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 MAGISTER

Título del proyecto:
Propuesta de políticas de uso de servicios mediante el modelo cloud computing o seguridad en la nube para las estructuras sensibles como la base de datos de una ONG
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Gustavo Miguel Vega Panchi
Tutores:
Mg. Renato Mauricio Toasa Guachi PhD. Maryory Urdaneta Herrera

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, **RENATO MAURICIO TOASA GUACHI** con C.I: **180472416-7** en mi calidad de Tutor del proyecto de investigación titulado: **PROPUESTA DE POLÍTICAS DE USO DE SERVICIOS MEDIANTE EL MODELO CLOUD COMPUTING O SEGURIDAD EN LA NUBE PARA LAS ESTRUCTURAS SENSIBLES COMO LA BASE DE DATOS DE UNA ONG.**

Elaborado por: **GUSTAVO MIGUEL VEGA PANCHI**, de C.I: **171016890-5**, 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., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

Mg. RENATO MAURICIO TOASA GUACHI

ORCID: 0000-0002-2138-300X

APROBACIÓN DEL TUTOR

Yo, **MARYORY URDANETA HERRERA** con C.I: **1759316126** en mi calidad de Tutor del proyecto de investigación titulado: **PROPUESTA DE POLÍTICAS DE USO DE SERVICIOS MEDIANTE EL MODELO CLOUD COMPUTING O SEGURIDAD EN LA NUBE PARA LAS ESTRUCTURAS SENSIBLES COMO LA BASE DE DATOS DE UNA ONG.**

Elaborado por: **GUSTAVO MIGUEL VEGA PANCHI**, de C.I: **171016890-5**, 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., marzo de 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

PhD. MARYORY URDANETA HERRERA

ORDIC: 0000-0001-8773-5349

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, **GUSTAVO MIGUEL VEGA PANCHI** con C.I: **171016890-5**, autor del proyecto de titulación denominado: **PROPUESTA DE POLÍTICAS DE USO DE SERVICIOS MEDIANTE EL MODELO CLOUD COMPUTING O SEGURIDAD EN LA NUBE PARA LAS ESTRUCTURAS SENSIBLES COMO LA BASE DE DATOS DE UNA ONG**. 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., marzo de 2024

Firmado electrónicamente por:
GUSTAVO MIGUEL VEGA PANCHI

_____

Firma: GUSTAVO MIGUEL VEGA PANCHI

ORCID: 0009-0000-8411-8476

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

El tema de investigación está enmarcado en la propuesta de políticas de uso de servicios mediante el modelo Cloud computing o seguridad en la nube para las estructuras sensibles como la base de datos de una ONG. Hoy en día, la protección de la información es fundamental en el desarrollo socioeconómico y bienestar de las organizaciones de modo que no sea vea vulnerada por factores internos o externos mediante los ciberataques de naturaleza informática. En este orden, se hace indispensable contar con políticas de uso de servicios modelos de seguridad de la información, con políticas y mecanismos que permitan mitigar estos ataques y a su vez medir su impacto, crecimiento y uso.

El presente proyecto se sostiene en el aseguramiento de la información mediante el modelo en la nube (cloud computing) con las que debe contar la ONG y las cuales debe seguir para la implementación de políticas de uso de este tipo de servicio, a fin de que se conserve la seguridad de los datos en este tipo de ambientes.

De acuerdo con la ACNUR (2023) las Organizaciones No Gubernamentales tiene como función prestación de servicios públicos; estas organizaciones no dependen del Estado ni de ningún ente público o privado; sin embargo, sus actividades y beneficios involucran a los distintos miembros de una comunidad. Su objetivo es el del beneficio común, lo que reciben está destinado al bienestar de las comunidades donde realizan sus proyectos. el principal objetivo de las ONG consiste en trabajar por la participación y la autogestión de las comunidades que ayudan. De esta forma, cada vez se ven más involucrados en su propio desarrollo y no dependen de agentes externos.

En esta línea es importante *contextualizar* que, el cloud computing de acuerdo con Recalde y Veloso (2022) “es una arquitectura de prestación y aprovisionamiento de servicios de tecnologías de la información y la comunicación que, en los últimos dos años, está adquiriendo bastante protagonismo” (p.24). Según analistas como Parra y Chimarro (2020), en los próximos cinco años se consolidará tanto entre los usuarios particulares de la red y servicios en línea, como entre las empresas; la manera de proteger los datos desde estos servicios.

La eficaz implementación de políticas de uso de servicio de información en la nube como controles de seguridad, privacidad, portabilidad, entre otros de la organización, reducirá el riesgo de que se presenten incidentes de seguridad que afecten la imagen de la entidad y generen un daño irreparable. Este estudio provee recomendaciones para minimizar los riesgos,

que se obtienen al tener información en la Nube especialmente la información sensible como la base de datos de la empresa en donde reposan la información sobre proveedores y cartera de clientes.

En el mundo actual que reviste de innovación y globalización, las empresas como organizaciones prestadoras de servicios, deben tomar acciones que beneficien el elemento más importante de su productividad y razón de ser como lo es el cliente, quien determina la demanda de los productos y/o servicios ofrecidos por estas, por lo que deben estar a la vanguardia de las tecnologías más recientes que les permitan proteger sus bases de datos y resguardar la información de sus clientes.

La empresa objeto de estudio responde a una ONG inició sus actividades operativas a partir del mes de julio del año 2011, está conformada por más de doscientos miembros comprendidos por empresas del sector público, privado, organizaciones de la sociedad civil, ONG, gremios y academia, de todo tamaño y origen, que se encuentran comprometidas con la aplicación de los diez principios y el respeto a los Derechos Humanos, Estándares Laborales, Medio Ambiente y la Lucha contra la Corrupción manejando información confidencial de clientes y proveedores por lo que amerita contar con sistema de servicio de cloud computing para la protección y seguridad de su base de datos.

El término "Cloud computing" se refiere a una manifestación tecnológica de las redes comunitarias, que incluyen, entre otros elementos, flujos de datos relevantes para individuos como los clientes de una ONG. Esta categoría es de gran importancia debido a su impacto en los derechos fundamentales de los titulares de los datos, quienes reciben un régimen de protección especial en comparación con el tratamiento que otros puedan dar a dichos datos. (Cortijo y Minta, 2022).

Es claro que las organizaciones deben reconocer y asegurar la libre circulación de información sensible de las personas como un principio fundamental (Escalona y Sánchez, 2020). Sin embargo, además de reconocer el derecho a recopilar, procesar y comunicar datos, es igualmente importante exigir un alto nivel de respeto hacia la persona a la que pertenecen esos datos. Si no se respeta este principio, la persona afectada verá reducida su capacidad para controlar el uso abusivo de su información (Recalde y Córdova, 2022).

La evolución del cloud computing ha ido demostrando su eficiencia para el resguardo de datos informáticos en donde sólo se emplea el uso de un dispositivo electrónico con acceso a Internet y acceder a los archivos o el software (Méndez, 2020). En este sentido y con el fin de obtener resultados de calidad en los procesos productivos y administrativos que se realizan

dentro de la organización, considerando esta acción como uno de los factores más importantes para poder trazar una ventaja competitiva respecto a la protección y seguridad de su base de datos e información confidencial relacionada a procesos eficientes, la mejora continua y el uso o implementación de la tecnología (Recalde y Tuabanda, 2023).

Las estructuras sensibles comprenden los ejes de sostenimiento de los datos con información delicada en informática, se consideran sensibles aquellos que puedan revelar aspectos de gran privacidad y se hallan en sistemas estructurales cibernéticos que pueden ser vulnerados y están constantemente expuestos a riesgos (Méndez , 2020).

De acuerdo con las estipulaciones de Sisti (2019) comprende una herramienta para recopilar y organizar información, estas pueden almacenar información sobre personas, productos, pedidos u otras cosas. Anteriormente se denominaba base de datos a una lista en una hoja de cálculo o en un programa de procesamiento de texto. Sin embargo, hoy en día se categoriza a las bases de datos como grandes plataformas digitales en donde ser resguarda información confidencial a gran escala de forma automatizada.

La propuesta de proyecto versa implementar políticas de uso servicios de cloud computing o seguridad en la nube para las estructuras sensibles como la base de datos de una ONG. Se busca garantizar la protección de la información recopilada contra ingresos no verificados, eliminación o alteración. Para lograrlo, se establecerán regulaciones como la encriptación de datos pasivos y activos, el control de accesos y los BackUp de seguridad. Además, se asegurará de que la información solo sea asequible por usuarios verificados, cumpliendo con las normas de privacidad y retención de información. También se certificará que los sistemas operativos y aplicativos o programas estén en la última versión y con los parches de seguridad actualizados, manteniendo firewalls de BDD y el Security Information and Event Management (SIEM) para proteger la información frente amenazas a la organización.

El proyecto también incluirá la configuración de sistemas de vigilancia y análisis de logs para identificar conductas inusuales y contrarrestar rápidamente los incidentes de seguridad. Asimismo, se establecerán planificaciones de recuperación en caso de fallos para garantizar la continuación del negocio en situaciones de interrupción o averías en la infraestructura.

Con el objetivo de desarrollar políticas basadas en el modelo de computación en la nube, se analizan los procesos, ventajas y limitaciones de este modelo, teniendo en cuenta ciertas incertidumbres sobre la seguridad de la información y la normativa vigente, y la determinación final es la reproducibilidad. Este modelo debe seguirse para garantizar un proceso de implementación segura. Para Haliux (2023) “los archivos almacenados en la nube son

responsabilidad de las empresas o de los individuos que utilizan el almacenamiento" (p.8). Las razones de esta rápida adquisición por parte de la ONG comprenden un nuevo modelo de políticas de protección para las organizaciones a menor precio y una baja complicación de gestión, que permite que estas respondan en seguridad hacia sus clientes.

Problema de investigación

Los modelos de computación en la nube se están convirtiendo en una forma alternativa de implementar servicios tecnológicos. La nube incluye almacenamiento, informática y espacio de archivos ubicados fuera de las oficinas del consumidor y conectados a través de Internet, y puede albergar varios servicios. Una Organización No Gubernamental - ONG ha migrado sus servicios a las plataformas digitales, por lo que ahora cuenta con más de 40 servicios de cloud computing en los que se incluyen jurídicos, financieros, planificación y administrativos.

Una organización no gubernamental (ONG) que estamos analizando inició sus operaciones en julio de 2011. Tiene más de 200 miembros, provenientes de todo el mundo, desde empresas públicas y privadas hasta organizaciones de la sociedad civil, otras organizaciones no gubernamentales, asociaciones profesionales y entidades académicas. El compromiso de todos estos miembros es seguir los diez principios de derechos humanos, normas laborales, medio ambiente y lucha contra la corrupción.

Actualmente toda organización de cualquier naturaleza siempre posee un centro de información para la toma de decisiones, siendo este el centro administrativo. Por tal razón, es de vital importancia que se cuente con procesos sistematizados mediante herramientas tecnológicas que admitan la gestión de información y bases de datos, pero primordialmente sobre su política de seguridad y tratamiento de dichos datos. Por lo que, sin políticas de servicios de cloud computing no podrán proteger sus registros y planificaciones confidenciales, que le permitan realizar sus actividades operativas de forma segura.

En Latinoamérica, según informe de Deloitte (2022) al cierre del trimestre en el año 2022 sólo el 40.5% de las empresas han contratado software de servicios de cloud computing, y se estimó que, para el primer semestre del 2023, alcanzaría un 55.5%, esto ha mostrado un índice muy bajo, por lo que aún las empresas no reconocen del todo la importancia de contar con este tipo de sistema que disminuya las amenazas y vulnerabilidades en los datos confidenciales, aumente la rentabilidad y eficiencia en cada operación.

Se estima que, hasta el año 2025, el 99% de los fallos de seguridad en la nube serán ocasionados por errores de los usuarios, según datos de la consultora Gartner. Asimismo, 9 de

cada 10 empresas van a compartir de forma inapropiada datos sensibles en la nube, siempre y cuando no logren tener un control sobre la manera en que utilizan los servicios cloud (INCENTRO, 2023).

Considerando esta información, la seguridad en la nube debe ser considerada de manera completa, involucrando a todas las partes interesadas. Los líderes empresariales deben establecer políticas y mecanismos de seguridad dentro de la organización, mientras que los funcionarios tienen la responsabilidad de acatarlas.

En Ecuador, se ha observado que la creciente movilidad en la entrega de servicios, el acceso desde varios dispositivos y la operación mediante flujos de datos presentan riesgos para la integridad y confidencialidad de la información en numerosas organizaciones. Por ejemplo, la violación de controles de identidad y autenticación o la alteración no autorizada de datos pueden ser ejemplos de esto (Escalona y Sánchez, 2020).

Las configuraciones incorrectas o las fallas de seguridad pueden causar filtraciones de datos confidenciales. Es posible que los datos confidenciales sean sustraídos, lo que podría tener graves consecuencias en términos de privacidad y cumplimiento de leyes. Por lo tanto, es fundamental implementar medidas de seguridad en la red para reducir estos peligros. Los ataques como estos tienen un impacto directo en la disponibilidad de los servicios en la nube. Los responsables de estos ataques pueden saturar los recursos de las organizaciones con tráfico malicioso, lo que impide que los servicios se presten adecuadamente.

En relación con lo mencionado anteriormente, esta ONG carece de políticas de seguridad y, por lo tanto, no tiene un modelo de gestión de seguridad en la nube para la información que maneja tanto con sus proveedores como con su base de clientes. Esto hace que sea difícil para ella responder a un posible ataque informático. La seguridad informática implica comprender los peligros y las consecuencias potenciales de las vulnerabilidades, que pueden causar pérdidas significativas para la empresa. Sin embargo, la entidad carece de este conocimiento y, por lo tanto, no ha implementado políticas internas ni mecanismos de seguridad que contribuyan a reducir estos riesgos, concentrándose especialmente en la protección de la confidencialidad, integridad y disponibilidad de la información.

Además, si el personal interno de la organización carece de cultura o comprensión de las políticas y medidas de prevención de seguridad informática, es posible que sea responsable directamente de abrir puertas para que un atacante pueda acceder a cualquier sistema de información de la organización. Además, se observa una falta de control adecuado en los

sistemas de gestión, lo que conduce a una merma de integridad, confiabilidad y disponibilidad de la información.

Debido a los puntos anteriores, la ONG requiere implementar políticas de uso de servicios mediante el modelo Cloud computing o seguridad en la nube para las estructuras sensibles como la base de datos de una ONG a fin de lograr una eficiencia operativa y la optimización de los procesos de la ONG, de acuerdo con cada una de sus necesidades particulares, posibilidad de integración con otras herramientas.

Objetivo general

Proponer políticas de uso de servicios mediante el modelo Cloud computing o seguridad en la nube para las estructuras sensibles como la base de datos de la ONG para el establecimiento de sistemas de seguridad informática.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre cloud competing relacionados a la protección de la base de datos.
- Diagnosticar la situación actual de la ONG sobre el tratamiento de seguridad referente a las estructuras sensibles.
- Proponer políticas de uso de servicios mediante el modelo cloud computing o seguridad en la nube basadas en controles de seguridad, privacidad y portabilidad.
- Valorar a través del criterio de especialistas las políticas de uso de servicios mediante el modelo *Cloud computing* o seguridad en la nube.

Vinculación con la sociedad y beneficiarios directos

La vinculación con la sociedad responde a ofertar un modelo de políticas de uso de servicios mediante el modelo Cloud computing o seguridad en la nube para las estructuras sensibles como la base de datos en organizaciones a fin de establecer sistemas de seguridad informática que manejan grandes flujos de datos de una ONG.

Desde esta investigación se documenta la relevancia que organizaciones como la ONG y empresas puedan con normativas y políticas esenciales para protección de la privacidad, de su información, especialmente hoy en día, en donde los datos se manejan desde plataformas tecnológicas que muchas veces llegan a ser vulneradas. En este sentido este proyecto se resume al desarrollo de una propuesta sustentada en garantizar el entorno digital seguro y confiable en donde se promueva una seguridad informática eficiente.

En este sentido, la necesidad creciente de las organizaciones y empresas de contar con políticas de uso de servicios mediante el modelo Cloud computing o seguridad en la nube para las estructuras sensibles como la base de datos y establecerlas de forma eficiente dentro de sus sistemas de información como activo fundamental, resulta como prioridad dentro de este proyecto que en principio es beneficiario la ONG y que al ser publicado beneficiará a otras organizaciones que estén en búsqueda de este tipo de modelo para implementar normas de seguridad informática.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

1.1.1 Contexto de la investigación

En la actualidad muchas organizaciones han hecho uso de la tecnología y de los sistemas de información a fin lograr sus objetivos, esto ha admitido que sus procesos sean optimizados cargando grandes datos de información a centrales digitales. En esta línea, los hitos son inherentes a lo que sus sistemas de informáticos puedan realizar (Cisneros, 2022).

En este caso, se ha tomado como parte y objeto de este estudio una Organización No Gubernamental - ONG las cuales son consideradas instrumentos que trabajan en pro al fortalecimiento y desarrollo sostenido de una comunidad, se caracterizan por ser de tipo privadas y sin ánimo de lucro que surgen a raíz de iniciativas civiles y populares. Estas iniciativas suelen estar relacionadas con iniciativas sociales, culturales, de desarrollo u otras que tienen como objetivo provocar transformaciones significativas en áreas específicas, comunidades, regiones o naciones (Haliux, 2023).

La seleccionada para llevar a cabo este proyecto ha migrado sus servicios a las plataformas digitales, por lo que ahora cuenta con más de 40 servicios de cloud computing en los que se incluyen jurídicos, financieros, planificación y administrativos, siendo necesario la implementación de políticas de uso de servicios mediante el modelo cloud computing o seguridad en la nube basadas en controles de seguridad, privacidad y portabilidad para las estructuras sensibles (Sisti, 2019).

Con base en estos criterios, no cabe duda de que la gestión eficiente de las tecnologías de la información es la base para alcanzar las metas propuestas no sólo para las operaciones, sino también para las organizaciones. Porque la tecnología de la información requiere actualizaciones e innovaciones continuas en infraestructura, comunicaciones, software, aplicaciones y más. Importantes inversiones financieras también se reflejan en la gestión y mantenimiento de estos servicios (Goyes, 2020).

En este sentido, los modelos de cloud computing representan un medio alternativo para implementar servicios técnicos. Cloud conocido o denominado generalmente como “La Nube”, incluyen áreas de acopio, proceso de información y archivos ubicadas fuera de las oficinas de un consumidor a través de una conexión a Internet y pueden albergar casi cualquier host. Compatible con todos los servicios y aumenta la seguridad de la base de datos. En el presente proyecto se plantea detallar políticas de uso de servicios mediante el modelo cloud computing o seguridad en la nube basadas en controles de seguridad, privacidad y portabilidad para las

estructuras sensibles como la base de datos de una ONG para el establecimiento de sistemas de seguridad informática.

1.1.2 Antecedentes

En cuanto a los antecedentes investigativos se ha llevado a cabo una revisión bibliográfica donde delimitaron dos estudios principales (uno de producción nacional y uno de literatura internacional) además de las fuentes complementarias, que forman los referentes teóricos considerados para este proyecto, tales como el proceso metodológico, los métodos y técnicas aplicadas para la consecución de resultados, además de las políticas de seguridad argumentadas en los enfoques teóricos del modelo cloud computing y la comparativa respecto a los resultados obtenidos

- **México**

Universidad: INFOTEC Centro De Investigación E Innovación En Tecnologías De La Información Y Comunicación.

Autor: Rodrigo Méndez

Año: 2020

Tema: PROPUESTA DE UN MODELO DE POLÍTICA PARA PROTECCIÓN DE DATOS PERSONALES PARA PROVEEDORES DE SERVICIOS DE CÓMPUTO EN LA NUBE

Descripción: El investigador propuso un modelo de política interna para una organización privada, sostenida en un estudio cuantitativo, que tuvo el objetivo de proporcionar soluciones a los proveedores de servicios de *cloud computing* que requieran llevar a cabo el correcto tratamiento de la información que reciben por parte de sus clientes, pero, sobre todo, de aquellos datos personales que almacenen a fin de cumplir con aquellas medidas requeridas por la normativa de privacidad y protección de datos personales aplicable en México. Este modelo se basó en principios rectores de la normativa en materia de protección de datos personales, mismos que han tenido la característica de ser atemporales y mundialmente reconocidos (Méndez R. , 2020).

- **Ecuador**

Universidad: Universidad Andina Simón Bolívar

Autor: José Luis Goyes Lara

Año: 2020

Tema: Estudio de impacto del modelo *cloud computing* en la gestión de servicios de información gerencial en la banca privada. Caso: Banco Internacional

Descripción: En el estudio el autor realizó una comparación entre el modelo *Cloud Computing* vs *On premise* para la gestión de Servicios de Información Gerencial, tomando

como caso de estudio al Banco Internacional del Ecuador, esto lo realizó a través de un análisis que se sostuvo en la información manejada por el sector financiero contar con un referente para la adopción de este paradigma tecnológico, considerando las siguientes perspectivas: financiera, tecnológica, normativa, de seguridad y de adopción del modelo. Todas éstas consideradas necesarias para la implementación de servicios en la nube, que garanticen la eficiencia, confidencialidad, disponibilidad e integridad de los datos, factores importantes para contar con la confianza de las áreas de negocio y, por tanto, del cliente. Llegó a la conclusión del nivel de disponibilidad del servicio en el SIG de Banco Internacional es de 99,76%. Se concluye que el nivel de disponibilidad en la nube está por encima del 99,9% que es considerado aceptable para los estándares de control y calidad de los servicios de TI. Por lo tanto**,** el modelo Cloud Computing en la gestión de Servicios de Información Gerencial, es más eficiente en costos y permite además el despliegue de servicios de forma más rápida que el modelo On Premise (Goyes, 2020).

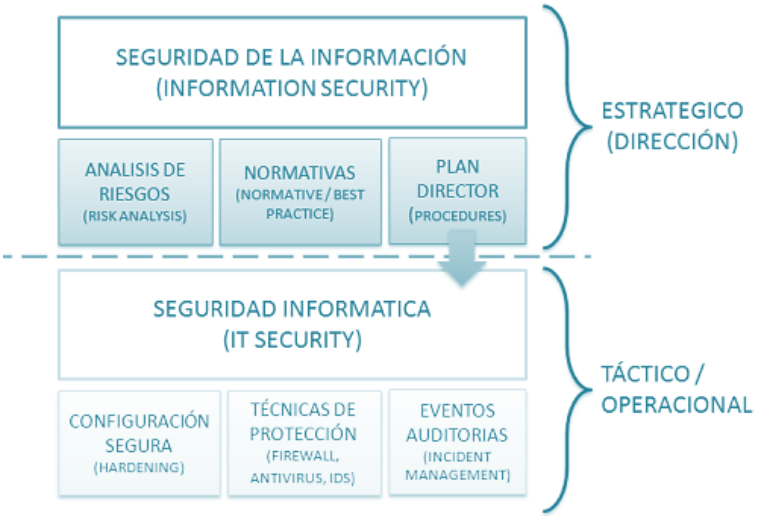
1.1.3 Definiciones fundamentales

Sistema de seguridad informática

El Sistema de Seguridad Informática (SGSI) se refiere a un conjunto de líneas y medidas organizativas compuestas por métodos y medios técnicos que se interconectan y conectan a canales de comunicación para garantizar el mantenimiento de un estado seguro de la instalación. El SGSI también ayuda a detectar y eliminar la lista más completa o compleja de amenazas a la propiedad y la información, utilizando métodos comunes de recopilación y procesamiento de información (Ver Figura 1) (Haliux, 2023).

Figura 1

Esquematización de los componentes del sistema de seguridad de la información



Nota: Esquematización del funcionamiento de la seguridad informática vs el de la seguridad de la información. Obtenido de (Sisti, 2019)

Por su parte, Sisti (2019) establece que un SGSI conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales.

Políticas de uso de servicios

Las políticas de uso de servicios han sido conceptualizadas como un conjunto de pautas de comportamiento que se aplican a nivel interno de una organización a fin de establecer normativas para la prestación de un determinado servicio. Estas pautas atienden la interacción de los equipos tecnológicos con un usurario a fin de resolver problemas y de delimitar orientaciones y para guiar el correcto manejo de información en las bases de datos a fin de protegerla de cualquier riesgo o amenaza (Cisneros, 2022).

Modelo Cloud computing o seguridad en la nube

El modelo de computación en la nube, también conocido como seguridad en la nube, se enfoca en la integración de políticas, procesos y tecnologías para proteger los datos, garantizar el cumplimiento de las regulaciones y proporcionar control sobre la privacidad, el acceso y la autenticación de usuarios y dispositivos (Goyes, 2020). Haliux (2023) afirma que la mayoría de los proveedores de servicios en la nube utilizan un modelo de responsabilidad compartida, lo que significa que garantizar la seguridad de la computación en la nube es una responsabilidad tanto del proveedor de servicios en la nube como de la empresa cliente. (Ver Tabla 1) (p42).

Tabla 1

Funcionamiento del Cloud Computing

Modelo de servicios de cloud computing	Responsabilidad de la organización	Responsabilidad de los proveedores de servicios
Infraestructura como servicio (IaaS)	Debe proteger los datos, aplicaciones, tus controles de redes virtuales, el sistema operativo y el acceso de los usuarios.	El proveedor de servicios en la nube protege las operaciones de computación, el almacenamiento y la red física, incluidos todos los parches y las configuraciones.
Plataforma como servicio (PaaS)	Proteger los datos, el acceso de los usuarios y las aplicaciones.	El proveedor de servicios en la nube protege las operaciones de computación, el almacenamiento, la red física, los controles de redes virtuales y el sistema operativo.
Software como servicio (SaaS)	ES responsable de proteger tus datos y el acceso de los usuarios.	El proveedor de servicios en la nube protege las operaciones de computación, el almacenamiento, la red física, los controles de redes virtuales, el sistema operativo, las aplicaciones y el middleware.

Nota: Matriz de funcionamiento de los modelos de servicios de cloud computing de acuerdo con la responsabilidad de la organización y de los proveedores de servicio. Tomado de (Cloud, 2022)

1.2. Proceso investigativo metodológico

El proceso metodológico de este proyecto está enmarcado en un diseño y enfoque cuantitativo siendo el método más adecuado para la gestión estratégica delimitada en este estudio para la ejecución de una encuesta que como técnica de recopilación de datos cuantificables, permite valorar datos exactos que dieron respuesta al objetivo específico de diagnosticar la situación actual de la ONG (organización sujeto de estudio) sobre el tratamiento de seguridad referente a las estructuras sensibles como su base de datos relacionado a sus proveedores y cartera de clientes para el mejoramiento de la eficiencia de los procedimientos de resguardo y establecimiento de políticas de seguridad interna de la organización.

Se considera el método cuantitativo ya que la naturaleza de la investigación admite un análisis estadístico de los datos para obtener conclusiones exactas sobre la situación actual de la organización y como está se encuentra referente a la seguridad de su base de datos. Los indicadores medidos en las encuestas respondieron a políticas de seguridad, datos y estructuras sensibles, cloud computing. De acuerdo con Hernández (2016) este diseño y método cuantitativo busca explorar la complejidad de factores que rodean a un fenómeno y la variedad de perspectivas y significados que tiene para los implicados. Ya que responde a una valoración concreta de la hipótesis de estudio.

La investigación adicionalmente se enmarcó en un tipo de investigación de índole descriptivo enfocándose en el análisis de las características del fenómeno de estudio con el propósito de clasificar, dividir y resumir cual es la situación actual de la empresa y como la propuesta de este proyecto podría intervenir de manera efectiva para contribuir con el objeto de estudio dando solución al problema planteado. Se escogió la investigación descriptiva porque versa en su línea el análisis del antecedente a los diseños de investigación cuantitativa, esto se traduce como que ambos son compatibles para la determinación de resultados exactos y científicos.

En la dirección de tecnología hay un total de ocho técnicos, la muestra se constituyó mediante la selección del Director de TIC, el Supervisor de Bases de Datos (BDD) y el Analista de Bases de Datos (BDD) quienes accedieron a participar de manera voluntaria en este proyecto bajo consentimiento con el fin de diagnosticar la situación actual de esta y así extraer valoraciones y premisas que permitieron facilitar la propuesta de estudio para definir políticas de uso de servicios mediante el modelo *cloud computing* o seguridad en la nube basadas en controles de seguridad, privacidad y portabilidad para las estructuras sensibles como la base de datos de una ONG para el establecimiento de sistemas de seguridad informática.

En lo que respecta al análisis de los datos cuantitativos se empleó bajo el programa estadístico Open EPI que permitió además de la carga de datos automáticamente establecer las relaciones, tendencias y patrones en los datos registrados, arrojando resultados concretos, esquematizados para su interpretación.

1.3. Análisis de resultados

En la dirección de tecnología hay un total de ocho técnicos, la muestra se constituyó mediante la selección del Director de TIC, el Supervisor de Bases de Datos (BDD) y el Analista de Bases de Datos (BDD); en referencia del objetivo de diagnosticar la situación actual de la ONG sobre el tratamiento de seguridad referente a las estructuras sensibles como su base de datos relacionado a sus proveedores y cartera de clientes para el mejoramiento de la eficiencia de los procedimientos de resguardo y establecimiento de políticas de seguridad interna de esta.

La Tabla 2 se muestran los datos recolectados de la pregunta 1. ¿Está informado sobre los Datos Confidenciales que se manejan en la organización?, la Figura 2 se muestra un gráfico circular con los datos de la tabla.

1. ¿Está informado sobre los Datos Confidenciales que se manejan en la organización?

Tabla 2

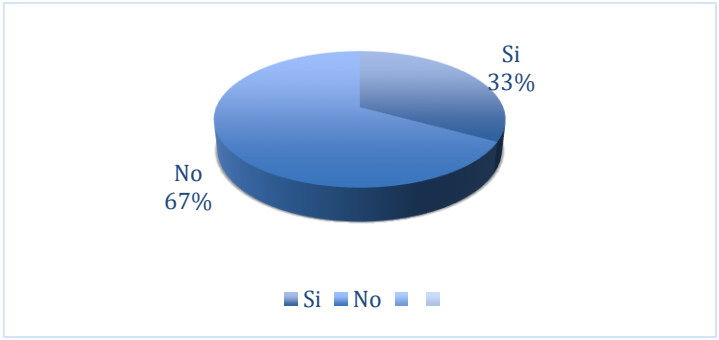
Conocimiento de los Datos Sensible

Variable	Frecuencia	Porcentaje
Si	1	33,00%
No	2	67,00%
Total	**3**	**100%**

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

Figura 2

Conocimiento de los Datos Sensible



Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

La Tabla 3 se muestran los datos obtenidos de la pregunta 2. ¿Se han establecido políticas de seguridad para el manejo de información confidencial?, la Figura 3 se muestra un gráfico circular con los datos de la tabla.

2. **¿Se han establecido políticas de seguridad para el manejo de información confidencial**?

Tabla 3

Existencias de políticas de seguridad

Variable	Frecuencia	Porcentaje
Si	0	00,00%
No	3	100,00%
Total	**3**	**100%**

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

Figura 3

Existencias de políticas de seguridad

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

La Tabla 4 se muestran los datos recolectados de la pregunta 3. ¿Utilizan herramientas seguras para cargar, transmitir y generar información que involucre datos confidenciales en la organización?, la Figura 4 se muestra un gráfico circular con los datos de la tabla.

3. **¿Utilizan herramientas seguras para cargar, transmitir y generar información que involucre datos confidenciales en la organización?**

Tabla 4

Uso de herramientas seguras

Variable	Frecuencia	Porcentaje
Si	0	00,00%
No	3	100,00%
Total	**3**	**100%**

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

Figura 4

Uso de herramientas seguras

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

La Tabla 5 se muestran los datos recolectados de la pregunta 4. ¿Conoce modelo Cloud Computing (Computación en la Nube) ?, la Figura 5 se muestra un gráfico circular con los datos de la tabla.

4. ¿Conoce modelo Cloud Computing (Computación en la Nube)?

Tabla 5

Conocimiento del modelo Cloud Computing

Variable	Frecuencia	Porcentaje
Si	1	33,00%
No	0	00,00%
He oído hablar de el	2	67,00%
Total	**3**	**100%**

Nota: Datos procesados posterior a la obtención de información en el uso de la encuesta a los participantes de estudio de la ONG. 2024

Figura 5

Conocimiento del modelo Cloud Computing

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

La Tabla 6 se muestran los datos recolectados de la pregunta 5. ¿En qué medida utiliza su organización servicios de computación en la nube actualmente?, la Figura 6 se muestra un gráfico circular con los datos de la tabla.

5. ¿En qué medida utiliza su organización servicios de computación en la nube actualmente?

Tabla 6

Uso de los servicios de Cloud Computing

Variable	Frecuencia	Porcentaje
No utilizamos servicios de computación en la nube	3	100,00%
Utilizamos servicios de cloud para almacenamiento de información	0	00,00%
Utilizamos servicios de computación en la nube para alojar aplicaciones	0	00,00%
Utilizamos una variedad	0	00,00%

de servicios de computación en la nube para múltiples propósitos		
Total	**3**	**100%**

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

Figura 6

Conocimiento del modelo Cloud Computing

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

La Tabla 7 se muestran los datos recolectados de la pregunta 6. ¿El personal de la organización reconoce cuando está siendo atacado por una técnica de phishing?, la Figura 7 se muestra un gráfico circular con los datos de la tabla.

6. ¿El personal de la organización reconoce cuando está siendo atacado por una técnica de phishing?

Tabla 7

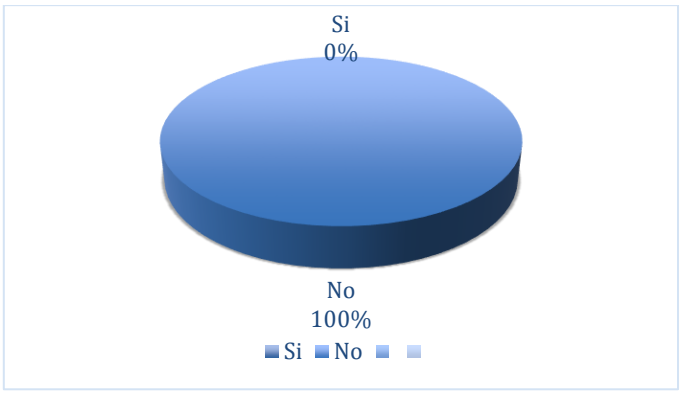
Reconocimiento de ataque (phishing)

Variable	Frecuencia	Porcentaje
Si	0	00,00%
No	3	100,00%
Total	**3**	**100%**

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

Figura 7

Reconocimiento de ataque (phishing)



Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

La Tabla 8 se muestran los datos recolectados de la pregunta 7. ¿Emplea técnicas de encriptación para enviar información confidencial a través de correo electrónico?, la Figura 8 se muestra un gráfico circular con los datos de la tabla.

7. ¿Emplea técnicas de encriptación para enviar información confidencial a través de correo electrónico?

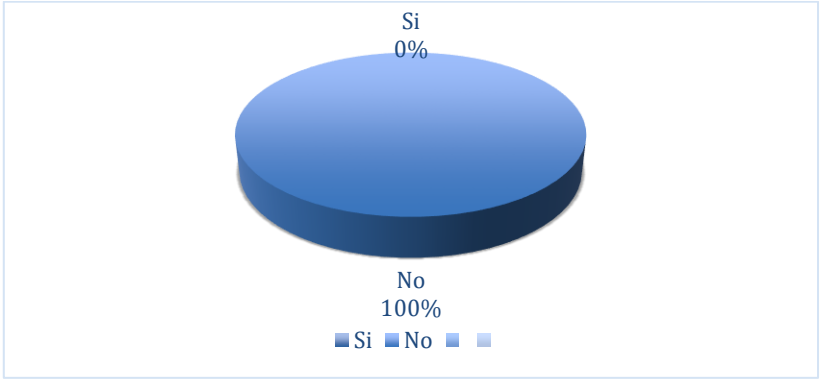
Tabla 8

Métodos de encriptación

Variable	Frecuencia	Porcentaje
Si	0	00,00%
No	3	100,00%
Total	**3**	**100%**

Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

Figura 8 *Métodos de encriptación*



Nota: Información procesada posterior a la recolección de datos en el uso de la encuesta a los participantes de estudio de la ONG. 2024

La Tabla 9 se muestran los datos recolectados de la pregunta 8. ¿Cuál sería el impacto primordial que podría generar la filtración de información confidencial?, la Figura 9 se muestra un gráfico circular con los datos de la tabla.

8. ¿Cuál sería el impacto primordial que podría generar la filtración de información confidencial?

Tabla 9

Impacto por fuga de datos

Variable	Frecuencia	Porcentaje
Legal	1	33,00%
Económico	2	67,00%
Operativo	0	00,00%
Imagen y reputación	0	00,00%
Continuidad del negocio	0	00,00%
Total	**3**	**100%**

Nota: Información procesada posterior a la recolección de datos en la aplicación de la encuesta a los sujetos de estudio de la ONG. 2024

Figura 9

Impacto por fuga de datos

Nota: Información procesada posterior a la recolección de datos en la aplicación de la encuesta a los sujetos de estudio de la ONG. 2024

CAPÍTULO II: PROPUESTA

En este capítulo se detalla el tema, la investigación realizada los instrumentos con sus respectivas validaciones sobre las políticas de seguridad para cubrir y atenuar las brechas de seguridad que pueden presentarse en el uso de bases de datos en la nube.

2.1. Fundamentos teóricos aplicados

Código Orgánico Integral Penal (COIP): El COIP contiene disposiciones relacionadas con la protección de datos personales y la responsabilidad penal por su tratamiento indebido. Este marco legal puede proporcionar orientación sobre las medidas de seguridad necesarias para proteger los datos personales en la nube y las consecuencias de no cumplir con estas medidas (COPI, 2014).

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (LCE): La LCE regula aspectos relacionados con la seguridad de la información en transacciones electrónicas. Puede proporcionar orientación sobre las medidas de seguridad necesarias para proteger la información en la nube y garantizar la autenticidad e integridad de los mensajes de datos (LCE, 2002)

Ley de Telecomunicaciones y regulaciones asociadas: Establecen requisitos específicos de seguridad para los proveedores de servicios de telecomunicaciones, que pueden ser relevantes para la seguridad de las bases de datos en la nube (Ley de Telecomunicaciones y regulaciones asociadas, 2015).

Ley de Protección al Consumidor: Contiene disposiciones relacionadas con la protección de la información personal de los consumidores, que pueden ser aplicables al tratamiento de datos en la nube (Ley de Protección al Consumidor, 2012).

La Ley Orgánica de Protección de Datos Personales (LOPDP) del Ecuador establece los principios fundamentales que rigen el tratamiento de datos personales y la protección de la privacidad de los individuos. Estos principios pueden ser aplicados en la propuesta de políticas de seguridad para bases de datos en la nube basadas en la familia ISO 27000 de la siguiente manera (Ley Orgánica de Protección de Datos Personales (LOPDP) , 2021).

Seguridad de la Información: Es el proceso de proteger la información contra el acceso no autorizado, el uso indebido, la divulgación, la interrupción, la destrucción o la modificación. Este concepto está respaldado por la teoría de la seguridad de la información, que incluye principios como la confidencialidad, la integridad y la disponibilidad (CIA) (Cisneros, 2022).

ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información (SGSI): Esta norma establece los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. Se basa en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA) para garantizar un enfoque sistemático de la gestión de la seguridad de la información (ISOTOOLS, 2020).

La norma ISO/IEC 27002, también conocida como Código de Práctica para la Gestión de la Seguridad de la Información, proporciona pautas detalladas y recomendaciones prácticas para establecer controles de seguridad de la información. Su enfoque se basa en la evaluación de riesgos, lo que permite la identificación y el tratamiento adecuado de las amenazas a la seguridad de la información (ISOTOOLS, 2022).

Norma ISO/IEC 27017: Controles de Seguridad para Servicios Cloud, La norma ISO/IEC 27017 complementa a la ISO 27001, proporcionando controles de seguridad para proveedores y clientes de servicios en la nube. A diferencia de otras normas, clarifica las responsabilidades de ambas partes para garantizar la seguridad de los servicios en la nube. Con 37 controles basados en la norma ISO/IEC 27002, y siete nuevos controles específicos para la nube, esta norma brinda una guía para garantizar la seguridad de los datos en la nube (BSIGROUP, 2021).

Gestión de Riesgos: Es el proceso de identificar, evaluar y priorizar los riesgos de seguridad de la información. Se basa en la teoría de la gestión de riesgos, que implica la identificación de activos, amenazas, vulnerabilidades y la selección de medidas de control adecuadas (Cisneros, 2022).

Cifrado: Es el proceso de convertir información legible en un formato ilegible para protegerla contra accesos no autorizados. Se basa en algoritmos matemáticos y teoría de la criptografía para garantizar la confidencialidad de la información. (Sisti, 2019)

Control de Acceso: Es el proceso de garantizar que solo las personas autorizadas tengan acceso a la información y los recursos. Se basa en la teoría de control de acceso, que incluye la autenticación, la autorización y la auditoría de acceso (Méndez R. , 2020).

Auditoría de Seguridad: Es el proceso de evaluar la efectividad de las políticas, controles y procedimientos de seguridad de la información. Se basa en la teoría de la auditoría, que implica la revisión sistemática de registros y actividades para garantizar el cumplimiento de las políticas de seguridad (Goyes, 2020).

2.2. Descripción de la propuesta

La presente propuesta está enmarcada en políticas de uso de servicios basadas en el Modelo Cloud Computing generalmente sigue una estructura organizada que incluye los siguientes elementos:

Introducción:

El propósito de la propuesta de políticas de uso de servicios basadas en el Modelo Cloud Computing es establecer un marco integral y coherente para gestionar de manera efectiva la seguridad, la privacidad y la portabilidad de los datos en entornos de nube. Esta propuesta tiene como objetivo principal garantizar la protección de la información, promover el cumplimiento normativo y facilitar la migración de datos entre diferentes plataformas de nube, asegurando al mismo tiempo la disponibilidad y la integridad de los datos.

Al establecer políticas claras y detalladas, la propuesta busca proporcionar orientación y directrices para todos los usuarios y responsables involucrados en la gestión y utilización de servicios en la nube. Esto incluye desde altos directivos y responsables de la toma de decisiones hasta los usuarios finales que interactúan con los servicios en la nube en su día a día.

Además, la propuesta pretende fomentar una cultura organizacional orientada a la seguridad y la protección de datos, promoviendo la concienciación y la formación de los funcionarios en prácticas seguras de uso de servicios en la nube. De esta manera, se busca reducir los riesgos de brechas de seguridad, pérdida de datos o incumplimiento normativo, y fortalecer la confianza de los usuarios en la seguridad y la fiabilidad de los servicios en la nube utilizados por la organización.

Objetivo:

El objetivo de la propuesta de políticas de uso de servicios basadas en el Modelo Cloud Computing es asegurar la protección y gestión eficiente de los datos en entornos de nube, garantizando la seguridad, la privacidad y la portabilidad de la información.

Alcance:

El alcance de la propuesta incluye la definición e implementación de políticas de uso de servicios basadas en el Modelo Cloud Computing en todas las áreas relevantes de la organización que interactúan con servicios en la nube. Esto abarca desde la alta dirección y los responsables de la toma de decisiones hasta los usuarios finales que utilizan activamente los servicios en la nube en su trabajo diario.

Las políticas propuestas cubren aspectos clave como el acceso y la autenticación segura, la protección de datos sensibles, el monitoreo y la detección de amenazas, el cumplimiento normativo y de privacidad, la portabilidad de datos, el respaldo y la recuperación de datos, y la educación y concienciación del usuario.

El alcance también considera la implementación de controles de seguridad, privacidad y portabilidad asociados a estas políticas en todos los servicios en la nube utilizados por la organización, así como la asignación de recursos y responsabilidades necesarios para llevar a cabo la implementación y el cumplimiento de estas políticas.

Además, la propuesta incluye mecanismos de evaluación periódica y mejora continua para verificar el cumplimiento de las políticas y ajustarlas según sea necesario, asegurando así que la organización se mantenga alineada con las mejores prácticas y estándares de seguridad en la nube.

Marco Normativo:

El marco normativo de la propuesta de políticas de uso de servicios basadas en el Modelo Cloud Computing incluye las siguientes regulaciones, estándares y mejores prácticas relevantes:

Reglamento General de Protección de Datos (GDPR): Esta normativa europea establece principios para el tratamiento de datos personales y garantiza los derechos de los individuos en cuanto a la privacidad y seguridad de sus datos.

ISO/IEC 27001: Esta norma internacional establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) y proporciona pautas para la implementación de controles de seguridad de la información.

Principios Rectores:

Los principios rectores de la propuesta de políticas de uso de servicios basadas en el Modelo Cloud Computing son fundamentales para orientar el diseño, la implementación y la gestión efectiva de estas políticas. Estos principios guían la actuación de la organización y establecen la base para la toma de decisiones relacionadas con la seguridad, la privacidad y la portabilidad de los datos en entornos de nube. Algunos de estos principios rectores podrían incluir:

Seguridad Integral: Priorizar la seguridad en todas las etapas del ciclo de vida de los datos y servicios en la nube, desde la recopilación hasta el almacenamiento y la transferencia.

Cumplimiento Normativo: Asegurar el cumplimiento con regulaciones y estándares aplicables relacionados con la privacidad, la protección de datos y la seguridad de la información.

Transparencia y Responsabilidad: Promover la transparencia en el tratamiento de datos y la rendición de cuentas en caso de incidentes de seguridad o violaciones de privacidad.

Privacidad por Diseño: Integrar consideraciones de privacidad desde el diseño y desarrollo de los servicios en la nube, minimizando la recopilación y el uso de datos personales.

Portabilidad de Datos: Facilitar la portabilidad de datos entre diferentes plataformas de nube, permitiendo a los usuarios acceder y transferir sus datos de manera segura y eficiente.

Educación y Concienciación: Promover la educación y la concienciación del personal sobre prácticas seguras de uso de servicios en la nube y el cumplimiento de las políticas establecidas.

Evaluación Continua: Realizar evaluaciones periódicas de la efectividad de las políticas implementadas y ajustarlas según sea necesario para mejorar la seguridad y la protección de datos.

Colaboración y Cooperación: Fomentar la colaboración y la cooperación entre diferentes departamentos y partes interesadas para garantizar una implementación coherente y efectiva de las políticas en toda la organización.

Estos principios rectores proporcionan una guía sólida para el desarrollo de políticas de uso de servicios en la nube que promuevan la seguridad, la privacidad y la portabilidad de los datos, al tiempo que garantizan el cumplimiento normativo y la confianza de los usuarios en el uso de servicios en la nube.

Proceso para la implementación:

Planificación:

- Definición de un equipo de implementación responsable de liderar el proceso.
- Establecimiento de objetivos claros y medibles para la implementación de las políticas.
- Identificación de recursos necesarios, incluyendo personal, tecnología y presupuesto.
- Desarrollo de un cronograma detallado con hitos y plazos específicos.

Análisis y Evaluación:

- Evaluación del entorno actual de servicios en la nube y de las políticas existentes, identificando brechas y áreas de mejora.
- Análisis de riesgos para identificar posibles amenazas y vulnerabilidades que puedan afectar la seguridad, privacidad y portabilidad de los datos en la nube.

- Revisión del marco normativo y de los principios rectores para asegurar el cumplimiento normativo y la alineación con los objetivos de la organización.

Desarrollo de Políticas:

- Diseño y desarrollo de políticas de uso de servicios en la nube basadas en los requisitos identificados durante el análisis y evaluación.
- Definición de controles de seguridad, privacidad y portabilidad asociados a cada política.
- Revisión y aprobación de las políticas por parte de la alta dirección y los responsables de cumplimiento normativo.

Ejecución:

- Comunicación de las políticas a todos los empleados y partes interesadas involucradas en el uso de servicios en la nube.
- Capacitación del personal sobre las políticas y procedimientos establecidos.
- Configuración e implementación de controles de seguridad y privacidad en los sistemas y servicios en la nube según lo especificado en las políticas.

Monitoreo y Control:

- Establecimiento de un sistema de monitoreo continuo para supervisar el cumplimiento de las políticas y detectar posibles violaciones.
- Implementación de controles automatizados para garantizar el cumplimiento de las políticas en tiempo real.
- Realización de auditorías periódicas para evaluar la eficacia de los controles y políticas implementadas.

Evaluación y Mejora Continua:

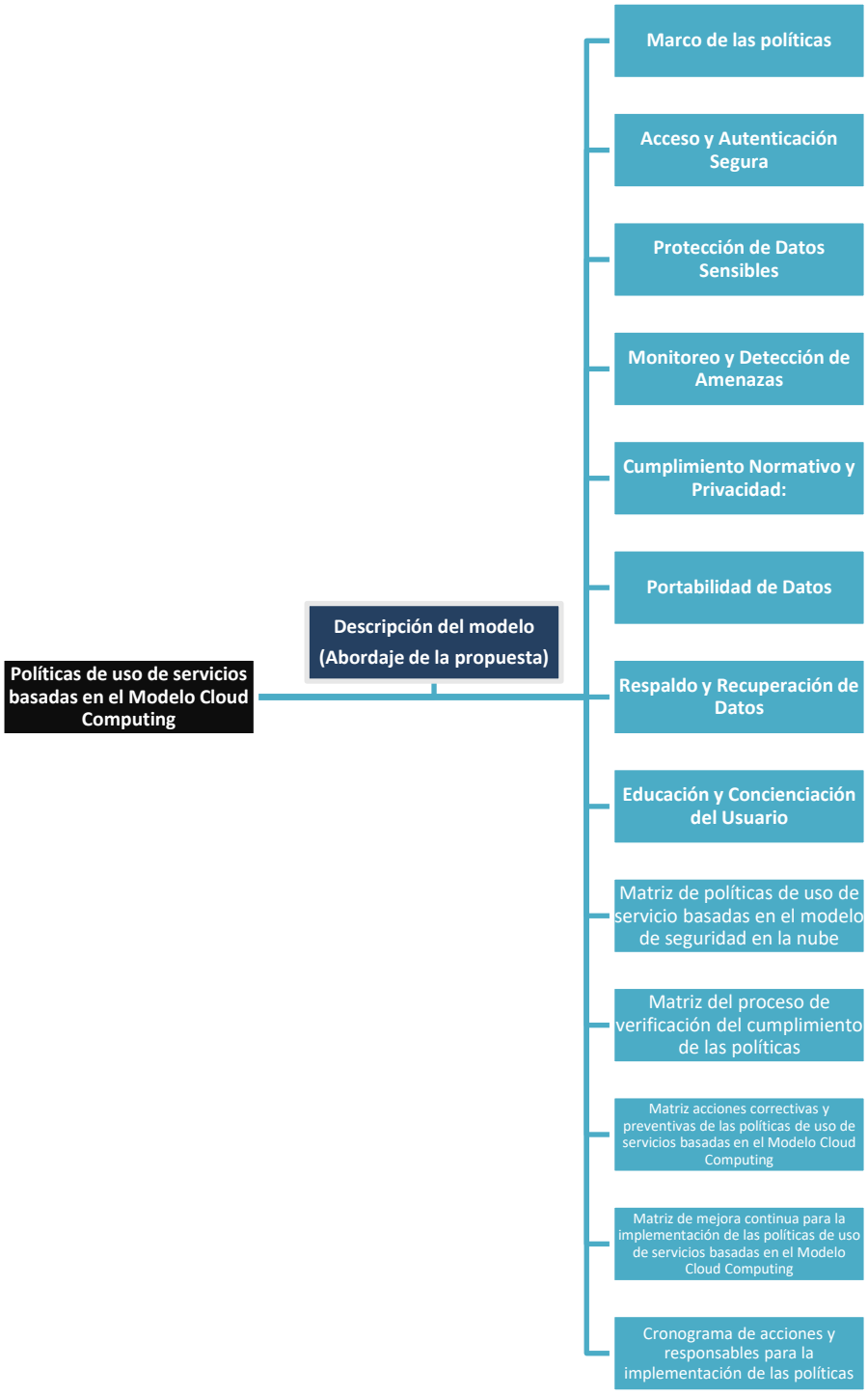
- Evaluación periódica del desempeño de las políticas y controles implementados.
- Identificación de áreas de mejora y ajuste de las políticas en función de los resultados obtenidos.
- Retroalimentación y revisión regular del proceso de implementación para garantizar la efectividad a largo plazo de las políticas de uso de servicios en la nube.

La estructura de una propuesta de políticas de uso de servicios basadas en el Modelo Cloud Computing proporciona una guía clara y organizada para el diseño e implementación de políticas efectivas que promuevan la seguridad, la privacidad y la portabilidad de los datos en entornos de nube (Ver Tabla 10).

1. Estructura general

Tabla 10

Indicador gráfico de la propuesta



Elaboración propia

2. Explicación del aporte

Propuesta de Políticas de Uso de Servicios basadas en el Modelo Cloud Computing:

1. Acceso y Autenticación Segura:

- Todos los usuarios deben autenticarse de manera segura antes de acceder a los servicios en la nube.

- Se deben implementar medidas de autenticación de múltiples factores para garantizar una capa adicional de seguridad.

- Se deben establecer políticas claras de gestión de contraseñas, incluyendo la periodicidad de cambio y la complejidad de estas.

    - Longitud adecuada: Cuanto más larga sea la clave, más difícil será de adivinar. Se recomienda utilizar claves de al menos 12 caracteres.

    - Combinación de caracteres: La clave debe contener una combinación de letras (mayúsculas y minúsculas), números y caracteres especiales.

    - Evitar información personal: No utilices información personal como nombres, fechas de nacimiento o números de identificación en tus claves.

    - Evitar patrones comunes: Evita secuencias o patrones simples como "123456" o "abcdef".

    - Utilizar herramientas seguras: Si es posible, utiliza generadores de claves seguras para crear claves aleatorias y únicas.

    - Cambiar regularmente: Es recomendable cambiar tus claves regularmente para mejorar la seguridad.

    - Almacenamiento seguro: Guarda tus claves en un lugar seguro y no las compartas con nadie.

    - No reutilizar claves: No uses la misma clave para diferentes cuentas o servicios ya que, si una clave se ve comprometida, todas las demás también estarán en riesgo.

2. Protección de Datos Sensibles:

- Se deben identificar y clasificar los datos sensibles almacenados en la nube.

- Se deben aplicar controles de cifrado tanto en reposo como en tránsito para proteger la confidencialidad de los datos.

- Se deben establecer políticas de acceso basadas en roles para limitar el acceso a los datos sensibles únicamente a usuarios autorizados.

3. Monitoreo y Detección de Amenazas:

- Se debe implementar un sistema de monitoreo continuo para detectar y responder a posibles amenazas o actividades sospechosas.

- Se deben establecer alertas y procedimientos de respuesta ante incidentes para mitigar cualquier brecha de seguridad de manera oportuna.

4. Cumplimiento Normativo y Privacidad:

- Se debe avalar el cumplimiento de las regulaciones de privacidad y protección de información, como el Reglamento General de Protección de Datos (GDPR) o la Ley de Privacidad del Consumidor de California (CCPA).

- Se deben establecer políticas y procedimientos para garantizar la privacidad de los datos del usuario y obtener el consentimiento adecuado para su procesamiento.

5. Portabilidad de Datos:

- Se debe garantizar la portabilidad de los datos del usuario, permitiendo su transferencia o exportación de manera segura y eficiente.

- Se deben establecer procedimientos claros para la migración de datos entre proveedores de servicios en la nube, asegurando la integridad y disponibilidad de estos durante el proceso.

6. Respaldo y Recuperación de Datos:

- Se deben establecer políticas de respaldo regulares para garantizar la disponibilidad y la integridad de la información en caso de caída del sistema o pérdida de información.

- Se deben realizar pruebas periódicas de los procedimientos de recuperación de datos para asegurar su eficacia en situaciones de emergencia.

7. Educación y Concienciación del Usuario:

- Se deben proporcionar capacitaciones periódicas sobre seguridad en la nube y buenas prácticas de uso a todos los usuarios.

- Se debe fomentar una cultura de seguridad entre los empleados, incentivando la denuncia de posibles incidentes de seguridad y promoviendo el uso responsable de los servicios en la nube.

Estas políticas de uso de servicios basadas en el modelo de seguridad en la nube están diseñadas para garantizar la protección de la información, la privacidad de los datos y la portabilidad de estos, mientras se cumplen con los estándares de seguridad y normativas aplicables:

- Matriz de políticas de uso de servicio basadas en el modelo de seguridad en la nube. (Ver Tabla 11)

- Matriz del proceso de verificación del cumplimiento de las políticas. (Ver Tabla 12)

- Matriz acciones correctivas y preventivas de las políticas de uso de servicios basadas en el Modelo Cloud Computing. (Ver Tabla 13)

- Matriz de mejora continua para la implementación de las políticas de uso de servicios basadas en el Modelo Cloud Computing. (Ver Tabla 14)

- Cronograma de acciones y responsables para la implementación de las políticas. (Ver Tabla 15)

Tabla 11

Matriz de políticas de uso de servicio basadas en el modelo de seguridad en la nube

alcance	Descripción	Controles de Seguridad	Controles de Privacidad	Controles de Portabilidad
Acceso y Autenticación Segura	Todos los usuarios deben autenticarse de manera segura antes de acceder a los servicios en la nube.	Autenticación de múltiples factores- Políticas de gestión de contraseñas	Control de acceso basado en roles- Registro de actividades de acceso	Interoperabilidad de datos- Estándares de transferencia de datos

Protección de Datos Sensibles	Identificación y clasificación de datos sensibles.	Cifrado de datos en reposo y en tránsito- Detección de intrusos	Consentimiento para el procesamiento de datos- Gestión de consentimiento del usuario	Mecanismos de exportación e importación de datos- Cumplimiento de estándares de seguridad y privacidad
Monitoreo y Detección de Amenazas	Implementación de un sistema de monitoreo continuo para detectar y responder a amenazas.	Sistema de detección de intrusiones- Análisis de registros de auditoría	Notificación de acceso no autorizado de datos- Respuesta a incidentes de seguridad	Integración con herramientas de gestión de eventos y seguridad- Procedimientos de respuesta a incidentes
Cumplimiento Normativo y Privacidad	Cumplimiento con regulaciones de confidencialidad y protección de información.	Auditorías de seguridad- Análisis de riesgos y evaluaciones de impacto	- Políticas de retención de datos- Derechos del titular de los datos	- Certificaciones de cumplimiento con estándares de privacidad- Cumplimiento con regulaciones de transferencia de datos internacionales
Portabilidad de Datos	Garantizar la portabilidad segura de los datos del usuario.	Mecanismos de migración de datos- Seguridad en la transferencia de datos	Consentimiento del usuario para la portabilidad de datos- Derecho a la portabilidad de datos	Interoperabilidad entre plataformas de nube- Garantía de integridad y disponibilidad durante la migración de datos
Respaldo y Recuperación de Datos	Establecimiento de políticas de respaldo y recuperación para garantizar la	Copias de seguridad regulares- Pruebas de	Políticas de retención de datos- Derecho al olvido del usuario	- Procedimientos de restauración de datos- Garantía de integridad y

	disponibilidad de datos.	recuperación de desastres		disponibilidad de los datos respaldados
Educación y Concienciación del Usuario	Proporcionar capacitaciones sobre seguridad en la nube y buenas prácticas de uso.	Programas de entrenamiento en seguridad- Campañas de sensibilización	Políticas de uso aceptable- Información transparente sobre la recopilación y uso de datos	Retroalimentación del usuario sobre las políticas y prácticas de seguridad- Evaluaciones periódicas de la conciencia en seguridad por parte de los usuarios

Fuente: Elaboración propia

La matriz proporciona una visión estructurada del proceso de verificación del cumplimiento, incluyendo las acciones a realizar en cada etapa y los responsables de llevar a cabo esas acciones. Esto facilita la gestión y supervisión del proceso de verificación del cumplimiento de las políticas de uso de servicios en la nube.

Tabla 12

Matriz del proceso de verificación del cumplimiento de las políticas

Etapa	Acciones	Responsables
Definición de Indicadores de Cumplimiento	Identificar métricas clave para evaluar el cumplimiento de las políticas.	Equipo de Seguridad de la Información
Establecimiento de Pautas y Procedimientos	Desarrollar procedimientos detallados para llevar a cabo la verificación del cumplimiento.	Equipo de Implementación
Recopilación de Datos	Recolectar datos relevantes para evaluar el cumplimiento de las políticas.	Equipo de TI, Equipo de Seguridad de la Información
Análisis de Datos	Analizar los datos recopilados para identificar posibles desviaciones o incumplimientos de las políticas.	Equipo de Seguridad de la Información

Evaluación del Cumplimiento	Evaluar el grado de cumplimiento de las políticas en función de los resultados del análisis de datos.	Equipo de Seguridad de la Información
Reporte de Resultados	Preparar informes detallados que resuman los resultados de la verificación del cumplimiento.	Equipo de Seguridad de la Información
Acciones Correctivas y Preventivas	Implementar medidas correctivas y preventivas para abordar desviaciones identificadas.	Equipo de Implementación, Equipo de Seguridad de la Información
Seguimiento y Mejora Continua	Realizar un seguimiento continuo del cumplimiento y ajustar procesos según sea necesario.	Equipo de Seguridad de la Información, Alta Dirección

Fuente: Elaboración propia

La tabla proporciona una visión clara de las acciones correctivas y preventivas que pueden tomarse para abordar posibles desviaciones o mejorar la seguridad y el cumplimiento en el uso de servicios en la nube. Estas acciones deben ser adaptadas según las necesidades y requisitos específicos de cada organización.

Tabla 13

Matriz acciones correctivas y preventivas de las políticas de uso de servicios basadas en el Modelo Cloud Computing

Descripción de la Acción	Objetivo	Responsables	Fecha de Implementación
Realizar una revisión exhaustiva de los controles de seguridad existentes en los servicios en la nube para identificar posibles brechas o deficiencias.	Identificar áreas de mejora en los controles de seguridad y fortalecer la postura de seguridad de los servicios en la nube.	Equipo de Seguridad de la Información, Equipo de TI	Dentro de los próximos 30 días
Actualizar las políticas y procedimientos de acceso a los servicios en la nube	Mejorar la gestión de accesos y reducir el riesgo de acceso no	Equipo de Seguridad de la	Dentro de los próximos 15 días

para garantizar una autenticación y autorización adecuadas.	autorizado a los datos en la nube.	Información, Equipo de TI	
Implementar un sistema de monitoreo continuo de la actividad en la nube para detectar y responder rápidamente a posibles amenazas o incidentes de seguridad.	Mejorar la detección temprana de amenazas y reducir el tiempo de respuesta ante incidentes de seguridad en la nube.	Equipo de Seguridad de la Información	Dentro de los próximos 45 días
Realizar sesiones de capacitación periódicas sobre seguridad en la nube para educar al personal sobre las mejores prácticas y políticas de seguridad.	Mejorar la conciencia y la capacitación del personal sobre seguridad en la nube para reducir el riesgo de errores humanos y violaciones de seguridad.	Equipo de Capacitación, Equipo de Seguridad de la Información	Programar sesiones mensuales a partir del próximo mes
Establecer un proceso formal de revisión y aprobación para la adopción de nuevos servicios en la nube, garantizando que cumplan con las políticas y estándares de seguridad establecidos.	Hay que asegurar que la incorporación de nuevos servicios en la nube se realice de manera segura y conforme a las políticas de la organización.	Equipo de Seguridad de la Información, Equipo de TI	Implementar antes de la próxima adquisición de servicios en la nube

Fuente: Elaboración propia

Tabla 14

Matriz de mejora continua para la implementación de las políticas de uso de servicios basadas en el Modelo Cloud Computing

Área de Mejora	Acción de Mejora	Responsables	Fecha de Implementación	Resultados Esperados	Seguimiento y Evaluación

Seguridad de la Información	Realizar una evaluación de riesgos anualmente para identificar nuevas amenazas y vulnerabilidades.	Equipo de Seguridad de la Información	Anualmente	Mejora en la identificación y gestión de riesgos de seguridad	Revisión de los resultados de la evaluación de riesgos
Procesos de Autorización	Revisar y actualizar los procedimientos de autorización de acceso trimestralmente para reflejar cambios en el personal y en los requisitos de acceso.	Equipo de TI, Equipo de Seguridad de la Información	Trimestralmente	Reducción de riesgos de acceso no autorizado	Auditoría de los procedimientos de autorización
Capacitación del Personal	Realizar sesiones de capacitación semestrales sobre seguridad en la nube para todo el personal.	Equipo de Capacitación, Equipo de Seguridad de la Información	Semestralmente	Mejora en la conciencia y el conocimiento sobre seguridad en la nube	Evaluación de la participación y retroalimentación del personal
Evaluación del Cumplimiento	Realizar auditorías internas semestrales para evaluar el cumplimiento de las políticas de uso de servicios en la nube.	Equipo de Auditoría Interna, Equipo de Seguridad de la Información	Semestralmente	Identificación de posibles desviaciones o áreas de mejora	Revisión de los informes de auditoría
Actualización de Políticas	Revisar y actualizar las políticas de uso de servicios en la nube anualmente para reflejar cambios en las tecnologías y regulaciones.	Equipo de Seguridad de la Información	Anualmente	Asegurar que las políticas sean actuales y relevantes	Revisión de las políticas actualizadas

Fuente: Elaboración propia

En esta matriz, se identifican áreas específicas de mejora continua, relacionadas con la implementación de las políticas de uso de servicios en la nube, junto con acciones concretas

para abordar esas áreas de mejora, los responsables de llevar a cabo esas acciones, las fechas de implementación, los resultados esperados y el seguimiento y evaluación asociados. Este enfoque sistemático de mejora continua ayuda a garantizar que las políticas se mantengan actualizadas y efectivas en un entorno tecnológico en constante evolución.

Tabla 15

Cronograma de acciones y responsables para la implementación de las políticas

Semana	Acciones	Responsables
Semana 1	Planificación del proceso de implementación	Equipo de Implementación
Semana 2	Análisis y evaluación del entorno actual	Equipo de Implementación
Semana 3	Desarrollo de políticas de uso de servicios	Equipo de Implementación
Semana 4	Revisión y aprobación de las políticas	Alta Dirección, Responsables de Cumplimiento Normativo
Semana 5	Comunicación de las políticas a la organización	Equipo de Implementación
Semana 6	Capacitación del personal sobre las políticas	Equipo de Implementación
Semana 7	Configuración e implementación de controles de seguridad	Equipo de TI
Semana 8	Monitoreo y control del cumplimiento de las políticas	Equipo de Seguridad de la Información
Semana 9	Evaluación de la efectividad de las políticas	Equipo de Implementación
Semana 10	Ajustes y mejoras en las políticas según los resultados	Equipo de Implementación

Fuente: Elaboración propia

En este cronograma, cada semana representa un período de tiempo específico durante el cual se llevan a cabo las acciones correspondientes. Esto facilita la planificación y el seguimiento del proceso de implementación de las políticas de uso de servicios en la nube.

Estrategias y/o técnicas

Para desarrollar las políticas de uso de servicios basadas en el Modelo Cloud Computing, se emplearon varias estrategias, métodos y enfoques que permiten un proceso estructurado y efectivo:

- Análisis de Riesgos y Evaluación de Impacto: Esta metodología se centra en identificar y evaluar los riesgos asociados con el uso de servicios en la nube, así como en determinar el impacto potencial de estos riesgos en la organización. Se utilizan técnicas como análisis FMEA (Failure Mode and Effects Analysis) o valoraciones de impacto en la confidencialidad para detectar las amenazas y vulnerabilidades más relevantes.
- Marco de Control de Seguridad de la Información (ISF Standard of Good Practice): Este marco proporciona una serie de controles y buenas prácticas para gestionar la seguridad de la información en entornos de nube. Se basa en estándares reconocidos internacionalmente, como ISO/IEC 27001, y proporciona orientación detallada sobre cómo implementar controles de seguridad efectivos en la nube.
- Gestión de Riesgos y Cumplimiento Normativo (GRC): Esta metodología integra la gestión de riesgos, el cumplimiento de las normas y la gobernanza en un enfoque holístico para gestionar los riesgos asociados con el uso de servicios en la nube. Se utilizan herramientas y procesos específicos para identificar, evaluar y mitigar los riesgos de seguridad y privacidad, así como para garantizar el cumplimiento con regulaciones y estándares relevantes.
- Desarrollo Ágil: Esta metodología se centra en la iteración rápida y la colaboración entre equipos multidisciplinarios para desarrollar políticas de uso de servicios en la nube de manera flexible y adaptable. Se utilizan técnicas como la planificación por iteraciones, la retrospectiva y la revisión continua para mejorar y ajustar las políticas en función de los comentarios y los cambios en el entorno.
- Revisión por Pares y Consulta Externa: Esta metodología implica la revisión y validación de las políticas por parte de expertos internos y externos en seguridad de la información y cumplimiento normativo. Se solicita retroalimentación y comentarios de diferentes partes interesadas para garantizar que las políticas sean completas, precisas y relevantes para las necesidades de la organización.

Estrategia de socialización de las políticas

En este apartado se presenta un plan de socialización para las políticas de uso de servicios basadas en el Modelo Cloud Computing:

- Identificación de Audiencia: Identificar a todas las partes interesadas relevantes dentro de la organización, incluyendo altos directivos, gerentes de departamento, personal de TI, usuarios finales y cualquier otra persona que interactúe con servicios en la nube.
- Desarrollo de Materiales de Socialización: Preparar materiales claros y concisos que expliquen las políticas de uso de servicios en la nube, incluyendo documentos informativos, presentaciones, infografías y videos explicativos. Asegurarse de que los materiales estén adaptados a las necesidades y niveles de comprensión de la audiencia objetivo.
- Programación de Sesiones de Capacitación: Organizar sesiones de capacitación presenciales o virtuales para presentar las políticas de uso de servicios en la nube a las diferentes partes interesadas. Programar múltiples sesiones para permitir la participación de todos los grupos relevantes y facilitar la interacción y el diálogo.
- Comunicación y Difusión: Utilizar diferentes canales de comunicación, como correos electrónicos, boletines, intranet corporativa y reuniones departamentales, para difundir información sobre las políticas de uso de servicios en la nube. Enviar comunicados regulares y recordatorios para mantener a todos informados sobre los próximos eventos y actualizaciones relacionadas con las políticas.
- Sesiones Interactivas de Preguntas y Respuestas (Q&A): Programar sesiones interactivas de preguntas y respuestas donde los participantes puedan hacer preguntas y aclarar dudas sobre las políticas de uso de servicios en la nube. Designar expertos en la materia para responder a las preguntas de manera clara y precisa.
- Creación de Recursos de Autoaprendizaje: Desarrollar recursos de autoaprendizaje, como tutoriales en línea, guías de usuario y preguntas frecuentes (FAQ), para que los empleados puedan consultar y revisar la información sobre las políticas en su propio tiempo. Publicar estos recursos en un repositorio accesible para todos los empleados, como la intranet corporativa o el portal de recursos humanos.
- Sesiones de Retroalimentación y Mejora Continua: Programar sesiones regulares de retroalimentación donde los empleados puedan proporcionar comentarios y sugerencias sobre las políticas de uso de servicios en la nube. Utilizar esta retroalimentación para identificar áreas de mejora y realizar ajustes en las políticas según sea necesario.
- Evaluación de la Efectividad de la Socialización: Realizar encuestas y evaluaciones para medir la efectividad de la socialización de las políticas de uso de servicios en la

nube. Analizar los resultados y utilizarlos para mejorar y ajustar el enfoque de socialización en el futuro.

La presente planificación tiene el fin de socializar las políticas enmarcadas en la propuesta a fin de garantizar una comprensión clara y una aceptación efectiva de las políticas de uso de servicios en la nube dentro de la organización, promoviendo así una mayor seguridad y cumplimiento en el uso de servicios en la nube.

2.3. Validación de la propuesta

Para la validación de la tesis, se seleccionaron especialistas con un perfil sólido en estudios sobre seguridad informática, una amplia experiencia laboral en el campo y una destacada participación en encuestas relacionadas con la temática. Estos criterios fueron fundamentales para asegurar la calidad y pertinencia de las evaluaciones realizadas. Para más detalles sobre los especialistas seleccionados, consultar la tabla siguiente (Ver Tabla 16) y los documentos en el (Anexo 2).

Tabla 16

Descripción del perfil de los especialistas

Nombres y Apellidos	Años de experiencia en el área	Titulo obtenido	Cargo
Diego Xavier Montenegro Carrera	20 años	Magíster en Seguridad Informática	Director
Franklin Edwin Vela Vela	10 años	Magíster en Seguridad Informática	Agente Consular

Nota: Los datos de los validadores fueron obtenidos de la documentación del Anexo 2

Los objetivos perseguidos mediante la validación son los siguientes:

- Verificar que la propuesta de políticas de uso de servicios mediante el modelo de computación en la nube para estructuras sensibles, como la base de datos de una ONG, sean relevantes y aplicables en el contexto actual.
- Comprobar que los especialistas comprenden la propuesta en su totalidad y pueden conceptualizarla adecuadamente.
- Cerciorarse que la propuesta esté actualizada en términos de normativas, tecnologías y mejores prácticas en seguridad informática y computación en la nube.
- Precisar si la propuesta cumple con estándares de calidad técnica en términos de precisión, claridad y coherencia.
- Determinar si la propuesta es factible de implementar en la práctica, considerando recursos, tecnología y procesos existentes.
- Determinar si la propuesta es pertinente para abordar los desafíos y necesidades específicas de la ONG en cuanto a seguridad de la información en la nube.

Estos valores representan el grado de cumplimiento de cada criterio evaluado por los especialistas en la validación de la tesis. Cada especialista deberá colocar una "X" en el valor correspondiente a su evaluación de cada indicador (Ver Tabla 17).

Tabla 17

Resultados de los validadores

Indicador	Especialista 1	Especialista 2	Total	Porcentaje
Impacto	4	5	9	12.86%
Aplicabilidad	5	5	10	14.29%
Conceptualización	5	4	9	12.86%
Actualidad	5	5	10	14.29%
Calidad Técnica	5	5	10	14.29%
Factibilidad	5	5	10	14.29%
Pertinencia	4	5	9	12.86%
Total	**33**	**34**	**67**	**95.71%**

Nota: El puntaje fue obtenido de la validación de los especialistas que consta en la documentación del Anexo 2

Para registrar la información de los resultados en la tabla, se utilizarán los siguientes indicadores y valores:

Muy adecuado: 5
Bastante adecuado: 4
Adecuado: 3
Poco adecuado: 2
Inadecuado: 1

2.4. Matriz de articulación de la propuesta

En esta matriz se resume la relación de la investigación realizada con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados (Ver Tabla 18).

Tabla 18

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Sistema de Gestión de Seguridad de la Información	• ISO 27001 - Sistemas de gestión de la seguridad de la información (ISO/IEC, 2022)	Revisión de literatura sobre políticas de seguridad en la nube, consultas a expertos (Gómez Fernández & Fernández Rivero, 2018)	Análisis documental, entrevistas a expertos	Descripción de políticas propuestas, análisis comparativo con normativas existentes	Encuestas, análisis de documentos
Seguridad de la Información	• ISO 27002 - Controles de seguridad de la información (ISO/IEC, 2022)	Revisión de literatura sobre modelos de seguridad en la nube, estudio de casos (ISOTOOLS, 2023)	Análisis de casos, implementación de modelos en entornos simulados	Evaluación de la efectividad de los modelos, identificación de áreas de mejora	Estudio de casos, simulaciones
Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube.	• ISO 27017 - Técnicas de seguridad (ISO/IEC, 2015)	Revisión de literatura sobre seguridad de bases de datos en la nube, análisis de riesgos (BSIGROUP, 2021)	Implementación de medidas de seguridad, monitoreo de la base de datos	Reducción de vulnerabilidades, mejora en la protección de datos	Análisis de riesgos, monitoreo de la base de datos

Encuestas a empleados	• Proceso de investigación cualitativa (Páramo Morales y otros, 2020)	Diseño de preguntas relacionadas con el uso de servicios en la nube, aplicación a una muestra representativa (QuestionPro, 2022)	Análisis estadístico de respuestas, identificación de tendencias y necesidades	Visión general de estado, comparación con estándares ISO	Investigación Bibliográfica

Fuente: Elaboración propia

CONCLUSIONES

El presente proyecto se basó en la proposición de políticas de uso de servicios mediante el modelo Cloud computing o seguridad en la nube para las estructuras sensibles como la base de datos de la ONG para el establecimiento de sistemas de seguridad informática, concluyendo lo siguiente:

Al contextualizar los fundamentos teóricos sobre cloud computing relacionados con la protección de la base de datos, se ha logrado establecer una comprensión sólida de los principios y prácticas fundamentales para garantizar la seguridad y la integridad de la información en entornos basados en la nube. Esto proporciona una base sólida para el desarrollo e implementación de políticas de seguridad efectivas que protejan los datos sensibles de la organización.

El diagnóstico de la situación actual de la ONG en cuanto al tratamiento de seguridad de las estructuras sensibles ha revelado que no existe tal tratamiento, sin embargo, se evidenció áreas de mejora y oportunidades para fortalecer la protección de la información. Por lo que identificar las debilidades y los riesgos existentes es el primer paso para implementar medidas efectivas que mitiguen las amenazas y garanticen la seguridad de los datos en la organización.

Al proponer políticas de uso de servicios basadas en el modelo cloud computing o seguridad en la nube, se ha desarrollado un marco integral que aborda los aspectos clave de seguridad, privacidad y portabilidad de los datos. Estas políticas proporcionan orientación y directrices claras para el manejo seguro de la información en entornos de nube, promoviendo la confianza y la conformidad con los estándares y regulaciones pertinentes.

RECOMENDACIONES

- Continuar actualizando y ampliando el conocimiento sobre las últimas tendencias y desarrollos en el campo del cloud computing y la protección de datos.
- Realizar regularmente revisiones y análisis de riesgos para asegurarse de que las políticas de seguridad estén alineadas con las mejores prácticas actuales.
- Capacitar al personal de manera continua para garantizar que estén al tanto de las últimas amenazas y soluciones en seguridad de la información en entornos de nube.

Recomendaciones basadas en el Diagnóstico de la Situación Actual:

- Implementar medidas correctivas inmediatas para abordar las debilidades y deficiencias identificadas en el tratamiento de seguridad de las estructuras sensibles.
- Establecer un programa de monitoreo y auditoría regular para evaluar el cumplimiento de las políticas de seguridad y detectar posibles vulnerabilidades.
- Mejorar la conciencia y la cultura de seguridad en toda la organización mediante programas de capacitación y sensibilización.

Recomendaciones basadas en la Propuesta de Políticas de Uso de Servicios:

- Comunicar claramente las políticas propuestas a todo el personal y asegurarse de que comprendan sus roles y responsabilidades en la implementación de estas.
- Establecer mecanismos de revisión y actualización periódica de las políticas para adaptarse a los cambios en la tecnología y las regulaciones.
- Fomentar la colaboración entre los equipos de seguridad, TI y cumplimiento normativo para garantizar una implementación integral y efectiva de las políticas.

Recomendaciones basadas en la Valoración por Especialistas:

- Incorporar los comentarios y sugerencias de los especialistas en seguridad de la información en la revisión y mejora de las políticas existentes.
- Realizar evaluaciones regulares de las políticas de seguridad por parte de expertos externos para obtener perspectivas imparciales y garantizar su eficacia.
- Mantenerse al tanto de las mejores prácticas y estándares de la industria mediante la participación en conferencias, grupos de trabajo y redes profesionales.

BIBLIOGRAFÍA

ACNUR. (2023). *Organizaciones no Gubernamentales*. Obtenido de https://www.acnur.org/acnur/nuestros-socios/organizaciones-no-gubernamentales

BSIGROUP. (2021). *ISO/IEC 27017 Controles de Seguridad para Servicios Cloud*. Obtenido de https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

Cisneros, D. (2022). *Análisis, diseño y desarrollo de un sistema de información web para automatizar los procesos de compras, inventarios y ventas (e-commerce). Caso de estudio: COMPUNEX*. Obtenido de http://repositorio.puce.edu.ec/handle/22000/20997

Cloud Security Alliance. (14 de 10 de 2021). *Cloud Security Alliance*. Obtenido de https://cloudsecurityalliance.org/blog/2021/10/14/the-6-phases-of-data-security

Cloud, G. (07 de 07 de 2022). *Responsabilidades compartidas y destino compartido en Google Cloud*. Obtenido de https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate?hl=es-419

COPI. (2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL*. Obtenido de Registro Oficial Suplemento 180 de 10-feb.-2014: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Cortijo, E. &. (2022). *PLICACIÓN IoT PARA EL MONITOREO DE CONSUMO ELÉCTRICO RESIDENCIAL UTILIZANDO SOFTWARE LIBRE*. Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3327

Deloitte. (2022). *Automatización con inteligencia.* Obtenido de https://www2.deloitte.com/content/dam/Deloitte/sv/Documents/consultoria/Automatizacion-con-inteligencia-2022.pdf

Escalona, M. &. (2022). *PROTOTIPO DE SISTEMA DE MONITOREO Y CONTROL DE CONSUMO DE ENERGÍA ELÉCTRICA PARA UN DOMICILIO APLICANDO EL CONCEPTO DE INTERNET DE LAS COSAS.* Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/2429

Gómez Fernández, L., & Fernández Rivero, P. P. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. En L. Gómez Fernández, & P. P. Fernández Rivero, *Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad* (pág. 165). AENOR - Asociación Española de Normalización y Certificación.

Goyes, J. (2020). *Estudio de impacto del modelo cloud computing en la gestión de servicios de información gerencial en la banca privada Caso: Banco Internacional*. Obtenido de https://repositorio.uasb.edu.ec/bitstream/10644/7468/1/T3265-MAE-Goyes-Estudio.pdf

Granda, R. &. (2022). *Transformación digital: propuesta metodológica para la automatización de procesos desde el enfoque del BPM.* Obtenido de https://doi.org/10.35290/rcui.v9n3.2022.621

Haliux, V. (2023). *Seguridad en el Cloud Computing: protegiendo tus datos en la nube.* . Obtenido de https://www.tokioschool.com/noticias/seguridad-cloud-computing/

INCENTRO. (2023). *¿Cómo garantizar la seguridad en la nube y proteger los datos de tu organización?* Obtenido de https://www.incentro.com/es-ES/blog/seguridad-en-la-nube

ISO/IEC. (2015). *ISO/IEC 27017*. Obtenido de https://www.iso.org/standard/43757.html

ISO/IEC. (2022). *ISO/IEC 27001*. Obtenido de https://www.iso.org/standard/27001

ISO/IEC. (2022). *ISO/IEC 27002*. Obtenido de https://www.iso.org/standard/75652.html

ISOTOOLS. (2020). *¿Qué es la ISO 27001?* Obtenido de Sistemas de Gestión la Seguridad de la Información: https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

ISOTOOLS. (2022). *IEC 27002:2022 Controles Organizacionales. Todo lo que necesita saber II*. Obtenido de https://www.isotools.us/2022/08/05/iso-iec-270022022-controles-organizacionales-todo-lo-que-necesita-saber/

ISOTOOLS. (2023). *Control de Seguridad de la información en la nube de la nueva ISO 27002*. Obtenido de https://www.isotools.us/2023/01/26/control-de-seguridad-de-la-informacion-en-la-nube-de-la-nueva-iso-27002/#:~:text=control%20de%20acceso.-,ISO%2027002,los%20intereses%20de%20la%20organizaci%C3%B3n.

LCE. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos* . Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Ley de Protección al Consumidor. (2012). Obtenido de (Ley No. 2000-21): https://www.dpe.gob.ec/wp-content/dpetransparencia2012/literala/BaseLegalQueRigeLaInstitucion/LeyOrganicadelConsumidor.pdf

Ley de Telecomunicaciones y regulaciones asociadas. (2015). Obtenido de Registro Oficial Nº 439 -- Miércoles 18 de febrero de 2015: https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Ley Orgánica de Protección de Datos Personales (LOPDP) . (2021). Obtenido de Registro Oficial Suplemento 459 de 26-may.-2021: https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Méndez, R. (2020). *PROPUESTA DE UN MODELO DE POLÍTICA PARA PROTECCIÓN DE DATOS PERSONALES PARA PROVEEDORES DE SERVICIOS DE CÓMPUTO EN LA NUBE*. Obtenido de https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/488/1/Tesis%20Rodrigo%20Mendez%20Solis%20INFOTEC.pdf

Méndez, R. (2020). *PROPUESTA DE UN MODELO DE POLÍTICA PARA PROTECCIÓN DE DATOS PERSONALES PARA PROVEEDORES DE SERVICIOS DE CÓMPUTO EN LA NUBE".* Obtenido de https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/488/1/Tesis%20Rodrigo%20Mendez%20Solis%20INFOTEC.pdf

Páramo Morales, D., Campo Sierra, S., & Maestre Matos, L. (2020). *Métodos de investigación cualitativa: fundamentos y aplicaciones.* Editorial Unimagdalena.

Parra, F. &. (2020). *Sistema integrado para la operación de un brazo robótico teleoperado en tiempo real mediante la plataforma Firebase con el uso de dispositivos móviles.* . Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/2395

QuestionPro. (2022). *Encuestas cualitativas: Qué son, beneficios y cómo hacerlas*. Obtenido de https://www.questionpro.com/blog/es/encuestas-cualitativas/#:~:text=Las%20encuestas%20cualitativas%20son%20una,o%20relatos%20de%20los%20encuestados.

Rcalde, P. &. (2022). *Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017.* . Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3369

Recalde, H. &. (2022). *IMPLEMENTACIÓN DE GESTOR DOCUMENTAL Y FLUJO DE TRABAJO EN LA NUBE PARA LA CRUZ ROJA ECUATORIANA.* . Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/2093

Recalde, P. &. (2023). *Propuesta de seguridad informática para el control de acceso dirigida a la infraestructura para el Colegio Nacional Cutuglagua aplicando la Norma ISO 27001; A9 control de acceso.* . Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/3562

Sisti, M. (2019). *SEGURIDAD INFORMÁTICA: LA PROTECCIÓN DE LA INFORMACIÓN EN UNA EMPRESA VITIVINÍCOLA DE MENDOZA*. Obtenido de https://bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

Tamayo, R. &. (2018). *nálisis de Uso y Aplicación de Cloud Computing en las Empresas de Ahorro y Crédito de la ciudad de Cuenca.* Obtenido de https://repositorio.uisrael.edu.ec/handle/47000/600

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

1. ¿Está informado sobre los Datos Confidenciales que se manejan en la organización?

2. ¿Se han establecido políticas de seguridad para el manejo de información confidencial?

3. ¿Utilizan herramientas seguras para cargar, transmitir y generar información que involucre datos confidenciales en la organización?

4. ¿Conoce modelo Cloud Computing (Computación en la Nube)?

5. ¿En qué medida utiliza su organización servicios de computación en la nube actualmente?

6. ¿El personal de la organización reconoce cuando está siendo atacado por una técnica de phishing?

7. ¿Emplea técnicas de encriptación para enviar información confidencial a través de correo electrónico?

8. ¿Cuál sería el impacto primordial que podría generar la filtración de información confidencial?