ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

“Propuesta de mejora para la Gestión de Seguridad de la Información SGSI bajo normas ISO 27001, para el Departamento de Análisis de Telecomunicaciones de la Unidad Nacional de Telecomunicación Móvil” (Quito - Ecuador)

Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autores:
Bach. Falcón Huallpa, Elida
Bach. Martínez Zambrano, Erik Javier

Docente Guía:
Mtro. Valderrama Herrera, Roberto Marcelo

TACNA – PERÚ

2022

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del autor”

DEDICATORIA

Dedico este proyecto a Dios por darme la fuerza para poder concluir esta meta, a mi esposa e hija, quien han estado a mi lado todo este tiempo en que se ha realizado este proyecto, a mis padres que desde el cielo me cuidan y guían en cada paso y a todos los que me ayudaron y brindaron su apoyo y consejo para lograr superarme en cada momento.

Erik

DEDICATORIA

Dedico este trabajo a Dios, a mi familia. A mi hijo Annibal que con cada palabra de aliento me muestra el camino que vamos recorriendo juntos, a mis hermanos y a mis hermanas Miriam Liz y Rina gracias por estar ahí.

Elida

AGRADECIMIENTOS

El agradecimiento de este proyecto va dirigido primero a Dios ya que con su bendición nos permitió desarrollar este proyecto, a mi esposa y mi hija que son un pilar fundamental en mi vida, a mis padres que siempre me inculcaron a enfrentar cada obstáculo y seguir superándome.

A mis estimados tutores, que gracias a ustedes me he permitido alcanzar una nueva meta, a través de sus conocimientos y buenas prácticas de enseñanza y a la Escuela de Posgrado Newman que me permitió alcanzar una meta más en mi vida y de igual manera ser un miembro más de su prestigiosa Institución.

Erik

AGRADECIMIENTOS

Agradezco a Dios y la vida, por permitirme terminar este nuevo proyecto, a mi Familia por estar siempre conmigo, a mi hijo porque mucho de este trabajo tiene el tiempo que deje de estar contigo mi campeón.

A mis Docentes de la Maestría en Gestión de Tecnologías de Información de la Escuela de Posgrado Newman por la paciencia, dedicación que nos brindaron.

A la Escuela de Posgrado Newman, por permitirme ser parte de esta gran familia de profesionales, me llena de mucho orgullo y satisfacción.

Elida

ÍNDICE DE CONTENIDOS

ÍNDICE DE LAS TABLAS

ÍNDICE DE LAS ILUSTRACIONES

SIGLAS

SGSI : Sistema de Gestión de Seguridad de la Información

UNATEM : Unidad Nacional de Telecomunicación Móvil

DAT : Departamento de Análisis de Telecomunicaciones

EGSI : Esquema Gubernamental de Seguridad de la Información

GT : Gestión de Tecnología

ISO : International Organización for Standardization

SGC : Sistema de Gestión de la Calidad

RESUMEN

El manejo de la información reservada y confidencial dentro de las entidades Gubernamentales del Estado Ecuatoriano hace prioritario implementar procedimientos de seguridad en el manejo de la información que permita llevar un mejor control, para ello se cuenta con el Sistema de Gestión de Seguridad de la Información (SGSI) basado en la normativa ISO 27001, consideramos que dichas herramientas permiten un adecuado control en el manejo, integridad y resguardo de la información, se ha visto en los últimos años ataques cibernéticos constantes que perjudican la labor en las Entidades del Estado Ecuatorianos. Esta Propuesta de mejora para la Gestión de Seguridad de la Información SGSI bajo normas ISO 27001, en el Departamento de la Unidad Nacional de Telecomunicación Móvil - UNATEM (Quito - Ecuador), tiene como fin el de resguardar la privacidad, integridad y disponibilidad de la información, para ello se utilizará una metodología que se apoya en un modelo FODA, mismo que proporciona a través de métodos sistemáticos el análisis de amenazas derivadas de la implementación de tecnologías, de igual manera un enfoque PHVA, el cual permite gestionar los riesgos para lograr determinar las modificaciones en los procesos que presenten inconvenientes (planificar, hacer, comprobar y mejorar). De esta manera vamos a poder obtener en una primera instancia un diagnóstico de la información y datos que tenemos y generamos dentro del Departamento de Análisis de Telecomunicaciones de la UNATEM, misma que se acogerá a la propuesta diseñada dentro de los parámetros de seguridad y normativa legal vigente.

Palabras claves: Normativa ISO 27001, Sistemas de Gestión de Seguridad de la Información.

ABSTRACT

The management of reserved and confidential information within the Government entities of the Ecuadorian State makes it a priority to implement security procedures in the management of information that allows better control, that is why there is the Information Security Management System (SGSI) based on the ISO 27001 standard, we believe that these tools allow adequate control in the management, integrity and protection of information, constant cyber attacks have been seen in recent years that harm the work of Ecuadorian State Entities. This Improvement Proposal for ISMS Information Security Management under ISO 27001 standards, in Unidad Nacional de Telecomunicaciones-UNATEM(Quito, Ecuador), has the purpose of protecting the privacy, integrity and availability of information, for this a methodology that is based on a SWOT model will be used, which provides through systematic methods the analysis of threats derived from the implementation of technologies, In the same way, a PDCA approach, which allows managing risks to determine the modifications in the processes that present inconveniences (plan, do, check and improve). In this way, we will be able to obtain, in the first instance, a diagnosis of the information and data that we have and generate within the Unidad Nacional de Telecomunicaciones of UNATEM, which will adhere to the proposal designed within the parameters of security and current legal regulations.

Keywords: Normative ISO 27001, Information Security Management Systems.

INTRODUCCIÓN

En la actualidad las Instituciones Gubernamentales del Estado Ecuatoriano, manejan su información de manera reservada utilizando tecnologías digitales con el fin de hacer uso de las nuevas tecnologías vigentes, se viene desarrollando en todas las Instituciones del Estado la implementación de Sistemas Informáticos (SI), de esta manera las Instituciones tendrán un mejor control, fácil transmisión y acceso a la información. Viendo el crecimiento de las nuevas tecnologías en el manejo de la información se prevé la implementación de procedimientos que permitan el manejo eficiente de la información en las instituciones del Estado Ecuatoriano, de tal manera que se implemente controles en la privacidad, seguridad probidad y disponibilidad del SI que permita descubrir riesgos o vulnerabilidad, mismos que se pueden presentar a nivel de software o hardware. Eventos de ese tipo se determinarán como amenazas, basados en el plagio, manipulación de Información en las Instituciones Gubernamentales con fines ilícitos y sin previa autorización judicial, hay que destacar que los SI permitirán un control permanente.

Para esto el Estado Ecuatoriano a través del Ministerio de Telecomunicaciones ha visto necesario expedir el “Esquema Gubernamental de Seguridad de la Información – EGSI, el cual será implementado de manera obligatorio dentro de las Instituciones de Administración Pública central, Institucional y que dependa de la Función Ejecutiva”.

En referencia a esto el Departamento de Análisis de Telecomunicaciones de la UNATEM (Quito - Ecuador), ha visto la

necesidad de adquirir infraestructura que permite y ayuda a la gestión interna de manejo de información que permita dar cumplimiento a las diligencias investigativas solicitadas a través de SI por parte de la Función Judicial dentro del eje investigativo del Estado, viendo esta perspectiva, es imperioso el desarrollo de una propuesta de implementación de SGSI sustentada en la Normativa ISO 27001, misma que permitirá a la Unidad determinar los riesgos a presentarse y los cuales pueden ser mitigados con la información presentada dentro de los Sistemas de Información que maneja.

CAPÍTULO I: ANTECEDENTES DE ESTUDIO

1. Título del Tema

Propuesta de mejora para la Gestión de Seguridad de la Información SGSI bajo normas ISO 27001, para el Departamento de Análisis de Tecnología de la Unidad Nacional de Telecomunicación Móvil (UNATEM - Ecuador 2023).

2. Planteamiento del Problema

En la actualidad es importante el manejo, resguardo de la información en toda institución se a esta pública o privada, es importante la seguridad de la información de esta manera se asegura un manejo correcto de la información en cuanto a la confidencialidad, integridad y disponibilidad de ella.

En la Constitución de la república del Ecuador se presenta y garantiza dentro del Art. 66 # 19 que las personas: “El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección”.

Es por ello que el SGSI se presenta como “un proceso integrado que permite proteger la identificación y gestión de la información y los riesgos a los que esta se puede ver enfrentada”, este proceso de gestión nos va a permitir a través de estrategias y operaciones que permitirán el aseguramiento y compartimentación de la información que se desarrolla dentro de las instalaciones sean públicas o privadas.

Es así que a través de la seguridad de la información podremos manejar de manera eficiente los datos que se manejan dentro de las dependencias del Estado obteniendo: disponibilidad, comunicación, identificación de problemas, análisis de riesgos, integridad, confidencialidad y recuperación de riesgos. Por

lo antes expuesto es preciso orientar y proponer la implementación de SGSI dentro de los departamentos que conforman la Unidad Nacional de Telecomunicación Móvil (UNATEM) y sus obligaciones con las otras dependencias gubernamentales.

En el Ecuador a partir del 15 de abril de 2019 entra en vigencia a través del Acuerdo Ministerial 025-2019, se presenta el “Esquema Gubernamental de Seguridad de la Información (EGSI)”, mismo que debe ser implementado de manera obligatoria dentro del sector público en la Administración Pública, Institucional y que dependen de la Función Ejecutiva.

La implementación de este esquema gubernamental de seguridad de información EGSI, se ha venido realizando de una manera muy pausada por parte de las instituciones gubernamentales, es así que se han presentado diferentes ataques y externos y pérdida de información por no prever e implementar este tipo de gestiones para mejorar la seguridad de la información.

En la actualidad podemos encontrar que todavía existe falencias dentro del manejo de información de las diferentes dependencias del Estado, esto producto de varias factores como pueden ser por desconocimiento, miedo al cambio, presupuesto entre otros; con estos antecedes, queremos demostrar que con la adecuada capacitación y guía se implementaría un mejor y más seguro manejo de la información que produce dentro de la Unidad, ya que al ser una información sumamente importante dentro del Componente de investigación e infracción y del Subsistema de Investigación y de la Fiscalía General de Estado, hay que tener muy en cuenta la implementación de todas las normativas, reglas de seguridad y protocolos, que nos permitan mantener la información de manera confidencial, organizada y con la mayor integridad y

disponibilidad cuando sea solicitada por la entidad gubernamental legalmente acreditada.

3. Objetivos de la Investigación

3.1 Objetivo General

Formular una propuesta de mejora para la Gestión de Seguridad de la Información SGSI bajo normas ISO 27001 del Departamento de Análisis de Telecomunicaciones de la Unidad Nacional de Telecomunicación Móvil (UNATEM - Ecuador 2023)

3.2 Objetivos Específicos

- Diagnosticar los puntos críticos del flujo, almacenamiento y despacho de la información que se genera dentro del Departamento de Análisis de Telecomunicaciones.
- Plantear una mejora en el flujo, almacenamiento y despacho de la información, a través de la implementación de políticas de manejo de información.
- Diseñar un software que permita controlar el flujo de información que se maneja en las Instituciones del Estado, con el fin de optimizar el manejo de información de manera digital, implementando funcionalidad en el uso de cero papeles para el Departamento de Análisis de Telecomunicaciones.
- Determinar el costo beneficio de la implementación de los procesos que permitirá mejorar los tiempos de entrega de información y ahorro en suministros de oficina (papel, impresiones, CD).
- Identificar las posibles zonas de riesgos por las cuales se pueden

presentar ataques o mal manejo de información, para implementar el (SGSI) en el Departamento de Análisis de Telecomunicaciones de la UNATEM.

- Proponer procesos que mejoren todos los puntos críticos del Departamento de Análisis de Telecomunicaciones de la UNATEM, para la implementación de un-Sistema de Gestión de Seguridad de la Información (SGSI).

4. Metodología

En la propuesta presentada para la implementación de Sistema de Gestión Seguridad de Información (SGSI), se va a tomar como parámetro principal las equivocaciones presentadas dentro del manejo de información, almacenaje, con el fin de presentar y mantener la integridad de la misma con el fin de presentar una información que permita cumplir con los requerimientos legales solicitados por la entidad gubernamental acreditada (MINTEL-ARCOTEL), para esto utilizaremos la metodología de análisis de gestión de riesgos de los sistemas de información como lo es (MAGERIT), esta metodología nos permitirá alcanzar nuestros objetivos propuestos, a través de un método sistemático con el fin de implementar y llevar un mejor control para identificar responsabilidades en el desempeño laboral, riesgos existentes, manejo de información sensible y reservada, riesgos que deben ser minimizados a través de medidas de seguridad que generarán confianza, para el Departamento de Análisis de Telecomunicaciones de la UNATEM. (Magazine, 2023)

Existen múltiples maneras de cómo manejar un riesgo, esto lo podemos realizar tratando de evitar lo que lo origina, minimizar los eventos que lo provocan, limitar sus consecuencias, colaborar con ciertas dependencias que

nos brinden servicios como seguros (bróker de seguros), y en el caso de ser inevitable el riesgo, proveer recursos y planes de contingencia para mitigar el riesgo presentado en el momento de presentarse. Hay que considerar que el riesgo es una opción real y no puede ser ignorada, ya que la seguridad total no existe, debiendo siempre tener presente que el riesgo estará presente y debemos conocer y tener presente, siempre que el umbral de calidad sea el óptimo para el servicio presentado. De igual manera no es aceptable correr riesgos con el fin de conseguir un beneficio que estará por encima del riesgo, siempre y cuando se tome la responsabilidad de las acciones tomadas.

Debemos considerar que estas decisiones son delicadas, ya que no se realiza de manera técnica, lo cual conlleva a tomar decisiones que presentarán una responsabilidad del riesgo tomado, considerando que es necesario conocer las condiciones en las que se trabaja, de esta manera se podrá conseguir la seguridad para poder trabajar en confianza con el sistema. Para esto lo más recomendable será mostrar una aproximación metódica, misma que permitirá tomar decisiones con fundamento, explicando racionalmente las medidas presentadas. (Dirección General de Modernización Administrativa, 2012)

El uso de la metodología FODA permitirá realizar un análisis de la situación actual mostrando los problemas, a través de la identificación de las debilidades y amenazas, aprovechando las fortalezas y oportunidades, que servirán para realizar los procesos de mejora que se desea implementar y permita llevar un manejo más adecuado de la información que se maneja dentro del Departamento de Análisis de Telecomunicaciones de la UNATEM. (Silva G., 2022)

5. Justificación

5.1 Justificación Teórica

En lo anteriormente expuesto hemos podido observar que, la “Ley Orgánica de Protección de Datos Personal en el Ecuador “ , tiene como propósito, **“*Garantizar el ejercicio del derecho a la protección de datos personal, que incluyen el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección”;*** la información que se desarrolla dentro de esta Unidad es de suma importancia ya que manejamos información de carácter sensible y reservada, por lo cual debe ser una de sus prioridades la implementación de un Sistema de Seguridad de la Información n (SGSI), misma que debe estar sustentado tanto en el Esquema Gubernamental de Seguridad de la Información (EGSI) y la normativa ISO 27001, lo cual permitiría tener un mejor control del manejo de la información que se genera dentro de la misma, demostrando la importancia y profesionalismo al momento de obtener, almacenar y presentar la información de manera reservada y segura para la entidad gubernamental acreditada.

5.2 Justificación Metodológica

Para esto se debe realizar un rediseño de los procesos actuales que presentan retrasos o inconvenientes en el manejo de la información, lo cual perjudica el control y buen manejo de la misma, presentados estos nuevos procesos serán incorporados en estas nuevas metodologías de trabajo, las cuales permitirán llevar un mejor control de flujo de información.

La implementación de estos nuevos procesos servirá como un preámbulo y permitirá tener un esquema más claro para poder implementar en mayor escala

estos tipos de servicios dentro de más Unidades que se encuentran establecidas dentro del subsistema de investigación.

5.3 Justificación Práctica

La propuesta presentada cumplirá de manera muy eficaz el uso práctico en la implementación de procesos que mejoraran notablemente la funcionalidad del trabajo diario que dese desempeña el personal asignado a esta Unidad, esto va a permitir el mejor uso y optimización de la infraestructura tecnológica que se tiene dentro de la Unidad, logrando un mejor desempeño y control dentro de los procesos que se realizan dentro de los departamentos de la Unidad.

6. Principales definiciones

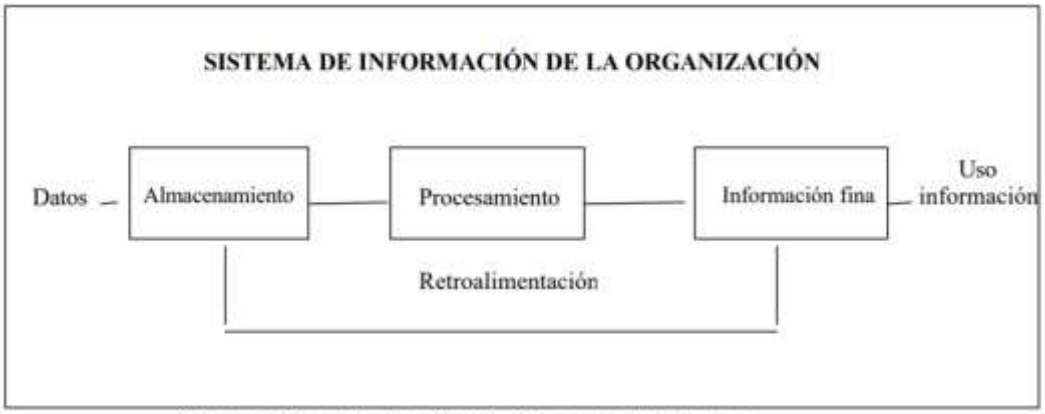
6.1 Información

La información es un recurso estratégico muy importante en la empresa la cual debe ser manipulada utilizando la tecnología que permita canalizar y transformar esta información que permita los logros de la empresa. (Carmen, Jose, & Santiago, 2019)

6.2 Sistema de Información

“Los sistemas de Información, se han convertido en un componente fundamental en las organizaciones exitosas, por lo que se considera importante analizarlos considerando diferentes perspectivas conceptuales, con la finalidad de comprender su esencia básica y aplicación en las diferentes áreas funcionales de la empresa. Al respecto, se realiza un bosquejo sobre diferentes posturas conceptuales planteadas por reconocidos autores en torno a este término, con el propósito de construir una definición integral de tan poderosa herramienta” (Encalada Vargas, 2019)

FIGURA 1.
SISTEMA DE INFORMACIÓN DE LA ORGANIZACIÓN EMPRESARIAL



Sistema de Información de la Organización empresarial: funciones

Nota la figura muestra el Sistema de Información de la organización empresarial Tomado de :(Hernández Trasobares, 2003), pág. 1

6.3 Sistemas de Información empresarial

Los sistemas de información empresariales han aparecido en los últimos años los cuales en la actualidad se presentan como para fundamental al momento de la implementación dentro de una organización. Es así que, la implementación de esto nos presenta un campo muy amplio lo cual no es solamente la implementación de software y hardware, mismo que son de manipulación continua para la generación de la productividad diaria, esto es más que solamente la manipulación de tecnología, es más bien la implementación de metodologías que permitan mejorar los tiempos de producción y eliminar procesos burócratas que generan estancamiento dentro de los procesos de una organización. De igual manera esto se presenta de manera competitiva frente a las otras organizaciones que compiten dentro del mercado mastranto estrategas de mejora en sus procesos, es por esto que toda organización debe considerar la implementación de sistemas de información que son de gran manera necesarios y de gran utilidad en las organizaciones. (Trasobares, s.f.)

6.4 Gestión de Tecnología (GT)

"La gestión tecnológica debe verse como el proceso que permite adquirir conocimiento necesario para realizar innovaciones tecnológicas, es decir, se crea valor para la empresa ya que se incrementa la eficiencia de las operaciones" (Terán Bustamante, Dávila Aragón, & Castañón Ibarra, 2019)

La tecnología en la empresa se vuelve eficiente cuando nos presenta todos los aspectos que relacionan a la capacidad de identificar las señales, dentro de un espacio que permitirá presentar las oportunidades y posible riesgos de su enfoque tecnológico y su interpretación; permitiendo presentar la factibilidad de lograr y recursos tecnológicos necesarios para la organización; con esto podemos llegar a asimilar la implementación de tecnologías que van a ser incorporadas en los procesos, adquiriendo nuevas experiencias y conocimientos al momento de su puesta en marcha. Esto se puede lograr, con la identificación funciones o etapas que muestren cuales son los parámetros necesarios para la implementación de este proceso, de igual manera se considere la presentación de un conjunto de herramientas o técnicas que permitan logren manejar las actividades planteadas y obtener experiencias que puedan servir en el futuro. (Nuchera, 1999)

6.5 Norma ISO

La Organización Internacional de Estandarización (International Organization for Standardization – ISO) y la Organización Mundial de normalización para las tecnologías eléctricas, electrónicas y demás relacionadas (Electrotechnical Commission – IEC), desarrollaron la familia de Normas ISO/IEC 27000, mismas que suministran lineamientos para la gestión de la seguridad en la información dentro de cualquier organización. (Palacios, 2018)

6.6 ISO 27001

“La norma ISO/IEC 27001:2013 tiene como objetivo "especificar los requisitos para establecer, implementar, mantener y mejorar continuamente una gestión de seguridad de la información sistema" (SGSI) que está integrado en la organización sistema de gestión global, con el propósito de ayudar a asegurar los recursos de información.

Su aplicación permite a la organización determinar y evaluar los riesgos de seguridad de la información e implementar procedimientos y mecanismos que preserven su integridad, confidencialidad y disponibilidad de la información. La organización puede entonces evaluarlos cíclicamente para mantener y mejorar el SGSI.” (Carvalho & Marques, 2019)

Es un Sistema de Gestión de la Seguridad de la Información (SGSI). Asegura la información con tres atributos: Confidencialidad, Integridad, Disponibilidad. (Baldecchi R. Q., 2014)

6.7 Seguridad de la Información

La Seguridad de la información es muy importante es por ello que se debe considerar las posibles amenazas se está por falta de conocimiento de las medidas de seguridad y aplicar elementos que permitan proteger la información ante diferentes ataques y proteger los datos de la empresa, siendo la seguridad de la información como la capacidad de brindar un nivel de confianza y acciones necesaria para evitar acciones ilícitas o mal intencionadas. (Postigo Palacios, 2020)

7. Alcances y limitaciones

7.1 Alcances

- Implementar el proceso de Sistema de Gestión de Seguridad de la Información SGSI, dentro del Departamento de Análisis de Telecomunicaciones de la UNATEM, permitiendo estar actualizado en cuanto al manejo y seguridad de la información acorde las nuevas exigencias que en la actualidad lo requiere con el uso de tecnologías de última generación y el manejo eficiente de la información, con el fin de precautelar, organizar y mejorar los procesos, brindando la información precisa y oportuna siendo un gran aporte al trabajo investigativo desarrollado dentro de la UNATEM.
- Permitir que el trabajo desarrollado dentro de la UNATEM mejore ampliamente y presente un enfoque más técnico, preciso y útil para las entidades gubernamentales acreditadas que manipulan y manejan la información obtenida dentro de esta Unidad.
- Evitar la fuga y divulgación de información que se genera dentro de la Unidad, lo cual perjudicaría el trabajo investigativo del área judicial encargada de las investigaciones.

7.2 Limitaciones

- Una de las limitaciones que podemos encontrar dentro del proceso de implementación de este sistema, es el poder establecer todas las fallas que encontramos dentro del proceso actual van apareciendo conforme se van implementando los procesos para el manejo de la seguridad de la información, de esta manera podemos establecer tiempos de ejecución de acuerdo a la criticidad de los errores que se vayan presentando.

- La resistencia al cambio por parte del personal que labora dentro de la UNATEM. La necesidad por parte de la unidad de capacitar al personal encargado del manejo de la información.
- Manejo de los principales factores que afectan y puedan producir un impacto mínimo que no afecte el trabajo diario tanto con el factor humano, tecnológico y procedimientos a ser establecidos en la UNATEM.

CAPÍTULO II MARCOTEÓRICO

2. Conceptualización de las variables o tópicos clave

El capítulo presenta la representación de los fundamentos y argumentos teóricos, que nos ayudan a sustentar el Sistema de Gestión de Seguridad de la Información SGSI, el mismo que nos permitirá demostrar los diferentes criterios desarrollados por autores que tienen experticia dentro del teman, con el fin de dar como sentado las diversas líneas de investigación, todo esto con el fin de cumplir los objetivos planteados dentro del proyecto de mejoramiento.

2.1.1 Gestión tecnológica en una organización

El modelo de gestión tecnológica se presenta de manera sistemática, estructurada, la tipificación de las fases con el fin de implementar los modelos de gestión, mostrando la forma de relacionarse y secuencia de las mismas, logrando fortalecer generando innovación, estas características permitirán tener una guía para diseñar las etapas para un modelo de gestión adaptado al entorno de una organización. (Venegas Loor, 2023)

Para resumir, se pudo apreciar en las diferentes definiciones, que podemos considerar a la gestión tecnológica como un proceso constituido, por una determinada serie de fases o etapas las cuales son indispensables para la generación, adquisición y acumulación de conocimientos, la cual, al ser bien aplicada y considerada como una estrategia de protección y resguardo de la privacidad de datos e información, dentro de una organización.

La Gestión tecnológica en una organización es entendida según Jiménez (2017) como “un proceso a través del cual se aplican un conjunto de herramientas que permiten identificar diversas situaciones e implementar cambios dentro de los sistemas informáticos de una empresa”.

En este sentido refiere R. Sánchez (2018) que; “la implementación de planes inclinados a gestionar los sistemas informáticos de una empresa, con el propósito de mejorar e innovar los procedimientos internos de tal empresa”.

En este sentido, determina Castro (2018) “las instituciones y empresas deben implementar gestiones tecnológicas en sus procesos basada en SGSI para proporcionar una alta productividad dentro de sus actividades básicas”.

Finalmente se considera que, una adecuada gestión tecnológica se considera una estrategia de protección y resguardo de la privacidad de datos e información, de una empresa.

2.1.2 Sistemas de Información (SI)

En la actualidad podemos ver como la cantidad de organizaciones va en aumento para integrar los sistemas de información dentro de sus operaciones, interactuar con proveedores y clientes; llegando a convertirse en grupos más competitivos dentro del mercado en el cual se desenvuelven. Dentro de las empresas, los sistemas de información gestionan los objetivos de cualquier otro sistema en general, tales como: el procesamiento de entradas, el almacenamiento de datos relacionados

con la entidad y la producción de reportes y otro tipo de instrumentos de resumen de datos. (Laura Mayer Lux, 2022)

Se pude definir como un esfuerzo organizado para recoger, procesar, adquirir y usar información y conocimiento, con el fin de para sugerir dentro de la formulación, ejecución y evaluación de políticas e intervenciones dentro de los procesos de manejo de información. En la actualizada podemos encontrar mucha información acerca de los sistemas de información organizacional misma que no es muy aplicada por diversos factores, como son el miedo al cambio, desconocimiento, presupuesto; la responsabilidad de los sistemas de información se encuentra dividida en diferentes áreas del estado, esto provoca que se realice un gran esfuerzo de coordinación para lograr la integración, intercambio y buen manejo de la información.

En razón que podemos definir a los Sistema de información tomando en consideración algunos autores que nos pueden guiar y hacer comprender de mejor manera que son los SI; es así que R. Andreu, indica que "…alcanza una cadena de complementos, que integran procedimientos desarrollados en un determinado entorno, dentro del cual intervienen dos (02) elementos mismos que se encuentran correlacionados (usuario / sistema); de igual manera presentamos a AT Acosta Castro, mismo que nos indica que "los SI operan sobre un conjunto de forma estructurada, lo cual servirá para recopilar y distribuir información de manera selectiva e indispensable para el correcto desarrollo de la organización y buen desempeño de sus directivos" y D Cohen Karen , nos indica que "los SI comprenden una indeterminada

cantidad de elementos que interactúan entre sí ”

En fin, en referencia a las definiciones o criterios presentados, se puede concluir que los sistemas de información presentan una funcionalidad que reside en la información de datos que presentan las organizaciones, la cual servirá a través de análisis para el correcto desarrollo de la operatividad. (Bron B, 2022)

2.1.2.1 Software

Entendiendo primeramente que es el Software podemos decir que, es un término informático mismo que hace referencia a programas de dispositivos computacionales, mismo que pueden ser de datos, procedimientos y pautas que permiten realizar indefinidas tareas dentro de un sistema informático. (Saara Tenhunen, 2023)

Existen algunas definiciones de diferentes autores las cuales las vamos a presentar como son de Sánchez (2013) lo define “… conjunto de mecanismos primordiales para los sistemas de información, la importancia es valiosa en vista que el equipo no generará ninguna acción sin la ejecución del mismo”, por estar razón consideramos la existencia de varios softwares, los cuales se presentan de manera simple y compleja; de igual manera García nos indica que, “…el profesional que se encarga del desarrollo de diferentes software se denominan como programadores los cuales realizan su desarrollo dentro de lenguajes determinados de programación, mismo que permite una interacciónentre el usuario y ordenador.

2.1.2.2 Software de seguridad

En la actualidad el ritmo acelerado de los procesos de desarrollo de software aumenta el riesgo de presentar debilidades en un sistema de software, lograr asegurar la información y los sistemas que la generan es primordial para las organizaciones. La gestión de la Seguridad Informática desde el inicio del desarrollo de software permitirá evitar que los mecanismos de seguridad deban ser ajustados dentro de un diseño ya existente, lo cual llevaría a cambios que provoquen vulnerabilidades en el software, y un aumento de costo y tiempo para conseguir una solución. (Sierra Huertas, 2023)

Por su parte Montecé nos indica que "…resalta que la seguridad de la información a través del tiempo ha ido evolucionando, debido a las potentes amenazas y riesgos existentes en la actualidad, algunas entidades que utilizan sistemas informáticos aún no han tomado conciencia de lo importante que es para su funcionamiento el cuidado y la seguridad de la información considerada como el bien fundamental".

Por su parte Romero, Figueroa, Vera, & Álava, 2018 nos indican que "…un programa de seguridad a la información se basa en codificary proteger archivos electrónicos en un sistema informático".

En base a las diferentes definiciones o conceptos podemos decir que se hace referencia al software o programas, se desarrollan con el fin de implementar un sistema de gestión de seguridad de información con el fin de establecer medidas de seguridad en la implementación de encriptaciones, claves, protección de virus y demás situaciones que puedan presentarse.

2.1.2.3 Virus informáticos

Se puede decir que un virus es un software informático, el cual, desarrollado a través de un lenguaje de programación con el único fin de infectar un sistema informático a través de diversos mecanismos de propagación, lo cual contiene una carga maliciosa que provocaría falla en el sistema y que además puede venir con medidas de seguridad para poder protegerse de los antivirus. (Peralta Castro, 2022)

Por su parte López indica que, "…se considera un conjunto de códigos informáticos ejecutados intencionalmente para instalarse y desplegarse en los sistemas operativos de manera reservada evitando la autorización del usuario. Por su parte García indica que "…es considerado un parásito que ataca los archivos o al sector de arranque de un sistema informático y que puede multiplicarse causando graves daños"

Es así que como lo han indicado los autores antes presentados podemos determinar que los virus llegan a afectar de manera considerable a los sistemas informáticos (Computadoras) a través de su duplicación, para lo cual hay que determinar algunas acciones con el fin de evitar estas afectaciones como son infección, alteración, perdida de información, hurto, y demás incidencias que puedan presentarse, todos con el propósito de propagarse y causar algún daño dentro de los sistemas. (Alvaro, 2022)

2.1.3 La estrategia de TI de una organización

En la relación que debe existir entre las tecnologías de la

información TI y la estrategia del negocio es un tema que ocupa los primeros lugares de interés para las organizaciones, más aún en que los desarrollos e innovaciones tecnológicas van tomando cada día más relevancia, impactando de manera significativa los comportamientos de las organizaciones, así como la aparición de nuevos modelos con base digital, estructuras en rojo, gestión de procesos por mediados TI. (Juan Carlos De la Cruz, 2022)

Por su parte Ortiz y Bayona indican que "…la información asume una importancia creciente y la incorporación de las Tecnologías de Información (TI) se torna fundamental en las organizaciones, con el fin de cubrir las necesidades del negocio, crecer o al menos, perdurar en su actividad, dada la dependencia, se requiere que la organización cuente con directrices, principios y aplique buenas prácticas para el buen Gobierno de TI". (Ortiz & Bayona-Oré, 2019)

Para Smith manifiesta que, "…implica la programación de un compendio de procesos, gestionados para lograr adaptarlo a la tecnología de una determinada organización con el fin de evaluar, clasificar y tomar acciones para establecer una mejora continua".

2.1.4 Las Tecnologías de Información en la Organización

La llegada de Internet y los constantes avances tecnológicos actuales conllevan una serie de transformaciones que han repercutido en el mundo empresarial dando lugar a nuevas formas de comunicarse, interaccionar, relacionarse, trabajar y aprender, así podemos identificar que las TIC se han convertido en una herramienta crucial para el futuro

de las organizaciones, estas pueden suponer oportunidades importantes para mejorar la productividad empresarial y gestión operativa. (Jesús Guasch, 2022)

Por su parte M Sánchez indica que “Las tecnologías de la información representan un elemento de rápida evolución, adoptadas por las empresas como factor determinante para afrontar la competencia dentro de una industria”.

2.1.5 Planificación Estratégica

En las definiciones presentadas sobre la Planificación Estratégica Ortiz indica que “…constituye un compendio de acciones con fines evaluativos de forma sistemática en una empresa con el propósito de fijar metas, re direccionar objetivos para mitigar las falencias o puntos débiles en las actividades de una empresa de forma rápida y eficaz”.

Por su parte Terán indica que “…permite definir lo que se requiere hacer en la organización, en este caso específico de estudio es sistemas de gestión de seguridad de información, como medio de esparcimiento que permitirá evaluar riesgos y oportunidades”.

2.1.6 El proceso de decisión estratégica y las necesidades de información

En proceso de la decisión estratégica, podemos decir que su concepción parte del reconocimiento de las características de la toma de decisiones en los contextos organizacionales, enfatizando en el nivel estratégico de decisión. Esta caracterización profundiza sobre las particularidades de las decisiones estratégicas y las ventajas y

capacidades organizacionales que genera, así como los diferentes componentes intrínsecos del proceso: situación-problema, individuo, información y elementos contextuales. (Rodríguez-Cruz, 2018)

En así que Díaz indica que "… tienen concebido que los cumplimientos de los objetivos estratégicos dependan en gran medida del buen desempeño de varias tareas informativas como la obtención de información del entorno, la identificación y representación de los flujos de información de los procesos, la estructuración de los datos operacionales y funcionales, la gestión interna de los conocimientos." (Pérez, 2018).

2.1.7 ISO (International Organization for Standardization)

"La ISO, es una organización no gubernamental fundada en 1947 con sede en Ginebra, que federa mundialmente de forma voluntaria y fuera de tratados, a las organizaciones nacionales de normalización de 148 países, como es el caso de la española AENOR (Asociación Española de Normalización), y su objetivo fundamental es: «***Promover el desarrollo de la estandarización y actividades relacionadas con el propósito de facilitar la comparabilidad, el intercambio internacional de bienes y servicios, y para desarrollar la cooperación en la esfera de la actividad intelectual, científica, tecnológica y económica»***. Los resultados del trabajo de la ISO son acuerdos internacionales publicados como normas o estándares internacionales mundialmente reconocidos" (R. Soage Santos, 2022)

La normativa además de ser aplicable a todo tipo de empresas en

cuanto a sus políticas, actividades de planificación, y responsabilidades, según Ortiz (2019) “se caracteriza por asegurar la privacidad e integridad de los datos y de la información, así como de los sistemas que la procesan creando una relación de confianza del cliente y la empresa”.

2.1.8 Norma ISO

La International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, desarrollaron la familia de Normas ISO/IEC 27000, proporciona todos los lineamientos para la gestión de la seguridad en la información en cualquier empresa (Palacios & Moreno, 2018).

2.1.9 El Sistema de Gestión de la Calidad (SGC)

El sistema de gestión de la calidad en las organizaciones hace referencia a un conjunto complejo de componentes explícitos y documentados que permitan lograr los objetivos de la calidad en la institución o empresa.

La implementación de SGC en una institución o empresa permite el desarrollo y modernidad eliminando de practica y procesos innecesarios que no proporcionan calidad los cuales fueron acumulados en el tiempo.

TABLA 1
ETAPAS PARA UN SISTEMA DE GESTIÓN, "IMPLEMENTACIÓN EFECTIVA DE UN SGSI ISO 27000"

Planificar (Establecer el SGSI)	Establecer la política, objetivos, procesos y procedimientos del SGSI pertinentes a la gestión de riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos generales de la organización.
Implementar (Implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Medir (Monitorear y revisar el SGSI)	Evaluar, y donde sea aplicable, medir el rendimiento del proceso contra la política del SGSI, sus objetivos y experiencia práctica, e informar los resultados para gestionar su revisión.
Mejorar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de auditorías internas del SGSI y de revisión de gestión u otra información relevante, para lograr mejora continua del SGSI.

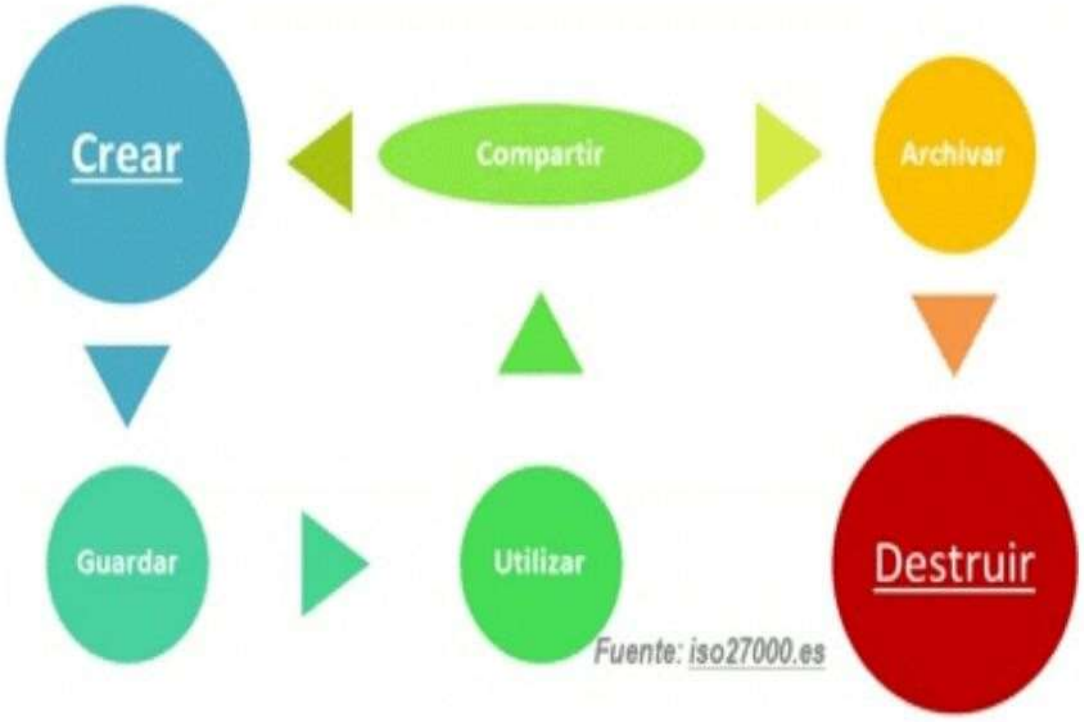
La tabla muestra un Sistema de gestión, "Implementación efectiva de un SGSI ISO 27000. tomado de:", (Baldecchi R. , 2014), pág. 5

2.1.10 Sistema de Gestión de Seguridad de la Información (SGSI)

"Toda la información almacenada y procesada por una organización está expuesta ante amenazas de ataque (por intereses comerciales, intelectuales y/o chantaje y extorsión), error (intencionado o por negligencia), ambientales (por ejem. Inundaciones o incendios), fallo en los sistemas (de almacenamiento de datos, informáticos, redes telemáticas), entre otras y también está sujeta a vulnerabilidades que representan puntos débiles inherentes a su propio uso en el ciclo de vida representado a continuación".

"Permitir que una información precisa y completa esté disponible de manera oportuna para aquellos autorizados que tienen una necesidad es un catalizador para la eficiencia del negocio".

FIGURA 2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN



Nota: la figura muestra un Sistema De Gestión de Seguridad de La Información Tomado de: (www.ISO27000.es)

"Para poder interrelacionar y coordinar las actividades de protección para la seguridad de la información, cada organización necesita establecer su propia política y objetivos para la seguridad de la información dentro de la coherencia del marco de globales de la organización". (ISO2700.es, 2022).

Beneficios de aplicar un Sistema de Gestión:

FIGURA 3
BENEFICIOS DE APLICAR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Nota La figura muestra el Sistema de gestión de la Seguridad de la Información. Tomado de: **www.ISO27000.es)**

2.1.11 ISO 27001

Es un Sistema de Gestión de la Seguridad de la Información (SGSI). Asegura la información con tres atributos: Confidencialidad, Integridad, Disponibilidad (Baldecchi R., 2014).

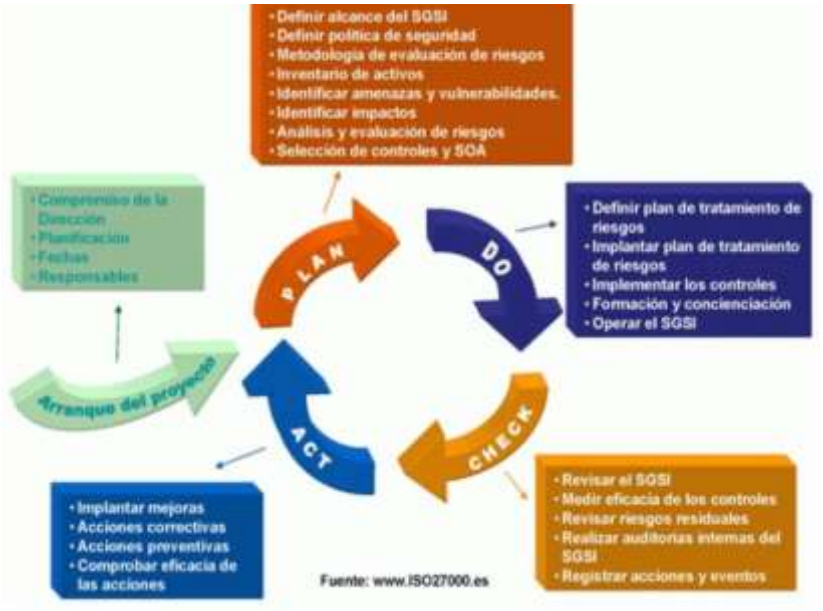
"Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013 segunda edición). Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones.

En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados" (ISO2700.es, 2022).

Fundamentos del Sistema de Gestión de la Seguridad 27001

El punto exigido en la norma pertenece al Plan – Do – Check – Act (Planificar-Hacer-Verificar-Actuar), los cuales deben ser aplicados en el SGSI en la empresa, utilizando como datos de entrada los requisitos de seguridad de la información la siguiente imagen muestra las etapas (Orostegui Forero, 2022):

FIGURA 4
PROCESOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD 27001



Nota: la figura muestra el proceso del Sistema de Gestión de la seguridad 27001. Tomado**:** (Ladino A., Villa S., & López E., 2011)**.**

2.1.12 Seguridad de la Información

La información es muy importante en una empresa ya que permite el funcionamiento de la misma es por ello la importancia del manejo y la seguridad de la información, en los últimos años el incremento en el manejo de la información, así como el uso de nuevas tecnologías como la internet exige que la información debe ser protegida y resguardada para ello es necesario del manejo e implementación de herramientas para tal fin. (Hernández, 2022)

"La organización Anti-Virus Test, que presta servicios de consultoría a empresas de seguridad informática, dice que en el 2008 había 9 millones de Software malicioso en el mundo. En el 2009 la empresa registraba 22 millones, sólo de esta amenaza" [1]. Con este panorama las empresas deben diseñar e implantar estrategias que les permita mejorar la seguridad de la información en su organización" (Ciudad Maestro, 2014).

La seguridad de la Información es un conjunto de procedimientos que permitan asegurar el manejo y la integridad de la información, utilizando los siguientes criterios:

- **Confidencialidad**: la Información es maneja exclusivamente por las personas autorizadas.
- **Integridad**: La información no debe ser modificada, alterada o recortada por personas no autorizadas, manteniendo la información su integridad y exactitud y tenga la validez pertinente.

- **Disponibilidad:** La información debe tener un acceso oportuno e inmediato por parte de las personas autorizadas (Baldecchi R., 2014).

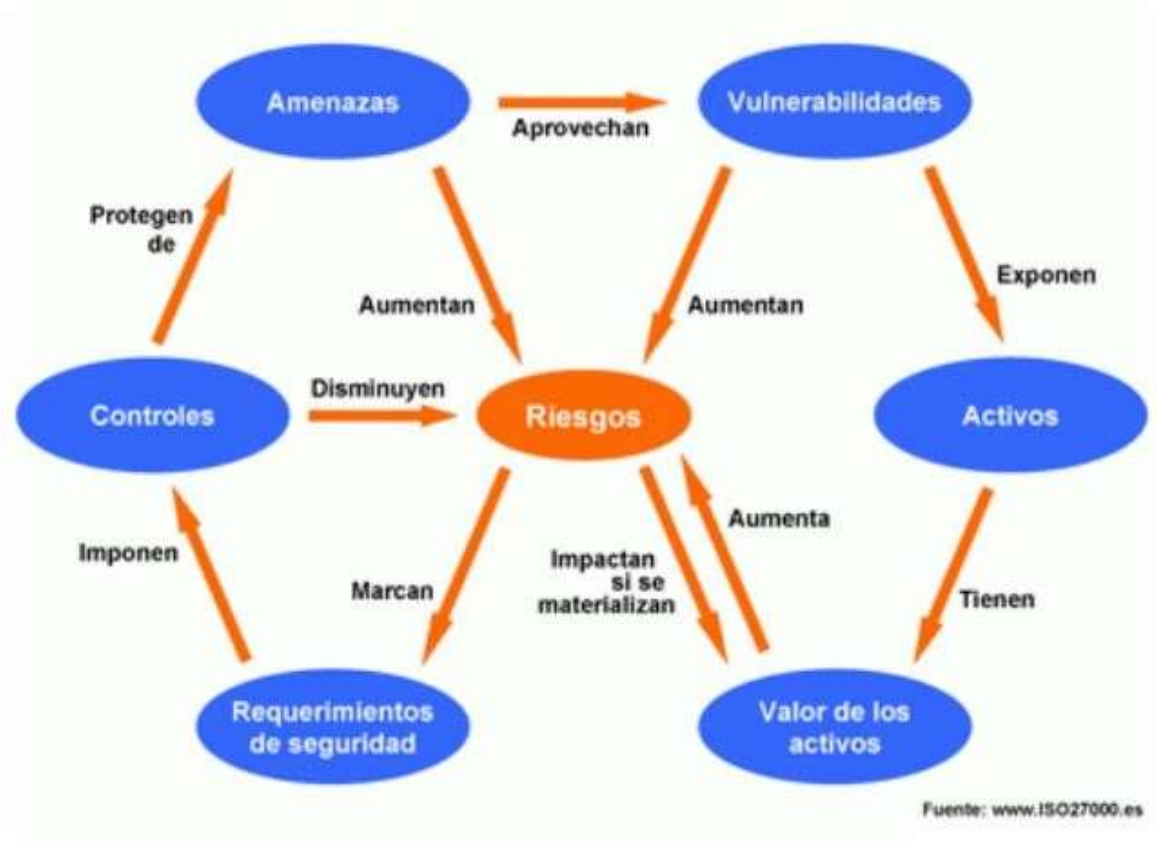
2.2 Evaluación de riesgos

"Cada organización debe determinar el proceso más apropiado disponiendo de ayudas más directas las guías ISO/IEC 27005 e ISO 31000. Las revisiones y actualizaciones periódicas y/o por cambios sustanciales que afronta la organización son requeridas para reflejar los cambios en los riesgos antes de que se produzcan para mantener un enfoque preventivo y de anticipación en acciones mitigadoras o de control.

Informes relevantes, entradas en su registro de riesgos con descripciones de riesgos, propietarios de riesgos identificados, etc., y métricas para demostrar su funcionamiento son información documentada típica de apoyo adicional.

Como ejemplos de operación (8.2) los informes de evaluación de riesgos, métricas de riesgos, listas priorizadas de riesgos, inventarios o catálogos de riesgos de información o entradas de riesgos de información en inventarios/catálogos de riesgos corporativos, etc. debates que surgen, memorandos formales, correos electrónicos que expresan preocupaciones sobre ciertos riesgos, o similares". (ISO2700.es, 2022)

FIGURA 5
EVALUACIÓN DE RIESGOS EN UN PROCESOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD 27001



Nota: la figura muestra la Evaluación de riegos en un proceso del Sistema de Gestión de la Seguridad 27001. Tomado**:** **(**www.ISO27000.es)

2.2.1 Tratamiento de riesgos

"La evidencia típica incluye una política y/o procedimiento por escrito para decidir e implementar consistentemente aquellos planes de tratamiento del riesgo adecuados.

Proporcionar informes relevantes, los planes de tratamiento de riesgos relacionados con aquellas situaciones no deseadas/inaceptables por la dirección, entradas en su registro de riesgos, métricas, etc. son formas de convencer a los auditores de que el proceso funciona correctamente". (ISO2700.es, 2022).

FIGURA 6
EVALUACIÓN DE RIESGOS EN UN PROCESOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD 27001

Nota: la figura muestra la Evaluación de riegos en un proceso del Sistema de Gestión de la Seguridad 27001**Fuente: (www.ISO27000.es)**

2.2.2 Herramientas para modelar procesos de la Norma ISO 27001

"A continuación, se presenta un resumen de algunas herramientas que soportan la implantación de la norma ISO 27001 en las empresas,estas herramientas funcionan basadas en procesos.

Nombre: Gesttic

Versión: Gesttic Oro

Ciudad: Vilassar de Mar (Barcelona)

Funcionalidades: Gestor de documentaciónCuadro de Mando Integral

Intranet corporativo

Gestor de Work flows

Extranet

Gestor de Proyectos

Ventajas:

1. Es un Gestor Documental multilingüe
2. Es adaptado a la Gestión de Sistemas de Calidad yMedio

   Ambiente "Sin Papeles"

Características Técnicas:

Viene con 20h de formación. Incluye 5 usuarios, 100 MBde disco duro y

300 MB de tráfico mensual. Puede adquirir ampliaciones de usuarios.

Tipo de Certificaciones:

1. OEA

2. ISO 9004

3. SICTED 4. ISO 9001

5. UNE EN 13816

6. UNE 187001

7. ISO 14001

8. EMAS: Eco Management and Audit

Scheme9. ISO 27001

Sector: Servicios, Público, Productivo

Soporte: 60 EUROS MES

Precio: 150 EUROS

Nombre: ISOTools

Versión: ISOTools Project

Manager**CIUDAD**: Madrid,

Sevilla, Córdoba

Funcionalidades:

1. Gestión de proyectos
2. Gestión de tiempos
3. Gestor de tareas
4. Gestor de costes
5. Gestor del riesgo
6. Gestor de la calidad
7. Gestión de Recursos
8. Gestor de adquisiciones

Ventajas:

Eficacia: Mejora de la eficacia, permitiendo una perfecta gestión del conocimiento a nivel organizativo y documental.

Dinamismo: Sistemas de gestión dinámicos enfocados hacia la mejora continua y a la obtención de resultados.

Organización: Una agenda le permite planificar avisarde todo lo que tiene que hacer.

Ahorro: Reduce los tiempos y costos de implantación y mantenimiento, optimizando la eficiencia de la mejora continua.

Accesibilidad: Disponibilidad de la información en cualquier momento y desde varios dispositivos.

Agilidad: Consultas rápidas de toda la información y tareas delsistema.

Centralización de la información: un dato único. Facilita la gestión del conocimiento de la organización

Funcionalidad para la ISO 27001 Evaluación de Seguridad de la Información, Controles 27002, Salvaguardas, Métricas e Indicadores, Cuadro de Mando Colaboración: Potencia el flujo interno de comunicación y la involucración de todo el personal.

Tipo de Certificaciones:

1. ISO 9001
2. ISO 14001
3. OHSAS 18001
4. ISO 27001
5. ISO 9004

Sector:

ISOTools es una herramienta estándar y personalizable válida para la gestión de cualquier tipo de organización:

- Empresas

- Organismos Públicos
- Asociaciones

Soporte: 28 EUROS MES

Precio: 15.330 euros

Nombre: Process Maker

Funcionalidades:

Software para definición, gestión de procesos y

flujos detrabajo.

- Diseño de Flujos de trabajo
- Creación Dinámica de formularios (Dynaform)
- Gestión de Casos y reportes
- Código fuente abierto
- Integración a otros sistemas.
- Basado en web, por lo que no requiere instalación, por lo tanto, se debe contar con un servidor donde pueda operar el software.
- Interface AJAX de fácil uso para la creación simple de procesos ytener una vista previa instantánea.
- Integración con bases de datos como MySql, Oracle, MSSQL.
- Fácilmente adaptable a cambios". (Ladino A., Villa S., & López E., 2011).

2.2.3 ISO/IEC 27000

"Es un conjunto de estándares desarrollados o en fase de desarrollo por la ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que brindan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización de tipo público o privada, grande o pequeña" (Junaid, 2023)

2.2.4 El modelo COBIT

"(Control Objectives for Information and related Technology) es el marco aceptado internacionalmente de buenas prácticas para el control de la información TI y los riesgos que conllevan. COBIT se usa para implementar el gobierno de TI y mejorar los controles de TI. De igual manera, contiene objetivos de control, directrices de aseguramiento, mediciones de desempeño y resultados, factores críticos de éxito y modelos de madurez". (Rene Aquino Arcata, 2021)

"Para apoyar a las organizaciones a satisfacer exitosamente los desafíos de los negocios actualmente, el IT Governance Institute (ITGI) publicó la versión de COBIT 4.1" (Alanoca Ticona, 2022)

FIGURA 7
EL MODELO COBIT

Nota: la figura muestra el Modelo COBIT. Tomado de: "La gestión en la seguridad de la información según Cobit, Itil e ISO 27000**",** (Montaño Orrego,)**.**

2.2.5 Acerca de Itil

"La Biblioteca de Infraestructura de Tecnologías de la Información ITIL está basado en un conjunto de mejores prácticas para la gestión de servicios de tecnologías de la información en lo referente a personas, procesos y tecnología, las cuales fueron desarrolladas por la OGC (Oficina Gubernamental de Comercio) del Reino Unido.

A través de buenas prácticas especificadas en ITIL se hace posible para departamentos y organizaciones reducir costos, mejorar la calidad del servicio, tanto a clientes externos como internos y optimizar al máximo las habilidades y destrezas del personal mejorando su productividad". (Remache Típan, 2022)

FIGURA 8
EL MODELO ITIL

Modelo ITIL V.3 Fuente: IT Process Map

Nota: la figura muestra El Modelo ITIL V.3 Fuentes: IT Process Map. Tomado de: "La gestión en la seguridad de la información según Cobit, Itil e ISO 27000",(Montaño Orrego, 2011).

2.3 Marco Legal

Con el avance de la tecnología y la creciente accesibilidad a la webque tiene a todo el mundo conectado constantemente, ha sido de utilidad para la masificación en la creación y uso de diferentes sitios web y APP (aplicaciones). Las mismas fueron diseñadas para satisfacer las necesidades de sus usuarios a través de un dispositivo electrónico, donde las necesidades son infinitas, como juegos, transacciones nacionales e internacionales, sin duda el uso de Internet ha llegado facilitar la vida de los usuarios, pero de igual manera al tener dichos beneficios también contamos con riesgos que se presentan constantemente con información nuestras información al estar expuestos a los ataques que se sufre a través de la web por esto encontramos los programas maliciosos son insertados en los sitios web o APP por delincuentes informáticos que han hecho de las Tecnologías de la Información y Comunicación (TIC) su nueva herramienta para cometer sus actos ilícitos, con este antecedente podemos preguntarnos, cuáles son los tipos de delitos que se generan enla red, qué leyes existen para sancionar los delitos informático, podemos decir que existen varias dificultades para combatir los delitos informáticos por la transaccionalidad de los mismos y la incompatibilidad de las leyes anivel mundial, considerando que en algunos países no existen Leyes para combatir los delitos informáticos y esto produce perdidas enromes a causade los mismos.

2.3.1 Constitución de la República del Ecuador

La constitución en el Artículo 1 indica que “El Ecuador es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada. La soberanía radica en el pueblo, cuya voluntad es el fundamento de la autoridad, y se ejerce a través de los órganos del poder público y de las formas de participación directa previstas en la Constitución. Los recursos naturales no renovables del territorio del Estado pertenecen a su patrimonio inalienable, irrenunciable e imprescriptible.” (Ecuador C. d., 2021)

2.3.2 Ley Orgánica de Protección de Datos Personales

El 26 de mayo de 2021 mediante Registro Oficial Suplemento No. 459 es publicada misma que “Tiene por objeto garantizar el derecho a la protección de datos personales, que incluye el acceso y decisión sobre la información y datos de este carácter, así como su correspondiente protección.

En lo principal, la ley se refiere a las condiciones que se deben verificar para que el tratamiento de datos personales sea legítimo. Se refiere, también, a las formas a través de las cuales el titular de los datos personales puede manifestar su voluntad para el tratamiento de sus datos.

Regula, además, el contenido y alcance de los derechos:

1) a la información;

2) de acceso;

3) de rectificación y actualización;

4) de eliminación;

5) de oposición;

6) a la portabilidad;

7) a no ser objeto de una decisión basada única o parcialmente en valoracionesautomatizadas;

8) de consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales;

9) a la educación digital". (Ecuador A. N., 2021)

2.3.3 Esquema Gubernamental de Seguridad de la Información – EGSI

Mediante Acuerdo Ministerial No. 025-2019, el 14 de noviembre de 2019, se expide el "Esquema Gubernamental de Seguridad de la Información (EGSI)", mismo que manifiesta "…preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riegos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados". (Ministerio de Telecomunicaciones, 2021)

CAPÍTULO III MARCO REFERENCIAL

En la actualidad existen una gran variedad de modelos, normas y marcos referenciales dentro del tema de SGSI, de esta manera está claro que se pretende guiar hacia el camino a las instituciones para que se pueda lograr la alineación de la misión institucional y el uso apropiado y eficiente de la tecnología.

La innovación y avances tecnológicos han permitido a las personas comunicarse de maneras innovadoras y diferentes a épocas anteriores, con el crecimiento acelerado de las comunicaciones la delincuencia se ha visto en la necesidad de hacer uso de la tecnología para con el único fin de incrementar su espacio de cobertura en el cometimiento de sus fechorías, por tal motivo el gobierno debe estar siempre innovando y acorde a todos los avances tecnológicos, incrementando su conocimiento y procedimientos técnicos científicos con el uso de la tecnología, de esta manera se brindará un mejor servicio a la sociedad.

Consecuentemente podemos decir que el problema se podría definir de manera simple, es así que, debemos realizar un análisis externo que nos permita identificar los cambios necesarios (amenazas y oportunidades), y de igual manera un análisis interno mismo que nos permitirá enfrentar los obstáculos frente a todas las interrogantes (debilidades y fortalezas), con el fin de establecer estrategias que permitan el cumplimiento de nuestros objetivos planteados. (Vecino, 2017)

Análisis Externo

El análisis externo nos debe permitir crear un listado amplio de diferentes oportunidades, mismas que permitirán mejorar la productividad a la hora de obtener información relevante y manejar de manera óptima y segura la información

obtenida dentro de los aplicativos informáticos, de igual manera determinar y reconocer las amenazas que se vayan presentando las cuales debemos evadir con el fin de mejorar los procedimientos.

La UNATEM debe presentar una capacidad de responder de manera agresiva y de igual manera mantener una defensa permanente contra los factores presentados, presentando estrategias capaces de determinar y aprovechar las oportunidades presentadas y minimizar los riesgos de amenazas potenciales presentadas dentro del camino.

Análisis Interno

El análisis interno hacer referencia a todos los aspectos dentro de la UNATEM, presentando contradicciones marcadas para el correcto direccionamiento, estos componentes son originados internamente dentro de la Unidad. Es así que, todos los aspectos internos presentados dentro de la Unidad presentarán fortalezas como debilidades mismas que pueden afectar el funcionamiento interno, con este antecedente, es necesario establecer protocolos para tomar acciones pertinentes que permitan realizar un mejor desarrollo dentro de la Unidad.

Matriz FODA

Presentamos el análisis de la matriz FODA, en la cual presentaremos las Fortalezas, Oportunidades, Debilidades y Amenazas; mismas que actualmente se presentan dentro del Departamento de Análisis de Telecomunicaciones de la Unidad Nacional de Telecomunicación Móvil, descubiertas en la recopilación de información dentro de la Unidad.

TABLA 2
MATRIZ FODA

FORALEZAS	OPORTUNIDADES
• Presenta asesoramiento externo por parte de entidades de control gubernamental. • Manejo de políticas de seguridad interna para el personal. • Departamento de TIC´s interno independiente. • Control biométrico del personal, de acuerdo al horario y niveles de seguridad según la función. • Auditorias permanentes del funcionamiento de los sistemas y gestión administrativa para el correcto manejo de la información.	• Presentar un plan de mejora para el manejo de información reservada. • Demostrar un mejor enfoque en la seguridad de la información con el fin de adquirir mejor tecnología. • Capacitar constantemente al personal de la Unidad en el manejo de la información, haciendo hincapié en la seguridad de la información. • Manejar un presupuesto anual para la implementación de mejoras dentro de la seguridad de la información.
DEBILIDADES	**AMENAZAS**
• No se cuenta con un departamento de respaldo (backup) para la continuidad del servicio. • El licenciamiento del software es mínimo para el equipamiento tecnológico. • Conocimiento mínimo del manejo de seguridad de la información. • Políticas de seguridad sin estandarización. • Falta de capacitación del personal de la Unidad con respecto a la seguridad de información. • Poco interés directivo al	• Antivirus limitado para el parque informático de la Unidad. • Eliminación de información sin protocoles de respaldo establecidos. • No se cuenta con un equipo firewall de respaldo (backup) en el caso de fallas del principal. • Accesos indebidos a la información reservada, no consentidos ni controlados. • Pérdida de capacidad operativa personal por falta de personal calificado. • Cambio permanente de personal y

departamento de TIC´s para mejorar la gestión de seguridad de la información.	disposiciones con el manejo de la información.

La Tabla muestra la Matriz FODA. (Chicaiza Castillo, 2020) Fuente: Elaboración propia

3.1 Reseña Histórica

El estado Ecuatoriano, con el fin de incorporar nuevas estrategias y mecanismos que ayuden y mejoren los procedimientos de seguridad, a través de la Policía Nacional, en sus procedimientos investigativos, con apoyo de la tecnología y en cooperación con el Ministerio del Interior, Ministerio de Telecomunicaciones, Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL) y Fiscalía General del Estado, logran crear laUnidad Nacional de Telecomunicación Móvil (UNATEM), con el fin de lograr tecnificar los procedimientos investigativos y de cooperación a las investigaciones y apoyo técnico operativo para el cumplimiento de las diligencias investigativas que llevan a cabo la Fiscalía General del Estado en coordinación con el eje investigativo y de inteligencia de la Policía Nacional, a partir del 2019 se ha visto necesaria la creación de esta Unidad, siempre con elprincipio de legalidad y celeridad de la información.

Es así, que la Unidad esta conforma por tres departamentos de apoyo técnico como son:

1. El Departamento de Análisis de Telecomunicaciones
2. Departamento de Apoyo Técnico en campo
3. Departamento de Interceptación de Información

De esta manera permitiendo brindar un mejor servicio al eje investigativo dela Fiscalía y la Policía Nacional en el Ecuador.

En cuanto al talento humano que presta sus servicios dentro de esta Unidad, se cuenta con un contingente de 120 servidores públicos, entre los que conforman el personal directivo, técnico operativo y administrativo; mismo que se encuentran en constante capacitación del manejo de plataformas y equipos tecnológicos, con el fin de mantener un conocimientoacorde a los avances de la tecnología.

Así mismo presentamos la misión y visión de la Unidad como lo detallamos a continuación.

Misión

FIGURA 9
MISIÓN UNATEM

"*Apoyar a las investigaciones con la intercepción telefónica y telecomunicaciones, conforme lo dispone la autoridad competente, mediante técnicas de investigación a fin de establecer los elementos de convicción, en apoyo a la administración de justicia*".

Nota: la figura muestra la Misión Unidad Nacional de Telecomunicación Móvil (UNATEM), Tomado de: Resolución 087-2020-FGE

Visión

FIGURA 10
VISION UNATEM

"Constituirse en una unidad técnica de investigación policial a través de las telecomunicaciones, coadyuvando en forma directa a la investigación criminal, dentro de los diferentes medios en el cual se desenvuelven las telecomunicaciones".

Nota: la figura muestra la Visión Unidad Nacional de Telecomunicación Móvil (UNATEM), Tomado de: Resolución 087-2020-FGE

3.2 Presentación de Actores

La normativa ISO 27001, necesita que se presenten actores que estén acorde a sus requerimientos, estos son presentados en este caso deacuerdo a los criterios de BALAGUER (2014) donde nos indica que “Los responsables de realizar las acciones para la implementación del SGSI, deben ser profesionales calificados, sobre todo capacitados y con experiencias previas para un logro exitoso del proyecto”.

De esta manera vamos a identificar los actores/funciones en la cual se encuentra la Dirección de Proyecto.

Dirección de Proyecto

En la Dirección de proyecto se encuentran los siguientes actores:

FIGURA 11
ORGANIGRAMA DIRECCION DE PROYECTOS

Nota: la figura muestra el organigrama de la dirección de proyectos de la Unidad Nacional de Telecomunicación Móvil (UNATEM), Tomado de: Resolución 087-2020-FGE

TABLA 3
PRESENTACIÓN DE ACTORES

Actor/ cargo	Función
Dirección de Proyecto	Estará a cargo de un Director, el cual será el mayor responsable delproyecto, se encargará directamente de realizar una conexión entre el cliente y los proveedores, valores, tiempos de implementación y control.
Proveedores de servicios	Determinar las aptitudes relevantes para cada rol durante la SGSI. Asegurar que los funcionarios sean conscientes la importancia del trabajo que realizan dentro del manejo de información en el eje investigativo. Mantener en constante capacitación y actualización al personal que desempeña el trabajo, reconociendo sus habilidades y fortalezas. Evaluar la actuación permanente de los funcionarios determinando la efectividad positiva obtenida.
Jefe de Equipo	Encargado de determinar las tareas asignadas a los grupos de funcionarios, dirigiendo, controlando entre otros.
Analistas	Encargado de realizar una verificación ya análisis de todos los posibles requisitos a ser solicitados por el eje investigativo y Fiscalía, para la obtención de información relevante dentro de una investigación
Diseñador	Encargado de estructurar el proyecto a realizar con el propósito de tratar de lograr incorporar las funcionalidades y requisitos presentados.
Programadores	Encargados de diseñar e implementar el código fuente que cumpla con los requisitos útiles y necesarios para el SGSI.
Probadores de software	Encargados de pruebas de estrés dentro del software desarrollado con el fin de encontrar falencias y posibles mejoras a ser implementadas, de igual manera verificar si todas las necesidades fueron tomadas en cuenta y han sido desarrolladas.
Instaladores	Encargado de proveer e instalar el software que cumpla con los requerimientos necesarios para la implementación de SGSI.
Auditor Interno	Realizar una auditoria internad al final de proyecto que permita comprobar la implementación adecuada del SGSI ISO 27001.

La Tabla muestra los actores que intervienen en la dirección del Proyecto. Fuente: Elaboración propia

Jefe de Equipo

Como podemos apreciar en esta estructura el Jefe del Equipo deberá planificar y ejecutar las acciones dentro del proyecto, estableciendo control de cómo se va desarrollando.

A continuación, presentamos como está estructurada la UNATEM:

FIGURA 12
ORGANIGRAMA DE LA UNATEM

Nota: la figura muestra el organigrama de la Unidad Nacional de Telecomunicación Móvil (UNATEM), Tomado de Fuente: Elaboración propia

Nota: Esquema de la estructura funcional de la organización y la responsabilidad de los actores. (Esguerra y Ortiz, 2018)

Dentro de este organigrama podemos identificar que el jefe de la Unidad es el responsable de supervisar y controlar mientras dure el proyecto; cada grupo establecido de las diferentes actividades, contará con un director encargado de verificar la operatividad de sus funciones.

3.3. Diagnóstico Sectorial

En esta fase se deberá implementar los objetivos, estrategias y el alcance de la Unidad con el único fin de definir los parámetros y lineamientos, dando como inicio la planificación del SGSI.

Una organización debe conocer en su total funcionamiento, operaciones y actividades; y de acuerdo a la misión y visión establecidas con el fin de implementar planificaciones estratégicas, estaríamos aplicando un diagnóstico sectorial. Por esta razón Andreu (2012) nos indica que: "…este tipo de diagnóstico se basa en el estudio personalizado de cada sector operativo de la empresa y permitirá valorarla internamente para a partir de los resultados poder establecer directrices que permita hacer frente a las falencias encontradas"

De esta manera podemos identificar que el inicio de este capítulo nos muestra los aspectos relevantes de la UNATEM, como su estructura, funcionarios, organigramas, misión, visión, entre otros; esto con el fin de poder determinar la situación actual de la misma. Con todo esto podemos evidenciar las políticas, directrices, procesos y estrategias.

3.4. Políticas de gestión

La UNATEM, es una Unidad transversal de la DIGIN la cual se encarga de apoyar técnicamente al eje investigativo de la Fiscalía General del Estado en todo el territorio nacional, con el fin de brindar elementos de

convicción dentro de investigaciones con apoye técnico y profesional de los funcionarios que la componen, y todo esto se lo hace a través del cumplimiento de las siguientes políticas de gestión:

- Atender los diferentes pedidos Fiscales que se generen a través del Sistema Informático implementado por la Fiscalía General del Estado, y que tengan relación con los Reportes de Telecomunicaciones de los abonados de las diferentes Operadoras de Servicio Móvil Avanzado (SMA), dentro del debido proceso (Investigación Previa, Instrucción Fiscal,Actuaciones Fiscales Urgentes y Actuaciones Administrativas) y con estricta observancia a lo garantizado en el artículo 66 numeral 19, 20 y 21 de la Constitución de la República del Ecuador, el artículo 499.2 del Código Orgánico Integral Penal y demás normativa pertinente.
- Atender los requerimientos de Reportes de Telecomunicaciones solicitados por los Defensores Públicos y Privados, dentro del debido proceso (Investigación Previa, Instrucción Fiscal, Actuaciones Fiscales Urgentes y Actuaciones Administrativas), cumpliendo con los requisitos legales y constitucionales que permitan recabar, registrar y entregar la información de manera oportuna de conformidad a lo que dispone el artículo 499.2 del COIP y el Manual de Procedimientos de la UNATEM.
- Obtener de los Sistemas Informáticos de las Operadoras de Servicio Móvil Avanzado (SMA), los Reportes de Telecomunicaciones de abonados, de acuerdo con los manuales, instructivos, protocolos y normas técnicas relacionadas, a fin de garantizar el buen uso y manejo

de la información evitando que haya alteración o difusión no autorizada de la misma.

- Almacenar en un motor de Base de Datos especializada la información obtenida de los Sistemas Informáticos de las Operadoras de Servicio Móvil Avanzado (SMA), a fin de que los diferentes organismos de control realicen las verificaciones y auditorías en el ámbito de sus competencias,cuando estos lo estimen pertinente, debiendo mantener la reserva que laley exige.
- Garantizar que la información obtenida a través de los Sistemas Informáticos Implementados por las Operadoras de Sistema Móvil Avanzado (SMA), sea procesada con aplicación del Manual de Procedimientos y los Instructivos correspondientes, cumpliendo con la reserva por parte de los y las servidores públicos que integran la UNATEM,de conformidad con lo dispuesto en los artículos 490, 576, 584 del COIPy lo referente a actuaciones y técnicas especiales de investigación bajo las penas previstas para estos casos en el mismo cuerpo legal.
- Reducir los tiempos de respuesta constituyéndose en una herramienta deapoyo en las investigaciones que realiza la Fiscalía General del Estado y el Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses.
- Garantizar la seguridad de la información, especialmente cuando se trate de obtención, registro y entrega, generando mecanismos de control o paraevitar y prevenir posibles fugas de información o mal uso de la misma, hasta que se realice la entrega de los indicios y

elementos de convicción a los sujetos procesales a quienes la ley faculta su requerimiento.

Personal Técnico

Con el fin de tener éxito en las políticas establecidas la UNATEM está conformada por personal técnico altamente capacitado, infraestructura tecnológica de última generación, entre otros; con el fin dar cumplimiento y soporte de apoyo a la Fiscalía y eje investigativo con el fin de poder implementar la gestión y diseño de un SGSI.

En lo que se refiere a las técnicas, podemos indicar que la misión, visión y políticas establecidas, nos permite enfocar de mejora manera la presentación e ideas que permitan establecer estrategias entre las que podemos mencionar:

1. Unidad altamente especializada y técnica con el fin de atender requerimientos a nivel nacional con el uso de tecnología entregado información oportuna y eficiente.
2. Elementos de convicción válida dentro de una investigación que permita ala eje investigativo y Fiscalía vincular a los diferentes miembros de una organización.
3. Funcionarios técnicos altamente capacitados en el aspecto técnico y de análisis con el fin de brindar apoyo a nivel nacional.
4. Innovación de procedimientos con el fin de establecer más y mejores maneras de aportar un apoyo eficaz y eficiente dentro de las investigaciones.
5. Implementación de mejoras ambientales al ser una unidad con procesos cero papeles.

Directivas y Estrategias

En lo que se refiere a la vinculación por perspectiva, referidas dentro de la directriz estratégica responde a los métodos del BSC, incluyendo el recurso humano, procesos, entidad requirente y recursos económicos. Podemos evidenciar dicha relación de las siguientes perspectivas:

TABLA 4
DIRECTRICES ESTRATEGIAS DE LA POLITICA DE GESTION

No.	DIRECTRICES ESTRATEGIAS	PERSPECTIVAS
1	Jefe de la Unidad	Financiera
2	Empresas proveedoras de servicios de Comunicación.	Financiera
3	Satisfacción del eje investigativo y Fiscalía.	Clientes
4	Implementación de mejoras permanentes en procesos.	Procesos
5	Mejoramiento de procesos ambientales	Procesos
6	Recurso humano técnico altamente capacitado y motivado dentro de la obtención de RT.	Recurso humano

La Tabla muestra Las Directrices Estratégicas de la Política de Gestión Fuente: Elaboración propia

Dentro de las líneas estratégicas Sánchez (2011) considera que:"…etapa donde se planifica la responsabilidad del personal en concordancia a los productos, procedimientos, sistemas de apoyo y metas de la organización, delimitada por el establecimiento de objetivosestratégicos y la identificación de procesos.

Identificación de procesos

De acuerdo a lo que establece Ortiz (2019), "…se considera un proceso al compendio de actividades interrelacionadas hacia determinados elementos con el fin de obtener resultados." (p.59)

Es así que, la razón al discutir acerca de la identificación de procesos está determinada como unas estrategias que permiten dar apoyo, análisis de los sectores de la unidad, con el fin de determinar nuevas planificaciones capaces de neutralizar los inconvenientes presentados.

CAPÍTULO IV

En la presente Propuesta de mejora para la Gestión de Seguridad de la Información SGSI bajo normas ISO 27001, en el Departamento de la Unidad Nacional de Telecomunicación Móvil (UNATEM).

Se plantea lo siguiente:

- Diagnóstico
- Diseño de la Mejora
- Mecanismos de Control
- Beneficio/costo de la propuesta de mejora

4. Propuesta de Mejora

4.1. Diagnóstico

La UNATEM, es una Unidad investigativa de tecnológico investigativo para la Fiscalía General del Estado, a través de las disposiciones realizadas por la autoridad competente, con el fin de brindar elementos de convicción dentro de investigaciones con apoye técnico y tecnológico de la mano con los funcionarios que la integran, todo esto se lo hace a través del cumplimiento de políticas de gestión.

La información requerida se obtiene de diferentes maneras las cuales en algunos casos sirve como información relevante dentro de una etapa procesal dentro de la fiscalía, el tiempo que transcurre para la obtención es muy largo de hasta 4 meses de tiempo de espera, lo cual ocasiona en la mayoría de los casos que la información obtenida llegue a destiempo perjudicando notablemente una investigación, en vista que esta sirve de gran manera para la vinculación de un usuario con otros.

En la actualidad el Departamento de Análisis de Telecomunicaciones de la UNATEM, realiza un trabajo de maneja manual para los procedimientos de obtención y entrega de información, esto ocasiona que la información pase de mano en mano incumpliendo normas de manejo de información reservada y confidencial , la función judicial como ente solicitante no tiene establecido un procedimiento adecuado y seguro para la solicitud de la información a las operadoras telefónicas lo cual provoca pérdida de información relevante, y retraso en la obtención de la información validada para las diligencias judiciales; todos estos mecanismos actuales perjudican notablemente el cumplimiento acertado por parte de la Fiscalía y el aporte que realiza la UNATEM dentro de las investigaciones.

Dentro del diagnóstico actual podemos identificar a través del análisis FODA las siguientes Fortalezas, Oportunidades que podemos aprovechar para mejorar en el manejo y desempeño del manejo de seguridad de la información, de igual manera, conocer las debilidades que perjudican y entorpecen el manejo de información y amenazas que se presentarían como un riesgo latente y como se podría controlar y evitar.

TABLA 5
FODA DE LA UNATEM

FORALEZAS	OPORTUNIDADES
• Control y asesoramiento externo por parte de entidades de control gubernamental, mismas que permitirán llevar un mejor control y organización en procesos de seguridad de la información. • Manejo e implementación de políticas	• Realizar un plan de mejora de procedimientos para el manejo de seguridad de información, en cumplimiento a la normativa legal vigente, para el manejo de información de carácter reservada y confidencial, dentro de las investigaciones de la

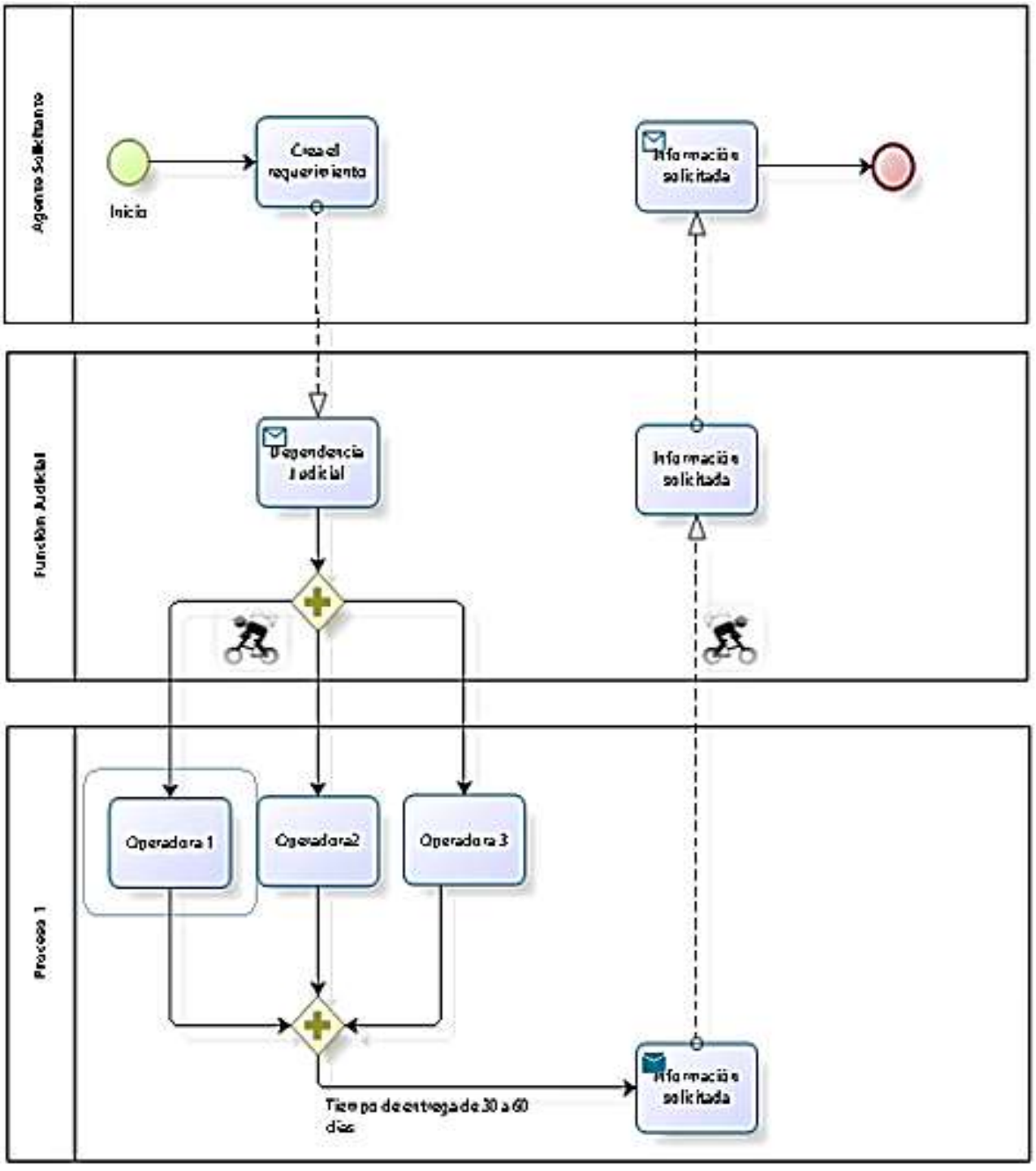
de seguridad interna para el talento humano a través de capacitación y control permanente del cumplimiento de funciones de acuerdo al perfil. • Departamento de TIC´s interno independiente, mismo que se encargará del control, manejo, mantenimiento y demás aspectos de su interés dentro de la infraestructura de tecnología para el correcto y adecuado funcionamiento. • Control biométrico de control para el talento humano, de acuerdo a los horarios de trabajo y niveles de seguridad en concordancia a la función designada. • Auditorías internas y externas permanentes, con el fin de verificar el funcionamiento de los sistemas, desempeño del talento humano y gestión administrativa para el correcto manejo de la información.	Fiscalía General del Estado. • Demostrar los beneficios a través de un direccionamiento más adecuado para mejorar la seguridad de la información con tecnología nueva que permita alcanzar los niveles de seguridad óptimos. • Capacitaciones constantes del talento humano de la Unidad, unidades del eje investigativo y Fiscalías de la función judicial en el manejo de la información, haciendo hincapié en la seguridad de la información, con el fin de establecer parámetros regulados en seguridad de información • Contemplar un presupuesto financiero anual, con el fin de implementar y desarrollar procedimientos y mejoras dentro de la seguridad de la información.
DEBILIDADES	**AMENAZAS**
• No contar con un departamento que sirva como respaldo (backup) para dar continuidad a la obtención de información presenta un riesgo permanente dentro de la Unidad. • El licenciamiento de software actual es mínimo incumpliendo la normativa legal que indica el uso de licencias originales y legales para el desempeño de las funciones establecidas dentro de la infraestructura tecnológica. • Bajo conocimiento dentro del campo de manejo de seguridad de la información,	• Licenciamiento de Antivirus insuficiente para la infraestructura tecnológica de la Unidad, lo cual ocasiona inseguridad y expone al departamento a cualquier ataque informático interno o externo, voluntario o involuntario. • Eliminación de información sin establecer protocolos de seguridad y control, con la falta de respaldos adecuados y cumpliendo la normativa legal vigente. • La falta de un equipo de seguridad perimetral (firewall) que sirva como

permitiendo el cometimiento de infracciones y errores muy básicos dentro del manejo de información, perjudicando en ocasiones las diligencias investigativas. • No se cuenta con políticas de seguridad estandarizadas, lo que dificulta un control adecuado y correcto para el manejo de información de carácter reservada y confidencial. • Falta de capacitación del talento humano de la Unidad, en referencia al manejo y protocolos que se deben seguir en seguridad de información. • Desinterés por parte del área directiva a los procesos y procedimientos que desea implementar el departamento de TIC´s para mejorar la gestión de seguridad de la información.	respaldo (backup), en el caso de fallas del actual, perjudicaría notablemente el cumplimiento de las diligencias investigativas solicitadas por la Fiscalía General del Estado, a través de la autoridad competente. • El Acceso no consentido y manipulación de la información generada, considerada de carácter reservada y confidencial, puede ocasionar graves perjuicios dentro de las investigaciones llevadas a cabo por la Fiscalía General de Estado y Unidades del eje investigativo. • Falta de capacidad operativa, talento humano no calificado para cumplir con funciones establecidas dentro de la unidad y talento humano calificado asignada a otras dependencias, perjudican el desenvolvimiento y cumplimiento de las diligencias judiciales.

La Tabla muestra las Fortalezas, Oportunidades, Debilidades y Amenazas en la UNATEM las cuales se puede aprovechar para mejorar el manejo y desempeño en la seguridad de la información: Elaboración propia

FIGURA **13**

DISEÑO ACTUAL



Nota: El diseño actual del manejo de la información en la UNATEM. Fuente Elaboración propia.

4.2. Diseño de la mejora.

La UNATEM al ser un eje de apoyo técnico hacia las Fiscalía General de Estado propone implementar nuevos métodos que permitan el cumplimiento de las delegaciones judiciales, de manera ágil y oportuna, entregando una información que cumpla el debido proceso, de acuerdo a la normativa legal del Estado Ecuatoriano tenemos:

- **Constitución de la República del Ecuador**

  La constitución en el Artículo 1 indica que “El Ecuador es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada. La soberanía radica en el pueblo, cuya voluntad es el fundamento de la autoridad, y se ejerce a través de los órganos del poder público y de las formas de participación directa previstas en la Constitución. Los recursos naturales no renovables del territorio del Estado pertenecen a su patrimonio inalienable, irrenunciable e imprescriptible.” (Constituyente, 2021)

- **Ley Orgánica de Protección de Datos Personales**

  El 26 de mayo de 2021 mediante Registro Oficial Suplemento No. 459 es publicada misma que “Tiene por objeto garantizar el derecho a la protección de datos personales, que incluye el acceso y decisión sobre la información y datos de este carácter, así como su correspondiente protección.

En lo principal, la ley se refiere a las condiciones que se deben verificar para que el tratamiento de datos personales sea legítimo. Se refiere, también, a las formas a través de las cuales el titular de los datos personales puede manifestar su voluntad para el tratamiento de sus datos. Regula, además, el contenido y alcance de los derechos:

1). A la información
2). De acceso
3). De rectificación y actualización;
4). De eliminación
5). De oposición
6). A la portabilidad
7). A no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas
8). De consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales
9). A la educación digital". (Ministerio de Telecomunicaciones, 2021)

- **Esquema Gubernamental de Seguridad de la Información – EGSI**

Mediante Acuerdo Ministerial No. 025-2019, el 14 de noviembre de 2019, se expide el "Esquema Gubernamental de Seguridad de la Información (EGSI)", mismo que manifiesta "…preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riegos de seguridad de la información y la selección de controles para el tratamiento de los riesgos identificados". (MINTEL, 2019)

Es así que teniendo claro los objetivos establecemos las directrices que se deben cumplir por parte del personal de la UNATEM, con el fin de precautelar la seguridad de la información. Con esto designaremos un responsable encargado de controlar y monitorear permanentemente los niveles de seguridad a ser implementados con el fin de prevenir el cometimiento de acciones incorrectas dentro del maneo de la información, todo esto debe ir de la mano de la normativa legal vigente dentro de la Constitución, los responsables de la seguridad de la información deberán, documentar, actualizar las políticas de acuerdo a las disposiciones que se vayan implantando, de igual manera pruebas de estrés con el fin de verificar las normas establecidas y mejores que pueden ser implementadas de acuerdo a la necesidad presentada.

De acuerdo a las políticas de seguridad sugeridas para la UNATEM debemos establecer a través de un análisis de riesgos, en función de los activos de la información que se genera dentro de la Unidad, mismo que presentará un análisis cuantitativo y cualitativo, basada en la arquitectura de procesos PDCA (Plan – Do – Check – Act), estimación cualitativa de riesgos PGV (Probabilidad, Gravedad, Vulnerabilidad); esto nos llevará a definir un aspecto de amenazas misma que se divide en humanas, naturales y tecnológicas.

Para esto se debe definir los parámetros que deber ser tomados en cuenta para SGIS, el cual permitirá garantizar la confidencialidad, integridad y disponibilidad de la información generada dentro de la Unidad.

En este punto podemos indicar los actores externos que se

encargarán de ejecutar los diferentes requerimientos de información como son: los Sres. Fiscales o por Agentes del eje investigativo, realizarán el requerimiento a través del Sistema Informático implementado por la Fiscalía General del Estado, dentro del debido proceso (Investigación Previa, Instrucción Fiscal, Actuaciones Fiscales Urgentes y Actuaciones.

Los Defensores Públicos y Privados, dentro del debido proceso (Investigación Previa, Instrucción Fiscal, Actuaciones Fiscales Urgentes y Actuaciones Administrativas), cumpliendo con los requisitos legales y constitucionales que permitan recabar, registrar y entregar la información de manera oportuna de conformidad a lo que dispone el Manual de Procedimientos de la UNATEM.

De igual manera los agentes internos se presentarán como Analistas de operaciones mismo que se encargarán a través del uso de los Sistemas Informáticos de las Operadoras Telefónicas, de obtener la información solicitada, en cumplimiento de la normativa legal, manuales, instructivos, protocolos y normas técnicas relacionadas, a fin de garantizar el buen uso y manejo de la información evitando que haya alteración o difusión no autorizada de la misma.

Almacenar en un motor de Base de Datos especializada la información obtenida de los Sistemas Informáticos de las Operadoras de Servicio Móvil

Avanzado (SMA), a fin de que los diferentes organismos de control realicen las verificaciones y auditorías en el ámbito de sus competencias, cuando estos lo estimen pertinente, debiendo mantener

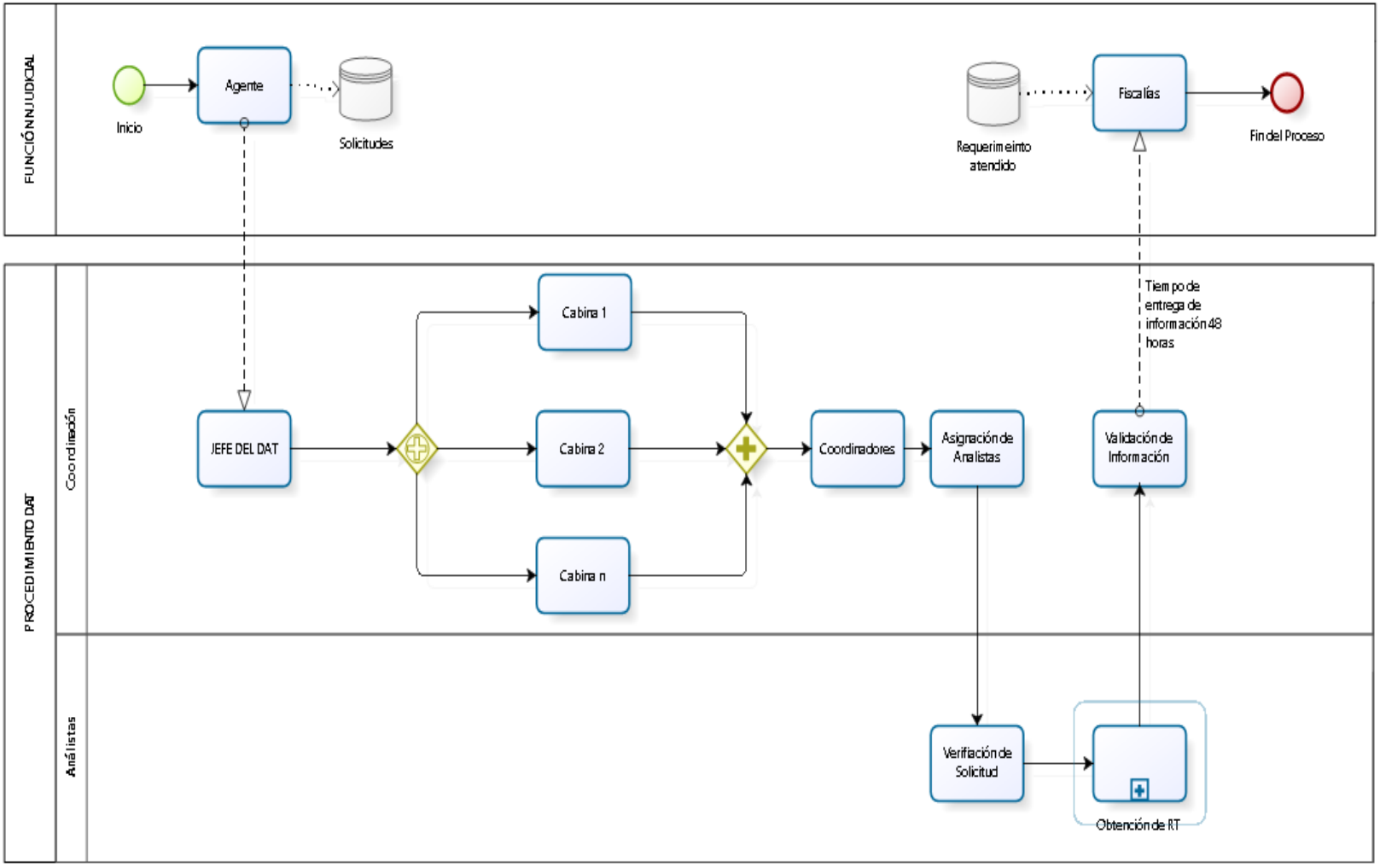
la reserva que la ley exige.

Garantizar que la información obtenida a través de los Sistemas Informáticos Implementados por las Operadoras de Sistema Móvil Avanzado (SMA), sea procesada con aplicación del Manual de Procedimientos y los Instructivos correspondientes, cumpliendo con la reserva por parte de los y las servidores públicos que integran la UNATEM, de conformidad con lo dispuesto en los artículos 490, 576, 584 del COIP y lo referente a actuaciones y técnicas especiales de investigación bajo las penas previstas para estos casos en el mismo cuerpo legal. Reducir los tiempos de respuesta constituyéndose en una herramienta de apoyo en las investigaciones que realiza la Fiscalía General del Estado y el Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses.

Garantizar la seguridad de la información, especialmente cuando se trate de obtención, registro y entrega, generando mecanismos de control o para evitar y prevenir posibles fugas de información o mal uso de la misma, hasta que se realice la entrega de los indicios y elementos de convicción a los sujetos procesales a quienes la ley faculta su requerimiento.

Con el fin de obtener un insumo para ser transformado en elemento de convicción, con la celeridad que el proceso investigativo pre procesal y procesal penal lo requiere, se ha visto la necesidad de implementar nuevos procedimientos y políticas de manejo de información de manera oportuna y segura como se muestra en la siguiente gráfica:

FIGURA 14
DISEÑO DE MEJORA



Nota: El diseño de mejora del manejo de la información en la UNATEM. Fuente Elaboración propia.

4.3. Mecanismos de control.

Los mecanismos de Control en la propuesta consisten en implementar sistemas dentro de la Unidad que permitan realizar todo este trámite de manera automática a través de conexiones con las instituciones de tecnología móvil, para la obtención de información en tiempo no mayor a 48 horas y de esta manera presentar la información con políticas de seguridad de información muy necesarias ya que la información que se maneja internamente en sensible y reservada para el área judicial.

TABLA 6
CONTROLES SEGÚN LA NORMA ISO/IEC 27001

ID	Controles según la norma ISO/IEC 27001	Estado Actual	Brecha	Estado Esperado	Nivel
A.5	Políticas de seguridad de la información	3%	97%	100%	Inicial
A.6	Organización de la seguridad de la información	5,00%	95%	100%	Inicial
A.7	Seguridad relacionada con el personal	25,00%	75%	100%	Inicial
A.8	Gestión de activos	30,00%	70%	100%	Repetible
A.9	Control de acceso	30,00%	70%	100%	Repetible
A.10	Criptografía	3%	97%	100%	Inicial
A.11	Seguridad física y del entorno	50%	50%	100%	Repetible
A.12	Seguridad operativa	23,00%	77%	100%	Repetible
A.13	Seguridad de las comunicaciones	16%	84%	100%	Repetible
A.14	Adquisición, desarrollo y mantenimiento de sistemas	20,00%	80%	100%	Inicial
A.15	Relaciones con proveedores	35%	65%	100%	Inicial
A.16	Gestión de los incidentes de seguridad de la información	10%	90%	100%	Inicial
A.17	Aspectos de seguridad de la información en la gestión de continuidad de la Unidad	0%	100%	100%	Inicial
A.18	Cumplimiento	0%	100%	100%	Inicial
	TOTAL PROMEDIO	18%			

La Tabla muestra los controles según la norma ISO/EIC 27001 Fuente Elaboración Propia

Dentro de los mecanismos de control a ser implementados, tomando en cuenta el manejo de información reservada, se tiene previsto:

La contratación de servicios tecnológicos

La contratación de servicios tecnológicos que permitan el correcto desempeño del trabajo realizado por los diferentes funcionarios que laboran dentro del departamento en la UNATEM, los cuales detallamos los mecanismos de control en la siguiente tabla:

TABLA 7
MECANISMOS DE CONTROL

ORD	DETALLE	CONCEPTO	APLICABILIDAD
1	**Seguridad Perimetral (Firewall)**	La seguridad perimetral (firewall) permitirá la combinación de aplicaciones informáticas y mecanismos, misma que servirá para la seguridad de equipos físicos, detección de ataques, intrusos de las instalaciones de mayor relevancia y sensibilidad. (Ramirez Villarreal, 2022)	Se implementará dentro del data center del departamento con el fin de brindar seguridad y administrar permisos a los diferentes usuarios con su respectivo perfil.
2	**Data Center Virtual (CLOUD)**	Data center virtual o (CLOUD) son contenedores de red privados, en el cual podemos colocar servidores virtuales con sus respectivas características técnicas, software y configuración, políticas de seguridad y protección. (Medara, 2023)	Permitirá incorporar servidores de manejo de un sistema documental, servidor SFTP para la recepción de información reservada encriptada y cifrada, servidor Backup que permita terne un repositorio de la información en caso de pérdidas y un firewall lógico que permita

			brindar las seguridades necesarias para los equipos alojados dentro del DCV.
3	**Switch Administrable**	Un Switch administrable permite aislar el tráfico de acuerdo al grupo y función dentro de su perfil asignado, copias de seguridad, administración entre otros. Esto permite adquirir una protección firme para la red. (Woton, 2023)	Permitirá llevar una mejora administración y proporcionará seguridad a la red del departamento con el fin de establecer políticas de uso de acuerdo al perfil del usuario.
4	**Computador Personal**	Un computador personal es un ordenador o PC rentable de uso general que está desarrollada para el uso de un único usuario, cada una dependerá de la tecnología que presente lo cual permitirá al usuario cumplir sus funciones establecidas. (theastrologypage, 2023)	Los computadores personales serán para trabajo exclusivo de los usuarios de los aplicativos que se usaran para extraer información, la cual deberá contar con sus respectivos permisos de acuerdo al perfil del usuario.
5	**Antivirus**	Es un tipo de software que es usado para detectar, evadir, buscar y eliminar virus que se encuentran dentro de un ordenador con el único fin de realizar daños. (Espinoza, 2022)	Licencias de antivirus que permitan mantener la seguridad de los equipos en todo momento con el fin de evitar posibles ataques o infecciones.
6	**UPS – TRIFASICO DE 6KVA**	EL UPS (Uninterruptable Power Supply), conocido también como sistema de alimentación	El UPS permitirá mantener una alimentación eléctrica permanente dentro del

		Ininterrumpida (SAI) el cual permite mantener un flujo de energía eléctrica permanente a través de baterías, en el momento de un fallo eléctrico. (TRANSELEC, 2022)	departamento en el caso de que exista una pérdida de fluido eléctrico, de acuerdo al trabajo 7/24/365.
7	**Cableado Estructurado**	El cableado estructurado compone una plataforma por la cual viaja información de voz, datos, imágenes y otros; mismo que ofrece necesidades generales en referencia a la transmisión confiable de información. Esto permite una organización de conexión física dentro de un área determinada, y permite acoplarse a los diferentes cambios de acuerdo a la necesidad requerida. (Chileno Campos, 2023)	Implementación de un cableado estructurado con puntos certificados que permitirá el correcto funcionamiento de la comunicación de la red y flujo de información que se maneja dentro del departamento de la UNATEM.
8	**Enlaces de Datos**	Un enlace de datos corresponde a un método para conectar un lugar a otro, lo cual permitirá emitir y obtener datos de manera digital, esta transferencia se realizará de acuerdo a protocolos establecidos permitiendo el traslado de datos de un lugar a otro. Dentro del modelo OSI en redes, este enlace compone básicamente la 2da. capa, la	Se realizará una conexión de enlaces de datos principal y backup asimétrico y dedicado, con cada uno de nuestros proveedores del sistema móvil, con el fin de establecer y mantener una conexión permanente de tráfico de información segura.

		cual brinda instrucciones y funciones para el traspaso de información logrando censurar errores que se pueden presentar dentro de la capa física. (Vinicio, 2023)	
9	**Control de Acceso Biométrico**	Un control de acceso biométrico, sirve como sistema de identificación personal el cual permitirá llevar un registro del talento humano, siendo administrable permitiendo el registro de características predeterminadas como el ingreso autorizado de acuerdo al perfil, control de horario de entrada y salida. (Bizneo, 2022)	Con la implementación de un controla de acceso biométrico que valide la huella y el rostro se podrá establecer horarios de entrada y salida del personal, acceso único de acuerdo al perfil y responsabilidades.

La Tabla muestra los mecanismos de control. Fuente Elaboración Propia.

Seguridad de la Información

La UNATEM con el fin de mejorar sus procedimientos ha impulsado una estratégica de seguridad de información, estableciendo procedimientos y protocolos de manejo de información con las debidas políticas de usuarios dependiendo de su perfil, con el fin de evitar manipulación maliciosa, perdida de información, y demás aspectos que pueden ir apareciendo, para esto se ha visto necesario la implementación de políticas de seguridad de datos, mismas que se rigen por las siguientes normas:

- Clasificación de la información, misma que debe ser protegida en toda circunstancia, considerando la integridad y manejo seguro, permitiendo el

acceso únicamente a personal calificado.

- Exponer técnicas básicas de seguridad de la información que la Unidad debe establecer para proteger de eventos peligrosos que afectarían la privacidad, respetabilidad y acceso a la información.
- Socializar a todo el personal de la Unidad acerca de la importancia de la seguridad de la información y funciones estratégicas de cada uno.
- El área administrativa implementará normas y políticas que permitan registrar un control del uso de recursos de información y protección de la misma. Los clientes que no respeten la estrategia, los principios y los métodos de seguridad de los datos de la empresa pueden enfrentarse a sanciones según los términos de los contratos que firmen con la empresa y la legislación aplicable.

Para efecto de la Unidad la función judicial y el ente regulatorio de la UNATEM le corresponderá asignar al personal que pasarán a cumplir con las funciones de acuerdo al perfil asignado, cumpliendo requisitos primordiales con el fin de ser acreditados como idóneos, lo cual es aprobar las evaluaciones integrales de confianza (pruebas socioeconómicas, toxicológicas y de polígrafo) lo cual lo acreditará para ser designado y pueda permanecer en la Unidad.

De igual manera presentamos las funciones de acuerdo al perfil de usuario con el fin de mejorar el rendimiento y productividad aplicando normas de seguridad de información y procedimientos establecidos:

TABLA

NORMAS DE SEGURIDAD DE INFORMACIÓN Y PROCEDIMIENTOS ESTABLECIDOS

ORD.	GESTIÓN	OBSERVACIONES
1	Fiscal	Coordinar en conjunto con el jefe de departamento el correcto funcionamiento de los aplicativos desarrollados por las operadoras telefónicas y demás obligaciones y funciones que se presenten y estén acorde al cargo dentro de sus funciones.
2	Jefe de Unidad	El Jefe establecerá políticas de administración de recursos, planificará y supervisara el personal acreditado para el departamento, gestionará la actualización de software y hardware para fortalecer y garantizar el adecuado funcionamiento, tendrá acceso a los aplicativos únicamente como administrador de cuentas usuarios para la habilitación, creación, asignación y eliminación de usuarios dependiendo del perfil del servidor judicial.
3	Coordinador Operador	El coordinador tendrá una política de navegación únicamente para los aplicativos de gestión documental interna y correo electrónico institucional, con el fin de mantener la reserva de la información y llevar un control permanente, realizará el uso correcto de las cuentas de usuario de Fiscalía, validará la información obtenida dentro de los aplicativos por parte de los analistas de operadora, supervisará y controlará las actividades desarrolladas por los

		analistas y demás funciones asignadas de acuerdo a su perfil.
4	Analista Operadora	El analista tendrá una política de navegación únicamente para los aplicativos de obtención de información sin salida al internet, esto con el fin de evitar filtración de información a agentes externos y ajenos a la función judicial. Realizará la obtención de información dentro de los aplicativos de las operadoras, realizará el análisis de la información y reportará la existencia de inconsistencias dentro de la información obtenida y del funcionamiento del aplicativo y demás funciones asignadas de acuerdo a su perfil.
5	Perfil Técnico	El perfil técnico realizará el control físico y virtual de cada uno de los equipos de la red, conexiones de enlaces, coordinación con proveedores técnicos externo, soporte técnico preventivo y correctivo de la Unidad. Verificará el correcto funcionamiento y uso del hardware y software del departamento, se realizará el mantenimiento preventivo y correctivo de acuerdo a una planificación anual establecida, realizar auditorías internas del funcionamiento y manejo de los aplicativos y demás funciones asignadas de acuerdo a su perfil.

6	Analista Estratégico	El analista estratégico se encargará de realizar un análisis estadístico de rendimiento de productividad de acuerdo a los tiempos y carga de diligencias y demás funciones asignadas de acuerdo a su perfil.

La Tabla muestra las normas de la seguridad de la información. Fuente Elaboración Propia.

Implementación de Políticas y Procedimientos de Seguridad

La implementación de políticas y procedimientos de seguridad son de suma importancia dentro de la Unidad, en vista de que al gestionar información de carácter reservada y privada es de gran importancia para las investigaciones que llevan a cabo la función judicial, vemos la necesidad de implementar mejoras en los procedimientos, políticas, recursos tecnológicos, que permitan mejorar de manera efectiva la obtención, análisis y entrega de información.

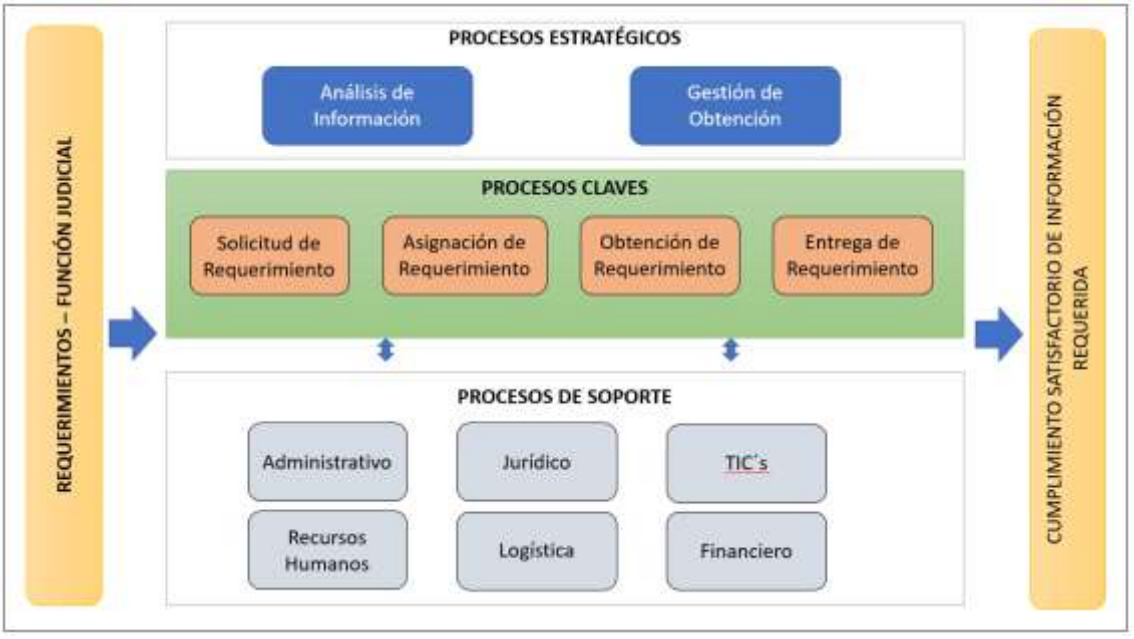
La implementación de procedimientos que gestionen tecnologías amigables para el medio ambiente incluye herramientas y servicios, como pueden ser servicios de consultoría, asesoría técnica, legal, capacitación y más; lo cual nos lleva a obtener resultados dentro de la reducción de insumos que provocan el alto grado de gasto y ambiental y física de las cosas, por esta razón, la implementación dentro de este proyecto es realizar procedimientos con el uso de la tecnología y así eliminar el uso de papelería, insumos de tinta, dispositivos de almacenamiento CD o DVD, lo cual provoca un gasto enorme dentro de la Unidad al realizar un promedio de 24.000 RT anuales provocando un costo ambiental muy perjudicial.

Alcance de SGSI

Los límites de la Unidad y el cumplimiento del SGSI, deberán ser establecidos y cumplidos por el talento humano de la unidad sin excusa ni excepción, de igual manera las personas externas que tienen acceso a los recursos de datos. La política debe ser aplicada a todos los procedimientos internos de la Unidad y abarca todo tipo de información que se obtenga a través de papeles (escritos o impresos), se almacene digitalmente o se remita a través de correos institucionales u otros periféricos de almacenaje de información. La seguridad de la información de los directivos debe estar acorde a los principios de la norma ISO/IEC 27001:2013, así como también todo requerimiento legítimo, administrativo u otros. Presentamos los elementos que influyen en el alcance del SGSI:

Procesos y Servicios

FIGURA 15
PROCESO Y SERVICIOS



Nota: la figura muestra los procesos y servicios en la institución de la UNATEM. Fuente Elaboración propia

La seguridad de la información dentro de la organización y el desarrollo de procesos de la UNATEM, se establece en todos los pasos de ayuda mismos que son funcionales y vitales, especialmente en los procesos claves, esto con el fin de establecer la seguridad de la información de manera efectiva, considerando la gestión de riesgos y los requisitos establecidos en los reglamentos con el fin de incrementar la seguridad tanto de los ejes externos que van hacer uso de la información remitida.

Ubicaciones:

TABLA 8
UBICACIONES

Procesos Claves	Proceso	Responsable	Descripción
Solicitud de Requerimiento	Solicitud de diligencias investigativas	Fiscalías y Unidades Especializadas	Comprende el proceso de solicitar a la unidad, la información que apoye a las investigaciones a través dentro del área tecnológica.
Asignación de Requerimiento	Verificar y asignar la diligencia investigativa	Jefe del Departamento y Coordinadores	Comprende en realizar un análisis del requerimiento solicitado para asignar a un analista.
Obtención de Requerimiento	Obtener la diligencia investigativa asignada.	Analistas operadores	Comprende en obtener la información requerida por la FGE y Unidades Especializadas.

Entrega de Requerimiento	Validar y entregar la información solicitada	Coordinadores	Comprende en realizar una validación y verificación del requerimiento atendido para proceder a enviar la información solicitada.

La Tabla muestra las ubicaciones. Fuente Elaboración Propia

4.4. Beneficio/costo de la propuesta de mejora

La implementación de políticas y procedimientos de seguridad son de suma importancia dentro de la Unidad, en vista de que al gestionar información de suma importancia para las investigaciones que llevan a cabo la función judicial, vemos la necesidad de implementar mejoras en los procedimientos, políticas, recursos tecnológicos, que permitan mejorar de manera efectiva la obtención, análisis y entrega de información.

Evaluación económica financiera

TABLA 9
EVALUACIÓN ECONÓMICA FINANCIERA

DATOS DEL PROYECTO

	Horas por día	8
	Días por mes	22
	Costo por Hora / Personal TIC's	USD. 40,00
	Costo por día / Consultor externo	USD. 85,00
	Costo por Hora Coordinador de Gestión ISO	USD. 30,00
	Costo por Hora Auditor	USD. 55,00
	Duración del Proyecto por meses	5

La Tabla muestra la evaluación económica y financiera. Fuente Elaboración Propia.

TABLA 10
COSTOS DE RECURSO DEL PERSONAL

COSTO DE RECURSOS DE PERSONAL DE TRABAJO POR HORAS											
Rol	1er. Mes		2do. Mes		3er. Mes		4to.Mes		5to. Mes		TOTAL
	Participación por horas	Total / mes	Participación por horas	Total / mes	Participación por horas	Total / mes	Participación por horas	Total / mes	Participación por horas	Total / mes	
Personal TIC's	160	6400	160	6400	160	6400	160	6400	172	6880	32.480,00
Consultor externo	88	7480	88	7480	88	7480	88	7480	88	7480	37.400,00
Coordinador de Gestión ISO	160	4800	160	4800	160	4800	160	4800	160	4800	24.000,00
Auditor	0	0	0	0	0	0	0	0	88	4840	4840
TOTAL											98.720,00

La Tabla muestra los costos del recurso del personal. Fuente Elaboración Propia

Presupuesto del proyecto

TABLA 11
PRESUPUESTO DEL PROYECTO

Presupuesto del Proyecto	
Equipo de Trabajo	98.720,00
Inversión Tecnológica	18.900,00
Reserva de Contingentica (5%)	5.881,00
Total Línea Base	123.501,00
Reserva de Gestión	6.175,05
Presupuesto del proyecto	129.676,05

La Tabla muestra el presupuesto del proyecto. Fuente Elaboración Propia

TABLA 12
BENEFICIOS ESPERADOS

BENEFICIOS ESPERADO MENSUAL	
Promedio de gastos de obtención de información antes de implementar	60.000,00
Promedio de gastos de obtención de información después de implementar	6.000,00
Beneficio	54.000,00

La Tabla muestra los beneficios esperados. Fuente Elaboración Propia

CAPÍTULO V

Conclusiones

- Que, se ha formulado una propuesta de mejora para la Gestión de Seguridad de la Información SGSI bajo normas ISO 27001 del Departamento de Análisis de Telecomunicaciones de la Unidad Nacional de Telecomunicación Móvil, el cual cumple con todos los parámetros establecidos dentro de la normativa legal, para brindar un servicio adecuado que sirva como evidencia irrefutable dentro de una investigación.
- Que, se ha diagnosticado e implementado un modelo de flujo adecuado y cumpliendo la normativa legal vigente, permitiendo un mejor desempeño para la obtención y manejo de la información, que se genera dentro del Departamento de Análisis de Telecomunicaciones de la UNATEM.
- Que, se implementará procedimientos, políticas de seguridad, procesos y servicios, que permitan de manera eficientemente el manejo de información, con procedimientos acertados y seguros, lo cual representa un ahorro muy significativo de USD. 54.000,00 enfocado en las eventualidades de seguridad de información.
- Que, el desarrollo e implementación de un sistema informático que permita controlar y manejar el flujo de información, utilizando políticas de seguridad de la información lo cual permitirá un manejo ágil y seguro, con un ahorro significativo en el consumo de papel, de esta manera ayudando al medio ambiente.
- Que, la implementación de un modelo de flujo adecuado y cumpliendo la normativa legal vigente, permite un mejor desenvolvimiento del proyecto se

aprecia muy rentable al permitir reducir los incidentes y riegos en seguridad de la información, en razón de los gastos antes de la implementación representaba un gasto de USD. 60.000,00 y una vez implementada su gasto mensual representa un valor de USD. 6.000,00.

- Que, se ha identificado la vulnerabilidad dentro de la gestión en manejo de datos dentro de la Unidad, lo cual permitirá manejar las debilidades y falencias, y de esta manera poder tener un mejor control interno de la confidencialidad, integridad y disponibilidad de la información.
- Que, el diseño e implementación de un Sistema de Gestión de Seguridad de la Información - SGSI, permite reconocer los riegos y vulnerabilidades, que afectan notablemente el desenvolvimiento y manejo de información reservada y confidencial, dentro del Departamento de Análisis de Telecomunicaciones de la UNATEM.

Recomendaciones

- Se debe socializar al personal de la Unidad siempre acerca de los riesgos y vulnerabilidades que se pueden presentar con el fin de estar preparados para cualquier tipo de anomalía que pueda presentarse dentro de la ejecución de su trabajo.
- Se debe realizar controles permanentes y periódicos con el fin de verificar posibles vulnerabilidades y riesgos que pueda afectar el cumplimiento de las diligencias solicitadas.
- Se debe mantener actualizadas las políticas de seguridad de la información de la Unidad, en razón de que la información siempre va a estar de manera expuesta a amenazas (humanas, tecnológicas y naturales).
- Se debe implementar acciones de prevención que permitan actuar de manera oportuna al ataque de cualquier tipo, manteniendo una capacitación permanente del personal encargado de resguardar la seguridad de la información dentro de la Unidad.
- Se debe llevar un control y actualización de la infraestructura tecnológica, con el fin de mantener con control adecuado y seguro de la información que se desarrolla dentro de la Unidad.

Bibliografía

Alanoca Ticona, Y. (17 de 06 de 2022). *https://repositorio.neumann.edu.pe*. Obtenido de https://repositorio.neumann.edu.pe/items/73bfa3b3-015b-4985-8101-6dc003de6b8e/full

Alvaro, G. (2022). *Auditoría de Seguridad Informática.* Bogotá: StarBook .

Baldecchi, R. Q. (2014). Implementación efectiva de un SFSI ISO 27001. *V Congreso Internacional sobre Gobierno, Riesgos, Auditoria y Seguridad de la Información* (pág. 6). Montevideo: CIGRAS.

Bizneo. (2022). *https://www.bizneo.com/.* Obtenido de https://www.bizneo.com/blog/control-de-acceso-biometrico/#:~:text=El%20control%20de%20acceso%20biom%C3%A9trico%20es%20un%20sistema%20de%20identificaci%C3%B3n,jornada%20laboral%20de%20los%20trabajadores.

Bron B, M. O. (01 de 01 de 2022). *https://revistas.unesum.edu.ec/*. Obtenido de https://doi.org/10.47230/unesum-ciencias.v6.n1.2022.289

Carmen, D. P., Jose, L., & Santiago, R. (2019). *Organizacion y Transformacion de los sistemas de informacion en la empresa.* Madrid: ESIC EDITORIAL.

Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI). IEEE* (págs. 1-6.). Funchal, Portugal: IEEE.

Castro, M. F., Contreras, S. Y., & Pazmiño, I. O. (2018). Los sistemas de información y su importancia en la transformación digital de la empresa actual. *ESPACIOS*.

Chicaiza Castillo, D. V. (ene de 2020). *https://repositorio.uta.edu.ec/jspui/handle/123456789/30690.*

Chileno Campos, C. A. (30 de 01 de 2023). *http://repositorio.unjfsc.edu.pe/handle/20.500.14067/7282.* Obtenido de http://hdl.handle.net/20.500.14067/7282

Ciudad Maestro, E. (2014). La gestión de la calidad en las organizaciones de educación superior. Aportación del enfoque de la Organización Internacional de Normalización (ISO). *Revista Complutense de Educación-Universidad Complutense de Madrid*, 647-686.

Constituyente, A. (25 de 01 de 2021). *www.defensa.gob.ec.*

Ecuador, A. N. (21 de Mayo de 2021). Ley Orgánica de Protección de Datos Personales. *Ley Orgánica de Protección de Datos Personales*. Quito, Pichincha, Ecuador.

Ecuador, C. d. (25 de Enero de 2021). Constitución de la Reública del Ecuador. *Registro Oficial 449 de 20-oct-2008*. Quito, Pichincha, Ecuador.

Encalada Vargas, E. (2019). Sistemas de información como herramienta para reorganizar procesos de manufactura. *Revista venezolana de gerencia Vol 24*, 24 al 85.

Equipo editorial, Etecé. (13 de Junio de 2022). *https://concepto.de/software/. Última edición.* Recuperado el 01 de octubre de 2022

Espinoza, J. (05 de 2022). *Repositorio Dspace.* Obtenido de http://repositorio.ulasamericas.edu.pe/handle/123456789/3423

Garzón Santos, C. A. (11 de 10 de 2021). *http://repositorio.unal.edu.co/handle/unal/80759.* Recuperado el 01 de 10 de 2022

Gerencia, R. V. (2018). *Gestión Tecnológica en pymes del sector.* Maracaibo.

Gómez, Á. (2022). *Auditoría de seguridad informática.* Ediciones de la U.

Hernandez Trasobares, A. (2003). Los Sistemas de Información: Evolución y Desarrollo. *Universidad de Zaragoza*, 14.

Hernández, M. (04 de 2022). *https://ojs.supercias.gob.ec*. Obtenido de https://ojs.supercias.gob.ec/index.php/X-pedientes_Economicos/article/view/100

Isabel, V. S., & López E, P. A. (2011). Fundamentos de ISO 27001 y su AplicacIÓN en las Empresas. *ScintiaEt Tchnica, vol. XVII, núm. 47 - Univeridad Tecnológica de Pereira*, 334.

ISO2700.es. (02 de 10 de 2022). *ISO2700.es*. Obtenido de https://www.iso27000.es/sgsi.html

Jesús Guasch, J. T. (07 de 2022). *https://espaciospublicos.uaemex.mx*. Obtenido de https://espaciospublicos.uaemex.mx/article/view/19292

Juan Carlos De la cruz Maldonado, D. A.-A., & [, J. M.-Q. (s.f.).

Juan Carlos De la Cruz, D. A. (2022). *dialnet.unirioja.es*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8403333

Junaid, T. S. (01 de 2023). *https://www.researchgate.net*. Obtenido de https://www.researchgate.net/publication/367166657_ISO_27001_Information_Security_Management_Systems?enrichId=rgreq-7972c0eb571b2ad8298f2db088676658-XXX&enrichSource=Y292ZXJQYWdlOzM2NzE2NjY1NztBUzoxMTQzMTI4MTExMzMxNDgyNEAxNjczODQ4NDAyNjkw&el=1_x_2&_esc=pu

Ladino A., M. I., Villa S. , P. A., & López E., A. M. (2011). Fundamentos de ISO 27001 y su Aplicación en las Empresas. *Scientia et Technica Año XVII, No 47*, 334-339.

Laura Mayer Lux, J. V. (06 de 2022). *Revista chilena de derecho y tecnología.*

Obtenido de http://dx.doi.org/10.5354/0719-2584.2022.65299

Limón, M. L. (2018). Tecnologías de información y desempeño organizacional de las pymes del noreste de. *Revista Venezolana de Gerencia, 2018, vol. 23, núm. 82, April-June, ISSN: 1315-9984*, 15.

Magazine, A. (2023). *https://www.tuvsud.com*. Obtenido de https://www.tuvsud.com/es-es/servicios/formacion/academy-magazine/metodologia-magerit

Medara, R. S. (2023). Consolidación dinámica de máquinas virtuales en un centro de datos en la nube mediante la optimización de onda de agua modificada. 45.

Ministerio de Telecomunicaciones. (26 de 05 de 2021). *https://www.telecomunicaciones.gob.ec/.* Obtenido de https://www.telecomunicaciones.gob.ec/

MINTEL. (10 de 01 de 2019). *www.gobiernoelectronico.gob.ec.* Obtenido de www.gobiernoelectronico.gob.ec

Montaño Orrego, V. (2011). La gestión en la seguridad de la información según Cobit, Itil e Iso 27000. *Revista Pensamiento Americano-SSN: 2027-2448 Vol 2 No. 6.*, 21-23.

Nuchera, A. H. (1999). La gestión de la tecnología como factor estratégico de la competitividad industrial. *Economía Industrial*, 54.

Orostegui Forero, F. (2022). *http://repository.unipiloto.edu.cO*. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/12289

Ortiz, J. H., & Bayona-Oré, S. (2019). Implementación de un Marco para el Gobierno TI en una Entidad Financiera. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 103.

Palacios, Y. E., & Moreno, L. (2018). *Diseño de un Sistema de Gestión de Seguridad*

de la Información (SGSI) bajo la Norma ISO 27001:2013 para la Empresa UNISANAR IPS DE Quibdó. Quibdó, Chocó: Universidad Nacional Abierta y a Distancia – UNAD.

Peralta Castro, R. G. (20 de 10 de 2022). *http://repositorio.ulasamericas.edu.pe/*. Obtenido de http://repositorio.ulasamericas.edu.pe/handle/upa/2572

Pérez, M. D. (2018). Procedimiento para el diseño de Sistemas de Gestión de Información en Cooperativas de Producción. *Dialnet Métricas*.

Postigo Palacios, A. (2020). *Seguridad Informatica.* Madrid: Ediciones Paraninfo S.A.

R. Soage Santos, E. G. (2022). *https://www.taylorfrancis.com*. Obtenido de https://www.taylorfrancis.com/chapters/oa-edit/10.1201/9781003308829-26/calibration-cone-penetrometers-according-international-organization-standardization-requirements-soage-santos-g%C3%B3mez-meyer-peuchen-yetginer-lunne-carrington

Ramirez Villarreal, M. (09 de 09 de 2022). *http://repositorio.uigv.edu.pe/handle/20.500.11818/6559.* Obtenido de http://intra.uigv.edu.pe/handle/20.500.11818/6559

Remache Típan, M. L. (02 de 2022). *http://bibdigital.epn.edu.ec*. Obtenido de http://bibdigital.epn.edu.ec/handle/15000/22414

Rene Aquino Arcata, R. Z. (09 de 2021). *https://revistas.ulasalle.edu.pe/*. Obtenido de https://revistas.ulasalle.edu.pe/innosoft/article/view/56

Rodríguez Y. (2018). Modelo de uso de información para la toma de decisiones estratégicas en organizaciones de información. *Coleccion Brasil*, 14.

Ronald M. Hernández, I. S. (2019). Tecnología de Información y Comunicación (TIC) y su práctica en la evaluación educativa. *Propósitos y Representaciones*.

Saara Tenhunen, T. M. (09 de 01 de 2023). *https://arxiv.org/*. Obtenido de

https://arxiv.org/abs/2301.03554

Sierra Huertas, T. (05 de 01 de 2023). *https://repository.unad.edu.co/*. Obtenido de https://repository.unad.edu.co/

Silva G., Z. J. (03 de 2022). *https://dialnet.unirioja.es/*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8383507

Soriano, M. (2014). *Seguridad en redes y seguridad de la información .* Technická 2, Praha 6, Czech Republic: České vysoké učení technické v Praze.

Telecomunicaciones, M. d. (14 de Noviembre de 2019). Esquema Gubernamental de Seguridad de la Información - EGSI. *Acuerdo Ministerial Nro. 025-2019*. Quito, Pichincha, Ecuador.

Terán Bustamante, A., Dávila Aragón, G., & Castañón Ibarra, R. (2019). Gestión de la tecnología e innovación: un Modelo de Redes Bayesianas. *SCielo*, 63-100.

theastrologypage. (2023). *https://es.theastrologypage.com/personal-computer.* Obtenido de https://es.theastrologypage.com/personal-computer

TRANSELEC. (01 de 11 de 2022). *https://www.transelec.com.ar/.* Obtenido de https://www.transelec.com.ar/soporte/18411/

Trasobares, A. H. (s.f.). *https://dialnet.unirioja.es/*. Obtenido de https://dialnet.unirioja.es/servelt/artivulo?codigo=793097

Vecino, P. H. (2017). ISO standards and reference framework for ICT governance. General revision. *Fundación Dialnet*, 81.

Venegas Loor, L. V. (25 de 01 de 2023). *repositorio.unesum.edu.ec.* Obtenido de http://repositorio.unesum.edu.ec/handle/53000/4741

Vinicio, V. (25 de 01 de 2023). *http://repositorio.unesum.edu.ec.* Obtenido de http://repositorio.unesum.edu.ec/handle/53000/4741

Woton. (30 de 01 de 2023). *https://community.fs.com/.* Obtenido de

https://community.fs.com/es/blog/managed-switch-vs-unmanaged-switch-which-to-choose.html

Yisel Niño Benitez, N. S. (2018). Requisitos de Seguridad para aplicaciones web. *Revista Cubana de Ciencias Informáticas*.