INSTITUTO SUPERIOR TECNOLÓGICO SAN ANTONIO

Escuela de tecnología e innovación

Diseño de un marco de políticas de seguridad para la migración a la nube en Segurilab, con enfoque en la protección de datos y normativas locales, Quito 2025.

Rafael Alexander Suntasig Paredes

Ciberseguridad

Trabajo de fin de carrera presentado como requisito

para la obtención del título de

Tecnólogo Superior en Ciberseguridad

Quito, 14 de mayo de 2025

INSTITUTO SUPERIOR

TECNOLÓGICO SAN ANTONIO

Escuela de tecnología e innovación

HOJA DE CALIFICACIÓN

DE TRABAJO DE FIN DE CARRERA

Diseño de un marco de políticas de seguridad para la migración a la nube en Segurilab, con enfoque en la protección de datos y normativas locales, Quito 2025.

Rafael Alexander Suntasig Paredes …/….

Christian Ruben Molina Caza, Ing.

Quito, 14 de mayo de 2025

DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales del Instituto Superior Tecnológico San Antonio TESA, incluyendo la Política de propiedad Intelectual TESA, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a TESA para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Nombres y apellidos: Rafael Alexander Suntasig Paredes

Código estudiante: 2082/7897

Cédula de identidad: 1720908027

Lugar y fecha: Quito, mayo de 2025

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, pese a estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en ttp://bit.ly/COPETheses.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Instituto Superior Tecnológico San Antonio TESA institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on http://bit.ly/COPETheses.

DEDICATORIA

Quiero dedicar este logro a las personas que han sido fuente de inspiración y me han dado fuerzas y motivación para superarme hasta este punto. Ustedes han sido fundamentales en mi camino:

A ti mi Alexia, en el momento en que supe que sería padre busqué la manera de superarme y no conformarme, tú eres mi fuente inagotable de energía y motivación, la razón que me impulsa a cumplir mis objetivos, teniéndote a ti presente he superado los dilemas que han aparecido a lo largo de mi vida. Este logro es tan tuyo como mío, mi princesa. A Liliana, la madre de mi hija, gracias por darle vida a nuestra princesa y acompañarla en su crecimiento. Tu presencia es importante en su desarrollo y de alguna forma, también lo ha sido en el mío.

A mis padres Myriam y Patricio, a ustedes que creyeron en mí, por su sacrificio y apoyo incondicional a pesar de las dificultades que se han presentado a lo largo del camino han estado para mí, con un mensaje de aliento para no desfallecer. Ahora puedo decir que cumplo una de sus aspiraciones como padres, el verme graduado de una carrera de tercer nivel y ser el hombre que han criado con amor y enseñanzas valiosas que he atesorado hasta estos días y no me he rendido hasta culminar este logro.

Este logro también va dedicado para mis hermanas Kamila y Josselyn que han estado para mi apoyándome en mis desveladas, dándome palabras de aliento para no rendirme en mis estudios y han sido confidentes en mis días de tristeza.

Este logro es el producto de esfuerzo, dedicación y desveladas que he invertido para alcanzarlo, no puedo evitar mirar al cielo y decirte: “tú negrito, tú cholito, lo logró”, no sabes la falta que me haces, te fuiste muy joven abuelita.

AGRADECIMIENTO

En este logro han colaborado muchas personas y me tomo este espacio para agradecer su apoyo, enseñanzas y consejos.

A mis padres, gracias por apoyarme y alentarme a estudiar una carrera de tercer nivel, como ustedes dicen: *"el estudio será tú herramienta para enfrentarte al mundo real"*.

A Berenice Sarmiento, mi tutora de prácticas, quien me brindó las herramientas que me han ayudado a desarrollar mis actividades tanto profesionales como académicas, aportando con nuevos conocimientos e inculcándome el gusto por las normativas y políticas de seguridad de la información.

Mi sincero agradecimiento a TESA y a cada uno de los profesores. A TESA, por contar con docentes que han demostrado pasión y vocación por la enseñanza. No solo han formado al estudiante, sino también al profesional que hoy emerge. Espero ejercer tan bien esas enseñanzas para dejar en alto a la institución y decir ante la sociedad, con orgullo, que me formé en TESA.

Una mención especial al Ing. Christian Molina, porque en sus materias he podido ver que en el mundo de la ciberseguridad podemos especializarnos en diferentes áreas. Hoy estoy motivado a seguir estudiando y superándome con alguna especialización.

RESUMEN

El incremento del uso de servicios en la nube por parte de las empresas que manejan datos personales genera interrogantes de si la protección de datos y el cumplimiento de normativas legales se está cumpliendo. Este proyecto de titulación tiene como objetivo diseñar y evaluar un marco de políticas de seguridad para la migración a la nube en empresas ecuatorianas, tomando como objeto de estudio a la empresa Segurilab, ubicada en Quito, con la finalidad de asegurar la protección de datos y el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPD).

El trabajo de investigación tendrá un enfoque cualitativo, centrado en analizar los aspectos relacionados con la seguridad en Segurilab. Se evaluará el estado actual de la seguridad, los riesgos asociados a la transición a la nube y el cumplimiento normativo para realizar las respectivas mejoras en las áreas de Segurilab, se harán encuestas tanto a personal de Segurilab como a expertos externos, para tener una visión más completa al momento de diseñar las políticas.

Como resultado y entregable, se elaborará un manual de políticas de seguridad para la migración a la nube, que incluirá buenas prácticas adaptadas al contexto legal, sirviendo como herramienta para garantizar a las empresas el cumplimiento legal y mejorar la gestión de la seguridad de la información.

Palabras clave: Políticas de seguridad, migración a la nube, Ley Orgánica de Protección de Datos Personales, seguridad de la información, normativas legales, protección de datos.

ABSTRACT

The growing adoption of cloud services by companies handling personal data raises concerns about whether data protection and compliance with legal regulations are being adequately addressed. This graduation project aims to design and evaluate a security policy framework for cloud migration in Ecuadorian companies, with a case study focused on Segurilab, a company based in Quito. The objective is to ensure data protection and compliance with the Organic Law on Personal Data Protection (LOPD).

The research will adopt a qualitative approach, focusing on analyzing security aspects within Segurilab. The current state of security, the risks associated with cloud migration, and regulatory compliance will be assessed to implement necessary improvements within Segurilab's operations. Surveys will be conducted with Segurilab staff as well as external experts to gain a comprehensive understanding when designing the policies.

As a result, a security policy manual for cloud migration will be developed, incorporating best practices tailored to the legal context. This manual will serve as a tool for companies to ensure legal compliance and enhance the management of information security.

Keywords: Security policies, cloud migration, Organic Law on Personal Data Protection, information security, legal regulations, data protection.

TABLA DE CONTENIDOS

CAPÍTULO I INTRODUCCIÓN 15

1.1. Planteamiento del Problema 15

1.2. Justificación 17

1.3. Alcance 18

1.4. Objetivos General y Específicos 19

CAPÍTULO II MARCO TEÓRICO 20

CAPÍTULO III. MARCO METODOLÓGICO 22

3.1. Tipo de investigación 22

3.2. Enfoque 23

3.3. Herramientas metodológicas 23

3.5. Estudios iniciales 24

3.6. Desarrollo 24

Encuesta para Expertos en Seguridad de la Información y Migración a la Nube 24

Encuesta para el personal de Segurilab para evaluar el conocimiento de las diferentes áreas de Segurilab. 26

CAPITULO IV. RESULTADOS Y DISCUSIÓN 29

4.1. Análisis de resultados (descripción) 29

Encuesta a 30 trabajadores de Segurilab 29

4.2. Interpretación y discusión de resultados 38

CONCLUSIONES 39

RECOMENDACIONES 40

REFERENCIAS BIBLIOGRÁFICAS.....41

ANEXO A: Marco de políticas de seguridad para la migración a la nube en Segurilab, con enfoque en la protección de datos y normativas locales, Quito 2025. 43

1.Introducción 47

2.Definiciones 48

3.Marco Legal y Normativo.....49

4.Responsabilidades.....50

I Equipo de Tecnologías de la Información (TI):.....50

II Personal Administrativo y Médico: 51

III Recursos Humanos: 51

IV Gerencia: 52

5.Recolección y Tratamiento de Datos 52

Obtención de datos de pacientes 53

Tratamiento de datos.....54

6.Derechos de los Titulares.....55

7.Conservación de Copias de datos 56

Tiempo y frecuencia de las copias de seguridad.....56

Almacenamiento de Copias de Seguridad 56

Tratamiento de las copias de seguridad 57

Recuperación de Datos 57

Auditorías de Seguridad.....57

8.Transferencia de Datos 58

Mecanismos de transferencia de datos....58
9.Plan de respuesta a incidentes de Seguridad....59
Objetivos del plan de respuesta a incidentes....59
Roles y responsabilidades....59
Fases del plan de respuesta a incidentes....60
Garantías de Transparencia y Cumplimiento Normativo....63
10.Gestión de Contraseñas....63
Parámetros de la gestión de contraseñas....63
Revocación de accesos....65
11.Concienciación y Formación....65
12.Control de Acceso....66
Pasos para garantizar el control de acceso....66
Prevención a accesos no autorizados....67
Dispositivos personales en Segurilab....67
Ante robo o pérdida....68
Parte legal....68
13.Auditoría interna....68
1.Preparación de la auditoria....68
2.Análisis documental....69
3.Ejecución de la auditoría....69
4.Evaluación y análisis de resultados....70

5.Informe.....70

6.Monitoreo y seguimiento.....71

REFERENCIAS BIBLIOGRÁFICAS.....72

Índice de Tablas

Tabla 1. Matriz de operacionalización de variables.....24

Tabla 2.Plataformas que usa Segurilab. 64

Índice de figuras

Figura 1. Área Laboral 29

Figura 2. Capacitación sobre seguridad 30

Figura 3. Uso de plataformas en la nube 30

Figura 4. Nivel de confianza en la nube 31

Figura 6. Contraseñas para sistema en la nube 32

Figura 5. Riesgos de seguridad al almacenar datos 32

Figura 7. Nivel de phishing en Segurilab 33

Figura 8. Riesgos de seguridad 34

Figura 9. Normativas para aplicar 34

Figura 10. Controles de seguridad para el manual 35

Figura 11. Servicios de un proveedor de servicio en la nube 36

Figura 12. Consideraciones legales para una política 36

Figura 13. Acciones claves para implementación efectiva del manual 37

CAPÍTULO I
INTRODUCCIÓN

1.1. Planteamiento del Problema

Hace 10 años el uso de la tecnología en la nube creció exponencialmente, permitiendo a las empresas acceder a herramientas que brindan servicios sencillos que permiten manejar el modelo de negocio de una empresa sin depender de espacios enormes para el almacenamiento de la información, poco a poco se acaba con los espacios que son destinados para servidores o sala de discos duros que almacenan toda la información que se recibe. Pero, existen desafíos, estos son el cumplir con las normativas locales, en Ecuador la Ley Orgánica de Protección de Datos Personales se aprobó con el fin de dar las garantías de que la información que se obtiene en las empresas, de clientes de trabajadores, de proveedores es tratada correctamente y que los tiempos de conservación, sea digital o físicamente se cumplan.

En esta investigación se va a tratar el problema de la falta de políticas de seguridad adecuadas para dar la garantía de que los datos son protegidos en el proceso de migración a la nube en la empresa Segurilab. Al trabajar en plataformas en la nube, se puede presentar escenarios de ataques donde la integridad y disponibilidad de la información se vea comprometida es ahí donde las políticas que se van a desarrollar darán una guía de cómo debemos actuar ante estos escenarios y cómo se debe proceder para evitar que el ataque no sea de gran impacto y la información no se pierda ya que busco evitar esa fuga de información con la identificación y bloqueo del supuesto ataque que busca apropiarse de la empresa Segurilab.

El informe de la Cámara de Comercio de Quito (2022) destaca que el 40% de las PYMES desconfían del uso de la nube, a raíz de que existen riesgos de seguridad no resueltos, lo que frena la transformación digital en el país. Además, la normativa que se ha instaurado en el Ecuador es reciente, por lo que muchas empresas están en la búsqueda de

asesoría por parte de expertos en el campo y ahora el problema es que no hay especialistas formados en este campo, carreras como Ciberseguridad, Desarrollo Web, Inteligencia Artificial son carreras que han nacido en estos últimos años pero aún los futuros expertos están estudiando y especializándose en este extenso campo, para contestar a interrogantes de las principales vulnerabilidades que enfrentan las empresas ecuatorianas al migrar sus operaciones y datos a la nube, el impacto de políticas de seguridad, los beneficios de hacer uso de una buena o mala política de seguridad, clasificar las políticas de acuerdo a la función que va a desarrollar la empresa, en la investigación trato de la empresa Segurilab, una empresa que brinda salud ocupacional, se tratará todo el camino que recorre la información desde que se recibe la información, hasta que se haya cumplido con el propósito para el cual se recogió y cómo se procede con la correcta eliminación, debido a que toda información que se recoge se debe conservar hasta un tiempo límite, esto está fijado en normativas ecuatorianas que a lo largo de la investigación iré enumerando, como la LOPD, el código del trabajador, ley de la salud, ley tributaría.

Busco diseñar un conjunto de políticas de seguridad que aseguren la protección de datos y el cumplimiento de las leyes ecuatorianas que se han aprobado desde el año 2021 y se ha exigido su implementación desde el año 2023, en el gobierno del anterior presidente Guillermo Lasso, indicando todo el proceso que tiene la información y cómo se debe proceder en la migración a la nube, para garantizar que la integridad y disponibilidad de la información no se vea comprometida. Buscaré realizar una comparativa con normativas internacionales, ya que en la sociedad ecuatoriana lo que viene o se usa afuera tiene una mayor reputación que una guía que se realizó en Ecuador, por un estudiante de Ciberseguridad

1.2. Justificación

A raíz de las exigencias por parte del gobierno del expresidente del Ecuador Guillermo Lasso, se viene un escenario de oportunidades y desafíos para todas las empresas ecuatorianas, se exige que toda empresa que trabaje con información explique cómo obtiene la información, cómo trabaja, cómo la almacena, quien tiene acceso a la misma y qué pasos realiza la empresa para la respectiva eliminación una vez ya expire su tiempo de conservación.

Las empresas que estén actualizados y tengan sus políticas de seguridad al día, serán empresas que tendrán ese extra y por lo tanto los ciudadanos darán un voto de confianza y se inclinaran por recurrir a los servicios de negocios que cumplan con las normativas vigentes. Además, las empresas pueden acceder a obtener certificaciones de estándares de calidad, permitiendo a la empresa unirse a una pequeña lista de empresas que cumplen con el correcto manejo de la información.

Esta investigación proporcionará soluciones concretas al reto que supone a la empresa Segurilab el migrar su desempeño de negocio a la nube, para ello se enfocará en que la integridad de la información y disponibilidad de la misma sea el idóneo, ya que en mi caso la información que maneja Segurilab es sensible, esta información sensible ya que se trata de datos médicos e información personal, número de identificación, vivienda, datos bancarios, entre otros.

El impacto esperado de este trabajo es amplio y significativo. Se pretende minimizar los riesgos asociados a la migración a la nube, optimizar el uso de recursos tecnológicos, garantizar el cumplimiento de las normativas vigentes y fortalecer la confianza de los clientes en los servicios ofrecidos por las empresas ecuatorianas. Al diseñar políticas claras y adaptadas, se espera fomentar un entorno empresarial más seguro, eficiente y competitivo, impulsando la transformación digital en el país de manera responsable y sostenible.

En conclusión, esta investigación busca ser un aporte relevante para el desarrollo empresarial y tecnológico de Ecuador, promoviendo la adopción de prácticas de ciberseguridad que no solo protejan los activos informáticos, sino que también fortalezcan la posición estratégica de las empresas en el mercado global

1.3. Alcance

El proyecto se centrará en la empresa Segurilab centro médico de especialidades, es una empresa que se dedica a brindar el servicio de salud ocupacional, redactaré los pasos que se debe realizar para hacer la migración a la nube. Incluiré una revisión de las normas en vigencia en el Ecuador, especialmente la Ley Orgánica de Protección de Datos Personales (LOPD). A lo largo del documento que realizaré incluiré políticas de seguridad que cumplirán los requisitos que impone la (LOPD), encontraremos políticas de contraseñas, políticas de red, políticas de uso de dispositivos personales, de copias de seguridad, entre otras. Finalmente, realizaré una comparación con guías de buenas prácticas que hayan adoptado empresas a nivel internacional. El resultado de este trabajo será una guía práctica de los procesos que realizará Segurilab para la migración a la nube sin comprometer la información que día a día va recibiendo de sus pacientes, trabajadores y proveedores. Además, haré la comparativa con las políticas que se hayan manejado en empresas extranjeras de países del primer mundo, obteniendo recomendaciones para que Segurilab se maneje bajo estándares internacionales como normativas ISO.

Con todo lo que desarrollará, entregaré un conjunto de instrucciones y políticas prácticas para que las empresas ecuatorianas adopten de acuerdo con su modelo de negocio, las políticas de uso y manejo de la información que se recibe, evitando que la información se vea comprometida por ciberataques o personas que no deberían tener acceso a dicha información, realicen cambios no deseados.

1.4. Objetivos General y Específicos

Objetivo general

- Diseñar y evaluar políticas de seguridad para la migración a la nube en empresas ecuatorianas, asegurando la protección de datos y el cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPD).

Objetivos Específicos

- Analizar el marco normativo vigente en Ecuador relacionado con la migración a la nube, evaluando su impacto en la protección de datos personales y la seguridad de la información en las empresas.
- Diseñar políticas de seguridad para la migración a la nube en empresas ecuatorianas, considerando las normativas locales y estándares internacionales de protección de datos.
- Evaluar el cumplimiento de las políticas de seguridad en la migración a la nube mediante el análisis de prácticas actuales en el contexto empresarial ecuatoriano.

CAPÍTULO II
MARCO TEÓRICO

Se debe colocar los sustentos técnicos, científicos y teóricos en las que se basa el trabajo de titulación.

Seguridad de la información

La seguridad de la información hace referencia a lo a protección de los datos contra los accesos no autorizados, alteración, destrucción o pérdida de los mismos. Según la norma ISO/IEC 27001(2007) , la seguridad de la información se respalda en 3 pilares; confidencialidad, integridad y disponibilidad (CIA). En el ámbito empresarial, la correcta gestión de la seguridad da garantías de que los activos de información que una empresa maneja en sus operaciones están seguros.

Migración a la nube

Google Cloud (s.f.), define la migración a la nube como:

"El proceso de trasladar aplicaciones, datos, infraestructuras, seguridad y otros objetos a un entorno de computación en la nube. Se trasladan datos, aplicaciones y cargas de trabajo de TI de los servidores locales a la nube pública, sin embargo, la migración a la nube también incluye la transferencia de datos y aplicaciones de un proveedor de servicios en la nube a otro" (párr. 2).

¿Por qué migrar a la nube?

Uno de los motivos por los que las empresas migran a la nube es la facilidad que da al momento de disminuir costos y se hace una infraestructura tecnológica más eficiente. Además, al eliminar la necesidad de contar con grandes salas para alojar los servidores en un espacio físico y su respectivo mantenimiento, las empresas pueden dedicar ese capital en fortalecer los servidores de herramientas para un monitoreo en tiempo real y la adquisición de

más espacio en la nube, de ser necesario. Se hace una gestión más flexible y escalable de los recursos tecnológicos, en función de lo que se requiere, se adquiere una herramienta.

Normativa aplicable: LOPD y estándares internacionales

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPD) impone la obligación a quienes manejan datos personales de asegurar su tratamiento bajo principios como la seguridad, confidencialidad, integridad, legalidad y consentimiento informado por parte de los titulares (Asamblea Nacional del Ecuador, 2021).

Además, la norma internacional ISO/IEC 27001 proporciona una estructura para establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI). Este enfoque contribuye a prevenir riesgos, promover prácticas seguras y fomentar una cultura organizacional enfocada en la protección continua de la información (ISO, 2007).

Buenas prácticas y marcos internacionales

Dentro de los lineamientos internacionales más relevantes se encuentran los publicados por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos. El NIST SP 800-53 presenta una serie de controles de seguridad aplicables a los sistemas de información, mientras que el NIST SP 800-61 detalla procedimientos para actuar frente a incidentes de seguridad informática. En este sentido, Guerra (2023) destaca la importancia de que las organizaciones cuenten con planes de respuesta bien definidos, además de realizar simulacros periódicos que permitan comprobar su efectividad (pág.1).

Importancia de un marco de políticas de seguridad

Contar con un conjunto claro de políticas de seguridad permite a las organizaciones estructurar adecuadamente las funciones, responsabilidades y mecanismos necesarios para la gestión segura de los datos. Según Ruiz (2024), la ausencia de políticas adecuadas al momento de migrar hacia entornos en la nube puede ocasionar interrupciones en los servicios, pérdida de información crítica y posibles sanciones legales (pág.52).

CAPÍTULO III.
MARCO METODOLÓGICO
(DISEÑO E IMPLEMENTACIÓN)

3.1. Tipo de investigación

3.1.1. Según el propósito

Esta investigación se clasifica como descriptiva y aplicada, ya que se realizará un análisis inicial del estado de la seguridad en Segurilab, los posibles riesgos asociados a la migración a la nube y las normativas vigentes. Se tiene como objetivo diseñar un marco de políticas de seguridad haciendo uso de las políticas existentes y estándares en el Ecuador. La empresa Segurilab, que presta el servicio de salud ocupacional. Su enfoque práctico de protección de datos y el cumplimiento de las normativas locales y estándares internacionales, genera esta necesidad del departamento de TI de buscar la normativa para crear y diseñar una serie de directrices que aseguran la transición segura y eficiente a la nube.

3.1.2. Según la manipulación de variables

En esta sección la investigación es de tipo no experimental, al no alterarse directamente las variables, ya que realizará un análisis de la seguridad actual que se gestiona en Segurilab y los posibles riesgos que se pueden encontrar al hacer la migración a la nube. Se hará una actualización de las políticas existentes, se revisará las buenas prácticas que usan los trabajadores para identificar y tener un plan de acción ante los incidentes que se pueden presentar usando la LOPD(Ley Orgánica de protección de Datos Personales), ISO 27001, entre otros estándares.

3.1.3. Según el tiempo

Será de tipo transversal, ya que se realizará en un momento del tiempo, iniciando con el análisis del estado actual de la seguridad en Segurilab y los riesgos que se pueden hacer presentes en la transición a la nube. Claro está que en las recomendaciones de la elaboración de este marco va a estar la recomendación de hacer un seguimiento a la implementación de

las políticas, no obstante, en nuestra investigación se evaluará las políticas y buenas prácticas existentes y qué tan afines a la normativa vigente están y con esta base se rediseñará y se hará un marco de políticas de seguridad alineado con la Ley Orgánica de Protección de Datos Personales, ISO/IEC 27001.

3.2. Enfoque

Esta investigación tendrá un enfoque cualitativo, ya que se hará un análisis de los aspectos relacionados con la seguridad en Segurilab, la migración a la nube y el cumplimiento normativo y en base al entendimiento de cómo está seccionado y con la ayuda de las normativas vigentes en Ecuador y estándares para la gestión de la información, fuentes teóricas, se diseñará un marco de políticas de seguridad para Segurilab. Corrigiendo las áreas que deben mejorar y mejorar la eficiencia de la protección de datos y transición a la nube.

3.3. Herramientas metodológicas

Se utilizará el estudio de caso para llevar a cabo una revisión y análisis exhaustivo de la seguridad en Segurilab, enfocándose en los aspectos relacionados con la nube y las políticas actuales que requieren mejoras o nuevas implementaciones. Este enfoque permitirá identificar los riesgos existentes y evaluar si las políticas de seguridad actuales están siendo aplicadas correctamente. A partir de este análisis, se propondrán mejoras en la gestión de seguridad, incorporando buenas prácticas y cumpliendo con las normativas vigentes en Ecuador, con el objetivo de garantizar una transición segura y eficiente hacia la nube.

3.4. Técnicas

Las técnicas empleadas para esta investigación son:

- Análisis documental: revisando los documentos relacionados con las políticas de seguridad existentes en Segurilab, normativas nacionales e internacionales LOPD y ISO 27001, permitiendo mejorar las políticas y adoptar nuevas de ser necesario.

- Entrevistas: conversatorios con responsables del área de TI en Segurilab, con el objetivo de recopilar información de los procedimientos y prácticas actuales.
- Estudio de caso: estudiando el estado inicial de la seguridad en Segurilab, con sus riesgos y políticas a mejorar para garantizar una transición segura y eficiente a la nube.

3.5. Estudios iniciales

Tabla 1. Matriz de operacionalización de variables

Definición conceptual	**DIMENSIONES ¿QUÉ ASPECTO SE PUEDE MEDIR? PENSAR EN GENERALIDAD**	**INDICADORES**	**Instrumento**
Marco de políticas para la migración a la nube en Segurilab. ***¿Qué?*** *Solo nos limitamos a definir* **Definición** Conjunto de directrices que aseguran una transición segura y eficiente a la nube, garantizando la protección de datos y cumpliendo con las normativas locales e internacionales. ***¿Qué quiero saber de esto?*** Aplicación	- Técnica - Social - Institucional Actor: TI *¿Cómo se manifiesta aquello quiero sabe?* Aplicación del marco de políticas para la migración a la nube en Segurilab. *Debe preguntarse de manera general*	- *¿Cuáles métricas manifiestan que han existido aplicación?* - ¿Cuáles políticas han sido adaptadas para la empresa? - Considera que el marco de políticas para migración ha contribuido a la seguridad empresarial. o SI/NO o Totalmente de acuerdo o De acuerdo o No de acuerdo ¿Qué nivel de importancia le atribuyen los trabajadores al marco de políticas?	- Entrevista - Encuesta - Entrevista/encuesta - Firewall *¿Con qué voy a conocer que la variable independiente tuvo efecto en la variable dependiente?*

3.6. Desarrollo

Mostraremos las encuestas con las que sustentaremos la elaboración del presente documento. Una encuesta a 8 expertos en Seguridad de la información y Migración a la Nube y otra encuesta a 30 personas que trabajan en diferentes áreas de Segurilab.

Encuesta para Expertos en Seguridad de la Información y Migración a la Nube

Instrucciones: Por favor, responda las siguientes preguntas sobre los aspectos importantes a considerar en un manual de políticas de seguridad para la migración a la nube

en una empresa. Su opinión es crucial para la elaboración de un marco adecuado de políticas de seguridad.

1. En su experiencia, ¿Cuál es el principal riesgo de seguridad al migrar una empresa a la nube?

- Pérdida de datos
- Acceso no autorizado
- Incumplimiento normativo
- Falta de control sobre los recursos

2. ¿Qué normas y marcos considera fundamentales al diseñar políticas de seguridad en la nube? (Seleccione 2 opciones)

- ISO/IEC 27001
- NIST SP 800-53
- GDPR
- Ley Orgánica de Protección de Datos Personales (LOPD - Ecuador)

3. ¿Cuáles son los tres controles de seguridad más importantes que deberían incluirse en un manual de políticas para migración a la nube?

- Control de acceso y autenticación (MFA)
- Cifrado de datos en tránsito y reposo
- Segmentación de redes
- Gestión de vulnerabilidades
- Monitoreo continuo y auditorías
- Gestión de incidentes de seguridad
- Plan de recuperación ante desastres

4. Desde una perspectiva de seguridad, ¿Cuáles son los dos criterios más relevantes al momento de seleccionar un proveedor de servicios en la nube?

- Cumplimiento normativo (ISO, GDPR, LOPD, etc.)
- Auditorías y pruebas de seguridad independientes
- Contratos claros con cláusulas de seguridad (SLA, protección de datos)
- Capacidad de respuesta ante incidentes y recuperación de servicios

5. ¿Cuáles son las dos principales consideraciones legales o de privacidad que deben contemplarse en una política de seguridad para migración a la nube?

- Protección de datos personales durante y después de la migración
- Derechos de acceso, rectificación y eliminación de datos
- Cumplimiento con leyes locales y normativas internacionales
- Inclusión de cláusulas de privacidad en contratos con proveedores

6. ¿Qué acciones considera claves para una implementación efectiva y mejora continua del manual de seguridad en la nube?

- Capacitación del personal y simulacros de incidentes
- Evaluaciones periódicas de amenazas y vulnerabilidades
- Monitoreo continuo de seguridad y pruebas de penetración
- Revisión y actualización del manual basado en incidentes o nuevas tecnologías

Encuesta para el personal de Segurilab para evaluar el conocimiento de las diferentes áreas de Segurilab.

1. **¿En qué área de la empresa trabaja?**

- Atención al cliente
- Administración
- Recursos Humanos

 Tecnología / Seguridad informática

 Otro(Detallar):_____

2. ¿Ha recibido alguna capacitación sobre seguridad de la información en el último año?

 Sí

 No

3. ¿Utiliza algún sistema o plataforma en la nube en su trabajo diario?

 Sí

 No

4. **¿Qué tan seguro cree que es almacenar información en la nube?**

 Muy seguro

 Poco seguro

 Nada seguro

 No sé

5. **¿Cuáles considera que son los principales riesgos de seguridad al almacenar datos en la nube?**

 Robo de información

 Acceso no autorizado

 Pérdida de datos

 Uso indebido de la información personal

 No sé

6. **¿Cuándo crea una contraseña para un sistema en la nube, qué tan seguido usa una combinación de letras, números y símbolos?**

 Siempre

 A veces

- Nunca

7. **¿Alguna vez ha recibido un correo electrónico sospechoso solicitando información personal o credenciales de acceso?**
   - Sí, y lo reporté
   - Sí, pero no supe qué hacer
   - No estoy seguro
   - No

CAPITULO IV.
RESULTADOS Y DISCUSIÓN

4.1. Análisis de resultados (descripción)

Encuesta a 30 trabajadores de Segurilab

Se realizó una encuesta a 30 trabajadores de la empresa de Segurilab, los encuestados fueron personal de diferentes áreas, ya que el objetivo de la encuesta era el de evaluar el nivel de conocimiento sobre la seguridad de la información del personal que trabaja en la empresa. Vamos a realizar el respectivo análisis pregunta por pregunta:

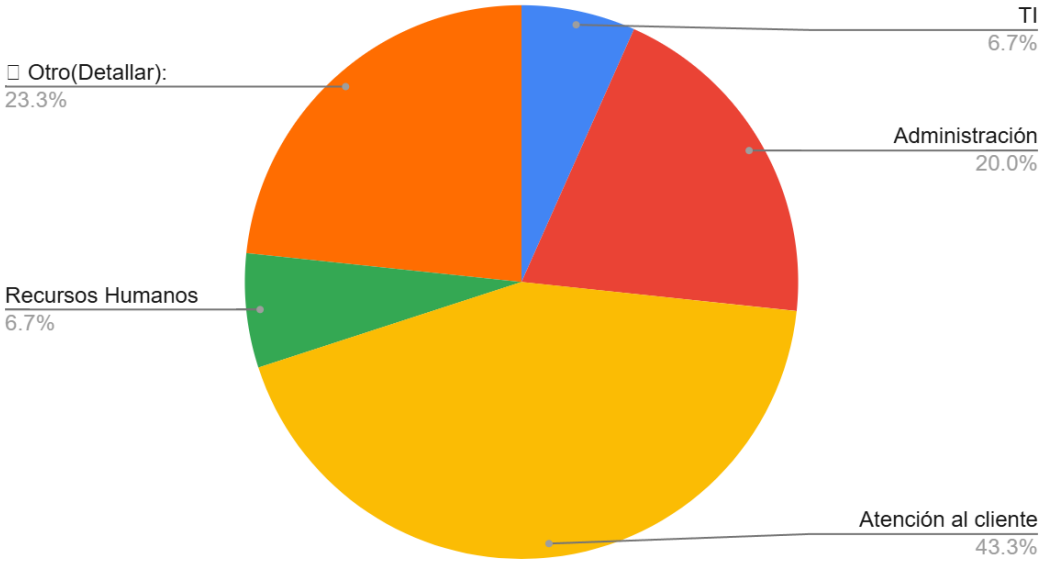


Figura 1. Área Laboral

Para la pregunta 1, ¿En qué área de la empresa trabaja?, los resultados nos indican que la mayoría de los encuestados forman parte de áreas técnicas y operativas como área administrativa, departamento de TI, atención al cliente y en el apartado otros, encontrados a doctores y personal de laboratorio, todas las áreas manejan cantidades de datos que requieren ser tratados bajo el cumplimiento normativo.

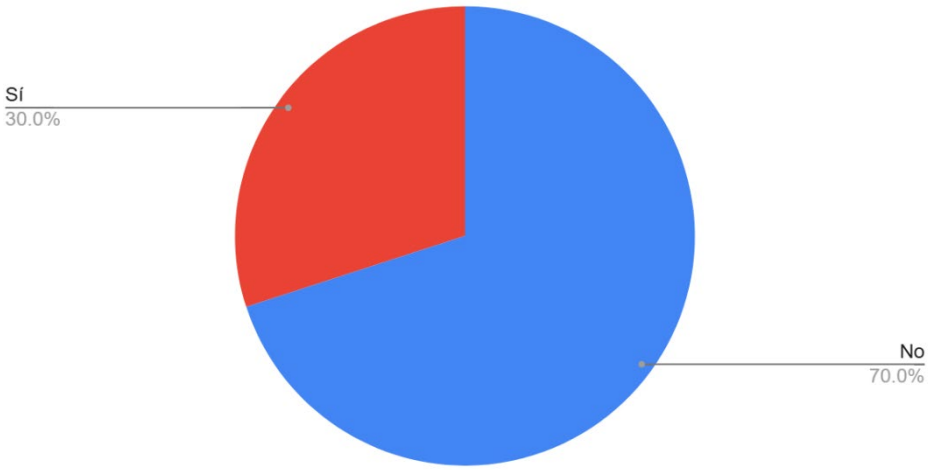


Figura 2. Capacitación sobre seguridad

En la pregunta número 2, ¿Ha recibido alguna capacitación sobre seguridad de la información en el último año?, tenemos que 20 de 30, es decir el 70% de los encuestados no han recibido capacitación sobre seguridad de la información, este es una aspecto que se debe tener presente ya que haremos enfasí en que hay una necesidad urgente de desarrollar programas de capacitación en periodos de tiempo de 6 meses ya que hay muchos riesgos en la actualidad y más aún cuando se está usando plataformas digitales y espacios en la nube.

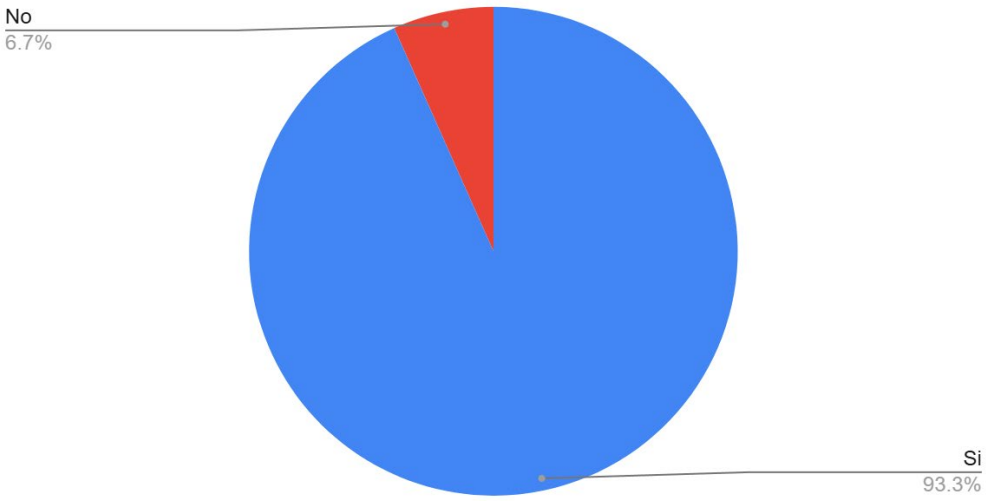


Figura 3. Uso de plataformas en la nube

En la pregunta 3, ¿Utiliza algún sistema o plataforma en la nube en su trabajo diario?, El 93,3% de los encuestados si han maneja sistemas o una plataforma en la nube, la empresa ha ido implementando el uso de tecnologias modernas, como lo es el servicio de sistemas para registrar la información y una nube propia, ya que en un inicio los datos se almacenaban en documentos físicos y grandes habitaciones que almacenaban carpetas de los pacientes. Sin embargo, al implementar estas tecnologías se debe realizar la implementación de protocolos que se rijan a entidades regulatorias y cumplan con normativas locales. Garantizando la integridad, la disponibilidad y confidencialidad de la información que se procesa.

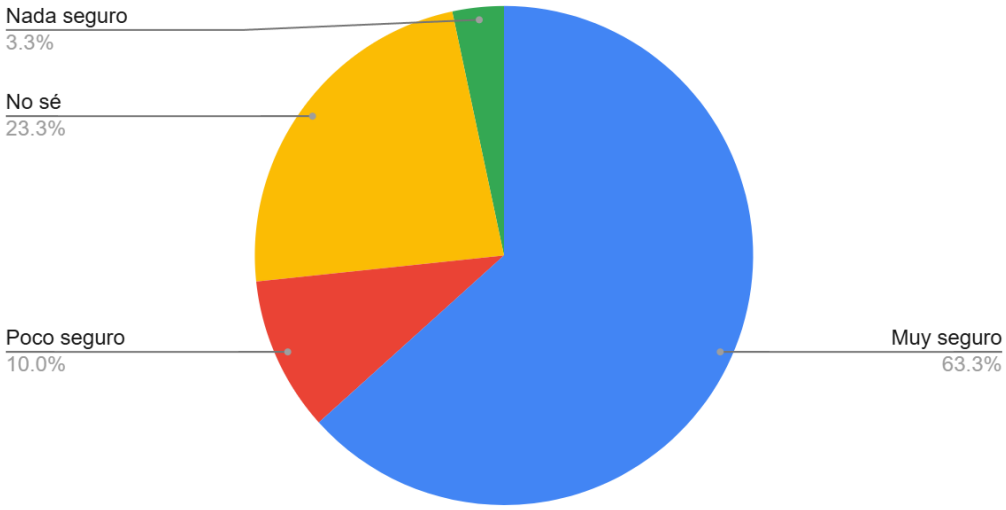


Figura 4. Nivel de confianza en la nube

En la pregunta ¿Qué tan seguro cree que es almacenar información en la nube?, esta interrogante se evidencia opiniones divididas, la mayoría de los encuestados confían en la seguridad de usar la nube para el almacenamiento de la información, sin embargo, los demás encuestados ya sea por desconocimiento técnico o por rumores que escuchan o han leído, tienen el prejuicio de que el uso de la nube es malo.

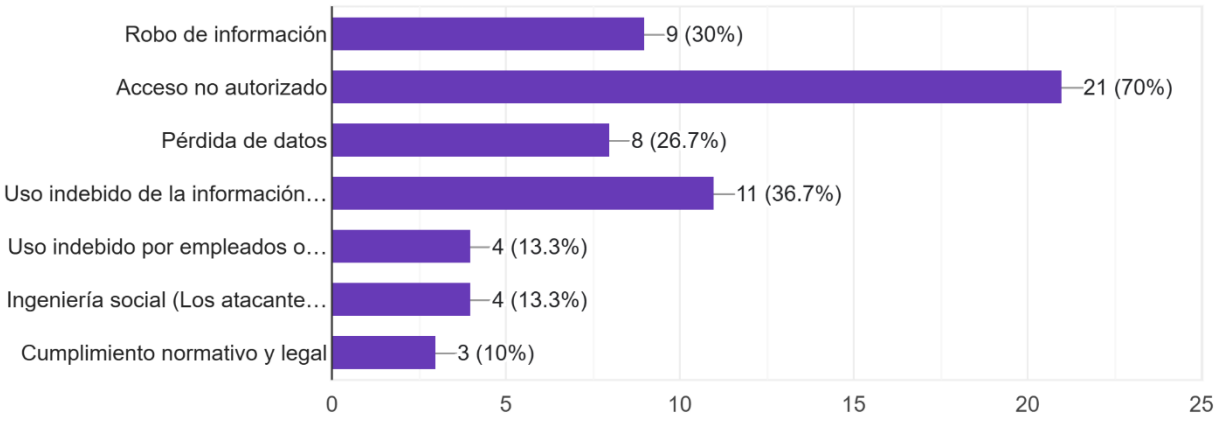


Figura 6. Riesgos de seguridad al almacenar datos

En la pregunta 5, ¿Cuáles considera que son los principales riegos de seguridad al almacenar datos en la nube?, se ve que los encuestados tienen nociones acertadas sobre los riesgos de seguridad al almacenar datos en la nube, no obstante, invita a los directivos el incentivar capacitaciones sobre los riesgos específicos y técnicos que existen al momento de manejar datos sensibles, ya que se esperaba que repunte 2 o 3 opciones y no que se repartan como se observa en la gráfica.

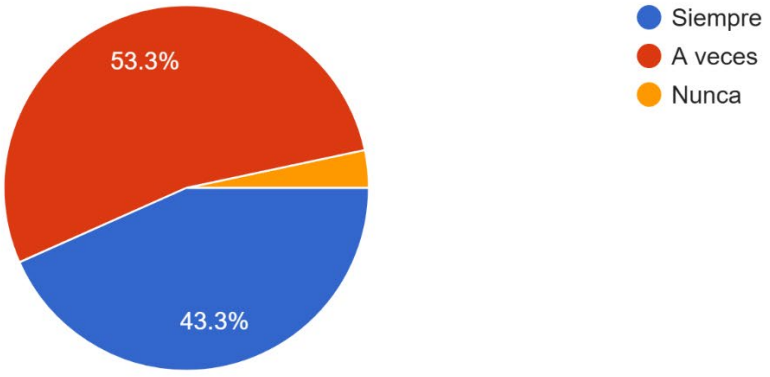


Figura 5. Contraseñas para sistema en la nube

En la pregunta 6, Cuándo crea una contraseña para un sistema en la nube, ¿qué tan seguido usa una combinación de letras, números y símbolos?, el 43,3% de los encuestados, 13 de 30, usan combinaciones de letras, números y símbolos para crear contraseñas robustas para acceder a sus sistemas de nube. Conversado con los trabajadores, comentaban que los usuarios y contraseñas eran otorgados por el departamento de TI y no podían alterar las contraseñas y un encuestado comentó que no recibió credenciales para manejar un sistema en la nube, más bien le compartieron usuario y contraseña que ya usaba un encargado del área donde desempeñaba sus actividades, el encuestado era pasante de laboratorio.

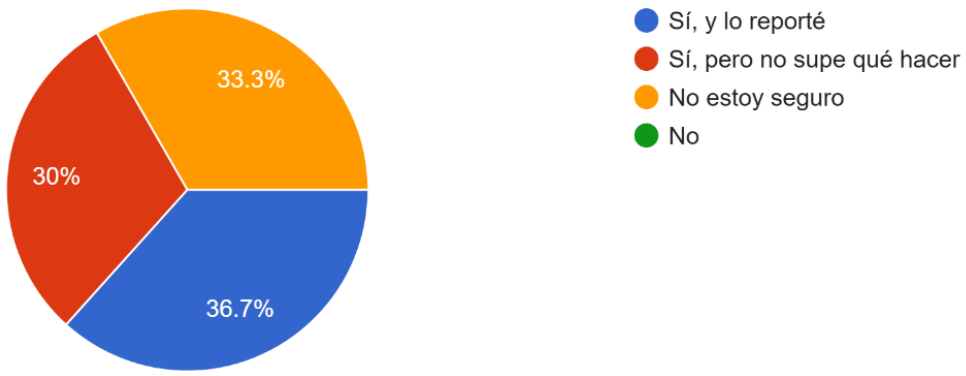


Figura 7. Nivel de phishing en Segurilab

En la pregunta 7, ¿Alguna vez ha recibido un correo electrónico sospechoso solicitando información personal o credenciales de acceso?, en esta pregunta se observa como los trabajadores han sido blanco de intentos de ciberataques como phishing, un riesgo real de ingeniería social y suplantación de identidad, algunos de los usuarios pudieron identificar estos correos y realizar la respectiva notificación para banear el usuario que intentó este ciberataque, no obstante, el 63,3% no tienen conocimiento de como identificar un ciberataque, no podían reconocer un correo real de uno engañoso que busca obtener acceso a las credenciales de los usuarios.

Encuesta a expertos

Se realizó estas preguntas a 8 expertos en el campo de la ciberseguridad y la protección de datos.

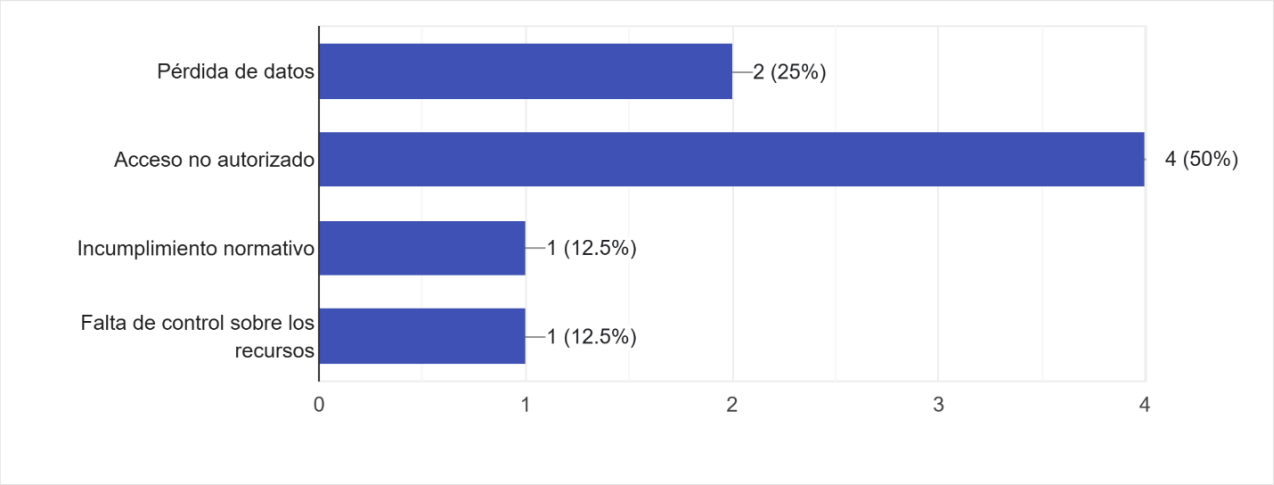


Figura 8. Riesgos de seguridad

En la primera pregunta a expertos, En su experiencia, ¿Cuál es el principal riesgo de seguridad al migrar una empresa a la nube?, el 50% de expertos opinan que el principal riesgo de seguridad al migrar las actividades de una empresa a la nube es el acceso no autorizado, es importante que se respeten los principios de seguridad de la información (CIA), como son la integridad y confidencialidad de la información.

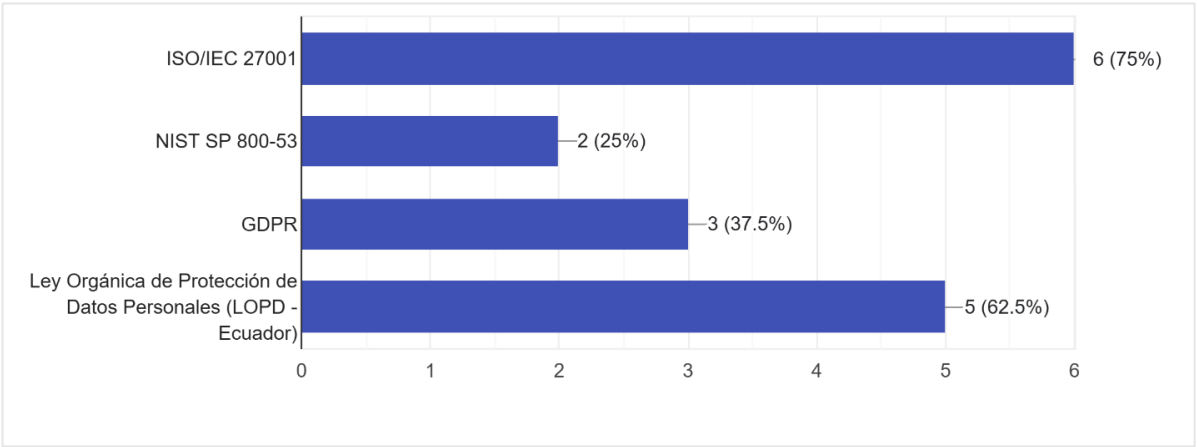


Figura 9. Normativas para aplicar

En la pregunta 2 a expertos, ¿Qué normas y marcos considera fundamentales al diseñar políticas de seguridad en la nube?, Las normativas ISO/27001 y LOPD son las más importantes que se deben tener en cuenta al momento de diseñar las politicas de seguridad en la nube. La norma ISO brinda estándares internacionales para la gestión segura de la información y la Ley Orgánica de Protección de datos ecuatoriana, que se aplica en Ecuador, que en un futuro muy cercano se va a encargar de ejecutar las respectivas notificaciones y sanciones a las empresas que no estén alineadas al cumplimiento normativo. Ambas opciones son el eje central para diseñar politicas de seguridad de datos y transición a la nube.

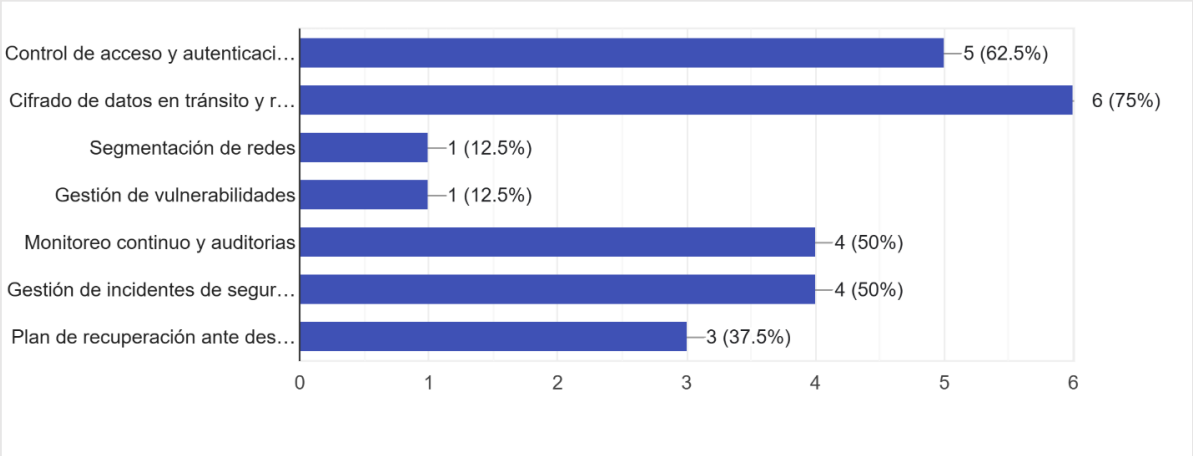


Figura 10. Controles de seguridad para el manual

En la pregunta 3 a expertos, ¿Cuáles son los 3 controles de seguridad más importantes que deberían incluirse en un manual de políticas para migración a la nube?, esta pregunta es el reflejo de que las medidas preventivas y robustas tienen relevancia para los expertos. Especifican que es importante fortalecer las defensas iniciales, como contraseñas seguras, usar medios de cifrado de la información para evitar que cualquier persona pueda acceder a datos que no tienen permiso de visualizar.

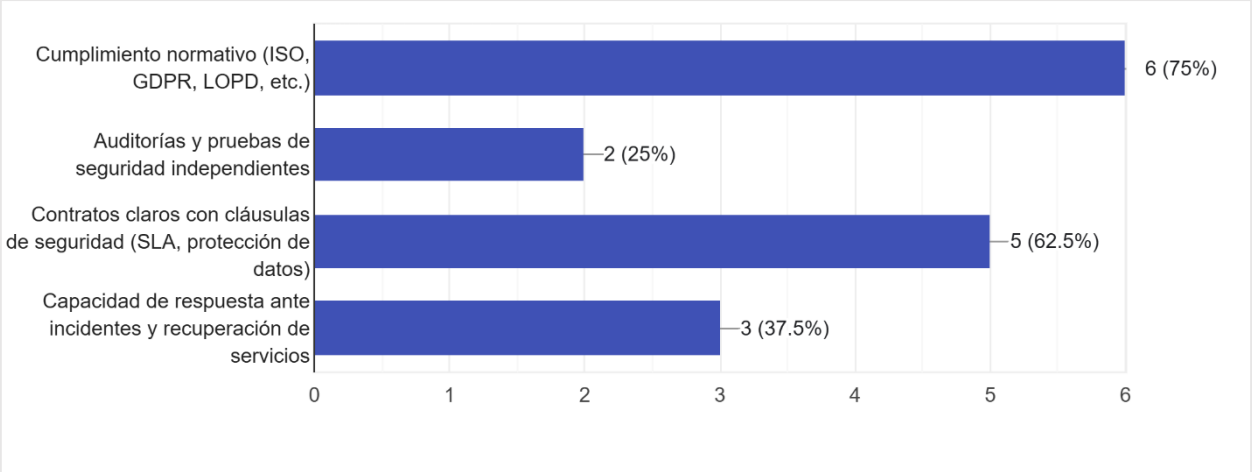


Figura 11. Servicios de un proveedor de servicio en la nube

En la pregunta 4 a expertos, Desde una perspectiva de seguridad, ¿Cuáles son los dos criterios más relevantes al momento de seleccionar un proveedor de servicios en la nube?, los expertos señalan que al momento de buscar proveedor de servicios en la nube, las acciones más importantes que se debe analizar es que sean transparentes y cumplan con las normativas de protección de datos, el facilitar los documentos necesarios para obtener toda la evidencia de las incidencias, vulnerabilidades, partes de la estructura organizacional de la empresa que han sido afectadas, en caso de ser víctimas de ciberataques es esencial para tener un buen proveedor de servicios en la nube.

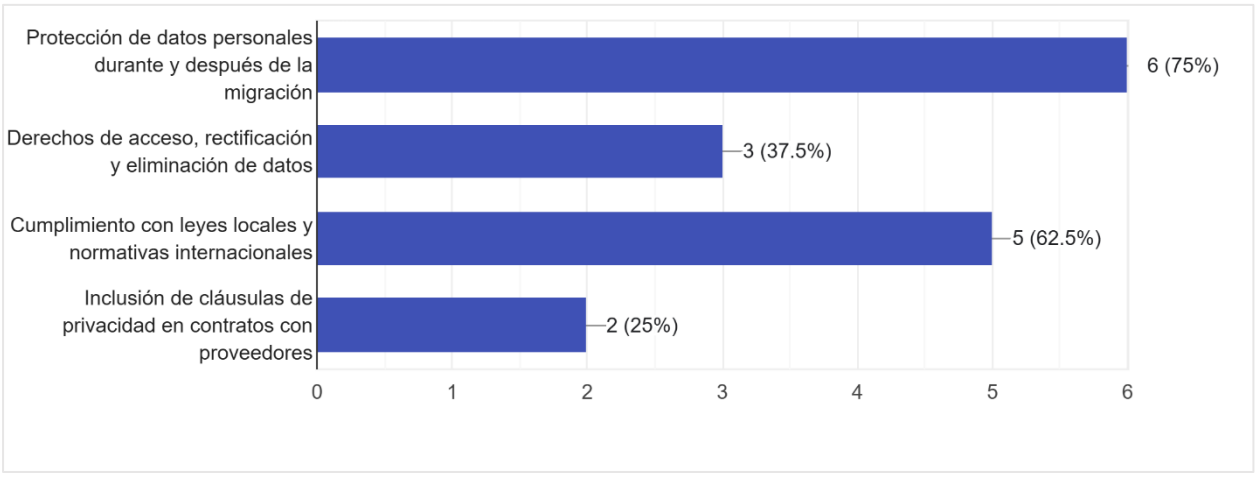


Figura 12. Consideraciones legales para una política

En la pregunta 5 a expertos, ¿Cuáles son las dos principales consideraciones legales o de privacidad que deben contemplarse en una política de seguridad para migración a la nube?, la protección de datos personales durante y después de la migración, el cumplimiento con las leyes locales y la adopción de estándares internacionales son las principales consideraciones legales y de privacidad que se deben adoptar al momento de diseñar una política de seguridad para hacer la transición a la nube. Se debe integrar las medidas técnicas y los instrumentos legales que cubran el ciclo completo de los datos, de esta manera se garantiza calidad en el tratamiento de datos, privacidad de la información e integridad de la misma.

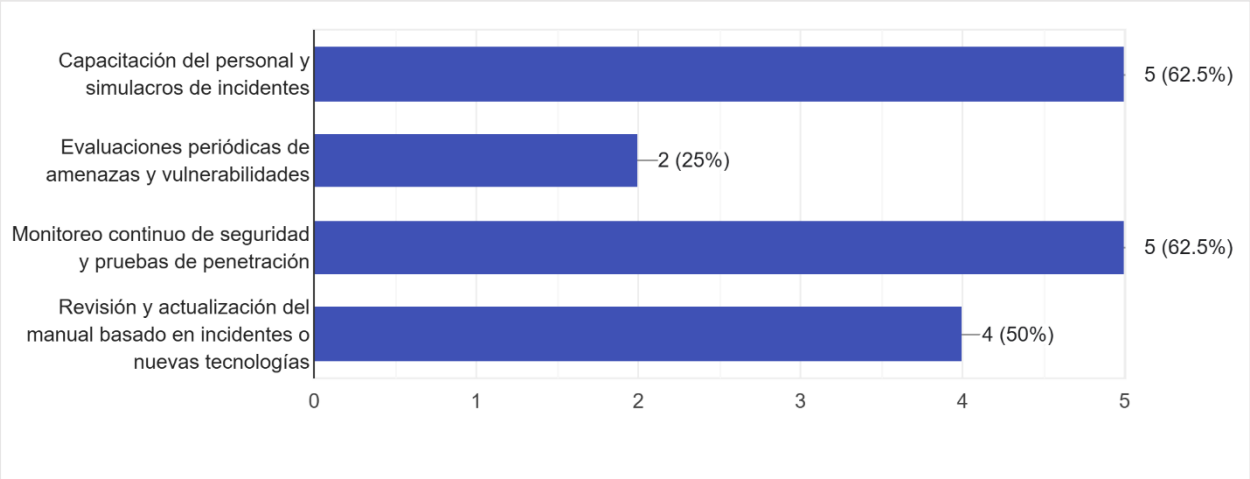


Figura 13. Acciones claves para implementación efectiva del manual

Finalmente, en la pregunta 6 a expertos, ¿Qué acciones considera claves para una implementación efectiva y mejora continua del manual de seguridad en la nube?, en esta interrogante se presenta la visión de los expertos sobre las estrategias que consideran efectivas para implementar y hacer una actualización del marco de políticas de seguridad en la nube. Se coincide en un alto porcentaje, el 62,5%, 5 expertos tienen claro que la capacitación del personal en temas de seguridad de la información, cómo se tratan los datos, cómo se almacenan, cómo se eliminan los datos una vez cumple su función es importante, además, capacitarlos para que puedan tener un tiempo de respuesta eficaz ante los incidentes que pueden producirse en la empresa con pruebas y escenarios simulados, ayudará a que los

trabajadores de Segurilab se mantengan actualizados en temas de ciberataques y plan de gestión de incidentes.

4.2. Interpretación y discusión de resultados

En resumen, los resultados de la encuesta son el reflejo de que si bien se han adoptado las nuevas tecnologías para almacenar la información sensible que se maneja en Segurilab y una parte de los encuestados tiene noción de buenas prácticas para el manejo de la información, es necesario el capacitar a todo el personal, para que pueda crear una contraseña robusta, gestionar las credenciales correctamente, tener una guía donde poder consultar buenas prácticas para el tratamiento de la información, directrices que se brindan en el marco de políticas de seguridad para la migración a la nube, con el enfoque en la protección de datos y normativas locales.

Por último, en temas de ciberataques, se observa que muchos trabajadores no están capacitados para identificar amenazas como el phishing, es necesario desarrollar un plan de respuesta ante incidentes, crear escenarios simulados de ataques para medir el tiempo de respuesta de los trabajadores, en sí, capacitar al trabajador en temas de seguridad de la información para realizar la transición de la información a servicios de la nube.

CONCLUSIONES

Se logró diseñar y evaluar las políticas de seguridad para la migración a la nube en empresas ecuatorianas, en particular, en Segurilab. El marco de políticas de seguridad se complementó con la encuesta que se realizó previamente a los trabajadores de Segurilab, así identifiqué la necesidad de fortalecer la seguridad de la información y el cumplimiento de la Ley Orgánica de Protección de datos Personales, así mismo la necesidad de implementar capacitaciones para el personal, las mismas que deben ser en periodos cortos, cada 6 meses, ya que muchos ciberataques se van perfeccionando.

Los proveedores de servicios a la nube implementan fuertes medidas de seguridad, entendemos el cifrado de la información, monitoreo continuo de la actividad que se realiza con los datos, autenticación multifactor, pero algo muy importante es el comportamiento que tiene el usuario al momento de gestionar la información y los medios para acceder a las plataformas de servicio de nube, el usar una buena contraseña, usar dispositivos que tienen un programa antivirus, no compartir las credenciales con terceros, son buenas prácticas que todo usuario que trabaja con datos debe realizar.

RECOMENDACIONES

Segurilab debe implementar el manual de políticas de seguridad propuesto y hacer una difusión masiva a todos los trabajadores que forman parte de la empresa, además, se deben establecer los tiempos de actualización y revisión del marco de políticas en base a los avances de los ciberataques o si se sufrió de un ataque y se aplicó un plan de gestión de riesgos, realizando la respectiva auditoria y revisión del caso, sin que exista un conflicto de intereses.

Toda información obtenida de las encuestas debe tratarse con la respectiva confidencialidad ya que la información que brindaron permitió realizar las mejoras de diferentes aspectos sobre la protección de datos en Segurilab y las auditorías a las que se someterán a futuro servirán para prevenir posibles incidencias que pueden comprometer los sistemas y la información que se maneja en la organización.

El ambiente laboral que Segurilab debe promulgar debe ser de carácter colaborativo ya que capacitarse en temas de seguridad y como debemos tratar la información que se maneja día a día, es algo que detectamos que se debe realizar y así pongo énfasis en mi diseño de marco de políticas.

REFERENCIAS BIBLIOGRÁFICAS

Areitio, J. (2010). *Protección de Cloud Computing en seguridad y privacidad*. Proyecto Grupo de Investigación Redes y Sistemas LEFIS-APTICE (financiado por Sócrates. European Commission). Facultad de Ingeniería, ESIDE, Universidad de Deusto. **https://www.redeweb.com/_txt/666/42.pdf**

Asamblea General de las Naciones Unidas. (2017). *Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Grupo de Trabajo IV (Comercio Electrónico), 55º período de sesiones, Nueva York, 24 a 28 de abril de 2017*.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. **https://www.asambleanacional.gob.ec/es/noticias/5325-ley-organica-de-proteccion-de-datos-personales**

Celleri-Pacheco, J., Rivas Asanza, W., Andrade-Garda, J., & Rodríguez-Yáñez, S. (2018). Análisis del uso del Cloud Computing en empresas de Ecuador. *Alternativas, 19*(2), 69–73. **https://doi.org/10.23878/alternativas.v19i2.251**

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide* (SP 800-61 Rev. 2). National Institute of Standards and Technology. **https://doi.org/10.6028/NIST.SP.800-61r2**

Erickson, J. (2023, marzo 16). What is cloud migration? Importance, benefits, & strategy. *Oracle*. **https://www.oracle.com/es/cloud/cloud-migration/**

Gobierno del Ecuador. (2024). *Acuerdo Ministerial No. 0003-2024 de la Estrategia de Gobierno Electrónico* [PDF]. **https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2024/03/Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf**

Google Cloud. (s. f.). ¿Qué es el cloud computing? *Google Cloud*. **https://cloud.google.com/learn/what-is-cloud-computing?hl=es**

International Organization for Standardization. (2011). *ISO/IEC 19011:2011 – Directrices para la auditoría de sistemas de gestión*.

Más del 80% de organizaciones de América Latina ya adoptan «cloud». (2024, enero 3). *MIT Technology Review*. **https://www.technologyreview.es/s/15955/mas-del-80-de-organizaciones-de-america-latina-ya-adoptan-cloud**

National Institute of Standards and Technology. (2010). *Contingency Planning Guide for Federal Information Systems* (SP 800-34 Rev. 1). **https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final**

National Institute of Standards and Technology. (2020). *Zero Trust Architecture* (SP 800-207). **https://doi.org/10.6028/NIST.SP.800-207**

Pérez, A., & Gómez, L. (2021). La migración a la nube y sus implicaciones en la ciberseguridad en Ecuador. *Revista de Ciberseguridad, 5*(2), 45–60. **https://doi.org/10.1234/abc5678**

Rodríguez, G. (2020). Privacidad y seguridad en la nube: Algunas implicaciones jurídico-económicas desde el comercio electrónico transfronterizo.

ANEXO A: Marco de políticas de seguridad para la migración a la nube en Segurilab, con enfoque en la protección de datos y normativas locales, Quito 2025.

Marco de políticas de seguridad para la migración a la nube en Segurilab, con enfoque en la protección de datos y normativas locales, Quito 2025.

Rafael Suntasig

ÍNDICE

1. INTRODUCCIÓN 47

2. DEFINICIONES 48

3. MARCO LEGAL Y NORMATIVO 49

4. RESPONSABILIDADES 50

I Equipo de Tecnologías de la Información (TI): 50

II Personal Administrativo y Médico: 51

III Recursos Humanos: 51

IV Gerencia: 52

5. RECOLECCIÓN Y TRATAMIENTO DE DATOS 52

Obtención de datos de pacientes 53

Tratamiento de datos 54

6. DERECHOS DE LOS TITULARES 55

7. CONSERVACIÓN DE COPIAS DE DATOS 56

Tiempo y frecuencia de las copias de seguridad 56

Almacenamiento de Copias de Seguridad 56

Tratamiento de las copias de seguridad 57

Recuperación de Datos 57

Auditorías de Seguridad 57

8. TRANSFERENCIA DE DATOS 58

Mecanismos de transferencia de datos 58

9. PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD 59

Objetivos del plan de respuesta a incidentes 59
Roles y responsabilidades 59
Fases del plan de respuesta a incidentes 60
Garantías de Transparencia y Cumplimiento Normativo 63
10. GESTIÓN DE CONTRASEÑAS 63
Parámetros de la gestión de contraseñas 63
Revocación de accesos 65
11. CONCIENCIACIÓN Y FORMACIÓN 65
12. CONTROL DE ACCESO 66
Pasos para garantizar el control de acceso 66
Prevención a accesos no autorizados 67
Dispositivos personales en Segurilab 67
Ante robo o pérdida 68
Parte legal 68
13. AUDITORÍA INTERNA 68
1. Preparación de la auditoria 68
2. Análisis documental 69
3. Ejecución de la auditoría 69
4. Evaluación y análisis de resultados 70
5. Informe 70
6. Monitoreo y seguimiento 71
REFERENCIAS BIBLIOGRÁFICAS 72

Índice de Tablas

Tabla 1. Matriz de operacionalización de variables.....24

Tabla 2.Plataformas que usa Segurilab. 64

1. **Introducción**

En Segurilab buscamos con la implementación de esta política, la gestión de la información desde que es ingresada a nuestros diferentes sistemas hasta la respuesta a posibles incidentes que pueden ver comprometida la integridad de la misma.

Esta política tiene varios enfoques que se desarrollan a continuación:

I Protección de información sensible

- Tipo de alcance: Toda la información clasificada como confidencial, privada o sensible (historia clínica y demás datos médicos) estará protegida, incluyendo datos financieros, personales de clientes, proveedores y trabajadores de la empresa.
- Beneficios: Reduce el riesgo de pérdida o robo de información, al ser víctima de ciberataques, evitando que se produzcan fugas de datos o accesos no autorizados.

II Cumplimiento de normativas legales

- Tipo de alcance: Implementando la política de seguridad de datos garantizamos que la empresa cumple con las leyes y normativas vigentes, a la Ley Orgánica de Protección de Datos Personales.
- Beneficios: Evita sanciones legales y multas por incumplimiento normativo, mejorando la reputación de la organización por demostrar responsabilidad en el manejo de datos.

III Prevención de ciberataques

- Tipo de alcance: Cubre la detección, prevención y mitigación de ataques como malware, ransomware, phishing y otras amenazas a la seguridad de los sistemas.
- Beneficios: Disminuye las interrupciones operativas y los costos asociados con la recuperación de la información por ataques a cambio de recompensas.

IV Concientización y formación del personal

- Tipo de alcance: Implica la capacitación de los empleados sobre las mejores prácticas para la gestión segura de datos y la detección de amenazas, correo con malware, intentos de robo de la información.
- Beneficios: Aumenta la capacidad de los empleados para identificar y responder a riesgos de seguridad, lo que reduce la vulnerabilidad interna.

V Gestión de acceso y control interno

- Tipo de alcance: La política establecerá controles por medio de roles y perfiles en los sistemas para limitar el acceso a la información según el cargo de cada empleado y necesidad de uso.
- Beneficios: Previene accesos no autorizados, asegura que únicamente las personas autorizadas manipulen datos críticos y garantiza la trazabilidad de las actividades dentro de los sistemas.

VI Planificación de respuestas ante incidentes

- Tipo de alcance: Desarrollar un plan de contingencia para manejar las amenazas que comprometerían los datos y su integridad.
- Beneficios: Reduce el impacto de los incidentes y acelera la recuperación, minimizando la interrupción del negocio y el daño a la reputación.

2. **Definiciones**

Acceso a la red. -Conexión a los sistemas y recursos de Segurilab mediante redes internas o externas.

Autenticación. -Proceso de verificar la identidad de los usuarios mediante credenciales seguras.

Gestión MDM. – Según IBM, (s.f.), la gestión de dispositivos móviles (MDM) es un conjunto de herramientas y una metodología probada que se utilizan

para proporcionar herramientas y aplicaciones de gran productividad para los dispositivos móviles de los empleados, a la vez que se garantiza la seguridad de los datos corporativos

Incidente. - Evento que compromete la confidencialidad, integridad o disponibilidad de la información de una empresa. Estos incidentes contienen malware, accesos no autorizados, fugas de información, Phishing, busca de una recompensa a cambio de la información comprometida, a través de correos engañosos se logra el acceso a equipos y bases de datos de empresas.

Información sensible. -Información que necesita protegerse de la falta de disponibilidad, el acceso no autorizado, la modificación o la divulgación pública debido a posibles efectos adversos en un individuo, institución, seguridad nacional o seguridad pública.

Red de invitados. -Red separada de la corporativa, diseñada para el acceso temporal de visitantes sin acceso a los sistemas internos.

VPN. -Crea una conexión de red privada entre dispositivos a través de Internet. Las VPN se utilizan para transmitir datos de forma segura y anónima a través de redes públicas.

3. **Marco Legal y Normativo**

Segurilab, en el presente documento, establece su compromiso con el cumplimiento de las normativas relevantes para la protección de datos personales, asegurando la seguridad, confidencialidad e integridad de la información. Las normativas aplicables son;

- **La Ley Orgánica de Protección de Datos Personales:** La LOPD regula la recolección, almacenamiento, tratamiento y transferencia de datos personales en Ecuador, garantizando los derechos de los titulares sobre su información. Los principios

clave de la ley incluyen la protección de la privacidad, la seguridad en el tratamiento de datos y la transparencia en la gestión de la información personal.

- **Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)**: La ley asegura que los titulares puedan acceder a sus datos personales, corregir errores, eliminar información en casos específicos y oponerse al tratamiento de sus datos.
- **Reglamento General de Protección de Datos (GDPR):** Esta normativa europea establece estándares internacionales para la protección de datos personales, que incluyen la obligación de obtener el consentimiento explícito para el tratamiento de datos, la protección de datos desde el diseño y la evaluación de impacto en la privacidad.
- **Normas ISO 27001:** La norma ISO 27001 ofrece un marco de referencia para la gestión de seguridad de la información, que incluye la protección adecuada de los datos personales almacenados y tratados dentro de la organización. En el contexto de protección de datos, sugiere medidas para garantizar la confidencialidad, integridad y disponibilidad de la información.

4. **Responsabilidades**

La seguridad de la información en Segurilab depende de la participación y el compromiso de todos los niveles que tiene Segurilab. Esta parte de la política asigna roles y responsabilidades claras para garantizar la correcta implementación, cumplimiento y mejora continua de las medidas de seguridad que se establecieron en esta política.

I **Equipo de Tecnologías de la Información (TI):**

Responsabilidades:

- Mantenimiento y gestión de usuarios y contraseñas para las plataformas Labint, MedEsp e Inthelo, así como la plataforma en la nube.

- Realización de copias de seguridad diarias de servidores y auditorías para garantizar la integridad de los datos.
- Evaluación de riesgos y revisiones internas para identificar amenazas y vulnerabilidades en la infraestructura tecnológica.

Roles:

- Encargado de la gestión y mantenimiento de las plataformas y sistemas.
- Responsable de evaluar y mitigar riesgos, así como de realizar revisiones internas y auditorías de seguridad.

II **Personal Administrativo y Médico:**

Responsabilidades:

- Cumplimiento de las políticas y procedimientos de seguridad de la información en el manejo diario de datos médicos y administrativos.
- Colaboración en la capacitación continua sobre buenas prácticas de seguridad.
- Reporte inmediato de cualquier incidente de seguridad identificado.

Roles:

- Acceso y manipulación de datos conforme a las políticas establecidas.
- Responsable del manejo seguro de datos clínicos y de la concientización sobre la importancia de la seguridad de la información.

III **Recursos Humanos:**

Responsabilidades:

- Garantizar que los empleados reciban la capacitación inicial y continua en seguridad de la información.

- Coordinar la implementación de medidas correctivas en caso de incidentes relacionados con la seguridad de la información.

Roles:

- Encargado de coordinar la capacitación del personal y de actuar como enlace entre el personal y el equipo de TI en temas de seguridad.

IV **Gerencia:**

Responsabilidades:

- Aprobar y respaldar la implementación de políticas y medidas de seguridad.
- Proporcionar el apoyo necesario para garantizar el cumplimiento de la normativa y la mejora continua en seguridad.

Roles:

- Líder responsable de respaldar y promover la cultura de seguridad de la información dentro de Segurilab.

Estas responsabilidades y roles establecen una clara división de tareas y compromisos para asegurar que la seguridad de la información sea una prioridad en todos los niveles de la organización. La colaboración efectiva entre los diferentes actores es esencial para el éxito de la implementación y mantenimiento de esta política.

5. **Recolección y Tratamiento de Datos**

Segurilab, se compromete a cumplir con la Ley Orgánica de Protección de Datos Personales(LOPD) para garantizar la privacidad y seguridad de la información de los pacientes y trabajadores.

1. **Recolección y clasificación de datos:**

Segurilab obtiene el consentimiento explícito de los pacientes y empleados antes de recolectar cualquier tipo de información. Posteriormente, la información se clasifica según su nivel de sensibilidad, en cumplimiento con lo establecido en la LOPD, para su adecuado tratamiento.

2. **Conservación y eliminación de datos:**

Segurilab conservará los datos personales por períodos específicos, según el tipo de dato, en cumplimiento con las normativas nacionales pertinentes, como la LOPD, la Ley de la Salud, el Código tributario Ecuatoriano y el Código del Trabajo. Los tiempos de conservación son los siguientes:

- Datos clínicos: se conservarán durante 10 años (MSP, s.f.), desde la última interacción con el paciente. En pacientes menores de edad, se deben almacenar hasta 10 años después de alcanzar la mayoría de edad.
- Datos administrativos y contables: Se conservarán durante 7 años, en cumplimiento con la normativa tributaria ecuatoriana.
- Datos laborales: Se almacenarán durante 5 años después del término de la relación laboral.

Una vez cumplido los tiempos fijados, los datos serán eliminados de manera segura haciendo uso de métodos de borrado irreversible y la respectiva destrucción física en caso de conservar documentos físicos, garantizando la confidencialidad y la protección de los datos durante la fase de eliminación.

Obtención de datos de pacientes

Al ingresar a Segurilab, los pacientes deben registrar sus datos personales en un formulario llamado **Acta de recepción de pacientes**, que confirma su asistencia. Los datos se ingresan al sistema Labint, y se puede solicitar información adicional según el perfil requerido,

como antecedentes familiares, hábitos de vida, enfermedades, y otros datos necesarios para la historia clínica.

A medida que el paciente interactúa con los diferentes servicios de Segurilab, deberá proporcionar la información adicional necesaria para asegurar un servicio óptimo. Es responsabilidad del paciente proporcionar información veraz y completa. La recolección de datos se puede realizar, desde las llamadas telefónicas, correos electrónicos, mensajes de texto, WhatsApp, redes sociales y otros canales. También se puede recopilar información de ubicación para servicios a domicilio con el consentimiento del paciente.

Desde el departamento de contabilidad, se solicita información para el cobro y facturación, conservando la información de manera confidencial.

Con las actividades que realiza Segurilab, se recopila datos clínicos de los pacientes, incluyendo diagnósticos, antecedentes médicos, hábitos, resultados de laboratorio, procedimientos médicos, vacunas, entre otros.

Tratamiento de datos

Segurilab utiliza la información recopilada de los pacientes únicamente para los fines establecidos, garantizando que el tratamiento de datos se realiza conforme a la ley y los principios de transparencia, seguridad y confidencialidad.

La información recolectada se utilizará de la siguiente manera:

- Proporcionar los resultados en línea a los usuarios a través de las plataformas Labint y Nube.
- Evaluar la elegibilidad de los usuarios para ciertas ofertas, productos o servicios;
- Evaluar las ofertas, productos y servicios que pueden ser de interés para los usuarios.
- Proporcionar soporte a los usuarios.

- Comunicar y brindar información adicional que pueda interesarle sobre Segurilab, tales como noticias, ofertas especiales, anuncios y materiales de marketing de Segurilab y nuestros socios comerciales.
- Enviar recordatorios, avisos técnicos, actualizaciones, alertas de seguridad y boletines de servicio de soporte y mensajes administrativos o de marketing.
- Proporcionarle publicidad a través de los servicios, mensajes de correo electrónico, mensajes de WhatsApp y otros métodos de comunicación;
- Administrar encuestas, sorteos, concursos u otras actividades promocionales patrocinadas por Segurilab o sus socios.

6. **Derechos de los Titulares**

Los clientes, pacientes y empleados de Segurilab tienen derechos sobre la información que proporcionan, los cuales pueden ejercer de acuerdo con la Ley Orgánica de Protección de Datos Personales. Los artículos que respaldan estos derechos son:

Art. 12.-Derecho a la información.

Art. 13.- Derecho de acceso.

Art 14.- Derecho a rectificación y actualización.

Art 15.- Derecho de eliminación.

Art 16.- Derecho de oposición.

Art. 17.- Derecho a la portabilidad.

Art 19.- Derecho a la suspensión del tratamiento.

Art 20.- Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.

Los titulares pueden ejercer sus derechos presentando una solicitud escrita a través de los canales de Segurilab, correo, formulario en línea o por escrito en las

instalaciones. Se procesará la solicitud respetando la confidencialidad y seguridad de la información proporcionada.

7. **Conservación de Copias de datos**

Esta sección tiene como objetivo el garantizar que los datos personales y sensibles que se manejan en Segurilab están protegidos mediante el uso de copias de seguridad y procesos de recuperación eficaces. Al trabajar con información sensible de los clientes y trabajadores, Segurilab, asegura que toda información manejada cumple con la LOPD, y con otras normativas relevantes relacionadas con la seguridad y privacidad de los datos, garantizando la integridad, disponibilidad y confidencialidad de los datos.

Tiempo y frecuencia de las copias de seguridad

Estas copias deberán realizarse automáticamente, con el respaldo de una configuración por parte del departamento de análisis de sistemas en cada equipo de Segurilab.

- Copias diarias: Las copias de los datos críticos que Segurilab maneja, información de los clientes e historias clínicas que van ingresando día a día al sistema, respetando las regulaciones que exigen conservar información de salud un periodo de 5 a 10 años, después de la última atención médica.
- Mensuales: Las copias de la información financiera como recibos, estados financieros, contratos que se realicen, información de pacientes nuevos, entiéndase a pacientes del año actual.
- Semestral: las copias se harán de inventarios de maquinaria y equipos que están en Segurilab.

Almacenamiento de Copias de Seguridad

Se detalla las maneras en que Segurilab, garantiza la integridad, disponibilidad y confidencialidad de la información al momento de realizar copias de seguridad.

- **Almacenamiento local:** Dispositivos externos: discos duros y dispositivos NAS permitiendo crear réplicas de los sistemas que se manejan en Segurilab(Labint, Intelho, Mdesp, Segurilearn, NIGISU).
- **Almacenamiento en la nube:** Segurilab, cuenta con su propia nube donde guardan su información fuera del sitio físico, protegiendo los datos contra desastres como incendios, terremotos, inundaciones.

Tratamiento de las copias de seguridad

Las copias de seguridad serán tratadas con el mayor nivel de protección:

- **Cifrado de las copias**: Las copias de seguridad se cifrarán para garantizar que los datos sean ilegibles en caso de que sean accesos sin autorización.
- **Accesos restringidos**: El acceso a las copias de seguridad estará limitado a personal autorizado, y se utilizarán contraseñas seguras, junto con autenticación multifactorial, para proteger el acceso a los datos.

Recuperación de Datos

Segurilab tiene un proceso formal de recuperación de datos que se lleva a cabo tras cualquier incidente o desastre. Se realizarán pruebas periódicas de recuperación para garantizar que los datos puedan ser restaurados de manera eficiente y en el menor tiempo posible.

Auditorías de Seguridad

Segurilab llevará a cabo auditorías de seguridad regulares para verificar que las copias de seguridad y los procedimientos de recuperación estén funcionando correctamente y sean efectivos.

8. **Transferencia de Datos**

Segurilab establece las condiciones bajo las cuales podrá transferir los datos personales de clientes, pacientes y trabajadores, dando las garantías que dicho proceso se realizará cumpliendo con la Ley Orgánica de Protección de Datos Personales(LOPD). Las condiciones para la transferencia de datos son las siguientes:

- Cuando la ley lo exija: cuando las normativas lo exijan, como la LOPD, la Ley de la Salud, el Código tributario Ecuatoriano, entre otras normas legales.
- Con la autorización expresa del titular: Segurilab solicitará el consentimiento del titular en caso de requerir la autorización, para proceder con la transferencia a terceros.
- Para salvaguardar la salud e integridad de los titulares: en situaciones donde se requiera la divulgación de la información de manera urgente para proteger la salud y bienestar de los pacientes o trabajadores.

Mecanismos de transferencia de datos

La transferencia de datos personales se llevará a cabo de acuerdo con los siguientes principios y procedimientos:

- **Contratos de Confidencialidad:** Toda transferencia de datos a terceros se realizará mediante contratos de confidencialidad que garanticen el cumplimiento de las normativas de protección de datos y la seguridad de la información. Estos contratos serán obligatorios, tanto para los empleados internos como para los terceros con quienes se compartan los datos.
- **Seguridad en la Transferencia:** Las transferencias de datos se realizarán por medios seguros, como conexiones cifradas (SSL/TLS) y protocolos de comunicación protegidos, para evitar que la información sea interceptada por terceros no autorizados durante su transmisión, respetando los derechos de los titulares.

- **Transferencias Internacionales:** En caso de que los datos sean transferidos a filiales, subsidiarias o socios comerciales fuera de Ecuador, se garantizará que dichas transferencias estén alineadas con las regulaciones de la LOPD.

9. **Plan de respuesta a incidentes de Seguridad**

Segurilab, al manejar información sensible, está expuesta a diversos tipos de amenazas cibernéticas, tales como ataques de malware, ransomware, accesos no autorizados, phishing y filtraciones de datos. Estos riesgos pueden comprometer la integridad, disponibilidad y confidencialidad de la información que se procesa. Se establecen los procesos que Segurilab ejecutará para este tipo de incidentes de seguridad, logrando reducir el impacto y restableciendo las operaciones/funciones que desempeña día a día.

Objetivos del plan de respuesta a incidentes

Los objetivos del plan de respuesta a incidentes serán:

- Detectar y clasificar proactivamente los incidentes de seguridad que intentan acceder a los sistemas de Segurilab.
- Contener, mitigar y erradicar la amenaza y el daño causado por el incidente.
- Recuperar los sistemas comprometidos en el incidente.
- Notificar a las autoridades de Segurilab, clientes, trabajadores, cómo fue el incidente, si se ha visto comprometida la información y como se ha logrado mitigar el daño que ha causado dicho incidente.

Roles y responsabilidades

Equipo de respuesta a incidentes: Son los encargados de coordinar la respuesta ante incidentes de seguridad y de ejecutar las acciones necesarias para mitigar los daños. El departamento de análisis de sistemas administrará los sistemas y servidores, haciendo su

respectivo monitoreo y control de incidencias, además que tendrá el control de las credenciales de los servidores

Ingeniero de redes: Gestiona y da seguridad a la infraestructura de las redes de la compañía.

Analista de datos: Será el responsable de toma de decisiones importantes, si se debe avisar a la **Superintendencia de Protección de Datos,** como lo indica **LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES**

Departamento legal: Se encargará de verificar que se esté realizando el cumplimiento que exige la ley y emitirá las notificaciones legales de acuerdo con la incidencia y su alcance, jefes, clientes, trabajadores.

Soporte técnico: Dará asistencia mientras se está resolviendo la incidencia, restaurando sistemas y datos dependiendo de la necesidad de los trabajadores de la empresa.

Analista de riesgos: Evaluará el impacto potencial del incidente en la empresa y ayuda asignando la prioridad que tiene el proteger elementos Segurilab.

Área de capacitación: Desarrollará prácticas de capacitación para el personal de Segurilab para prevenir incidentes y tener un plan de acción en caso de sufrir ataques.

Fases del plan de respuesta a incidentes

1. Preparación

- Capacitar al personal de Segurilab sobre las políticas de seguridad y realizar simulacros de incidentes midiendo tiempo de respuesta y cómo actúa el personal ante los diferentes incidentes.
- Contar con herramientas que permitan la detección, monitoreo y notificación de los incidentes de seguridad.
- Políticas definidas, identificar los activos de Segurilab, los diferentes datos que se manejan y quien tiene acceso a la información.

2. Detección y análisis

- Uso de firewalls y análisis de registros para detectar comportamientos fuera de lo común en las redes de Segurilab.
- Detectar, clasificar y notificar el incidente (NIST, 2012) y qué índice de gravedad tiene, siendo bajo, medio o crítico.
- Registrar detalles del incidente, incluir cuándo y cómo se detectó, que equipos afectó y su clasificación de ataque.

3. Contención

- Aislar los equipos afectados, con el objetivo de evitar que se propague el incidente que se produjo.
    - Contención a corto plazo: desconectar equipos afectados o bloquear direcciones IP sospechosas.
    - Contención a largo plazo: Cambios de configuración y emplear el uso de parches de seguridad.

4. Erradicación

- Eliminar la amenaza: limpiando los sistemas del malware y cerrar las brechas de seguridad que permitieron que se dé el ataque.
- Identificar cómo ocurrió el ataque y realizar las pertinentes correcciones para evitar que se vuelva a producir el mismo ataque.
- Aplicar parches a las vulnerabilidades detectas y realizar las respectivas actualizaciones de los sistemas que se vieron comprometidos en el ataque.

5. Recuperación

- Reiniciar y restaurar los equipos comprometidos a partir de las respectivas copias de respaldo que se debieron realizar en periodos cortos antes del ataque.
- Comprobar que los equipos afectados están funcionales en su totalidad.

- Realizar revisiones en periodos cortos, a los equipos afectados.

6. Notificación y comunicación

   Interna: Se informará al personal de Segurilab sobre la situación vivida y los pasos que se siguieron para corregir la incidencia que se produjo.

   Externa: Se notificará a los clientes y autoridades, dando transparencia del ataque se vivió, el alcance que logró y si la información se vio comprometida.

7. Retroalimentación

   Se harán las revisiones del incidente vivido, con los departamentos implicados; Equipo de respuesta a incidentes, ingeniero de redes, gerencia del área de tecnología, analista de riesgos, para evaluar la gestión que se realizó al momento que se produjo la incidencia y mejorar el proceso ante futuros incidentes que se puedan dar. Además, se evaluará si las políticas de seguridad se deben actualizar. Y con el área de capacitación, crear simulaciones de incidentes para hacer reuniones con el personal y darles habilidades para saber actuar ante posibles incidentes-

8. Cumplimiento normativo

   Ley Orgánica de Protección de Datos Personales de Ecuador (LOPDPE):

- Segurilab cumple con las disposiciones de esta ley, que regula el tratamiento de los datos personales, particularmente en lo que respecta a la confidencialidad y el derecho a la protección de los datos de los pacientes.
- En caso de que un incidente que comprometa datos personales, Segurilab está obligada a notificar a la **Superintendencia de Protección de Datos** y a los individuos afectados dentro de los plazos establecidos en la ley, como lo establece el artículo 43 de **LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES** .

Garantías de Transparencia y Cumplimiento Normativo

Segurilab garantiza la transparencia en el manejo de incidentes de seguridad que afecten a los datos personales que gestiona. En caso de una violación de datos personales, el responsable del tratamiento de datos es el encargado de notificar a la autoridad de protección de datos dentro de los plazos establecidos por la Ley Orgánica de Protección de Datos Personales (LOPD), que estipula un plazo de 72 horas para realizar dicha notificación. En caso de que el riesgo para los datos comprometidos sea alto, Segurilab también notificará a los individuos afectados. Si no se cumple con el plazo de 72 horas, Segurilab deberá justificar la demora.

10. **Gestión de Contraseñas**

Segurilab, como empresa comprometida en ser líder en salud a nivel nacional, busca cumplir con los principios fundamentales en el manejo de la información que sus clientes proporcionan a nuestro personal altamente capacitado: confidencialidad, integridad, disponibilidad. Se establecen los lineamientos que todos los empleados de Segurilab deberán seguir para garantizar el acceso seguro a los sistemas que manejan información sensible. Se protegerán los datos de los clientes, pacientes y trabajadores haciendo uso de contraseñas robustas y procedimientos de seguridad avanzados.

Parámetros de la gestión de contraseñas

1. El enrolamiento del personal a la plantilla de Segurilab se realizará en su oficina matriz y se manejará de la siguiente manera para el correo electrónico:
   - El departamento de análisis de sistemas recopilará información del trabajador, para proceder con la generación de su usuario y contraseña del correo institucional.

- Al generarse usuario y contraseña institucional, se proporcionará un usuario definitivo y una contraseña temporal, que deberá ser modificada por el trabajador y de ser necesario hacer la implementación de verificación de 2 o más pasos.

Para las demás plataformas que usa Segurilab, el proceso será el siguiente: **Sistemas de Segurilab**

Tabla 2.Plataformas que usa Segurilab.

Sistema de Segurilab	Descripción	Descripción	Personal Autorizado
LABINT	Sistema de ingreso, validación, facturación y emisión de resultados	Acceso restringido precisa de usuario y contraseña	Recepcionista, médicos, contables, asesores comerciales y analistas de laboratorio
MEDESP	Sistema de agendamiento de citas médicas, citas en laboratorio clínico e imagen	Acceso restringido precisa de usuario y contraseña	Clientes y empresas
SEGURICLOUD	Sistema de almacenamiento masivo en línea	Acceso restringido precisa de usuario y contraseña	Se dan accesos a ciertos colaboradores
INTELHO	Sistema de historias clínicas	Acceso restringido precisa de usuario y contraseña	Acceso a los médicos, jefes y análisis de datos
NIGISU	Sistema contable	Acceso restringido sólo personal de contabilidad con usuario y contraseña	Acceso para el departamento de contabilidad, gerencia en caso de precisar.

2. Requisitos de contraseñas:

Las características que deberán tener las contraseñas serán:

- El uso de contraseñas iguales o superiores a 12 caracteres.
- Incluir letras mayúsculas y minúsculas, números y caracteres especiales.
- Hacer uso de contraseñas únicas para cada sistema que maneja Segurilab
- Así mismo, se debe incluir autenticación de dos o más pasos de acuerdo con el tipo de información o sistema de Segurilab que se quiere obtener acceso.
- Hacer uso de gestor de contraseñas personal, que permitirá generar contraseñas seguras y tener una base de datos en el equipo permitiendo usar una clave maestra, dándole facilidad de manejo de credenciales al trabajador.

- Además, para dar más garantías de que el acceso a los sistemas que maneja Segurilab, se realizarán actualizaciones de contraseñas cada cierto tiempo, tiempo recomendado no más de 6 a 12 meses.

Revocación de accesos

De manera inmediata el departamento de análisis de sistemas retirará el acceso a los sistemas a las credenciales de los trabajadores que dejen de ser parte de Segurilab.

11. **Concienciación y Formación**

Al capacitar a los trabajadores sobre cómo se debe manejar la información, como realizar reportes de acuerdo con las políticas que se han descrito en el presente documento, permite tener una respuesta más rápida evitando que se produzcan ataques o teniendo la información del tipo de ataque que se intenta apropiar de los datos de Segurilab, para ejecutar el plan de acción ante incidentes.

Las capacitaciones enfocadas en las amenazas que representan los ataques de Phishing, Ransomware, malware, ataques que buscan aprovecharse y obtener acceso a las bases de datos de Segurilab. Con estas capacitaciones el personal crea un sentido de pertenencia donde se toma en cuenta los aportes que se recogen en la capacitación, ya que se da diferentes ideas sobre como identificar y cómo actuar ante el ataque. Con estas capacitaciones fomentaremos que la protección de la información es una responsabilidad compartida entre todos los miembros de Segurilab.

Será importante incluir diversos materiales de apoyo para las capacitaciones, desde; presentaciones, encuestas, carteles. Además, para darle más importancia a las capacitaciones, el dar reconocimientos y recompensas incentiva a la buena práctica del cuidado de los datos.

12. **Control de Acceso**

Esta sección de la política establece las directrices para gestionar el acceso a la red de Segurilab, garantizando la seguridad y confidencialidad de los datos de sus clientes, pacientes y trabajadores.

Pasos para garantizar el control de acceso

- El personal de análisis de sistemas será responsable de controlar el acceso a la red de Segurilab.
- Los métodos de autenticación incluirán contraseñas o credenciales institucionales (usuario y contraseña), siguiendo las directrices especificadas para la generación de contraseñas, que están explicadas en el punto ***"10. Gestión de contraseñas"***
- De acuerdo con el rol que cumple el trabajador de Segurilab, se le dará acceso a una red, para que pueda desempeñar sus funciones.
- La red será fragmentada en subredes, teniendo diferenciadas las redes para cada departamento que trabaja en Segurilab.
- Los dispositivos que se conecten a la red Wi-Fi de Segurilab, serán verificados por el departamento de análisis de sistemas(o bien se deberán conectar obligatoriamente a la red de invitados)
- Redes sociales, Facebook, YouTube, WhatsApp, entre otra, su acceso será restringido, a excepción de departamentos que requieran de su acceso para su funcionamiento, departamento de Marketing.
- Se asignará una red de invitados para personal externo, incluyendo pacientes y proveedores.
- Hacer uso de VPN, para acceder a los sistemas de Segurilab de manera externa, de esta manera se da garantía de protección de la información y que únicamente la persona autorizada accederá a la información.

Prevención a accesos no autorizados

- Las redes serán monitoreadas continuamente para identificar posibles accesos no autorizados o intento de acciones sospechosas.
- Todo intento de acceso no autorizado será identificado y reportado para analizarse en el departamento de análisis de sistemas.
- El personal de Segurilab, será capacitado sobre cómo hacer un reporte de incidencias en la red.

Dispositivos personales en Segurilab

En esta sección se indica la manera correcta del uso de dispositivos personales por parte de los trabajadores de Segurilab. Se busca proteger los datos y sistemas de Segurilab mientras se da una flexibilidad de trabajar.

Procesos para usar dispositivos personales

- Se hará un listado de los dispositivos que se pueden usar en Segurilab.
- Definir los requisitos mínimos que deben tener los dispositivos, ya que deben soportar las herramientas de seguridad su instalación y funcionamiento.
- Se hará uso de software de gestión móvil (MDM) para gestionar los datos remotamente en caso de pérdida o robo del dispositivo del trabajador de Segurilab.
- Usar bloqueo del dispositivo personal con clave o patrón de desbloqueo, para acceder con usuario y contraseña a los sistemas de Segurilab.
- Mantener actualizado el dispositivo con las versiones más recientes, así se evitará errores de software.
- Cumplir con las políticas propuestas en este documento para evitar que se creen brechas de acceso y se produzca un ciberataque, donde se ubicará la información en el dispositivo, cómo se procederá con el almacenamiento de los datos y si está permitido o no el uso de dispositivos de almacenamiento externo.

Ante robo o pérdida

Se debe notificar inmediatamente a la empresa si su víctima de robo del dispositivo. Así mismo, el departamento de análisis de sistemas procederá con el bloqueo al acceso del dispositivo y el bloqueo de la información de la empresa que ese dispositivo recibe, esto gracias al software de gestión móvil.

Parte legal

Aunque la empresa haga un monitoreo del dispositivo por razones estrictamente de seguridad, no se va a tener acceso a datos personales del trabajador, inclúyase fotos, correos, personales, contactos, etc. El monitoreo se regirá a Ley de Protección de Datos.

Dar garantía desde la parte legal que el trabajador de Segurilab es consciente de las penalidades legales que implica el usar la información de la empresa y los sanciones que puede sufrir Segurilab si se llega a filtrar cualquier tipo de dato.

13. **Auditoría interna**

Para evaluar cómo ha sido la implementación y cumplimiento de las políticas de seguridad de datos. Se detalla el proceso de auditoría interna que se seguirá en Segurilab:

1. **Preparación de la auditoria**

   Definir un objetivo: Evaluar el cumplimiento de las políticas de seguridad de datos, identificando los riesgos y evaluar la efectividad de las medidas de seguridad que se han implementado cada 6 meses.

   Definir el alcance que se le dará:

   - Desde la recolección y tratamiento de datos personales.
   - Manejo de la Ley Orgánica de Protección de datos personales.
   - Gestión de las contraseñas que se usan para los sistemas de Segurilab.
   - Control de acceso a la red y dispositivos personales.
   - Copias de seguridad y recuperación.

- Plan de respuesta a incidentes.

Equipo auditor: Evitar conflictos de interés con el personal encargado de realizar la auditoría interna, eso si deben tener conocimiento en ciberseguridad y normativa aplicable.

2. **Análisis documental**

   El equipo que implementó las políticas y procedimientos que se han implementado en Segurilab proporcionaran toda la documentación para la auditoria:

   - Política de seguridad de datos.
   - Política de gestión de contraseñas en Segurilab.
   - Procedimientos para la obtención de datos y buenas prácticas.
   - Plan de respuesta a incidentes.
   - Registros de capacitaciones al personal de Segurilab.
   - Auditorias anteriores registradas, si existen.

3. **Ejecución de la auditoría**

   - Entrevistas/Encuestas

     Realizar encuestas al personal de Segurilab que sean afines al área que se está auditando, serán anónimas y servirán para evaluar el funcionamiento.

   - Revisión técnica
     - Revisar los registros de control de acceso para verificar el cumplimiento de las políticas.
     - Analizar la complejidad de las contraseñas que se usan en Segurilab para el acceso a los sistemas.
     - Verificar los tiempos de las copias de seguridad y cómo se gestiona su almacenamiento.

- Estudiar los documentos de incidentes y las acciones ejecutadas para la mitigación del incidente.

Finalizando la parte técnica de ser posible se debe realizar pruebas de seguridad, haciendo uso de software para el análisis de vulnerabilidades, revisión del firewall implementado en Segurilab.

4. **Evaluación y análisis de resultados**
    - Comparar los resultados obtenidos durante la auditoria con los puntos que se han establecido para ejecutar en el trabajo día a día que se realiza en Segurilab e identificar en qué áreas de Segurilab no se están cumpliendo y se debería mejorar la ejecución de las políticas.
    - Proponer mejoras de acuerdo con los resultados, desde más reglas en el firewall usado, mejora en las contraseñas que se están usando para el manejo de sistemas, implementar autentificación en 2 o más pasos.
    - Reformular puntos de la política o hacer la implementación de nuevos parámetros en caso de detectar nuevos riesgos en las áreas de trabajo de Segurilab.

5. **Informe**

Se muestra un ejemplo de la estructura del informe:

1. Introducción
    - Definir objetivos, alcance y nombres del equipo que realizará la auditoría interna.
2. Metodología
    - Como se procederá con la auditoria.
        - Entrevistas, documentos que se revisarán.

3. Resultados
    - Cumplimiento e incumplimiento detectados.
    - Áreas de buen y mal manejo de políticas de seguridad.
4. Recomendaciones
    - Propuestas de mejora en la seguridad de los datos en Segurilab.
5. Conclusión
    - Resumen de la auditoria, con las fortalezas y debilidades encontradas en el proceso.

6. **Monitoreo y seguimiento**

Coordinar un plan de acción con el equipo de Segurilab para mejorar la gestión de la información en las áreas de trabajo detectadas que se recoge en el informe. Haciendo uso desde capacitaciones más detalladas.

Programar una revisión del plan de acción ejecutado, debe ser en un periodo más corto a la próxima auditoria.

REFERENCIAS BIBLIOGRÁFICAS

Areitio, J. (2010). *Protección de Cloud Computing en seguridad y privacidad*. Proyecto Grupo de Investigación Redes y Sistemas LEFIS-APTICE (financiado por Sócrates. European Commission). Facultad de Ingeniería, ESIDE, Universidad de Deusto. https://www.redeweb.com/_txt/666/42.pdf

Asamblea General de las Naciones Unidas. (2017). *Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Grupo de Trabajo IV (Comercio Electrónico), 55º período de sesiones, Nueva York, 24 a 28 de abril de 2017*.

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. https://www.asambleanacional.gob.ec/es/noticias/5325-ley-organica-de-proteccion-de-datos-personales

Celleri-Pacheco, J., Rivas Asanza, W., Andrade-Garda, J., & Rodríguez-Yáñez, S. (2018). Análisis del uso del Cloud Computing en empresas de Ecuador. *Alternativas, 19*(2), 69–73. https://doi.org/10.23878/alternativas.v19i2.251

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide* (SP 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Erickson, J. (2023, marzo 16). What is cloud migration? Importance, benefits, & strategy. *Oracle*. https://www.oracle.com/es/cloud/cloud-migration/

Gobierno del Ecuador. (2024). *Acuerdo Ministerial No. 0003-2024 de la Estrategia de Gobierno Electrónico* [PDF]. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2024/03/Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf

Google Cloud. (s. f.). ¿Qué es el cloud computing? *Google Cloud*. https://cloud.google.com/learn/what-is-cloud-computing?hl=es

International Organization for Standardization. (2011). *ISO/IEC 19011:2011 – Directrices para la auditoría de sistemas de gestión*.

Más del 80% de organizaciones de América Latina ya adoptan «cloud». (2024, enero 3). *MIT Technology Review*. https://www.technologyreview.es/s/15955/mas-del-80-de-organizaciones-de-america-latina-ya-adoptan-cloud

National Institute of Standards and Technology. (2010). *Contingency Planning Guide for Federal Information Systems* (SP 800-34 Rev. 1). https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

National Institute of Standards and Technology. (2020). *Zero Trust Architecture* (SP 800-207). https://doi.org/10.6028/NIST.SP.800-207

Pérez, A., & Gómez, L. (2021). La migración a la nube y sus implicaciones en la ciberseguridad en Ecuador. *Revista de Ciberseguridad, 5*(2), 45–60. https://doi.org/10.1234/abc5678

Rodríguez, G. (2020). Privacidad y seguridad en la nube: Algunas implicaciones jurídico-económicas desde el comercio electrónico transfronterizo.

TECNOLÓGICO SAN ANTONIO Tesa

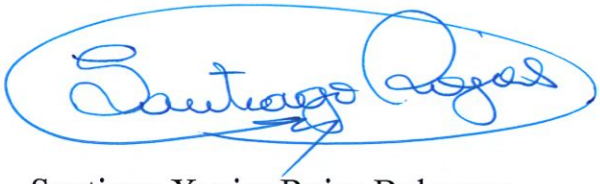
CERTIFICADO DE ORIGINALIDAD

TESA

La Dirección de Carrera de Ciberseguridad , certifica que el trabajo de titulación denominado, "Diseño de un marco de políticas de seguridad para la migración a la nube en Segurilab, con enfoque en la protección de datos y normativas locales", presentado por Rafael Alexander Suntasig Paredes, ha sido sometido a un análisis de similitud mediante la herramienta Turnitin.

El resultado obtenido refleja un 10 % de similitud, porcentaje que se encuentra dentro de los parámetros establecidos por el Instituto Superior Tecnológico San Antonio – TESA, cumpliendo con los criterios de originalidad y autenticidad académica exigidos por la institución.

Quito, 22 de mayo de 2025



Santiago Xavier Rojas Bukovac

Decano Escuela Tecnología e Innovación

