debe mantener actualizado el registro de los pacientes en Odontología, debido a que en cada cita se realiza el proceso de curación de distintas piezas dentales, de este modo el especialista mantendrá un seguimiento correcto del tratamiento que debe tener cada paciente.

2.11.2 Acta de designación de DPD

Es recomendable crear una Acta o Memorándum de Designación para que esta asignación sea formal y demostrable ante una autoridad, esta debe incluir:

- Nombre y cargo de la persona designada como Responsable.
- Número de cédula.
- Fecha de la designación.
- Enumeración clara y precisa de sus responsabilidades.
- Compromiso de la empresa de proporcionarle los recursos necesarios.
- Firma del representante legal y de la persona designada.

Ejemplo de formato de Acta de designación:

ACTA DE DESIGNACIÓN DE CARGOS

En la ciudad de ……, a los …… días del mes …… del …… siendo las ……, tras la convocatoria realizada por ……, se reúnen los directivos de la empresa …… con registro Único Contribuyente ……, el Gerente General Sr/a……, Gerente de Recursos Humanos Sr/a……, en función de testigo del evento el Sr/a……, para proceder a la designación formal del Delegado de Protección de Datos Personales (DPD), al Sr/a……, con cédula de identidad ……, quien será el responsable de velar por el cumplimiento normativo de la Ley Orgánica de protección de datos personales (LOPDP), a continuación se detalla las principales responsabilidades que deberán ser acatadas por el designado del cargo.

Responsabilidades

- Supervisar el cumplimiento normativo de la LOPDP ecuatoriana.
- Brindar atención al personal de la empresa sobre las solicitudes ARCO.
- Mantener actualizada la documentación del registro de actividades de la empresa referente al manejo de los datos personales.
- Coordinar auditorías para evitar e identificar riesgos asociados a la protección de datos.
- Proceder como intermediario con la autoridad de protección de datos personales.
- Asesorar al personal de la empresa sobre las buenas prácticas respecto al manejo de los datos personales.

Compromiso de la empresa

La empresa …… se compromete a brindar los recursos necesarios, ya sean técnicos, humanos o financieros, para la aplicación de sus funciones, además de facilitar el acceso a la información requerida para el cumplimiento de su labor. Siendo las …… del mismo día el Sr/a …… Gerente General de la empresa ……, declara finalizada la reunión. En constancia de lo expuesto, firman:

Gerente General	Delegado DPD.
Nombre:	**Nombre:** . . . . .
Gerente de RR.HH	Testigo
Nombre:	**Nombre:** . . . . .

2.12 Diferencia entre DPD y RTDP

Como se estableció previamente, la diferencia radica en el cargo y rol que mantiene cada uno, el Responsable del Tratamiento de Datos Personales (RTDP) es la persona jurídica que asume la responsabilidad legal y toma las decisiones sobre la finalidad y tratamiento de los datos, además de ser el encargado de delegar al DPD.

Por otro lado, el Delegado de Protección de Datos (DPD) supervisa que las decisiones del RTDP estén dentro de la normativa vigente, el DPD es un profesional interno o externo de la organización que mantiene conocimientos especializados, experiencia en protección de datos y conocimiento de la LOPDP, no tiene derecho a tomar decisiones sobre el tratamiento de los datos, pero actúa independientemente a la hora de supervisar el cumplimiento normativo por parte del responsable del tratamiento, adicionalmente tiene la responsabilidad de solventar las solicitudes ARCO, por ejemplo:

La empresa Borealplast decide implementar el sistema de un biométrico para mejorar el control de registros de asistencia de sus empleados, para ello toma decisiones sobre la finalidad que tendrán los datos y el medio por el cual serán recolectados. Dado que este sistema es considerado sensible por almacenar datos biométricos (huellas dactilares), se debe informar al DPD para que supervise la decisión, analice y detecte posibles riesgos.

2.13 Software Contable y Privacidad de Datos

Contífico

Contífico es un software adoptado por la empresa Borealplast para gestionar sus operaciones financieras y administrativas. Su uso es central en la empresa, debido a que a través de esta

plataforma se almacenan datos sensibles de clientes, empleados y socios, este proceso está sujeto a la LOPDP artículo 47 del capítulo VII, la empresa debe suscribir un contrato con Contítico que garantice el cumplimiento de la LOPDP y algunas cláusulas específicas como:

- Garantizar la confidencialidad y seguridad de los datos proporcionados por la empresa.
- Defina el procedimiento en caso de brechas de seguridad.
- Realice la devolución de los datos al finalizar el contrato.
- La falta de este contrato es considerada una falta grave dentro del art. 68 de la LOPDP.

Contífico es el repositorio central de los datos personales sensibles y no sensibles de la empresa, si no está sujeta a la normativa vigente se encuentra expuesta a riesgos significativos de incumplimiento de la LOPDP.

2.13.1 Arquitectura del Software Contable Contífico

Contífico es un software contable que almacena su información en la nube, es utilizado por empresas ecuatorianas para el desarrollo de inventarios, facturación electrónica, ventas, cuentas por cobrar y pagar[25]. Su arquitectura no se explica en su página oficial, pero se evidencian características inherentes a las plataformas SaaS (Software as a Service), que se refieren a aplicaciones que alojan su información en la nube y se ofrecen en internet, es decir, los usuarios pueden acceder al software desde cualquier dispositivo con conexión a internet. SaaS es una arquitectura multiinquilino, es decir, múltiples usuarios comparten una misma instancia de software, lo que ayuda a optimizar costos mediante economías de escala, pero mantienen mecanismos robustos de aislamientos de datos para cumplir con todas las regulaciones de la LOPDP. La escalabilidad del software contable es altamente escalable, es decir, se adapta a las demandas según las necesidades de los usuarios y mantiene auditorías periódicas de seguridad alineadas con estándares ISO 27018:2019[26].

2.13.2 Datos sensibles tratados por Borealplast en Contífico

La Ley Orgánica de Protección de Datos Personales establece los parámetros necesarios para la protección de datos sensibles. De acuerdo al art. 4 de la LOPDP, los datos sensibles necesitan una protección más robusta ya que el mal manejo de estos datos puede provocar discriminación o

vulneración de los derechos fundamentales de los titulares, el tratamiento de estos datos sensibles está prohibidos [1], salvo en casos extremadamente excepcionales como:

- Existir un "sí" rotundo en su firma de consentimiento informado
- El usuario no está obligado a firmar un consentimiento si no es libre.
- El titular debe conocer quién, para qué y cuánto tiempo serán almacenados sus datos.

Aunque Borealplast se encuentra catalogada como una PyME, está realizando el tratamiento de datos sensibles en su sistema contable y en el sistema de registro de asistencia del biométrico, recoleta y trata los siguientes datos sensibles presentados en la tabla 10:

Tabla 10.
IDENTIFICACIÓN DE DATOS SENSIBLES TRATADOS EN BOREALPLAST SEGÚN LA LOPDP

Categoría de Dato Sensible (LOPDP Art. 4)	**Ejemplo en Borealplast**	**Sistema / Proceso donde se Recolecta**	**Justificación / Riesgo**
Datos de salud	Información sobre alergias graves y discapacidad	Archivos físicos y digitales de Recursos Humanos.	Puede provocar discriminación laboral como el despido injustificado o la no contratación.
Datos biométricos	Registro de huella dactilar para control de asistencia.	Sistema biométrico de control de acceso y asistencia.	Son únicos e irrevocables. Su robo o duplicación compromete la identidad del empleado de forma permanente y puede usarse para suplantación.
Datos financieros y patrimoniales	Número de cuenta bancaria, historial de transacciones salariales.	Software contable Contífico, manipulado por el área de contabilidad de la empresa.	Su exposición puede ocasionar robos, fraudes financieros, o extorsión contra empleados, clientes o socios.

Categoría de Dato Sensible (LOPDP Art. 4)	Ejemplo en Boreal-plast	Sistema / Proceso donde se Recolecta	Justificación / Riesgo
Datos de afiliación	Información sobre el tipo de seguro.	Archivos de RR.HH.	Puede usarse para represalias en el ámbito laboral o algún tipo de discriminación.
Datos de origen étnico o racial	Están presentes en documentos de identidad o en información autodeclarada. También incluye la religión.	Archivos generales de RR.HH., como contratos.	Su manejo indebido es la base de discriminaciones graves.

Estas operaciones no son ajenas al tratamiento de datos sensibles. La recolección que realizan de huellas dactilares (biometría) para el control de asistencia de sus empleados a través de Contífico y los archivos de RR.HH, coloca directamente a la empresa bajo el ámbito de aplicación estricto de la LOPDP y la implementación inmediata de la guía metodológica propuesta, para establecer las medidas de seguridad que prevengan sanciones y, lo más importante, proteger los derechos fundamentales de todos los stakeholders de la empresa.

2.13.3 Buenas Prácticas de Privacidad de Datos

Las buenas prácticas no solo se refieren al trabajo con ética y moral, sino también a mantener hábitos que garanticen la seguridad de nuestros datos personales, dentro de la ciberseguridad existen algunos estándares y normas para garantizar la protección de la información personal estas buenas prácticas están relacionadas con los principios de la LOPDP y los estándares internacionales ISO 27201, a continuación, se presenta recomendaciones claves para garantizar la seguridad de la información[27]:

- **Gestión de acceso basada en roles, responsabilidades y solicitudes ARCO:** el acceso a la información debe basarse estrictamente en los roles y responsabilidades de cada usuario.

- **Mantener una autenticación robusta:** se debe utilizar contraseñas complejas y estas deben ser actualizadas periódicamente.
- **Cifrado de datos:** esto permite que la información esté protegida ante accesos no autorizados o interceptaciones.
- **Registro de Actividad y Auditoría (Logs):** se debe mantener un registro detallado de las acciones realizadas sobre los datos personales, es decir, (qué modificó, quién accedió, cuándo y desde dónde), esto garantiza el cumplimiento de la LOPDP y la detección de incidentes maliciosos.
- **Minimización y Calidad de Datos:** Los datos recolectados deben ser estrictamente solo los necesarios para la finalidad contable y de facturación.
- **Firmar acuerdos de confidencialidad con los usuarios del sistema:** toda empresa debe realizar el proceso de firma de la carta de autorización para el manejo y protección de los datos personales que serán recolectados del titular.
- **Capacitación al personal contable sobre privacidad de datos:** es necesario realizar capacitaciones a los stakeholders que pertenecen a una organización, para así prevenir accidentes de flujo de información.
- **Realizar una auditorías internas:** se debe realizar una auditorías internas de cómo se ingresan y almacenan los datos,
- **Cláusulas de privacidad:** Integrar cláusulas de privacidad en contratos con proveedores tecnológicos.
- **Aplicar metodologías:** Aplicar la metodología ISO 27001 para identificar activos, riesgos y controles.
- Solicitar a Contífico, el encargado de prestar el servicio del sistema contable a la empresa, un reporte sobre el cumplimiento de la privacidad sobre los datos personales.

2.14 Trabajos Relacionados

Después de haber revisado fuentes bibliográficas de varios proyectos de investigación, revistas científicas a nivel nacional e internacional, artículos y libros, se encontraron investigaciones que aportaron un importante contenido para la realización de este trabajo, entre ellos tenemos:

Según Álvarez (2017), en la Revista de Derecho, con la temática titulada como "Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales ", menciona que la protección de los datos personales tiene origen como un mecanismo jurídico en la era de las tecnologías de la información para proteger este último derecho a la vida privada [28]. Sus objetivos clave incluyen la conceptualización de qué son los datos personales y la designación de una parte responsable del procesamiento de estos y el nivel de protección necesario. Como tal, la Constitución del Ecuador, en su calidad de República, expresa que "se reconoce el derecho a la protección de los datos personales, los capítulos básicos otorgan a cada persona la capacidad para decisión propia. Para decidir cómo van a ser utilizados sus datos.

Mientras que Pérez, P.(2020), en la Revista de la Facultad de Derecho en su artículo titilado como "La protección de los datos personales como derecho fundamental: su autonomía y vigencia propia en el ordenamiento jurídico estatal" examina la defensa de datos como un derecho fundamental independiente y contrastan con otros derechos como el honor, la intimidad y la privacidad que a enfrentar la era digital resultan obsoletos, un elemento crítico de la investigación es la explicación de dato personal, se define como aquella información que puede ser utilizada para confeccionar un perfil, como el nombre, la dirección, correo electrónico, grabaciones de voz y fotografías, número de cuentas bancarias, datos familiares, información laboral, social o económica, referencias ideológicas, raciales, étnicas o religiosas. Por esta razón, se tiene que proteger que terceros no accedan a utilizar esta información para evitar actos de discriminación o la configuración de perfiles mediante la recopilación y tratamiento de datos [29].

Según la Asamblea Nacional del Ecuador (2021), de acuerdo al artículo 66 numeral 19 de la constitución de la Republica reconoce y asegura a los ecuatorianos el derecho a la protección de sus datos personales, es decir las personas tienen el derecho de decidir sobre su información personal, así como exigir que sus datos este protegidos, además se establece que para la recolección de estos datos se necesita la autorización del titular o una orden legal, este artículo permite tener una mejor orientación en el monitoreo de los niveles de seguridad, analizar los riesgos que

se pueden presentar y con ello implementar un sistema de gestión de seguridad efectivo dentro de cualquier empresa sin importar si es grande o pequeña, privada o pública [1].

En tanto que, Porven, Morejón y Pérez (2021), en su proyecto titulado como La protección de datos personales. presupuestos constitucionales para su protección en los procesos judiciales en cuba, definen los datos personales como información alfabética, numérica, fotográfica o grafica que concierna a personas físicas, que estén identificadas o estén por identificarlas, además existen los datos sensibles que son aún más delicados y pueden afectar nuestra privacidad si llegaran a ser revelados como el origen racial y étnico, opiniones políticas, formas de pensar, estado de salud o preferencia sexual, convicciones religiosas, también enfatizan sobre el derecho que tenemos cada uno de nosotros para ver el uso de nuestra información, Aunque la protección de datos y la privacidad tengan relación, son diferentes, la primera se refiere al control sobre nuestra información mientras que la segunda nos permite mantener alejada nuestra vida privada lejos de los demás [30].

En tanto que Serrano, M. (2023),en su artículo titulado "La protección de los datos personales en defensa de la dignidad individual ante los riesgos de pérdida de privacidad" analiza y explica como la tecnología puede amenazar la dignidad de una persona, el impacto positivo y negativo que ha tenido la tecnología en los derechos, la importancia de mantener la privacidad en el entorno digital, la naturaleza jurídica del derecho a la protección de datos y el papel de habeas data en Latinoamérica, presenta la ley de protección de datos como un pilar fundamental en el entorno digital, directamente relacionado con la dignidad humana, además resalta que se debe extender la cultura de la protección de datos a ciudadanos, empresas privadas y públicas para mejorar la calidad de vida dentro y fuera del internet sin amenazar la dignidad y los derechos, la autora recomienda mantener sus datos personales con responsabilidad, y siempre verificar que sus datos este protegidos por la ley orgánica de protección de datos personales[31].

Según Miguel Arcos, Karina Matute y Mesías Fernández (2023), en su proyecto publicado en la Revista Ibérica de Sistemas de Tecnologías de Información, titulado "Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos", se evidencia que tanto la legislación ecuatoriana como la colombiana comparten principios fundamentales en materia de protección de datos. Ambas normas reconocen el derecho de las personas a la intimidad personal y familiar, así como a la protección de su buen nombre, garantías que el Estado debe respetar y hacer

cumplir, el derecho de los ciudadanos a conocer, actualizar y rectificar la información personal almacenada en bancos de datos, ya sean de entidades públicas o privadas [32].

Los autores destacan estas leyes porque buscan salvaguardar los derechos fundamentales de privacidad y protección de datos personales. En este contexto, un Sistema de Gestión de Seguridad de la Información (SGSI) se muestra como una herramienta estratégica para las organizaciones, ya que proporciona un marco estructurado para garantizar el tratamiento adecuado de la información personal conforme a los requerimientos normativos, previene el manejo indiscriminado de datos clasificados como confidenciales e implementa mecanismos de protección contra amenazas en el ciberespacio. Para lograr los objetivos establecidos, las organizaciones deben designar personas específicas a cargo del tratamiento y la seguridad de los datos personales, imponer restricciones internas con sanciones definidas por infracción a las políticas. La comparación internacional muestra que, aunque Ecuador está avanzando en lo que respecta a la protección de datos personales y la adopción de estándares como el SGSI es vital para alcanzar niveles adecuados de ciberseguridad como se demanda hoy en día [32].

Además, Redrobán Barreto (2023), en su artículo ”Protección de Datos Personales en Ecuador a consecuencia de la emergencia sanitaria Covid-19”, publicado en la Revista Universidad y Sociedad, detalla cómo el uso de aplicaciones digitales durante la pandemia creció no como una elección o una opción, sino como una necesidad imperiosa para preservar la salud de las personas [33]. A medida que este proceso se dio con tal fuerza entre los habitantes de la red, el incremento del uso de aplicaciones digitales expuso a sus usuarios a una mayor posibilidad de ciberdelito. Los usuarios de plataformas digitales expusieron información a través de datos personales, así como datos sensibles (relacionados con acciones como la compra de productos y el contenido de algunas páginas, así como URL de acceso no seguras) sin tener en consideración jamás de lo que podía acarrear el uso de aplicaciones digitales. El propio autor remarca la importancia de un correcto tratamiento y una correcta regulación del tratamiento de datos de personas para garantizar y proteger derechos fundamentales que todas las personas tienen, como el derecho al honor, el derecho a la imagen, el derecho a la intimidad personal y familiar. Sin embargo, a la vez, en un mundo donde las redes sociales tienen predominancia en la relación entre los seres humanos, el poder de garantizar estos derechos es extremadamente difícil. Por todo ello Redrobán opina que el tratamiento y la protección de datos no puede ser considerado únicamente responsabilidad del Estado (ya que si así fuera el país podría decidir qué información a quién dar y cuándo), sino que hace falta que también exista una conciencia social respecto a un uso,

una utilización y un tratamiento de datos de personas que salvaguarde la ética, la seguridad y la capacidad de haber dado un consentimiento informado [33].

Finalmente, Yunganaula, B.(2024), en su proyecto de integración curricular titulada como "Propuesta de un plan de implementación para el cumplimiento de la ley orgánica de protección de datos personales en la empresa Cabletel", presenta la LOPDP como una normativa esencial y de cumplimiento obligatorio en Ecuador, aborda la necesidad de una empresa de cumplir con la promulgada ley orgánica de Protección de datos personales(LOPDP) y el análisis de la norma ISO/IEC 27002, estableciendo principios, requisitos y sanciones para asegurar un manejo adecuado de la información por parte de las empresas, según el autor, la Ley Orgánica de Protección de Datos Personales (LOPDP) es una normativa fundamental para las empresas en Ecuador, incluyendo Cabletel, todas las empresas que manejan datos personales de usuarios están obligados a cumplir con esta regularización, aunque este estudio solo se centró en la empresa Cabletel sirve como ejemplo para cualquier empresa que tenga la necesidad de garantizar la seguridad y privacidad de los datos personales ante el avance acelerado de la tecnología y el manejo masivo de información por parte de las empresas [7].

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1 Enfoque y tipos de investigación

3.1.1 Enfoque

Para esta investigación se adoptó un enfoque mixto (cualitativo-cuantitativo), con base en Balmaceda [34], quien refiere a la investigación cualitativa como la encargada de recolectar y analizar datos cuantitativos para comprobar los resultados obtenidos durante la fase cualitativa. Además, Hernandez-Sampieri,menciona que la investigación cuantitativa se debe realizar de manera organizada, lo cual es primordial para realizar cualquier trabajo de investigación y así comprobar suposiciones, esta investigación es objetiva y trata de no influir con sus sentimientos, creencias o deseos, también menciona la investigación cualitativa sobre como realiza la recolección de datos durante las entrevistas, análisis de documentos y las observaciones. Es por ello por lo que para esta investigación se adoptó el enfoque cuantitativo para realizar un diagnóstico inicial, basándose en encuestas y análisis de brechas de cumplimiento, y el enfoque cualitativo para la interpretación de normas como la LOPDP e ISO 27001-27701 y la validación para la presente guía.[35].

3.1.2 Tipo de investigación

Durante la investigación se realizaron los siguientes tipos de investigación:

Investigación bibliográfica

La investigación bibliográfica o también conocida como documental, ayuda a recolectar y seleccionar información que hemos considerado importante durante el análisis de artículos, libros, revistas, archivos, tesis, entre otros, es decir no se realiza la recolección de datos nuevos, sino que usamos información existente, esto ayuda a ahorrar tiempo ya que no debemos realizar encuestas a un número considerado de personas para obtener una información confiable[36].

La investigación bibliográfica es importante porque permite probar las hipótesis planteadas mediante las investigaciones existentes; además, facilita al investigador en la adquisición de un

conocimiento exhaustivo del tema de su interés, lo cual es indispensable para garantizar un marco teórico sólido. Esta investigación es aplicada en todas las disciplinas ya que se debe entender la investigación desde el punto de vista de otros, para desarrollar de la manera correcta nuestra investigación, se debe prestar atención a las publicaciones recientes, así como a su validez y confianza en algunos casos es necesario verificar la reputación del autor o editor, esta fiabilidad se la puede identificar muchas veces por el número que citaciones del documento que muestra o al tipo de cuartil al que pertenece, una recomendación para el uso de datos bibliográficos es utilizar palabras claves, revisión por pares y recientes, además se recomienda utilizar bases de datos especializadas de alto impacto, tales como: Scopus, PubMed, ScienceDirect, Jstor y Wer of Science, ya que reducen el riesgo de utilizar referencias obsoletas o poco rigurosas[37].

Por ello este tipo de investigación se utilizó para recolectar información por medio de revistas, artículos y tesis en páginas web

Investigación de campo

La investigación de campo constituye la metodología central aplicada en el desarrollo del proyectos para ello, es necesario acudir al lugar para investigar y recaudar directamente la información desde el lugar donde ocurre los hechos, los datos obtenidos, son datos llamados primarios, porque son recabados de primera mano directamente de los informantes claves, ya sea por medio de entrevistas, encuestas, registros de observaciones, pruebas y algunas otras técnicas de recolección de datos que tienen la finalidad de darnos la información más relevante del tema de estudio. El objetivo principal de este enfoque es analizar y comprender los fenómenos de estudio en su entorno natural, para facilitar la recolección de datos, es decir, estudiar las acciones y eventos diarios de las personas[38].

Esta investigación se aplicó al recopilar la información en el lugar de los hechos, es decir, en la empresa Borealplast de la ciudad de Quito. El trabajo de campo consistió en realizar entrevistas y encuestas a todo el personal de la empresa, además de registros de observaciones participativas para identificar problemáticas específicas relacionadas con el manejo de los datos personales, los cuales constituyen el objeto central de este estudio.

Investigación descriptiva

Según Guevara, este tipo de investigación es la base para entender cualquier situación, ya que describe las características de un grupo, situación o un fenómeno sin alterarlo, responde a las preguntas: ¿Qué está pasando? o ¿Cómo es esto? Su principal característica es que debe ser

fácil de entender; por ejemplo, cuando un notario detalla su caso de manera precisa, verdadera y ordenada, no se debe modificar nada, solo debe registrar lo que se ve. Dentro de los métodos que menciona el autor [39], es la observación, ya que se debe observar y anotar lo que sucede, además menciona que existen dos tipos de observaciones como son:

- **Observación Cuantitativa**: se fija en números y cantidades.
- **Observación Cualitativa**: se fija en las cualidades y características.

En este proyecto, la investigación descriptiva está presente cuando se realizó el diagnóstico del estado actual de la empresa, en los requisitos legales, como son la LOPDP y la ISO 27001/27701, y en la descripción de la propuesta de implementación de la guía metodológica.

3.2 Diagrama de Proceso

En la figura 10 se detalla el proceso de implementación de la LOPDP para Borealplast, la guía está estructurada en tres fases principales, las cuales presentan un enfoque de mejora continua adaptándose a la normativa vigente de la LOPDP. Este esquema refleja el proceso que sustenta la investigación realizada para la guía metodológica propuesta.

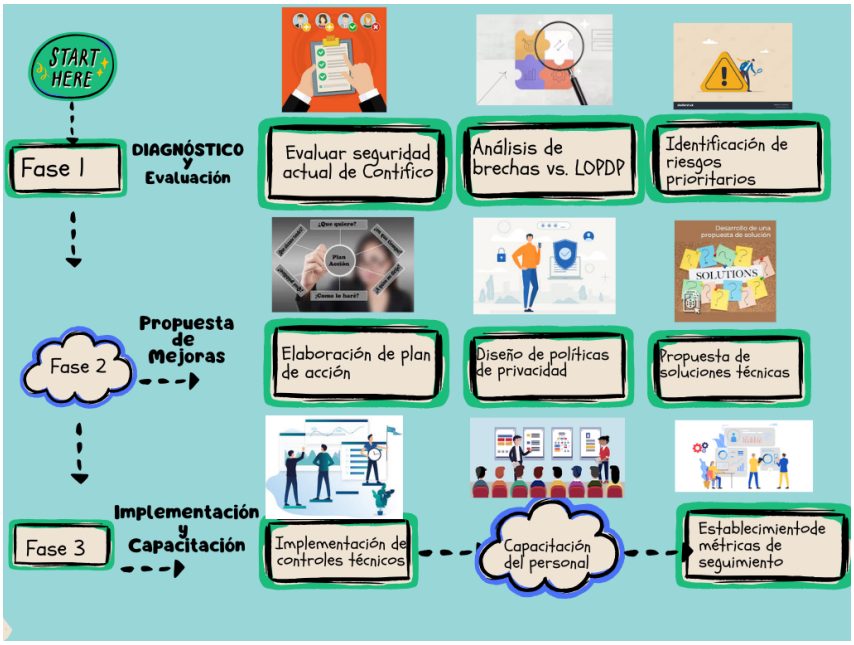


Fig. 10.
Diagrama de Proceso. **Fuente:** Elaboración propia

3.2.1 Fase 1 – Evaluación y Diagnóstico

En esta fase se realizó un análisis absoluto de la seguridad de la empresa, tomando como punto de partida el software contable Contífico, el cual es el encargado de registrar los datos personales de clientes, socios y empleados. Dentro de las actividades realizadas para este proceso se incluyeron:

- Análisis y diagnóstico de la seguridad de la información de la empresa.
- Comparación de las normativas de Borealplast frente a la normativa vigente de la LOPDP.
- Identificación de riesgos respecto al tratamiento de datos, entre ellos se detectaron brechas de información leves, falta de cifrado, accesos no auditados, consentimientos no documentados y la falta de políticas internas respecto al cumplimiento de la normativa.
- Otro método aplicado en esta base fue la observación directa, la cual permitió identificar los controles de seguridad que mantiene la empresa hasta el momento antes de implementar la guía propuesta.

En esta fase se obtuvo con precisión el nivel de cumplimiento que mantiene Borealplast respecto a la LOPDP, permitiendo establecer un punto de inicio para el desarrollo de la Guía metodológica.

3.2.2 Fase 2 – Propuesta de Mejoras

Luego de haber realizado la primera etapa, con los hallazgos obtenidos, se elaboró un plan de acción enfocado en solucionar las brechas identificadas, dentro de las actividades propuestas tenemos:

- Elaboración de un plan de mejoras considerando la LOPDP y los estándares internacionales como las ISO 27001/27701, para garantizar la finalidad, protección y manejo correcto de los datos personales.
- Diseño de políticas de privacidad alineadas a la LOPDP.
- Rediseñar la estructura organizacional, con el fin de incluir al DPD.
- Diseñar plantillas para protocolos ARCO y consentimientos informados.

Estas actividades están enfocadas a garantizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales y así de esta manera evitar posibles sanciones; asimismo, se comprometen a elevar el prestigio de la empresa, ya que las PYMES que implementan la LOPDP son reconocidas por cultivar la confianza de todos sus stakeholders claves.

3.2.3 Fase 3 – Implementación y Capacitación

Para el desarrollo de esta fase se realizaron algunas acciones piloto de implementación para las medidas propuestas, poniendo como prioridad las de mayor impacto en la protección de datos personales, e identificando las que son posibles ejecutar en el contexto actual de Borealplast, entre ellas tenemos:

- Desarrollo de políticas para el desarrollo de contraseñas robustas y renovables periódicamente.
- Capacitación al personal sobre los derechos y principios fundamentales de la LODPD, esto también se refiere a las buenas prácticas a la hora de manejar nuestros datos personales.
- Capacitación orientada a los controles de seguridad básicos, entre ellos el manejo adecuado de contraseñas, el correcto tratamiento de datos, la elaboración de políticas internas y la gestión de cometimientos informados.

Estas actividades ayudaron a sensibilizar sobre la importancia de la implementación de la LOPDP, creando así una organización orientada al cumplimiento normativo. Estas fases no solo permitieron identificar las brechas de seguridad de la información de la empresa, sino que también garantizaron un avance para que Borealplast se mantenga dentro de la normativa vigente de la LOPDP y de los estándares internacionales ISO 27001/27701.

3.3 Método Delphi

Delphi es un método predictivo que permite que un grupo de expertos dentro de una materia o campo concreto, evalúen un proyecto o tema de investigación a través de distintos cuestionarios repetidos y anónimos, con el fin de facilitar la toma de decisiones y llegar a un consenso.

La eficiencia y eficacia del método van a depender de si los investigadores consideran cuidadosamente el tema, el marco de investigación y finalmente los resultados esperados antes de iniciar el estudio[40].

3.3.1 Historia

Hace más de 50 años se realizó el primer experimento Delphi, y ha transcurrido más de 40 años desde que fue publicado el primer artículo sobre el procedimiento y uso del modelo, desde entonces se ha convertido en un modelo muy utilizado y reconocido para realizar predicciones y facilitar la toma de decisiones, para llegar a este resultado, el método ha tenido que superar varias fases como la crítica, popularidad y reevaluación. Con el transcurso de los años, los campos de aplicación para el método Delphi se han ampliado, destacando sus fortalezas, así como sus debilidades, es posiblemente el método técnico con nombre propio más reconocido, debido a que se ha basado en la opinión de expertos y sobre la que más se puede encontrar información.n [41]

Fue creada como estrategia durante la Guerra Fría; su nombre, Delphi, lo propuso el filósofo Abraham Kaplan, inspirado en el Oráculo de Delfos, un templo que en la antigüedad era muy visitado por los antiguos griegos cuando deseaban saber el futuro y obtener un consejo.[42].

3.3.2 Etapas del método DELPHI

Para aplicar el método Delphi según Munaretto y col., se debe tomar en cuenta las siguientes etapas[43]:

- **Definición del problema:** esta es la etapa principal del método, pues es donde se establece el tema o problema que se va a investigar, el tema o problema de investigación debe estar limitado para garantizar una correcta evaluación por parte de los expertos.
- **Elección del Facilitador:** este rol puede ser asumido por el propio investigador o a la vez se puede seleccionar a un experto, debido al análisis de los datos recolectados que se debe realizar.
- **Determinación de conocimientos de los expertos seleccionados:** es recomendable que los expertos cuenten con experiencia y profundo conocimiento en el área a evaluar, para obtener información válida y relevante en el estudio.
- **Elección de participantes:** dentro de este parámetro se debe realizar la selección del grupo de expertos dentro del campo de interés relacionado con el tema de investigación planteado, de esta manera se garantizará la calidad de los resultados.

- **Formulación de cuestionarios:** para la formulación de preguntas se debe delimitar el problema con exactitud, para obtener resultados precisos y eficaces.
- **Distribución de los cuestionarios:** los cuestionarios deben ser enviados a los expertos junto a una invitación escrita de manera formal; este proceso debe ser anónimo para evitar que los resultados sean alterados y de esta manera mantener la objetividad de las respuestas,
- **Análisis y evaluación de resultados:** se debe realizar varias rondas de los cuestionarios para tratar de tener la misma conclusión de los expertos.
- **Producción de datos y Tabulación de resultados:** En el caso de no llegar al consenso en el primer cuestionario, se debe realizar una tabulación de las respuestas obtenidas en cada ronda de los cuestionarios y de esta manera preparar el nuevo cuestionario que va a ser nuevamente distribuido, identificando la retroalimentación de los expertos en el área investigada.
- **Consenso final:** luego de obtener un consenso de la mayor parte de los expertos, se puede dar por validado el tema de investigación que se ha propuesto.
- **Compilación de las respuestas y presentación de los resultados:** cuando se ha obtenido finalmente un consenso final satisfactorio, se realiza la compilación general de todas las preguntas realizadas en todas las rondas, se interpretan los resultados y se presentan los resultados obtenidos en el estudio Delphi.

3.3.3 Ventajas y Desventajas

En la figura 11 se presentan cuáles son las ventajas y desventajas del método Delphi; sin embargo, se puede demostrar que es un método muy beneficioso debido a la escasez de las desventajas.

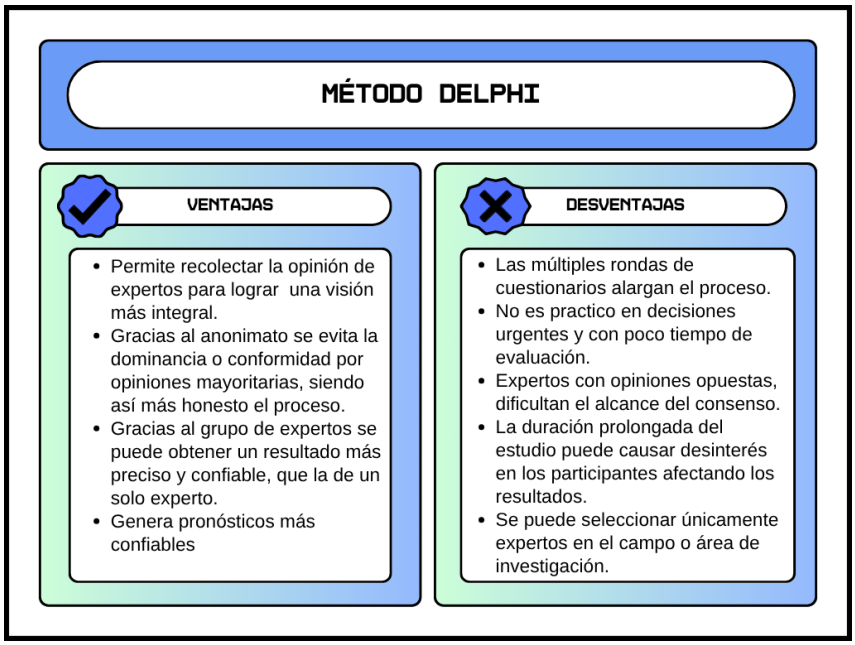


Fig. 11.
Ventajas y desventajas del método Delphi. **Fuente:** Elaboración propia

3.3.4 Características de Delphi

Durante el proceso Delphi existen dos grupos diferentes: el primero, el grupo monitor el cual se encarga de delimitar el tema y tener claro el horizonte de investigación, además de la responsabilidad de seleccionar los expertos que mantengan compromiso y colaboración. El segundo grupo está compuesto por los expertos, los cuales deben contestar a las preguntas planteadas por el primer grupo. Este método presenta las siguientes características importantes [44]:

- **Muestra:** debe estar compuesta por un grupo de expertos cuidadosamente seleccionados.
- **Anonimato:** es necesario que las encuestas sean anónimas, además de que ningún experto puede conocer la identidad de los otros expertos que conforman el grupo de controversia, de esta manera se obtienen resultados más honestos.
- **Moderador:** es el encargado de distribuir los informes o cuestionarios de resultados durante el proceso.
- **Debe ser utilizado para complejos altos:** es decir, debe realizarse cuando el tema es muy interesante y complicado de solucionar.

- **Presupuestos necesarios:** debido a que se requiere de expertos para que validen el tema de investigación, se debe tener en cuenta el presupuesto que se debe cancelar a cada uno por su entrevista e input.
- **Evaluación final:** se debe realizar un informe donde estén presentes los resultados obtenidos y las estrategias brindadas por parte de los expertos.

CAPÍTULO IV
RESULTADOS Y ANÁLISIS

Este capítulo tiene la finalidad de evidenciar los hallazgos obtenidos y la necesidad de la guía metodológica propuesta para la empresa Borealplast.

4.1 Planificación

Para llevar a cabo el desarrollo de la guía metodológica para la implementación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en la empresa Borealplast, se realizó una planificación de 10 meses, en donde se obtuvo una definición clara de los objetivos, cronograma, recursos y metodología de trabajo. El plan de trabajo se realizó en las siguientes fases:

- Diagnóstico inicial y recolección de la información.
- Análisis de las brechas de los datos personales respecto a las normas ISO y la LOPDP.
- Desarrollo de la guía metodológica.
- Validación y corrección de la propuesta realizada.

Estas fases se centraron en un enfoque metodológico que incluye la realización de entrevistas con los stakeholders claves de la empresa, además la comparación de las prácticas actuales referente a la recolección y manejo de datos respecto a la LOPDP e ISO 27001/27701, tienen como fin asegurar que la investigación sea exhaustiva y que los resultados sean aplicables en la empresa Borealplast.

Además, para el proceso de validación se utilizará el método Delphi, debido a que la guía se enviará a profesionales del área de protección de datos o seguridad de la información y que estén relacionados con la LOPDP. Este método permite obtener un consenso sobre nuestro tema de investigación a través de cuestionarios anónimos.

La implementación del método Delphi permite asegurar un consenso sobre la pertinencia, aplicabilidad y tecnicismo de nuestra guía.

4.2 Recolección de información

Para la recolección de la información en la empresa Borealplast, se trabajó con 20 personas aplicando entrevistas, encuestas y registros de observaciones participativas abarcando el 100 % del personal de la empresa. La recolección de la información se realizó de manera anónima y virtual para garantizar la confidencialidad y el anonimato de todos los participantes y así obtener un mayor porcentaje de sinceridad en las respuestas.

Este método permitió identificar el conocimiento real del personal involucrado y la situación actual en la que se encuentra la empresa referente al cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), además de identificar las vulnerabilidades asociadas al software contable y los sistemas biométricos de asistencia. También, se ha recibido la aprobación del Gerente General y Gerente de Recursos Humanos para la recolección de esta información , clarificando el propósito de la recopilación de los datos dentro de la investigación.

Desde un punto de vista legal, el estudio se realizó dentro de las normativas vigentes, como la Ley Orgánica de Protección de Datos Personales, para así garantizar la confiabilidad de la investigación.

4.2.1 Análisis de los problemas hallados

El análisis de los problemas en la empresa se inició con un cuestionario que revelo una clara brecha de conocimiento en el personal, con lo cual se confirmó los problemas planteados inicialmente.

La figura 12, evidencia los resultados obtenidos de la primera pregunta.

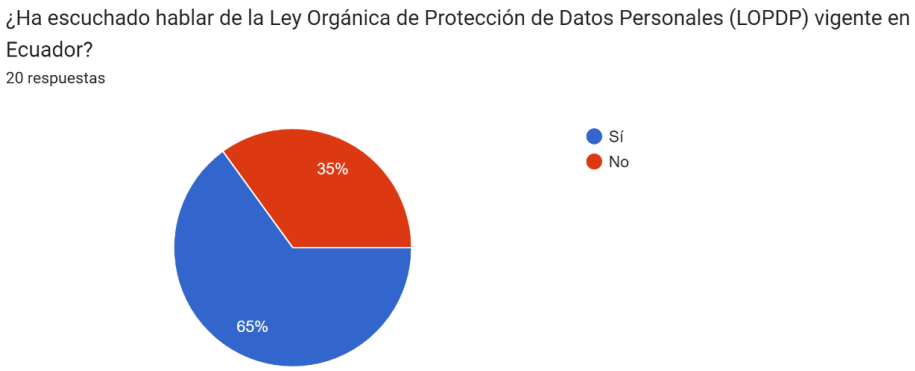


Fig. 12.
Respuestas de la primera pregunta

Según la encuesta realizada, el 65 % de los encuestados conocen o han escuchado sobre la Ley Orgánica de protección de datos personales, mientras que un 35 % no la conoce en absoluto. Por ello, podemos analizar que el mayor porcentaje de los stakeholders, si están informados sobre la LOPDP, y esto representa el riesgo de presentar alguna sanción a la organización al no mantener un correcto manejo respecto a la protección de datos personales.

Fig. 13.
Respuestas de la segunda pregunta

Según la entrevista realizada, se puede visualizar en la figura número 13 que el 60 % de encuestados no conocen el tipo de sanciones que se aplican por faltar a la ley, es decir, se percibe desinformación sobre riesgos legales y financieros a los que está expuesta la empresa.

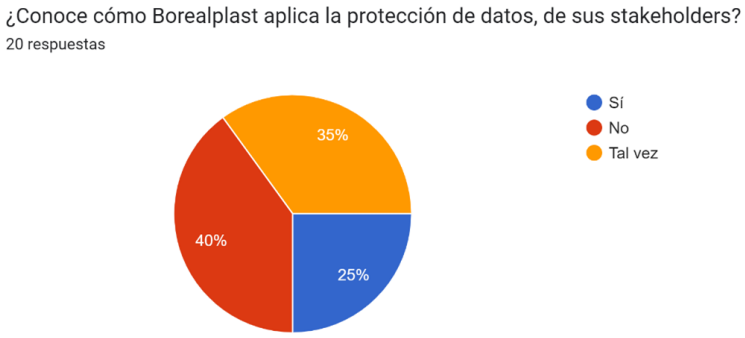


Fig. 14.
Respuestas de la tercera pregunta

Según la figura 14, el conocimiento de los stakeholders clave de la empresa es muy bajo, esto evidencia una falta de comunicación interna sobre las políticas de la empresa.

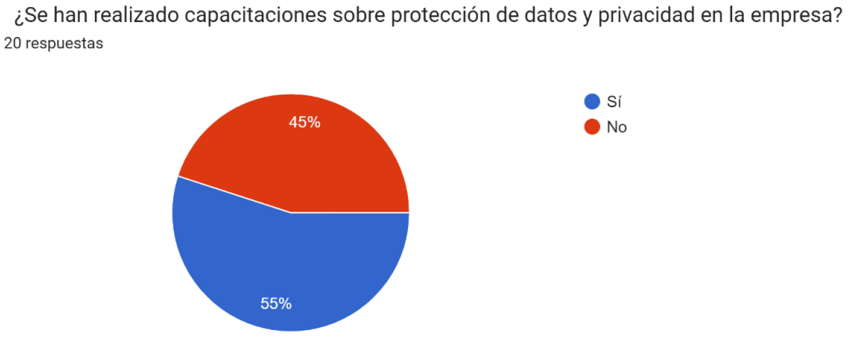


Fig. 15.
Respuestas de la Cuarta pregunta

En la figura 15, se puede evidenciar con un 55 % de los encuestados, que la empresa no ha realizado capacitaciones sobre la protección de datos o privacidad de ellos, representando un signo de alerta para la seguridad de la información de la empresa, ya que existe personal que podría causar un flujo de información al no estar capacitado.

Fig. 16.
Respuestas de la quinta pregunta.

Según la encuesta ejecutada, en la figura 16, se evidencia que solo un 30 % de los encuestados conocen a quién acudir para ejercer sus solicitudes ARCO, mientras que el 45 % no está seguro y el 25 % no lo sabe, esto evidencia una falta de documentación y protocolos dentro de la organización.

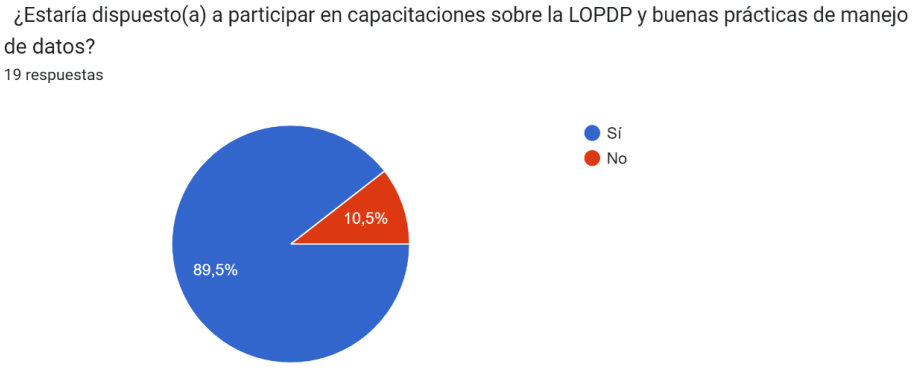


Fig. 17.
Respuestas de la sexta pregunta.

En la figura 17, se evidencia con un 89.5 % que el personal está dispuesto a participar en capacitaciones para garantizar la seguridad de los datos personales.

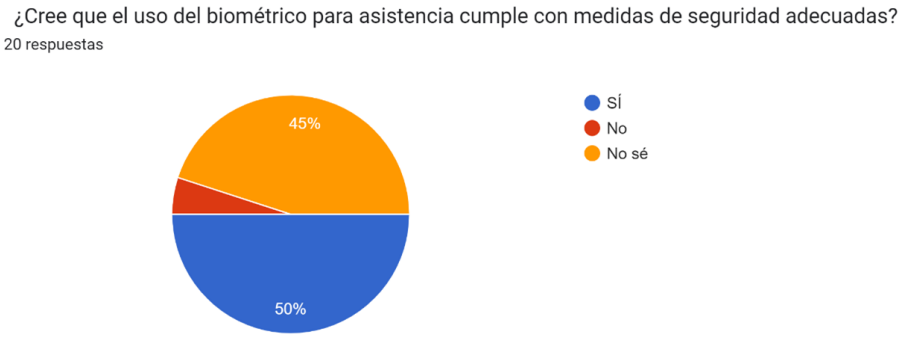


Fig. 18.
Respuestas de la séptima pregunta.

Según la figura 18, se puede determinar que solo el 50 % de los encuestados, tienen la seguridad que los sistemas biométricos están cumpliendo con las medidas de seguridad adecuadas para la protección de datos personales, mientras que en otro 50 %, explican, que no conocen o no saben si el sistema es el correcto.

Fig. 19.
Respuestas de la octava pregunta.

Según la figura 19, con un porcentaje del 100 % de los encuestados, se indica que nunca se ha reportado una pérdida o filtración de la información, esto podría deberse a la falta de conocimiento sobre qué son las brechas de seguridad y a la ausencia de un Delegado de Protección de Datos.

Fig. 20.
Respuestas de la novena pregunta.

En la figura 20, respecto al consentimiento de manejo de datos personales, el 35 % afirma que Borealplast si solicita su consentimiento libre e informado, el cual no es un porcentaje que garantice el cumplimiento de la ley, sin embargo, el 55 % de los encuestados no están seguros si la empresa ha realizado este proceso, mientras que el 10 % afirma que Borealplast no ha realizado este proceso, por ello no se puede concluir que la empresa este cumpliendo con la normativa.

Fig. 21.
Respuestas de la Decima pregunta.

En la figura 21, se puede evidenciar que el 30 % conoce la existencia de políticas referentes al manejo de datos personales, mientras que el otro 30 % desconoce por completo si existen algunas políticas y el 40 % no están seguros sobre la existencia de estas políticas.

Fig. 22.
Respuestas de la Décima primera pregunta.

Según la figura 22, el 70 % de los encuestados, afirman no saber a quién acudir, en caso de que un dato personal este incorrecto o necesite ser actualizado, esto evidencia la falta de protocolos para la gestión de solicitudes ARCO, un principio fundamental dentro de la Ley Orgánica de protección de datos personales, y poniendo en riesgo a la organización debido a que esto puede ser sancionado en caso de una auditoría realizada por la Autoridad de Protección de datos personales de la Superintendencia de protección de datos personales.

De acuerdo con el cuestionario aplicado, se coincide que es necesario la implementación de la Ley Orgánica de protección de datos personales dentro de la empresa Borealplast, ya que los resultados obtenidos evidencian una baja madurez y cultura organizacional en protección de datos. Por ello, se confirma la necesidad urgente de una guía metodológica para la implementación de la LOPDP. Esta propuesta se desarrolla como una solución directa a la falta de procedimientos necesarios para el cumplimiento de la LOPDP y que esté alineada con estándares ISO 27001 e ISO 27701.

4.2.2 Resultados de la fase 1

A continuación, se presentan los distintos hallazgos obtenidos en la organización de acuerdo a la metodología aplicada en las distintas secciones.

Análisis y Diagnóstico

En la tabla 11, se presentan los hallazgos obtenidos en la primera etapa de la fase 1, luego de realizar la entrevista planteada al inicio.

Tabla 11.
RESULTADOS DE LA ENTREVISTA AL GERENTE GENERAL

Método de Recolección	**Hallazgos**
Para la recolección de información en esta etapa se realizó una entrevista directa al Gerente general de la empresa, quien supo responder con sinceridad a las preguntas realizadas durante la entrevista. Esta entrevista permitió identificar las siguientes brechas:	La empresa no presenta políticas internas que garanticen la seguridad y privacidad de los datos personales.
	La empresa no tiene un DPD para el manejo de los datos personales.
	La empresa recolecta datos personales y sensibles de sus stakeholders; sin embargo, no tiene establecido legalmente las finalidades de su recolección
	Las contraseñas de Contífico no han sido actualizadas durante los últimos 3 meses.
	El acceso a Contífico esta segmentado, sin embargo, todo el personal administrativo tiene accesos sin ningún protocolo previo.
	La base de datos generada por el sistema biométrico no se encuentra cifrada.

Método de Recolección	Hallazgos
	La empresa no ha solicitado el consentimiento informado de ninguno de sus stakeholders.
	La empresa no realiza capacitaciones ni evaluaciones de impacto referentes a la LOPDP.
	La empresa desconoce si ha firmado algún acuerdo de confidencialidad con el proveedor de Contífico.
	La empresa desconoce con exactitud las sanciones a las que está expuesta por el incumplimiento de la LOPDP.

Comparación de normativas Borealplast VS LOPDP

Para este proceso se realizó un checklist estructurado y un cuestionario que fue aplicado a un total de 20 trabajadores de la empresa entre personal operativo y administrativos, con la finalidad de verificar el conocimiento respecto a la LOPDP y los derechos ARCO, entre otros aspectos importantes, en la tabla 12 se presenta un resumen de los hallazgos obtenidos en estos procesos.

Tabla 12.

RESULTADOS DE LA ENCUESTA SOBRE CONOCIMIENTO DE LOPDP EN LA EMPRESA

Ítem evaluado	Hallazgos
Conocimiento LOPDP	El 68 % de los encuestados desconocen sobre la LOPDP. El 90 % no sabe o desconoce qué es una brecha de seguridad de la información y desconoce si sus datos han sido vulnerados.
Protección y sanciones LOPDP	El 72 % de los encuestados no saben si la empresa protege sus datos personales y desconocen las sanciones del incumplimiento de la LOPDP.
Capacitaciones	El 60 % de los encuestados están seguros de no haber sido capacitados sobre la LOPDP.
Derechos ARCO	El 65 % de los encuestados no conocen sus derechos ARCO.
Capacitaciones LOPDP	El 91.7 % está dispuesto a participar en capacitaciones de la LOPDP y buenas prácticas.
Consentimiento	Solo el 40 % cree que la empresa ha obtenido su consentimiento para el manejo de los datos personales.
Designación DPD	El 60 % de los trabajadores no sabe a quién acudir en caso de un requerimiento ARCO.

Identificación de riesgos

El análisis de riesgos permite identificar amenazas, vulnerabilidades y posibles impactos sobre los datos personales. En la tabla 13 se presenta el detalle de los riesgos identificados en la organización en base a la LOPDP e ISO 27001:

Tabla 13.
ACTIVIDADES DE ANÁLISIS DE RIESGOS PARA LA PROTECCIÓN DE DATOS PERSONALES

Actividad	Descripción	Referencia
Identificación de activos	Identificación de datos, sistemas y procesos que requieren protección.	ISO 27001 6.1.2
Identificación de amenazas	Ciberataques, accesos indebidos y fallos técnicos.	ISO 27001 6.1.2 / LOPDP - Art.47
Evaluación de vulnerabilidades	Contraseñas débiles, configuraciones inseguras.	ISO 27001 A.12.6.1/ LOPDP Art. 40
Evaluación de impacto	Consecuencias sobre titulares y organización.	LOPDP - Art.42
Plan de tratamiento	Definición de controles técnicos, administrativos y legales.	ISO 27001 6.1.3/ LOPDP Art. 41 y 47

Observación directa

Durante la realización de este proyecto, se realizó un trabajo híbrido, el cual consta de visitas presenciales a la empresa, en la tabla 14 se presentan las brechas identificadas durante estas visitas.

Tabla 14.
RESULTADOS DE LA OBSERVACIÓN DIRECTA EN LA EMPRESA

Observación directa	Hallazgos
Seguridad y privacidad	-Existen cámaras en la empresa que garantizan la seguridad de la empresa, pero no existe un protocolo adecuado para el manejo de las imágenes respecto a la privacidad establecida en la LOPDP.
Manejo de datos personales	-Los trabajadores manejan datos personales de los clientes, sin protocolos establecidos en la LOPDP sobre el manejo de datos, lo cual expone a un flujo de información y a posibles pérdidas de clientes.
Solicitudes ARCO	-No existe un punto establecido para la recaudación de solicitudes ARCO.

Observación directa	Hallazgos
Consentimiento informado	-No existen procesos establecidos para la adquisición de consentimientos informados de los titulares de datos.

4.2.3 Resultados de la fase 2

Plan de mejoras

De acuerdo con los referenciales normativos utilizados (LOPDP, ISO 27001 e ISO 27701), los resultados obtenidos permitieron evaluar el nivel de cumplimiento de los procesos relacionados con el tratamiento de datos personales en Borealplast. El análisis se realizó contrastando la información obtenida mediante observación directa, encuestas, capacitaciones y checklist estructurado con los artículos y controles específicos de cada normativa. La integración de la normativa evidencia que Borealplast requiere:

- Formalizar políticas
- Actualizar controles técnicos
- Mejorar prácticas de seguridad digital
- Documentar el cumplimiento

De esta forma, los resultados de la fase 1 proporcionan insumos esenciales para la elaboración de la guía metodológica de implementación. El plan de mejoras es la integración de decisiones estratégicas sobre los cambios que debe realizar la organización, en la tabla 15 se presenta un plan estructurado de acuerdo a los resultados obtenidos en la primera fase.

Tabla 15.

PLAN DE MEJORA BASADO EN LOPDP E ISO 27001/27701

Norma / Artículo o Control	**Debilidad identificada / Hallazgo**	**Impacto**	**Acción de mejora y salvaguarda propuesta**	**Política sugerida**
LOPDP-Art. 37 / ISO 27001-A.9	Ausencia de controles de acceso físico y lógico; no existe registro formal.	Alto	Implementar controles de acceso por roles, autenticación robusta y registro de accesos.	Política de Control de Acceso Físico y Lógico.
LOPDP- Art.43 / ISO 27001-A.16	No existe procedimiento formal de notificación y respuesta a incidentes.	Alto	Crear protocolo de gestión de incidentes: detección, análisis, contención y notificación.	Política de Gestión y Notificación de Incidentes.
LOPDP-Art.51 / ISO 27701-7.2	No existe registro documentado de actividades de tratamiento.	Medio	Crear y mantener el Registro de Actividades de Tratamiento.	Política de Registro del Tratamiento.
LOPDP-Art. 42 / ISO 27001-6.1.2	No se ha realizado análisis formal de riesgos.	Alto	Aplicar metodología de identificación y tratamiento de riesgos.	Política de Gestión de Riesgos de Seguridad y Privacidad.

Norma / Artículo o Control	Hallazgo / Debilidad identificada	Impacto	Acción de mejora y salvaguarda propuesta	Política sugerida
LOPDP-Art. 5 y Art. 48 / ISO 27701-5.2	Roles de Responsable, Encargado y DPD no definidos.	Medio	Asignar roles y responsabilidades; elaborar descripciones formales.	Política de Gobernanza de Datos Personales.
LOPDP-Art. 25 / ISO 27701-6.2	No existe clasificación de datos personales y sensibles.	Medio	Crear inventario y clasificación de datos según criticidad.	Política de Clasificación y Protección de Datos.
LOPDP Art. 10 / ISO 27001-A.5	Principios de tratamiento no documentados.	Medio	Documentar lineamientos de licitud, finalidad y minimización.	Política de Principios de Tratamiento.
LOPDP-Art. 37 al 42 / ISO 27001-A.12	No existen procedimientos de respaldo ni monitoreo.	Alto	Implementar backups, monitoreo y auditorías.	Política de Seguridad Operativa y Monitoreo.

Diseño de políticas

Se desarrollaron procedimientos para: consentimiento informado, derechos ARCO, gestión de brechas, clasificación de datos, análisis de riesgos, relación con terceros y control de acceso. Cada procedimiento está alineado con las exigencias normativas y con los controles de ISO 27001/27701.

A continuación, en la tabla 16, se presentan los procesos y actividades que debe implementar la empresa Borealplast, los cuales están justificados dentro de la normativa vigente y de los estándares internacionales.

Tabla 16.
PROPUESTA DE POLÍTICAS

Proceso / Actividad	**LOPDP (Art.)**	**ISO 27001**	**ISO 27701**	**Políticas / Procedimientos**	**Evidencia necesaria**
Consentimiento informado	Art. 7, 8, 9	A.5.1	7.3	Política de Privacidad y Consentimiento; Procedimiento para registro del consentimiento	Formatos firmados, registros digitales
Derechos ARCO/ARSD	Art. 12-21	A.18.1	7.4	Procedimiento para Atención de Derechos; Formularios ARCO/ARSD	Registro de solicitudes
Gestión de brechas	Art. 43-46	A.16	6.4	Protocolo de Gestión de Incidentes; Registro de brechas	Matriz de incidentes, reportes internos
Clasificación de datos	Art. 25-26	A.8		Política de Clasificación; Inventario de activos y datos	Inventario y matriz de clasificación

Proceso / Actividad	LOPDP (Art.)	ISO 27001	ISO 27701	Políticas / Procedimientos	Evidencia necesaria
Análisis de riesgos	Art. 47, 42	Cláusula 6.1	8.3	Procedimiento de Evaluación de Riesgos; Matriz de riesgos	Identificación, valoración y tratamiento
Relación con terceros	Art. 33, 34, 35, 36	A.15	8.2	Política de Gestión de Proveedores; Anexos contractuales	Contratos y cláusulas de privacidad
Control de acceso	Art. 37	A.9	6.13	Política de Control de Acceso; Procedimiento de credenciales	Perfiles, roles, bitácoras de acceso

Estructura organizacional

La correcta estructura de una organización garantiza un buen funcionamiento y alineamiento con la normativa vigente, la definición de roles es fundamental para garantizar gobernanza, trazabilidad y responsabilidad en Borealplast. En la tabla 17, se exponen cuáles son los roles que debe presentar la empresa y cuáles son las responsabilidades y alineaciones con la LOPDP e ISO.

Tabla 17.

ROLES Y RESPONSABILIDADES EN EL TRATAMIENTO DE DATOS PERSONALES

Rol	Responsabilidad	LOPDP / ISO
Responsable del Tratamiento	Define finalidades y medios, garantiza derechos ARCO, responde ante la autoridad.	LOPDP Art. 47 / ISO 27701-5.2.1 / ISO 27001-5.3
Encargado del Tratamiento	Procesa datos bajo instrucciones del responsable.	LOPDP Art. 4, 47 / ISO 27701-5.2.3
Delegado de Protección de Datos (DPD)	Asesora, supervisa, gestiona incidentes y actúa como punto de contacto.	LOPDP Art. 48-49 / ISO 27701-6.3.3
Titular	Persona natural cuyos datos se tratan.	LOPDP Art. 4

Diseño de plantilla de protocolos ARCO

Se puede implementar una plantilla para gestionar las distintas solicitudes ARCO, a continuación, se presenta un ejemplo del texto que puede presentar la plantilla.

FORMATO DE SOLICITUD ARCO

Datos del titular

Nombre:

Cédula:

Correo:

Teléfono:

Tipo de solicitud:

☐ Acceso

☐ Rectificación

☐ Cancelación

☐ Oposición

Descripción de la solicitud:

. . . . . .

. . . . . .

. . . . . .

Para brindar atención a esta solicitud se debe añadir la copia de cédula del titular, de acuerdo a lo establecido en la normativa vigente.

4.2.4 Resultados de la fase 3

Desarrollo de políticas de contraseñas

Estas políticas se desarrollan con la finalidad de evitar flujo de información de la empresa, en la tabla 18 se presenta las políticas enfocadas en las contraseñas.

Tabla 18.
PROPUESTAS DE POLÍTICAS PARA SEGURIDAD DE CONTRASEÑAS

Política	Descripción
Robustez	Mínimo 12 caracteres, combinar números, mayúsculas, minúsculas y símbolos.
Caducidad	Las contraseñas deben ser actualizadas periódicamente.
Almacenamiento	Prohibición de anotarlas en lugares visibles o guardarlas en algún archivo sin cifrar.
Protección de Cuentas	Para acceder a información personal, se debe realizar autenticación de múltiples factores (MFA).

Capacitación sobre LOPDP al personal

El cronograma presentado en la tabla 19, se elaboró de acuerdo a las necesidades de la empresa y considerando el presupuesto reducido.

Tabla 19.
CRONOGRAMA DE CAPACITACIONES SOBRE LOPDP

Cronograma	Punto a desarrollar	Descripción
1° Capacitación	Conocimiento	Capacitar al personal sobre ¿Qué es LOPDP?
2° Capacitación	Principios	Presentación sobre los principios de la LOPDP (legalidad, finalidad, lealtad, consentimiento, seguridad, confidencialidad).
3° Capacitación	Buenas Prácticas	Infundir al personal operativo y administrativo sobre las buenas prácticas en el manejo de datos personales.
4° Capacitación	Consentimiento	Capacitación y obtención de la carta de consentimiento informado y finalidades de los datos almacenados.
5° Capacitación	Derechos ARCO	Presentación de los derechos ARCO, establecimiento de canales para atención de solicitudes ARCO.

4.3 Desarrollo de la propuesta

La propuesta consiste en el desarrollo de una guía metodológica para la implementación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en la empresa Borealplast, considerando los estándares internacionales ISO 27001/27701. El desarrollo de esta investigación se fundamenta en los resultados obtenidos en entrevistas y cuestionarios realizados en la empresa, en los cuales se diagnosticó una brecha significativa en el conocimiento y aplicación de la

LOPDP. Este documento se ha estructurado para servir como herramienta práctica y sistemática, abordando los diferentes problemas identificados en la empresa y dando cumplimiento a los objetivos de la investigación. Además, servirá de referencia no solo para Borealplast, sino también para todas las PYMES que deseen implementar la LOPDP, pues servirá como manual para mantenerse dentro del cumplimiento normativo vigente y en la protección de datos personales.

4.3.1 Base legal aplicada

Según la Asamblea General, la protección de datos personales es un derecho fundamental establecido en la Constitución de la República del Ecuador por el Director del Registro Oficial, el Ingeniero Hugo del Pozo Barrezueta, el 11 de mayo de 2021 con oficio número PAN-CLC-2021-0384[8]. En él se esclarecen en los distintos capítulos los derechos, obligaciones, principios, infracciones y demás reglas que garantizan el respaldo de los datos personales de una persona identificada o identificable.

4.3.2 Objetivos de la Guía

Para esta Guía Metodológica se establecieron los siguientes objetivos:

- Garantizar el cumplimiento normativo en todas las actividades.
- Establecer políticas y procedimientos claros para la recolección, almacenamiento y utilización de los datos personales.
- Garantizar que los stakeholders tengan fácil acceso a las solicitudes ARCO.
- Planificar programas de capacitación sobre la protección de datos personales, que garanticen la adopción de mejores prácticas y responsabilidades respecto a la información personal.

Estos objetivos están orientados al cumplimiento de la normativa para evitar sanciones a la empresa. La implementación de la LOPDP no es opcional, es un requisito fundamental para que la organización mantenga un prestigio ante la seguridad de la información.

4.3.3 Explicación del aporte

El aporte de esta guía metodológica radica en fortalecer la protección de datos personales en Borealplast, tanto a nivel interno como externo, mediante un marco normativo alineado con la LOPDP y estándares internacionales ISO 27001/27701. La guía no solo garantiza el cumplimiento legal normativo, sino que también fortalece la confianza institucional dentro del mismo sector empresarial, al mismo tiempo que fortalece la credibilidad ante la sociedad, además fomenta una cultura de privacidad y seguridad de la información, debido a que las organizaciones que promueven la cultura de privacidad y priorizan la protección de datos, se posicionan como entidades más seguras con los clientes, empleados y otros grupos de interés.

Adicionalmente, la adopción de estas medidas permite conocer el procedimiento frente a las solicitudes de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) de los titulares y así mitigar significativamente el riesgo de sanciones económicas y legales derivadas del incumplimiento de la LOPDP, las cuales pueden alcanzar montos sustanciales y afectar la sostenibilidad financiera y reputacional de la organización.

Dentro de una organización existen dos perfiles, los cuales se detallan en el siguiente apartado:

- **Responsable del tratamiento de datos personales:** es la entidad o persona física que se encarga de decidir qué datos son recogidos, para qué, cómo y cuándo, se van a tratar; por ejemplo, en este proyecto, el responsable es la empresa Borealplast.
- **Delegado de protección de datos:** es la persona física designada por el responsable, encargada de supervisar y asesorar el cumplimiento normativo del responsable, sin la potestad de tomar decisiones finales, pero verifica que todo se haga conforme a la ley.

La principal diferencia es el rol y el propósito de cada uno; por ello, se presentan las obligaciones, funciones y perfiles que debe cumplir cada uno de estos.

4.3.4 Derechos ARCO para la empresa

Toda persona identificada o identificable tiene derechos sobre sus datos personales, para la aplicación de estos derechos, debe seguir un protocolo definido, cuya tramitación varía dependiendo del requerimiento. En base a la LOPDP artículos 12-21, los derechos de los titulares son[1]:

- **Acceso:** es el derecho del titular para conocer cuáles son los datos que la empresa ha recolectado de ella.

- **Rectificación:** el objetivo de este derecho es ayudar al titular a corregir, completar o actualizar los datos del titular en caso de ser necesario.
- **Cancelación:** el titular puede solicitar que sus datos sean eliminados cuando ya no sean necesarios dentro de la empresa.
- **Oposición:** el titular puede negarse a la utilización de alguno de sus datos para ciertos fines.

Para ejecutar una potestad de cualquiera de estos derechos, se debe presentar una solicitud con la descripción precisa y clara del derecho a ejercer, juntamente con el nombre del titular, teléfono, correo o algún medio para ser notificado sobre la resolución de su requerimiento.

4.3.5 Destinatarios-Borealplast

La implementación de esta guía está destinada a todos los usuarios, clientes, socios, empleados y, en general, para todos aquellos que presenten interés en el tratamiento de datos personales. Estas pueden ser personas naturales o jurídicas, que pueden solicitar información por medios digitales como WhatsApp o páginas digitales relacionadas con el producto o servicio que brinde la empresa. A continuación, se detalla la utilidad de esta guía metodológica para algunos destinatarios:

Alta gerencia

Este destinatario es crucial, porque está compuesta por el personal clave como el gerente general, gerente comercial, gerente de operaciones y el director financiero quienes tienen la potestad de tomar decisiones que hacen que la empresa se convierta en un responsable o un infractor, además de ser los responsables de aprobar la guía y asignar el presupuesto necesario para la implementación.

Responsable del Tratamiento de Datos Personales

Es la persona natural o jurídica encargada de dar cumplimiento a la Ley Orgánica de Protección de Datos y de establecer normas que debe cumplir el DPD. La guía es el manual para que el responsable identifique cuáles son las acciones que debe realizar para cumplir con la normativa vigente.

Delegado de protección de datos (DPD)

Es el encargado de la protección de los datos, en caso de una auditoría por parte de la autoridad de protección de datos, esta persona debe presentar la documentación necesaria que certifique la correcta protección de la información, esta guía es esencial para el delegado, ya que es su caja de herramientas para la protección de la información, pues en ella se puede identificar los principios, derechos y sanciones referente al manejo de los datos personales, es su manual de instrucciones para dar cumplimiento con la LOPDP sin ninguna complicación.

Clientes, Empleados y demás interesados

Estos son beneficiarios directos de la implementación de esta guía, pues su nivel de satisfacción será alto al saber que están trabajando con una empresa que protege su información y respeta sistemáticamente sus derechos ARCO.

Sin embargo, la protección de nuestros datos personales, no son solo trabajo del área de sistemas o TI de la empresa, es responsabilidad de todos mantener segura nuestra información personal, todos tienen un papel fundamental respecto a la protección de los datos personales, desde el nivel operativo hasta el cargo más alto de la gerencia, puede ayudar para que la empresa cumpla con la ley y evite sanciones.

4.3.6 Bases de datos personales

Las bases de datos serán inscritas en el Registro Nacional de Protección de Datos Personales, en caso de ser necesario.

4.3.7 Finalidades del Tratamiento de datos-Borealplast

Estas finalidades estarán alineadas con la Ley Orgánica de protección de datos personales para garantizar su seguridad, algunos de los principales datos personales recolectados de los stakeholders serán:

Clientes: los datos personales recolectados son el nombre, RUC, teléfono, dirección y correo electrónico. El tratamiento de estos datos será para la gestión comercial, logística, atención al cliente, facturación electrónica, seguimiento de pedidos, logística de entrega y envío de comprobantes.

Por ejemplo, para facturar el pedido de un millar de empaques plásticos para productos de la marca Estrella, un cliente habitual de la empresa Borealplast que fabrica esponjillas, guantes,

estropajos, cloro, entre otros productos, necesitamos su RUC para facturar y la dirección a la cual va a ser enviada el pedido, si no obtenemos estos datos, no se puede cumplir con el contrato de venta.

Empleados: los datos recolectados son teléfono, cédula, correo, historial académico, referencias laborales, seguridad social, así como también datos financieros y familiares.

Para ilustrar, la empresa solicita los datos personales y bancarios a sus empleados para realizar el depósito de su salarios, además de los aportes al IESS y controles de asistencia mediante su sistema biométrico, así como los datos familiares en caso de una emergencia.

Socios: los datos recolectados serán RUC, razón social, teléfono, correo, información bancaria, los cuales serán utilizados para el cumplimiento de obligaciones contractuales, formalizar alianzas estratégicas, gestión de pagos y facturación.

Por ejemplo, cuando se establece una alianza con un socio, son necesarios los datos bancarios de la empresa para realizar el depósito o transferencia y el RUC para la facturación legal.

4.3.8 Medios de comunicación para los Titulares

En la implementación de la Ley Orgánica de Protección de Datos Personales (LOPDP), es sustancial establecer medios de comunicación accesibles y seguros para garantizar la transparencia y confianza con los titulares. Estos medios deben estar orientados para que los titulares puedan ejercer sus derechos y resolver dudas sobre el manejo que está realizando la empresa con sus datos personales.

Clientes

Los datos recolectados de los clientes serán utilizados únicamente para realizar el proceso de compra, entrega y envío de facturas del pedido solicitado, los medios por los cuales podrían ser notificados sobre el manejo de los datos personales de acuerdo con la LOPDP serán, correos, carta de consentimiento informado o un formulario web en la página oficial de la empresa.

A continuación, se detallan los modelos mencionados, los cuales podrían ser empleados por cualquier empresa PYMES, considerando que están desarrollados en un lenguaje claro y sencillo.

CARTA DE CONSENTIMIENTO INFORMADO

Fecha y lugar

En cumplimiento de lo establecido por la Ley Orgánica de Protección de Datos Personales, la empresa Nombre de la empresa, solicita su consentimiento libre , específico e informado para el tratamiento de sus datos personales. Yo, ……, con cédula de ciudadanía ……, por medio de la presente otorgo mi consentimiento para el tratamiento de mis datos personales. Entre los datos recolectados para el tratamiento de acuerdo con la LOPDP son: los datos de identificación, contactos, datos laborales, financieros y en general, todos los datos que deban ser recolectados y que estén contemplados dentro de la Ley Orgánica de Protección de Datos personales, bajo los siguientes términos:

Finalidad del tratamiento de Datos

Los datos deben ser utilizados exclusivamente para fines laborales, prestación de servicios, gestión de clientes o incluso fines comerciales y demás datos, dependiendo del rol que realice el titular, garantizando la confidencialidad y seguridad de la información. El titular tiene acceso a las solicitudes ARCO, pudiendo revocar su consentimiento en cualquier momento, estos procesoS los puede realizar a los siguientes contactos: protecciondedatos@borealplast.com o al Tel.: 099 430 7899 Ofic.: 099 043 8869.

_____

Firma del titular

Nombre: _____

Fecha: _____

Este modelo puede ser acoplado al formato de la empresa deseada, debido a que deja muy claro por qué se solicita el consentimiento, cuales van a ser los datos recolectados y las finalidades que van a tener, manteniéndose conforme a la normativa ecuatoriana, de igual manera presenta el contenido necesario para ser enviado por medio de un correo en caso de solicitar el consentimiento por ese medio, con la diferencia que debe ser firmado digitalmente, no se puede firmar de manera física y luego escanear el documento para ser reenviado por correo, este proceso es considerado ilegal.

¿Cuándo se aplica la carta de consentimiento informado?

La carta de consentimiento debe ser obtenida antes de la recolección, registro o utilización de los datos personales del titular de manera libre e informada, por ejemplo:

- En los empleados debe ser aplicada antes de que empiecen a trabajar.
- En los clientes se debe realizar la aceptación de la utilización de sus datos personales antes de ejecutar su pedido. Un ejemplo puede ser: Delivery o KFC, en sus apps, emite un mensaje de confirmación de utilización de sus datos para continuar con el detalle de su pedido.
- En los socios se debe aplicar antes de realizar cualquier tipo de contrato.

En fin, la carta de consentimiento informado debe ser aplicada antes de almacenar cualquier información personal;de esta manera, se evita el riesgo de sanciones y se aumenta la confianza en el sector empresarial.

Formulario web

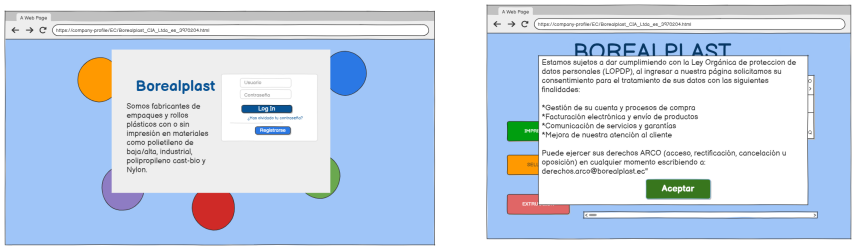


Fig. 23.
Diseño de Formulario web. **Fuente:** Elaboración propia

La figura 23 es un ejemplo práctico de implementación de consentimiento digital, donde la empresa solicita la autorización para el tratamiento de sus datos personales de acuerdo a la Ley Orgánica de protección de datos personales, este ejemplo es claro y preciso debido a que detalla las finalidades, informa sobre el acceso a los derechos ARCO por medio del correo oficial del DPD, culminando con la solicitud de consentimiento obligatorio por medio del botón aceptar, ya que para continuar en la página de la empresa debe estar de acuerdo, caso contrario debe abandonar la navegación en ella, dando a entender si el titular acepta o niega la solicitud.

Para el almacenamiento de esta información, la empresa debe manejar su base de datos interna cifrada, donde almacenada la información de los usuarios que realicen la aceptación o negación del tratamiento de sus datos, también pueden utilizar servicios como AWS CloudTrail o similar

que son sistemas de logs especializados, libre de la herramienta que seleccionen se debe contemplar los requisitos que debe demostrar ante la autoridad, por ejemplo fecha y hora exacta que dio el consentimiento, como se obtuvo la información, la IP e identificación del usuario.

¿Cuándo se aplica el consentimiento digital informado?

El consentimiento informado se debe obtener siempre antes de la recolección de los datos del titular, sin importar si es de manera digital o física, y debe cumplir con los principales requisitos de ser específico, libre e inequívoco. El consentimiento digital se lo debe aplicar en sitios web donde se solicite la información de una persona identificable a la hora de navegar en dicha página, su método de respuesta se genera al seleccionar el botón "Aceptar" o similar, si la persona no selecciona dicho botón, la base de datos no registrara el acceso a la página, ni recolectará ni archivara ninguna información.

Empleados

Al tener un contacto directo con los empleados se puede obtener la carta de consentimiento informado, previo a una capacitación para que sean informados del manejo de sus datos personales y cuál va a ser la finalidad de los datos recolectados. Los ejemplos presentados anteriormente en la sección de clientes pueden ser utilizados para cualquiera de los destinatarios o a la vez se puede encontrar una variedad de ejemplos en internet, ya que no establece la LOPDP un formato exacto para el diseño de estos modelos.

Socios

Para los socios, los canales de comunicación pueden ser directos, a través de la Gerencia y un correo institucional del delegado de protección de datos, de esta manera se garantiza la confianza en el manejo de la información de los socios. También es recomendable que se firme una carta de consentimiento informado del manejo de datos personales.

4.3.9 Recomendaciones basadas en la LOT

Estas recomendaciones se desarrollan de acuerdo con el análisis actual de Borealplast. La LOT establece medidas que existían antes de la entrada de la LOPDP, lo cual también presenta una carencia dentro de la empresa, que puede ser optimizada con las siguientes recomendaciones [7]:

- **Tratamiento de datos:** la LOT exige que las organizaciones mantengan un registro laboral de sus empleados y la LOPDP establece las finalidades del tratamiento de estos datos.

- **Mecanismo de alerta:** se debe implementar un sistema que notifique a los titulares en caso de un flujo de información, esto garantizará el cumplimiento no solo normativo, sino que también construirá la confianza de los stakeholders.
- **Auditorías periódicas:** la empresa debe realizar auditorías para verificar el cumplimiento normativo dentro y fuera de la empresa.
- **Capacitación continua:** se debe mantener en constante capacitación a todos los integrantes de la organización para asegurar la información de los clientes que llega a las manos de sus empleados.
- **Desarrollo de políticas internas:** implementar dentro de la organización políticas que garanticen la protección de la información y mantenerlas actualizadas de acuerdo a la normativa vigente.

4.3.10 Recomendaciones basadas en la LOPDP para Borealplast

La falta de cumplimiento de la Ley Orgánica de protección de Datos Personales puede conllevar a sanciones como la afectación de la reputación de la empresa, multas administrativas e incluso la pérdida de confianza de los socios importantes, clientes y colaboradores. Por ello, se recomienda a las organizaciones, sin importar su tamaño, en este caso particular, la empresa Borealplast, que desarrollen un plan para el cumplimiento de la LOPDP y que este plan sea analizado por expertos para su correcta implementación.

En esta sección se presentan recomendaciones que se han planteado luego del análisis diagnóstico realizado a Borealplast. Estas recomendaciones permitirán no solo cumplir con la LOPDP, también desarrollar un sistema duradero para proteger los datos personales. Dentro de las recomendaciones basadas en la LOPDP y la norma ISO/IEC 27001:2022 tenemos:

Diseño de mecanismo de consentimiento: Este punto es importante, ya que es fundamental obtener el consentimiento de los titulares para el uso de sus datos, este debe ser redactado de forma clara, precisa y debe presentar la finalidad de la recolección de sus datos, de esa manera los titulares no se sentirán forzados a firmar el documento, en el apartado de medios de comunicación sección clientes, se presenta los modelos para la obtención del consentimiento explícito para el manejo de los datos personales.

Establecimiento de un canal de atención a derechos ARCO: Es recomendable habilitar uno o varios canales formales para que los titulares de los datos personales puedan solicitar los derechos de acceso, rectificación, eliminación, oposición y portabilidad, con plazos de respuesta definidos. Por ejemplo, los canales de atención serían:

- Para los clientes o empleados que manejan la modalidad online se pondrá a disposición el correo empresarial del DPD, protectordedatos@borealplast.com o a los teléfonos específicos nnnnnn ext. 2 para el DPD. Este correo debe ser revisado diariamente por el responsable y resolver los requerimientos en el tiempo establecido por la ley.
- Para quienes manejen la modalidad presencial, se pondrá a disposición un formulario en la recepción de información de la empresa o en un punto de atención de solicitudes de datos personales.

Es recomendable que la información sobre el manejo de la LOPDP (formulario de consentimiento de manejo de datos personales), este disponible en la página web oficial, para que de esta manera tengan acceso cualquier persona interesada en recibir información sobre los servicios o productos que brinda la empresa.

Designación de un Delegado de Protección de Datos (DPO): Se debe nombrar un encargado para supervisar el cumplimiento normativo, verificar problemas de seguridad, crear un software en caso de ser necesario y mantener un contacto directo con la autoridad de control.

Procedimiento de notificación de brechas de seguridad

Es fundamental implementar protocolos para la detección, el análisis y la notificación de amenazas latentes o accesos no permitidos hacia los sistemas de datos personales y comunicar de manera inmediata a quienes corresponda. Esta notificación se la debe hacer por medio de los canales establecidos por la empresa. Para realizar este proceso es importante tener en cuenta los siguientes aspectos:

- No intentar resolver el problema.
- Identificar, dónde, cómo y cuándo fue robada la información
- Qué datos fueron afectados.?
- Quién fue el afectado

La notificación inmediata es clave para minimizar el impacto del incidente y limitar la cantidad de datos comprometidos

Capacitación continua del personal: Es importante que el personal sea capacitado en temas referentes a la privacidad, confidencialidad y protección de sus datos personales, ya que hoy en día el manejo de herramientas tecnológicas se da fuera y dentro de una empresa. Para el cumplimiento de este requerimiento, se deben realizar capacitaciones continuas al personal de la empresa sobre qué son y cuáles son los datos personales que no deben ser compartidos, el objetivo principal de esta acción es capacitar al personal sobre cómo deben actuar cuando alguien solicite su información personal.

En el apartado siguiente se especifica una posible capacitación que puede ser utilizada por la organización.

4.3.11 Componente de Formación y Capacitación

Esta fase aborda la capacitación para los integrantes de la empresa Borealplast, debido a que un 60 % de los empleados reconoce no haber recibido capacitaciones sobre la protección de datos personales, es decir no tienen conocimiento ni formación sobre la privacidad de la información, estos detalles fueron obtenidos gracias a la encuesta realizada en la etapa de diagnóstico de la empresa (fase 1), evidenciado en la tabla 12, el proceso de capacitación al personal es un componente crucial para el éxito de la guía. Algunas de las recomendaciones para la formación y capacitación del personal ya fueron presentadas en la tabla 19. Sin embargo, se puede estimar añadir las siguientes consideraciones:

- Programas de capacitación con contenido sencillo y relevante de la LOPDP.
- Materiales didácticos como trípticos, guias, afiches de fácil visualización dentro de la empresa, carteles con información para el correcto manejo de los datos personales.
- Talleres trimestrales sobre privacidad y ciberseguridad básica.

Cronograma de capacitaciones al personal de Borealplast

En la figura 24, se presenta el cronograma asignado para las capacitaciones del personal general y personal de oficina de la empresa Borealplast

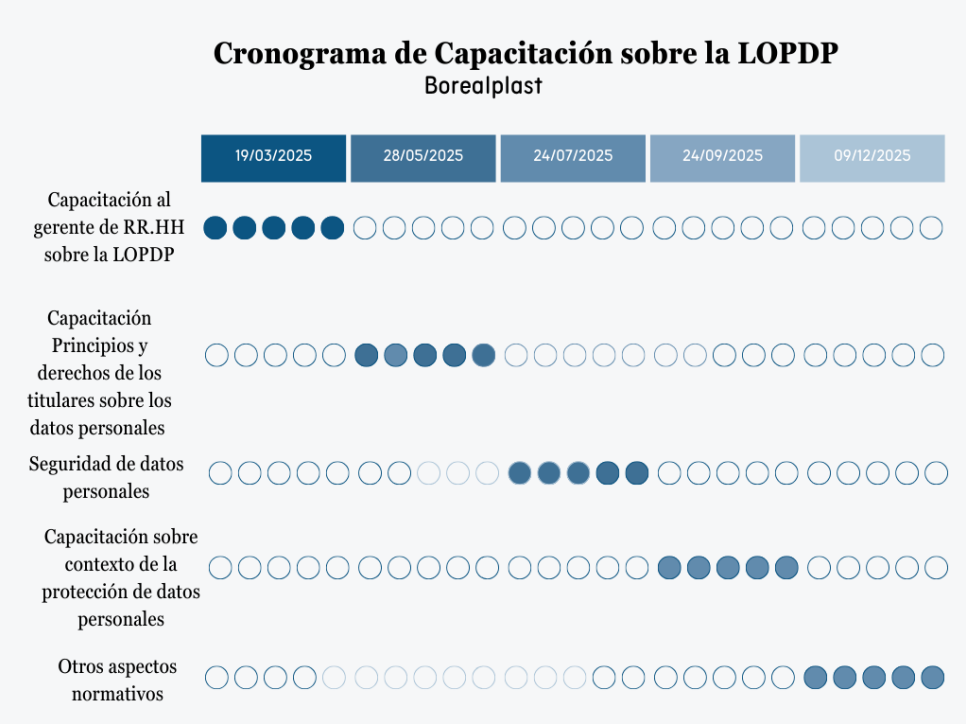


Fig. 24.
Cronograma de Capacitación para Borealplast sobre la Protección de Datos Personales basado en la Ley Orgánica de Protección de Datos (LOPDP). **Fuente:** Elaboración propia

Este cronograma puede ser adaptado por cualquier empresa, ya que sus fechas pueden ser modificables de acuerdo con la necesidad de cada organización.

4.3.12 Recomendaciones basadas en la norma ISO 27001:2022

La implementación de una guía con estándares internacionales como la norma ISO/IEC 27001:2022 permitirá a Borealplast mitigar riesgos asociados a la protección de datos. A continuación, se detallan algunas recomendaciones relacionadas con la norma ISO/IEC 27001:2022.

- **Cláusula 6.1.2. Análisis de riesgos de seguridad de la información:** Identificar puntos críticos y evaluar las amenazas y vulnerabilidades que pueden estar asociadas con el flujo de la información, incluyendo el sistema contable Contífico, bases de datos, correos y sistemas biométricos[45].

- **Anexo A. Gestión de controles de acceso:** Este proceso ayuda a mantener un control de acceso estricto hacia la información, es decir, solo la persona que maneja la información puede acceder a ella solamente si es estrictamente necesario[46].

- **Cláusula 9.2. Auditorías internas de seguridad:** Es indispensable realizar auditorías recurrentes para verificar la administración adecuada de la información y la correcta implementación de la LOPDP y la SGSI, identificando brechas y oportunidades para mejorar los sistemas[47].

- **Anexo 8.13. Respaldo y recuperación de datos:** Realizar procedimientos seguros de respaldo de la información crítica, asegurando la integridad y la disponibilidad de los datos.

- **Cláusula 10.1. Mejora continua:** Para asegurar la eficiencia, el sistema no debe ser estático, debe ser dinámico y actualizado de manera constante, de acuerdo con las revisiones, indicadores o correcciones ante cualquier falla[48].

4.4 Implementación de la Guía

El desarrollo de esta guía se la realizó en base a las guías oficiales estructuradas en la Superintendencia de Datos Personales.

Paso 1. Designación formal del Delegado de Protección de Datos El gerente general de Borealplast debe nombrar formalmente al profesional (abogado o ingeniero en sistemas o TI) que supervisará el cumplimiento de la Ley Orgánica de Protección de Datos Personales, se debe garantizar que el DPD cuente con el perfil adecuado y firmar un acta de designación. El acta para este paso, puede ser la misma que se sugirió en el apartado de Acta de designación de DPD.

Paso 2. Registro del DPD ante la Superintendencia de Protección de Datos (SPDP) La empresa debe realizar obligatoriamente el registro del DPD designado siguiendo los siguientes pasos:

- Recolección de la información del delegado: copia de cédula, acta de designación formal y hoja de vida.

- Completar formulario: Completar el formulario de registro, este formulario ya se encuentra disponible en los medios oficiales de SPDP.

- Seguimiento del proceso: realizar seguimiento al proceso hasta recibir la confirmación del registro y formalizar su posición como enlace oficial de la empresa.

- Archivar constancia de registro

Paso 3. Firma de acuerdo de confidencialidad

El responsable de la empresa debe extender un acuerdo de confidencialidad al DPD, claro, preciso y conciso para garantizar la protección total de la información de la empresa.

Paso 4. Levantamiento de la Información

El DPD debe realizar un inventario de bases de datos y documentar todos los flujos de información en la empresa. Además, debe documentar los hallazgos del tratamiento de datos. Se recomiendan las siguientes acciones específicas:

1. Realizar inventario completo de las bases de datos:

- Datos de clientes
- Datos de empleados
- Datos de socios

2.Identificar para cada flujo:

- Tipos de datos recolectados
- Finalidades del tratamiento
- Medios de recolección
- Terceros con quienes se comparten
- Plazos de conservación

3. Utilizar matriz de inventario (Excel o software especializado)

4. Documentar hallazgos en Registro de Actividades de Tratamiento

Paso 5. Concienciación y Capacitación Inicial

El DPD debe realizar un programa de capacitaciones con el fin de sensibilizar al personal administrativo sobre las buenas prácticas y la LOPDP. Además, debe informar sobre los mecanismos de consentimiento y derechos para los titulares.

Es importante que el personal sea capacitado en temas referentes a la privacidad, confidencialidad y protección de sus datos personales, ya que hoy en día el manejo de herramientas tecnológicas se da fuera y dentro de una empresa. Para el cumplimiento de este requerimiento se deben realizar capacitaciones continuas al personal de la empresa, sobre qué son, y cuáles son los datos

personales que no deben ser compartidos?, el objetivo principal de esta acción es capacitar al personal sobre cómo deben actuar cuando alguien solicite su información personal.

En el apartado,Componente de Formación y Capacitación, se especifica una posible capacitación que puede ser utilizada por la organización para las capacitaciones del personal administrativo y personal operativo de la empresa Borealplast.

Paso 6. Implementación de mecanismos de consentimiento: Se debe obtener el consentimiento libre, informado, específico e inequívoco de los titulares; los medios para obtener este consentimiento son: correos, carta de consentimiento informado o un formulario web en la página oficial de la empresa. En el apartado de medios de comunicación mencionado anteriormente se presentó, en detalle cuales son los medios para implementar estos mecanismos.

Paso 7. Establecer canales para derechos ARCO

Se debe crear uno o varios canales formales para que los titulares de los datos personales puedan solicitar los derechos de acceso, rectificación, eliminación, oposición y portabilidad, con plazos de respuesta definidos.

Por ejemplo, los canales de atención seria: Para los clientes o empleados que manejan la modalidad online se pondrá a disposición el correo empresarial del DPD, protectordedatos@borealplast.com o a los teléfonos específicos nnnnnn ext. 2 para el DPD. Este correo debe ser revisado diariamente por el responsable y resolver los requerimientos en el tiempo establecido por la ley. También se debe implementar un punto de atención de derechos ARCO en la empresa debido a las personas que se encuentren seguidas dentro de la empresa y deseen recibir información personalmente.

Paso 8. Establecer políticas

Se deben establecer políticas de tecnologías de la información y seguridad de la información, estas políticas deben ser redactadas de acuerdo a la normativa vigente para garantizar los controles de seguridad; sin embargo, estas políticas deben ser aptas para la adopción por parte de la empresa.

Políticas sugeridas:

- Las contraseñas de los softwares deben ser actualizadas periódicamente
- Las contraseñas no deben estar autoguardadas
- Configurar sistemas de monitoreo y detección de incidentes

- Realizar cifrado en la información sensible.
- Establecer políticas de Conservación y Eliminación de Datos
- Verificación de la identidad del titular (antecedentes penales, registro civil).
- Realizar auditorías internas para verificar el cumplimiento normativo.
- Revisar y actualizar las políticas anualmente o cuando cambie la ley.
- Realizar el proceso de protección de datos del catálogo de clientes.
- Verificar que la información obtenida por el biométrico esté cifrada.
- Verificar el acuerdo de manejo de protección de datos personales de la empresa Borealplast con el software contable Contífico.

Paso 9. Formación Continua del DPD

El Delegado de protección de datos debe mantenerse en constante capacitación debido a la evolución constante normativa que existe, tanto en la LOPDP como en la SPDP, para de este modo garantizar el cumplimiento normativo de manera actualizada.

A continuación, en la tabla 20 se presentan las estrategias de formación para el DPD con una inversión razonable, tomando como ejemplo una organización PyME.

Tabla 20.

ESTRATEGIAS DE CAPACITACIÓN CONTINUA PARA EL DPD EN EMPRESAS PYMES.

Estrategia	Ejemplos/Recursos	Frecuencia	Costo
Autoformación Guiada	▪ Cursos gratuitos de firmas legales y protección de datos asociados a la Superintendencia de Datos. ▪ Leer sentencias y resoluciones de la autoridad de control.	Trimestral	Bajo
Redes de Contacto e Intercambio	▪ Unirse a grupos oficiales como LinkedIn sobre la protección de datos. ▪ Contactar a DPDs de otras PYMES para compartir experiencias y mejores prácticas.	Trimestral	Bajo/Gratuito
Cursos Online Específicos	▪ Cursos cortos y accesibles en plataformas especializadas. ▪ Cursos de la IAPP (International Association of Privacy Professionals).	Anual	Medio
Eventos y Conferencias	▪ Asistir a al menos una conferencia o seminario nacional al año sobre privacidad y seguridad. ▪ Participar en foros o charlas locales de la Cámara de Comercio o universidades.	Anual	Medio
Certificaciones Formales (Largo plazo)	▪ Obtener una certificación reconocida (p.ej.: Certified Information Privacy Manager - CIPM de IAPP). Esto da un alto nivel de credibilidad.	Cada 2-3 años	Alto

4.5 Validación de la Guía

La validación de la guía metodológica es una etapa determinante para garantizar la eficacia, pertinencia y aplicabilidad en el marco operativo de Borealplast. El principal objetivo de esta fase es verificar que las políticas y controles estén alineados correctamente con la Ley Orgánica de Protección de Datos Personales (LOPDP).

Para la validación descrita se ha seleccionado a especialistas que tengan conocimientos sobre el tema abordado y experiencia en seguridad de la información, además de presentar interés en la participación de esta evaluación. En la tabla 21 se presenta a detalle la información de los expertos seleccionados para la validación de la guía.

La validación de la guía consiste en analizar el contenido y determinar si es precisa, práctica y escalable. Esta validación la realizarán los expertos mencionados en la tabla 21 .

Cada experto validó la guía mediante la escala del Likert de 5 puntos, de acuerdo a las seis dimensiones que presentó la rúbrica estructurada, las dimensiones evaluadas fueron:

Tabla 21.
DATOS DE EXPERTOS SELECCIONADOS

Nombre o Alias	Formación Académica/ Experiencia	Años de experiencia	Cargo
Wilson Xavier Brito	MsC. Experto en Seguridad Informática/ Sistemas	20	Experto
Jhonatan Domínguez	MsC. Experto en Seguridad Informática.	5	Experto
Nely Chacha	Delegada de protección de datos, Frametech S.a.	4	Experto
Evelyn Alexandra Paredes	Lic. Experta en Ciencias Informáticas/ Ciencias de Datos	6	Analista
Jorge Valdivieso	Ing. Experto en seguridad industrial	16	Experto
María Luisa Ochoa	Ing. Socia Borealplast.	16	Analista

A. Contenido legal y normativo Valoración Provisional: 4/5

Comentario: La guía presenta los principios y obligaciones establecidos en la Ley Orgánica de Protección de Datos Personales vigentes en Ecuador, la normativa presentada está actualizada y es pertinente para las operaciones de la empresa. El procedimiento adecuado para la implementación de los derechos ARCO está presentado de forma sencilla, clara y práctica, lo que facilita su aplicación en entornos con bajos conocimientos normativos y tecnológicos.

B. Estructura y claridad Valoración Provisional: 4.5/5

Comentario: La estructura de la Guía es práctica y escalable; el lenguaje empleado es sencillo, claro y accesible para el personal operativo de la empresa, el cual no es profesional en protección de datos; los ejemplos ilustrados en la guía son casos prácticos y adaptables a organizaciones que comparten el mismo sector empresarial.

C. Aplicabilidad y viabilidad Valoración Provisional: 4.6/5

Comentario: El cronograma de actividades propuesto es viable para el desarrollo dentro de la organización y está alineado correctamente con los objetivos iniciales de la guía, las recomendaciones son técnicas y proporcionales al riesgo, y las responsabilidades y roles recomendados están bien definidos, sin embargo, se menciona especificar los plazos de ejecución.

D. Herramientas y formatos Valoración Provisional: 4/5

Comentario: Los formatos presentados, como la carta de consentimiento informado, consentimiento digital y acta de designación, están estructurados para su uso inmediato. Sin embargo,

sería aconsejable una retroalimentación respecto a los consentimientos digitales. Los criterios y métricas de verificación son precisos y medibles, facilitando el cumplimiento de los objetivos referentes a la protección de datos.

E. Formación y cultura organizacional Valoración Provisional: 4/5

Comentario: La guía presenta un cronograma de capacitación no solo para informar sobre la Ley Orgánica de protección de datos personales, también presenta capacitaciones estratégicas para sensibilizar al personal sobre la protección de sus datos personales y datos sensibles. Las actividades de mantenimiento y continuidad son factibles y bien estructuradas. Sin embargo, se recomienda que la empresa incluya material didáctico visual dentro de la empresa como apoyo para que los empleados, clientes y socios se sientan informados y seguros dentro de la empresa, generando así una experiencia enriquecedora al concientizar sobre la protección de los datos.

F. Impacto y recomendaciones generales Valoración Provisional: 4.6/5

Comentario: Los expertos reconocen que la guía contribuye a la reducción del riesgo legal y operativo en las organizaciones pequeñas y medianas. Además, recomiendan que su implementación se realice de manera paulatina para que no ocasionen un impacto económico negativo dentro de la organización, debido a la complejidad operativa que conlleva.

4.5.1 Recomendaciones finales de los expertos

Fortalecer la información sobre la gestión de incidentes: Debe considerar ampliar la información referente a la gestión de brechas de seguridad, incluir un modelo de notificación a la autoridad y detallar los protocolos de comunicación que existen entre el DPD y el titular de los datos.

Actualización periódica de la guía: Debido a que las leyes se mantienen en constantes actualizaciones, la guía debe establecer un mecanismo de actualización para incorporar futuras reformas de la LOPDP.

Elaboración de guía para autoevaluación empresarial: Es recomendable incorporar un checklist empresarial que permita a las organizaciones verificar el nivel de cumplimiento normativo.

Formatos editables: Es recomendable proporcionar los formatos de consentimiento informado en versión digital editable, para brindar ayuda a las organizaciones al agilizar la implementación de la LOPDP.

4.5.2 Consenso final

El instrumento utilizado para el proceso de validación se presenta en el anexo 4.5.3.

Como se estableció previamente, la validación de esta guía se realizó en tres rondas con dos etapas cada una. La primera etapa contempla la validación por parte de los expertos Wilson Brito, Jonathan Domínguez, Nelly Chacha y Evelyn Paredes y la segunda etapa contempla la validación dentro de la empresa, realizada por los ingenieros Jorge Valdivieso y María Luisa Ochoa, los resultados obtenidos durante este proceso se evidencian en la tabla 22 que se presentan a continuación:

Tabla 22.
RESUMEN DE CONSENSOS DE EXPERTOS

Nº Ronda	**Nº Expertos**	**Sumatoria todos los valores**	**Promedio**
1er	6	$68 + 78 + 54 + 60 + 56 + 48$	60.66 %
2da	6	$72 + 80 + 57 + 62 + 60 + 54$	64.17 %
3ra	6	$81 + 86 + 90 + 90 + 93 + 93$	89.88 %

4.5.3 Proceso de análisis- Tercera ronda.

En esta sección se analizan los resultados obtenidos por los expertos en la tercera y última ronda.

Resultados de los 4 expertos:

$$\text{PROMEDIO} = \frac{81 + 86 + 90 + 90}{4}$$

$$\text{PROMEDIO} = 86{,}75\,\%$$

Resultados de la validación dentro de la empresa:

$$\text{PROMEDIO} = \frac{93 + 93}{2}$$

$$\text{PROMEDIO} = 93\,\%$$

Promedio final:

$$\text{PROMEDIO} = \frac{93 + 86{,}75}{2}$$

$$\text{PROMEDIO} = 89,88\,\%$$

De acuerdo con los parámetros de aprobación establecidos en la matriz de validación, al obtener un 89.88 %, de promedio final, la propuesta se encuentra aprobada con correcciones menores, superando ampliamente el 80 % requerido para su aprobación.

CONCLUSIONES

- El diagnóstico realizado evidenció la ausencia de políticas internas, accesos no segmentados en la empresa, ausencia de roles definidos, falta de procesos formalizados, como la obtención del consentimiento informado, y la falta de cifrado en la base de datos, lo que genera riesgos legales y operativos para Borealplast. Este análisis se fundamentó en la norma ISO 27001, cláusulas 4 (Contexto de la organización), cláusula 5 (Liderazgo), cláusula 6 (Planificación y análisis de riesgos) y anexo A (Controles de seguridad), tablas 11,12,13,14 de la fase 1 y Anexo 33.

- Se desarrolló una guía metodológica aplicable y robusta incorporada con criterios técnicos de la norma ISO 27001, A.9 para los controles de acceso y A.10 para proteger la confidencialidad e integridad de la información. Asimismo, se integraron los criterios legales y de gobernanza de la LOPDP e ISO 27701, cláusula 5.2 para la definición de roles (responsable y encargado) y cláusula 7 para la evaluación de riesgos de privacidad. Además, se establecieron procedimientos para gestionar las solicitudes ARCO, priorizando riesgos y proponiendo medidas correctivas adaptadas al contexto operativo y financiero de la organización.

- La guía metodológica fue validada mediante el método Delphi con expertos en seguridad y protección de la información, así como la aprobación de la alta gerencia de la empresa, quienes confirmaron la aplicabilidad, pertinencia y efectividad de la guía. El consenso final obtenido fue del 89.88 % de aprobación, evidenciado en la tabla 22 y la sección de análisis de resultados de la tercera ronda, demostrando que la guía final es una herramienta viable, escalable y práctica para la implementación en Borealplast, debido a que no afecta su operatividad diaria.

- Esta investigación es un aporte representativo, no solo para Borealplast, sino que también puede ser utilizada por otras PYMES ecuatorianas que necesiten adecuarse a la LOPDP. Además, demuestra la relevancia al incorporar estándares internacionales como las normas ISO 27001/27701 y así generar confianza en los clientes, empleados y demás involucrados en la organización.

RECOMENDACIONES

- Es recomendable que la empresa Borealplast implemente de forma inmediata las políticas internas referentes a la protección de datos, protocolos para gestionar las solicitudes ARCO y segmentación de accesos. Además, debe definir roles del tratamiento según la ISO 27701, sección 5.2, y el artículo 48 de la LOPDP, para referir la asignación del Delegado de Protección de Datos.

- Es recomendable que la empresa Borealplast, para materializar el contenido de la guía, nombre formalmente un responsable de tratamiento de datos (RTDP), para que realice la designación de un Delegado de protección de Datos (DPD) establecido en el artículo 48 de la LOPDP, asignando obligaciones paralelas a la ISO 27001, priorizando la gestión de accesos (A.9) y el cifrado de datos (A.10).

- A partir de las conclusiones obtenidas, es recomendable que la empresa mantenga un cronograma de revisión y actualización de la guía metodológica, considerando los avances tecnológicos y las futuras reformas de la LOPDP. Además, debe incluir auditorías internas para verificar el cumplimiento normativo.

- Asimismo recomiendo implementar de manera inmediata la capacitación al personal general de la empresa, dando mayor importancia al área de manejo de datos sensibles como lo son las áreas de Contabilidad y RR.HH. Además, se debe planificar capacitaciones periódicas sobre buenas prácticas de privacidad, ciberseguridad, gestión de incidentes, solicitudes ARCO y el cumplimiento normativo.

BIBLIOGRAFÍA

[1] Asamblea Nacional del Ecuador, *Ley Orgánica de Protección de Datos Personales*, https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf, mayo de 2021.

[2] Ministerio de Telecomunicaciones y de la Sociedad de la Información, *Resumen Ejecutivo: Ley Orgánica de Protección de Datos Personales*, https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/Resumen.pdf, Accedido el: [13/05/2024], nov. de 2023.

[3] J. A. V. Cordero, «Las normas ISO/IEC como mecanismos de responsabilidad proactiva en el Reglamento General de Protección de Datos,» *IDP. Revista de Internet, Derecho y Política*, n.º 33, 23 de jul. de 2021, Number: 33 Publisher: Universitat Oberta de Catalunya, issn: 1699-8154. doi: 10.7238/idp.v0i33.376366. dirección: https://raco.cat/index.php/IDP/article/view/n33-viguri (visitado 28-06-2025).

[4] «Protección de Datos Personales,» Municipio de Quito. (), dirección: https://www.quito.gob.ec/?page_id=10025 (visitado 26-06-2025).

[5] «Ley de Protección de Datos Personales – Dirección Nacional de Registros Públicos.» (), dirección: https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/ (visitado 10-07-2025).

[6] «Una vez aprobada, las empresas públicas y privadas deben empezar a aplicar la Ley de Protección de Datos Personales,» Dirección Nacional de Registros Públicos. (3 de jun. de 2021), dirección: https://www.registrospublicos.gob.ec/una-vez-aprobada-las-empresas-publicas-y-privadas-deben-empezar-a-aplicar-la-ley-de-proteccion-de-datos-personales/ (visitado 27-06-2025).

[7] J. B. Yunganaula Yunganaula, «PROPUESTA DE UN PLAN DE IMPLEMENTACIÓN PARA EL CUMPLIMIENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN LA EMPRESA CABLETEL,» 2024, Publisher: Universidad Católica de Cuenca. dirección: https://dspace.ucacue.edu.ec/handle/ucacue/16705 (visitado 27-06-2025).

[8] H. D. P. Barrezueta, «DIRECTOR DEL REGISTRO OFICIAL,»

[9] K. J. O. Quiroz y G. L. S. Oña, «DESARROLLO DE UNA ONTOLOGÍA QUE ABARQUE EL ÁMBITO DE RECOLECCIÓN Y PROCESAMIENTO DE INFORMACIÓN PERSONAL EN BASE A LO ESTABLECIDO EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES,»

[10] NQA, *Guía de Implementación de ISO/IEC 27701:2019*, Primera, Guía práctica para la implementación del Sistema de Gestión de Información de Privacidad (PIMS) basado en ISO/IEC 27701:2019, NQA, Reino Unido, 2023. dirección: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%5C%20QRFs%5C%20and%5C%20PDFs/NQA-ISO-27701-Mini-Implementation-Guide-ES.pdf (visitado 15-01-2024).

[11] Universidad César Vallejo, L. S. Rodriguez Baca, C. F. Cruzado Puente De La Vega et al., «Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana,» *Propósitos y Representaciones*, vol. 8, n.º 3, 2020, issn: 23077999, 23104635. doi: 10.20511/pyr2020.v8nSPE3.786. dirección: https://revistas.usil.edu.pe/index.php/pyr/article/view/786 (visitado 28-06-2025).

[12] A. E. B. Rivera y L. A. T. Rios, «DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN NORMA ISO 27001:2022 EN EMPRESA SAN SERVICES S. de R. L.,»

[13] J. M. L. Ardila y L. Y. M. Gamez, «METODOLOGIA PARA EL DIAGNOSTICO Y CUMPLIMIENTO DE LA NORMA ISO 27001:2022,»

[14] E. Lachaud, «ISO/IEC 27701 standard: Threats and opportunities for GDPR certification,» *European Data Protection Law Review*, vol. 6, n.º 2, págs. 194-210, 2020, issn: 23642831, 2364284X. doi: 10.21552/edpl/2020/2/7. dirección: https://papers.ssrn.com/abstract=3521250 (visitado 28-06-2025).

[15] A. P. Roca, «El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado,» *Revista de Derecho Político*, n.º 108, págs. 165-194, 4 de ago. de 2020, Number: 108, issn: 2174-5625. doi: 10.5944/rdp.108.2020.27998. dirección: https://revistas.uned.es/index.php/derechopolitico/article/view/27998 (visitado 28-06-2025).

[16] Asamblea Nacional del Ecuador, *Ley Orgánica de Telecomunicaciones*, https://identidadradiocultural.com.ec/transparencia/normativa/LeyOrganicaDeTelecomunicacionesLOT.pdf, Accedido el: [19/04/2025], 2015.

[17] F. U. Cuevas Cely, «Diagnóstico de la implementación de los controles del anexo A de la norma ISO/IEC 27001 acorde a la política de seguridad de la información de la Corporación de Especialistas del Dolor,» Tesis de especialización, Fundación Universitaria Los Libertadores, Bogotá, Colombia, 2021. dirección: https://repository.libertadores.edu.co/server/api/core/bitstreams/99fde922-620c-44d1-b210-d8552383e143/content.

[18] N. Lefkovitz y K. Boeckl, «Spanish Translation of the NIST Privacy Framework Version 1.0,» National Institute of Standards y Technology, Gaithersburg, MD, 1 de sep. de 2021. doi: 10.6028/nist.cswp.01162020es. dirección: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020es.pdf (visitado 17-07-2025).

[19] «Anexo 10.» (), dirección: https://www.iso27000.es/iso27002_10.html (visitado 26-11-2025).

[20] A. B. Ardila, A. N. López y S. L. D. Losada, «Sistemas de vigilancia y su efecto en el derecho a la intimidad desde el discurso de la seguridadEn la actualidad, existen sistemas de vigilancia, como las herramientas de reconocimiento facial, que justifican su existencia en la noción de seguridad perso,» *Revista Latinoamericana de Derechos Humanos*, vol. 33, n.º 1, págs. 33-51, 2022, Number: 1, issn: 2215-4221. doi: 10.15359/rldh.33-1.2. dirección: https://www.revistas.una.ac.cr/index.php/derechoshumanos/article/view/16388 (visitado 28-06-2025).

[21] Berroa Hiciano, Román Arturo, *CONFIGURACIÓN JURÍDICA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE LOS DATOS PERSONALES EN REPÚBLICA DOMINICANA. ESPECIAL REFERENCIA A LA TUTELA DE LOS DATOS EN EL ÁMBITO DE LAS SOCIEDADES DE INFORMACIÓN CREDITICIA.* Accedido el: [25/11/2024], 2020. dirección: https://ruidera.uclm.es/server/api/core/bitstreams/c8878a98-aeeb-4565-8604-56f94a8a0853/content.

[22] «REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016 - relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos),»

[23] GDPR.EU. «Everything you need to know about the GPDR Data Protection Officer (DPO).» (2025), dirección: https://gdpr.eu/data-protection-officer/ (visitado 13-06-2024).

[24] G. V. Fuel Rodríguez, «IMPLEMENTACIÓN DE LA LEY ORGANICA DE PROTECCIÓN DE DATOS PERSONALES EN LA COOPERATIVA DE AHORROY CRÉDITO "PABLO MUÑOZ VEGA" CONSIDERANDO LOS ESTÁNDARES ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC27701:2019 Y EL SGSI INSTITUCIONAL,» *Universidad Técnica del Norte*, 2024, Publisher: Universidad Técnica del Norte. dirección: https://repositorio.utn.edu.ec/bitstream/123456789/16197/2/PG%5C%201875%5C%20TRABAJO%5C%20GRADO.pdf (visitado 27-06-2025).

[25] «Planes y precios Siigo|contifico,» Contífico. (), dirección: https://contifico.com/planes/ (visitado 20-07-2025).

[26] «¿Qué es el software como servicio (SaaS)? | Microsoft Azure.» (), dirección: https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-saas (visitado 20-07-2025).

[27] J.-F. CARPENTIER, *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Ediciones ENI, 1 de mayo de 2016, 450 págs., Google-Books-ID: LKE5_6gzBmgC, isbn: 978-2-409-00180-2.

[28] L. E. Álvarez, «Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales,» 2017.

[29] P. Peña-Pérez, «La protección de los datos personales como derecho fundamental: su autonomía y vigencia propia en el ordenamiento jurídico estatal,» *Revista de la Facultad de Derecho de México*, vol. 70, n.º 278, págs. 915-936, 13 de nov. de 2020, Number: 278-2, issn: 2448-8933. doi: 10.22201/fder.24488933e.2020.278-2.77065. dirección: https://www.revistas.unam.mx/index.php/rfdm/article/view/77065 (visitado 31-03-2025).

[30] Y. P. Hondares, R. M. Almora y A. P. Véliz, «La protección de datos personales. Presupuestos constitucionales para su protección en los procesos judiciales en cuba: The protection of personal data. Constitutional budgets for your protection in judicial processes in cuba,» *REVISTA CIENTÍFICA ECOCIENCIA*, vol. 8, págs. 126-161, 28 de dic. de

2021, issn: 1390-9320. doi: 10.21855/ecociencia.80.644. dirección: https://revistas.ecotec.edu.ec/index.php/ecociencia/article/view/644 (visitado 27-06-2025).

[31] Fundación Carolina y Telefónica SA, eds., *Derechos digitales en Iberoamérica: situación y perspectivas*, Madrid: Fundación Carolina, 2023, 1 pág., isbn: 978-84-09-49022-6.

[32] M. Arcos-Argudo, K. Matute-Pinos y M. Fernández-mora, «Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos,» *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, issn: 16469895.

[33] W. E. Redrobán Barreto, «Protección de datos personales en Ecuador a consecuencia de la emergencia sanitaria Covid-19,» *Revista Universidad y Sociedad*, vol. 15, n.º 2, págs. 194-206, abr. de 2023, Publisher: Editorial Üniverso Sur", issn: 2218-3620. dirección: http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2218-36202023000200194&lng=es&nrm=iso&tlng=en (visitado 04-05-2025).

[34] T. Cueva Luza, O. Jara Córdova, J. L. Arias Gonzáles, F. A. Flores Limo y C. A. Balmaceda Flores, *Métodos mixtos de investigación para principiantes*, 1.ª ed. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú, 21 de jul. de 2023, isbn: 978-612-5069-96-2. doi: 10.35622/inudi.b.106. dirección: https://editorial.inudi.edu.pe/index.php/editorialinudi/catalog/book/119 (visitado 17-08-2025).

[35] R. Hernández Sampieri y C. P. Mendoza Torres, *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*, First edition. México: McGraw-Hill Education, 2018, OCLC: 1076932853, isbn: 978-1-4562-6096-5.

[36] F. A. Reyes-Ruiz L. & Carmona Alvarado, « La investigación documental para la comprensión ontológica del objeto de estudio.,» Universidad Simón Bolívar, 2020. dirección: https://bonga.unisimon.edu.co/server/api/core/bitstreams/2af35a4b-2abf-4f78-a550-0a4e4764e674/content.

[37] «Investigación bibliográfica - Cómo llevar a cabo una - TestSiteForMe.» Section: Métodos de investigación. (26 de oct. de 2020), dirección: https://www.testsiteforme.com/investigacion-bibliografica/ (visitado 17-08-2025).

[38] «Qué es la investigación de campo: Definición, métodos, ejemplos y ventajas - TestSiteForMe.» Section: Métodos de investigación. (28 de feb. de 2022), dirección: https://www.testsiteforme.com/investigacion-de-campo/ (visitado 03-09-2025).

[39] G. P. Guevara Alban, A. E. V. Arguello y N. E. C. Molina, «Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción),» *RECIMUNDO*, vol. 4, n.º 3, págs. 163-173, 16 de jul. de 2020, issn: 2588-073X. doi: 10.26820/recimundo/4.(3).julio.2020.163-173. dirección: https://www.recimundo.com/index.php/es/article/view/860.

[40] M. Mozuni y W. Jonas, «An Introduction to the Morphological Delphi Method for Design: A Tool for Future-Oriented Design Research,» *She Ji: The Journal of Design, Economics, and Innovation*, vol. 3, n.º 4, págs. 303-318, 1 de dic. de 2017, issn: 2405-8726. doi: 10.1016/j.sheji.2018.02.004. dirección: https://www.sciencedirect.com/science/article/pii/S2405872617300710 (visitado 19-10-2025).

[41] J. Landeta, «Current validity of the Delphi method in social sciences,» *Technological Forecasting and Social Change*, vol. 73, n.º 5, págs. 467-482, 1 de jun. de 2006, issn: 0040-1625. doi: 10.1016/j.techfore.2005.09.002. dirección: https://www.sciencedirect.com/science/article/pii/S0040162505001381 (visitado 19-10-2025).

[42] E. Charro, «Investigando en educación: el método Delphi,» pág. 20, issn: 1989-4155.

[43] M. Ramírez y T. Ramírez, «El método DELPHI como herramienta de investigación. Una revisión,» *11 de marzo de 2024*, pág. 16, 2024, issn: 2789-3855,

[44] F. Calabuig Moreno y J. Crespo Hervàs, «Uso del método Delphi para la elaboración de una medida de la calidad percibida de los espectadores de eventos deportivos (Using Delphi method to develop a measure of perceived quality of sport event spectators),» *Retos*, vol. 15, págs. 21-25, 1 de ene. de 2009, issn: 1988-2041, 1579-1726. doi: 10.47197/retos.v0i15.34993. dirección: https://revistaretos.org/index.php/retos/article/view/34993 (visitado 19-10-2025).

[45] Escuela Europea de Excelencia. «Documentación en ISO 27001:2022: Lista actualizada de los documentos obligatorios en la última revisión.» Artículo que detalla la documentación obligatoria y recomendada para implementar un SGSI según ISO 27001:2022, Escuela Europea de Excelencia. (2023), dirección: https://www.escuelaeuropeaexcelencia.com/2023/01/documentacion-en-iso-270012022-lista-actualizada-de-los-documentos-obligatorios-en-la-ultima-revision/ (visitado 15-01-2024).

[46] NQA, *Guía de Implantación de ISO/IEC 27001:2022*, Primera, Guía práctica para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001:2022, NQA, Reino Unido, 2023. dirección: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%5C%20QRFs%5C%20and%5C%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf (visitado 15-01-2024).

[47] Info-Savvy. «ISO 27001 Clause 9.2: Internal Audit.» Artículo especializado sobre los requisitos y implementación de auditorías internas según el clause 9.2 de ISO 27001:2022, Info-Savvy. (2023), dirección: https://info-savvy.com/iso-27001-clause-9-2-internal-audit/ (visitado 15-01-2024).

[48] IT Governance USA. «Continual Improvement and ISO 27001:2022.» Artículo sobre el enfoque de mejora continua en el Sistema de Gestión de Seguridad de la Información según ISO 27001:2022, IT Governance USA. (2023), dirección: https://www.itgovernanceusa.com/blog/continual-improvement-and-iso270012013 (visitado 15-01-2024).

ANEXOS

ANEXO #1: Glosario de términos

ARCO (Derechos): acrónimo utilizado para identificar el conjunto de derechos que poseen los titulares de los datos personales (Acceso, Rectificación, Cancelación y Oposición). Cifrado: proceso que garantiza la confidencialidad de la información mediante accesos o lecturas de personas o sistemas autorizados.

Delegado de Protección de Datos (DPD): persona designada por el responsable del tratamiento de datos que actúa como enlace entre la autoridad de control y la empresa.

Dato Personal: cualquier tipo de información que haga a una persona identificable, como su nombre, cédula, correo, dirección, entre otros.

Dato Personal Sensible: toda aquella información que puede generar riesgos de discriminación o afectación a los derechos fundamentales.

ISO/IEC 27001: estándar internacional que garantiza la privacidad de la información personal.

ISO/IEC 27701: extensión de la norma ISO 27001 que establece requisitos específicos para el manejo de datos sensibles.

LOPDP: acrónimo utilizado para identificar la normativa ecuatoriana, Ley Orgánica de Protección de Datos Personales.

LOT: siglas para identificar la Ley Orgánica de Telecomunicaciones, ley que está relacionada con la protección y seguridad de datos en el sector de las telecomunicaciones.

Responsable del Tratamiento de Datos Personales (RTDP): persona natural o jurídica que decide sobre la finalidad de los datos que almacenará la organización.

SGSI: siglas utilizadas para el Sistema de Gestión de Seguridad de la Información, en el cual se evidencian las políticas de control relacionadas con los riesgos asociados a la información de una organización.

Titular de los Datos: persona natural propietaria de los datos personales que van a ser tratados dentro de una organización.

Tratamiento de Datos Personales: se refiere a cualquier actividad relacionada con la recolección, almacenamiento, eliminación y uso de los datos personales del titular.

ANEXO #2: Carta de Auspicio

BOREALPLAST CIA. LTDA
Moldeando el Futuro

CARTA DE AUSPICIO

BOREALPLAST S.A.
Dirección: Sebastián Moreno E1-25 y Av. Galo Plaza Lasso
Teléfono: 0994903739
Correo Electrónico: vfonseca@borealplast.com

Quito, marzo 26 del 2025

A quien corresponda,

Por medio de la presente, Borealplast S.A., empresa dedicada a la fabricación de fundas de empaque para alimentos y artículos de limpieza, expresa su interés en auspiciar el trabajo de tesis titulado **"Desarrollo de una Guía metodológica para la implementación de la Ley Orgánica de Protección de Datos Personales en la empresa Borealplast basada en estándares internacionales y buenas prácticas de seguridad"**, realizado por la Sra. Martha Cecilia Tiviano Gancino con cedula 1805144241, en el marco de su formación académica.

Consideramos que este trabajo es de gran relevancia para nuestra empresa, ya que contribuirá a fortalecer el cumplimiento normativo en materia de protección de datos personales y a mejorar nuestras prácticas de seguridad de la información. Por tal motivo, brindaremos la colaboración necesaria para el desarrollo de la investigación, facilitando el acceso a la información pertinente dentro de los límites permitidos por la ley y la política interna de la empresa.

Quedamos a disposición para cualquier coordinación adicional que se requiera y reiteramos nuestro apoyo a la Sra. Martha Cecilia Tiviano Gancino en la realización de su trabajo de tesis.

Atentamente,

BOREALPLAST CIA. LTDA.

Jorge Valdivieso Canelos
Gerente General
Borealplast Cía. Ltda

Verónica Fonseca
Gerente Comercial
Borealplast Cía. Ltda.

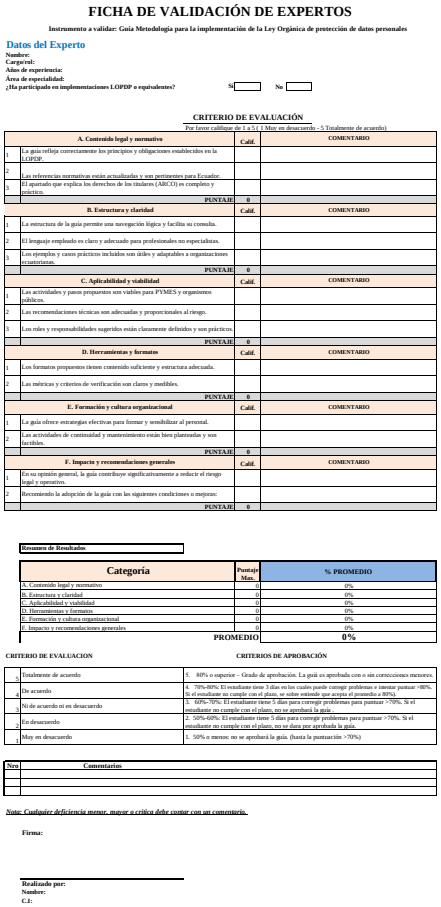
Direcc.: Sebastián Moreno E1-25 y Galo Plaza Lasso esquina Telfs.: 02 280 8861 / 02 280 0717 / 02 248 0064
Cel.:099 430 3739 Ofic.: 099 043 6269
QUITO - ECUADOR

Fig. 25.
Carta de auspicio extendida por el gerente general y gerente de Recursos Humanos de la empresa Borealplast.

El presente anexo evidencia la carta de auspicio extendida oficialmente por la gerencia de la empresa Borealplast, la cual manifiesta su respaldo absoluto en el presente trabajo de titulación "Desarrollo de una guía metodológica para la implementación de la Ley Orgánica de protección de datos personales en la empresa Borealplast" y se compromete a facilitar en acceso a la información necesaria de la empresa.

ANEXO #3: Validación de Expertos

El objetivo de esta entrevista es determinar el nivel de calidad de la guía metodológica desarrollada durante este proyecto para la empresa Borealplast.



FICHA DE VALIDACIÓN DE EXPERTOS

Instrumento a validar: Guía Metodología para la implementación de la Ley Orgánica de protección de datos personales

Datos del Experto

Nombre:
Cargo/rol:
Años de experiencia:
Área de especialidad:
¿Ha participado en implementaciones LOPDP o equivalentes? Si ☐ No ☐

CRITERIO DE EVALUACIÓN

Por favor califique de 1 a 5 (1 Muy en desacuerdo - 5 Totalmente de acuerdo)

	A. Contenido legal y normativo	Calif.	COMENTARIO
1	La guía refleja correctamente los principios y obligaciones establecidos en la LOPDP.		
2	Las referencias normativas están actualizadas y son pertinentes para Ecuador.		
3	El apartado que explica los derechos de los titulares (ARCO) es completo y práctico.		
	PUNTAJE	0	
	B. Estructura y claridad	**Calif.**	**COMENTARIO**
1	La estructura de la guía permite una navegación lógica y fácilita su consulta.		
2	El lenguaje empleado es claro y adecuado para profesionales no especialistas.		
3	Los ejemplos y casos prácticos incluidos son útiles y adaptables a organizaciones ecuatorianas.		
	PUNTAJE	0	
	C. Aplicabilidad y viabilidad	**Calif.**	**COMENTARIO**
1	Las actividades y pasos propuestos son viables para PYMES y organismos públicos.		
2	Las recomendaciones técnicas son adecuadas y proporcionales al riesgo.		
3	Los roles y responsabilidades sugeridos están claramente definidos y son prácticos.		
	PUNTAJE	0	
	D. Herramientas y formatos	**Calif.**	**COMENTARIO**
1	Los formatos propuestos tienen contenido suficiente y estructura adecuada.		
2	Las métricas y criterios de verificación son claros y medibles.		
	PUNTAJE	0	
	E. Formación y cultura organizacional	**Calif.**	**COMENTARIO**
1	La guía ofrece estrategias efectivas para formar y sensibilizar al personal.		
2	Las actividades de continuidad y mantenimiento están bien planteadas y son factibles.		
	PUNTAJE	0	
	F. Impacto y recomendaciones generales	**Calif.**	**COMENTARIO**
1	En su opinión general, la guía contribuye significativamente a reducir el riesgo legal y operativo.		
2	Recomiendo la adopción de la guía con las siguientes condiciones o mejoras:		
	PUNTAJE	0	

Resumen de Resultados

Categoría	Puntaje Máx.	% PROMEDIO
A. Contenido legal y normativo	0	0%
B. Estructura y claridad	0	0%
C. Aplicabilidad y viabilidad	0	0%
D. Herramientas y formatos	0	0%
E. Formación y cultura organizacional	0	0%
F. Impacto y recomendaciones generales	0	0%
PROMEDIO		0%

CRITERIO DE EVALUACION

5	Totalmente de acuerdo
4	De acuerdo
3	Ni de acuerdo ni en desacuerdo
2	En desacuerdo
1	Muy en desacuerdo

CRITERIOS DE APROBACIÓN

5. 80% o superior – Grado de aprobación. La guía es aprobada con o sin correcciones menores.

4. 70%-80%: El estudiante tiene 3 días en los cuales puede corregir problemas e intentar puntuar >80%. Si el estudiante no cumple con el plazo, se sobre entiendo que acepta el promedio a 80%).

3. 60%-70%: El estudiante tiene 5 días para corregir problemas para puntuar >70%. Si el estudiante no cumple con el plazo, no se aprobará la guía.

2. 50%-60%: El estudiante tiene 5 días para corregir problemas para puntuar >70%. Si el estudiante no cumple con el plazo, no se dara por aprobada la guía.

1. 50% o menos: no se aprobará la guía. (hasta la puntuación >70%)

Nro	Comentarios

Nota: Cualquier deficiencia menor, mayor a crítica debe contar con un comentario.

Firma:

Realizado por:
Nombre:
C.I.:

Fig. 26.
Evidencia del instrumento utilizado para la validación

En este anexo, se evidencia la ficha de validación aplicada a todos los expertos seleccionados por su trayectoria en los distintos campos referentes a la seguridad de la información.

ANEXO #4: Firma de acta de Entrega-Recepción

Fig. 27.
Firma de Acta de Entrega-Recepción.

Fig. 28.
Firma de acta de entrega-recepción en el área de RR.HH.

Una vez concluido el proceso de validación por expertos y directivos de la empresa Borealplast, la empresa procede a la aceptación formal de la guía para la implementación de la LOPDP.

ANEXO #5: Capacitación a stakeholders

Fig. 29.
Capacitación a stakeholders

Fig. 30.
Firma de asistencia a capacitación

Capacitación sobre la LOPDP y los derechos ARCO al personal operativo de la empresa Borealplast.

ANEXO #6: Acta de Entrega-Recepción

BOREALPLAST CIA. LTDA
Moldeando el Futuro

ACTA DE ENTREGA-RECEPCION

En la Ciudad de Quito, a los 22 días del mes de octubre del 2025, se procede a legalizar la entrega de la "Guía Metodología para la implementación de la Ley Orgánica de protección de datos personales, en la empresa BOREALPLAST Cía. Ltda.," reuniéndose el Sr. Jorge Valdivieso Canelos, Srta. Verónica Fonseca y la Sra. Martha Cecilia Tiviano, estudiante de la carrera Tecnologías de la Información en la universidad Técnica del Norte.

El objetivo de la presenta acta es para generar la constancia de la entrega-recepción de la guía metodología elaborada pro Sra. Martha Cecilia Tiviano, siendo la parte receptora la misma que tiene interés en el documento, la cual luego de una revisión exhaustiva está conforme con el contenido y trabajo realizado, procediendo a su recibimiento con satisfacción, siendo un aporte útil para el cumplimiento normativo en protección de datos dentro de la empresa.

Para constancia de lo anterior y fe de conformidad, firman el acta las personas que han intervenido en ella.

Sr. Jorge Valdivieso Canelos
C.I 1705336434
GERENTE GENERAL

Srta. Verónica Fonseca
C.I. 1709787251
GERENTE COMERCIAL

Sra. Martha Cecilia Tiviano
C.I. 18051442141
ESTUDIANTE

Dir.: Sebastián Moreno E1-25 y Galo Plaza Lasso esquina Telfs.: 02 280 8861 / 02 280 0717 / 02 248 0064
Cel.:099 430 3739 Ofic.: 099 043 6269 Quito - Ecuador

Fig. 31.
Acta de entrega-recepción en el área de RR.HH.

ANEXO #7: Certificado de Recepción

BOREALPLAST CIA. LTDA
Moldeando el Futuro

CERTIFICADO DE RECEPCION A CONFORMIDAD

Por medio de la presente, BOREALPLAST Cía. Ltda., con RUC 1792202949001, representada por el Sr. Jorge Valdivieso, en su cargo de Gerente General, certifica que ha recibido con satisfacción la propuesta titulada "Guía Metodológica para la implementación de la Ley Orgánica de protección de datos personales en la empresa BOREALPLAST Cía. Ltda.," realizada por la señora Martha Cecilia Tiviano Gancino con cedula de identidad 1805144241, siendo la misma parte de su trabajo de titulación.

Luego de la revisión correspondiente, la empresa MANIFIESTA SU PLENA CONFORMIDAD, considerando que el proyecto final se alinea a la propuesta presentada inicialmente, siendo útil para la futura aplicación de la Ley Orgánica de protección de datos personales dentro de nuestra organización, considerando que:

- Cumple con los objetivos planteados.
- El proyecto se ha desarrollado abarcando el entorno de nuestra organización.
- Establece criterios legales y técnicos basados en la normativa ecuatoriana vigente.
- Establece mecanismo de seguimientos y mejora continua para el cumplimiento normativo.
- Propone políticas aptas para nuestra organización.

El presente certificado se expide a petición de la interesada, para los fines que estime convenientes.

Atentamente,

Sr. Jorge Valdivieso Canelos
C.I. 1705336434
GERENTE GENERAL
BOREALPLAST

Dir.: Sebastián Moreno E1-25 y Galo Plaza Lasso esquina Telfs.: 02 280 8861 / 02 280 0717 / 02 248 0064
Cel.:099 430 3739 Ofic.: 099 043 6269 Quito - Ecuador

Fig. 32.
Certificado de recepción a conformidad extendida por el Ing. Jorge Valdivieso.

ANEXO #8: Checklist

RESUMEN-CHECKLIST LOPDP- BOREALPLAST

Ítem	Cumple	Parcial	No cumple	No aplica	Evidencia
Gobernanza y responsabilidades					
Existencia de política de protección de datos personales					Entrevista
Responsable para designar el DPD					Entrevista
Registro de actividades de tratamiento (RAT)					Cuestionario/Obs. Directa
Existencia de pocedimientos para documentar el tratamiento					Entrevista
Consentimiento y base legal					
Documentación de Consentimiento					Cuestionario
Formularios con finalidades y derechos					Entrevista
Tratamiento basado en base legal de la nomativa LOPDP					Entrevista
Finalidades del tratamiento					
Finalidades documentadas y definidas					Entrevista
Los datosnno son utilizados para fines personales					Entrevista/Obs. Directa
Derechos de los titulares					
Politicas para ejercicio de derechos					Cuestionario
Plazos de atención solicitudes ARCO definidos					Entrevista
Seguridad de la información					
Controles técnicos y organizativos básicos					Entrevista/Obs. Directa
Gestión de incidentes de seguridad- DPD					Cuestionario
Transferencias y encargados					
Contratos con RTD y DPD					Entrevista/Obs. Directa
Transferenciasnacionales e internacionales controladas					Entrevista/Obs. Directa

Fig. 33.
Checklist de la LOPDP

En el presente anexo se expone un resumen del checklist realizado a la empresa para identificar el nivel de cumplimiento normativo inicial, para luego realizar una comparación del nivel de cumplimiento después de aplicar la guía propuesta.

ANEXO #9: Entrevista

Instrumento de evaluación para personal administrativo de la empresa

1. ¿Existen políticas para la protección de datos personales?
2. ¿Se ha designado un Responsable del Tratamiento de Datos Personales?
3. ¿Existe un DPD o un rol equivalente?
4. ¿Se realiza el registro de las actividades sobre el manejo de datos personales?
5. ¿Existen procedimientos documentados para el tratamiento de datos personales?
6. ¿Se solicita consentimiento informado a los clientes y empleados?
7. ¿Están definidas las finalidades del tratamiento de datos?
8. ¿Se garantiza que los datos personales no se utilicen para finalidades incompatibles?
9. ¿Existen procedimientos para que los titulares ejerzan sus derechos ARCO?
10. ¿La organización ha implementado controles técnicos y organizativos para proteger los datos personales?
11. ¿Existen procedimientos para la gestión de incidentes?
12. ¿Las transferencias nacionales e internacionales de datos personales, están debidamente controladas?

Fig. 34.
Entrevista de la LOPDP-Gerente general

En el presente anexo, se evidencian las preguntas realizadas al personal operativo de la empresa.