UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
EVALUACIÓN DE PRÁCTICAS DE CONTROL DE SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA LEY DE PROTECCIÓN DE DATOS CASO DE ESTUDIO MINISTERIO DE AGRICULTURA Y GANADERÍA - PNSAE
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
Autor:
Jonathan Marcelo Diaz Almachi
Tutor:
Mg. Christian Patricio Vaca Benalcázar CPA

Quito – Ecuador

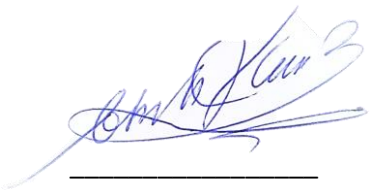
2022

APROBACIÓN DEL TUTOR

Yo, **Christian Patricio Vaca Benalcázar** con C.I: **1719368555** en mi calidad de Tutor del proyecto de investigación titulado: **EVALUACIÓN DE PRÁCTICAS DE CONTROL DE SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA LEY DE PROTECCIÓN DE DATOS CASO DE ESTUDIO MINISTERIO DE AGRICULTURA Y GANADERIA – PNSAE**.

Elaborado por: **Jonathan Marcelo Diaz Almachi**, de C.I: **1722467923**, estudiante de la Maestría: **Seguridad Informática**, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, 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., 09 de septiembre de 2022



_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Jonathan Marcelo Diaz Almachi con C.I: 1722467923, autor del proyecto de titulación denominado: **EVALUACIÓN DE PRÁCTICAS DE CONTROL DE SEGURIDAD DE LA INFORMACIÓN ALINEADA A LA LEY DE PROTECCIÓN DE DATOS CASO DE ESTUDIO MINISTERIO DE AGRICULTURA Y GANADERIA – PNSAE**. Previo a la obtención del título de Magister en **Seguridad Informática**.

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 Sistema 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., 09 de septiembre de 2022

_____

Firma

ORCID: 0000-0002-9655-5419

Tabla de contenidos

APROBACIÓN DEL TUTOR……2
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE…… 3
INFORMACIÓN GENERAL…… 1
Contextualización del tema…… 1
Problema de investigación ……2
Objetivo general …… 2
Objetivos específicos …… 2
Vinculación con la sociedad y beneficiarios directos: …… 2
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO ……4
1.1. Contextualización general del estado del arte ……4
1.2. Proceso investigativo metodológico …… 10
Investigación Cualitativa …… 10
1.3. Análisis de resultados …… 11
CAPÍTULO II: PROPUESTA ……13
1.4. Matriz de articulación de la propuesta …… 24
CONCLUSIONES …… 25
RECOMENDACIONES …… 26
BIBLIOGRAFÍA …… 27

Índice de tablas

Tabla 1 Impacto de las infracciones……6
Tabla 2 Registros últimos tres años……8
Tabla 3 Artículos de la Ley Orgánica de Protección de Datos Personales……15
Tabla 4 Análisis de Brecha Situación Actual……17
Tabla 5 Análisis de Brecha alineada a la LOPDP cubierto con COBIT 2019 (Buenas Prácticas)22
Tabla 6 Matriz de articulación……24

Índice de figuras

Figura 1 Infracciones del responsable de protección de datos personales 7
Figura 2 Infracciones del encargado de protección de datos 8
Figura 3 Principios de COBIT 10
Figura 4 Indicadores de registro ciclo Invierno 2022 12
Figura 5 Indicadores de registro ciclo Verano 2022 12
Figura 6 Objetivo de Gestión de COBIT 2019 APO 14
Figura 7 Objetivo de Gestión de COBIT 2019 APO 14
Figura 8 Identificar Normas para el Tratamiento de los Datos 16
Figura 9 Análisis de Brecha Situación Actual – Estado 18
Figura 10 Enfoque - estado en análisis 19
Figura 11 Enfoque - estado en proceso 20
Figura 12 Enfoque - estado hecho 21

INFORMACIÓN GENERAL

Contextualización del tema

De acuerdo (Garzón & Olmos, s. f.) “la aparición del Internet y su uso globalizado a nivel personal y en el entorno empresarial el cual nos permite “estar conectados”, sin embargo, al mismo tiempo estos avances tecnológicos también se transforman en una amenaza toda vez que trae consigo la aparición de nuevas vulnerabilidades y riesgos de seguridad dado la fácil accesibilidad y exposición de información vital o sensible para la Compañías (por ejemplo, los datos personales) gracias a esa conectividad”. Por tal motivo, es de fundamental importancia la ley de protección de datos personales.

Debido a los actuales casos de robo de información, empresas públicas y privadas en el país que han sido víctimas de hackers, a su vez miles de personas a nivel nacional a las cuales se les ha suplantado su identidad y de igual manera vulnerada su información personal y bancaria, se ve el interés en realizar un estudio de la LOPDP en el Ecuador.

Mediante su estudio se plantea guiar en la implementación de la ley orgánica de protección de datos en las diferentes empresas públicas y privadas del país y hacer el uso consciente de manera en que su información será utilizada una vez aplicada la ley.

Por el lado de la empresa donde trabajo se ve la necesidad de implementar ya que se maneja una cantidad de información de clientes muy amplia la cual se debe garantizar el uso de información otorgada, con el fin de que todos los datos registrados y almacenados sean de total confidencialidad y hacer uso solo para los fines pertinentes y no ser expuestas a terceras personal con lo que la empresa y los clientes se garantice el uso adecuado de sus datos personales.

Cabe señalar que todo tratamiento de datos personales que se realice en cualquier parte del territorio nacional sea el responsable quien esté domiciliado en el Ecuador están sujetos a su cumplimiento, así como el uso de información en sistemas informáticos.

Sin embargo, algunas de las condiciones en especial son como se maneja información de niños y con algún tipo de enfermedad, como pacientes con enfermedades reservadas, son datos o información delicada con lo que se debe de tratar con el mayor sigilo y garantizando su custodia.

Problema de investigación

La falta de políticas de seguridad de la información alineadas a buenas prácticas limita que se cumpla con lo establecido en la LOPDP, de manera que mediante la implementación de controles de buenas prácticas sugeridas en COBIT se podría mitigar el riesgo a sanciones e incumpliendo a la ley de protección de datos personales y a su posible reglamento.

Objetivo general

Evaluar las prácticas de control de la seguridad de información mediante la identificación de las brechas que mantiene la institución en cuanto a los datos personales con la finalidad de proponer controles que permitan su cumplimiento.

Objetivos específicos

- Realizar un análisis de la normativa legal respecto a la protección de datos de las personas por medio de la revisión de la revisión de la LOPDP y COBIT 2019.
- Analizar las brechas mediante un formulario técnico sobre el tratamiento de los datos ingresados al sistema, para verificar la seguridad de la información registrada.
- Establecer procedimientos a través de una matriz de las buenas prácticas para prevenir incidentes en el tratamiento de los datos personales.
- Brindar seguridad sobre los datos que proporcionan los agricultores en el Ecuador con la finalidad de contribuir al cumplimiento del objetivo ODS N°11.

Vinculación con la sociedad y beneficiarios directos:

Los beneficiarios directos de esta propuesta son el Ministerio de Agricultura por medio del proyecto Nacional de Semillas para Agrocadenas Estratégicas (PNSAE) de la Subsecretaria Producción Agrícola, así también la ciudadanía en general y sobre todo los agricultores a nivel nacional, para esto el beneficio se refleja mediante:

Beneficiarios Directos

- En el Proyecto Nacional de Semillas para Agrocadenas Estratégicas (PNSAE) evitando sanciones o multas dispuestas por la normativa al contar con controles para el cumplimiento de dicha ley y su reglamento.
- Mediante una capacitación a los agricultores sobre la importancia del nivel de acceso a la información que se les da a través de encuestas, formularios web, entre otros.
- Garantizando la seguridad de los datos personales entregados mediante medios físicos o digitales.

Beneficiarios Indirectos

- Empresas Cooperantes encargadas de entregar el producto a través de paquetes tecnológicos parcialmente subvencionados.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

a. Normativa Legal relacionada con la Protección de datos Personales

i. **Constitución del Ecuador.**

La Constitución de la República del Ecuador, es la Norma Suprema, a la que está sometida toda la legislación ecuatoriana, donde se establecen las normas fundamentales que amparan los derechos, libertades y obligaciones de todos los ciudadanos, así como las del Estado y las Instituciones del mismo. Consta de 444 artículos.

ii. **La ley de Comercio Electrónico**.

En Ecuador a partir del año 2022 se aprobó la ley del comercio electrónico, mediante decreto 3496, El objetivo de esta ley "Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.". Para poder comprender lo que significa un documento electrónico y los requisitos para su validez jurídica y para poderlos emplear en un proceso judicial, se debe conocer lo siguiente:

Documento Electrónico, es toda información que ha sido creada, generada, procesada enviada, recibida, comunicada o archivada por medios electrónicos, sin perjuicio de que pueda comunicarse por cualquier medio, hay que tomar en cuenta que debe ser realizada por medios electrónicos para que se configure como documento electrónico.

Los documentos electrónicos son: correo electrónico, registro electrónico, servicios web (Internet en general), información electrónica, mensajes de texto y chat.

La norma más trascendente está en el artículo 2 la cual establece la validez jurídica de los documentos electrónicos y lo hace en términos del principio de equivalencia funcional, la misma que señala que "los mensajes de datos tendrán igual valor jurídico que los documentos escritos".

La relevancia jurídica, determina la eficacia, valoración y efecto de los documentos electrónicos, se someterán al cumplimiento de lo establecido en la

ley y su reglamento, esto quiere decir que el valor probatorio de un documento electrónico estará supeditado a la autenticidad e integridad del mismo. (Dirección de Educación en Línea, 2017).

iii. **Ley Orgánica de Protección de Datos Personales**

El 10 de mayo de 2021, el pleno de la Asamblea Nacional del Ecuador aprobó con 118 votos afirmativos, el proyecto de Ley de Protección de Datos Personales, que fue entregado el pasado 19 de septiembre de 2019 por la Presidencia de la República, a través del Ministerio de Telecomunicación y de la Sociedad de la Información (Mintel) y la Dirección Nacional de Registro de Datos Públicos (Dinardap).

Los datos personales son toda aquella información que nos identifica o nos hace identificables, por lo general los datos personales hace referencia cuando se habla de la cédula, nombres, apellidos, números de teléfono, etc.

Sin duda alguna, olvidamos que también se debe llamar datos personales a todo tipo de fotografía, videos, preferencias a gustos en redes sociales, sin olvidar la meta data que existe detrás de cada dato, aunque parezca insignificante son datos personales que a su vez en el entorno digital permiten construir una huella digital, que se puede decir que es registro que dejamos mientras utilizamos herramientas de tecnologías de información y comunicación.

Gracias al avance tecnológico de cierta manera nuestra información está presente en el entorno virtual, ya sea si en algún momento nos registramos en alguna red social donde ingresamos nuestra información personal o cuando en busca de información dejamos huellas como dirección de correos electrónicos entre otros, haciendo así que nuestro rastro quede almacenado en los gestores de búsqueda, sin darnos cuenta estamos incrementando la data en la internet.

Es por ello que la ley pretende darnos ese derecho, el derecho a la protección de información personal, pues de alguna manera puede parecer no peligroso, pero repercuta en un arma de doble filo ya que se puede vulnerar los derechos y la imagen de un individuo.

Es importante reconocer como el derecho a la educación digital en el cual se establezca que somos responsables de educarnos en materia de protección de datos y de cómo debemos construir nuestra huella digital, la reputación en línea

y gestionar de mejor manera nuestros datos, aun sabiendo que normar el internet es muy complicado porque no existen barreras aún en el país.

Los aspectos más relevantes de esta normativa son los que se detallan en el ver **Anexo 1**.

Para un adecuado tratamiento se debe verificar las posibles sanciones que la ley ha dictaminado para quienes incumplan con su normativa.

Riesgos Legales

Tabla 1

Impacto de las infracciones.

	Impacto
Infracción leve	Los servidores o funcionarios del sector público serán sancionados con una multa de uno (1) a (10) salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado.
	Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero es una entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.
Infracción grave	Los servidores o funcionarios del sector público serán sancionados con una multa de diez (10) a veinte (20) salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado.
	Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero es una entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

Nota: Elaboración propia a partir de (GUÍA DE PROTECCIÓN DE DATOS PERSONALES, s. f.).

Figura 1

Infracciones del responsable de protección de datos personales.

INFRACCIONES DEL RESPONSABLE DE PROTECCIÓN DE DATOS	
Se consideran infracciones leves	No tramitar, fuera del término previsto o negar injustificadamente las peticiones o quejas realizadas por el titular.
	No implementar protección de datos desde el diseño y por defecto.
	No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales.
	Elegir un encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales.
	Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales
Se consideran infracciones graves	Utilizar información o datos para fines distintos a los declarados.
	Ceder o comunicar datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente ley.
	No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales, las particularidades del tratamiento de las partes involucradas.
	No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarla.
	Realizar tratamientos de datos personales sin observar los principios y derechos desarrollados en la presente ley.
	que mantenga con el responsable del tratamiento de datos personales inclusive en lo que respecta a la transferencia o comunicación internacional.
	No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales.

Nota: Elaboración propia a partir de (GUÍA DE PROTECCIÓN DE DATOS PERSONALES, s. f.).

Figura 2

Infracciones del encargado de protección de datos.

INFRACCIONES DEL ENCARGADO DE PROTECCIÓN DE DATOS	
Se consideran infracciones leves	No facilitar el acceso al responsable del tratamiento de datos personales a toda la información.
	No permitir o no contribuir a la realización de auditorías e inspecciones por parte del responsable del tratamiento de datos personales o de otro auditor autorizado.
Se considera infracciones graves	Realizar tratamientos de datos personales sin observar los principios y derechos desarrollados en la presente ley
	No tratar datos personales de conformidad con lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales inclusive en lo que respecta a la transferencia o comunicación internacional.
	No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales.

Nota: Elaboración propia a partir de (GUÍA DE PROTECCIÓN DE DATOS PERSONALES, s. f.).

Todas estas infracciones detalladas anteriormente se deberán tomar en cuenta al realizar el tratamiento de los datos ya que la normativa lo establece y de no cumplirlas será motivo de sanción para la institución y los responsables de la información.

b. Riesgos sector Agrícola

El nivel de muestra de los datos en la agricultura es muy alto, la necesidad de querer adquirir un beneficio hace que los agricultores no ven el riesgo a los que se expone sus datos personales, a nivel nacional de acuerdo a los registros consultados al área de sistemas del PNSAE indica que, la cantidad de registros en los últimos tres años varía entres 25mil a 70mil registros de agricultores por año, esto implica dirección y coordenadas de predios y domicilio como se muestra en la Tabla 4.

Tabla 2

Registros últimos tres años.

Año	Cantidad Registros
2020	27.358
2021	26.520
2022	79.854

Nota: PNSAE

Como se puede apreciar en el año en curso se ha triplicado el incremento de registros a nivel nacional haciendo así que la seguridad de los datos se vuelva más crítica y primordial de manera que se debe ir mitigando los riesgos en las posibles fuja de información.

c. Ciberseguridad

Es cuidar la información propia y de terceros, datos que pueden estar almacenados en dispositivos electrónicos, computadores, celulares, entre otros, con el fin de proteger en lo que se refiere a la confidencialidad de los datos y disponibilidad en la que se pueda acceder y cuando se quiera acceder conservando la integridad de la información. (CISCO, 2021).

Se debe trabajar con las personas con la finalidad de buscar proteger y concientizar para evitar posibles robos de datos y suplantación de identidad, verificar la funcionalidad de los sistemas internamente y cómo interactúan entre sí y ver donde puedan existir brechas de seguridad ya hoy en día el activo más importante en cualquier área es la información. (CISCO, 2021).

d. Marcos de Referencia para la LOPDP

- **ISO 27002**

Se centra en la gestión de las buenas prácticas para la seguridad de la información en la actualidad es fundamental ya que garantiza la continuidad y el mantenimiento de los procesos de seguridad alineados a los objetivos estratégicos de la organización.

La normativa describe cómo se pueden establecer los controles, los mismos que deben ser elegidos en base a una evaluación de riesgo de los niveles activos más importantes de la empresa, la ISO 27002 se puede utilizar para apoyar la implementación del sistema de gestión de seguridad de información en cualquier tipo de organización pública o privada.

La ISO 27002 tiene por objetivo establecer directrices, principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información tomando en cuenta la administración de controles teniendo en cuenta los entornos de riesgos encontrados en la organización.

- **SysAdmin Audit, Networking and Security Institute (SANS) 20 CSC**

Los SANS Top 20 CSC están asignados a los controles del NIST, **Anexo 2.**

- **Objetivo de control para la información y tecnologías relacionadas (COBIT) 2019**

Creado por la asociación de control y auditoría de sistemas de información (ISACA) e IT Governance Institute. (“¿Qué es COBIT?”, 2019).

Es una guía de mejores prácticas presentada como Framework dirigidas al control y supervisión de tecnologías de la información, también proporciona una visión empresarial de gobierno de TI que tiene la tecnología y la información como protagonistas en la creación de valor para las empresas.

COBIT mantiene un equilibrio entre la precisión de beneficios y la optimización de los niveles de riesgo, así como el uso de los recursos para crear un valor óptimo de TI, permite integrar la información y tecnología relacionada para toda la organización incluyendo el alcance completo de todas las áreas de responsabilidades funcionales y de negocios considerando los intereses relaciones de TI y de grupos de interés internos y externos.

Fundamente su lógica de trabajo bajo principios, que se detallan en la Figura 1.

Figura 3

Principios de COBIT.

Nota: Elaboración propia a partir de COBIT 2019.

1.2. Proceso investigativo metodológico

Investigación Cualitativa

“La investigación cualitativa es aquel modelo de investigación que estudia las prácticas sociales, a las que comprende como realidades complejas y simbólicas que no pueden ser reducidas a valores numéricos. Asimismo, supone que ciertas realidades solo pueden ser

comprendidas desde la observación participante (investigación-acción)". (*Investigación cualitativa y cuantitativa*, s. f.).

Uno de los procesos metodológicos puede ser la hipótesis ya que están referidas al sentido, como enfoque deductivo.

En la investigación se aplica técnicas de: entrevistas, cuestionarios abiertos, grupos focales, notas de campo, esto como lista para el cotejo o instrumento para la recolección y registros de datos.

La encuesta que se aplica a la muestra de registro de agricultores se puede visualizar en el **Anexo 3**.

Con esta investigación se pretende comprender el área sobre la que se tiene poco conocimiento o comprensión inadecuada, aportar información descriptiva, comprender el contexto sobre el que se quiere actuar, a su vez la validación de resultados, con la interpretación, clarificación y comprensión de los datos de estudio.

1.3. Análisis de resultados

Población de registro de agricultores para el beneficio de paquetes tecnológicos.

El PNSAE a través de la Subsecretaría de Producción Agrícola entrega paquetes subvencionados parcialmente a todos los agricultores a nivel nacional, mediante ciclos de intervención los cuales se dividen dos; invierno y verano, ciclos en el cual los agricultores se registran con el fin de acceder a mencionado beneficio otorgado por el gobierno, es decir que cada intervención hay una variación de registros.

Es muy importante el gran volumen de información que se va registrando en cuanto a datos personales de agricultores en todo el territorio nacional, por lo que la información está sujeta a un gran riesgo de fuga de información, por lo que se analizará de cómo se va generando esta data con una proyección de las últimas intervenciones realizadas en el presente año, con el fin de constatar un crecimiento en cada temporada y a su vez el crecimiento de información recolectada.

En la figura 2 se observa que la provincia con mayor cantidad de registros es Guayas, seguido de Manabí por lo que identificamos como los sectores más vulnerables en cuanto a posibles fugas de información y tratamiento de datos personales.

Los siguientes datos están dados por registros a nivel de provincias durante el ciclo de intervención Invierno 2022, con un total de 35880 registros, como se muestra en la figura 4 y

durante el ciclo de intervención Verano 2022, con un total de 42741 registros, como se muestra en la figura 5.

Figura 4

Indicadores de registro ciclo Invierno 2022.

Nota: PNSAE, invierno 2022.

Figura 5

Indicadores de registro ciclo Verano 2022

Nota: PNSAE, verano 2022.

CAPÍTULO II: PROPUESTA

2.1 Fundamentos teóricos aplicados

Se utilizó la ley de datos personales y COBIT 2019 para poder validar y realizar la propuesta utilizando tanto la ley y controles lo cual se puede evidenciar en el **Anexo 4.**

De igual manera utilizando en método de encuesta a los agricultores se puede observar que el mayor porcentaje de ellos tienen conocimiento en cuanto a LOPDP y de cuál es el tratamiento que se da a sus datos entregados en campo.

Encuesta ver **Anexo 5.**

A continuación, podemos identificar la tabla para la muestra obtenida de la encuesta realizada a nivel nacional.

Para la realización de la tabla se utilizó la nomenclatura siguiente:

- Nivel de Confianza el 90%
- p= proporción de éxito 10%
- p= proporción de fracaso 90%
- E= error de 5%
- N= población
- n= Valor o muestra

ver **Anexo 6**

Se puede decir que el 80% de agricultores no tienen conocimiento de la LOPDP y 20% tiene algo de conocimiento sobre la ley y de cómo se maneja la información entregada a los técnicos facilitadores de campo.

De acuerdo a lo fundamentado para establecer el trabajo de investigación se toma en cuenta que para la recolección de información por parte del personal técnico en campo se debe establecer lo siguiente:

En el marco COBIT 2019 está conformado por 40 objetivos, los mismo que son 5 de gobierno y 35 de gestión, dentro de los dominios tendremos los objetivos de gestión en este caso (APO) el mismo que agrupa 14 objetivos los cuales permiten gestionar de una manera adecuada.

Es así que se toma como referencia los objetivos de gobierno y gestión de COBIT 2019, como se podrá visualizar en la figura 6 y 7.

Figura 6

Objetivo de Gestión de COBIT 2019 APO.

APO13 Gestionar la Seguridad	
APO13.01	Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)
APO13.02	Definir y administrar un plan de tratamiento de riesgos de seguridad de la información
APO13.03	Monitorear y revisar el SGSI

Nota: Elaboración propia a partir de (COBIT, 2019).

Figura 7

Objetivo de Gestión de COBIT 2019 APO.

APO14 Datos Gestionados	
1	Definir la estrategia de gestión de Datos y Comunicarlo
2	Definir y mantener un glosario empresarial consistente y mantenerlo
3	Establecer los procesos e infraestructura para la metadata y su gestión
4	Definir la estrategia de calidad de datos
5	Establecer metodologías y herramientas para un perfil de datos (multiplataforma)
6	Establecer un enfoque para medir y valorar la calidad de los datos
7	Establecer un enfoque para la sanitización de datos.
8	Manejar el ciclo de vida de los activos de información
9	Dar apoyo a la retención y archivado de datos
10	Gestionar los procesos de respaldo y recuperación de datos

Nota: Elaboración propia a partir de (COBIT, 2019).

Mediante los artículos establecidos en la LOPDP se consideran los más relevantes en virtud de los procesos que tiene el PNSAE con el propósito de instaurar alguno de ellos hacia el tratamiento de la información dentro y fuera de la institución pública.

Tabla 3

Artículos de la Ley Orgánica de Protección de Datos Personales.

Ley Orgánica de Protección de Datos Personales	
Artículo 12	Derecho a la información.
Artículo 13	Derecho al acceso.
Artículo 15	Derecho de eliminación.
Artículo 19	Derecho a la suspensión del tratamiento.
Artículo 23	Derecho a la educación digital.
Artículo 33	Transferencia o comunicación de datos personales.
Artículo 35	Acceso a datos personales por parte de terceros.
Artículo 37	Seguridad de datos personales.
Artículo 38	Medidas de seguridad en el ámbito del sector público.

Nota: Elaboración propia a partir de (Gob.ec (S/f)).

De acuerdo a la LOPDP establece en algunos de sus artículos el uso adecuado de la información de manera en que se debe llevar a cabo el aseguramiento y tomando en cuenta que los objetivos de gobierno y gestión en COBIT 2019 plantea.

Para identificar las normas para el tratamiento de los datos podemos observar en la figura 8.

Figura 8

Identificar Normas para el Tratamiento de los Datos.

Normas	LOPDP	COBIT 2019
El titular de datos personales tiene derecho a ser informado conforme a los principios de lealtad y transparencia por cualquier medio.	Art. 12	APO14
El titular tiene derecho a conocer y a obtener gratuitamente acceso a todos sus datos personales sin necesidad de presentar justificación alguna.	Art. 13	APO14
El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales cuando él lo solicite.	Art. 15	APO14
El titular dará consentimiento cuando el responsable del tratamiento haya entregado información suficiente al titular que le permita conocer la finalidad a que se destinará sus datos.	Art. 33	APO14
El tratamiento de los datos personales por terceros deberá estar regulado por un contrato donde se establezca de manera clara y precisa que no se utilizará para finalidades diferentes a las señaladas en el contrato.	Art. 35	APO13
Aplicar medidas necesarias para enfrentar cualquier tipo de riesgo, amenaza o vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental conforme al principio de datos personales.	Art. 38	APO13

Nota: Elaboración propia a partir de (Gob.ec (S/f)) y (COBIT, 2019).

2.2 Descripción de la propuesta

Para un manejo adecuado de los datos personales se plantea como mínimo las siguientes interrogantes e indicaciones:

- ✓ Quién utilizará los datos.
- ✓ Datos que recolecta.
- ✓ Cuál es la finalidad de los datos.
- ✓ Cuál es el proceso para ejercer derechos de acceso y rectificación.
- ✓ Se deberá notificar en el caso de que existan cambios en la política de privacidad.
- ✓ Contará con medidas para precautelar la seguridad de los datos personales.
- ✓ Una base legal que sustenta el tratamiento de los datos.

✓ Términos y condiciones de uso.

Cabe recalcar que para el manejo adecuado hay que tomar en cuenta el proceso que realiza la institución e ir acoplando acorde a la necesidad que se desea cubrir en cuanto a la garantía de la protección de datos personales.

Se procede a realizar un análisis de brecha con la situación actual y se puede recomendar una aplicación de acuerdo a la ley orgánica de protección de datos personales y buenas prácticas con COBIT 2019. ver **Anexo 7**

Tabla 4

Análisis de Brecha Situación Actual.

Enfoque	Estado actual	Estado futuro	Prioridad
¿El proyecto cuenta con políticas de seguridad al receptar información de agricultores a nivel nacional?	NO	Contar con Políticas	Alto
¿Cuentan con acuerdos de confidencialidad de los datos recolectados?	NO	Contar con acuerdos	Alto
¿Tienen políticas de Seguridad de Información dentro del área de Sistemas?	SI	Reforzar	Medio
¿Al entregar información de los registros de los agricultores se los realiza por medios autorizados?	N/A	Mejorar el control	Medio
¿Se tiene controles de medios electrónicos a utilizar dentro de la institución para salvaguardar la información y evitar fuga de datos?	NO	Contar con Controles de Seguridad	Medio
¿Tiene controles de acceso a la información de base de datos?	SI	N/A	Bajo
¿Si un agricultor desea dar por terminado su solicitud al beneficio,	NO	N/A	Alto

se procede a eliminar su información de la base de datos?			
¿El Proyecto cuenta con planes de contingencia en lo que se refiere a la base de datos?	NO	Establecer planes de contingencia	Alto
¿Cuenta con personal responsable de seguridad de información y monitoreo de posibles vulnerabilidades dentro de la plataforma?	NO	Establecer profesionales encargados en ciberseguridad	Medio
¿El Proyecto cuenta con un responsable del tratamiento de los datos personales?	NO	Establecer un responsable	Alto

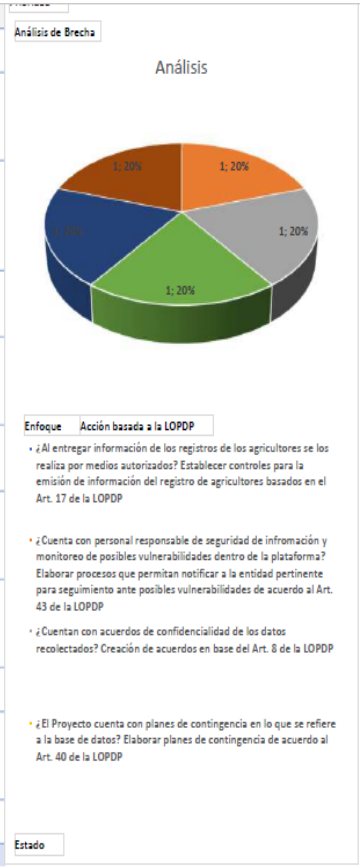
Nota: Elaboración propia.

Después del Análisis de Brechas realizado en la institución se puede identificar los enfoques y el estado de cada uno como, por ejemplo: No implementado, Si implementado (pero falta de actualización).

Figura 9

Análisis de Brecha Situación Actual - Estado.

Enfoque	Análisis	En Proceso	Hecho	Total general
¿Al entregar información de los registros de los agricultores se los realiza por medios autorizados?			1	1
Establecer controles para la emisión de información del registro de agricultores basados en el Art. 17 de la LOPDP			1	1
¿Cuenta con personal responsable de seguridad de infromación y monitoreo de posibles vulnerabilidades dentro de la plataforma?	1			1
Elaborar procesos que permitan notificar a la entidad pertinente para seguimiento ante posibles vulnerabilidades de acuerdo al Art. 43 de la LOPDP	1			1
¿Cuentan con acuerdos de confidencialidad de los datos recolectados?	1			1
Creación de acuerdos en base del Art. 8 de la LOPDP	1			1
¿El Proyecto cuenta con planes de contingencia en lo que se refiere a la base de datos?		1		1
Elaborar planes de contingencia de acuerdo al Art. 40 de la LOPDP		1		1
¿El proyecto cuenta con politicas de seguridad al receptar información de agricultores a nivel nacional?		1		1
Desarrollo de Políticas en base del Art. 38 de la LOPDP		1		1
¿El Proyecto cuenta con un responsabe del tratamiento de los datos personales?	1			1
Establecer responsables de acuerdo al Art. 48 de la LOPDP	1			1
¿Se tiene controles de medios electrónicos a utilizar dentro de la institución para salvaguardar la información y evitar fuga de datos ?	1			1
Establecer controles de medios eléctronicos dentro de la institución basados en el Art. 17 de la LOPDP	1			1
¿Si un agricultor desea dar por terminado su solicitud al beneficio, se procede a eliminar su información de la base de datos ?	1			1
Establecer un acuerdo en base al Art. 15 de la LOPDP	1			1
¿Tiene Controles de acceso a la información de base de datos ?			1	1
Sugerir mejoras al área encargada de los accesos en base al Art.37 de la LOPDP			1	1
¿Tienen Políticas de Seguridad de Información dentro del área de Sistemas?		1		1
Actualizar las Políticas de acuerdo a las normativas vigentes, en base del Art.37 de la LOPDP		1		1
Total general	5	3	2	10

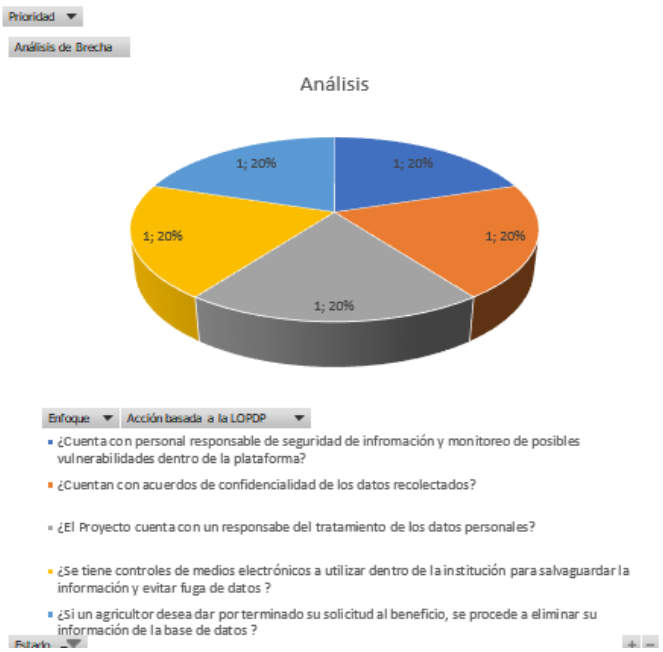


Nota: Elaboración propia.

Se puede verificar que hay tres estados: En análisis, en proceso y hecho, ya que algunas recomendaciones se han ido acogiendo y realizando acorde a lo recomendado.

Figura 10

Enfoque - estado en análisis.



Nota: Elaboración propia.

Figura 11

Enfoque - estado en proceso.

Nota: Elaboración propia.

Figura 12

Enfoque - estado hecho.

Nota: Elaboración propia.

a. Explicación del aporte

En el marco de la seguridad informática y la protección de datos personales enfocado a los agricultores en todo el territorio nacional, hace que la propuesta de trabajo se enfoque en el objetivo ODS N°11 ya que permite contribuir con las comunidades sostenibles, lo que de cierta manera aporta un avance en la actualidad, por lo que directamente se basa a un derecho que todas personas ya sea natural o jurídica deben beneficiarse y que por ley accede al tratamiento de los datos personales.

No obstante, dentro del Art. 23 de la LOPDP establece el derecho a la educación digital, no todas las personas han logrado acceder a ese derecho, por motivos al desconocimiento o caso omiso, con este trabajo, se pretende que de alguna manera los agricultores sean beneficiarios directos con lo que contempla la normativa vigente.

b. Estrategias y/o técnicas

Para la elaboración del producto se realizó la revisión de la normativa legal y vigente para poder realizar un análisis en cuanto a la ley orgánica de protección de datos personales, también se realizó un análisis de brecha GAP de la situación actual de la institución para poder tener en cuenta dónde partimos y dónde queremos llegar con el producto.

Parte de la elaboración de la propuesta está también contemplado una alineación en cuanto a la LOPDP con buenas prácticas COBIT 2019, donde de acuerdo al artículo de la ley se puede cubrir con los dominios de COBIT 2019 del porqué debe existir cada propuesta detallada.

2.3 Validación de la propuesta

Esta matriz fue planteada al área de sistemas y de planificación del PNSAE, para la ejecución y puesta en marcha y así cumplir con la normativa vigente.

Tabla 5

Análisis de Brecha alineada a la LOPDP cubierto con COBIT 2019 (Buenas Prácticas).

Estado actual	Estado futuro	Brecha	Acción basada a la LOPDP	Buenas Prácticas COBIT 2019
NO	Contar con Políticas	50%	Desarrollo de Políticas en base del Art. 38 de la LOPDP	APO14
NO	Contar con acuerdos	75%	Creación de acuerdos en base del Art. 8 de la LOPDP	APO13
SI	Reforzar	75%	Actualizar las Políticas de acuerdo a las normativas vigentes, en base del Art.37 de la LOPDP	APO13
SI	Mejorar el control	50%	Establecer controles para la emisión de información del registro de agricultores basados en el Art. 17 de la LOPDP	APO14
NO	Contar con Controles de Seguridad	75%	Establecer controles de medios electrónicos dentro de la institución	APO14

			basados en el Art. 17 de la LOPDP	
SI	Actualizar controles de acceso a las Bases de Datos	75%	Sugerir mejoras al área encargada de los accesos en base al Art.37 de la LOPDP	APO13
NO	Establecer acuerdos de terminación de tratamiento de datos	25%	Establecer un acuerdo en base al Art. 15 de la LOPDP	APO14
NO	Establecer planes de contingencia	75%	Elaborar planes de contingencia de acuerdo al Art. 40 de la LOPDP	APO12
NO	Establecer profesionales encargados en ciberseguridad	50%	Elaborar procesos que permitan notificar a la entidad pertinente para seguimiento ante posibles vulnerabilidades de acuerdo al Art. 43 de la LOPDP	MEA02
NO	Establecer un responsable	75%	Establecer responsables de acuerdo al Art. 48 de la LOPDP	APO14

Nota: Elaboración propia.

Mediante lo determinado por la ley y buenas prácticas de COBIT se procede armar la matriz RACI con la que se indicará los roles y responsabilidades de cada uno de los que interactúen en el proceso. **Anexo 8**

1.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 6

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	Recursos Tic's
Análisis de la Normativa legal respecto a la LOPDP	Ley Orgánica de Datos Personales	Revisión documental y experimental	Revisión de la normativa legal y vigente	De acuerdo a lo revisado se puede verificar ciertas normas y artículos que ayudarán a cumplir con la normativa vigente	PDF
Análisis de Buenas Prácticas – COBIT 2019	Marco de Trabajo para Gobierno y Gestión de la Información	Revisión documental y experimental	Revisión de la actualización vigente	Uso de buenas prácticas para la implementación de objetivos de gobierno y gestión	PDF
Encuestas realizadas a los beneficiarios directos e indirectos	Proceso investigativo metodológico, investigación cualitativa	Encuestas, revisión documental.	Elaboración de encuestas.	Se elaboran encuestas con el fin de analizar la situación actual de los procesos de recolección de datos.	Word, Excel
Análisis de brechas mediante una matriz GAP	Análisis FODA como técnica de gestión	Experimental	Elaboración de matriz GAP	El análisis de brecha ayuda a identificar en qué punto se encuentra la institución en cuanto al tratamiento de datos y a qué punto se quiere llegar.	Word, Excel

Fuente: Elaboración propia

CONCLUSIONES

Durante el análisis de la normativa legal de la ley orgánica de protección de datos personales se pudo evidenciar que dentro de uno de los artículos se encuentra el derecho a la educación digital, como tal el Art. 23 es un derecho que todas las personas en el territorio nacional deberá acceder y hacer educados para que puedan de alguna manera garantizar y de ser el caso autorizar el uso adecuado del procedimiento de la información personal, el Art. 3 Ámbito de aplicación territorial, esto quiere decir que la ley se cumplirá dentro de todo el territorio nacional, y de acuerdo a lo establecido a partir del 26 de mayo del 2023 se deberá aplicar y de no acatar con la disposición se presentarán las posibles sanciones.

Después de realizar el análisis de brecha se pudo identificar que la institución actualmente no cuenta con políticas ni controles de seguridad al momento de receptar información, poniendo así en peligro toda la información recolectada de los agricultores, dejando unas brechas de seguridad expuestas a pérdida de información y mal uso de los datos.

Mediante la elaboración de la matriz de brecha GAP se pudo ir alineando los enfoques o controles a la LOPDP precisamente cubriendo cada uno de ellos con buenas prácticas de COBIT 2019 para una adecuada implementación y así prevenir incidentes durante el tratamiento de los datos personales.

Con el desarrollo de esta propuesta se pudo contribuir con uno de los objetivos ODS para ser exactos el N°11 el cual cubre el desarrollo de las comunidades sostenibles, esto al ser el agricultor un beneficiario directo, se establece el derecho a la protección de datos personales.

RECOMENDACIONES

Se recomienda una vez aplicada la ley orgánica de protección de datos personales realizar un nuevo estudio a la normativa ya que puede darse alguna modificación o a su vez verificar el ente regulador de hacer cumplir lo establecido, que otras disposiciones adapta, con el fin de que la institución no sea sancionada por el incumplimiento a la normativa.

En el trabajo realizado se estableció propuestas para solventar las brechas de seguridad encontradas con el propósito de mejorar el control de los procesos actuales que tiene el PNSAE con respecto al tratamiento de los datos personales, por lo que se recomienda poner en práctica dichas recomendaciones, con el fin de garantizar el uso adecuado de los datos.

El uso de buenas prácticas es recomendable alinear a la LOPDP para así tener unos objetivos de gobierno y gestión adecuada, también se recomienda la revisión de la ISO 2700 2 ya que está también enfocada a los controles.

Uno de los fuertes y fortaleciendo el objetivo ODS N°11 es realizar capacitaciones al personal de técnicos de campo y a su vez ellos transmitan los conocimientos en las juntas realizadas y socializando a los agricultores sobre el uso adecuado de los datos personales, esto de alguna manera llegará a más personas a nivel nacional haciendo así un mejor futuro en cuanto a la educación digital.

BIBLIOGRAFÍA

Aguilar Corredin, E. L., & Montero Mahecha, Y. A. (2018). *Metodología dirigida a compañías distribuidoras de tecnología para el manejo y protección de los datos personales de terceros de acuerdo a la ley estatutaria 1581 del 2012 y el decreto 1377 de 2013*.

Arellano López, C. A. (2020). El derecho de protección de datos personales. *Biolex*, *12*(23), 163-174.

Amaro, M. C. (2020). La seguridad de los datos personales y la obligación de notificar las brechas de seguridad. *Revista de Derecho, Empresa y Sociedad (REDS), 16*, 151-162.

Benussi Díaz, C. (2020). Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes. *Revista chilena de derecho y tecnología*, *9*(1), 227-279.

Burbano Sánchez, M. V. (2021). *Diseño de un marco de trabajo para el análisis de impacto del proyecto de ley de protección de datos en el Ecuador en empresas privadas.* Quito, 2021.

Calisaya Sana, C. Y., & Tarrillo Villegas, M. (2018). *Implementación de controles de seguridad para la protección de datos personales en una Universidad Privada para el cumplimiento parcial de la Ley 29733 basado en los controles de seguridad de la NTP-ISO/IEC 17799: 2007*.

¿Qué es COBIT 5? Entendiendo el Gobierno de TI ó IT Governance. (2018, enero 24). Genius IT Training. https://geniusitt.com/blog/que-es-cobit-5/

Dirección de Educación en Línea (Director). (2017, marzo 22). Ley de comercio electrónico—Ley 67—Derecho Informático—Udla en línea. https://www.youtube.com/watch?v=6wPYEPx9UIk

Enríquez Álvarez, L. F. (2017). *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 (Tema Central)*.

Investigación cualitativa y cuantitativa. (s. f.). Significados. Recuperado 19 de agosto de 2022, de https://www.significados.com/investigacion-cualitativa-y-cuantitativa/

GUÍA DE PROTECCIÓN DE DATOS PERSONALES. (s. f.). 6.

Garzón, M. P. R., & Olmos, D. P. A. (s. f.). *Seguridad informática: Relación e impacto frente a la ley de protección de datos personales (Ley 1581 de 2012).*

Gob.ec (S/f). *Gob.ec. Recuperado el 23 de junio de 2022, de* https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Gómez, I., & Montoya, N. (2018). *Propuesta de implementación y cumplimiento de la LGPDPPSO a través de la plataforma de protección de datos personales en posesión de INFOTEC*. Tesis de Maestría, INFOTEC Centro de Investigación e Innovación en

Pineda, L. O. (2021). El derecho fundamental a la protección de datos personales en Ecuador. *P erspectivas*, *5*

Ruiz Concha, J. J. (s. f.). *Modelo para la implementación de la ley de protección de datos personales basado en el SGSI de la norma ISO 27001*

Rallo Lombarte, A. (2019). *El nuevo derecho de protección de datos*.

ANEXO 1

LOPDP			LEY DE COMERCIO ELECTRÓNICO		
Articulo	Ley	Descripción	Articulo	Ley	Descripción
Art. 12	Derecho a la información	El titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparencia por cualquier medio.	Art. 5	Confidencialidad y reserva	Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención.
Art. 13	Derecho de acceso	El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente sin necesidad de presentar justificación alguna.	Art. 7	Información original	Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos
Art. 15	Derecho de eliminación	El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales.	Art. 9	Protección de datos	Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

Art. 33	Transferencia o comunicación de datos personales	Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legitimas del responsable y del destinatario.	Art. 34	Terminación contractual	La terminación del contrato entre las entidades de certificación acreditadas y el suscriptor se sujetará a las normas previstas en la Ley Orgánica de Defensa del Consumidor.
Art. 35	Acceso a datos personales por parte de terceros	No se considerará transferencia o comunicación cuando el acceso a datos personales por un tercero sea necesario para la presentación de un servicio al responsable del tratamiento de datos personales.	Art. 35	Notificación de cesación de actividades	Las entidades de certificación de información acreditadas, deberán notificar al Organismo de Control, por lo menos con noventa días de anticipación, la cesación de sus actividades y se sujetarán a las normas y procedimientos establecidos en los reglamentos que se dicten para el efecto
Art. 38	Medidas de seguridad en el ámbito del sector público	El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, acceso no autorizado, perdida, alteración, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.	Art. 40	Infracciones administrativas	Para los efectos previstos en la presente ley, las infracciones administrativas se clasifican en leves y graves.
			Art. 41	Sanciones	La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de

			información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios
	Art. 49	Consentimiento para el uso de medios electrónicos	De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información
	Art. 58-2	Obtención y utilización no autorizada de información	La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares

ANEXO 2

20 CONTROLES SANS	
CSC 1	Inventario de dispositivos autorizados y no autorizados
CSC 2	Inventario de software autorizado y no autorizado
CSC 3	Configuraciones seguras de hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores
CSC 4	Evaluación y reparación continuas de vulnerabilidades
CSC 5	Uso controlado de Privilegios administrativos
CSC 6	Mantenimiento, monitoreo y análisis de registros de auditoría
CSC 7	Protecciones de correo electrónico y navegador web
CSC 8	Defensas contra malware
CSC 9	Limitación y control de puertos, protocolos y servicios de red
CSC 10	Capacidad de recuperación de datos
CSC 11	Configuraciones seguras para dispositivos de red, como cortafuegos, enrutadores y conmutadores
CSC 12	Defensa de límites
CSC 13	Protección de datos
CSC 14	Acceso controlado basado en la necesidad de saber
CSC 15	Control de acceso inalámbrico
CSC 16	Monitoreo y control de cuentas
CSC 17	Evaluación de habilidades de seguridad y capacitación adecuada para llenar los vacíos
CSC 18	Seguridad del software de aplicaciones
CSC 19	Respuesta y gestión de incidentes
CSC 20	Pruebas de penetración y ejercicios del equipo rojo

ANEXO 3

FORMATO DE ENCUESTA

Ministerio de Agricultura y Ganadería

INFORMACIÓN DE RECOLECCIÓN DE DATOS

La siguiente encuesta está diseñada para verificar como se realiza el proceso de recolección de información por parte de los técnicos a los agricultores.

Preguntas	SI	Poco Conocimiento	NO
¿Sabe usted para que se usarán los datos recolectados por los técnicos de campo?			
¿Sabe usted que tiempo tiene de duración su información dentro de los sistemas del proyecto del PNSAE?			
¿Sabe usted que sus datos entregados pueden ser utilizados por terceras personas?			
¿Sabe usted que sus datos personales son utilizados para el único fin por el cual entrego su información?			
¿Sabe usted como identificar a un funcionario del ministerio de agricultura y ganadería?			
¿Sabe usted de la protección de datos personales?			
¿Sabe usted que una vez terminado el proceso de la intervención sus datos siguen siendo tratados para seguimiento y evaluación?			

ANEXO 4

CONTROLES NORMATIVA PROPUESTA				
Artículo	LOPDP	Proceso COBIT	Nombre del Proceso	Control COBIT
Art. 12	Derecho a la información	APO14	Datos Gestionados	Gestionar los procesos de respaldo y recuperación de datos
Art. 13	Derecho de acceso	APO14	Datos Gestionados	Gestionar los procesos de respaldo y recuperación de datos
Art. 15	Derecho de eliminación	APO14	Datos Gestionados	Manejar el ciclo de vida de los activos de información
Art. 33	Transferencia o comunicación de datos personales	APO14	Datos Gestionados	Establecer los procesos e infraestructura para la metadata y su gestión
Art. 35	Acceso a datos personales por parte de terceros	APO13	Gestionar la Seguridad	Definir y administrar un plan de tratamiento de riesgos de seguridad de la información
Art. 38	Medidas de seguridad en el ámbito del sector público	APO13	Gestionar la Seguridad	Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)

ANEXO 5

FORMATO DE ENCUESTA LLENO

Ministerio de Agricultura y Ganadería

INFORMACIÓN DE RECOLECCIÓN DE DATOS

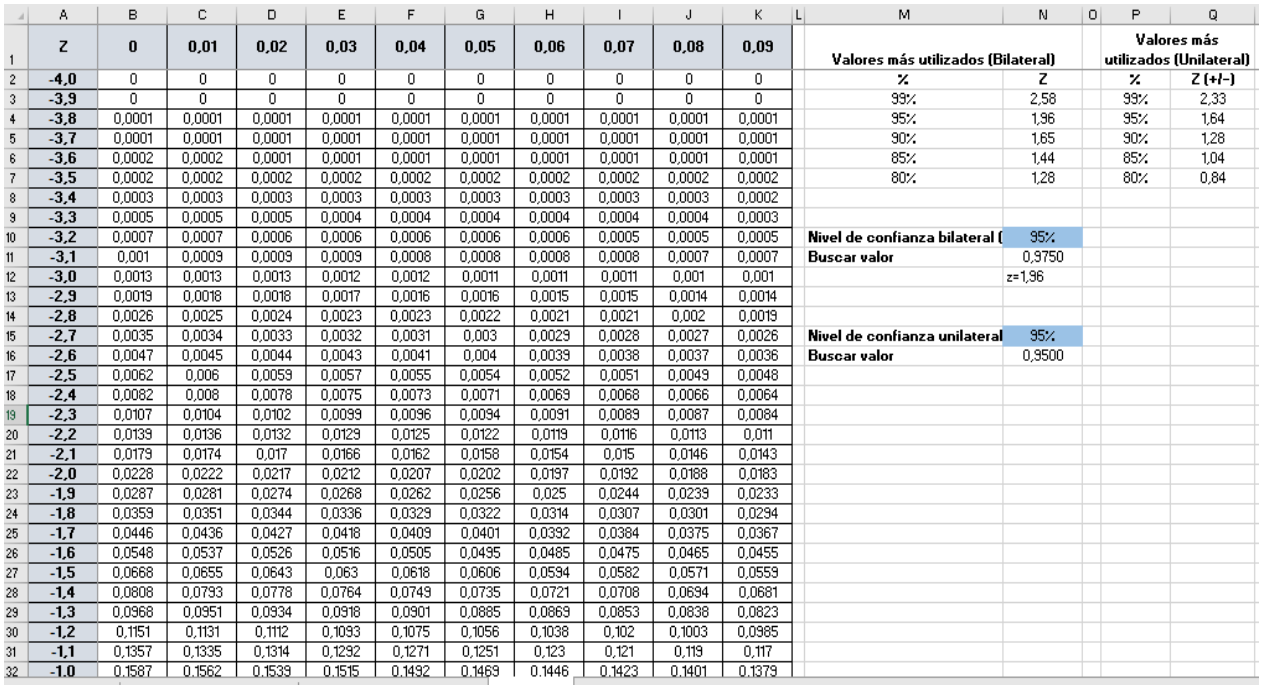
La siguiente encuesta está diseñada para verificar como se realiza el proceso de recolección de información por parte de los técnicos a los agricultores y si los agricultores tienen conocimiento de cómo y para que se está utilizando su información entregada.

Preguntas	SI	Poco Conocimiento	NO
¿Sabe usted para que se usarán los datos recolectados por los técnicos de campo?	X		
¿Sabe usted que tiempo tiene de duración su información dentro de los sistemas del proyecto del PNSAE?		X	
¿Sabe usted que sus datos entregados pueden ser utilizados por terceras personas?			X
¿Sabe usted que sus datos personales son utilizados para el único fin por el cual entrego su información?		X	
¿Sabe usted como identificar a un funcionario del ministerio de agricultura y ganadería?	X		
¿Sabe usted de la protección de datos personales?			X
¿Sabe usted que una vez terminado el proceso de la intervención sus datos siguen siendo tratados para seguimiento y evaluación?		X	

ANEXO 6

Análisis de la Muestra

Muestras Cualitativa	
Población Finita/Conocida	
Nivel de Confianza	90%
Z	1,65
p	10%
q	90%
E	5%
N	1300
n	**92**



Z	0	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09
-4,0	0	0	0	0	0	0	0	0	0	0
-3,9	0	0	0	0	0	0	0	0	0	0
-3,8	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001
-3,7	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001
-3,6	0,0002	0,0002	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001	0,0001
-3,5	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002
-3,4	0,0003	0,0003	0,0003	0,0003	0,0003	0,0003	0,0003	0,0003	0,0003	0,0002
-3,3	0,0005	0,0005	0,0005	0,0004	0,0004	0,0004	0,0004	0,0004	0,0004	0,0003
-3,2	0,0007	0,0007	0,0006	0,0006	0,0006	0,0006	0,0006	0,0005	0,0005	0,0005
-3,1	0,001	0,0009	0,0009	0,0009	0,0008	0,0008	0,0008	0,0008	0,0007	0,0007
-3,0	0,0013	0,0013	0,0013	0,0012	0,0012	0,0011	0,0011	0,0011	0,001	0,001
-2,9	0,0019	0,0018	0,0018	0,0017	0,0016	0,0016	0,0015	0,0015	0,0014	0,0014
-2,8	0,0026	0,0025	0,0024	0,0023	0,0023	0,0022	0,0021	0,0021	0,002	0,0019
-2,7	0,0035	0,0034	0,0033	0,0032	0,0031	0,003	0,0029	0,0028	0,0027	0,0026
-2,6	0,0047	0,0045	0,0044	0,0043	0,0041	0,004	0,0039	0,0038	0,0037	0,0036
-2,5	0,0062	0,006	0,0059	0,0057	0,0055	0,0054	0,0052	0,0051	0,0049	0,0048
-2,4	0,0082	0,008	0,0078	0,0075	0,0073	0,0071	0,0069	0,0068	0,0066	0,0064
-2,3	0,0107	0,0104	0,0102	0,0099	0,0096	0,0094	0,0091	0,0089	0,0087	0,0084
-2,2	0,0139	0,0136	0,0132	0,0129	0,0125	0,0122	0,0119	0,0116	0,0113	0,011
-2,1	0,0179	0,0174	0,017	0,0166	0,0162	0,0158	0,0154	0,015	0,0146	0,0143
-2,0	0,0228	0,0222	0,0217	0,0212	0,0207	0,0202	0,0197	0,0192	0,0188	0,0183
-1,9	0,0287	0,0281	0,0274	0,0268	0,0262	0,0256	0,025	0,0244	0,0239	0,0233
-1,8	0,0359	0,0351	0,0344	0,0336	0,0329	0,0322	0,0314	0,0307	0,0301	0,0294
-1,7	0,0446	0,0436	0,0427	0,0418	0,0409	0,0401	0,0392	0,0384	0,0375	0,0367
-1,6	0,0548	0,0537	0,0526	0,0516	0,0505	0,0495	0,0485	0,0475	0,0465	0,0455
-1,5	0,0668	0,0655	0,0643	0,063	0,0618	0,0606	0,0594	0,0582	0,0571	0,0559
-1,4	0,0808	0,0793	0,0778	0,0764	0,0749	0,0735	0,0721	0,0708	0,0694	0,0681
-1,3	0,0968	0,0951	0,0934	0,0918	0,0901	0,0885	0,0869	0,0853	0,0838	0,0823
-1,2	0,1151	0,1131	0,1112	0,1093	0,1075	0,1056	0,1038	0,102	0,1003	0,0985
-1,1	0,1357	0,1335	0,1314	0,1292	0,1271	0,1251	0,123	0,121	0,119	0,117
-1,0	0,1587	0,1562	0,1539	0,1515	0,1492	0,1469	0,1446	0,1423	0,1401	0,1379

Valores más utilizados (Bilateral)	
%	Z
99%	2,58
95%	1,96
90%	1,65
85%	1,44
80%	1,28
Nivel de confianza bilateral (	95%
Buscar valor	0,9750
	z=1,96
Nivel de confianza unilateral	95%
Buscar valor	0,9500

Valores más utilizados (Unilateral)	
%	Z (+/-)
99%	2,33
95%	1,64
90%	1,28
85%	1,04
80%	0,84

ANEXO 7

MATRIZ DE ANÁLISIS DE BRECHA - GAP

Ministerio de Agricultura y Ganadería

Análisis de Brechas

Proyecto	Análista Funcional del Proyecto	Fecha
Proyecto Nacional de Semillas para Agrocadenas Estratégicas (PNSAE)	Sandra Elizabeth Ron	20/8/2022

Enfoque	Estado actual	Estado futuro	Brecha	Acción basada a la LOPDP	Buenas Prácticas COBIT 2019	Prioridad	comienzo	Final	Viable	Dueño	Estado	notas
¿El proyecto cuenta con políticas de seguridad al receptar información de agricultores a nivel nacional?	NO	Contar con Políticas	50%	Desarrollo de Políticas en base del Art. 38 de la LOPDP	APO14	Alto	1/7/2022	30/11/2022	SI	TI	En Proceso	
¿Cuentan con acuerdos de confidencialidad de los datos recolectados?	NO	2 Acuerdos	75%	Creación de acuerdos en base del Art. 8 de la LOPDP	APO13	Alto	1/8/2022	30/9/2022	SI	Jurídico / TI	Análisis	
¿Tienen Políticas de Seguridad de Información dentro del área de Sistemas?	SI	Reforzar	75%	Actualizar las Políticas de acuerdo a las normativas vigentes, en base del Art.37 de la LOPDP	APO13	Medio	1/1/2022	31/12/2022	SI	TI	En Proceso	Depende de la gobernanza de TI y del Ministerio
¿Al entregar información de los registros de los agricultores se los realiza por medios autorizados?	N/A	Mejorar el control	50%	Establecer controles para la emisión de información del registro de agricultores basados en el Art. 17 de la LOPDP	APO14	Medio	1/8/2022	15/8/2022	SI	TI / Planificación	Hecho	Aprobado por Gerencia
¿Se tiene controles de medios electrónicos a utilizar dentro de la institución para salvaguardar la información y evitar fuga de datos ?	NO	Contar con Controles de Seguridad	75%	Establecer controles de medios eléctronicos dentro de la institución basados en el Art. 17 de la LOPDP	APO14	Medio	1/8/2022	30/9/2022	SI	TI	Análisis	
¿Tiene Controles de acceso a la información de base de datos ?	SI	N/A	75%	Sugerir mejoras al área encargada de los accesos en base al Art.37 de la LOPDP	APO13	Bajo	1/8/2022	2/8/2022	SI	TI	Hecho	Sugerencia entregada al área responsable
¿Si un agricultor desea dar por terminado su solicitud al beneficio, se procede a eliminar su información de la base de datos ?	NO	N/A	25%	Establecer un acuerdo en base al Art. 15 de la LOPDP	APO14	Alto	1/8/2022	30/9/2022	SI	Jurídico / TI	Análisis	
¿El Proyecto cuenta con planes de contingencia en lo que se refiere a la base de datos?	NO	Establecer planes de contingencia	75%	Elaborar planes de contingencia de acuerdo al Art. 40 de la LOPDP	APO12	Alto	1/8/2022	15/10/2022	SI	TI / Planificación	En Proceso	
¿Cuenta con personal responsable de seguridad de infromación y monitoreo de posibles vulnerabilidades dentro de la plataforma?	NO	Establecer profesionales encargados en cibersegurdad	50%	Elaborar procesos que permitan notificar a la entidad pertinente para seguimiento ante posibles vulnerabilidades de acuerdo al Art. 43 de la LOPDP	MEA02	Medio	1/8/2022	15/10/2022	SI	TI / Planificación	Análisis	
¿El Proyecto cuenta con un responsabe del tratamiento de los datos personales?	NO	Establecer un Responsable	75%	Establecer responsables de acuerdo al Art. 48 de la LOPDP	APO14	Alto	1/8/2022	15/10/2022	SI	RRHH	Análisis	Depende del área de RRHH y Planificación de la Institución

Anexo 8

Matriz RACI

Roles y responsabilidades

PNSAE

Responsable, A Rinde Cuentas, Consultado, Informado

ROLES	Gerencia	Coordinación TI	Planificación	Responsable de Procesos TI	Riesgo y Cumplimiento	Área Jurídica	Líder Técnico	Responsable del SISCOMTEC	Responsable DB
Procesos									
Establecer políticas de seguridad al receptar información de agricultores a nivel nacional	I	R	C	A	C	I	C	I	I
Designar responsable de seguridad de información y monitoreo de posibles vulnerabilidades dentro de la plataforma	I	I	I	A	R	I	C	A	C
Derecho de eliminación	C	I	I	R	A	A	I	A	C
Transferencia o comunicación de datos personales	C	R	I	R	A	I	C	A	C
Acceso a datos personales por parte de terceros	C	C	I	C	A	I	I	A	C
Establecer controles de medios electrónicos a utilizar dentro de la institución para salvaguardar la información y evitar fuga de datos	I	R	I	A	A	C	I	C	I
Crear acuerdos de confidencialidad de los datos recolectados	I	R	I	A	A	A	I	I	C
Elaborar Políticas de Seguridad de Información dentro del área de Sistemas	I	R	C	A	A	C	I	A	C

R	Responsable	Asignado para completar la tarea
A	Rinde Cuentas	Esta persona realiza la tarea o entrega. Ellos se comprometen a hacer el trabajo o tomar las decisiones.
C	Consultado	Un asesor, parte interesada o experto en la materia que es consultado antes de una decisión o acción
I	Informado	Debe ser informado después de una decisión o acción

Anexo 9

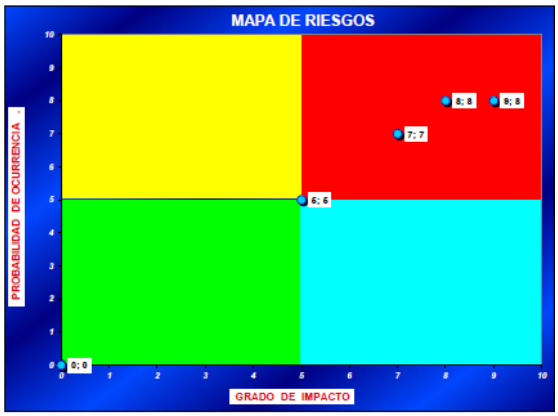
MAPA DE RIESGOS EN LA RECOLECCIÓN DE DATOS

MAPA DE RIESGOS INSTITUCIONAL 2022

RAMO / SECTOR: SECTOR PÚBLICO

INSTITUCIÓN: MINISTERIO DE AGRICULTURA Y GANADERÍA

No. de Riesgo	RIESGO	Clasificación del Riesgo	III. VALORACIÓN DE RIESGOS VS. CONTROLES	
			Valoración Final	
			GRADO DE IMPACTO	PROBABILIDAD DE OCURRENCIA
2022_1	INFORMACIÓN REGISTRADA SIN POLITICAS DE SEGURIDAD	De Recursos Humanos	8	8
2022_2	INFORMACIÓN DE PREDIOS Y COORDENADAS REGISTRADA SIN POLITICAS DE SEGURIDAD	De Recursos Humanos	7	7
2022_3	ENTREGA DE INFORME DE INFORMACIÓN DE AGRICULTORES A NIVEL NACIONAL	Administrativo	5	5
2022_4	PERDIDA DE INFORMACIÓN DE UBICACIÓN GEOGRAFICA Y DIRECCIONES DE PREDIOS DE LOS AGRICULTORES	De Recursos Humanos	9	8



SUPERVISÓ

DAVID FERNANDO SILVA TURNER,
Coordinador de Control Interno

AUTORIZÓ

CHRISTIAN RICARDO SUAREZ SUAREZ,
Titular de la Institución

INTEGRÓ

SANDRA ELIZABET RON,
Enlace de Administración de Riesgos