



UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

**Facultad de Ciencias Administrativas, Contables y
Comercio Carrera de Gestión de la Información Gerencial**

**TRABAJO DE UNIDAD DE INTEGRACIÓN
CURRICULAR**

MODALIDAD ESTUDIO DE CASO

Previo a la obtención del título de:

Licenciado (a) en Gestión de la Información Gerencial

TEMA

**Aplicación de la Ley Orgánica de Protección de Datos Personales en la
Recolección de Información de la empresa CEDEPA**

AUTORA

Cantos Burgos Madeleine Maoly

TUTOR

Lic. Jonathan Coveña Menendez, Mg

MANTA- ECUADOR

Tema:

**Aplicación de la Ley Orgánica de Protección de Datos Personales en la Recolección de
Información de la empresa CEDEPA Año 2025 (Estudio de Caso)**

	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1 Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutora de la Facultad de Ciencias Administrativas de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido, revisado y aprobado preliminarmente el Trabajo de Integración Curricular con la modalidad Estudio de Caso, bajo la autoría del estudiante: **Cantos Burgos Madeleine Maoly**, legalmente matriculado/a en la carrera de GESTIÓN DE LA INFORMACIÓN GERENCIAL, período académico 2025 (2) 2026 (1), cumpliendo el total de 240 horas, cuyo tema del proyecto es: **Aplicación De La Ley Orgánica De Protección de Datos Personales en la Recolección de Información.**

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, y la originalidad de la misma, requisitos suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Lugar, 17 de julio de 2026.

Lo certifico,



Lic. Jonathan Covaña Menéndez, Mg.E.I.I.
Docente Tutor(a)

Nota 1: Este documento debe ser realizado únicamente por el/la docente tutor/a y será receptado sin enmendaduras y con firma física original.

Nota 2: Este es un formato que se llenará por cada estudiante (de forma individual) y será otorgado cuando el informe de similitud sea favorable y además las fases de la Unidad de Integración Curricular estén aprobadas.

UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ

Facultad de Ciencias Administrativas, Contables y Comercio

Carrera de Gestión de la Información Gerencial

**APROBACIÓN DEL TRABAJO DE INVESTIGACIÓN POR EL
TRIBUNAL**

Los miembros del tribunal de grado aprueban el informe de Estudio de Caso, presentado por la Srta. Cantos Burgos Madeleine Maoly; de acuerdo con las disposiciones reglamentarias emitidas por la Universidad Laica “Eloy Alfaro de Manabí”.

Con el tema “Aplicación de la Ley Orgánica de Protección de Datos Personales en la Recolección de Información”

Para constancia firman:



Mgrt. Ivan Ochoa

PRESIDENTE DEL TRIBUNAL



Mgrt. Mercy Rojas Once

MIEMBRO DEL TRIBUNAL



Mgrt. Mario Arauz Chávez

MIEMBRO DEL TRIBUNAL



Certificado de análisis
Compilatio Magister+ | ULEAM-ECU

CANTOS BURGOS MADELEYNE MAOLY

ID : 467e375a77eea8d647aef837f927fb1a7338e658



9%

Textos sospechosos

Nombre del fichero : CANTOS BURGOS MADELEYNE MAOLY.txt
Tamaño del archivo original : 573,1 kB
Número de palabras : 9322

Depositante : Jonathan Kléber Cervera Menéndez
Fecha de depósito : 17 de julio de 2026
Tipo de carga : interface
Fecha de fin de análisis : 17 de julio de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :



Incluido en el porcentaje de textos sospechosos :

Similitudes 5%

Pasajes con similitudes a fuentes encontradas en diferentes colecciones.



Detección de IA 4%

Textos estilísticamente próximos a un texto generado por una IA.

Este índice es un indicador y no una prueba. Comprueba con el autor si domina los conocimientos mencionados en el documento.



Idiomas no reconocidos 3%

Pasajes en los que parte del vocabulario utilizado no forma parte del diccionario de la lengua.

Puede tratarse de un intento del autor de modificar el texto para evitar ser detectado.



No incluido en el porcentaje de textos sospechosos :

Textos entre comillas 3%

Pasajes entre comillas, a menudo indicativos de una cita.

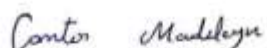
Autoría

Yo, Cantos Burgos Madeleine Maoly, portadora de la cédula de ciudadanía 1317217436, estudiante de la Facultad de Ciencias Administrativas, Contables y Comercio de la Universidad Laica Eloy Alfaro de Manabí, declaro que el presente trabajo de investigación titulado:

“Aplicación de la Ley Orgánica de Protección de Datos Personales en la Recolección de Información de la empresa CEDEPA (Estudio de Caso)”

es de mi autoría intelectual y ha sido desarrollado como requisito académico para la obtención del título correspondiente. El contenido de esta investigación es resultado de un proceso de análisis, recopilación y evaluación de información realizado bajo principios éticos, académicos y metodológicos, respetando las normas de citación y propiedad intelectual vigentes.

En constancia de lo expuesto, suscribo la presente declaración de autoría.



Cantos Burgos Madeleine Maoly
C.I. 1317217436

Dedicatoria

Dedico este trabajo de investigación, en primer lugar, a Dios, por brindarme fortaleza, salud y sabiduría para culminar esta importante etapa de mi formación académica.

A mis padres, quienes han sido el pilar fundamental de mi vida, por su amor incondicional, esfuerzo constante, sacrificio y apoyo durante todo mi proceso educativo. Gracias por creer en mí incluso en los momentos más difíciles, por sus consejos, valores y enseñanzas que me han permitido crecer tanto personal como profesionalmente.

Este logro también les pertenece a ustedes, porque cada meta alcanzada es el reflejo de su dedicación, confianza y motivación permanente. gratitud, por lo que dedicarles este trabajo es una muestra del amor y respeto por ustedes.

Cantos Burgos Madeleine Maoly

Reconocimiento

En primer lugar, quiero agradecer a mis padres, por ser mi fuente de inspiración para alcanzar este objetivo académico, puesto con su apoyo incondicional, comprensión y acompañamiento han sido fundamentales durante cada etapa de mi vida.

Gracias por los esfuerzos realizados para brindarme las herramientas necesarias para mi educación, por sus palabras de aliento en los momentos de dificultad y por enseñarme el valor de la perseverancia, la responsabilidad y el compromiso.

De igual manera, agradezco a la Universidad Laica Eloy Alfaro de Manabí, a la Facultad de Ciencias Administrativas, Contables y Comercio, a mis docentes y a todas las personas que contribuyeron al desarrollo de esta investigación, compartiendo conocimientos y experiencias que enriquecieron este trabajo.

A todos ellos, mi más profunda gratitud por haber sido parte de este importante logro académico y personal.

Cantos Burgos Madeleine Maoly

Índice

Tema:.....	2
Certificado del tutor	3
Certificado Anti-plagio	4
Autoría.....	5
Dedicatoria	6
Reconocimiento	7
Introducción.....	9
Antecedentes de la investigación	10
Justificación.....	13
Marco Conceptual.....	15
Protección de datos personales.....	15
La Ley Orgánica de Protección de Datos Personales en Ecuador	16
Importancia de la aplicación de la Ley Orgánico de Protección de Datos Personales en las organizaciones	18
Riesgos asociados al incumplimiento de la normativa de protección de datos	18
Recolección de datos	19
Criterios de calidad para la recolección de datos	19
La importancia de la recolección de datos personales en los sistemas de información	20
Marco Metodológico.....	22
Triangulación de la información	25
Análisis de resultados	33
Conclusiones.....	34
Recomendaciones	35
Referencias Bibliográficas	36
Anexos	40
Propuesta	43

Introducción

En un contexto caracterizado por el mundo de la digitalización en los procesos organizacionales, la información se ha consolidado como un recurso estratégico para las empresas. El manejo de datos personales, en particular, implica importantes responsabilidades éticas y legales, puesto que un tratamiento ineficiente puede afectar derechos fundamentales como la privacidad y la confidencialidad.

Ante los retos y desafíos que se han presentado en relación con este tema, surge la ley de protección de datos donde es un factor clave y estratégico dentro de cualquier gestión de las empresas donde administran diariamente datos relacionados con clientes, proveedores e interna, sin embargo, aquí es donde la gestión de la información complementa este accionar cumpliendo así con los criterios de seguridad y confidencialidad de manera eficiente.

En el contexto ecuatoriano la promulgación de la ley de protección de datos personales en 2021 configuró un marco jurídico destinado a regular el tratamiento de la información en entidades públicas y privadas, estableciendo un principio, derechos y obligaciones que buscan garantizar la confidencialidad y seguridad de los datos, aunque en la práctica aun presentan limitaciones en determinado sectores productivos en especial en el sector automotriz donde áreas operativas como el departamento de cobranzas quienes manejan información de manera constante, intensiva y sensible, lo que incrementa los riesgos asociados al mal uso de la información.

En la presente investigación se toma campo de acción la empresa CEDEPA, la cual se encuentra localizada en la ciudad de Manta en la provincia de Manabí, la cual tiene como objetivo analizar el nivel de cumplimiento de la Ley Orgánica de Protección de Datos Personales en el tratamiento de información dentro del departamento de cobranza tomando en cuenta el proceso de recolección, tratamiento y seguridad de los datos personales de los

involucrados. La investigación nace bajo un enfoque cualitativo de investigación acción para comprender y analizar el contexto actual

La recolección de información estará apoyada en técnicas como la observación directa y la entrevista, orientadas a obtener una visión integral del estado actual de la gestión de datos y a identificar oportunidades de mejora que fortalezcan el cumplimiento normativo.

Finalmente, los resultados del estudio revelan que, aunque existen controles básicos para el tratamiento de la información y una preocupación institucional por resguardar la confidencialidad de los datos, todavía existen limitaciones en cuanto a la formalización de políticas, capacitación del personal y aplicación sistemática de mecanismos de control, por lo que se recomienda una propuesta de solución para mejorar estas falencias que no permiten implementar la normativa de manera integral.

Antecedentes de la investigación

En los últimos años, la protección de los datos personales es un tema que tiene mucha importancia, puesto que todas las organizaciones manejan datos y pueden tener riesgos relacionados con la filtración, uso no autorizado y mal tratamiento de la información, por lo que diversos países se han sumado en fortalecer sus marcos normativos en materia de privacidad de los datos. Es el caso de Ecuador, en donde surgió la necesidad en la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021), la cual regula la recolección, almacenamiento, acceso, transferencia y tratamiento de datos en instituciones públicas y privadas.

La relevancia de este marco legal se manifiesta a través de diversos estudios anteriores, la Superintendencia de Protección de Datos (2024) subrayan la importancia de fortalecer la gobernanza de los datos en el sector privado donde existen brechas en cuanto al resguardo de los datos. En este sentido se detalla la información de los estudios anteriores

desde lo internacional para aterrizar en lo local y así contextualizar las variables de estudios dentro de diversos campos o situaciones reales:

A nivel internacional, García y Rebellón (2022) comparación la legislación colombiana con el Reglamento General de Protección de Datos de la Unión Europea identificando vacíos en los marcos en el continente latinoamericano donde se refleja la necesidad en adoptar estándares sólidos frente a los desafíos en el entorno digital.

Por otro lado, a nivel nacional Iza y Mora (2023) sostienen que pese a que la LOPDP representa un progreso normativo significativo las organizaciones afrontan obstáculos vinculados al conocimiento especializado a la cultura informacional y a la existencia de mecanismos internos eficaces, investigaciones de alcance local como la desarrollada por Cevallos (2024) muestran diferencias entre los planteamientos teóricos y su aplicación efectiva en instituciones públicas lo que permite proyectar la presencia de retos semejantes en entidades privadas de mediana escala

En este contexto, las empresas del sector comercial se encuentran particularmente expuestas, puesto que manejan información personal, financiera y de contacto de clientes y proveedores. En este caso hemos tomado como campo de estudio a CEDEPA en el periodo 2025, la cual es una empresa ubicada en la ciudad de Manta, provincia de Manabí, dedicada desde 1985 a la comercialización de repuestos automotrices para vehículos de gasolina y diésel. Su trayectoria empresarial le ha permitido posicionarse como una de las organizaciones más representativas del sector de autopartes en la región, gracias a su amplia variedad de productos, calidad en el servicio y asesoría técnica especializada.

La misión de CEDEPA se orienta a ofrecer repuestos automotrices a precios competitivos y con disponibilidad inmediata, con el fin de satisfacer las necesidades del mercado de autopartes mediante un servicio caracterizado por la calidad y garantía.

Por otro lado, la visión es liderar la comercialización de repuestos automotrices en la provincia de Manabí ofertando productos a la vanguardia de la tecnología con altos estándares de calidad para satisfacer las necesidades del mercado con atención de excelencia y soporte técnico personalizado

En contraste dentro de esta organización interna, el departamento de cobranzas tiene una importancia, no solo por su impacto directo en la sostenibilidad financiera de la empresa, sino también por el volumen de información sensible que maneja. Diversos actores institucionales, el personal de cobranzas, el área administrativa y el departamento legal, convergen participando en la recopilación, procesamiento, actualización y almacenamiento de datos de clientes, deudores y proveedores. Es importante tener en cuenta que las interacciones que se manejan en esta área son complejas, lo que llamó la atención para analizar el cumplimiento de la normativa que se está mencionando en este estudio.

La investigación se enfoca en la recolección y el tratamiento de los datos personales en el departamento de cobranzas, donde procesos tales como: registro, protección, actualización y difusión de la información se realiza de manera constante.

En este sentido la ley orgánica de protección de datos personales rige con efectividad las responsabilidades que las instituciones deben de cumplir, así como las sanciones por incumplimiento. Es importante mencionar que en temas relacionados con esta investigación existen pocos donde se analicen si las empresas privadas cumplen la normativa tal y como lo dispone para su compromiso ético y legal.

Este escenario evidencia un vacío investigativo relacionado con la aplicación práctica de la normativa en empresas comerciales del sector automotriz en Manta, especialmente en áreas donde el tratamiento de datos es intensivo. Por ello, el estudio de caso de CEDEPA resulta pertinente para comprender los niveles de cumplimiento, los mecanismos de seguridad aplicados y las prácticas internas vinculadas a la protección de datos personales.

Justificación

La presente investigación se justifica por varias razones de orden académico, social, profesional e institucional, así como por la necesidad de analizar un fenómeno estudiado en el contexto empresarial ecuatoriano: la aplicación de la Ley Orgánica de Protección de Datos Personales (LOPD) en empresas privadas medianas, particularmente en áreas operativas donde el tratamiento de información personal es constante, como es el caso del departamento de cobranza. de CEDEPA:

Desde el ámbito académico, el estudio tiene importancia debido a las limitaciones en investigaciones en el sector comercial sobre la aplicación de la normativa, sin embargo existe investigaciones orientada al análisis jurídico de la LOPDP y a comparaciones con otros marcos internacionales todavía se identifican vacíos relacionados con su aplicación práctica en entornos organizacionales. Al centrarse en CEDEPA una microempresa con trayectoria en el mundo automotriz, el estudio aporta evidencia empírica valiosa sobre la manera en que se interpreta, asume y aplica las disposiciones establecidas por la normativa de protección de datos permitiendo así identificar las prácticas que actualmente se implementan, así como las debilidades que existen en su gestión informacional. De tal manera que el que estudio contribuya al fortalecimiento del ámbito académico vinculado al cumplimiento normativo, la gobernanza de datos y la gestión de la información, procesos que a día de hoy adquieren un valor central en un escenario empresarial marcado por la digitalización acelerada y la creciente preocupación por la seguridad de la información.

Por otro lado, desde una perspectiva social la investigación tiene relevancia al abordar la protección de los datos personales como un derecho que incide directamente en la confianza, seguridad y la relación entre empresas y clientes. Las organizaciones que administran información sensible particularmente datos financieros y personales tienen la responsabilidad de actuar de manera ética para así garantizar su tratamiento bajo criterios de

legalidad, transparencia y confidencialidad. Tomar en cuenta a CEDEPA nos permite conocer como las pequeñas y medianas empresas del sector automotriz se encuentran preparadas para cumplir las normativas vigentes, teniendo en cuenta que las personas proporcionan información que debe ser tratada con cuidado. Por tanto, este estudio aporta desde el fortalecimiento de una cultura de protección de datos en una sociedad de la información que se encuentra cada vez deteriorada por ataques cibernéticos.

En este contexto basándonos en el ámbito profesional y organizacional este estudio es pertinente, por la capacidad de identificar oportunidades de mejorar continua en procesos internos de la empresa CEDEPA, enfocando al departamento de cobranzas permitiendo así detectar riesgos de carácter legal, procedimental, tecnológico e informacional.

Los hallazgos obtenidos constituyen, además, un factor relevante para el fortalecimiento de las políticas internas, mejorar la capacitación del talento humano, la implementación de medidas de seguridad más fuertes y la consolidación de una gestión informacional regentada con los principios de la normativa vigente.

Cabe señalar que el desarrollo de la investigación estuvo condicionado por ciertas limitaciones, principalmente relacionadas con la disponibilidad de tiempo del personal de CEDEPA para colaborar en el proceso investigativo y con el acceso restringido a información, en virtud de las políticas internas de la empresa y de la propia normativa de protección de datos. Estos aspectos delimitaron analizar al departamento de cobranzas, sin comprometer la validez de los resultados que se han alcanzados en el estudio

Escoger a CEDEPA como campo de estudio es interesante al ser una empresa con una larga trayectoria en el mercado local de la provincia de Manabí, por lo cual tiene una gama de clientes donde se gestiona información personal y financiera de manera constante. En este sentido, todos estos aspectos han sido tomados en cuenta para analizar como esta empresa

que ha venido desarrollando practicas traccionales enfrenta los desafios de la normativa mencionada en este estudio,

Bajo este escenario se establece el siguiente objetivo general:

Analizar el cumplimiento de la Ley Orgánica de Protección de Datos Personales en el tratamiento de datos personales en el departamento de cobranza de CEDEPA, en el año 2025.

En este sentido para lograr el cumplimiento del objetivo general a continuación se detallan los siguientes objetivos específicos:

- Diagnosticar el estado actual del proceso de recolección y uso de los datos personales en el departamento de cobranza de CEDEPA en el año 2025
- Analizar los mecanismos internos relacionados con el manejo y protección de datos personales en el departamento de cobranza de CEDEPA en el año 2025
- Proponer una estrategia que permita fortalecer el cumplimiento Ley Orgánica de Protección de Datos Personales en el tratamiento de datos personales para reducir riesgos asociados al tratamiento de la información.

Marco Conceptual

Protección de datos personales

En la sociedad actual, donde nos encontramos inmersos en el mundo tecnológico, los datos personales han tomado un papel central en la interacción entre ciudadanos y plataformas digitales la protección de datos personales entra en juego como un derecho fundamental que garantiza la seguridad e integridad de los ciudadanos. Sin embargo, son los mismos ciudadanos quienes deciden qué información compartir y sobre qué condiciones, a partir de su consentimiento, lo que refuerza el control sobre su espacio privado. En concordancia con ello, se sostiene que:

"El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Constitución de la República del Ecuador, 2008, Art. 66. Literal 19, p.33)

En contraste la CEPAL (2020), describe a la protección de datos personales, como: La protección de datos se refiere a los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, de saber qué datos están siendo retenidos y usados y de corregir las inexactitudes. Si la investigación involucra a personas, se deben considerar las obligaciones legales y éticas con respecto a compartir los datos. (Comisión Económica para América Latina y el Caribe, CEPAL, 2020).

La ley orgánica de protección de datos personales en Ecuador

La Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en el Registro Oficial Suplemento N.º 459 el 26 de mayo de 2021, constituye un hito en la consolidación de los derechos digitales en el Ecuador. Esta normativa establece un marco jurídico que garantiza a los ciudadanos el control efectivo sobre su información personal, fortaleciendo la seguridad jurídica frente al uso y tratamiento de datos en entornos digitales.

Tomando en cuenta lo anterior, "el titular tiene derecho a conocer, acceder, rectificar, actualizar, eliminar y oponerse al tratamiento de sus datos personales" (LOPDP, 2021), lo cual demuestra una protección manifiesta del principio de autodeterminación informativa. La LOPDP, por lo tanto, es importante que esta ley se cumpla porque no solo protege la integridad de las personas, además permite que ellos sean participe acerca del uso de su información creando una administración transparente y responsable de los datos personales.

Principios del tratamiento de datos

Todas las leyes tienen sus principios los cuales permiten que esta normativa se cumpla de manera rigurosa garantizando que su gestión respete los derechos de los involucrados. En el caso de la LOPDP, estos principios orientan tanto en instituciones del ámbito público como privado Ley Orgánica de Protección de Datos Personales (LOPDP), a continuación, se detallan:

- Juridicidad
- Honestidad
- Transparencia
- Finalidad
- Relevancia y minimización
- Proporcionalidad
- Confidencialidad
- Calidad y precisión
- Seguridad de los datos personales
- Responsabilidad proactiva y demostrable
- Aplicación favorable al titular

Es importante tener en cuenta que su alcance va más allá del mero cumplimiento del marco legal vigente, ya que promueve la adopción de políticas destinadas a reforzar la seguridad de los datos, brindar mayor transparencia a los procesos internos y proteger los derechos de quienes confían su información a las instituciones. En este contexto, la LOPDP se posiciona como una herramienta estratégica para mitigar el riesgo legal y, al mismo tiempo, fortalecer la confianza y independencia del control: La autoridad encargada de la protección de datos debe ejercer un control independiente, imparcial y autónomo sobre el cumplimiento de la ley.

Importancia de la aplicación de la Ley Orgánico de Protección de Datos

Personales en las organizaciones

La incorporación efectiva de la Ley de Protección de Datos Personales (LOPD) en los procesos organizacionales se ha convertido en un pilar fundamental para buscar fortalecer la integridad y seguridad de los datos, para mejorar la transparencia en los procesos internos para garantizar los derechos de quienes confían su información a las empresas. Por tanto, la LOPDP establece como un instrumento importante para reducir brechas legales reforzando la confianza institucional.

En este sentido, Sevilla Moncayo (2024) sostiene, desde este punto de vista, que para que las organizaciones apliquen la LOPDP es necesario que incorporen de manera coherente medidas regulatorias, técnicas y organizativas, con el objetivo de asegurar la correcta y responsable gestión de los datos personales. Este requerimiento fomenta el fortalecimiento de los sistemas de control interno y ayuda a generar un ambiente de confianza entre los trabajadores internos y los clientes y empleadores externos.

El autor expresa que esta responsabilidad recae en todas las organizaciones, independientemente de su ubicación o tamaño, las cuales deben revisar y ajustar sus procesos internos para alinearlos con los requisitos legales vigentes, por lo que no solo responde a obligaciones legales, sino que también persigue un objetivo más amplio como garantizar que la información proporcionada por las personas se gestione con rigor, cuidado y respeto.

Riesgos asociados al incumplimiento de la normativa de protección de datos

El incumplimiento de las disposiciones constitucionales relacionadas con la protección de datos personales genera riesgos jurídicos y administrativos para las instituciones públicas y privadas, puesto que la Constitución de la República del Ecuador reconoce el derecho de las personas a la protección de sus datos personales, al acceso y decisión sobre la información que les concierne, así como a su debida confidencialidad. En

este sentido, el tratamiento inadecuado de datos puede derivar en la vulneración de derechos fundamentales, responsabilidades legales y acciones constitucionales por parte de los titulares de la información (Constitución de la República del Ecuador, 2008).

Recolección de datos

En el ámbito de la gestión organizacional, la recolección de datos constituye una fase fundamental, ya que de ella depende la calidad de la información que será utilizada en los procesos administrativos y estratégicos. En este sentido, se reconoce que:

La gestión de la información comienza con este proceso, que implica la recopilación de datos internos generados por sistemas de información empresarial, así como la adquisición de datos externos de fuentes como proveedores, clientes o bases de datos públicas, para esto se utilizan diversas técnicas y tecnologías utilizadas para capturar datos de manera efectiva, como la entrada manual de datos, la automatización de la captura de datos a través de dispositivos como escáneres o sensores, y la integración de sistemas para recopilar datos de múltiples fuentes. (Laudon, 2016).

Criterios de calidad para la recolección de datos

- La precisión se utiliza para medir el grado de concordancia entre los datos y un objeto real; representa el grado en que los datos están libres de errores y son fiables, así como el grado en que los datos corresponden (o se aproximan) a los valores reales de los elementos, también conocido como el valor correcto
- La integridad es una de las dimensiones de calidad de datos más comúnmente aplicadas y generalmente proporciona una medida de la presencia de datos. Esta dimensión representa el grado en que todos los datos esperados y requeridos (registros, atributos) están presentes o no faltan, respectivamente
- La consistencia, también conocida como representación consistente, es el grado en que los datos no presentan contradicciones entre sí o siguen una regla

establecida, y se proporcionan en el mismo formato, compatible con datos anteriores

- La vigencia o actualidad se refiere al grado en que los datos están suficiente o razonablemente actualizados para la tarea prevista.
- La relevancia, como dimensión, representa el grado en que los datos cumplen con las expectativas y requisitos del usuario.
- La fiabilidad se utiliza, en algunos casos, como sinónimo de precisión; a pesar de ello, otros definen la dimensión como el grado en que un valor inicial de datos coincide con un valor posterior.
- La puntualidad también se aplica con frecuencia y puede representar hasta qué punto la antigüedad de los datos es adecuada para el uso previsto, o la diferencia de tiempo entre un evento en tiempo real y el tiempo que tarda la captura o verificación de datos correspondiente.
- La puntualidad puede medirse como la duración, explícitamente la diferencia de tiempo entre la recopilación de los datos.
- La validez de los datos representa el grado en que estos concuerdan con las normas establecidas.

La importancia de la recolección de datos personales en los sistemas de información

Es importante mencionar que el proceso de gestión de la información empezando por la recolección y continuando con el tratamiento de datos personales requieren una atención delicada por quienes son los responsables de los sistemas de información, puesto que existen las implicaciones éticas y legales que conllevan proteger los datos de las personas.

Como señala el investigador en *Information & Management*, “es importante que los gestores de sistemas de información comprendan los temas relacionados con la privacidad de

la información personal para proteger los derechos de quienes proporcionan los datos y de quienes son objeto de recolección” (Gelderman, 1999).

Seguridad de la información

En un entorno organizacional cada vez más dependiente de la información, su adecuada protección se vuelve indispensable para evitar riesgos y garantizar un uso responsable de los datos. La seguridad de la información, por tanto, no se limita al ámbito tecnológico, sino que abarca medidas físicas, organizativas y humanas orientadas a resguardar los activos informativos.

Desde la perspectiva de Gómez (2007) la seguridad de la información es la disciplina que abarca los sistemas de protección física, la prevención de accidentes o la prevención de actividades desleales por parte de los empleados de una organización o empresa.

De esta manera los tres pilares fundamentales de la seguridad de la información son:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Basándose en esta noción más extensa de la seguridad de la información, es imprescindible ubicar sus principios en un entorno organizativo, donde los datos superan su carácter meramente técnico para transformarse en un elemento estratégico del que depende el desempeño corporativo. En el contexto de los negocios, entender realmente la privacidad, la integridad y la disponibilidad no solo implica implementar herramientas tecnológicas, sino

que además está muy relacionado con organizar los procesos internos, determinar las responsabilidades y reconocer los riesgos asociados a la gestión de datos.

Competencias digitales para la seguridad de la información

Las competencias digitales constituyen un conjunto de conocimientos, habilidades y actitudes necesarias para el uso seguro, crítico y responsable de las tecnologías de la información. Dentro de este marco, las competencias relacionadas con la seguridad adquieren especial relevancia, ya que permiten a los usuarios proteger dispositivos, datos personales y la información institucional frente a riesgos digitales.

El Marco Europeo de Competencias Digitales (DigComp), La privacidad, la protección de los datos, el manejo de la información y la implementación anticipada de acciones para garantizar la seguridad digital son algunos de los aspectos esenciales que incluye el campo de la seguridad. En el contexto de una organización, para asegurar el cumplimiento de la regulación de protección de datos, disminuir los peligros de equivocaciones humanas y promover una cultura empresarial enfocada en la seguridad informativa, es fundamental desarrollar y fortalecer estas habilidades en los recursos humanos.

Marco Metodológico

En este estudio se optó por un enfoque cualitativo sustentado en la investigación-acción, apoyado en un estudio de caso que permitió adentrarse de manera profunda en el contexto analizado y captar, con mayor sensibilidad, las vivencias y percepciones de quienes formaron parte del proceso. Paralelamente, se desarrolló un diagnóstico de la situación vigente a partir de la observación sistemática, orientado a construir una visión precisa y actual del escenario investigado, lo cual permitió identificar los problemas actuales. El desarrollo de esta investigación se realizó bajo un enfoque descriptivo y explicativo,

orientado a caracterizar los aspectos fundamentales del objeto de estudio, también a comprender los factores que influyen en su dinámica.

En esta investigación se aplicaron diversos métodos de carácter científico entre ellos, el análisis y la síntesis el análisis permitió examinar de manera rigurosa la documentación académica vinculada con las variables del estudio, posibilitando una revisión profunda y crítica de los aportes teóricos existentes. A partir de este proceso, la síntesis hizo viable rescatar los planteamientos más relevantes del material consultado, los cuales sirvieron como fundamento para la construcción de nuevos aportes dentro del trabajo investigativo.

Por otro lado, el análisis documental y bibliográfico fue empleado para la recopilación de estudios previos vinculados con el tema abordado, lo que permitió comprender en profundidad la forma en que esta problemática ha sido tratada en investigaciones anteriores. A través de esta revisión, se obtuvo una base sólida de conocimiento que orientó el desarrollo teórico del estudio.

De igual manera, se aplicó el método inductivo–deductivo. Desde la perspectiva inductiva, fue posible construir conceptos, planteamientos teóricos y generalizaciones a partir de la observación y de la evidencia empírica disponible, identificando regularidades y comportamientos recurrentes que condujeron a interpretaciones de carácter general. En cuanto al enfoque deductivo, este facilitó el contraste entre los postulados teóricos y el contexto real en el que se desarrolló el caso analizado.

Para el desarrollo del estudio se recurrió a distintas técnicas de recolección de información. La observación directa tuvo un papel central al permitir identificar la realidad de CEDEPA, apoyándose en una ficha diseñada específicamente con las categorías correspondientes a las variables de investigación, lo que facilitó la obtención de datos concretos con la ayuda de participantes claves.

Por otro lado, la entrevista fortaleció la recopilación de la información para poder obtener y analizar resultados, así mismo la muestra estuvo conformada por 6 colaboradores del Departamento de Cobranza de CEDEPA.

Triangulación de la información:

Pregunta	Participante 1	Participante 2	Participante 3	Cita	Autor
¿Qué tipo de datos personales se recolectan actualmente en el departamento de cobranza de CEDEPA?	Nombre, Número de cédula, Teléfono Y Correo Electrónico.	Se necesita todos los datos ya que son clientes directos.	Numero de cédula, nombres, dirección, teléfono, correo.	Según María Alejandra Vera Saltos y María Belén Vivero Andrade (2019), los datos personales constituyen información valiosa para las organizaciones, por lo que resulta necesario identificar qué tipo de información es recolectada y tratada dentro de los procesos empresariales.	Los informantes coinciden en que el departamento de cobranzas recopila datos como nombres, número de cédula, dirección, teléfono y correo electrónico, información indispensable para la gestión de los clientes. Este hallazgo guarda relación con lo que indica la teoría, quienes destacan el valor estratégico de los datos personales dentro de las organizaciones. Sin embargo, la recopilación de este tipo de información implica una responsabilidad institucional, puesto que un manejo ineficiente lo que podría afectar la privacidad de los titulares y generar incumplimientos legales relacionados con la protección de datos personales.
¿Cuáles son los medios y canales utilizados en la	De manera directa al cliente	Por medio de formularios, llamadas y sistema digital	formularios, tienen que llenar una solicitud de crédito	Los procedimientos de recogida de datos fueron clasificados hace años atendiendo a la presencia o	Los entrevistados manifiestan que la captura de la información se realiza mediante formularios, llamadas telefónicas y sistemas

recolección de los datos (formulario, llamadas, sistemas digitales etc.)?				no presencia física del entrevistador, dando lugar a procedimientos tradicionales como la entrevista personal, telefónica y postal; actualmente estos modos se han visto mejorados por nuevas tecnologías como encuestas electrónicas y sistemas digitales” (Díaz de Rada, 2024).	digitales, esto se apoya en lo que es indicado por Díaz de Rada (2024), pero si estos canales no tienen controles de seguridad y verificación efectivos, podrían presentarse errores en la recopilación de la información tales como: filtraciones, vulnerabilidad de los datos y a la confidencialidad de los clientes.
¿El cliente es informado sobre el uso que se dan a sus datos personales al momento de la recolección? ¿Como se realiza este proceso?	La recolección de datos es solo tributarios, los que pertenecen a la cartera son informados	Si es informado y se lo dicen por medio del formulario en la cual se le indican las formas de pagos y condiciones de uso de datos	Se hace conocer que sus datos serán utilizados como requisitos para el crédito de la empresa	Según la Ley Orgánica de Protección de Datos Personales, el titular debe ser informado de manera clara sobre el tratamiento y uso de sus datos personales al momento de su recolección, garantizando así un consentimiento informado y transparente.	Los participantes expresan que los clientes son informados sobre cómo se van a usar sus datos personales y sobre que mecanismo se recolectan ya sea mediante formularios y/o explicaciones relacionadas con los créditos otorgados, regentándose a la Ley Orgánica de Protección de Datos Personales. Sin embargo, es importante destacar que si la información proporcionada no cumple con los requisitos suficientes como: claridad, suficiente o verificable, podría vulnerarse el principio de consentimiento informado.
					Los colaboradores indicaron que en CEDEPA la información es almacenada tanto en formato

¿Qué procedimientos se siguen actualmente para almacenar y gestionar la información personal de los clientes?	Se almacenan en la base de datos del sistema power SAI	En la base de datos, por este medio verifican cualquier novedad para actualizar la información también	Se guardan física y digitalmente, el sistema lo manejan las personas que tienen acceso a las cobranzas	Según Gloria Ponjuán Dante (2011), la gestión de la información incluye procedimientos relacionados con el almacenamiento, organización y utilización de la información dentro de las organizaciones.	físico como digital, en sistema Power SAI, utilizando medidas de seguridad como el acceso restringido al personal autorizado, por tanto, esto se asemejan con las directrices de Ponjuán Dante (2011) sobre la gestión de la información. pero, es imperativo hacer énfasis que la falta de mecanismos avanzados para la protección de datos puede tener riesgos tales como: pérdida, alteración o acceso a los datos de manera incorrecta, comprometiendo la integridad y confidencialidad de la información.
¿Existen políticas internas o normativas institucionales relacionadas con la protección de datos personales?	Están en proceso de implementarlo	Si existe, ya que el cliente si es informado sobre el uso de sus datos	Si, se está planificando	Las organizaciones deben desarrollar políticas y procedimientos internos que orienten el tratamiento de los datos personales y aseguren el cumplimiento de las obligaciones legales en materia de protección de datos (ISO/IEC 27701, 2019).	Los puntos de vistas de los participantes evidencian que CEDEPA se encuentra en proceso implementar políticas de protección de datos personales, puesto que, aunque existe una intención de alinearse con la normativa, aun no se ha consolidado la ley formalmente, lo que podría generar inconvenientes en la gestión de la información.

¿Qué medidas de seguridad (técnicas o administrativas) se aplican para proteger los datos personales dentro del departamento?	Solo las personas que están a cargo tienen acceso a esos datos la cual cada uno tiene su usuario y contraseña	Usan claves para poder ver los datos de los clientes y no todos tienen acceso a dicha información	Se mantiene en documentos físicos y también la información que están almacenada en la base de datos es segura	El responsable del tratamiento deberá aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de los datos personales (Reglamento General de Protección de Datos, art. 32, 2016)	Los autores claves coinciden en que la protección de la información se basa principalmente en usuarios, contraseñas y restricciones de acceso. Sin embargo, de acuerdo con lo que indica la teoría la ausencia de medidas complementarias, como protocolos de seguridad, monitoreo permanente o cifrado de información, podría limitar la capacidad de respuesta frente a incidentes de seguridad y accesos no autorizados.
¿El personal recibe capacitación sobre la ley orgánica de datos personales y su aplicación? ¿Con que frecuencia?	Se está planificando las capacitaciones del personal	Si están planificando capacitación	Cada 6 meses se planifica dar capacitación	Según Chiavenato (2007), La Capacitación es el proceso educativo de corto plazo, aplicado de manera sistemática y organizada, por medio del cual las personas adquieren conocimientos, desarrollan habilidades y competencias en función de objetivos definidos.	Los entrevistados mencionan que la institución tiene previsto desarrollar capacitaciones periódicas sobre protección de datos personales. Este planteamiento coincide con la perspectiva de Chiavenato (2007), quien resalta la capacitación como un mecanismo para fortalecer conocimientos y competencias. No obstante, mientras estas actividades permanezcan únicamente en fase de

					planificación, el personal podría carecer de los conocimientos necesarios para aplicar correctamente la normativa, aumentando el riesgo de errores en el tratamiento de los datos personales.
¿Como se gestionan los accesos a la información personal dentro del departamento de cobranza?	El administrador de la base lo gestiona	En la base de datos se gestiona los datos	Con su respectivo usuario y contraseña solo tienen acceso	Las organizaciones necesitan contar con mecanismos que garanticen la disponibilidad de la información y el acceso seguro a las aplicaciones y recursos a través de múltiples sistemas (Montoya & Restrepo, 2012).	Los entrevistados coinciden en que el acceso a la información personal dentro del departamento de cobranzas se gestiona mediante bases de datos protegidas con usuarios y contraseñas, permitiendo el acceso únicamente al personal autorizado, la teoría señala que las organizaciones deben contar con mecanismos que garanticen el acceso seguro a la información y a los sistemas. No obstante, aunque el uso de usuarios y contraseñas representa una medida básica de control, no se evidencian mecanismos más avanzados de gestión y supervisión de accesos, lo que podría generar vulnerabilidades en la protección de los datos

					personales si no existen políticas de control, monitoreo y actualización permanente de la seguridad de los sistemas.
¿Cuáles consideras que son los principales riesgos o debilidades en el manejo actual de los datos personales en el departamento?	No hay riesgos porque cada uno tiene su usuario y contraseña	Hackeo de alguna información	No hay Porque todo está bajo control	La falta de controles adecuados en el tratamiento de datos personales puede generar riesgos relacionados con la pérdida, alteración, acceso no autorizado o divulgación indebida de la información (Ramírez, 2021).	Los participantes presentan opiniones divididas respecto a los riesgos en el manejo de los datos personales. Mientras algunos consideran que no existen riesgos debido al uso de usuarios y contraseñas y al control interno de la información, otro participante reconoce la posibilidad de hackeos o vulneración de los datos. Por lo que la teoría indica que la falta de controles adecuados puede generar riesgos como accesos no autorizados o divulgación indebida de la información. Desde un punto de vista analítico, las respuestas evidencian una percepción de confianza en las medidas actuales; sin embargo, considerar que no existen riesgos puede reflejar desconocimiento sobre las

					amenazas digitales y vulnerabilidades existentes en el tratamiento de datos personales. Por ello, aunque se aplican controles básicos de acceso, la institución aún podría estar expuesta a riesgos de seguridad informática si no fortalece sus mecanismos de protección y prevención.
¿Qué acciones o mejoras considera necesarias para fortalecer el cumplimiento de la ley orgánica de datos personales en CEDEPA?	Implementar la ley orgánica de protección de datos	A través de capacitación	Capacitaciones continuas	La protección de los datos personales no solo depende de un marco legal robusto, sino también de la implementación de buenas prácticas que minimicen los riesgos y garanticen el respeto de los derechos de los titulares (Velasco-Urgilés, Proaño-Reyes & Castro-Sánchez, 2025).	Los participantes expresan que una de las necesidades principales para mejorar y fortalecer el cumplimiento de la Ley Orgánica de Protección de Datos Personales en CEDEPA es la implementación de la normativa y que este acompañada de capacitaciones periódicas para el personal, y esto lo dice la teoría, quienes nos dan un mensaje importante que la protección de datos personales no es solo cumplimiento de normativa, sino también de una aplicación efectiva por parte de la empresa. Finalmente, se evidencia que la empresa tiene la necesidad de

					optimizar y fortalecer sus procesos internos en materia de protección de datos.
--	--	--	--	--	---

Análisis de resultados

En este apartado se detallan los resultados de los instrumentos aplicados, lo cual nos permiten constatar que la gestión de datos personales en el departamento de cobranzas de CEDEPA se encuentra en una fase de transición de una manera operativa tradicional y los nuevos requisitos establecidos por la Ley Orgánica de Protección de Datos de Datos Personales. Aunque la organización dispone de mecanismos básicos para la recopilación, almacenamiento y acceso a la información de sus clientes, la investigación evidencia que gran parte de estos procesos responden más a necesidades funcionales del negocio que a una estructura formal de protección de datos.

Uno de los aspectos más relevantes encontrados es la existencia de una cultura organizacional orientada al control operativo de la información, pero no necesariamente a la gestión integral de los riesgos asociados a los datos personales, lo que incide en la percepción de varios colaboradores, quienes perciben que las medidas actuales contribuyen de manera adecuada a la protección de la información. Sin embargo, dicha percepción contrasta con las exigencias normativas vigentes, las cuales requieren una gestión preventiva basada en políticas institucionales, evaluación de riesgos, capacitación continua y mecanismos de supervisión permanentes.

Asimismo, se evidenció una diferencia importante entre el conocimiento práctico y el conocimiento normativo. Los colaboradores conocen los procedimientos que ejecuta diariamente; sin embargo, las respuestas muestran limitaciones respecto a los principios y obligaciones establecidos por la legislación sobre protección de datos personales, lo que adquiere relevancia porque el desconocimiento de la normativa puede convertirse en una fuente de vulnerabilidad para la institución, puesto que dificulta la adopción de medidas acordes con las obligaciones legales y aumenta el riesgo de incumplimientos.

Durante la entrevista también quedó en evidencia que la organización es consciente de la necesidad de fortalecer la protección de los datos personales, razón por la cual ha considerado desarrollar capacitaciones, elaborar políticas internas y promover el cumplimiento de la normativa aplicable, por lo que estas acciones todavía se encuentran en una etapa inicial, de modo que persiste una diferencia importante entre lo que exige el marco legal y las prácticas que actualmente se ejecutan dentro de la institución.

Por otra parte, se identificó que las medidas de seguridad implementadas se concentran, en su mayoría, en controles básicos como la gestión de usuarios, el uso de contraseñas y las restricciones de acceso, por lo que es importante mencionar que estos mecanismos constituyen una primera barrera de protección, pero no responden por completo a los riesgos presentes en los entornos digitales actuales.

En términos institucionales, el problema principal no radica en la inexistencia de acciones para proteger la información, sino en que dichas acciones carecen de una estructura formal que las integre y estandarice, lo que trae como consecuencia, la protección de los datos personales depende en gran medida de procedimientos cotidianos y de los criterios de cada responsable, situación que puede generar diferencias en su aplicación, dificultar una respuesta oportuna frente a incidentes y reducir la capacidad de atender adecuadamente las exigencias de los organismos reguladores.

Conclusiones

1. La investigación permitió establecer que el departamento de cobranzas de CEDEPA recopila, almacena y utiliza datos personales como parte de los procesos vinculados con la gestión de créditos y la recuperación de cartera, pero estas actividades se

desarrollan principalmente con un enfoque operativo, sin contar con procedimientos formalmente estructurados que respondan de manera integral a las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales.

2. Los resultados evidencian que CEDEPA posee mecanismos de control básicos para resguardar la información, tales como el uso de credenciales de acceso, contraseñas, restricciones para el ingreso a los sistemas y el almacenamiento digital de los registros, no obstante, el no contar con políticas institucionales, protocolos documentados y medidas de seguridad más avanzada incide en la capacidad de la empresa para ofrecer una protección de los datos personales eficiente.
3. Finalmente, se identificó una actitud favorable por parte de los colaboradores y de la institución hacia el fortalecimiento del cumplimiento de la Ley Orgánica de Protección de Datos Personales reflejando interés por impulsar programas de capacitación, establecer políticas internas y reforzar los mecanismos destinados a proteger la información.

Recomendaciones

1. Establecer procedimientos específicos para la recolección, almacenamiento, uso y tratamiento de los datos personales, alineándolos con los principios y disposiciones establecidos en la Ley Orgánica de Protección de Datos Personales para permitir que las actividades relacionadas con la gestión de la

información se desarrollen por procesos definidos para fortalecer la transparencia y la seguridad en el tratamiento de los datos.

2. Fortalecer los mecanismos de protección de la información mediante la elaboración de políticas institucionales, la documentación de procedimientos internos y la implementación progresiva de medidas de seguridad técnicas y administrativas que permitan prevenir accesos no autorizados, pérdidas de información y posibles vulneraciones de los datos personales.

3. Implementar la propuesta de solución desarrollada en este estudio, como una herramienta estratégica para fortalecer la gestión y protección de los datos personales dentro del departamento de cobranzas de CEDEPA para favorecer el cumplimiento de la Ley Orgánica de Protección de Datos Personales

Referencias Bibliográficas

- Alulema Rosero, R. F. (2023). Diseño de una herramienta para la recolección de información de gestión preventiva de la seguridad y salud ocupacional utilizando indicadores según la normativa aplicable a las MiPymes del centro histórico del cantón Riobamba. <https://dspace.espoch.edu.ec/items/eb5d06b7-f7d6-497b-81e3-716e847dff72>
- Cevallos Mendoza, N. L. (2024). Cumplimiento normativo de la información como aplicación en la gestión de información en el departamento recursos humanos de la Universidad Laica Eloy Alfaro de Manabí Eloy Alfaro de Manabí, 2024. <https://repositorio.uleam.edu.ec/handle/123456789/6670>

Chavarri Holguin de Barandiaran, G. S. Implementación de estrategias para la recopilación de información de los auditores del Sistema Nacional de Control en la región Lambayeque.

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/96743/Chavarri_HDBG_S-SD.pdf?sequence=1&isAllowed=y

Chiavenato, I., Villamizar, G. A., & Aparicio, J. B. (2007). *Administración de recursos humanos* (Vol. 2). México: McGraw-hill.

Comisión Económica para América Latina y el Caribe. (2020). *Protección de datos personales y privacidad en América Latina y el Caribe*. CEPAL.

Constitución de la República del Ecuador. (2008). *Constitución de la República del Ecuador*. Registro Oficial N.º 449. Asamblea Nacional del Ecuador.

de Rada, V. D. (2000). Utilización de nuevas tecnologías para el proceso de "recogida de datos" en la investigación social mediante encuesta. *Reis*, 137-166.
<https://www.jstor.org/stable/40184278>

García Posada, J. D., & Rebellón González, L. I. (2022). *La Ley general de protección de datos de Colombia frente al reglamento general de protección de datos de la Unión Europea* (Bachelor's thesis, Derecho).
<https://repositorio.uceva.edu.co/bitstream/handle/20.500.12993/2833/T00032093.pdf?sequence=1&isAllowed=y>

Gelderman, M. (1999). The relation between user satisfaction, usage of information systems and performance. *Information & management*, 34(1), 11-18.

Gómez, J. (2007). *Seguridad de la información: fundamentos y gestión*. Alfaomega.

Hallberg, J., & Hunstad, H. (2005). *Information security management*. Wiley.

International Organization for Standardization. (2019). *ISO/IEC 27701:2019. Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines*. ISO.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3521250

Iza Noroña, L. M., & Mora Cedeño, G. A. (2023). *Análisis comparativo de la ley orgánica de protección de datos personales del Ecuador con la legislación mexicana desde un enfoque de ciberseguridad y delitos informáticos* (Master's thesis).

<https://dspace.ups.edu.ec/bitstream/123456789/26605/1/UPS-CT011043.pdf>

Laudon, K. C., & Laudon, J. P. (2016). *Management information systems: Managing the digital firm* (14th ed.). Pearson Education.

Ley Orgánica de Protección de Datos Personales. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento N.º 459. Asamblea Nacional del Ecuador.

Mero Delgado, E. J. (2024). Análisis de la gestión documental y recopilación de información en la gerencia general de la empresa “Aseo integral de Montecristi EP” año 2022.

<https://repositorio.ulead.edu.ec/bitstream/123456789/5622/1/ULEAM-GIG-056.pdf>

Montoya, J. A., & Restrepo, Z. (2012). Gestión de identidades y control de acceso desde una perspectiva organizacional. *Ingenierías USBMed*, 3(1), 23-34.

<https://revistas.usb.edu.co/index.php/IngUSBmed/article/view/261>

Ponjuán Dante, G. (2011). *La gestión de información y sus modelos representativos. Valoraciones*. Revista Ciencias de la Información, 42(2), 11–17.

Ramírez, Y. A. R. (2021). Importancia de las estrategias de enseñanza aprendizaje en la formación de estudiantes de nivel superior. *Revista Docencia Universitaria*, 2(1), 23-31. <https://revistadusac.com/index.php/revista/article/view/21>

Regulation, P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Regulation (eu)*, 679(2016), 10-3.
https://dvbi.ru/Portals/0/DOCUMENTS_SHARE/RISK_MANAGEMENT/EBA/GDP_R_eng_rus.pdf

Saltos, M. A. V., & Andrade, M. B. V. (2019). ¿Vida privada o muerte a la privacidad? Protección de datos personales en la relación empresa-cliente en Ecuador. *USFQ Law Review*, 6(1), 233-256.
<https://revistas.usfq.edu.ec/index.php/lawreview/article/view/1397/1623>

Sevilla Moncayo, J. (2024). *La aplicación de la Ley Orgánica de Protección de Datos Personales en las organizaciones ecuatorianas*. [Tesis de grado o publicación académica]. Institución editora.

Velasco-Urgilés, S. G., Proaño-Reyes, G. M., & Castro-Sánchez, F. D. J. (2025). Buenas prácticas para la protección de datos personales. *Noesis*, 7(ESP2), 794-813.
https://ve.scielo.org/scielo.php?pid=S2739-03652025000400794&script=sci_arttext

Anexos

Anexo 1: Ficha de observación

Ficha de Observación

Objetivo: Observar el cumplimiento de la Ley de Protección de Datos Personales y los procedimientos utilizados durante la Recolección de Información para gestionar la información.

Observador: _____

Fecha: _____

Lugar: _____

Hora de inicio: _____ **Hora de término:** _____

Categoría: Ley de Protección de Datos Personales

Nº	Pregunta de Observación	Sí	No	Observaciones
1	¿Se informa a las personas sobre la finalidad de la recolección de sus datos?	☐	X	Se les informa solo cuando ellos preguntan
2	¿Se solicita consentimiento previo para recolectar datos personales?	☐	X	
3	¿Se especifica qué tipo de datos personales serán recolectados?	Si ☐	☐	Se les pide numero de cedula, dirección, Correo, nombres y celular
4	¿Se informa a los usuarios sobre sus derechos respecto al uso y tratamiento de sus datos?	☐	X	
5	¿Los datos recolectados se manejan con medidas de confidencialidad?	X ☐	☐	Se guarda en la base de datos y son confidenciales
6	¿Existen medidas visibles para garantizar la seguridad de la información recolectada?	☐	X	

Nota: Corresponden a las preguntas relacionadas a la variable Ley de Protección de Datos Personales

Categoría: Recolección de Información

Nº	Pregunta de Observación	Sí	No	Observaciones
7	¿Existe un sistema o protocolo establecido para gestionar la información recolectada?	☐	X	
8	¿La información recolectada se almacena de manera segura (física o digitalmente)?	X ☐	☐	La información es almacenada física y digitalmente
9	¿Se controla quién accede a la información almacenada?	X ☐	☐	Solo el supervisor y el area de contabilidad tienen acceso
10	¿La información se utiliza exclusivamente para los fines para los que fue recolectada?	X ☐	☐	
11	¿Se realiza alguna acción de seguimiento, actualización o eliminación de la información recolectada?	☐	X	

12	¿El personal que gestiona la información está capacitado en protección de datos y competencias informacionales para la protección de la información?	X	☐	Se esta realizando el proceso de capacitación
----	--	---	--------------------------	---

Nota: Corresponden a las preguntas relacionadas a la variable Recolección de Información

Anexo 2: Entrevista

Entrevista

Título del estudio: Aplicación de la Ley Orgánica de Protección de Datos Personales en la Recolección de Información

Objetivo de la entrevista:

Recopilar, con fines estrictamente académicos, información relevante sobre el nivel de conocimiento, aplicación y cumplimiento de la Ley Orgánica de Protección de Datos Personales en los procesos de recolección de información, garantizando que los datos obtenidos serán utilizados únicamente para el desarrollo de la presente investigación.

Datos del entrevistado Nombre completo: Edad:

Género:

Cargo o profesión:

Años de experiencia laboral:

Fecha de la entrevista:

Preguntas de la entrevista

1. ¿Qué tipo de datos personales se recolectan actualmente en el departamento de cobranza de CEDEPA?
2. ¿Cuáles son los medios y canales utilizados en la recolección de los datos (formulario, llamadas, sistemas digitales etc.)?
3. ¿El cliente es informado sobre el uso que se dan a sus datos personales al momento de la recolección? ¿Como se realiza este proceso?
4. ¿Qué procedimientos se siguen actualmente para almacenar y gestionar la información personal de los clientes?
5. ¿Existen políticas internas o normativas institucionales relacionadas con la protección de datos personales?
6. ¿Qué medidas de seguridad (técnicas o administrativas) se aplican para proteger los datos personales dentro del departamento?
7. ¿El personal recibe capacitación sobre la ley orgánica de datos personales y su aplicación? ¿Con que frecuencia?
8. ¿Como se gestionan los accesos a la información personal dentro del departamento de cobranza?

9. ¿Cuáles consideras que son los principales riesgos o debilidades en el manejo actual de los datos personales en el departamento?
10. ¿Qué acciones o mejoras considera necesarias para fortalecer el cumplimiento de la ley orgánica de datos personales en CEDEPA?

Anexo 3: Entrevistas al personal de Cedepa



Nota: Corresponden a las fotografías tomadas dentro del campo de estudio

Propuesta

Sistema Integral de Gestión y Protección de Datos Personales basado en la Ley Orgánica de Protección de Datos Personales para el departamento de cobranzas de CEDEPA

Introducción

La protección de los datos personales constituye un elemento estratégico dentro de la gestión organizacional, debido a que las empresas manejan información sensible de clientes, proveedores y colaboradores que requiere ser administrada bajo principios de seguridad, confidencialidad, transparencia y responsabilidad.

De acuerdo con lo que se evidencio en el presente estudio, el departamento de cobranzas de CEDEPA desarrolla procesos relacionados con la gestión de la información como: recopilación, almacenamiento y tratamiento de datos personales, no obstante, se identificaron oportunidades de mejora relacionadas con la falta de procedimientos formalizados, políticas internas documentadas, mecanismos de seguimiento y fortalecimiento del capital humano en la aplicación de la normativa.

Como respuesta a esta necesita se plantea la solución a través de la implementación de un Sistema Integral de Gestión y Protección de Datos Personales, el cual está orientado a fortalecer el cumplimiento normativo, establecer lineamientos internos para el tratamiento de la información y reducir los riesgos asociados con la gestión de la información en CEDEPA.

La propuesta contempla varios componentes que trabajan de manera complementaria y sincronizada entre ellos se encuentran: el consentimiento informado, transparencia en el uso de la información, gestión documental, capacitación del personal, controles de seguridad y mecanismos de control.

Objetivo General

Fortalecer el cumplimiento de la Ley Orgánica de Protección de Datos Personales mediante la implementación de un Sistema Integral de Gestión y Protección de Datos Personales que permita mejorar los procesos de recolección, tratamiento, almacenamiento y seguridad de la información en el departamento de cobranzas de CEDEPA.

Objetivos específicos de la propuesta

- Establecer procedimientos internos para la recolección, almacenamiento, actualización y tratamiento de datos personales.
- Implementar mecanismos de consentimiento informado y transparencia para garantizar los derechos de los titulares de la información.
- Diseñar políticas internas orientadas a la protección y seguridad de los datos personales.
- Fortalecer las competencias del personal mediante procesos permanentes de capacitación.
- Implementar mecanismos de seguimiento y evaluación del cumplimiento de las medidas adoptadas.

Componentes del Sistema Integral de Gestión y Protección de Datos Personales

Componente 1. Diagnóstico y planificación del tratamiento de datos personales

Actividades:

- Identificación de los tipos de datos personales recopilados por CEDEPA.
- Clasificación de la información según nivel de sensibilidad.
- Identificación de responsables del tratamiento de datos.
- Revisión de formularios, sistemas y documentos utilizados actualmente.

- Identificación de riesgos asociados al manejo de información.

Producto esperado:

Informe de diagnóstico del tratamiento de datos personales en el departamento de cobranzas.

Componente 2: Gestión de Políticas internas y Procedimientos

Actividades:

- Elaboración de documentos
- Política interna de protección de datos personales.
- Procedimientos de recopilación y almacenamiento de información.
- Procedimientos de actualización y eliminación de datos obsoletos.
- Procedimientos de gestión de solicitudes de los clientes.
- Procedimientos de respuesta sobre riesgo de datos.

Resultados esperados:

Manual interno para la gestión y protección de datos personales.

Componente 3: Consentimiento Informado y Sistema de Transparencia Digital

Actividades:

- Diseño de formularios de consentimiento informado.
- Elaboración de declaraciones de privacidad.
- Definición sobre la finalidad del tratamiento de datos.
- Establecimiento de registro digital de consentimiento.
- Implementación de procesos de elaboración de normas que informen a

los

usuarios y documenten sus necesidades.

Resultados esperados:

Sistema de consentimiento informado, tanto escrito como digital.

Componente 4:

Actividades: Fortalecimiento de la seguridad de la información

- Revisión de los permisos para acceder al sistema.
- Actualización constante de nombres de credenciales.
- Definir las descripciones y responsabilidades de los cargos.
- Gestionar documentos físicos y digitales.
- Establecer copias de seguridad de los datos.
- Realizar evaluaciones continuas de vulnerabilidades.

Resultados esperados:

Matriz de control de acceso a la información y seguridad.

Componente 5. Capacitación y cultura organizacional

Actividades:

- Impartir capacitación sobre lo siguiente:
- Principios de la Ley de Protección de Datos Personales.
- Derechos de los titulares de los datos.
- Manejo adecuado de los datos personales.
- Riesgos asociados con las filtraciones de datos o el acceso no

autorizado.

- Mejores prácticas de seguridad digital.

Resultados esperados:

Competencia y sensibilidad individual.

Componente 6. Seguimiento y mejora continua

- **Actividades:**
- Evaluación periódica del cumplimiento de procedimientos.

- Auditorías internas sobre manejo de información.
- Revisión de registros de consentimiento.
- Actualización de políticas según cambios normativos.
- Elaboración de informes de mejora.

Producto esperado:

Informe periódico de cumplimiento y mejora continua.

Responsables de implementación

Área	Responsabilidad
Gerencia General	Aprobar la propuesta, asignar recursos y supervisar cumplimiento
Departamento de Cobranzas	Aplicar procedimientos, gestionar consentimiento y custodiar información
Área Administrativa	Control documental y actualización de políticas
Área de Sistemas	Seguridad tecnológica, accesos y respaldo de información
Personal operativo	Cumplimiento de procedimientos establecidos

Indicadores de evaluación

Indicador	Meta esperada
Personal capacitado en protección de datos	100% del personal involucrado
Procedimientos documentados implementados	100%
Clientes con consentimiento informado registrado	≥95%
Revisiones de seguridad realizadas	Trimestralmente
Incidentes de acceso no autorizado	Reducción progresiva

Beneficios esperados

Institucionales

- Mayor cumplimiento de la Ley Orgánica de Protección de Datos Personales.
- Reducción de riesgos legales y administrativos.
- Fortalecimiento de la gestión de información institucional.

Operativos

- Estandarización de procesos relacionados con datos personales.
- Mayor control documental.
- Mejor administración de accesos y responsabilidades.

Cientes

- Mayor transparencia sobre el uso de su información.
- Protección de sus derechos como titulares de datos.
- Incremento de la confianza hacia CEDEPA.