



**UNIVERSIDAD TECNOLÓGICA ISRAEL  
ESCUELA DE POSGRADOS “ESPOG”**

**MAESTRÍA EN SEGURIDAD INFORMÁTICA**

*Resolución: RPC-SO-02-No.053-2023*

**PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER**

<b>Título del proyecto:</b>
PROPUESTA DE MODELO EVALUADOR DE CUMPLIMIENTO DE LA NORMATIVA DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR.
<b>Línea de Investigación:</b>
Sistemas de información e Informática.
<b>Campo amplio de conocimiento:</b>
Tecnologías de la Información y la Comunicación (TIC)
<b>Autor:</b>
Chavez Mora Arthur Wilson
<b>Tutor:</b>
Mg. Recalde Varela Pablo Marcel

**Quito – Ecuador**

**2023**

## APROBACIÓN DEL TUTOR



Yo, PABLO MARCEL RECALDE VARELA con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: PROPUESTA DE MODELO EVALUADOR DE CUMPLIMIENTO DE LA NORMATIVA DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR.

Elaborado por: ARTHUR WILSON CHAVEZ MORA, de C.I: 0929613230, estudiante de la Maestría: SEGURIDAD INFORMÁTICA, de la UNIVERSIDAD TECNOLÓGICA ISRAEL, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2023

**Firma**

**ORCID: 0000-0001-7256-2836**

## DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE



Yo, ARTHUR WILSON CHAVEZ MORA con C.I: 0929613230, autor del proyecto de titulación denominado: PROPUESTA DE MODELO EVALUADOR DE CUMPLIMIENTO DE LA NORMATIVA DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR. Previo a la obtención del título de Magister en seguridad de la información.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al modelo Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2023

Firma

ORCID: 0000-0001-7600-345

## Índice de Contenido

APROBACIÓN DEL TUTOR .....	ii
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE .....	iii
INFORMACIÓN GENERAL .....	1
Contextualización del tema .....	1
Problema de investigación .....	1
Objetivo general .....	2
Objetivos específicos .....	2
Vinculación con la sociedad y beneficiarios directos: .....	3
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO .....	4
1.1. Contextualización general del estado del arte .....	4
1.2. Proceso investigativo metodológico .....	5
1.3. Análisis de resultados .....	6
CAPÍTULO II: PROPUESTA .....	7
2.1 Fundamentos teóricos aplicados .....	7
2.2 Descripción de la propuesta .....	9
2.3 Validación de la propuesta .....	17
2.4 Matriz de articulación de la propuesta .....	19
CONCLUSIONES .....	21
RECOMENDACIONES .....	22
BIBLIOGRAFÍA .....	23
ANEXOS .....	25

## Índice de tablas

<b>Tabla 1.</b> Contextualización de los tipos de datos personales. ....	7
<b>Tabla 2.</b> Tabla de las métricas de evaluación .....	10
<b>Tabla 3.</b> Preguntas en base a los principios de la LOPDP. ....	14
<b>Tabla 4.</b> Preguntas en base a los derechos titulares. ....	16
<b>Tabla 5.</b> Matriz de articulación. ....	19

## Índice de figuras

<b>Figura 1.</b> Definición de dato personal de la DINARP .....	8
<b>Figura 2.</b> Valoración de una pregunta cerrada.....	11
<b>Figura 3.</b> Valoración de pregunta de opción múltiple.....	11
<b>Figura 4.</b> Preguntas condicionales y de valoración dividida.....	12
<b>Figura 5.</b> Principios de la LOPDP.....	13

## **INFORMACIÓN GENERAL**

En el mundo digital actual, se ha experimentado un avance extraordinario que ha beneficiado enormemente el desarrollo de la humanidad en términos de comunicación, accesibilidad a la información y globalización, no obstante es objeto de un riesgo que perjudica significativamente a los usuarios en términos de privacidad.

### **Contextualización del tema**

Con el advenimiento de esta nueva era tecnológica, el tratamiento de datos masivos de personas se ha convertido en uno de los insumos tecnológicos más fundamentales. Inicialmente, esto no suponía un problema, pero con el tiempo, esta práctica ha dado lugar a numerosos casos de venta y mal manejo de información sensible de los ciudadanos, traspasando los límites legales y vulnerando el derecho a la privacidad de aquellos individuos que, por diversas razones, comparten sus datos confiando en que las empresas los utilizarán de manera legítima como el caso de filtración de datos de Ecuador en el 2019 (El Universo, 21, octubre, 2019).

De acuerdo con Álvarez (2021) En el entorno actual, se vuelve esencial afrontar de manera completa y eficaz la cuestión de resguardar la información personal. Se requiere implementar sistemas que posibiliten la evaluación y garantía del acatamiento de las leyes en vigor. La sugerencia de un modelo evaluativo para verificar el acatamiento de las regulaciones de seguridad de la información personal emerge como una herramienta esencial, permitiendo que las entidades tomen conciencia de su obligación y perfeccionen sus procedimientos en salvaguardar la confidencialidad de los usuarios y clientes.

La salvaguardia de información personal abarca aspectos legales, éticos y sociales. Garantizar el dominio y la privacidad de la información de índole personal es un derecho esencial de cada individuo. Por lo tanto, este trabajo se enfoca en presentar un modelo de valoración de la salvaguardia de información en territorio ecuatoriano, fomentando la garantía y la sensación de protección al utilizar tecnologías de información, al mismo tiempo que impulsa el respeto hacia los derechos fundamentales de los ciudadanos ecuatorianos. (Guamán, 2019)

### **Problema de investigación**

En el contexto empresarial y organizacional, la recopilación de datos de clientes, proveedores y trabajadores es una necesidad fundamental. Sin embargo, la falta de conocimiento sobre los procesos adecuados para manejar esta información puede llevar a que muchas instituciones en Ecuador no cumplan con la normativa legal vigente.

Según DINARP (2021), a partir del 10 de mayo de 2021, el gobierno de Ecuador, durante la sesión completa de la Asamblea Nacional con respaldo de ciento dieciocho votos a favor, se dio luz verde a la LOPDP (Ley Orgánica de Protección de Datos Personales) normativa impulsada por la Dirección Nacional de Registros Públicos (DINARP), ley que promueve las buenas prácticas y el tratamiento correcto de información personal, no obstante numerosas empresas desconocen los principios y derechos plasmados en la ley a la que están sujetos, lo que resulta en un incumplimiento de la legislación y plantea problemas legales significativos.

Mediante la investigación y presentación de un enfoque evaluativo para asegurar el seguimiento de las normativas de resguardo de datos en el entorno de Ecuador, se persigue entregar las bases de una herramienta concreta y eficaz para que las organizaciones puedan valorar su nivel de acatamiento y adoptar medidas adecuadas destinadas a preservar la privacidad y resguardo de información personal, Igualmente, se tiene como objetivo fomentar la comprensión de la importancia de la protección de datos y estimular una cultura de observancia legal en la gestión de información en el sector empresarial del país.

¿Con la propuesta del modelo, se puede evaluar el nivel de incumplimiento de la LOPDP por parte de las empresas en Ecuador?

### **Objetivo general**

Proponer un modelo de evaluación que evidencia el cumplimiento de la LOPDP en Ecuador.

### **Objetivos específicos**

- Contextualizar la legislación vigente acerca de la salvaguardia de información personal en el contexto ecuatoriano, identificando principios y derechos de los titulares.
- Definir los criterios y parámetros clave, basado en las regulaciones referentes a la salvaguardia de la información personal, considerando aspectos técnicos, organizativos y legales.
- Desarrollar un modelo de evaluación, que permita a las organizaciones autoevaluarse y que refleje su nivel de cumplimiento ante la ley.
- Validar el modelo propuesto mediante la observación de especialistas en la (LOPDP) sobre su aplicabilidad en organizaciones ecuatorianas sujetas a la normativa.

**Vinculación con la sociedad y beneficiarios directos:**

Este proyecto tiene una conexión directa con la sociedad y puede tener un impacto significativo en múltiples aspectos. Al abordar un tema actual y relevante como el resguardo de información personal de la ciudadanía.

El modelo evaluativo planteado ofrece una herramienta concreta que puede contribuir a elevar la administración de los datos y reforzar la salvaguardia de la información personal. Dado que la privacidad y resguardo de los datos son inquietudes compartidas por individuos, empresas y entidades por igual, este enfoque tiene el potencial de generar un impacto positivo en la sociedad ecuatoriana al promover una mayor conciencia en torno a la seguridad de la información personal.

Al mejorar temas de protección y privacidad de datos, los derechos de millones de ciudadanos se protegen y se crea un entorno de confianza en el uso de servicios digitales, esto conlleva un crecimiento en la usabilidad de la tecnología ampliando la demanda creando una cultura digital en el país.

Según la DINARP (2021), en Ecuador, con la LOPDP, cada titular tiene derecho a tomar decisiones sobre el uso de su información además de conocer los fines específicos de los negocios y proveedores de servicios digitales. Esta iniciativa refleja un compromiso con el ODS dieciséis, que promueve sociedades pacíficas, justas e inclusivas. Al asegurar que los individuos mantengan dominio sobre su información personal y estén informados sobre su uso, ayuda a construir un entorno digital más ético y transparente, generando así confianza en las organizaciones y promoviendo la equidad en la era digital.

## **CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO**

En cada una de las empresas, instituciones y organizaciones por el contexto actual del crecimiento y auge de la cultura digital se ven envueltas en tratar datos, lo que conlleva un reto para cada una de estas entidades, en infraestructura, en procesos y en seguridad.

### **1.1. Contextualización general del estado del arte**

La seguridad siendo uno de los tópicos más relevantes de la actualidad, se ha visto envuelta en una evolución con la incursión de los departamentos de TI en la estructuras organizacionales, el desafío radica en la contextualización y concientización sobre los conceptos de seguridad y privacidad en todas las áreas sobre cómo manejar los datos, respetando los estándares y principios de privacidad de sus usuarios, lo que nos lleva al cumplimiento de una normativa de la cual su propósito principal es asegurar todo derecho e integridad de los datos personales de todos los ecuatorianos (Cano, 2012).

Es muy común escuchar hoy en día términos como “Big Data”, “Machine learning” y minería de datos, términos fuertemente utilizados para referirnos a un conjunto de datos que después de un proceso se puede convertir en información relevante, en la contextualización de la problemática planteada nos enfocaremos específicamente en la obtención de estos insumos y lo que implica para los usuarios a nivel de seguridad y privacidad, para ello debemos tener claro algunos conceptos.

Carrión (2017) define al dato como una entidad distinta acerca de un acontecimiento verídico que en el ámbito de las empresas, esto se amplía como un registro de transacciones, la importancia del almacenamiento de datos radica en solo almacenar datos que tengan relevancia y que se presten con un punto de conexión en común para convertirse en información descartando los que no tienen sentido, dicho dato solo representa una fracción de lo que realmente existe en la realidad, es como si fueran las pistas que necesitamos para encontrar una verdad en nuestra búsqueda del conocimiento.

Dentro de la tipología de los datos hay uno del cual en los últimos años ha dejado varios antecedentes sobre su manejo y tratamiento viendo involucrado a varias empresas en problemas legales, hablamos de los datos personales, bajo consulta el 8 de julio a la Comisión Europea (s.f.) la información personal se considera como cualquier dato vinculado a una persona, que esté identificada o pueda ser identificable. Esto incluye diversas informaciones que, al ser recopiladas en conjunto, podrían conducir a la identificación de una persona.

En contraste cuando se habla de datos, nos resulta difícil no asociarlos a la privacidad según Posey (2021) la privacidad es cuando alguna institución o individuo debe determinar cuándo un dato se puede compartir con terceros, además de limitar el número de individuos que tiene acceso a dicho dato, por último define a la privacidad como una actitud proactiva por parte de estas entidades para prevenir el acceso de no autorizado asegurando que los datos estén respectivamente cubierto y no sean fácilmente leídos.

Es fundamental destacar que, considerando estos conceptos, en Ecuador antes del 2019 se prestaba escasa atención al significado de los derechos relacionados con los datos que un individuo pudiera proporcionar.

Aunque en otras naciones ya se habían presentado casos en los que la confidencialidad y protección de la información eran cuestiones recurrentes, no fue sino hasta la filtración más notable dentro del país que la conciencia sobre la relevancia de proteger los datos de los ciudadanos comenzó a surgir.

«Ecuador tiene menos de 17 millones de habitantes y, según una firma de seguridad, la mayoría de los datos personales de casi todos ellos han sido expuestos.» (BBC News Mundo, 16, septiembre, 2019).

## **1.2. Proceso investigativo metodológico**

Para el desarrollo de esta propuesta se utilizaron varios tipos de investigación, que aportará validez y veracidad al proyecto los cuales se detallaran a continuación:

Con sustento de los conceptos empleados, se hizo uso de la investigación bibliográfica en donde se ha citado la opinión y criterio de otros investigadores como lo define Serrano (2016) como series de acciones orientadas a ubicar y recuperar archivos vinculados a un tópico, un autor o un campo específico del conocimiento. Una bibliografía consiste en un listado de referencias consultadas en la construcción de un escrito, donde indica la fuente original para reforzar un argumento y comparar sobre el análisis de otros autores.

La investigación cualitativa es de gran relevancia en este proyecto, dado que el fin clave es evaluar el grado de adhesión de las empresas a las regulaciones de protección de datos. se vuelve indispensable tomar en cuenta la opinión y el criterio de expertos sobre la seguridad informática y la aplicación de la LOPDP, según Cueto, (2020) la investigación cualitativa se adentra en la esencia misma de la comprensión humana dicha investigación se sumerge en la rica diversidad de perspectivas subjetivas que cada individuo aporta a su exploración del mundo.

### **1.3. Análisis de resultados**

Como resultado de este proyecto, se expone la lógica de evaluación que emplea preguntas específicas, basadas en propios indicadores referenciados en la normativa, para demostrar el cumplimiento de la ley. Esta metodología se fundamenta principalmente en los principios y derechos de la LOPDP. Se proyecta como una solución parcial hasta que la reglamentación oficial de aplicabilidad entre vigencia, por parte de la DINARP.

El proyecto ofrece a las empresas una guía automatizada a través de un cuestionario que evalúa su nivel de cumplimiento. Proporciona información detallada sobre los artículos correspondientes y sugiere enfoques para mantenerse al tanto de las nuevas disposiciones a nivel nacional.

Para demostrar la eficacia y validez de la lógica de evaluación de la propuesta, se definirán indicadores de cumplimiento que abarquen los aspectos cruciales que las empresas deben respetar. Importante mencionar que la valoración de este proyecto está basada en la visión de expertos especializados ciberseguridad y en el cumplimiento de la LOPDP.

## CAPÍTULO II: PROPUESTA

En este capítulo se detalla a profundidad los conceptos consultados aplicado a la propuesta del modelo, se aborda el desarrollo lógico de evaluación y los sustentos vinculados a los artículos de la ley.

### 2.1 Fundamentos teóricos aplicados

#### Datos Personales

En la búsqueda de la información y el conocimiento, se recepta como único insumo de alimentación los denominados datos, estos los existen de varios tipos dependiendo su aplicabilidad, en el contexto de este proyecto solo se enfocará en los datos personales que su vez tiene ramificaciones en su definición como lo detalla el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios INFOEM en el 2019.

#### Tabla 1.

*Contextualización de los tipos de datos personales.*

Tipo	Descripción
Identificación	Datos que identifican o vuelven identificable a una persona.
Laborales	Datos relacionados con solicitudes de empleo o referencia a las actividades laborales de una persona.
Patrimoniales	Datos vinculados al estado económico de una persona, responsabilidad fiscal y patrimonio a nombre de dicho individuo.
Administrativos y jurisdiccionales	Información que tiene estrecha relación con una persona física, ya sea en procedimientos administrativos o en el ámbito laboral, civil, penal, tributario, comercial o de cualquier otra disciplina legal.
Académicos	Datos que identifican el historial académico y de formación.
Tránsito y movimiento migratorio	Información necesaria para libre tránsito dentro y fuera de un país

*Nota.* \*No incluye datos personales sensibles. Fuente: INFOEM



Art. 133.- Las leyes serán orgánicas y ordinarias.

Serán leyes orgánicas:

1. Las que regulen la organización y funcionamiento de las instituciones creadas por la Constitución.
2. Las que regulen el ejercicio de los derechos y garantías constitucionales.
3. Las que regulen la organización, competencias, facultades y funcionamiento de los gobiernos autónomos descentralizados.
4. Las relativas al régimen de partidos políticos y al sistema electoral. (CRE, 2008)

### **Ley Orgánica de Protección de Datos Personales**

Con la LOPDP se busca cuidar los derechos de los titulares, otorgando el poder de decisión de a quien entregar su información personal y tener la confianza del tratamiento por parte de las entidades que receipten dichos datos.

Esta ley cuenta con trece principios que las entidades cuyas funciones dependen de la captura de información personal de clientes, proveedores y trabajadores debe cumplir, además catorce derechos que protegen a los ciudadanos de la forma en la que usen su información.

Según la UASB (2021) Este reglamento no solo revoluciona la seguridad de datos personales a nivel global, sino también ocasiona cambios significativos en la industria de la seguridad de la información, ya que se fundamenta en la gestión de riesgos.

### **2.2 Descripción de la propuesta**

Es innegable que la ley introduce múltiples directrices y un nuevo enfoque en cuanto a lo que verdaderamente se entiende por seguridad de la información, especialmente en relación a la seguridad de los datos personales. En este sentido, es evidente que muchas instituciones del ámbito privado no poseen un conocimiento profundo de los principios que deben adoptar, modificar e implementar en sus métodos para garantizar el acatamiento de las regulaciones. A continuación, se presenta la siguiente propuesta detallada para abordar esta situación.

Para poder decir que una entidad cumple con lo planteado en LOPDP debe existir en principio una etapa de evaluación, con el fin de no depender al cien por ciento de un consultor externo, se propone de diseño del modelo que permite a las entidades por medio de preguntas sabes cuales son específicamente las deficiencias en los procesos y seguridad en el tratamiento de datos.

## Métricas de evaluación

Se toman en cuenta cuatro parámetros que posibilitarán a valoración del nivel de acatamiento de la pregunta planteada. Estos parámetros van desde uno que no se cumple hasta cinco que se cumplen en su totalidad. A continuación, se ofrece una tabla que detalla las métricas correspondientes.

**Tabla 2.**

*Tabla de las métricas de evaluación*

<b>Indicador</b>	<b>Descripción</b>
No se cumple en absoluto	Indica que no se ha establecido ningún proceso ni conocimiento de las exigencias establecidas por la normativa. No se han implementado acciones para satisfacer los requisitos legales.
En proceso de implementación	Refleja que se están realizando esfuerzos iniciales para implementar medidas conforme a la normativa, aunque aún hay un largo camino por recorrer para alcanzar el cumplimiento total.
Progreso significativo hacia el cumplimiento	Muestra que se han tomado medidas sustanciales para cumplir con la normativa, evidenciando avances notables en la implementación, pero aún quedan aspectos por resolver.
Cumple parcialmente con éxito	Indica que se han adoptado medidas que han logrado un cumplimiento parcial de los requisitos, aunque todavía hay aspectos que deben mejorarse o ajustarse para estar completamente en línea con la normativa.
Cumple completamente y con total eficacia	Demuestra que se han implementado procesos sólidos y se ha logrado cumplir plenamente con todos los aspectos requeridos por la normativa, demostrando una adhesión efectiva y completa a los estándares legales.

*Nota.* Estas métricas se usan en las preguntas del modelo según la necesidad.

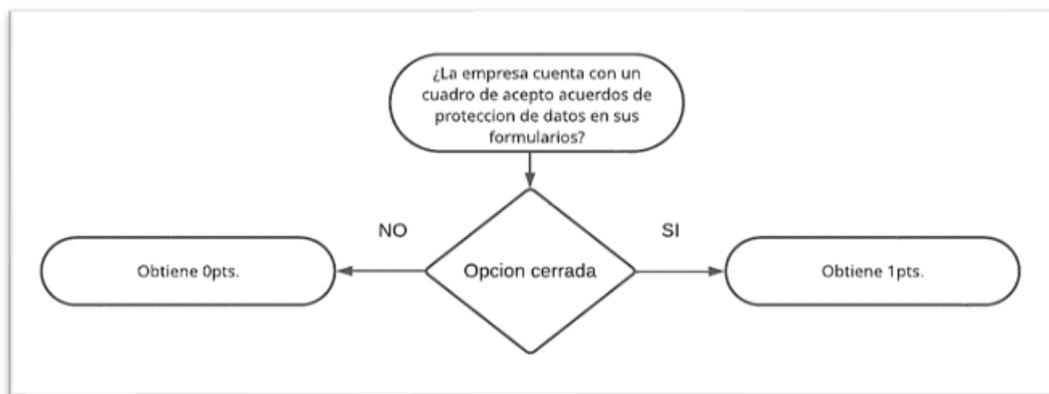
## Valoración y forma de calificación

Existirán tres formas de puntuar las preguntas, dado que esto va a depender del alcance de la misma eso quiere decir que no todas las preguntas tienen la misma valoración, puesto que pueden ser condiciones, de opción cerrada o de opción múltiple, la puntuación máxima por pregunta es de un punto y la mínima es de cero a continuación de presentar los tres posibles casos de valoración.

**Caso uno:** Cuando una de las preguntas tiene una pregunta de opción cerrada de si o no la valoración se lleva de la siguiente manera.

**Figura 2.**

*Valoración de una pregunta cerrada.*

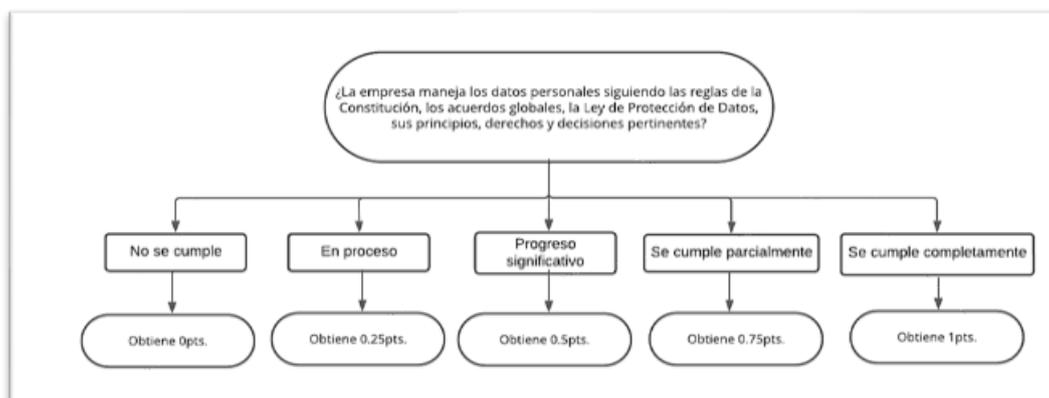


*Nota.* Todas las preguntas de este tipo solo obtienen dos posibles resultados

**Caso dos:** Cuando una pregunta tiende a una interpretación de varios aspectos o contempla varios puntos dentro de la misma se utilizará las opciones múltiples, como se muestra a continuación.

**Figura 3.**

*Valoración de pregunta de opción múltiple.*

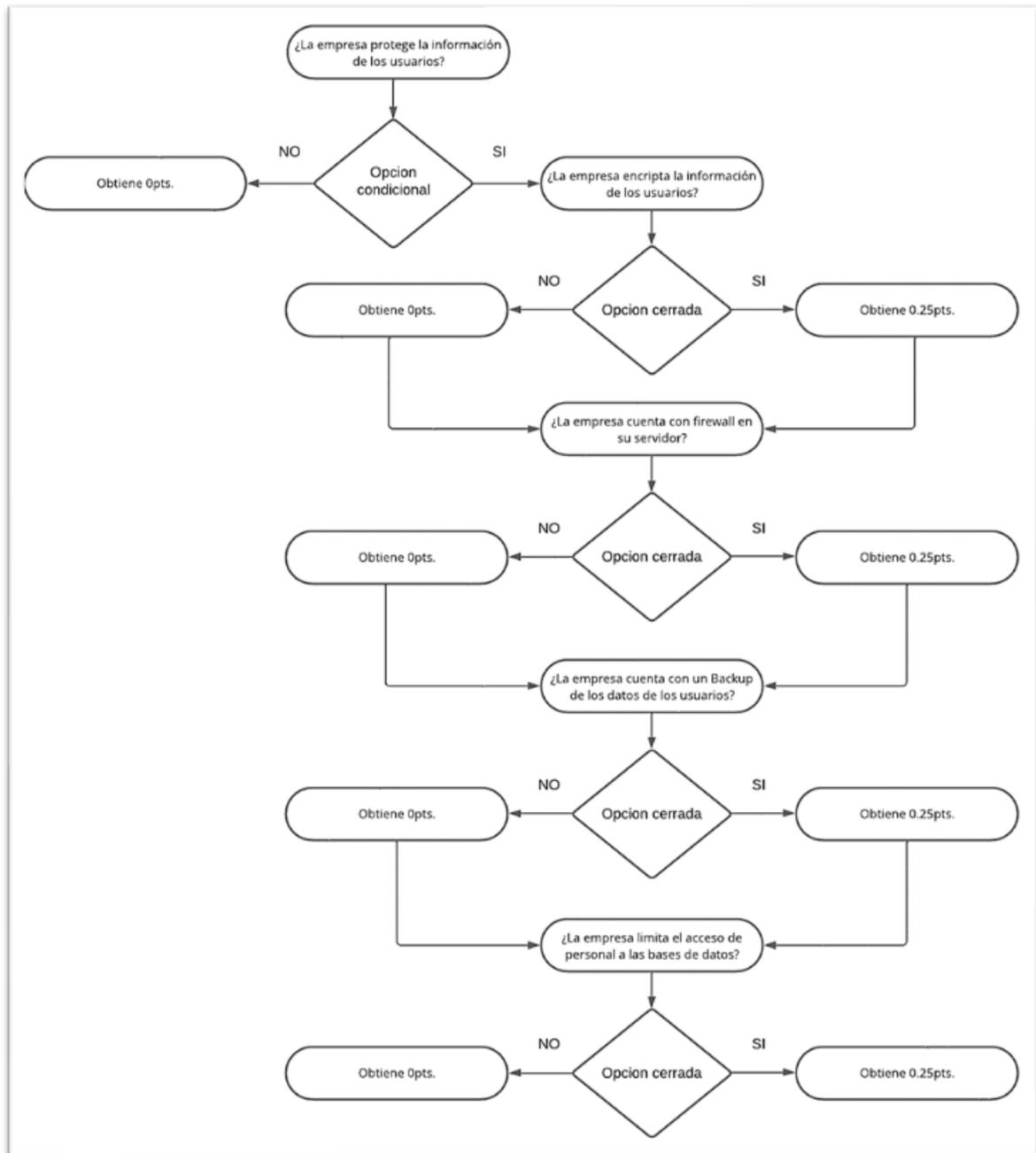


*Nota.* Las opciones múltiples solo se aplican si la pregunta tiene varios puntos

**Caso tres:** Cuando una pregunta depende de la respuesta de otra, la valoración se divide para el numero de preguntas hijas y se asigna de la siguiente manera.

**Figura 4.**

*Preguntas condicionales y de valoración dividida.*



*Nota.* La puntuación de deben ser el proporcional en relación a número de preguntas hijas.

Al concluir la evaluación, se calculará la puntuación del cumplimiento de la LOPDP. Esto se basará en el puntaje obtenido por pregunta, utilizando una fórmula porcentual para mostrar el indicador de cumplimiento.

$$IDC = 100x \frac{\sum_{i=1}^n Puntaje_i}{n}$$

- $n$  es el número total de preguntas
- $Puntaje_i$  es el puntaje obtenido en la pregunta  $i$
- $IDC$  es el Indicador de cumplimiento

Durante la ejecución de este proyecto, no hay una regulación específica de la Ley. Esta carencia de normativa hace que los criterios de evaluación tengan un peso equivalente en este momento. Sin embargo, es relevante destacar que en el futuro podrían surgir situaciones que requieran asignar diferentes ponderaciones según las circunstancias particulares.

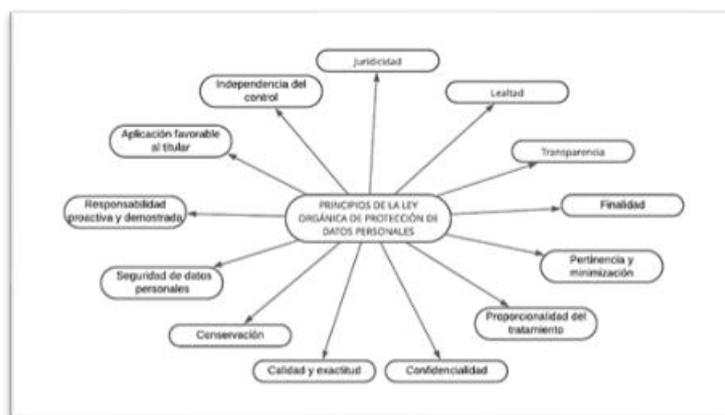
### Banco de preguntas

En la siguiente sección, se mostrará una figura que sintetiza los principios de la ley. Aunque hay otros principios en la Constitución de la República, acuerdos internacionales respaldados por el Estado y leyes adicionales, esta Ley específica se basa en los principios que se detallan más adelante.

Art. 10.- Principios. -Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios. (LOPDP, 2021)

**Figura 5.**

*Principios de la LOPDP.*



*Nota.* La figura muestra cuales son los principios de LOPDP

A continuación, se proporciona un desglose exhaustivo del cuestionario que se empleará, junto con las referencias correspondientes a los artículos conectados con la ley. Este análisis detallado ofrece una comprensión más completa de los temas abordados en el cuestionario y de cómo se relacionan con las disposiciones legales pertinentes.

**Tabla 3.**

*Preguntas en base a los principios de la LOPDP.*

Principio	Pregunta
Juridicidad	¿La empresa garantiza el manejo de datos personales cumpliendo rigurosamente con los principios, derechos y deberes establecidos en la Constitución, tratados internacionales y la Ley Orgánica de Protección de Datos?
Lealtad	¿La empresa asegura que la recopilación, utilización, consulta u otros procesos relacionados con datos personales sean transparentes y comprensibles para los titulares, de manera que estos estén conscientes de la obtención y tengan un entendimiento claro de cómo sus datos serán tratados en el presente y futuro?
Transparencia	¿La empresa asegura que la información sobre el manejo de datos personales esté fácilmente disponible, sea fácil de entender y se presente en un lenguaje claro, garantizando la transparencia en este procedimiento?
Finalidad	¿La empresa garantiza que los propósitos para el manejo de datos personales sean claros, legítimos y comunicados de manera adecuada a los titulares?
Pertinencia y minimización	¿La empresa garantiza que solo se recopila y utiliza la información personal esencial y necesaria para cumplir con el propósito del tratamiento?
Proporcionalidad del tratamiento	¿La empresa asegura que el tratamiento de datos personales sea pertinente, necesario y oportuno en relación a sus propósitos de recopilación o en consideración de la naturaleza de los datos sensibles?

Principio	Pregunta
Confidencialidad	¿La empresa garantiza que los datos personales son tratados con confidencialidad y no se usan o revelan para fines distintos a los originales, excepto si la ley permite un nuevo tratamiento legítimo?
Calidad y exactitud	¿El encargado de manejar datos personales garantiza que la información sea precisa, completa y clara, y toma medidas para eliminar o corregir rápidamente datos incorrectos en relación con sus fines de uso?
Conservación	¿La empresa asegura que los datos personales se mantendrán solo durante el tiempo requerido para su propósito de tratamiento y establece plazos para su eliminación o revisión periódica?
Seguridad	¿La empresa implementa las medidas adecuadas de seguridad, incluyendo las aceptadas por la tecnología actual, para proteger los datos personales contra riesgos, considerando la naturaleza de los datos y el contexto?
Responsabilidad proactiva y demostrada	¿El encargado de manejar datos personales demuestra su compromiso implementando medios para asegurar la protección de datos, como estándares, prácticas destacadas, códigos de protección u otros enfoques adecuados, para cumplir con las normas y proteger los datos?
Aplicación favorable al titular	¿Cuándo hay dudas sobre la interpretación de leyes o contratos de protección de datos, responsables de tratamiento y administrativos suelen aplicarlas de manera favorable al dueño de los datos?
Independencia del control	¿La Autoridad de Protección de Datos está encargada de realizar un control independiente y neutral, además de llevar a cabo acciones para asegurar el ejercicio de la salvaguardia de los datos y el acatamiento de las responsabilidades estatales para resguardar los derechos?

*Nota.* Estas preguntas están basadas en lo estipulado en el art.10 de la LOPDP.

**Tabla 4.***Preguntas en base a los derechos titulares.*

<b>Derecho</b>	<b>Pregunta</b>
Normativa especializada	¿La empresa asegura que los datos personales sujetos a regulaciones especiales, como los de libertad de expresión o de sectores específicos, se traten conforme a los principios legales y de esta Ley, respetando la legalidad, equidad y necesidad?
Derecho a la información	¿La empresa informa de manera clara y comprensible a las personas cuyos datos recopila sobre su uso, tiempo de conservación, responsable y cómo ejercer sus derechos según la LOPDP?
Derecho de acceso	¿La empresa asegura el acceso gratuito a la información personal y detalles según el Artículo 13 de LOPDP, sin necesidad de justificación por parte del titular?
Derecho de rectificación y actualización	¿La empresa garantiza el derecho de los titulares de datos a corregir y actualizar información incorrecta o incompleta, según el Artículo 14 de la LOPDP?
Derecho de eliminación	¿La empresa asegura el derecho de los titulares de datos a pedir la eliminación de sus datos, siguiendo el Artículo 15 de LOPDP?
Derecho de oposición	¿La empresa asegura el derecho de los titulares de datos a oponerse al tratamiento de sus datos, como lo dicta el Artículo 16 de la LOPDP?
Derecho a la portabilidad	¿Garantiza que los titulares puedan recibir sus datos en un formato compatible y legible, o transferirlos a otros responsables, según la normativa?

*Nota.* Estas preguntas están basadas en estipulado en los artículos del 11 al 24.

La relevancia de estas preguntas radica en la búsqueda de un entendimiento exhaustivo de los procedimientos de una entidad con respecto a la normativa. Es fundamental destacar que los principios delineados en las disposiciones se centran en las responsabilidades inherentes a las empresas, dirigidas a garantizar la apropiada gestión de los datos personales de los usuarios.

### **2.3 Validación de la propuesta**

Con el objetivo de respaldar y validar la viabilidad de esta propuesta, se describe minuciosamente cómo el modelo propuesto puede enfrentar y solucionar la problemática planteada. Para demostrar esto, se aprovechará la experiencia y el conocimiento proporcionados por dos especialistas en el campo de la protección de la información.

Se llevaron a cabo dos entrevistas con los consultores de Intellectum Consulting S.A.S., durante las cuales se resaltó la relevancia de la evaluación como una etapa integral previa a la emisión de una opinión profesional sobre el riesgo que una empresa podría enfrentar. Esto es especialmente significativo en el contexto de procesos y metodologías que carecen de salvaguardias para prevenir posibles vulnerabilidades que puedan comprometer la seguridad de la organización.

María Paola Bolaños, ingeniera de sistemas y computación y consultora en el ámbito de la LOPDP, resalta la importancia de considerar cinco áreas clave al evaluar una entidad: administrativa, operacional, jurídica, física y tecnológica. Para medir el cumplimiento normativo, se emplea una matriz en una hoja de cálculo, en la cual la organización se clasifica en cinco niveles de madurez. El nivel uno representa un estadio temprano, con escasa madurez en los procesos de la empresa, mientras que el nivel cinco indica una alta capacidad para cumplir con la normativa.

Es crucial destacar que esta evaluación se basa en el reglamento de acatamiento de la AEPD (Agencia Española de Protección de Datos), puesto que en Ecuador, al ser un país que recién implementa esta ley después de los eventos ocurridos en 2019, aún no cuenta con su propio reglamento establecido.

Paola destaca que el modelo de evaluación, como un recurso de autoevaluación empresarial, es esencial. Sin embargo, resalta dos puntos cruciales que deben tenerse en cuenta. En primer lugar, aunque las preguntas se basan en los principios de la ley, no es suficiente medir la madurez de una entidad solo con preguntas de opción cerrada (sí o no). Es esencial condicionar y desglosar las preguntas afines para profundizar y comprender en qué medida los procesos de seguridad se están implementando. Esto permitirá que el modelo proporcione resultados más precisos y cercanos a la realidad.

En segundo lugar, plantea que el modelo tiene un gran potencial y se espera que evolucione para incluir un registro de avances en cuanto a madurez, trabajando en conjunto con el IDC (Índice de cumplimiento). Además, sugiere la posibilidad de generar estadísticas que reflejen el progreso de la organización a lo largo del tiempo, lo que proporcionaría una visión clara y concreta de la evolución de la entidad en términos de seguridad y cumplimiento normativo.

Pedro Vicente Ponce, magíster en ciberseguridad y gerente de Intelectum Consulting S.A.S., resalta tanto el propósito del modelo como la fórmula empleada para calcular el IDC. No obstante, pone a consideración un punto crucial en el proceso de valoración. Específicamente, se refiere a las métricas de evaluación. El modelo no puede simplemente categorizar a una empresa como "cumple", "está en proceso" o "no tiene iniciativas de seguridad", sin establecer métricas concretas o rangos de valoración. La carencia de esta medida de evaluación resulta en una falta de claridad en cuanto al propósito de simplemente responder preguntas dentro del sistema.

Todas estas retroalimentaciones del modelo han sido cuidadosamente consideradas en la elaboración de la propuesta final de este proyecto. El objetivo es asegurar que el proceso de autoevaluación empresarial sea lo más realista y efectivo posible. La propuesta se presenta como una guía que señala los aspectos a nivel organizacional que deben mejorarse para potenciar los servicios digitales y asegurar la confidencialidad y resguardo de la información personal de clientes, proveedores y empleados.

## 2.4 Matriz de articulación de la propuesta

La siguiente matriz resume todo el proceso de las propuestas y su metodología empleada.

**Tabla 5.**

*Matriz de articulación.*

<b>EJES O PARTES PRINCIPALES</b>	<b>SUSTENTO TEÓRICO</b>	<b>SUSTENTO METODOLÓGICO</b>	<b>ESTRATEGIAS / TÉCNICAS</b>	<b>DESCRIPCIÓN DE RESULTADOS</b>	<b>INSTRUMENTOS APLICADOS</b>
<b>Datos personales</b>	Un dato de carácter personal es toda información vinculada a una persona física reconocible o que puede ser identificada.	La metodología es bibliográfica, con el fin de profundizar los conceptos clave del proyecto	Mediante la bibliografía, se detallo y amplio en concepto, obtenido una clasificación de los datos personales	Clasificación de los tipos de datos personales e identificación de su importancia a nivel de privacidad.	Fuente bibliográfica
<b>LOPDP</b>	Ley vigente en Ecuador que asegura tratamiento seguro de los datos personales por parte de las empresas.	La metodología es bibliográfica, con los artículos de la ley se puso formular las preguntas del modelo de evaluación	Mediante la bibliografía se contextualiza principios de la ley y derechos de los titulares	Planteamiento de las incógnitas que las empresas deben resolver para poder acatar con las disposiciones de la ley	Fuente bibliográfica

<b>EJES O PARTES PRINCIPALES</b>	<b>SUSTENTO TEÓRICO</b>	<b>SUSTENTO METODOLÓGICO</b>	<b>ESTRATEGIAS / TÉCNICAS</b>	<b>DESCRIPCIÓN DE RESULTADOS</b>	<b>INSTRUMENTOS APLICADOS</b>
<b>Métricas de evaluación</b>	Se propone las métricas que garantizan un punto de referencia al medir el nivel de cumplimiento de la ley.	La metodología es bibliográfica, se basa en métricas estándar en la escala de Likert.	Da a conocer el nivel de cumplimiento de la normativa de la LOPDP	Clasifica a las empresas en un nivel de madurez dentro de la escala propuesta	Fuente bibliográfica Entrevistas
<b>Valoración del modelo</b>	La valoración de la propuesta permite la mejora continua por medio de la observación de otro punto de vista.	La metodología es cualitativa y de entrevista	Entrevista realizada a dos especialistas de la seguridad de la información y de la LOPDP.	Observaciones sobre aspectos importantes a considerar en el desarrollo del modelo de evaluación.	Fuente bibliográfica Entrevistas

*Nota.* Elaboración propia.

## **CONCLUSIONES**

Identificando los conceptos relevantes del proyecto se lleva a la conclusión de que cuando hablamos de seguridad comprende más allá de la parte técnica y de TI sino que viene a presentarse ya como una cultura digital en la que las empresas deben aprender a involucrarse e ir evolucionando con la tecnología.

El modelo de evaluación comprende varios aspectos que solo se logra ver si contextualiza bien la problemática inicial, medir el nivel cumplimiento de una empresa representa tener claro que se espera como resultado para definir parámetros y métricas que aseguren mitigar la brecha entre un resultado cualquiera e información útil para tomar decisiones.

El modelo introduce un enfoque híbrido de evaluación en las preguntas, lo que facilita su adaptación una vez que la regulación nacional de protección de datos entre en vigencia en Ecuador. Esto representa una valiosa oportunidad de flexibilidad, ya que no es rígido y permite progresar en conformidad con la ley.

Los expertos que evaluaron la propuesta han expresado su satisfacción y han señalado posibles áreas de mejora. Entre las recomendaciones se encuentra el desarrollo de un sistema de software que aumente la visibilidad y accesibilidad de este modelo.

## **RECOMENDACIONES**

Se recomienda establecer programas de formación y concienciación que promuevan la seguridad informática como un componente esencial de la cultura corporativa. Esto debe incluir a todos los niveles de la empresa para fomentar la comprensión y el compromiso con las prácticas seguras en línea.

Para mejorar la efectividad del modelo de evaluación, se sugiere que las empresas dediquen tiempo a realizar un análisis profundo de su situación y problemáticas iniciales. Esto garantizará que las métricas definidas sean específicos y alineados con sus necesidades reales.

Dado el esquema híbrido del modelo, se recomienda seguir monitoreando las actualizaciones en la normativa de resguardo de datos en Ecuador. Aprovechar la oportunidad de adaptar el modelo a los nuevos requisitos legales permitirá mantener su relevancia y efectividad a medida que evoluciona el panorama normativo.

Para mantener la calidad y coherencia del modelo, se aconseja mantener una colaboración continua con expertos en diversas áreas. Integrar diferentes perspectivas asegurará que el modelo siga siendo sólido y relevante a medida que se expande o se transforma en un sistema más avanzado.

## BIBLIOGRAFÍA

- Álvarez, L. E. (2021, febrero 12). *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*. Foro, revista de derecho. <https://revistas.uasb.edu.ec/index.php/foro/article/view/500/2418>
- BBC News Mundo. (2019, septiembre 16). Filtración de datos en Ecuador: la “grave falla informática” que expuso la información personal de casi toda la población del país sudamericano. *BBC*. <https://www.bbc.com/mundo/noticias-america-latina-49721456>
- Cano, J. (2012). Seguridad de la información y privacidad: dos conceptos convergentes. *Revista Sistemas Edición 123*. <https://acis.org.co/archivos/Revista/123/Revista%20Sistemas%20Edici%C3%B3n%20123.pdf>
- Cárdenas, A., & Xavier, W. (2023). Propuesta de estrategia para evitar la fuga de información en empresas constructoras utilizando detección por comportamiento (UEBA) CASO DE ESTUDIO: SCMI INC (USA). Quito, Ecuador: Universidad Tecnológica Israel.
- Carrión, J. (2017). *Diferencia entre dato información y conocimiento*. Repositorio UDGVirtual. [http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/869/3/Diferencia\\_entre\\_dato\\_informaci%C3%B3n.pdf](http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/869/3/Diferencia_entre_dato_informaci%C3%B3n.pdf)
- Comisión Europea. (s/f). ¿Qué son los datos personales? Recuperado el 18 de julio de 2023, de [https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data\\_es](https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_es)
- Cueto, E. (2020). Investigación cualitativa. *Applied Sciences in Dentistry*, 1(3).
- Dinarp. (2021, noviembre 9). *Ley de Protección de Datos Personales - Dirección Nacional de Registros Públicos*. Dirección Nacional de Registros Públicos. <https://www.registropublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/>
- El Universo. (2019, octubre 21). ¿Qué pasó con los datos filtrados en Ecuador? <https://www.eluniverso.com/larevista/2019/10/21/nota/7569752/que-paso-datos-filtrados-ecuador/>
- Guaman, C. R. S., Vivar, S. A. M., Rivera, D. P. P., & Calderon, F. A. C. (2019). PERCEPCION DE SEGURIDAD DE LA INFORMACION EN LAS PEQUENAS Y MEDIANAS EMPRESAS EN SANTO DOMINGO. *Investigacion Operacional*, 40, 421+. <https://go.gale.com/ps/i.do?id=GALE%7CA583252489&sid=googleScholar&v=2>

.1&it=r&linkaccess=abs&issn=02574306&p=AONE&sw=w&userGroupName=a  
non%7E2442f2c3&aty=open-web-entry

Infoem. (2019). ¿Qué es la protección de datos personales?  
<https://www.infoem.org.mx/es/contenido/datos-personales>

Llaguno, S., & Leonardo, E. (2022). Modelo de seguridad informática en los aspectos organizativos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NITS. Quito: UISRAEL.

Passailaigue, R. (2017, febrero 5). *LEYES ORGÁNICAS Y ORDINARIAS - Ecomundo*. Ecomundo | Educación Particular Bilingüe; Unidad Educativa Particular Bilingüe Ecomundo. <https://ecomundo.edu.ec/leyes-organicas-y-ordinarias/>

Posey, B. (2021, julio 22). *Privacidad de datos, seguridad de datos y protección de datos*. ComputerWeekly.es; TechTarget.  
<https://www.computerweekly.com/es/definicion/Privacidad-de-datos-seguridad-de-datos-y-proteccion-de-datos>

Serrano Gallardo P, Bojo Canales C, Gómez Sánchez A. (2016, mayo). *La revisión bibliográfica: primera etapa en la actividad científica*. Enfermería21.  
<https://www.enfermeria21.com/revistas/metadatos/articulo/80908/puesta-al-dia-en-la-busqueda-de-informacion-cientifica-la-revision-bibliografica-primer-etapa-en-la-actividad-cientifica/>

UASB. (2021, marzo 15). *Protección de datos*. Observatorio Ciberderechos y Tecnosociedad. <https://www.uasb.edu.ec/ciberderechos/proteccion-de-datos/>

Vela, V., & Edwin, F. (2022). *ESTUDIO DE UN SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) PARA BASE DE DATOS SQL SERVER CASO DE ESTUDIO: MINISTERIO DE RELACIONES EXTERIORES Y MOVILIDAD HUMANA*. Quito: UISRAEL.

## ANEXOS

### Formato de entrevista a los especialistas

 <p>Universidad Israel</p>	<p>ESCUELA DE POSGRADOS "ESPOG" MAESTRÍA EN SEGURIDAD INFORMÁTICA</p>
Nombre: _____	Fecha: _____
Empresa: _____	Cargo: _____
<p>1. ¿Cuál es su experiencia con la seguridad de la información?</p> <p>2. ¿Conoce los artículos, principios y derechos de la LOPD aprobada en mayo del 2021?</p> <p>3. ¿Al momento de evaluar si una entidad está cumpliendo con la normativa, que puntos toma a consideración?</p> <p>4. Según el listado proporcionado de preguntas ¿Que tan certero es que nos proporcionen información útil del cumplimiento de la ley?</p> <p>5. ¿Cree que el modelo evaluador de forma porcentual ayuda a algunas entidades a conocer indicadores clave de cumplimiento de la LOPD?</p> <p>6. ¿Considera que el modelo proporcionado tiene aplicabilidad dentro del desarrollo de un sistema con un histórico de avances de cumplimiento?</p> <p>7. ¿Qué recomendación puede dar sobre el modelo con el fin de mejorar su veracidad y confiabilidad?</p> <p>8. ¿Cómo puede ayudar este tipo de modelos de autoevaluación a los profesionales de la seguridad de la información a nivel de toma de decisiones dentro de una empresa?</p>	