# REPÚBLICA DEL ECUADOR

## VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

**PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:**

## MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

**TÍTULO DEL PROYECTO:**

**Modelo de sistema de Gestión de Seguridad de la información para establecer controles basados en la Norma ISO/IEC 27001:2022, para el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la dirección distrital Milagro 09D17**

**TUTOR**

**PALACIOS ZAMORA KERLY VANESSA**

**AUTOR**

**LOCKE ARAGUILLIN KEVIN PAUL**

**MILAGRO, OCTUBRE 2023**

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

# VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

**Milagro, 16 de julio, 2023**

## CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

En calidad de Tutor del Proyecto de Investigación, nombrado por el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro.

## CERTIFICO

Que he analizado el Proyecto de Investigación con el tema: **Modelo de sistema de Gestión de Seguridad de la información para establecer controles basados en la Norma ISO/IEC 27001:2022, para el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la dirección distrital Milagro 09D17**, elaborado por **LOCKE ARAGUILLIN KEVIN PAUL**, el mismo que reúne las condiciones y requisitos previos para ser defendido ante el tribunal examinador, para optar por el título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**.

Firmado electrónicamente por:
KERLY VANESSA
PALACIOS ZAMORA

**PALACIOS ZAMORA KERLY VANESSA**

**C.I: 0922337225**

# DECLARACIÓN DE AUTORÍA DE LA INVESTIGACIÓN

**Milagro, 06 de octubre, 2023**

El autor de esta investigación declara ante el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro, que el trabajo presentado es de mi propia autoría, no contiene material escrito por otra persona, salvo el que está referenciado debidamente en el texto; parte del presente documento o en su totalidad no ha sido aceptado para el otorgamiento de cualquier otro título de una institución nacional o extranjera.

Firmado electrónicamente por:
KEVIN PAUL LOCKE ARAGUILLIN

**LOCKE ARAGUILLIN KEVIN PAUL**

**C.I: 0940323728**

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

# VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO
## DIRECCIÓN DE POSGRADO
## CERTIFICACIÓN DE LA DEFENSA

El TRIBUNAL CALIFICADOR previo a la obtención del título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**, presentado por **ING. LOCKE ARAGUILLIN KEVIN PAUL**, otorga al presente proyecto de investigación denominado "MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA ESTABLECER CONTROLES BASADOS EN LA NORMA ISO/IEC 27001:2022, PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL DE LA DIRECCIÓN DISTRITAL MILAGRO 09D17", las siguientes calificaciones:

| | |
|---|---|
| TRABAJO DE TITULACION | 60.00 |
| DEFENSA ORAL | 34.33 |
| **PROMEDIO** | **94.33** |
| **EQUIVALENTE** | **Muy Bueno** |


Mgti. MENDOZA CABRERA DENIS DARIO
**PRESIDENTE/A DEL TRIBUNAL**


Ph.D. CHACON LUNA ANA EVA
**VOCAL**


Ph.D. VINUEZA MORALES MARIUXI GEOVANNA
**SECRETARIO/A DEL TRIBUNAL**

# DEDICATORIA

Este trabajo actual está dedicado en primer lugar a Dios, así como también a mi abuela, hermano, esposa e hijos, También quiero reconocer a mis educadores, quienes desempeñaron un papel esencial en la culminación de esta tesis, y agradezco su apoyo constante e incondicional.

# AGRADECIMIENTO

Inicialmente, quiero mostrar mi agradecimiento a mis maestros, personas con un amplio conocimiento que han invertido energía en orientarme hasta mi situación presente. El recorrido no ha estado exento de obstáculos, sin embargo, gracias a su voluntad de impartir sus saberes y su dedicación continúa, he logrado importantes logros, incluyendo la exitosa culminación de mi estudio y la obtención de un título profesional con gratificación.

# CESIÓN DE DERECHOS DE AUTOR

Doctor

ING. FABRICIO GUEVARA VIEJÓ, PhD
Rector de la Universidad Estatal de Milagro

Presente

Mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor al Trabajo realizado como requisito previo para la obtención de mi Título de Cuarto Nivel, cuyo tema fue: **Modelo de sistema de Gestión de Seguridad de la información para establecer controles basados en la Norma ISO/IEC 27001:2022, para el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la dirección distrital Milagro 09D17.** Elaborado por **LOCKE ARAGUILLIN KEVIN PAUL** y que corresponde al Vicerrectorado de Investigación y Posgrado.

Milagro, 06 octubre, 2023

Firmado electrónicamente por:
KEVIN PAUL LOCKE ARAGUILLIN

**LOCKE ARAGUILLIN KEVIN PAUL**

**C.I: 0940323728**

# ÍNDICE GENERAL

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# RESUMEN

El objetivo de este proyecto es proponer un modelo de SGSI que permitirá como herramienta metodológica garantizar la seguridad de los datos. Hoy en día, la información se ha convertido en el recurso más valioso en las organizaciones y es esencial analizarla de manera exhaustiva para protegerla de posibles amenazas. En este contexto, uno de los activos que recibe especial atención es la información personal, que incluye datos que pueden identificar a una persona, ya sea de forma directa o indirecta, como números de identificación, información de ubicación y aspectos relacionados con su identidad física, fisiológica, genética, mental, económica, cultural o social. Para lograrlo, se utiliza el ciclo de mejora continua P.H.V.A. (Planear, Hacer, Chequear y Actuar), el cual consta de cuatro fases, con el fin de alcanzar un nivel de madurez adecuado para reducir los riesgos relacionados con la gestión de información personal. Además, se sugieren políticas y controles de seguridad siguiendo las normas ISO 27001, 27002, guía ISO 27701, considerando los resultados de las evaluaciones de riesgo e impacto, y teniendo en cuenta las particularidades del tratamiento, las partes involucradas y el tipo y cantidad de datos personales, con el objetivo de disminuir los riesgos y preservar la confidencialidad de esa información personal.

**Palabras claves:** Protection de datos, standard ISO 27701, enfoque PDCA.

# ABSTRACT

The objective of this project is to propose an ISMS model that will allow as a methodological tool to guarantee data security Today, information has become the most valuable resource in organizations and it is essential to analyze it thoroughly to protect it from possible threats.

In this context, one of the assets that receives special attention is personal information, which includes data that can identify a person, either directly or indirectly, such as identification numbers, location information and aspects related to their physical, physiological, genetic, mental, economic, cultural or social identity.

To achieve this, the P.H.V.A. (Plan, Do, Check and Act) continuous improvement cycle is used, which consists of four phases, in order to reach an adequate level of maturity to reduce the risks related to the management of personal information. In addition, security policies and controls are suggested following ISO 27001, 27002, ISO 27701 guide, considering the results of the risk and impact assessments, and taking into account the particularities of the treatment, the parties involved and the type and amount of personal data, with the aim of reducing the risks and preserving the confidentiality of that personal information.

**Keywords:** Data protection, ISO 27701 standard, PDCA approach.

# INTRODUCCIÓN

Actualmente de acuerdo al artículo 66 de la LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, incluye "seguridad de la información". Esta sección requiere que los responsables de la introducción de la información recopilada sean efectivos y eviten el acceso no autorizado, la tecnología de cambio o distribución, las medidas administrativas y legales. De esta forma, pretende reducir el riesgo de pérdida, robo o mal uso de los datos personales, garantizando a los ciudadanos y usuarios la confianza en el tratamiento de su información.

De acuerdo a los Art. 71, 72, en el Ecuador las empresas públicas y privadas ya pueden ser multadas con hasta el 1 % de sus ingresos facturados por hacer mal uso de los datos personales de sus clientes o usuarios. Las multas y demás sanciones administrativas entraron en vigor el 26 de mayo de 2023, considerando que han pasado dos años después de la publicación de la Ley de Datos Personales y las instituciones en todos sus niveles deben implementar los controles correspondientes, para su cumplimiento.

El inciso 3 del artículo 66 de la ley aborda específicamente la "Seguridad de la Información". Este apartado exige a los responsables del tratamiento de datos personales implementar medidas técnicas, administrativas y legales que protejan eficazmente la información recopilada y eviten su acceso, modificación o divulgación no autorizados. De este modo, se busca mitigar los riesgos de pérdida, robo o uso indebido de los datos personales, garantizando la confianza de los ciudadanos y usuarios en el manejo de su información.

Para ello, la ley establece la obligación de adoptar políticas y procedimientos que aseguren la confidencialidad e integridad de los datos, así como la capacidad de reacción ante incidentes de seguridad. Asimismo, se prevé la designación de un

responsable de seguridad de la información dentro de las organizaciones, encargado de supervisar y garantizar el cumplimiento de las disposiciones de la ley.

Esta legislación se enmarca dentro del derecho fundamental a la privacidad y al control sobre la información personal, alineándose con estándares internacionales y protegiendo los derechos de los ciudadanos en el contexto digital. Al establecer directrices claras sobre la seguridad de la información, la ley busca fomentar un ambiente confiable para la innovación tecnológica y el desarrollo de la sociedad en la era digital, a la vez que protege los intereses y la dignidad de las personas en el manejo de sus datos personales.

# CAPÍTULO 1

## 1.1 Planteamiento del problema

El Ministerio de Inclusión Económica y Social de la dirección distrital Milagro 09D17, como se indica en el ACUERDO MINISTERIAL No. 030 El MIES 09D17 Milagro, en su NIVEL DISTRITAL. Se encuentra considerado como GESTIÓN DISTRITAL - TIPO A, HABILITANTES DE APOYO, y sus instalaciones físicas se encuentran ubicadas en la Av. 17 de septiembre y AV. Colon Centro de la ciudad de milagro en la Provincia del Guayas.

Esta dependencia es la responsable de coordinar las actividades inherentes al área social, así como promover, incentivar y apoyar programas y proyectos sociales en beneficio de los sectores más vulnerables de la población. Y, en lo que corresponde al departamento de Tecnologías de la Información dentro de sus atribuciones y responsabilidades tiene la de ejecutar procesos de Soporte Tecnológico, Help desk, Administración de Redes, Bases de Datos, mantenimiento de equipos a usuarios internos.

A partir del año 2019, en el Ecuador existen numerosos reportes de filtración de datos personales, entre los que sobresale la de 20 millones de individuos, el día 17 de septiembre del año 2019 que responsabilizo a la empresa Novaestrat, La información de los ciudadanos ecuatorianos que se vio comprometida incluye detalles como el nombre completo, dirección domiciliaria, dirección de correo electrónico, números de identificación y de registro tributario, historiales laborales, y más. Además, se extiende a datos bancarios y financieros, abarcando números de cuentas, saldos y registros de crédito. Incluso información sobre el nivel educativo.

Años después de los sucesos mencionados el 26 de mayo de 2023 entro en vigencia Ley Orgánica de Protección de Datos Personales (LOPDP) ecuatoriana, cuyo

propósito de esta legislación es asegurar el derecho de los ciudadanos ecuatorianos a la protección de sus datos personales, así como a tener acceso y control sobre esa información. La Ley establece normativas que regulan, anticipan y elaboran principios, derechos, responsabilidades y procedimientos de protección.

La problemática en el presente caso de estudio radica en que el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17, mantiene un SGSI orientado únicamente a la Seguridad de la Información y no cuenta con políticas y controles orientados a la protección de datos personales, de tal manera que existe el desafío de garantizar la seguridad de la información y proteger los datos de carácter personal.

Esta deficiencia representa un riesgo significativo para la integridad, confidencialidad y disponibilidad de los datos almacenados y procesados. Además, la ausencia de un SGSI actualizado pone en peligro el cumplimiento de normativas legales y reglamentarias relacionadas con la protección de datos personales, lo que podría resultar en sanciones y daño reputacional para la institución.

Dada la obsolescencia del actual SGSI y la creciente complejidad y sofisticación de las amenazas cibernéticas, es imperativo revisar y actualizar el sistema de seguridad existente, para proponer un nuevo modelo de SGSI basado en las últimas normas ISO, que permitirá no sólo fortalecer la seguridad de la información en el Departamento de TI, sino también optimizar procesos, mejorar la conformidad normativa y reducir riesgos.

En consideración de lo antes expuesto esta actualización es crucial para mantener la integridad de los datos y asegurar la continuidad de los servicios y programas que dependen del manejo eficaz de la información. De este modo, se

contribuirá a una gestión más segura y eficiente, lo cual es especialmente crítico dado que el Ministerio trabaja con poblaciones vulnerables que podrían ser desproporcionadamente afectadas por brechas en la seguridad de la información.

Bajo estas premisas el Departamento de Tecnologías de la Información del MIES 09D17 Milagro, debe proponer un modelo de Sistema de Gestión de Seguridad de la Información, basado en la Norma ISO/IEC 27001:2022 y la guía ISO 27701:2019, para abordar la privacidad de la información. Este enfoque se alinea con la normativa que establece los requisitos para la seguridad de datos sensibles en todo tipo de instituciones públicas y privadas, tales como:

- La falta de medidas de control para asegurar la Infraestructura tecnológica (Red y recursos técnicos, como hardware y software).
- No existen políticas que detallen los controles correspondientes para el Departamento de TI que se vincula en procesos del tratamiento de datos.
- No existen políticas que detallen los controles correspondientes para el personal que labora en el área de TI y participa en el tratamiento de datos.

La propuesta de implementar un Modelo de Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001:2022 y la guía ISO 27701 brindará al Departamento de TI del MIES 09D17 milagro un enfoque integral para fortalecer la protección de datos personales y mitigar riesgos informáticos.

La legislación de protección de datos y la Norma ISO/IEC 27001, 27002, con su extensión ISO/IEC 27701:2019 influyen positivamente en la seguridad y privacidad de la información personal, beneficiando a la ciudadanía desde el Departamento de TI del MIES 09D17 Milagro, la adopción de un Sistema de Gestión de Seguridad de la Información fortalecería la confianza ciudadana al prevenir riesgos como robo de

identidad y acceso no autorizado, garantizando un manejo responsable y legal de la información tratada en la institución.

## 1.2 Objetivos

### *1.2.1 Objetivo General*

Proponer un Modelo de Sistema de Gestión de Seguridad de la Información (SGSI) para establecer controles basados en la Norma ISO/IEC 27001:2022, en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17.

### *1.2.2 Objetivos Específicos*

- Identificar vulnerabilidades y riesgos en la seguridad de la información en la infraestructura tecnológica y sistemas del departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17.
- Diseñar un Modelo de Sistema de Gestión de Seguridad de la Información basado en las normas ISO 27001, 27002, 27701 para el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17.
- Evaluar el Modelo de Sistema de Gestión de Seguridad de la Información propuesto para su implementación en el departamento de Tecnologías de la Información, mediante la contribución de grupos de expertos en seguridad focal.
- Establecer un plan estratégico de mejora continua que asegure la actualización constante y la adaptación del Modelo de Sistema de Gestión de Seguridad de la

Información a través de un proceso dinámico de perfeccionamiento con los recursos disponibles.

### 1.3 Alcance y limitaciones

Este estudio se enfoca en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17.

El alcance del presente proyecto está basado en proponer un Modelo de SGSI, para establecer controles de seguridad conforme a las normas ISO/IEC 27001:2022 e ISO 27701 en el departamento de TI.

Este proyecto proporciona ventajas significativas a un conjunto específico de participantes relacionados con la Dirección Distrital 09D17 MIES Milagro, que incluye a las diferentes áreas de Inclusión Social, los usuarios pertenecientes a los diversos servicios brindados por el MIES y principalmente al Departamento de Tics.

La propuesta basada en un Modelo de SGSI, pretende mejorar lo siguiente:

- Mejorar la imagen Administrativa y Social de la entidad;
- Seguridad y Protección de los datos

Existen limitaciones en las que se incluyen las siguientes:

La obtención de información puede verse limitada por la colaboración y accesibilidad a registros y sistemas del departamento de Tecnologías de la Información. La calidad y disponibilidad de los datos afectan la precisión y confiabilidad de los resultados.

Los recursos disponibles, incluyendo personal, tiempo y presupuesto, pueden restringir el alcance del estudio. Esto podría requerir la selección y priorización de aspectos específicos debido a las limitaciones de recursos y tiempo.

Debido a que el estudio se centra en un departamento específico de la institución, los resultados y conclusiones pueden no ser completamente aplicables a otras instituciones o departamentos de Tecnologías de la Información.

Las modificaciones o cambios en los lineamientos tecnológicos y cambios en la infraestructura del entorno físico del MIES 09D17 Milagro y el Departamento de TI, pueden afectar la eficacia de los controles y el nivel de seguridad de la información. Estos cambios que podrían estar fuera del alcance del estudio y posiblemente impacten en los resultados.

La colaboración y participación del personal que labora en el departamento de Tecnologías de la Información son esenciales para obtener información precisa y completa. La falta de colaboración o resistencia del personal puede comprometer la validez de los resultados obtenidos.

### 1.4 Estado del arte

En esta investigación, se emplea un análisis de tipo exploratorio que involucra la revisión de trabajos publicados en el motor de búsqueda Google académica. El propósito principal es revisar los estudios que abordan la evaluación de la seguridad de la información utilizando guías de implementación en lo que respecta a políticas y controles.

Hierro (Hierro, 2019) La investigación emplea enfoques inductivos y deductivos. El enfoque inductivo parte de ejemplos específicos para llegar a conclusiones generales, mientras que el enfoque deductivo parte de premisas generales para llegar a explicaciones específicas. En el proyecto de investigación, se aplicarán estos métodos para alcanzar los objetivos propuestos. Esto implicará utilizar procesos científicos y metodológicos para abordar la problemática y mejorarla a través del análisis de sucesos y hechos específicos.

Ávila (Ávila, 2023), en su trabajo de tesis menciona que, en el año 2021, Ecuador lideró la lista de países con más ciberataques según Kaspersky. "Panorama de Amenazas en América Latina 2021" y mostró un incremento del 24% en ciberataques durante 8 meses comparado con el 2020. La divulgación de datos en instituciones generó problemas grabes, como por ejemplo los ataques a la Agencia Nacional de Tránsito y Municipio de Quito en abril del 2021.

Quimis (Quimis, 2020) en su tesis de grado indica que la delincuencia cibernética abarca un espectro más amplio y engloba delitos convencionales como el fraude, el robo, el chantaje, la falsificación y el desvío de fondos públicos en los cuales se han empleado computadoras y redes como herramientas. Con el avance de la programación y la expansión de Internet, los delitos informáticos han aumentado en frecuencia y complejidad.

Neptali (Neptali, 2019) en su trabajo de titulación menciona que, en América Latina, naciones como Argentina, Chile, Colombia y Perú, entre otros países vecinos de Ecuador, han mostrado interés en fortalecer la seguridad de sus sistemas de información. Para lograr esto, han adoptado en sus sistemas diversos enfoques y estándares reconocidos, como COBIT, ISO 27001, ITIL e ICREA, adaptándolos a sus sistemas para protegerlos de las amenazas cibernéticas actuales a las que están expuestos.

Mendoza (Mendoza, 2022) en su trabajo de tesis aplicó un enfoque de investigación documental para organizar información específica utilizando un proceso científico. Los resultados evidenciaron que el uso de las TIC en el proceso cognitivo impulsa la investigación en contextos escolares, contribuyendo al desarrollo de las habilidades y capacidades de los estudiantes para la indagación. Entre los métodos teóricos que aplico se encuentra la encuesta.

Pilco (Pilco, 2017) en su tesis indica que la población es un grupo de elementos usados en la investigación, como personas, documentos o hechos, a los que se aplican encuestas para obtener información. En el comercio Guamán, con solo dos colaboradores, se puede encuestar a todos. En esta investigación, la muestra es igual a la población, es decir, las dos personas.

Topacio (Topacio, 2023) en su trabajo de tesis indica que la norma ISO 27001 guarda una conexión con la ISO 27002, donde se describe el Anexo A. En este anexo se establecen los controles estratégicos que sirven como orientación para su implementación. Según (Chopra y Chaudhary, 2020), estos requisitos posibilitan la creación, ejecución, mantenimiento y mejora constante de la Seguridad de la Información.

La Declaración universal de los derechos humanos (Legislación y Leyes Nacionales, 2019), La Declaración de Derechos Humanos de 1948 en Nueva York marcó el inicio de los derechos ciudadanos. A lo largo del tiempo, surgieron derechos humanos de segunda y tercera generación. Entre estos últimos, destaca el derecho a proteger datos personales, incorporado en las legislaciones de muchos países latinoamericanos.

Las Naciones Unidas, (NACIONES UNIDAS, 2020), La OIM, UIT, OCHA, ACNUDH, PNUD, PNUMA, UNESCO, ACNUR, UNICEF, UNOPS, UPU, Voluntarios de las Naciones Unidas, ONU-Mujeres, PMA y OMS respaldan una declaración conjunta. Esta declaración promueve el uso de datos y tecnologías en la respuesta a la COVID-19, respetando la privacidad y derechos humanos. Está en línea con principios de protección de datos y privacidad de la ONU, así como con recomendaciones de la Estrategia de Datos del Secretario General.

La Comisión de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral, (ASAMBLEA NACIONAL DEL ECUADOR, 2021), Ecuador es un Estado basado en derechos, justicia y democracia. La Constitución establece deberes estatales para proteger los derechos, promover desarrollo y eliminar pobreza. Garantiza entorno seguro, cultural y libre de corrupción. El artículo 66, apartado 19, asegura derechos de información personal, incluyendo acceso, control y protección de datos con consentimiento.

Ministerio de Telecomunicaciones y de la Sociedad de la Información, (MINTEL, 2021), El Artículo 178 sanciona la infracción a la privacidad. Quienes accedan o divulguen información personal sin consentimiento enfrentarán prisión de uno a tres años.

ISO (Internacional Organization for Standardization) es la Organización Internacional de Normalización, (ISO Standards, 2023). La ISO/IEC 27001 es el estándar global para sistemas de gestión de seguridad de la información. La familia ISO/IEC 27000 incluye más normas sobre protección de datos y ciberseguridad. Estas normativas ayudan a diversas organizaciones a manejar la seguridad de activos como datos financieros, propiedad intelectual y datos confiados por terceros.

Pazmiño (Pazmiño, 2021) La tesis propone un plan de contingencia para asegurar los activos de información en el Departamento de TI de la EPMR. La metodología MAGERIT será usada para comprender los riesgos de los activos y resaltar la importancia de controlar ciertos activos críticos, mejorando así decisiones efectivas y oportunas.

Briceño en su libro (Briceño, 2021). La tríada de seguridad de la información abarca confidencialidad, integridad y disponibilidad. Este modelo, usado por más de dos

décadas, se centra en la protección de datos y permite analizar aspectos de seguridad a través de estos tres principios.

La confidencialidad, esencial para la privacidad, protege datos de acceso no autorizado. Puede ser aplicada en varios niveles de procesos.

La integridad asegura que los datos no sufran cambios no autorizados, ya sean alteraciones no permitidas o incluso cambios permitidos, pero no deseables.

La disponibilidad asegura el acceso a datos cuando se necesitan. Interrupciones en la cadena de comunicaciones pueden causar problemas debido a fallas eléctricas, ataques o vulnerabilidades, impidiendo el acceso a la información.

En el Blog AEC GOVERTIS, de la Asociación Española para la Calidad, (QAEC, 2021). En su resumen de antecedentes expone que, en el año 2019, la LOPDP fue propuesta por el presidente Lenin Moreno debido a filtraciones de datos en Ecuador. Tras discusiones en la Asamblea Nacional, fue aprobada el 10 de mayo de 2021 y sancionada por el presidente el 21 de mayo del mismo año.

La consultora ingertec (ingertec, 2018). En su sitio web oficial explica que La ISO 27701:2019 es una extensión de ISO/IEC 27001 para gestionar datos personales. Ayuda a cumplir regulaciones como el RGPD y LOPDGDD, permitiendo certificar buenas prácticas. Es apta para todo tipo de organizaciones, mejorando procesos de datos personales con nuevos controles de seguridad.

El Organismo de Certificación global NQA, (NAQ, 2020). ISO 27701 se integra con sistemas existentes, con requisitos variables. Categorías: 1) PIMS vinculados a ISO 27001, 2) PIMS vinculados a ISO 27002, 3) Guías para responsables de datos, 4) Guías para encargados. ISO 27001 usa ciclo Deming: Planificación (metas, recursos, riesgos), Ejecución (implementación), Verificación (evaluación, resultados), Actuación (mejora).

Estructura de alto nivel Anexo SL ISO 27001. (ESCUELA EUROPEA DE LA EXCELENCIA, 2017), contiene diez cláusulas obligatorias que son las siguientes: 1 Alcance, 2 Referencias normativas, 3 Términos y definiciones, 4 Contexto de la organización, 5 Liderazgo, 6 Planificación, 7 Apoyo, 8 Ejecución, Evaluación del rendimiento, 10 Mejora continua.

Tal como explican Gómez y Montoya. (López, 2018). El ser humano cambia y evoluciona, adaptando su relación con la sociedad. Busca superación y bienestar, además de sentir protección. El Derecho es esencial para este propósito, estableciendo leyes y normas que brindan tranquilidad, estabilidad y protección al individuo en la sociedad.

El Centro Europeo de Posgrados, (CEUPE, 2019) en su sitio oficial, se señala que la política de seguridad debe tener directrices específicas para fortalecer los controles de seguridad. Diseñadas para atender necesidades grupales o temáticas, abarcan asuntos como control de acceso, clasificación de información y seguridad física. También abordan temas como uso de recursos, privacidad de pantalla, dispositivos móviles y protección de datos.

En el blog de AUDIT (AUDIT, 2021), rememora que BS7799 fue el estándar previo a ISO 27001, nacido en 1995 en el Reino Unido por el comercio e industria y empresas privadas. Proporcionó prácticas de seguridad en TI sin certificación formal. En 1997, se adoptó un marco para implementarlo. Aunque sin certificación oficial, su efectividad lo hizo aceptado en 2000. Revisado en 1998 como "Código de Prácticas para la Gestión de Seguridad de la Información". En diciembre de 2000, se convirtió en ISO/IEC 17799 internacionalmente.

Como readapta la historia el Grupo ESGinnova. W. Edward Deming desarrolló el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) en 1950, conocido también como ciclo Deming. Japón adoptó esta metodología, llamada Kaizen. Aplicable en procesos y proyectos, mejora la organización si se usa adecuadamente. Ofrece una guía básica para la gestión de procesos, proyectos y sistemas.

Marco Sánchez (SÁNCHEZ, 2021), Desde 2019, Ecuador tiene una Ley de Protección de Datos Personales para regular el tratamiento de datos, salvaguardar derechos y promover la actividad económica. Empresas deben ajustarse y establecer roles claros para un manejo responsable de los datos, considerando implicaciones legales.

En la introducción de su análisis Nataly Cano y Diego Jaramillo, (cano, 2021). La LOPD en Ecuador (Ley Orgánica de Protección de Datos Personales) aborda necesidades tecnológicas, garantizando el ejercicio del derecho a la protección de datos. Regula principios, derechos y protección de datos para enfrentar situaciones tecnológicas emergentes.

Luis Enríquez (Foro, Revista de Derecho, 2021). Ecuador necesita con urgencia una ley de protección de datos que regule el manejo de datos personales por instituciones nacionales y extranjeras. Debe cumplir estándares para ser confiable en transferencias de datos, fomentando empresas ecuatorianas en línea y tratamiento global de datos personales.

Ortega y Zamora, (Ortega, 2022). El rápido avance tecnológico crea vulneraciones al derecho a la intimidad y dignidad humana en las legislaciones. Es esencial proteger los derechos de las personas de manera precisa y adaptada a la sociedad. La investigación busca demostrar la falta de una ley de protección de datos

personales en Ecuador, lo que permite libre acceso a la información personal por terceros e instituciones.

Idea Consultores & Asesores, (IDEA CONSULTORES & ASESORES, 2022). La información es esencial en una empresa y su seguridad es fundamental. Un Sistema de Gestión de Seguridad de la Información según la ISO27001 es crucial para garantizar una gestión adecuada de la seguridad de la información. Se debe tratar los riesgos a diferentes niveles y adaptarse a cambios en procesos y tecnología. La norma ISO-27001 permite mejora continua y flexibilidad en un entorno cambiante.

El entorno colaborativo, (Grupo ESGinnova, 2023). Las empresas usan el ciclo Deming para planificar objetivos y definir indicadores. Luego implementan procesos, controlando calidad y cumplimiento normativo. Una vez logrados resultados, inician un nuevo ciclo PHVA para adaptar políticas y procesos a cambios del mercado.

Un Sistema de Gestión de la Seguridad de la Información (SGSI) está diseñado para desarrollar una estrategia destinada a abordar los aspectos de la seguridad, incluyendo las observaciones necesarias para asegurar el cumplimiento mediante un análisis de riesgos.

**Términos y definiciones generales:**

INTEGRANTES DEL SISTEMA DE PROTECCIÓN DE DATOS. - Los componentes del sistema de protección de información personal son: el titular, la entidad responsable del procesamiento, la persona a cargo del procesamiento, el receptor, el organismo de supervisión de información personal y el representante de resguardo de datos personales. (Registro Oficial Organico de la República del Ecuador, 2021).

DECLARACIÓN DE APLICABILIDAD SOA. - Se ha creado la declaración de aplicabilidad (SoA) como un documento esencial en ISO 27001, útil para cualquier entidad, registrando y supervisando medidas de seguridad. Detalla controles relevantes y verifica su adecuación para Plasticaucho Industrial S.A. basado en la norma ISO/IEC 27002, que es una versión mejorada de la ISO 27001 en términos de controles. (Tigse, 2020).

PROTECCIÓN DE DATOS PERSONALES. - La privacidad no solo implica obtener y divulgar datos, sino también su uso y control, infringiendo la confidencialidad que las entidades públicas deben proteger, evitando compartir datos confidenciales. (Cuero, 2018).

SGSI. - Sistema de Gestión de la Seguridad de la Información "SGSI" Este enfoque tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información. También puede considerar otros aspectos como la trazabilidad, la no repudiación y la confiabilidad. (Gómez, 2019)

CICLO DE DEMING "PHVA". - El Ciclo PHVA (Planificar, Hacer, Verificar, Actuar) o círculo de Deming es una técnica cíclica creada por William Edwards Deming en 1950 para autoevaluación y mejora. Busca identificar mejoras y definir acciones para progreso constante en un enfoque sistemático. (Ayala, 2020)

ISO/IEC 27001. - La ISO 27001 es un estándar global para crear y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) que protege la confidencialidad, integridad y disponibilidad de los datos. Ayuda a identificar y controlar riesgos de seguridad. (Junaid, 2023)

ISO/IEC 27002. - La ISO/IEC 27002 es un conjunto de directrices para establecer seguridad informática, protegiendo activos y generando confianza. Se inician

procesos de supervisión en todas las áreas. Surge de la colaboración entre ISO y EC. (Carolina, 2021).

ISO/IEC 27701. - ISO/IEC 27701 Es un estándar global para mejorar la gestión de información personal en organizaciones, ampliando el ISO/IEC de Seguridad de la Información. Facilita la integración con otros estándares, cumple regulaciones como RGPD, y establece roles y requisitos. Ofrece certificación para respaldar buenas prácticas en gestión de datos personales. (Juárez, 2020).

SEGURIDAD DE LA INFORMACIÓN. - La seguridad de la información es esencial para el éxito de las organizaciones, tanto tecnológica como empresarialmente. La información es valiosa y clave para la ventaja competitiva. La amenaza de robo de datos es real en sectores públicos y privados. La operación de las organizaciones depende de la información, haciendo su protección fundamental en la era moderna. (Katerine, 2017)

SEGURIDAD INFORMÁTICA. - La Seguridad Informática protege la información y su procesamiento contra manipulación y accesos no autorizados, previniendo amenazas y daños. Su objetivo es proteger personas, dispositivos y datos de terceros maliciosos. Se enfoca en defender sistemas y datos de daños y accesos no permitidos. Hay varios enfoques de seguridad según lo que se quiera proteger. (Valenzuela, 2022).

PROTECCIÓN DE LA RED. - Frecuentemente la protección de la red es una inquietud fundamental al establecer una estructura de red. La mayoría de las configuraciones emplean enrutadores con cortafuegos incorporado, junto al software que permite gestionar el acceso de usuarios, supervisar el flujo de datos y aplicar rigurosamente los protocolos establecidos. (Bastidas, 2017).

MAGNITUD DE DAÑO. - Evaluar perjuicios es complejo; se puede simplificar considerando daños materiales, reputacionales, emocionales, etc. También se puede valorar cualitativamente, combinando factores en un término económico. Enfoque cualitativo implica considerar más que la pérdida económica. Magnitud del daño puede clasificarse: Bajo, si es aislado; Medio, si desorganiza una parte; Alto, si paraliza o destruye la organización. (Murillo, 2021).

# CAPÍTULO 2

## 2.1 Metodología

Este trabajo de investigación tiene como principal objetivo proponer un Modelo de SGSI basados en la Norma ISO/IEC 27001, 27002, 27701, enfocándose en el Departamento de TI del MIES 09D17 Milagro, con la finalidad de establecer controles que fomenten una mentalidad preventiva en relación con el cumplimiento de las normativas de protección de datos en Ecuador, mediante la comprensión y aceptación de estas normativas"

El documento incluye una metodología de carácter exploratorio y se fundamenta en los métodos que se detallan a continuación:

**Método Inductivo:** El método inductivo parte de lo particular a lo general. Busca comprender características generales de la información digital en el Departamento de TI del MIES 09D17 Milagro y desarrollar una herramienta metodológica para seguridad de datos personales. Está ligado a los Ítems de la Norma ISO 27701 para gestionar privacidad, según el estado del arte del proyecto. (Hierro, 2019).

**Método Deductivo:** Los resultados de la entrevista al jefe del Departamento de TI del MIES 09D17 Milagro se usan para analizar y justificar la necesidad de diseñar herramientas metodológicas de seguridad de datos. (Hierro, 2019).

**Método Cualitativo:** Este método busca recopilar información, común en investigaciones sobre el estado actual. Es esencial aquí para comprender la relevancia de la información en el Departamento de TI del MIES 09D17 Milagro, usando la entrevista busca una justificación técnica para el manejo de datos personales.

**Investigación Bibliográfica**: Para el desarrollo del proyecto, se requiere el uso de este método para la revisión de literatura relacionada al campo de estudio, esto en base a que en la actualidad existe una gran vulnerabilidad de la privacidad y uso de los

datos personales; por ello es importante conocer a fondo la Ley de Protección de Datos Personales. (Mendoza, 2022).

La investigación bibliográfica permitió realizar la primera etapa proporcionando una revisión de investigaciones previamente publicadas utilizando Google Académico, una herramienta en línea de acceso abierto que facilita la búsqueda de documentos académicos, incluyendo artículos, tesis, libros y resúmenes. Esta plataforma recopila fuentes de diversas procedencias, como editoriales universitarias, asociaciones profesionales, repositorios de preprints, universidades y otras instituciones académicas.

**Tabla 1** Búsqueda de referencias bibliográficas ISO/IEC 27001, 27002, 27701

| | TÍTULO | AÑO |
|---|---|---|
| | **Google Académico** | |
| ISO 27001, 27002, 27701 | https://scholar.google.es/, https://repositorio.unemi.edu.ec/, (documentos, datos, etc.) | 2019<br>2020<br>2021<br>2022<br>2023 |
| LOPDP, RGPD | La Visión de América Latina sobre el Reglamento General de Protección de Datos | 2019<br>2020<br>2021<br>2022<br>2023 |
| ISO 27001:2022 | NQA ISO/IEC 27001:2022, Norma de seguridad de la información, ciberseguridad y salvaguardia de la privacidad. | 2019<br>2020<br>2021<br>2022 |
| ISO 27002:2022 | NAQ ISO/IEC 27001:2022, Estándar de seguridad de la información que abarca ciberseguridad y preservación de la privacidad. | 2019<br>2020<br>2021<br>2022 |
| ISO 27701:2019 | NQA Sistema de Administración de la Privacidad de la Información (PIMS). | 2019 |

Fuente: Elaborado por Ing. Kevin Locke

**Entrevista:** Esta técnica fue dirigida al jefe del Departamento de TI del MIES 09D17 Milagro y se utiliza como el instrumento que permite obtener mayor información, para medir el nivel de conocimiento en la protección de los datos personales y qué medidas se considera para resguardarlos. (Mendoza, 2022).

Con el objetivo de evaluar los procedimientos informáticos vigentes en el Departamento de Tecnología de la Información (TI) de MIES 09D17 Milagro, se llevó a cabo una entrevista con el jefe del Departamento de TI a quien se le realizo un total de 16 preguntas abiertas y cerradas referentes.

Esto se realizó con la intención de identificar cómo se están ejecutando los procesos y descubrir posibles debilidades en términos de seguridad. Para determinar si existían políticas y controles en vigor para la protección de datos personales, aplicados en el mencionado Departamento de TI.

**Preguntas generales acerca del departamento de TI**

1. ¿Podría ofrecer una breve descripción de las funciones principales del Departamento de Tecnologías de la Información en MIES 09D17 Milagro?

El Departamento de TI del MIES 09D17 Milagro se encarga de gestionar la tecnología de la información y los recursos tecnológicos en general, además de promover y garantizar la seguridad de la información que se ingesta diariamente en la institución.

2. ¿Cuál es el volumen de datos que se maneja en este lugar y cuántos usuarios acceden a dichos datos?

El volumen de datos manejados y usuarios que acceden varía, pero aproximadamente en el día se ha calculado un promedio de 1500 personas.

3. ¿Qué tecnologías se están utilizando en la actualidad en el Departamento de TI?

Actualmente, se utilizan tecnologías como sistemas de gestión de bases de datos online y servidores virtualizados.

**Evaluación de la seguridad actual**

4. ¿El departamento actualmente tiene alguna política o procedimiento establecido, para la seguridad de la información y protección de datos personales?

   Sí, contamos con políticas y procedimientos de seguridad de la información, pero no para la protección de datos personales.

5. ¿Se han identificado previamente riesgos de seguridad o vulnerabilidades?

   En el pasado, se han identificado algunos riesgos de seguridad y vulnerabilidades, pero en la actualidad muchos son impredecibles.

6. ¿Existe algún registro o protocolo para dar seguimiento a incidentes de seguridad?

   Sí, tenemos un registro, pero no se cuenta con un protocolo de seguimiento cuando ocurren incidentes de seguridad.

7. ¿Cuáles son las principales amenazas a la seguridad de la información que el departamento enfrenta?

   Las principales amenazas de seguridad incluyen ataques cibernéticos, pérdida de datos y accesos no autorizados

**Comprensión de ISO/IEC 27001**

8. ¿Está familiarizado con la norma ISO/IEC 27001:2022 y la ISO 27701?

   Si estoy familiarizado con la norma ISO/IEC 27001:2022, pero no con la ISO 27701.

9. ¿Cuál es su opinión sobre la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en esta norma ISO/IEC 27001:2022 y la guía ISO 27701, para establecer controles en la protección de datos personales?

Creo que implementar un SGSI basado en esta norma sería beneficioso para fortalecer la seguridad de la información y ejecutar un adecuado tratamiento en los datos de carácter personal.

10. ¿Se han tomado medidas previas para alinearse con alguna norma, para la protección de datos personales?

    No se han tomado medidas para este tema.

**Recursos y Limitaciones**

11. ¿Qué recursos (humanos, financieros y tecnológicos) están disponibles en la actualidad para implementar un SGSI?

    Para obtener los recursos correspondientes a la implementación se deberá presentar la propuesta como proyecto y solicitar que sea agregada al PAC actual o proyectada en el del año siguiente. Por lo tanto, no existe en presupuesto.

12. ¿Cuáles son los principales obstáculos o limitaciones que prevé para la implementación de un SGSI?

    Las principales barreras incluyen las restricciones presupuestarias y la necesidad de capacitación adicional.

**Compromiso y Apoyo Organizacional**

13. ¿Qué nivel de respaldo espera recibir del liderazgo de la organización para la implementación de un SGSI?

    Esperamos un alto nivel de apoyo de la alta dirección, para implementar un SGSI. Previamente comunicando la necesidad de implementación para su aprobación.

14. ¿Cómo se prioriza la seguridad de la información en comparación con otros objetivos del departamento o de la institución?

La seguridad de la información se prioriza en consonancia con los objetivos institucionales.

**Preguntas de Seguimiento y Futuras Acciones**

15. ¿Está dispuesto a llevar a cabo una evaluación más detallada de las necesidades y riesgos de seguridad en el departamento?

    Estamos abiertos a una evaluación más detallada de las necesidades y riesgos de seguridad.

16. ¿Cuáles son los pasos inmediatos que considera necesarios para avanzar hacia una gestión más efectiva de la seguridad de la información y la protección de datos personales?

    Los pasos inmediatos incluyen una revisión exhaustiva de las políticas y controles de seguridad existentes y una capacitación del personal en seguridad de la información y protección de datos personales.

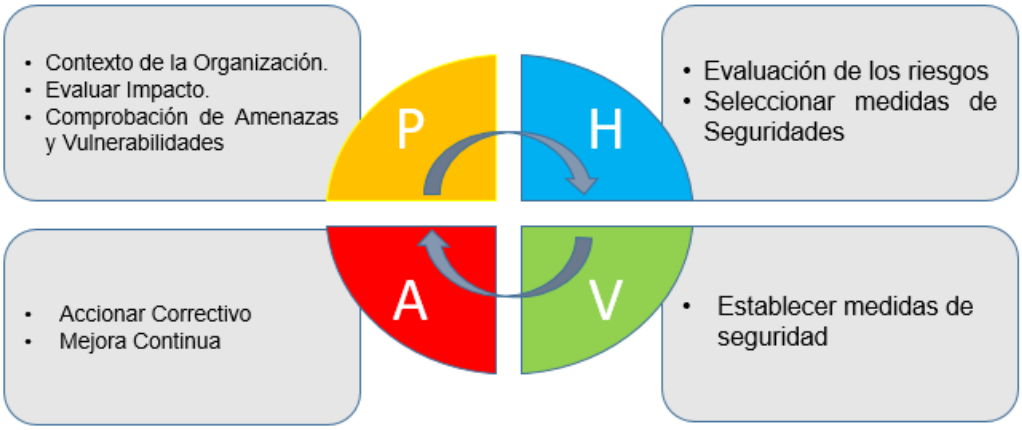
# CAPÍTULO 3

## 3.1 PROPUESTA DE SOLUCIÓN

Esta propuesta de solución se basa en la norma ISO 27701:2019, una extensión de la ISO 27001 e ISO 27002 que se enfoca en la privacidad de los datos. Esta norma proporciona directrices y requisitos adicionales que son esenciales para establecer políticas y controles efectivos dentro del Sistema de Gestión de Seguridad de la Información existente, en este caso dentro del departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17.

Para guiar la implementación exitosa del SGSI propuesto, se empleará el ciclo PHVA como un enfoque cíclico, ejecutando las siguientes fases: (Planificar, Hacer, Verificar, Actuar).

**Figura 1** Ciclo PHVA




Fuente: Elaborado por Ing. Kevin Locke

## 3.2 DECRIPCIÓN DE LA PROPUESTA DE SOLUCIÓN

La herramienta metodológica tiene como propósito proporcionar un sólido marco de referencia destinado a garantizar la seguridad de los datos personales. Su función principal es la de fortalecer no solo el Sistema de Gestión de Seguridad de la Información (SGSI) propuesto, sino también el cumplimiento riguroso de la Ley Orgánica de Protección de Datos Personales (LOPDP). Esto adquiere especial

importancia en el contexto ecuatoriano, donde las entidades reguladoras y de supervisión vigilan de cerca el manejo de la información sensible.

Al adoptar esta herramienta metodológica, el Departamento de Tecnologías de la Información no solo podrá salvaguardar de manera efectiva la integridad y confidencialidad de los datos, sino también demostrar un compromiso firme con la protección de la privacidad de los ciudadanos ecuatorianos. Además, se facilitará la adaptación y el cumplimiento de los requisitos legales y regulatorios específicos en materia de seguridad de datos en el país.

En última instancia, la implementación de esta metodología no solo contribuirá a la seguridad de los datos y al cumplimiento normativo, sino que también fortalecerá la confianza de los ciudadanos en la gestión de sus datos personales por parte del Departamento de Tecnologías de la Información, respaldando así los principios fundamentales de privacidad y seguridad de la información en Ecuador.

## 3.3 DESARROLLO DE LA PROPUESTA

**Fase 1: Planificación. -** En esta fase se realiza una evaluación de la situación actual del Departamento de TI del MIES 09D17 Milagro, mediante mecanismos de control de seguridad de la información.

- Contexto de la Organización
- Evaluar Impacto
- Comprobación de amenazas y Vulnerabilidades

En la tabla 2 se muestra la proporción de requisitos Obligatorios del SGSI y la proporción de Controles de Seguridad de la Información, con las siguientes valoraciones:

**Tabla 2** Proporción de Requisitos y Controles del SGSI

| CRITERIOS | PORCENTAJES |
|---|---|
| Desconocido | 0% al 100% |
| Inexistente | 0% al 100% |
| Inicial | 0% al 100% |
| Limitado | 0% al 100% |
| Definido | 0% al 100% |
| Gestionado | 0% al 100% |
| Optimizado | 0% al 100% |
| No Aplica | 0% al 100% |

Fuente: Elaborado por Ing. Kevin Locke

En la tabla 3, se evalúa los Requisitos Obligatorios del SGSI implementados y gestionados en el Departamento de TI del MIES 09D17 Milagro, siguiendo la estructura de la ISO 27001:2022. SL, (ESCUELA EUROPEA DE LA EXCELENCIA, 2017) y revisados mediante la "Declaración de Aplicabilidad SoA". (Tigse, 2020).

**Tabla 3** Requisitos obligatorios del SGSI

| Sección | Requisito ISO/IEC 27001 | Status |
|---|---|---|
| **4** | **Contexto de la organización** | |
| **4,1** | **Contexto organizacional** | |
| 4,1 | Determinar los **objetivos del SGSI** de la organización y cualquier aspecto que pueda comprometer su efectividad | Gestionado |
| **4,2** | **Partes interesadas** | |
| 4.2 (a) | Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc | Definido |
| 4.2 (b) | Determinar sus requisitos relevantes al respecto de la seguridad de la información y sus obligaciones | Definido |
| **4,3** | **Alcance del SGSI** | |
| 4,3 | Determinar y documentar el **alcance del SGSI** | Gestionado |
| **4,4** | **SGSI** | |
| 4,4 | Establecer, implementar, mantener y mejorar continuamente un **SGSI** de conformidad con la norma | Inexistente |
| **5** | **Liderazgo** | |
| **5,1** | **Liderazgo & compromiso** | |
| 5,1 | La alta dirección debe demostrar **liderazgo & compromiso** en relación con el SGSI | Limitado |

| | | |
|---|---|---|
| **5,2** | **Política** | |
| 5,2 | Establecer la **política de seguridad de la información** | Limitado |
| **5,3** | **Roles, responsabilidades & autoridades en la organización** | |
| 5,3 | Asignar y comunicar los **roles & responsabilidades** de la seguridad de la información | Inexistente |
| **6** | **Planificación** | |
| **6,1** | **Acciones para tratar con los riesgos & oportunidades** | |
| 6.1.1 | Diseñar / planificar el SGSI para satisfacer los requisitos, tratando con los riesgos & oportunidades | Gestionado |
| 6.1.2 | Definir y aplicar un **proceso de apreciación de riesgos de seguridad de la información** | Limitado |
| 6.1.3 | Documentar y aplicar un proceso de **tratamiento de riesgos de seguridad de la información** | Limitado |
| **6,2** | **Objetivos & planes de seguridad de la información** | |
| 6,2 | Establecer y documentar los objetivos y planes de seguridad de la información | Limitado |
| **6,3** | **Planificación de cambios** | |
| 6,3 | Los cambios sustanciales al SGSI deben ser llevados a cabo de manera planificada | Limitado |
| **7** | **Soporte** | |
| **7,1** | **Recursos** | |
| 7,1 | Determinar y proporcionar los recursos necesarios para el SGSI | Limitado |
| **7,2** | **Competencias** | |
| 7,2 | Determinar, documentar y poner a disposición las **competencias** necesarias | Limitado |
| **7,3** | **Concientización** | |
| 7,3 | Establecer un programa de **concientización en seguridad** | Inexistente |
| **7,4** | **Comunicación** | |
| 7,4 | Determinar la necesidad para las **comunicaciones internas y externas** relevantes al SGSI | Limitado |
| **7,5** | **Información documentada** | |
| 7.5.1 | Proveer la **documentación** requerida por la norma, así como la requerida por la organización | Inexistente |
| 7.5.2 | Proveer **títulos**, autores, etc para la documentación, **adecuar el formato** consistentemente, **revisarlos & aprobarlos** | Limitado |
| 7.5.3 | **Controlar la documentación** adecuadamente | Limitado |
| **8** | **Operación** | |

| | | |
|---|---|---|
| **8,1** | **Planificación y control operacional** | |
| 8,1 | Planificar, implementar, controlar & documentar el proceso del SGSI para gestionar los riesgos (i.e. un **plan de tratamiento de riesgos**) | Limitado |
| **8,2** | **Apreciación del riesgo de seguridad de la información** | |
| 8,2 | **(Re)hacer la apreciación & documentar los riesgos de seguridad de la información en forma regular** & ante cambios o modificaciones | Limitado |
| **8,3** | **Tratamiento del riesgo de seguridad de la información** | |
| 8,3 | Implementar el plan de tratamiento de riesgos (**tratar los riesgos!**) y documentar los resultados | Limitado |
| **9** | **Evaluación del desempeño** | |
| **9,1** | **Seguimiento, medición, análisis y evaluación** | |
| 9,1 | **Hacer seguimiento, medir, analizar y evaluar** el SGSI y los controles | Inexistente |
| **9,2** | **Auditoría interna** | |
| 9,2 | Planificar y llevar a cabo **auditorías internas** del SGSI | Limitado |
| **9,3** | **Revisión por la dirección** | |
| 9,3 | Emprender **revisiones por la dirección** del SGSI regularmente | Limitado |
| **10** | **Mejora** | |
| **10,1** | **Mejora continua** | |
| 10,1 | **Mejorar** continuamente el SGSI | Limitado |
| **10,2** | **No conformidad y acciones correctivas** | |
| 10,2 | Identificar, corregir y llevar a cabo acciones para prevenir la recurrencia de no conformidades, documentando las acciones | Inexistente |

Fuente: Elaborado por Ing. Kevin Locke

En la tabla 4, se muestra la proporción de controles de seguridad de la información implementados actualmente en el Departamento de TI del MIES 09D17 Milagro, revisados mediante la "Declaración de Aplicabilidad SoA "ANEXO A". (Topacio, 2023)

**Tabla 4** Controles de Seguridad de la Información

| A5 | Controles organizacionales | |
|---|---|---|
| A.5.1 | Políticas para la seguridad de la información | Inexistente |
| A.5.2 | Roles y responsabilidades en la seguridad de la información | Inexistente |
| A.5.3 | Segregación de tareas | Limitado |
| A.5.4 | Responsabilidades de gestión | Inicial |
| A.5.5 | Contacto con las autoridades | Gestionado |
| A.5.6 | Contacto con grupos de interés especial | No Aplica |
| A.5.7 | Inteligencia de amenazas | Inicial |
| A.5.8 | Seguridad de la información en la gestión de proyectos | Inexistente |
| A.5.9 | Inventario de activos de información y otros asociados a la misma | Gestionado |
| A.5.10 | Uso aceptable de activos de información y otros asociados a la misma | Gestionado |
| A.5.11 | Devolución de activos | No Aplica |
| A.5.12 | Clasificación de la información | Inexistente |
| A.5.13 | Etiquetado de la información | Limitado |
| A.5.14 | Intercambio de la información | Limitado |
| A.5.15 | Control de Acceso | Definido |
| A.5.16 | Gestión de la identidad | Inexistente |
| A.5.17 | Información de autenticación | Limitado |
| A.5.18 | Derechos de acceso | Definido |
| A.5.19 | Seguridad de la información en la relación con proveedores | Limitado |
| A.5.20 | Requisitos de seguridad de la información en contratos con terceros | Definido |
| A.5.21 | Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación) | Limitado |
| A.5.22 | Gestión del cambio, revisión y monitoreo de los servicios del proveedor o suministrador | Gestionado |
| A.5.23 | Seguridad de la información para el uso de servicios en la nube (cloud) | Limitado |
| A.5.24 | Planeamiento y preparación de la gestión de incidentes de seguridad de la información | Inexistente |
| A.5.25 | Evaluación y decisión en los eventos de seguridad de la información | Inexistente |
| A.5.26 | Respuesta a los incidentes de seguridad de la información | Inexistente |

| | | |
|---|---|---|
| A.5.27 | Aprendizaje sobre los incidentes de seguridad de la información | Inexistente |
| A.5.28 | Recolección de evidencia | No Aplica |
| A.5.29 | Seguridad de la información durante interrupciones | Limitado |
| A.5.30 | Preparación de las TIC para la continuidad de negocio | Limitado |
| A.5.31 | Requisitos legales, estatutarios, regulatorios y contractuales | Gestionado |
| A.5.32 | Derechos de propiedad intelectual | No Aplica |
| A.5.33 | Protección de registros | Inexistente |
| A.5.34 | Privacidad y protección de la PII (Información Identificable Personal) | Inexistente |
| A.5.35 | Revisión independiente de la seguridad de la información | Inexistente |
| A.5.36 | Cumplimiento con las políticas, reglas y normas de la seguridad de la información | Inexistente |
| A.5.37 | Procedimientos operacionales documentados | Gestionado |
| **A6** | **Controles personales** | |
| A.6.1 | Revisión de antecedentes | Inexistente |
| A.6.2 | Términos y condiciones de empleo | Inexistente |
| A.6.3 | Concientización, educación y entrenamiento en seguridad de la información | Inicial |
| A.6.4 | Proceso disciplinario | Limitado |
| A.6.5 | Responsabilidades luego de la finalización o cambio de empleo | Definido |
| A.6.6 | Acuerdos de confidencialidad o no revelación | Gestionado |
| A.6.7 | Trabajo remoto | Optimizado |
| A.6.8 | Reportes de eventos de seguridad de la información | No Aplica |
| A7 | **Controles físicos** | |
| A.7.1 | Perímetros de seguridad física | Optimizado |
| A.7.2 | Entrada física | Optimizado |
| A.7.3 | Seguridad de oficinas, despachos e instalaciones | Gestionado |
| A.7.4 | Supervisión de la seguridad física | Limitado |
| A.7.5 | Protección contra amenazas físicas y ambientales | No Aplica |
| A.7.6 | Trabajo en áreas seguras | Gestionado |
| A.7.7 | Escritorio y pantalla limpios | Gestionado |
| A.7.8 | Emplazamiento y protección de equipos | Definido |

| | | |
|---|---|---|
| A.7.9 | Seguridad de activos fuera de las instalaciones | No Aplica |
| A.7.10 | Medios de almacenamiento | Definido |
| A.7.11 | Servicios de suministro | Gestionado |
| A.7.12 | Seguridad del cableado | No Aplica |
| A.7.13 | Mantenimiento de equipos | Gestionado |
| A.7.14 | Eliminación o re utilización segura de equipos | Gestionado |
| **A8** | **Controles Tecnológicos** | |
| A.8.1 | Dispositivos terminales de usuario | Definido |
| A.8.2 | Derechos de acceso privilegiado | Limitado |
| A.8.3 | Restricción de acceso a la información | Limitado |
| A.8.4 | Acceso al código fuente | No Aplica |
| A.8.5 | Autenticación segura | Inicial |
| A.8.6 | Gestión de la capacidad | Inicial |
| A.8.7 | Protección contra código malicioso (malware) | Inicial |
| A.8.8 | Gestión de vulnerabilidades técnicas | Inexistente |
| A.8.9 | Gestión de la configuración | Limitado |
| A.8.10 | Borrado de información | Definido |
| A.8.11 | Enmascarado de datos | Inexistente |
| A.8.12 | Prevención de filtración de datos | Inexistente |
| A.8.13 | Respaldo de información | Gestionado |
| A.8.14 | Redundancia de las instalaciones de procesamiento de información | Optimizado |
| A.8.15 | Registración | Limitado |
| A.8.16 | Actividades de supervisión | Limitado |
| A.8.17 | Sincronización de reloj (clock) | Optimizado |
| A.8.18 | Uso de programas utilitarios privilegiados | Limitado |
| A.8.19 | Instalación de software en sistemas operacionales | Inicial |
| A.8.20 | Seguridad en redes | Inexistente |
| A.8.21 | Seguridad de servicios de red | Inexistente |
| A.8.22 | Segregación de redes | No Aplica |
| A.8.23 | Filtrado web | Inexistente |

| | | |
|---|---|---|
| A.8.24 | Uso de criptografía | Inexistente |
| A.8.25 | Desarrollo seguro del ciclo de vida | No Aplica |
| A.8.26 | Requerimientos de seguridad en aplicaciones | Inexistente |
| A.8.27 | Principios de arquitectura de sistemas e ingeniería seguras | No Aplica |
| A.8.28 | Generación de código seguro | No Aplica |
| A.8.29 | Prueba segura en el desarrollo y aceptación | No Aplica |
| A.8.30 | Desarrollo tercerizado | No Aplica |
| A.8.31 | Separación de entornos de desarrollo, prueba y producción | No Aplica |
| A.8.32 | Gestión de cambios | No Aplica |
| A.8.33 | Información de prueba | Inexistente |
| A.8.34 | Protección de sistemas de información durante pruebas de auditoría | Inexistente |

Fuente: Elaborado por Ing. Kevin Locke

El análisis realizado a partir de la Tabla 3, Requisitos Obligatorios del SGSI y la Tabla 4 de Controles del "Anexo A", muestran los resultados de evaluación en la tabla 5 de la siguiente manera:

**Tabla 5** Proporción de requisitos del SGSI y Proporción de controles del SGSI

| Status | Significado | Proporción de requisitos del SGSI | Proporción de controles de seguridad de la información |
|---|---|---|---|
| ? Desconocido | No ha sido siquiera revisado aún | **1%** | **0%** |
| **Inexistente** | Ausencia completa de una política, procedimiento, control, etc legibles | **21%** | **27%** |
| **Inicial** | El desarrollo apenas ha comenzado y requerirá un trabajo significativo para satisfacer los requisitos | **0%** | **8%** |
| **Limitado** | Progresando bien pero no completado aún | **61%** | **18%** |
| **Definido** | El desarrollo está más o menos completo aunque con ausencia de detalles y/o no está aún implementado, en cumplimiento vigente ni activamente avalado por la alta dirección. | **7%** | **9%** |

| | | | |
|---|---|---|---|
| **Gestionado** | El desarrollo está completo, el proceso / control ha sido implementado y recientemente comenzó a operar | **11%** | **15%** |
| **Optimizado** | El requisito está plenamente conforme, está plenamente operativo como se espera, está siendo activamente supervisado y mejorado, y hay evidencia sustancial para demostrar todo lo antedicho a los auditores | **0%** | **5%** |
| **No Aplica** | TODOS los requerimientos en el cuerpo principal de la norma ISO/IEC 27001 son obligatorios SI su SGSI va a ser certificado. Caso contrario, la gerencia a cargo, puede ignorarlos | **0%** | **18%** |
| | Total | 101% | 100% |

Fuente: Elaborado por Ing. Kevin Locke

En la Tabla 5, Se identificaron los requisitos obligatorios y controles del SGSI aplicados actualmente en el del Departamento de TI del MIES 09D17 Milagro. Y se concluyó que la falta de políticas y controles es un problema significativo, especialmente en una entidad que maneja datos personales sujetos a protección legal.

Por lo tanto, resulta necesario proponer un "Modelo de Sistema de Gestión de Seguridad de la Información para establecer controles basados en la Norma ISO/IEC 27001:2022, para el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17.

**La evaluación de riesgos y la implementación de medidas de seguridad para proteger los datos personales:** Tras identificar y evaluar los riesgos, se deben tomar medidas de seguridad proporcionales. Estas pueden ser controles técnicos como cifrados, autenticación de dos factores y firewalls, y también políticas sólidas para la protección de datos. La formación en seguridad de datos es clave para instaurar una cultura de seguridad en la institución.

Es esencial entender que la evaluación de riesgos y las medidas de seguridad son procesos en curso. Las amenazas cambian, por lo que es crucial revisar y actualizar

regularmente las estrategias de protección de datos. Cumplir con leyes y regulaciones de privacidad es fundamental para mantener estándares de seguridad y resguardar la privacidad.

**Evaluación de impacto:** Para actividades con riesgo significativo de procesamiento de datos personales, se realiza Evaluación de Impacto. Esto cubre datos tratados, proceso, responsables y encargados. Los resultados se reflejan en la Tabla 8, mostrando niveles de riesgo por operación. Esto guía decisiones y medidas para resguardar privacidad y seguridad de los datos.

**Tabla 6** Evaluación de Impacto

| Impacto | Descripción | Nivel |
|---|---|---|
| Bajo | Incidentes menores que son resueltos fácilmente y en poco tiempo, sin ningún problema significativo. | 1 |
| Medio | Incidentes importantes que a pesar de algunas dificultades, se superan satisfactoriamente. | 2 |
| Alto | Incidentes con consecuencias significativas que implican enfrentar desafíos importantes, pero aun así se logran superar. | 3 |
| Muy Alto | Incidentes con consecuencias irreversibles son los que no pueden superarse y dejan consecuencias graves e imposibles de revertir. | 4 |

Fuente: Elaborado por Ing. Kevin Locke

En la evaluación de impacto, se analiza el potencial impacto en confidencialidad, integridad y disponibilidad de datos personales. El impacto más alto se usa para priorizar medidas de protección. Este enfoque gestiona riesgos del tratamiento de datos, guiando decisiones informadas para salvaguardar privacidad y seguridad.

**Tabla 7** Evaluar el impacto

| # | PREGUNTA | | CRITERIO | PUNTAJE |
|---|---|---|---|---|
| 1 | El impacto generado por la divulgación no autorizada de los datos personales (confidencialidad) en el contexto de la actividad comercial de qué nivel es. | | Bajo | 1 |
| | | | Medio | 2 |
| | | | Alto | 3 |
| | | | Muy Alto | 4 |

| | | | | |
|---|---|---|---|---|
| 2 | El impacto ocasionado por la alteración no autorizada de los datos personales (integridad) | | Bajo | 1 |
| | | | Medio | 2 |
| | | | Alto | 3 |
| | | | Muy Alto | 4 |
| 3 | El impacto provocado por la destrucción o pérdida no autorizada de los datos personales (disponibilidad) en el contexto de la actividad comercial de qué nivel es. | | Bajo | 1 |
| | | | Medio | 2 |
| | | | Alto | 3 |
| | | | Muy Alto | 4 |

Fuente: Elaborado por Ing. Kevin Locke

Esta metodología evalúa el riesgo global del tratamiento de datos personales en actividades comerciales. Al abordar confidencialidad, integridad y disponibilidad, la institución toma decisiones informadas sobre protección y mitigación, referenciando resultados con la tabla 7.

**Tabla 8** Niveles de Riesgo

| NIVELES DE IMPACTO | IMPACTO / TOTAL |
|---|---|
| Bajo | 1 – 3 |
| Medio | 3– 6 |
| Alto | 6 – 9 |
| Muy Alto | 9 – 12 |

Fuente: Elaborado por Ing. Kevin Locke

**Definición de las posibles amenazas y la evaluación de su probabilidad:** Se define amenazas y evalúa su probabilidad en el Departamento de TI del MIES 09D17 Milagro, comprendiendo amenazas internas y externas en el procesamiento de datos personales.

Se identifican y analizan amenazas para el entorno de tratamiento de datos, enfocándose en tres procesos clave del Departamento de TI para abordar aspectos relevantes. Mediante preguntas se evalúa la probabilidad de amenazas, obteniendo una visión de riesgos potenciales en privacidad y seguridad de datos.

**Principales procesos en el Departamento de TI MIES 09D17 Milagro**

- Infraestructura tecnológica (Red y recursos técnicos, como hardware y software).
- El Departamento de TI se vincula en procesos del tratamiento de datos.
- El personal que labora en el área de TI participa en el tratamiento de datos.

**Tabla 9** Posibles amenazas y la evaluación de su probabilidad

| | |
|---|---|
| **Infraestructura tecnológica (Red y recursos técnicos, como hardware y software).** | |
| **1** | ¿Se lleva a cabo la introducción de datos personales utilizando internet? |
| **2** | ¿Existe un control estricto sobre el acceso de los usuarios a los datos personales? |
| **3** | ¿El procesamiento de datos está conectado a otros sistemas o servicios de tecnología de la información? |
| **4** | ¿Las personas no autorizadas pueden acceder fácilmente al entorno de procesamiento de datos? |
| **5** | ¿El tratamiento de datos personales se ha desarrollado, implementado o mantenido sin seguir las mejores prácticas pertinentes? |
| **El Departamento de TI se vincula en procesos del tratamiento de datos.** | |
| **6** | ¿Están debidamente establecidas las funciones y responsabilidades relacionadas con el procesamiento de datos? |
| **7** | ¿La utilización de la red, sistemas y recursos físicos dentro de la empresa carece de claridad o definición? |
| **8** | ¿Los empleados utilizan sus dispositivos personales para acceder al sistema de procesamiento de datos personales? |
| **9** | ¿Los empleados transfieren, almacenan o procesan datos personales fuera de las instalaciones de la organización? |
| **10** | ¿Se llevan a cabo actividades de procesamiento de datos sin generar archivos de registro? |
| **El personal que labora en el área de TI participa en el tratamiento de datos.** | |
| **11** | ¿La realización del tratamiento de datos personales recae en los servidores públicos que laboran en la institución? |
| **12** | ¿Una parte del proceso de tratamiento de datos es llevada a cabo por un tercero (encargado de datos)? |
| **13** | ¿Las obligaciones de los participantes en el tratamiento de datos personales carecen de claridad o no están debidamente establecidas? |

| | |
|---|---|
| 14 | ¿El personal involucrado en el tratamiento de datos personales no tiene suficiente conocimiento sobre temas de seguridad de la información? |
| **15** | ¿Los participantes en el proceso de tratamiento de datos no almacenan y/o eliminan de manera segura los datos personales? |

Fuente: Elaborado por Ing. Kevin Locke

Este proceso detallado en la tabla 9, evalúa riesgos en seguridad de datos y privacidad en el departamento de TI del MIES 09D17 Milagro. Asigna niveles basados en probabilidad de amenazas, señalando áreas críticas que necesitan atención urgente. Esto guía decisiones informadas para proteger integridad y confidencialidad de datos, manteniendo el cumplimiento y confianza de los interesados. (Pazmiño, 2021)

El valor final es calculado en tres niveles:

**Tabla 10** Niveles de posibles amenazas

| NIVELES | DETALLES | PUNTUACIÓN |
|---|---|---|
| Bajo | Posibilidad reducida de que la amenaza se materialice. | 1 |
| Medio | Posibilidad moderada de que la amenaza se materialice. | 2 |
| Alto | Posibilidad elevada de que la amenaza se materialice. | 3 |

Fuente: Elaborado por Ing. Kevin Locke

**Tabla 11** Evaluar la posibilidad de amenazas

| # | PROCESO A EVALUAR | POSIBILIDAD DE OCURRIR | | |
|---|---|---|---|---|
| | | | NIVEL | PUNTUACIÓN |
| 1 | Infraestructura tecnológica (Red y recursos técnicos, como hardware y software). | | Bajo | 1 |
| | | | Medio | 2 |
| | | | Alto | 3 |
| 2 | El Departamento de TI se vincula en procesos del tratamiento de datos. | | Bajo | 1 |
| | | | Medio | 2 |
| | | | Alto | 3 |
| 3 | El personal que labora en el área de TI participa en el tratamiento de datos. | | Bajo | 1 |
| | | | Medio | 2 |

| | | | |
|---|---|---|---|
| | | Alto | 3 |

Fuente: Elaborado por Ing. Kevin Locke

La probabilidad de amenazas se calcula sumando las tres puntuaciones de las áreas específicas según la tabla 11. Esto se basa en la escala de probabilidad mostrada en la tabla 12.

**Tabla 12** Escala de posibilidades

| Niveles | Totales en Posibilidades |
|---|---|
| Bajo | 1 – 3 |
| Medio | 3 – 6 |
| Alto | 6 – 9 |

Fuente: Elaborado por Ing. Kevin Locke

**Matriz de Riesgo:** El valor del riesgo se vincula a la posibilidad de un evento negativo sin medidas. Se usa una matriz con datos previos para evaluar la situación de la información y decidir si es preciso aplicar control. Esto ayuda a reducir el riesgo y evitar efectos dañinos.

**Tabla 13** Matriz de Riesgos

| | | Niveles de Impacto | | |
|---|---|---|---|---|
| | | Bajo | Medio | Alto |
| Nivel de Posibilidad | Bajo | | | |
| | Medio | | | |
| | Alto | | | |

Fuente: Elaborado por Ing. Kevin Locke

Luego de identificar los riesgos y obtener el resultado final, la institución se ajusta al nivel de riesgo establecido, considerando detalles no evaluados previamente de los datos personales.

Es esencial que el departamento de TI del MIES 09D17 Milagro tome medidas para reducir los riesgos identificados y asegurar la seguridad y privacidad de los datos personales.

**Fase 2: Hacer. -** Como lo indica NQA. Durante esta etapa, se lleva a cabo la implementación de todo lo planificado. El Organismo de Certificación global NQA, (NQA, 2020).

- Evaluación de los Riesgos
- Seleccionar Medidas de Seguridades

**Evaluación del Riesgo:** Después de evaluar el impacto del procesamiento de datos y la probabilidad de las amenazas, se realiza la evaluación de riesgos para comprender y cuantificar de manera efectiva el riesgo involucrado en el tratamiento de los datos personales. Esto permite identificar áreas críticas, tomar decisiones informadas y aplicar medidas de mitigación para asegurar la protección de la información y el cumplimiento normativo. (Pazmiño, 2021)

La evaluación de riesgos abarca varias acciones:

- Detectar amenazas potenciales en todas las etapas del procesamiento de datos.
- Examinar los factores que influyen en el nivel de riesgo.
- Valorar el impacto y la magnitud del riesgo.
- Implementar medidas de control para reducir la probabilidad de impacto.

Esta fase se enfoca en identificar cuidadosamente amenazas que puedan afectar la gestión de datos personales y los derechos de las partes interesadas. La exploración detallada sienta las bases para proteger información sensible y salvaguardar la privacidad.

Las amenazas pueden afectar la confidencialidad, integridad y disponibilidad. Se considera su ciclo de vida y diversos escenarios donde pueden surgir vulneraciones.

Una vez identificado un riesgo, se detalla su origen y las acciones que lo desencadenarían, clasificándolo según su prioridad. La probabilidad de ocurrencia y las

consecuencias se analizan, y se recurre a una matriz de riesgos para entender y categorizar los riesgos en la empresa.

**Medidas de Seguridad:** Tras completar la evaluación del nivel de riesgo, el departamento de TI del MIES 09D17 Milagro elige las medidas de seguridad apropiadas, para proteger los datos personales, apoyándose en las pautas proporcionadas por las normas ISO 27001, 27002 y 27701.

**Tabla 14** Medidas de seguridad seleccionadas, analizando el nivel de riesgos

| CLASIFICACIÓN | DESCRIPCIÓN | MEDIDA DE SEGURIDAD PARA CADA RIESGO |
|---|---|---|
| Directrices de seguridad y protocolos para la salvaguardia de información personal. | La institución elaborará y documentará su enfoque hacia el procesamiento de datos personales como parte integral de su estrategia global de seguridad de la información. | BAJO |
| | La política de seguridad será objeto de evaluación y aprobación, si es necesario, en un ciclo anual. | BAJO |
| | La institución generará una política de seguridad específica dedicada al procesamiento de datos personales. Esta política obtendrá la aprobación de la alta dirección y se difundirá entre los empleados y entidades externas pertinentes. | ALTO |

| | | |
|---|---|---|
| | Se creará y mantendrá un inventario de políticas y procedimientos específicos relacionados con la seguridad de los datos personales, alineados con la política general de seguridad. | ALTO |
| Roles y deberes. | La política de seguridad será sometida a revisión semestral. | MEDIO |
| Directrices de acceso y supervisión. | La separación de funciones en el control de acceso está de manera clara definida y documentada. | MEDIO |
| | Los roles que tienen privilegios de acceso excesivos son específicamente identificados y asignados a un grupo limitado de empleados. | MEDIO |
| | La institución mantiene un registro detallado de los recursos de tecnología de la información empleados en el procesamiento de datos personales, incluyendo hardware, software y red. Este registro contiene información crucial como el tipo de recurso, su ubicación y la persona encargada. | ALTO |
| | Los recursos tecnológicos son sometidos a revisiones y actualizaciones en intervalos regulares. | MEDIO |
| | Los roles que tienen acceso a recursos particulares son establecidos y consignados en documentos oficiales. | BAJO |
| | Las actualizaciones de los recursos de tecnología de la información son llevadas a cabo en ciclos anuales. | MEDIO |
| Manejo de modificaciones. | La entidad garantiza que cualquier alteración en el sistema de tecnología de la información sea documentada y supervisada por un individuo designado, como un oficial de TI o seguridad. Este proceso es objeto de monitoreo regular. | MEDIO |

| | | |
|---|---|---|
| | El desarrollo de software se efectúa en un entorno de pruebas desconectado del sistema de TI principal. En situaciones donde las pruebas requieren datos, se emplean datos ficticios en lugar de datos reales. En circunstancias excepcionales, se implementan procedimientos específicos para resguardar la integridad de los datos personales empleados en las pruebas. | BAJO |
| | Una política exhaustiva y documentada sobre cambios está establecida. | MEDIO |
| Procesadores de datos | Se establecen y documentan normativas y procesos oficiales que abarcan el tratamiento de información personal por parte de procesadores de datos (ya sean contratistas o subcontratistas) en la relación entre el responsable de datos y el procesador de datos, antes de que las actividades de procesamiento comiencen. Estas directrices y procedimientos imponen la obligación de mantener el mismo nivel de seguridad para los datos personales que se establece en la política de seguridad de la organización. | ALTO |
| | En caso de descubrirse una infracción de datos personales, el procesador de datos informa al controlador de manera pronta y sin demoras indebidas. | ALTO |
| | La entidad a cargo de los datos realiza auditorías periódicas para verificar que el procesador de datos cumple con los requisitos y compromisos acordados. Los empleados encargados del procesamiento de datos personales están sujetos a acuerdos explícitos de confidencialidad y no divulgación, los cuales se encuentran debidamente documentados. | ALTO |
| Gestión de incidentes / infracciones de información personal. | Establecer un plan de acción en caso de incidentes que contemple procedimientos minuciosos para asegurar una respuesta organizada ante situaciones concernientes a datos personales. | ALTO |
| | Cualquier violación de datos personales se reporta de manera inmediata a la dirección ejecutiva. | ALTO |
| | Se registra por escrito el plan de actuación frente a incidentes, el cual contiene un inventario de medidas de mitigación posibles y una asignación precisa de responsabilidades. | MEDIO |

| | | |
|---|---|---|
| | Los incidentes y las infracciones de información personal son registrados, incluyendo información detallada sobre el suceso y las medidas de mitigación implementadas posteriormente. | ALTO |
| Planificación de la Continuidad del Negocio | La entidad define los procedimientos y medidas fundamentales para garantizar el nivel necesario de continuidad y disponibilidad del sistema de tecnología de la información que maneja datos personales, en situaciones de incidentes o violaciones de dicha información. | ALTO |
| | Un Plan de Continuidad del Negocio es minuciosamente elaborado y registrado, abarcando acciones específicas y asignación de responsabilidades de manera clara. | MEDIO |
| | En el Plan de Continuidad del Negocio se establece un nivel asegurado de calidad de servicio para las operaciones clave del negocio que salvaguarda la seguridad de la información personal. | MEDIO |
| | Nombrar individuos particulares con la capacidad, la autoridad y la experiencia requeridas para dirigir la continuidad operativa en situaciones de incidentes o violaciones de información personal. | ALTO |
| | Evaluar la posibilidad de contar con una ubicación de respaldo, de acuerdo a las necesidades de la organización y el período de tiempo admisible de inactividad del sistema de tecnología de la información. | MEDIO |
| Privacidad del personal | La entidad garantiza que cada uno de sus empleados tenga un entendimiento claro de sus deberes y compromisos en relación con el manejo de información personal. Las funciones y deberes son comunicados de manera explícita durante las fases previas al empleo y/o en el proceso de orientación. | ALTO |
| | Previo a la asunción de sus responsabilidades, se requiere que los empleados examinen y acepten la política de seguridad de la entidad, así como que suscriban los pertinentes acuerdos de confidencialidad y no divulgación. | ALTO |
| | Los trabajadores que participan en la manipulación de información personal de alto riesgo están sujetos a disposiciones de confidencialidad particulares, las cuales son establecidas en virtud de su contrato laboral u otros acuerdos legales. | MEDIO |

| | | |
|---|---|---|
| Capacitación | La entidad garantiza que todos sus empleados cuenten con información suficiente acerca de los controles de seguridad del sistema de Tecnologías de la Información (TI) que son relevantes para su labor cotidiana. Los trabajadores que se ocupan del tratamiento de datos personales igualmente son debidamente instruidos sobre los requisitos de protección de datos y las responsabilidades legales relevantes, mediante campañas periódicas de sensibilización. | ALTO |
| | Diseñar y llevar a cabo de manera anual un programa de formación con objetivos y metas claramente establecidos. | MEDIO |
| Administración de Acceso y Autenticación | Se establece un sistema de administración de acceso que se aplica a todos los usuarios que ingresan al sistema de Tecnologías de la Información (TI). Este sistema posibilita la creación, aprobación, revisión y eliminación de cuentas de usuario. | MEDIO |
| | Se evita el uso de cuentas de usuario duplicadas. Si es necesario, se asegura que los usuarios en categorías comunes tengan roles y responsabilidades uniformes. | MEDIO |
| | Para autenticación, se emplea un mecanismo que implica la combinación de un nombre de usuario y una contraseña. Las contraseñas cumplen con un nivel de complejidad específico. | MEDIO |
| | El sistema de gestión de acceso dispone de la capacidad de identificar y rechazar el uso de contraseñas que no cumplan con un nivel específico de complejidad. | MEDIO |
| | Se establece y documenta una política de contraseñas precisa. Esta política abarca, al menos, aspectos como la longitud de la contraseña, el nivel de complejidad requerido, el periodo de validez y el número de intentos fallidos de inicio de sesión que se consideran aceptables. | ALTO |
| | Las contraseñas de los usuarios se almacenan en forma de "hash". | ALTO |
| | Para acceder a sistemas que manejan información personal, se da preferencia al uso de autenticación de doble factor. Los componentes de autenticación incluyen elementos como contraseñas, tokens de seguridad, datos biométricos, entre otros. | ALTO |

| | | |
|---|---|---|
| Registro y Supervisión | Se activan los registros de actividad para cada aplicación empleada en el tratamiento de información personal. Estos registros contemplan todas las formas de acceso a los datos (consulta, modificación, eliminación). | MEDIO |
| | Los registros de actividad cuentan con sellos temporales y se resguardan adecuadamente para evitar manipulaciones y accesos no autorizados. | MEDIO |
| | Se documentan las acciones efectuadas por administradores y operadores del sistema, incluso cambios en los usuarios. | MEDIO |
| | Se prohíbe la opción de eliminar o alterar el contenido de los registros. El acceso a los registros queda registrado y también se realiza un monitoreo para detectar cualquier actividad anormal. | ALTO |
| | Un sistema de supervisión procesa los registros de actividad y elabora informes acerca del estado del sistema, además de emitir alertas en caso de ser necesario. | BAJO |
| Seguridad del Servidor y Base de Datos | Se establece la configuración de los servidores de bases de datos y aplicaciones de forma que operen bajo cuentas separadas, con privilegios mínimos de sistema operativo para garantizar un funcionamiento adecuado. | MEDIO |
| | Los servidores de bases de datos y aplicaciones se limitan a procesar únicamente los datos personales que son verdaderamente necesarios para su tratamiento. | MEDIO |
| | Se contempla la posibilidad de implementar soluciones de encriptación en archivos o registros específicos mediante el uso de software o hardware. | ALTO |
| | Se evalúa la viabilidad de cifrar las unidades de almacenamiento. | MEDIO |
| | Se emplean técnicas de seudonimización para separar los datos de los identificadores directos, con el fin de evitar la asociación con el interesado sin información adicional. | ALTO |
| | Se incorporan metodologías que respalden la privacidad en el nivel de la base de datos. | ALTO |
| Seguridad en las Estaciones de Trabajo | Los usuarios no tienen la capacidad de desactivar u omitir la configuración de seguridad. | MEDIO |
| | Las aplicaciones antivirus y las firmas de detección deberán configurarse semanalmente. | MEDIO |

| | | |
|---|---|---|
| | Los usuarios no deberán contar con privilegios para instalar o desactivar aplicaciones no autorizadas en los equipos de cómputo. | MEDIO |
| | El sistema cuenta con intervalos de tiempo de inactividad de sesión, los cuales se activan cuando el usuario no ha interactuado durante un lapso determinado. | MEDIO |
| | Se llevan a cabo actualizaciones periódicas de las parches de seguridad críticos proporcionados por el desarrollador del sistema operativo. | BAJO |
| | En las estaciones de trabajo se activa el cifrado completo del disco. | BAJO |
| | Cuando las estaciones de trabajo empleadas para el procesamiento de datos personales están conectadas a Internet, se implementan medidas de seguridad para prevenir el procesamiento, copiado y transferencia no autorizados de los datos almacenados. | ALTO |
| | La comunicación a través de Internet se asegura mediante protocolos criptográficos (TLS/SSL). | MEDIO |
| | El acceso inalámbrico al sistema de TI únicamente se permite para usuarios y procesos específicos, empleando mecanismos de encriptación como protección. | MEDIO |
| | Se limita el acceso remoto al sistema de TI. En los casos excepcionales donde esto es necesario, se ejecuta bajo el control y supervisión de un individuo designado de la organización. | BAJO |
| | El flujo de tráfico hacia y desde el sistema de TI se monitorea y regula mediante firewalls y Sistemas de Detección de Intrusos. | BAJO |
| | Los servidores y estaciones de trabajo utilizados para el tratamiento de datos personales no tienen permitida la conexión a Internet. | MEDIO |
| Respaldo de Datos | Los procedimientos relativos a la creación de copias de seguridad y la recuperación de datos se establecen, documentan y se conectan de manera clara con las funciones y responsabilidades correspondientes. | MEDIO |

| | | |
|---|---|---|
| | Se garantiza que las copias de seguridad reciban el nivel adecuado de seguridad física y ambiental, conforme a los estándares aplicados a los datos originales. Se supervisa el proceso de ejecución de las copias de seguridad para asegurar su plenitud. | MEDIO |
| | Se llevan a cabo copias de seguridad completas de manera regular. | BAJO |
| | Las copias de seguridad son almacenadas de manera segura en diversas ubicaciones. | MEDIO |
| | Se someten a pruebas periódicas los dispositivos de respaldo para confirmar su idoneidad para usos de emergencia. | BAJO |
| | Si se recurre a un servicio externo para el almacenamiento de copias de seguridad, estas son cifradas antes de ser transmitidas por el controlador de datos. | ALTO |
| | Las copias de las copias de seguridad son encriptadas y se almacenan de manera segura fuera de línea. | BAJO |
| Dispositivos Portátiles y Móviles | Los protocolos de administración de dispositivos móviles y portátiles son definidos y documentados, estableciendo pautas claras para su uso apropiado. | MEDIO |
| | Los procedimientos para la gestión de dispositivos móviles y portátiles están claramente especificados y registrados, estableciendo normativas precisas para su uso adecuado. | MEDIO |
| | Los dispositivos móviles están sujetos a los mismos niveles de procedimientos de control de acceso al sistema de procesamiento de datos que otros dispositivos terminales. | ALTO |
| | La organización realiza borrados remotos de los datos personales relacionados con sus operaciones de procesamiento en caso de que un dispositivo móvil se vea comprometido. | BAJO |
| | Los dispositivos móviles permiten la segregación entre el uso personal y empresarial a través de contenedores de software seguros. | ALTO |
| | Los dispositivos móviles cuentan con medidas de protección física contra robos cuando no se encuentran en uso. | ALTO |
| | La autenticación de doble factor se aplica para acceder a los dispositivos móviles. | ALTO |
| | Los datos personales almacenados en los dispositivos móviles son encriptados. | ALTO |

| | | |
|---|---|---|
| Seguridad a lo Largo del Ciclo de Vida de la Aplicación | Los requisitos específicos en cuanto a seguridad son establecidos en las fases iniciales del ciclo de desarrollo. | BAJO |
| | Se incorporan tecnologías y técnicas diseñadas para respaldar la privacidad y la protección de datos, conocidas como Tecnologías de Mejora de la Privacidad (PET), acorde a los requerimientos de seguridad. | ALTO |
| | Se siguen estándares y prácticas de codificación segura. | BAJO |
| | Durante el proceso de desarrollo, se efectúan pruebas y validaciones que evalúan la incorporación de los requisitos de seguridad iniciales. | BAJO |
| | Una entidad de confianza realiza evaluaciones de vulnerabilidad y pruebas de penetración en aplicaciones e infraestructuras antes de su adopción operativa. Solo se aprueba la implementación si se alcanza el nivel requerido de seguridad. | MEDIO |
| | Se ejecutan pruebas de penetración de manera regular. | BAJO |
| | Los parches de software son evaluados y probados antes de ser implementados en un entorno de operación. | BAJO |
| Eliminación de Datos | Se realiza la sobreescritura basada en software en todos los dispositivos de almacenamiento antes de su descarte. En situaciones en las que esto no sea viable (como en el caso de Nas, Discos Externos, USB, etc.), se opta por la destrucción física. | BAJO |
| | Se procede a la destrucción del papel y de los medios portátiles que han sido utilizados para guardar datos personales. | BAJO |
| | En el escenario en el que se recurra a los servicios de un tercero para llevar a cabo la eliminación segura de medios o registros en papel, se establece un acuerdo de servicio y se documenta el proceso de destrucción de registros. | BAJO |
| | Si se involucra a un tercero, que actúa como procesador de datos, para la eliminación de medios o documentos en papel, se garantiza que el proceso tenga lugar en las instalaciones del controlador de datos, evitando de esta manera la transferencia de datos personales fuera del sitio. | BAJO |

| | | |
|---|---|---|
| Seguridad Física | El acceso físico a la infraestructura del sistema de TI está restringido para el personal no autorizado. | BAJO |
| | Para aquellos que acceden a las instalaciones de la organización, se establece una identificación clara mediante medios apropiados, como tarjetas de identificación, conforme a las circunstancias. | BAJO |
| | Se delimitan zonas de seguridad y se aseguran mediante controles de acceso adecuados. | MEDIO |
| | Se implementan sistemas de detección de intrusos en todas las áreas de seguridad. | BAJO |
| | En el servidor, se instalan sistemas automáticos de extinción de incendios, sistemas de aire acondicionado con control cerrado y sistemas de alimentación ininterrumpida (UPS). | MEDIO |
| | El personal externo de los servicios de apoyo tiene acceso restringido a las zonas seguras. | MEDIO |

Fuente: Elaborado por Ing. Kevin Locke

**Fase 3: Verificar. -** Como lo indica NQA. Durante esta etapa, se lleva a cabo la verificación de lo implementado. El Organismo de Certificación global NQA, (NQA, 2020).

- Establecer medidas de seguridad

Posterior a la creación del modelo de SGSI para salvaguardar la información personal, se detectan los posibles peligros a los que la institución podría estar expuesta. Esto implica verificar las amenazas y vulnerabilidades a las que se enfrenta.

Para llevar a cabo esta verificación de amenazas y vulnerabilidades en el Departamento de TI del MIES 09D17 Milagro, se aplica el SGSI propuesto, para la protección de datos personales, previa aprobación y aceptación por parte de la junta directiva del MIESS 09D17 Milagro. Comprendido que el personal que labora en la institución participa en el tratamiento datos personales que permite realizar la

evaluación de los riesgos a los que se exponen los datos y determinar qué medidas de seguridad deben aplicarse.

Para utilizar el SGSI propuesto de manera efectiva, es necesario que el personal de Tecnologías de la Información (TI) supervise y revise todas las etapas descritas en la Figura 3. Una vez que el proceso se completa, la junta directiva evalúa que se hayan cumplido todas las descripciones y busca oportunidades de mejora.

Dando continuidad a lo mencionado previamente, se procede con implementación del SGSI propuesto, en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17. Para ello se utiliza la guía publicada por El Organismo de Certificación global NQA, (NAQ, 2020). ISO 27701:2019 que es una extensión de la ISO/IEC 27001 para gestionar datos personales.

**Situaciones de aplicación y enfoque del informe.**

Con este propósito, se han identificado diversas operaciones de procesamiento de datos que se realizan en el Departamento de TI vinculando a la Infraestructura tecnológica y el personal que labora en esta área.

Es importante destacar que los casos de uso se enfocan exclusivamente en medidas de seguridad y no tienen la intención de ofrecer análisis legales. Su objetivo principal es proporcionar una propuesta con ejemplos prácticos sin emitir ninguna opinión sobre la legalidad o el cumplimiento de operaciones específicas de procesamiento de datos.

**Evaluación del Departamento de TI del MIES 09D17 Milagro**

Las acciones de procesamiento de datos más habituales en el Departamento de TI son:

- Administración de Redes y Bases de Datos

En el ámbito de la gestión correspondiente al tratamiento de datos personales, estos son ingresados en el Sistema Integral de Información MIES “SIIMIES” en la que se almacena la información de la ciudadanía que hace uso de los servicios brindados por la institución.

Seguidamente de completar el registro de todos los datos requeridos a través de la interfaz web, esta información pasa a ser almacenada en la base de datos central.

Semanalmente, el responsable del departamento de TI elabora un reporte que incluye estadísticas relacionadas con la atención a usuarios realizada y el número de tickets que aún están por ser atendidos.

**Descripción de la acción de procesamiento y su contexto.**

La acción de procesamiento de datos se describe de la siguiente forma:

**Tabla 15** Operación de Procesamiento de datos en el Departamento de TI

| DATOS | TIPO DE DATO |
|---|---|
| Propósito del procesamiento | Administración de requerimiento (Registro de tickets) |
| Métodos de procesamiento | INTERNO |
| Receptor de los datos | INTERNO |
| Herramienta de procesamiento de datos utilizada | SIIMIES |
| **DATOS PERSONALES DEL REQUIRENTE** | |
| Nombre y Apellido<br>RUC/CI/Pasaporte<br>Nombre del solicitante o institución<br>Correo electrónico<br>Teléfono<br>Requerimiento | Datos personales procesados |
| **DATOS PERSONALES DEL ADMINISTRADOR DE LAS B/D** | |
| Nombre y Apellido<br>Cargo<br>Fecha del informe | Propósito del procesamiento |

Fuente: Elaborado por Ing. Kevin Locke

Usando la información adquirida de la acción de procesamiento y su entorno, se lleva a cabo una evaluación de los riesgos a los que están sujetos los datos. Estos datos

pueden enfrentar varios riesgos que ponen en peligro su integridad, confidencialidad y disponibilidad.

**Evaluación de impacto**

En la evaluación de impacto, el responsable de Tecnologías de la Información (TI), siguiendo la tabla 7 evalúa la pérdida de confidencialidad, integridad y disponibilidad de los datos personales. Esta evaluación revela que los datos proporcionados en la capacitación al personal no están seguros. Como resultado, se determina el nivel de impacto de los datos personales que se procesarán y se define el tratamiento necesario. Posteriormente, los resultados de esta evaluación son revisados con la alta dirección para tomar decisiones.

**Tabla 16** Evaluación del procesamiento de datos en el Departamento de TI

| # | EVALUACIÓN DE IMPACTO | | |
|---|---|---|---|
| 1 | CONFIDENCIALIDAD | MUY ALTO | 4 |
| 2 | INTEGRIDAD | MUY ALTO | 4 |
| 3 | DISPONIBILIDAD | MUY ALTO | 4 |
| EVALUACIÓN DE IMPACTO GENERAL | | MUY ALTO 12 | |

Fuente: Elaborado por Ing. Kevin Locke

**Disminución o pérdida de confidencialidad e integridad**

En el contexto de la operación de Operación de Procesamiento de datos en el Departamento de TI, se considera un riesgo **Muy Alto.** La carencia de privacidad y la preservación de la integridad de los datos pueden generar problemas importantes para la institución, incluyendo la posible divulgación no autorizada de información y alteraciones en los datos procesados.

**Disminución o pérdida de disponibilidad**

En el contexto de la gestión de recursos, la falta de disponibilidad se considera un riesgo **Muy Alto**. La eventual eliminación no autorizada de datos procesados conlleva problemas significativos y puede dañar la reputación de la institución.

La valoración global del impacto en los niveles de confidencialidad, integridad y disponibilidad se califica como **Muy Alto**.

**Evaluación de amenazas y vulnerabilidades**

Utilizando la tabla 12 que describe las amenazas potenciales y su evaluación de probabilidad, se lleva a cabo la determinación del grado de probabilidad de que estas amenazas ocurran.

**Tabla 17** Evaluación de amenazas y vulnerabilidades, en la Operación de Procesamiento de datos del Departamento de TI

| # | PRINCIPALES PROCESOS EVALUADOS | PRBABILIDAD DE CURRENCIA | |
|---|---|---|---|
| | | NIVEL | PUNTUACIÓN |
| 1 | Infraestructura tecnológica (Red y recursos técnicos, como hardware y software). | ALTO | 2 |
| 2 | El Departamento de TI se vincula en procesos del tratamiento de datos. | ALTO | 3 |
| 3 | El personal que labora en el área de TI participa en el tratamiento de datos. | ALTO | 3 |
| PROBABILIDAD GENERAL DE OCURRENCIA | | ALTO 8 | |

Fuente: Elaborado por Ing. Kevin Locke

**Red y recursos técnicos (Hardware y Software)**

Dado que el sistema está conectado a Internet y permite requerimientos externos, la probabilidad de que se produzcan amenazas es **Alto**.

**Procesos vinculados a la operación de tratamiento de datos**

Dado que el proceso de la aplicación externa no está bien definido con políticas internas establecidas para el procesamiento de datos personales, se considera que la probabilidad de que ocurran amenazas es **Alto**.

**Diferentes partes implicadas en la operación de procesamiento de datos**

La probabilidad de que se produzcan amenazas se califica como **Alta**, ya que la operación de procesamiento de datos está a cargo de varios implicados y reposa en una sola B/D externa lo que significa que la institución no tiene un control absoluto sobre los datos.

**Ámbito de actividad y nivel de procesamiento.**

La institución no ha implementado medidas de seguridad para protegerse contra posibles ataques cibernéticos, ya que la operación de procesamiento implica a un gran número de personas, lo que resulta en una probabilidad **Alta** de amenazas.

**Valoración de riesgos e implementación de medidas de seguridad**

Basándose en los resultados de la evaluación de impacto y la probabilidad de que ocurran amenazas, se efectúa la valoración de riesgos utilizando la matriz que se mencionó previamente en la tabla 13.

**Tabla 18** Valoración de riesgos e implementación de medidas de seguridad

| | | NIVEL DE IMPACTO | | |
|---|---|---|---|---|
| | | BAJO | MEDIO | ALTO |
| NIVEL DE PROBABILIDAD | BAJO | | | |
| | MEDIO | | | |
| | ALTO | | | X |

Fuente: Elaborado por Ing. Kevin Locke

La evaluación de riesgos en la administración del Departamento de Tecnologías de la Información arroja un nivel de riesgo elevado, lo que significa que no se han implementado medidas adecuadas para mitigar posibles riesgos.

**Propuesta de Controles de Seguridad, para Riesgos de Nivel Alto.**

**Tabla 19** Controles de seguridad Nivel Alto.

| CLASIFICACIÓN | DESCRIPCIÓN | MEDIDA ANTE RIESGOS |
|---|---|---|
| Política de seguridad y protocolos para salvaguardar información personal. | La política de seguridad experimenta una revisión cada seis meses. | 5. Directrices de seguridad |
| Deberes y obligaciones. | Las funciones y responsabilidades del encargado de seguridad están de forma nítida definidas y registradas por escrito. | 6.1.1 Funciones y obligaciones en seguridad de la información. |
| Directrices de acceso y seguridad. | Las funciones que tienen permisos de acceso excesivos se encuentran de manera precisa definidas y son asignadas exclusivamente a un número limitado de miembros específicos del personal. | 9.1.1 Directrices de acceso y control. |
| Administración de recursos y activos. | Los recursos de tecnología de la información se someten a una revisión y actualización anualmente. | 8. Administración de bienes o Activos. |

| | | |
|---|---|---|
| Procesadores de datos | Los funcionarios públicos que manejan información personal están vinculados a acuerdos concretos de confidencialidad y no divulgación que están registrados por escrito. | 15. Interacción con proveedores. |
| Manejo de situaciones imprevistas o infracciones de la información personal. | Se registra cualquier incidente o violación de información personal, incluyendo información detallada sobre el suceso y las medidas de corrección que se llevaron a cabo posteriormente. | 16. Administración de sucesos relacionados con la seguridad de la información. |
| Continuidad del negocio | Nombrar a individuos con la responsabilidad, capacidad y autoridad adecuadas para supervisar la continuidad del negocio en situaciones de incidentes o violaciones de información personal. | 17. Consideraciones de seguridad de la información en la administración de la continuidad empresarial. |
| | Evaluar la opción de un sitio de respaldo, de acuerdo con la estructura de la empresa y el período de tiempo tolerable de inactividad del sistema de tecnologías de la información. | 17.1 Continuidad en la protección de la información. |
| Confidencialidad del personal que labora en la institución | Los trabajadores que participan en el tratamiento de información personal de alto riesgo están vinculados por disposiciones de confidencialidad particulares, las cuales se establecen a través de su contrato laboral u otros instrumentos legales pertinentes. | 7. Seguridad relacionada con el personal. |
| Capacitación | Elaborar y llevar a cabo un programa de formación anual que incluya metas y objetivos concretos. | 7.2.2 Sensibilización, instrucción y formación sobre seguridad de la información. |
| Gestión de Acceso y verificación de identidad. | Se da preferencia a la utilización de la autenticación de dos factores al ingresar a sistemas que manejan información personal. Los elementos de autenticación incluyen contraseñas, tokens de seguridad, tokens secretos, datos biométricos, entre otros. | 9. Control de acceso |
| Protección del servidor y la base de datos. | Implementar métodos que fortalezcan la confidencialidad a nivel de la base de datos. | 12. Resguardo de las operaciones. |
| Protección de la terminal de trabajo. | Se encuentra activada la encriptación completa del disco en las terminales de trabajo. | 14.1 Exigencias de seguridad para los sistemas de información. |
| | Las estaciones de trabajo utilizadas para el procesamiento de datos personales conectadas a Internet, aplicar medidas de seguridad para evitar el procesamiento, la copia y la | 14.1 Normas de seguridad de los sistemas de información. |

| | | |
|---|---|---|
| | transferencia no autorizados de datos personales almacenados. | |
| Protección de la red y de la comunicación. | Evitar que los servidores y estaciones de trabajo respaldados, que se emplean para procesar información personal, tengan acceso a Internet. | 13. Protección de las comunicaciones. |
| Respaldo de datos que componen la información. | Las duplicaciones de las copias de seguridad son encriptadas y guardadas de manera segura sin conexión a la red. | 12.3 Respaldo de datos. |
| Dispositivos móviles o portátiles | Implementar la autenticación de dos factores para ingresar a los dispositivos móviles. | 6.2 Dispositivos utilizados para trabajo móvil y teletrabajo. |
| | La información personal guardada en los dispositivos móviles debe ser protegida mediante cifrado. | 6.2 Dispositivos empleados en la movilidad laboral y el trabajo a distancia. |
| Eliminación de datos | Si se emplea un tercero, es decir, un procesador de datos, para la eliminación de medios o documentos en papel, se entiende que el proceso se realiza en las instalaciones del responsable de los datos (con el propósito de evitar la transferencia de información personal fuera del lugar). | 8.3.2 Eliminación de dispositivos y<br>11.2.7 Proceso seguro de eliminación o reutilización de equipos. |

Fuente: Elaborado por Ing. Kevin Locke

Basándose en la matriz que se mencionó previamente en la tabla 13. Puede ser utilizada para la evaluación en riesgos de nivel medio.

**Tabla 20** Valoración de riesgos e implementación de medidas de seguridad

| | | NIVEL DE IMPACTO | | |
|---|---|---|---|---|
| | | BAJO | MEDIO | ALTO |
| NIVEL DE PROBABILIDAD | BAJO | | | |
| | MEDIO | | X | |
| | ALTO | | | |

Fuente: Elaborado por Ing. Kevin Locke

**Propuesta de Controles de Seguridad, para Riesgos de Nivel Medio.**

**Tabla 21** Controles de seguridad Nivel Medio.

| CLASIFICACIÓN | DESCRIPCIÓN | MEDIDA ANTE RIESGOS |
|---|---|---|
| | La organización elabora una política específica de seguridad para el manejo de información personal, la cual es aprobada por la dirección y compartida con todos los empleados y partes externas pertinentes. | 5. Directrices de seguridad |

| | | |
|---|---|---|
| Directrices de seguridad y métodos para salvaguardar información personal. | La política de seguridad incluye al menos lo siguiente: las tareas y obligaciones de los empleados, las medidas fundamentales técnicas y organizativas implementadas para proteger los datos personales, y las personas o entidades externas responsables del procesamiento de estos datos. | 5. Directrices de seguridad |
| | Establecer y actualizar un registro de políticas y procedimientos particulares relacionados con la protección de la información personal, siguiendo la política de seguridad general como referencia. | 5. Directrices de seguridad |
| Roles y obligaciones. | Establecer una identificación precisa de las personas encargadas de llevar a cabo funciones específicas de seguridad, lo que incluye la designación de un oficial de seguridad. | 6.1.1 Delegación de responsabilidades en cuanto a la seguridad de la información. |
| Directrices de acceso y control. | Una política de gestión de accesos se encuentra minuciosamente elaborada y registrada. En este documento, la organización establece las directrices adecuadas para el control de acceso, los privilegios de acceso y las limitaciones para funciones de usuario específicas en relación a los procesos y procedimientos relacionados con la información personal. | 9.1.1 Directrices de control de acceso. |
| | La separación de responsabilidades en el control de acceso se encuentra de manera precisa definida y registrada. | 9.1.1 Directrices de control de acceso. |
| Administración de recursos y activos. | Se establecen y registran los roles que cuentan con acceso a recursos específicos. | 8. Administración de recursos. |
| Manejo de transformaciones. | Se encuentra una política exhaustiva y registrada para gestionar cambios. | 12.1 Responsabilidades y procedimientos operativos. |
| Procesadores de datos | La organización que gestiona los datos lleva a cabo auditorías periódicas para verificar que el procesador de datos cumple con los requisitos y obligaciones establecidos. | 15.1 Protección de la información en las interacciones con proveedores. |
| Manejo de eventos o infracciones de información personal. | El plan de acción ante incidentes se encuentra registrado e incluye una lista de | 16.1 Gestión de incidentes de seguridad de la información y mejoras. |

| | | |
|---|---|---|
| | medidas posibles para reducir los daños. | |
| Continuidad del negocio | Un Plan de Continuidad del Negocio “BCP” está minuciosamente elaborado y registrado, incluyendo acciones bien definidas y asignación de responsabilidades. | 17.1 Continuidad en la seguridad de la información. |
| | En el Plan de Continuidad del Negocio (BCP), se establece un nivel de calidad de servicio que se garantiza para los procesos comerciales esenciales que aseguran la seguridad de los datos personales. | 17.1 Continuidad en la seguridad de la información. |
| Protección de la información personal. | Antes de comenzar sus labores, se pide a los trabajadores que revisen y acepten la política de seguridad de la empresa, así como que firmen los acuerdos de confidencialidad y no divulgación correspondientes. | 7. Seguridad relacionada con el personal. |
| Formación | La organización garantiza que todos sus empleados estén debidamente informados sobre los sistemas de seguridad de tecnología de la información que son relevantes para sus tareas diarias. Además, aquellos empleados que participan en el tratamiento de datos personales reciben información adecuada sobre los requisitos de protección de datos y las responsabilidades legales correspondientes a través de campañas periódicas de sensibilización. | 7.2.2 Sensibilización, educación y capacitación en seguridad de la información. |
| Supervisión de acceso y verificación de identidad. | Se establece y registra una política de contraseñas específica que abarca aspectos como la longitud de la contraseña, su complejidad, la duración de su validez, y el número permitido de intentos fallidos de inicio de sesión. | 9.4 Supervisión de entrada a sistemas y programas. |
| | Las contraseñas de los usuarios se guardan en forma cifrada utilizando una técnica de (hash). | 9.4.3 Administración de contraseñas de usuarios. |
| Registro y seguimiento. | Se registran las actividades realizadas por los administradores y operadores del sistema, como la incorporación, eliminación o modificación de usuarios. | 12.4 Registro de actividad y vigilancia. |
| | No permitir la capacidad de borrar o alterar el contenido de los registros. También, llevar un registro de acceso a los registros y realizar un seguimiento para | 12.4 Registro de actividad y control. |

| | | |
|---|---|---|
| | identificar cualquier actividad inusual. | |
| | Un sistema de supervisión analiza los registros y genera informes sobre la condición del sistema, además de emitir notificaciones en caso de posibles alertas. | 12.4 Registro de actividad y control. |
| Protección del servidor y de la base de datos. | Se contempla la utilización de soluciones de cifrado en archivos o registros particulares mediante la aplicación de software o hardware de encriptación. | 12.1 Obligaciones y normas de funcionamiento. |
| | Se evalúa la posibilidad de encriptar unidades de almacenamiento. | 10. Encriptación |
| | Utilizar métodos de seudonimización al desvincular los datos de las identificaciones directas para evitar la asociación con la persona en cuestión sin información adicional. | 10. Encriptación |
| Protección de la estación de trabajo. | Se aplican de forma regular las actualizaciones de seguridad esenciales lanzadas por el creador del sistema operativo. | 14. Adquisición, creación y mantenimiento de los sistemas de información. |
| Protección de la red y las comunicaciones. | La conectividad inalámbrica al sistema de tecnología de la información se restringe exclusivamente a usuarios y procesos particulares, y se garantiza mediante el uso de medidas de encriptación. | La conexión sin cables al sistema de tecnología de la información se limita a usuarios y procesos específicos, asegurándose a través del empleo de técnicas de encriptación. |
| | Se previene el acceso a distancia al sistema de tecnología de la información. En situaciones donde esto resulte imprescindible, se lleva a cabo bajo la supervisión y control de un individuo designado en la organización. | Se prohíbe el acceso remoto al sistema de tecnología de la información, salvo en casos necesarios que sean gestionados y supervisados por una persona específicamente asignada en la organización. |
| Respaldo de datos. | Las duplicaciones de seguridad se conservan de manera protegida en diversas localizaciones. | 12.3 Respaldo de datos. |
| | Se realizan pruebas periódicas en los dispositivos de respaldo para asegurarse de que sean fiables en situaciones de emergencia. 12.3 Respaldo de datos. | 12.3 Respaldo de datos. |
| | Si se recurre a un servicio externo para guardar las copias de seguridad, estas son encriptadas antes de su transmisión desde la entidad que gestiona los datos. | 12.3 Respaldo de datos. |
| | La organización elimina de manera remota los datos | 6.2 Equipos para movilidad y trabajo a distancia. |

| | | |
|---|---|---|
| | personales (vinculados a su proceso de tratamiento) de un dispositivo móvil que haya sido comprometido. | |
| Dispositivos móviles/portátiles | Los dispositivos móviles permiten la división entre el uso personal y profesional del dispositivo mediante la implementación de contenedores de software seguros. | 6.2 Equipos para movilidad y trabajo a distancia. |
| | Se toman medidas para asegurar la protección física de los dispositivos móviles cuando no están siendo utilizados, con el objetivo de prevenir robos. | 6.2 Equipos para movilidad y trabajo a distancia. |
| Protección a lo largo del ciclo de vida de la aplicación. | Se llevan a cabo evaluaciones de penetración de manera regular. | 12.6 Administración de vulnerabilidades técnicas y 14.2 Seguridad en los procedimientos de desarrollo y asistencia. |
| | Se someten los parches de software a pruebas y evaluaciones previas a su instalación en un ambiente de funcionamiento. | 12.6 Administración de vulnerabilidades técnicas y 14.2 Seguridad en los procedimientos de desarrollo y asistencia. |
| Eliminación de datos | Si se recurre a un proveedor externo para eliminar de manera segura los medios de almacenamiento o documentos en papel, se establece un acuerdo de servicio y se mantiene un registro de la destrucción de los registros. | 8.3.2 Deshacerse de los medios de almacenamiento" y "11.2.7 Retirar o reutilizar dispositivos de almacenamiento de manera segura. |
| Seguridad de las instalaciónes | Se asegura de que todo el personal y los visitantes que entren a las instalaciones de la organización estén debidamente identificados mediante métodos adecuados, como tarjetas de identificación, según sea necesario. | 11. Protección física y del entorno. |
| | Establecer áreas seguras y resguardarlas mediante medidas de acceso adecuadas. | 11.1 Zonas protegidas. |
| | Implementar sistemas de detección de intrusiones en todas las áreas seguras. | 11.1 Zonas protegidas. |
| | Instalar en el servidor un sistema automático de extinción de incendios, un sistema de aire acondicionado especializado de circuito cerrado y un sistema de suministro eléctrico ininterrumpido (UPS-BACKUP). | 11.1 Zonas protegidas. |
| | El personal externo del servicio de asistencia tiene limitado el acceso a las zonas protegidas. | 11. Protección física y medioambiental. |

Fuente: Elaborado por Ing. Kevin Locke

Basándose en la matriz que se mencionó previamente en la tabla 13. Puede ser utilizada para la evaluación en riesgos de nivel bajo.

**Tabla 22** Valoración de riesgos e implementación de medidas de seguridad

| | | NIVEL DE IMPACTO | | |
|---|---|---|---|---|
| | | BAJO | MEDIO | ALTO |
| NIVEL DE PROBABILIDAD | BAJO | X | | |
| | MEDIO | | | |
| | ALTO | | | |

Fuente: Elaborado por Ing. Kevin Locke

**Propuesta de Controles de Seguridad, para Riesgos de Nivel Bajo.**

**Tabla 23** Controles de seguridad Nivel bajo.

| CLASIFICACIÓN | DESCRIPCIÓN | MEDIDA ANTE RIESGOS |
|---|---|---|
| Directrices de seguridad y métodos para proteger la información personal. | La organización registra su política sobre el tratamiento de datos personales como una parte integral de su política de seguridad de la información. | 5.1.1 Directrices de seguridad de la información. |
| | La política de seguridad se somete a revisión y, si es necesario, se aprueba de forma anual. | "5.1.2 Evaluación de las directrices de seguridad de la información." |
| Obligaciones y roles. | Los roles y deberes vinculados al manejo de datos personales están definidos de manera evidente y asignados conforme a la política de seguridad. | 6.1.1 Roles y obligaciones en la seguridad de la información. |
| | Durante reestructuraciones internas, despidos o cambios en los empleos, se establecen de manera clara los procesos para revocar derechos y responsabilidades, así como los procedimientos de traspaso. | 6.1.1 Roles y obligaciones en la seguridad de la información.<br>6.1.2 División de responsabilidades. |
| Directrices de gestión de acceso. | Asignar permisos de control de acceso específicos a cada función que participe en el tratamiento de datos personales. | 9.1.1 Normativa de acceso y control. |
| Administración de recursos y bienes. | La organización mantiene un registro de los recursos informáticos empleados en el tratamiento de datos personales, que incluye hardware, software y la infraestructura de red. | 8.1.1 Registro de recursos. |
| | El registro contiene los detalles esenciales, como el tipo de recurso, su ubicación y la persona responsable. | 8.1.2 Titularidad de los recursos. |
| Manejo de modificaciones. | La organización garantiza que cualquier modificación en el sistema de tecnología de la información se registre y vigile bajo la supervisión de un | 12.1.1 Normas de funcionamiento registradas. |

| | | |
|---|---|---|
| | individuo designado, y se realiza una revisión periódica de este procedimiento. | |
| | El proceso de desarrollo de software se lleva a cabo en un entorno de pruebas que no tiene conexión con el sistema de tecnología de la información. En situaciones en las que sea indispensable realizar pruebas, se emplean datos ficticios en lugar de datos reales. Cuando esto no sea factible, se implementan procedimientos específicos para proteger los datos personales utilizados en las pruebas. | 12.1.4 Distinción de los entornos de desarrollo, prueba y funcionamiento. |
| Procesadores de datos | Se establecen y documentan pautas y procedimientos formales que abordan el manejo de datos personales por parte de los procesadores de datos (contratistas o subcontratistas) antes de que comiencen sus actividades de procesamiento. Estas directrices y procedimientos deben cumplir con el mismo nivel de seguridad de datos personales que se establece en la política de seguridad de la organización. | 15.1.1 Directrices de seguridad de la información para las relaciones con los proveedores. |
| | Cuando el procesador de datos toma conocimiento de una infracción de datos personales, informa al controlador de manera inmediata y sin retrasos injustificados. | 15.1.2 Considerar la seguridad en los contratos con proveedores. |
| Manejo de incidentes o violaciones de datos personales. | Establecer un plan de acción para responder a incidentes, que incluye procedimientos minuciosos para asegurar una gestión organizada de las situaciones relacionadas con datos personales. | 16.1.5 Manejo de incidentes de seguridad de la información. |
| | Las infracciones de datos personales se notifican de manera inmediata a la dirección superior. | 16.1.2 Notificación de sucesos de seguridad de la información. |
| Continuidad del negocio | La organización define los procedimientos y controles esenciales que deben aplicarse para garantizar el nivel necesario de continuidad y disponibilidad del sistema de tecnología de la información que maneja datos personales en caso de incidentes o violaciones de datos personales. | 17.1.1 Planificación de la continuidad de la seguridad de la información. |
| Privacidad de los empleados. | La organización garantiza que todos sus empleados tengan una | 7 Protección de los recursos. |

| | | |
|---|---|---|
| | comprensión completa de sus deberes y responsabilidades en lo que respecta al tratamiento de datos personales. Las funciones y responsabilidades se comunican de manera transparente durante el proceso de incorporación y orientación. | |
| Control de acceso y verificación de identidad. | Se instaura un sistema de control de acceso que es válido para todos los usuarios que ingresan al sistema de tecnología de la información. Este sistema posibilita la creación, autorización, revisión y eliminación de cuentas de usuario. | 9.1.1 Directrices de control de acceso. |
| | Se evita la utilización de cuentas de usuario duplicadas, y en situaciones necesarias, se asegura que todos los usuarios compartidos tengan roles y responsabilidades idénticos. | 9.2.2 Administración de los permisos otorgados a los usuarios. |
| | Un método de verificación consiste en emplear una combinación de nombre de usuario y contraseña, y las contraseñas deben cumplir con ciertos requisitos de complejidad. | 9.4.3 Administración de las contraseñas de los usuarios. |
| | El sistema de gestión de accesos puede identificar y bloquear el uso de contraseñas que no cumplan con ciertos criterios de complejidad. | 9.4.3 Administración de contraseñas de usuario. |
| Registro y supervisión de actividades. | Los registros se activan para cada aplicación que se emplea en el tratamiento de datos personales, abarcando todos los tipos de acceso a los datos, como visualización, modificación y eliminación. | 12.4.2 Salvaguarda de los registros de información. |
| | Los registros cuentan con un registro de tiempo y se resguardan de forma adecuada para evitar alteraciones y acceso no autorizado. | 12.4.2 Resguardo de los registros de información. |
| Seguridad del servidor y la base de datos. | Los servidores de bases de datos y aplicaciones se ajustan para operar mediante una cuenta separada con privilegios mínimos del sistema operativo para su correcto funcionamiento. | 12.1 Obligaciones y procesos operativos. |
| | Los servidores de bases de datos y aplicaciones únicamente gestionan los datos personales que son esenciales y necesarios para su procesamiento. | 12.1 Obligaciones y procesos operativos. |

| | | |
|---|---|---|
| Protección de las estaciones de trabajo. | Los usuarios no pueden deshabilitar ni evadir la configuración de seguridad. | 14.1.1 Evaluación y definición de los requisitos de seguridad. |
| | Se establece una configuración semanal para las aplicaciones antivirus y las firmas de detección. | 14.2 Protección en las etapas de desarrollo y asistencia. |
| | Los usuarios no poseen autorización para instalar o desinstalar aplicaciones no permitidas. | 14.2 Seguridad en los procedimientos de desarrollo y apoyo. |
| | El sistema establece lapsos de tiempo de inactividad de la sesión cuando el usuario no ha realizado ninguna acción durante un intervalo predefinido. | 14.1.1 Evaluación y definición de los requisitos de seguridad. |
| Protección de la red y las comunicaciones. | Cuando se accede a través de Internet, la comunicación se asegura mediante protocolos de cifrado criptográfico "TLS/SSL". | 13.1 Administración de la seguridad de las redes. |
| Respaldos de Seguridad | Los procedimientos para respaldar y recuperar datos se encuentran definidos, documentados y están claramente relacionados con las funciones y responsabilidades correspondientes. | 12.3.1 Respaldo de información. |
| | Las copias de seguridad están resguardadas con medidas de protección física y ambiental adecuadas, conforme a los estándares utilizados para proteger los datos originales. | 12.3 Respaldo de datos. |
| | Se supervisa el proceso de respaldo para asegurarse de su integridad. | 12.3 Respaldo de datos. |
| | Se efectúan respaldos integrales de forma periódica. | 12.3.1 Respaldo de información. |
| Hace referencia a dispositivos móviles o portátiles. | Los procedimientos para administrar dispositivos móviles y portátiles se encuentran claramente definidos y documentados, y establecen pautas precisas para su uso adecuado. | 6.2 Dispositivos utilizados para movilidad y trabajo remoto. |
| | Se registran y autorizan previamente los dispositivos móviles que tienen permiso para acceder al sistema de información. | 6.2 Dispositivos utilizados para movilidad y trabajo remoto. |
| | Los dispositivos móviles se someten a los mismos procedimientos de control de acceso que otros dispositivos terminales para acceder al sistema de procesamiento de datos. | 6.2 Dispositivos utilizados para movilidad y trabajo remoto. |
| Seguridad durante todo el ciclo de vida de la aplicación. | Se establecen los requisitos de seguridad específicos durante las | 14.2 Seguridad en los procesos de desarrollo y asistencia. |

| | | |
|---|---|---|
| | fases iniciales del ciclo de vida del desarrollo. | |
| | Métodos y procesos especiales. destinado a apoyar la privacidad y protección de datos (también técnica de amplificación Política de Privacidad "PET" adoptada de requerimientos de seguridad. | 12.6 Administración de vulnerabilidades técnicas |
| | Adherirse a estándares prácticas y codificación segura. | 14.2 Seguridad en los procesos de desarrollo y asistencia. |
| | En desarrollo si comprobar y comprobar Implementación de requisitos Seguridad inicial. | 12.6 Administración de vulnerabilidades técnicas |
| Eliminación de datos | cobertura basada en software Se ha hecho antes en todos los medios. Tíralos. en casos futuros Esto es imposible (Nas, Disco externo, USB, etc.) Lesión física. | 11.2.7. Reciclaje o eliminación segura Equipo Almacenamiento 8.3.2 Liquidación armadura |
| | papel roto y soporte portátil Almacenamiento de datos personales. | 11.2.7. Reciclaje o eliminación segura Equipo Almacenamiento 8.3.2 Liquidación armadura |
| Seguridad de instalaciones | Acceso físico a la infraestructura. Indisponibilidad de los sistemas informáticos. Personal no autorizado. | 11.1. Zonas seguras. |

Fuente: Elaborado por Ing. Kevin Locke

# CONCLUSIONES Y TRABAJO FUTURO

La revisión de la documentación relacionada con la seguridad de los datos personales, que se encuentra en el estado actual del conocimiento en las normas ISO 27001, 27002 y 27701, fortalece la comprensión necesaria para aplicar las políticas, controles y medidas de seguridad para la protección de datos personales en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17.

El análisis de la situación actual de la seguridad de los datos personales en la institución ayuda a identificar las deficiencias y posibles riesgos presentes en el Departamento de TI, para proyectar el seguimiento correspondiente y la mejora continua del SGSI propuesto en materia de protección de datos personales.

La utilización del SGSI, proporcionara las políticas y controles idóneos para la seguridad de los datos personales que contribuyen a la protección de la data en general almacenada en sus bases de datos principales, definiéndose como las medidas de seguridad adecuadas, apegadas a la ley y disposiciones gubernamentales.

La evaluación de los datos obtenidos a través de las metodologías aplicadas mediante el SGSI, resalta las amenazas potenciales que deben considerarse ante la posibilidad de pérdida de información personal, lo que afectaría la confidencialidad, disponibilidad e integridad de estos datos.

## RECOMENDACIONES

Es recomendable que la alta dirección del MIES 09D17 Milagro lleve a cabo programas de sensibilización para concienciar al personal sobre la importancia de la información que se maneja internamente, con el objetivo de promover una cultura que resalte la gravedad de exponer datos personales.

Se sugiere realizar auditorías de cumplimiento cada seis meses para verificar que se están siguiendo las medidas de seguridad establecidas en los controles de la norma ISO/IEC 2700:2022 sobre seguridad de la información, en relación a la protección de datos personales.

Se aconseja mantener planes de mejora e implementación de medidas y controles de seguridad en la utilización de recursos tecnológicos en general, así como planes de respuesta a incidentes, con el propósito de fortalecer la protección de los datos personales gestionados por parte del Ddepartamento de TI.

Se recomienda la implementación del SGSI basado en las normas ISO/IEC 27001, 27002 y 27701, orientada a la gestión de la seguridad de la información y la privacidad en las empresas.

# BIBLIOGRAFÍA GENERAL


ASAMBLEA NACIONAL DEL ECUADOR. (2021). *Asamblea Nacional República del Ecuador* . Obtenido de Repositorio Institucional: https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/920-lmoreno/ro-459-5to-sup-26-05-2021.pdf

AUDIT. (2021). *AUDIT*. Obtenido de LA HISTORIA DE LA NORMA ISO 27001 E ISO 27002: https://www.audit.pe/articles/art20210218.html

Ávila, A. (2023). *MODELO DE SGSI.* UNEMI, MILAGRO. Obtenido de https://repositorio.unemi.edu.ec/

Ayala, J. (2020). Diseño de Implementación en la red de una. *PROPUESTA METODOLOGICA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN ANTI-SOBORNO EN EMPRESAS DE SEGURIDAD PRIVADA EN GUAYAQUIL.* UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL, GUAYAQUIL. Obtenido de http://repositorio.ucsg.edu.ec/

Bastidas, M. (2017). *Análisis de la Infraestructura de Red.* UNEMI, MILAGRO. Obtenido de https://repositorio.unemi.edu.ec/

Briceño, E. V. (2021). *SEGURIDAD DE LA INFORMACIÓN.* Costa Rica. Obtenido de https://www.researchgate.net/publication/349925231_Seguridad_de_la_Informacion

cano, N. (2021). *Análisis sobre el consentimiento del titular bajo la Ley de Protección [Analisis Universidad San Francisco de Quito].* Repositorio Institucional. Obtenido de https://www.usfq.edu.ec/sites/default/files/2023-05/legallab-003.pdf

Carolina, M. P. (2021). *POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN.* UNEMI, Milagro. Obtenido de https://repositorio.unemi.edu.ec/

CEUPE. (2019). *CENTRO EUROPEO DE POSGRADOS*. Obtenido de CENTRO EUROPEO DE POSGRADOS: https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html

Cuero, J. (2018). EL LIBRE ACCESO A LA INFORMACIÓN EN LOS DATOS DE CARÁCTER PERSONAL. *EL LIBRE ACCESO A LA INFORMACIÓN EN LOS DATOS DE CARÁCTER PERSONAL.* UTMACH, MACHALA, ECUADOR. Obtenido de http://repositorio.utmachala.edu.ec/

ESCUELA EUROPEA DE LA EXCELENCIA. (2017). Anexo SL: Estructura común de las normas de Sistemas de Gestión. *Artículos Técnicos, Destacado, Sistemas de Gestión*. Obtenido de https://www.escuelaeuropeaexcelencia.com/

ESCUELA SUPERIOR DE REDES RED CEDIA. (2019). *Gestión del riesgo de las TI NTC 27005.* Obtenido de https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI9.pdf

Foro, Revista de Derecho. (2021). *Luis Enríquez Álvarez*. Obtenido de Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales: https://revistas.uasb.edu.ec/index.php/foro/article/view/500/2418#toc

Gómez, A. (2019). *ANÁLISIS DE LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA ANÁLISIS DE LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA HÍBRIDA SNAIL.* UTMACH, MACHALA, ECUADOR. Obtenido de http://repositorio.utmachala.edu.ec/

Grupo ESGinnova. (2023). *Grupo ESGinnova*. Obtenido de EL ciclo PHVA para la Mejora Continua de las organizaciones: https://www.isotools.us/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/

Hierro, H. (2019). INFLUENCIA DEL MARKETING DIGITAL EN LA FIDELIZACIÓN DE CLIENTES Y SU RELACIÓN CON EL TIEMPO DE VIDA DE LAS PYMES DE LA ZONA 5. *INFLUENCIA DEL MARKETING DIGITAL EN LA FIDELIZACIÓN DE CLIENTES Y SU RELACIÓN CON EL TIEMPO DE VIDA DE LAS PYMES DE LA ZONA 5.* UNEMI, MILAGRO, ECUADOR. Obtenido de https://repositorio.unemi.edu.ec/

IDEA CONSULTORES & ASESORES. (2022). *IDEA CONSULTORES & ASESORES*. Obtenido de ISO 27001: PILARES FUNDAMENTALES DE UN SGSI: https://ideacalidad.blogspot.com/2022/03/iso-27001-pilares-fundamentales-de-un.html

ingertec. (2018). *ingertec*. Obtenido de ISO/IEC 27701:2019: https://ingertec.com/iso-27701/

ISO Standards. (2023). *ISO Standards*. Obtenido de ISO Standards: https://www.iso.org/standard/iso-iec-27000-family

Juárez, J. (2020). ISO 27701:2019 Privacidad de la Información. *EQA*. Obtenido de https://docplayer.es/167369533-Iso-27701-2019-privacidad-de-la-informacion.html

Junaid, T.-S. (2023). Information Security Management.

Katerine, P. L. (2017). *AUDITORIA DE LA SEGURIDAD INFORMÁTICA BASADO EN LA.* UNEMI. Obtenido de https://repositorio.unemi.edu.ec/

Legislación y Leyes Nacionales. (2019). *Historia de la normativa reguladora de la Protección de Datos de carácter.* Revista Cientifica Dominio de las Ciencias. Obtenido de https://dialnet.unirioja.es/descarga/articulo/6869937.pdf

López, I. C. (2018). *"PROPUESTA DE IMPLEMENTACIÓN Y CUMPLIMIENTO DE LA LGPDPPSO A TRAVÉS DE LA PLATAFORMA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE INFOTEC" [MAESTRAS EN DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, INFOTEC MÉXICO].* Repositorio Institucional. Obtenido de https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/273/3/INFOTEC_MDTIC_ICGL_NML_24102019.pdf

Mendoza, M. (2022). APLICABILIDAD DE LA INVESTIGACIÓN CIENTÍFICA CON LAS TICS EN EL ÁREA DE CIENCIAS NATURALES PARA LOS ESTUDIANTES DE 5TO GRADO DE LA UNIDAD EDUCATIVA "LOS GUAYACANES", PERIODO 2021. *APLICABILIDAD DE LA INVESTIGACIÓN CIENTÍFICA CON LAS TICS EN EL ÁREA DE CIENCIAS NATURALES PARA LOS ESTUDIANTES DE 5TO GRADO DE LA UNIDAD EDUCATIVA "LOS GUAYACANES", PERIODO 2021.* UNEMI, MILAGRO, ECUADOR. Obtenido de https://repositorio.unemi.edu.ec/

MINTEL. (2021). *MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN.* Obtenido de MINISTERIO DE TELECOMUNICACIONES Y DE LA

SOCIEDAD DE LA INFORMACIÓN: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Murillo, D. (2021). *POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN NORMAS ISO 27002 PARA EL DEPARTAMENTO INFORMÁTICO DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ.* UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ, MANABI, ECUADOR. Obtenido de http://repositorio.unesum.edu.ec/

NACIONES UNIDAS. (2020). *Respuesta a la COVID-19*. Obtenido de Declaración conjunta sobre protección de datos y privacidad en la respuesta a la COVID-19: https://www.un.org/es/coronavirus/joint-statement-data-protection-and-privacy-covid-19-response

NAQ. (2020). *NQA*. Obtenido de ORGANIZMO DE CERTIFICACIÓN GLOBAL: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Neptali, P. (2019). MODELO DE GESTIÓN DE SEGURIDAD LÓGICA DE LA INFORMACIÓN EN LA PROTECCIÓN DE LOS DATOS SENSIBLES DE LOS DISTRITOS DE EDUCACIÓN DEL ECUADOR. *MODELO DE GESTIÓN DE SEGURIDAD LÓGICA DE LA INFORMACIÓN EN LA PROTECCIÓN DE LOS DATOS SENSIBLES DE LOS DISTRITOS DE EDUCACIÓN DEL ECUADOR.* UNIVERSIDAD TÉCNICA DE AMBATO, AMBATO, ECUADOR. Obtenido de https://repositorio.uta.edu.ec/

NQA. (2020). *NQA*. Obtenido de ISO 27001: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Ortega. (2022). *La protección de datos personales en la legislación ecuatoriana y su vulneración.* Universidad Católica de Cuenca. Obtenido de https://fipcaec.com/index.php/fipcaec/article/view/251/420

Pazmiño, F. (2021). PROPUESTA DE UN PLAN DE CONTINGENCIA PARA SALVAGUARDAR LOS ACTIVOS DE INFORMACIÓN EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA EMPRESA PÚBLICA MUNICIPAL DE RESIDUOS SÓLIDOS RUMIÑAHUI-ASEO EPM EMPLEANDO LA METODOLOGÍA MAGERIT. *PROPUESTA DE UN PLAN DE CONTINGENCIA PARA SALVAGUARDAR LOS ACTIVOS DE INFORMACIÓN EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA EMPRESA PÚBLICA MUNICIPAL DE RESIDUOS SÓLIDOS RUMIÑAHUI-ASEO EPM EMPLEANDO LA METODOLOGÍA MAGERIT.* UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO, QUITO, ECUADOR. Obtenido de https://dspace.ups.edu.ec/

Pilco, C. (2017). APLICACIÓN DE POLÍTICAS DE CRÉDITO Y COBRANZA EN EL COMERCIAL “GUAMAN” UBICADO EN EL CANTÓN MILAGRO. *APLICACIÓN DE POLÍTICAS DE CRÉDITO Y COBRANZA EN EL COMERCIAL “GUAMAN” UBICADO EN EL CANTÓN MILAGRO.* UNEMI, MILAGRO, ECUADOR. Obtenido de https://repositorio.unemi.edu.ec/

QAEC. (2021). *Blog AEC GOVERTIS*. Obtenido de [ECUADOR Y SU PRIMERA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES]: https://dpd.aec.es/ecuador-y-su-primera-ley-organica-de-proteccion-de-datos-personales/

Quimis, C. (2020). PERSPECTIVA DEL DERECHO INFORMÁTICO Y SU SITUACION ACTUAL EN EL ECUADOR. *PERSPECTIVA DEL DERECHO INFORMÁTICO Y SU SITUACION ACTUAL EN EL ECUADOR.* UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ, MANABI, ECUADOR. Obtenido de https://repositorio.unesum.edu.ec/

Registro Oficial Organico de la República del Ecuador. (2021). *Registro Oficial Organico de la República del Ecuador.* Obtenido de Registro Oficial Organico de la República del Ecuador: https://www.registroficial.gob.ec/

SÁNCHEZ, M. V. (2021). *DISEÑO DE UN MARCO DE TRABAJO PARA EL ANALISIS DE IMPACTO DEL PROYECTO DE LEY DE PROTECCIÓN DE DATOS EN EL ECUADOR EN EMPRESAS PRIVADAS [ESPOL].* Repositorio Institucional. Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/21820/1/CD%2011295.pdf

Tigse, J. (2020). PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A. *PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.* UNIVERSIDAD TÉCNICA DE AMBATO, AMBATO, ECUADOR. Obtenido de https://repositorio.uta.edu.ec/

Topacio, M. (2023). PLAN DE SEGURIDAD BASADO EN LA NORMA ISO 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LA TRONCAL PROVINCIA DEL CAÑAR. *PLAN DE SEGURIDAD BASADO EN LA NORMA ISO 27001 PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE LA TRONCAL PROVINCIA DEL CAÑAR.* UNEMI, MILAGRO, ECUADOR. Obtenido de https://repositorio.unemi.edu.ec/

Valenzuela, F. (2022). *PLAN ESTRATÉGICO DE CIBERSEGURIDAD.* UNEMI, MILAGRO. Obtenido de https://repositorio.unemi.edu.ec/

## ANEXO 1 PREGUNTAS DE LA ENTREVISTA

**Preguntas generales acerca del departamento**

¿Podría ofrecer una breve descripción de las funciones principales del Departamento de Tecnologías de la Información en MIES 09D17 Milagro?

¿Cuál es el volumen de datos que se maneja en este lugar y cuántos usuarios acceden a dichos datos?

¿Qué tecnologías se están utilizando en la actualidad en el Departamento de TI?

**Evaluación de la seguridad actual**

¿El departamento actualmente tiene alguna política o procedimiento establecido para la seguridad de la información?

¿Se han identificado previamente riesgos de seguridad o vulnerabilidades?

¿Existe algún registro o protocolo para dar seguimiento a incidentes de seguridad?

¿Cuáles son las principales amenazas a la seguridad de la información que el departamento enfrenta?

**Comprensión de ISO/IEC 27001**

¿Está familiarizado con la norma ISO/IEC 27001:2022?

¿Cuál es su opinión sobre la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en esta norma?

¿Se han tomado medidas previas para alinearse con alguna norma de seguridad de la información?

**Recursos y Limitaciones**

¿Qué recursos (humanos, financieros y tecnológicos) están disponibles en la actualidad para implementar un SGSI?

¿Cuáles son los principales obstáculos o limitaciones que prevé para la implementación de un SGSI?

**Compromiso y Apoyo Organizacional**

¿Qué nivel de respaldo espera recibir del liderazgo de la organización para la implementación de un SGSI?

¿Cómo se prioriza la seguridad de la información en comparación con otros objetivos del departamento o de la institución?

**Preguntas de Seguimiento y Futuras Acciones**

¿Está dispuesto a llevar a cabo una evaluación más detallada de las necesidades y riesgos de seguridad en el departamento?

¿Cuáles son los pasos inmediatos que considera necesarios para avanzar hacia una gestión más efectiva de la seguridad de la información?

**ANEXO 2 INFORME TÉCNICO**

# MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

# DIRECCION DISTRITAL 09D17 MIES MILAGRO

# AREA DE TICS

**INFORME DE NECESIDAD DE CONTRATACIÓN**

## OBJETO CONTRACTUAL

**Estudio de un Sistema de Gestión de Seguridad de la Información para establecer controles basados en la Norma ISO/IEC 27001:2022, para el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17**

**Milagro, 06 de septiembre de 2023**

| UNIDAD REQUIRENTE | TICS |
|---|---|

## 1. ANTECEDENTES

Los antecedentes del estudio en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17 están marcados por la creciente importancia de la seguridad de la información y la protección de datos en el entorno actual. Con la digitalización de los procesos y la proliferación de datos sensibles, las organizaciones se enfrentan a amenazas cada vez más sofisticadas en términos de ciberseguridad y privacidad. Estas preocupaciones han llevado al desarrollo de normas internacionales como ISO/IEC 27001:2022 e ISO 27701, que establecen directrices para la gestión de la seguridad de la información y la protección de datos a nivel global.

En este contexto, el departamento de Tecnologías de la Información en el Ministerio de Inclusión Económica y Social se ha convertido en un punto crítico para garantizar la integridad y confidencialidad de la información sensible. Sin embargo, la evaluación de la implementación de controles de seguridad y la adaptación a estándares internacionales pueden ser desafiantes. Estos antecedentes subrayan la necesidad de un estudio enfocado en este departamento para evaluar su estado actual en términos de seguridad de la información y protección de datos, y proponer un Modelo de SGSI que permita abordar de manera efectiva estos desafíos.

Además, es importante destacar que la dinámica en la seguridad cibernética y la privacidad de datos está en constante evolución. Los cambios en regulaciones y tecnologías, así como las nuevas amenazas emergentes, hacen que la gestión de la seguridad de la información sea un proceso continuo. Por lo tanto, este estudio no solo se basa en una necesidad actual, sino que también sienta las bases para una estrategia de mejora continua que asegure la protección y la integridad de los datos en el departamento a lo largo del tiempo.

## 2. JUSTIFICACIÓN

Para llevar a cabo este estudio en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17 es de suma importancia por diversas razones:

1. Evaluación de la seguridad de la información y protección de datos: En un mundo cada vez más digitalizado, la seguridad de la información y la protección de datos son aspectos críticos para garantizar la confidencialidad, integridad y disponibilidad de la información sensible. Este estudio permitirá evaluar el estado actual de estas áreas en el departamento y determinar si se cumplen las normas ISO/IEC 27001:2022 e ISO 27701, lo que es fundamental para el manejo adecuado de la información.

2. Propuesta de un Modelo de SGSI: La creación de un Modelo de Sistema de Gestión de Seguridad de la Información (SGSI) específico para este departamento ayudará a establecer directrices claras y efectivas para la gestión de la seguridad de la información. Esto contribuirá a minimizar riesgos, mejorar la eficiencia operativa y garantizar la continuidad del negocio.

3. Análisis de políticas y procedimientos: Evaluar la presencia de políticas y procedimientos alineados con estándares internacionales es esencial para identificar posibles brechas en la seguridad de la información. La implementación de políticas y procedimientos adecuados es la base de cualquier programa de seguridad de la información sólido.

4. Riesgos y consecuencias de una mala gestión: El análisis de los riesgos relacionados con la protección de datos y las posibles consecuencias de una gestión deficiente de la seguridad de la información ayudará a concienciar sobre la importancia de estas cuestiones y a tomar medidas preventivas para mitigar posibles incidentes.

Sin embargo, es importante destacar las limitaciones del estudio:

1. Accesibilidad a la información: La obtención de información precisa puede verse obstaculizada por la colaboración y accesibilidad a registros y sistemas del departamento, lo que podría afectar la calidad de los resultados.

2. Recursos limitados: La disponibilidad limitada de recursos, incluyendo personal, tiempo y presupuesto, puede influir en el alcance del estudio, lo que podría requerir la selección y priorización de aspectos específicos debido a estas limitaciones.

3. Aplicabilidad limitada: Dado que el estudio se enfoca en un departamento específico de una institución particular, los resultados y conclusiones pueden no ser completamente aplicables a otras instituciones o departamentos de Tecnologías de la Información, lo que limita su generalización.

4. Cambios en el entorno: Las modificaciones en regulaciones, tecnologías y el entorno empresarial pueden afectar la eficacia de los controles de seguridad, lo que significa que los resultados del estudio pueden volverse obsoletos con el tiempo.

5. Colaboración del personal: La colaboración y participación del personal del departamento de Tecnologías de la Información son cruciales para obtener información precisa. La falta de colaboración o resistencia del personal podría comprometer la validez de los resultados.

## 3. ALCANCE

Este estudio se enfoca únicamente en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17. Su propósito es evaluar la implementación de controles de seguridad conforme a las normas ISO/IEC 27001:2022 e ISO 27701 en el departamento y analizar la seguridad de la información y protección de datos, para proponer un Modelo de SGSI.

El estudio analizará la presencia de políticas y procedimientos conforme a los estándares, la ejecución de controles técnicos y organizativos, la formación del personal en seguridad de la información, y el cumplimiento normativo de la protección de datos. También evaluará los riesgos de la protección de datos y las consecuencias de una mala gestión de la seguridad de la información.

Las limitaciones incluyen:

La obtención de información puede verse limitada por la colaboración y accesibilidad a registros y sistemas del departamento de Tecnologías de la Información. La calidad y disponibilidad de los datos afectan la precisión y confiabilidad de los resultados.

Los recursos disponibles, incluyendo personal, tiempo y presupuesto, pueden restringir el alcance del estudio. Esto podría requerir la selección y priorización de aspectos específicos debido a las limitaciones de recursos y tiempo.

Debido a que el estudio se centra en un departamento específico de la institución, los resultados y conclusiones pueden no ser completamente aplicables a otras instituciones o departamentos de Tecnologías de la Información.

Las modificaciones en regulaciones, tecnologías y el entorno empresarial pueden afectar la eficacia de los controles de seguridad y el nivel de seguridad de la información. Estos cambios, que podrían estar fuera del alcance del estudio, posiblemente impacten en los resultados.

La colaboración y participación del personal que labora en el departamento de Tecnologías de la Información son esenciales para obtener información precisa y completa. La falta de colaboración o resistencia del personal puede comprometer la validez de los resultados obtenidos.

## 4. DESCRIPCIÓN DEL BIEN/SERVICIO SOLICITADO

**Servicio**

| N° | Descripción del servicio | CPC (nivel 9) | Descripción CPC | Unidad de Medida | Cantidad | Costo |
|---|---|---|---|---|---|---|
| 1 | **ESTUDIO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA ESTABLECER CONTROLES BASADOS EN LA NORMA ISO/IEC 27001:2022, PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL DE LA DIRECCIÓN DISTRITAL MILAGRO 09D17** | **831420211** | **PRESTACION DE ASESORAMIENTO Y ASISTENCIA EN CUESTIONES RELACIONADAS CON LOS PROGRAMAS DE INFORMATICA COMO LA REALIZACION DE ESTUDIOS DE VIABILIDAD SOBRE LA UTILIZACION DE UN SISTEMA** | u | 1 | $16.000 |

## 5. CAPACIDAD INSTITUCIONAL INSTALADA

No Aplica

## 6. ANÁLISIS BENEFICIO, EFICIENCIA O EFECTIVIDAD

**Se deberá establecer al menos uno de los siguientes análisis:**

### Análisis Beneficio

El análisis de beneficios de llevar a cabo el estudio en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17 revela una serie de ventajas significativas:

1. Mejora de la seguridad de la información: El estudio se centra en evaluar y mejorar la seguridad de la información y la protección de datos. Esto resulta en un beneficio fundamental, ya que reduce la exposición a riesgos de seguridad cibernética, filtraciones de datos y violaciones de la privacidad. La inversión en seguridad de la información es una medida proactiva para proteger la integridad y confidencialidad de los datos sensibles.

2. Cumplimiento normativo: Al evaluar la implementación de controles de seguridad conforme a las normas ISO/IEC 27001:2022 e ISO 27701, el estudio contribuye al cumplimiento normativo. Esto es esencial para evitar posibles sanciones legales y garantizar que la organización opere de acuerdo con las regulaciones de seguridad de la información y privacidad de datos vigentes.

3. Reducción de riesgos y consecuencias: El análisis de los riesgos y las posibles consecuencias de una mala gestión de la seguridad de la información permite a la organización identificar y mitigar amenazas potenciales. Esto disminuye la probabilidad de incidentes costosos, como violaciones de datos, y minimiza el impacto financiero y reputacional en caso de que ocurran.

4. Eficiencia operativa: La propuesta de un Modelo de SGSI específico para el departamento proporciona un marco claro para la gestión de la seguridad de la información. Esto puede aumentar la eficiencia operativa al estandarizar procesos y procedimientos, lo que a su vez reduce los tiempos de respuesta a incidentes y mejora la toma de decisiones.

5. Concienciación y cultura de seguridad: El estudio también tiene el beneficio de aumentar la concienciación y promover una cultura de seguridad entre el personal del departamento de Tecnologías de la Información. Esto lleva a una mayor responsabilidad y cuidado en el manejo de la información, lo que a largo plazo contribuye a una organización más segura.

6. Optimización de recursos: A pesar de las limitaciones de recursos, el estudio permite identificar áreas críticas que requieren atención prioritaria. Esto optimiza el uso de recursos disponibles al enfocarse en las áreas de mayor riesgo o vulnerabilidad.

7. Sostenibilidad a largo plazo: La mejora de la seguridad de la información y la protección de datos no es solo un beneficio a corto plazo, sino que también asegura la sostenibilidad a largo plazo de la organización al reducir el riesgo de interrupciones costosas y daños a la reputación.

**Análisis Eficiencia**

El análisis de eficiencia de llevar a cabo el estudio en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17 implica examinar cómo este proceso puede ser realizado de manera efectiva y rentable. Aquí están los puntos clave:

1. Optimización de recursos: A pesar de las limitaciones de recursos mencionadas en la justificación, el estudio busca maximizar la utilización eficiente de estos recursos. Al enfocarse en áreas críticas y prioritarias, se evita el desperdicio de recursos en aspectos menos relevantes y se garantiza que cada recurso disponible se utilice de manera efectiva.

2. Reducción de costos a largo plazo: Aunque la inversión inicial para llevar a cabo el estudio puede ser significativa, los beneficios a largo plazo superan los costos. La mejora de la seguridad de la información y la prevención de incidentes de seguridad cibernética pueden evitar gastos considerables asociados con la recuperación después de un ataque o una violación de datos.

3. Eficiencia operativa: Al proponer un Modelo de SGSI, el estudio establece una estructura que facilita la gestión de la seguridad de la información. Esto puede conducir a una mayor eficiencia operativa al estandarizar procesos y procedimientos, lo que ahorra tiempo y recursos a lo largo del tiempo.

4. Enfoque en áreas de alto riesgo: La identificación y mitigación de riesgos a través del estudio permiten que el departamento se centre en áreas de alto riesgo. Esto garantiza que los recursos se dirijan a los aspectos más críticos de la seguridad de la información, lo que aumenta la eficiencia al abordar las amenazas más significativas primero.

5. Concienciación y capacitación: El estudio también puede mejorar la eficiencia al aumentar la concienciación y la capacitación del personal en seguridad de la información. Un personal bien informado y capacitado es más eficiente en la detección y prevención de amenazas, reduciendo así la necesidad de recursos para abordar incidentes.

6. Mejora continua: La implementación de un Modelo de SGSI implica una filosofía de mejora continua. A través de la retroalimentación y la adaptación constante a las nuevas amenazas y regulaciones, la organización puede mantener su eficiencia en la gestión de la seguridad de la información a lo largo del tiempo.

7. Reducción de interrupciones: Al mitigar los riesgos de seguridad, el estudio puede evitar interrupciones costosas en las operaciones del departamento. Esto es especialmente importante en un entorno donde la continuidad del negocio es esencial.

**Análisis Efectividad**

El análisis de efectividad se centra en evaluar cómo llevar a cabo el estudio en el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17 es capaz de lograr sus objetivos y producir resultados significativos. Aquí se destacan los aspectos clave relacionados con la efectividad:

1. Cumplimiento de objetivos: El estudio tiene un objetivo claro de evaluar la implementación de controles de seguridad conforme a las normas ISO/IEC 27001:2022 e ISO 27701, analizar la seguridad de la información y protección de datos, y proponer un Modelo de SGSI. La efectividad se mide en términos de si estos objetivos se cumplen de manera satisfactoria.

2. Mejora de la seguridad: La efectividad del estudio se refleja en su capacidad para mejorar la seguridad de la información y la protección de datos en el departamento. Si el estudio identifica deficiencias y debilidades en estos aspectos y propone soluciones efectivas, entonces se considera efectivo en su propósito principal.

3. Reducción de riesgos: La efectividad del estudio se evalúa en términos de su capacidad para identificar, evaluar y mitigar los riesgos de seguridad de la información. Si las recomendaciones y acciones propuestas ayudan a reducir significativamente estos riesgos, entonces el estudio es efectivo en la gestión de la seguridad.

4. Concienciación y capacitación: Un aspecto fundamental de la efectividad es su capacidad para aumentar la concienciación y la capacitación del personal en seguridad de la información. Si el estudio logra que el personal comprenda y adopte prácticas más seguras, es considerado efectivo en la promoción de una cultura de seguridad.

5. Adopción de estándares internacionales: La efectividad se mide en términos de si el departamento puede adoptar y mantener estándares internacionales, como ISO/IEC 27001:2022 e ISO 27701, después de la implementación de las recomendaciones del estudio.

6. Mejora continua: La efectividad también se relaciona con la capacidad del estudio para promover la mejora continua en la gestión de la seguridad de la información. Esto implica la adaptación a cambios en las amenazas cibernéticas, regulaciones y tecnologías en curso.

7. Evaluación de resultados a largo plazo: La verdadera efectividad del estudio se evalúa a lo largo del tiempo, midiendo la sostenibilidad de las mejoras y la capacidad del departamento para mantener un nivel adecuado de seguridad de la información a medida que evolucionan las circunstancias.

8. Rendición de cuentas y responsabilidad: La efectividad también está vinculada a la rendición de cuentas. Si el estudio identifica áreas de responsabilidad y supervisión, y se establecen mecanismos para garantizar la ejecución de acciones correctivas, se considera efectivo en la gestión de la seguridad.

## 7. CONCLUSIÓN

En base al análisis previo sustentos técnicos y legales, se determina que es necesario/a la/el "Estudio de un Sistema de Gestión de Seguridad de la Información para establecer controles basados en la Norma ISO/IEC 27001:2022, para el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17".

## 8. RECOMENDACIÓN

Finalmente se recomienda continuar con los trámites administrativos necesarios, para efectuar el proceso de contratación pública correspondiente a "Estudio de un Sistema de Gestión de Seguridad de la Información para establecer controles basados en la Norma ISO/IEC 27001:2022, para el departamento de Tecnologías de la Información del Ministerio de Inclusión Económica y Social de la Dirección Distrital Milagro 09D17".

## 9. FIRMAS DE RESPONSABILIDAD

| ELABORADO POR: | CARGO | FIRMA |
|---|---|---|
| | | |
| **REVISADO POR:** | **CARGO** | **FIRMA** |
| | | |
| **APROBADO POR:** | **CARGO** | **FIRMA** |
| . | | |