UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

TEMA:

"PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A."

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

SUBLINEA DE INVESTIGACIÓN: Seguridad de Unidades Informáticas

AUTOR: Christian Damian Torres Chango

TUTOR: Ing. Dennis Chicaiza, Mg.

Ambato – Ecuador

Enero 2020

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación con el tema: "PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A.", del Sr. Christian Damián Torres Chango, estudiante de la Carrera de Ingeniería en Sistemas Computacionales Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe final reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato, enero de 2020

EL TUTOR

Ing. Dennis Vinicio Chicaiza Castillo, Mg.

AUTORÍA DEL TRABAJO

El presente Proyecto de Investigación titulado: "PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A.", es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, enero de 2020

Christian Damian Torres Chango

C.I.: 1805193875

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, enero de 2020

Christian Damian Torres Chango

C.I.: 1805193875

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Félix Fernández PhD. e Ing. Hernán Naranjo Mg, revisó y aprobó el Informe Final del Proyecto de Investigación titulado "PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A.", presentado por el señor Christian Damián Torres Chango de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ing. Elsa Pilar Urrutia, Mg.
PRESIDENTA ENCARCADA DEL TRIBUNAL

Ing. Félix Fernández PhD.
DOCENTE CALIFICADOR

Ing. Hernán Naranjo Mg.
DOCENTE CALIFICADOR

DEDICATORIA

A mis amados padres Isaías Torres y Magdalena Chango ya que fueron el pilar fundamental en mi educación brindándome las mejores enseñanzas en base a su esfuerzo, por su perseverancia para que el futuro de sus hijos sea lleno de éxitos, por su apoyo incondicional para lograr mis metas y llegar a ser un profesional.

A mi familia por su motivación para que llegue a ser un profesional, por formar parte de los cimientos en mi formación académica y por enseñarme a valorar el esfuerzo de mis padres.

Christian Damian Torres Chango

AGRADECIMIENTO

Primeramente, a nuestro Dios ya que él nunca me abandono en los momentos difíciles que se aparecieron en mi vida, por hacerme un hombre de bien dándome a conocer que en esta vida siempre vamos a contar con él y sobre todo con su amor infinito.

A mi madre Magdalena por su infinito amor, paciencia, dedicación que gracias a ello me ha hecho un hombre sabio.

A mi hija Scarleth Torres, mi hermana Jessica Torres y Nancy Moreta por ser mi inspiración de ser un profesional y ejemplo a seguir de nuestra familia.

Gracias a mi primo Bolívar Torres por sus palabras motivadoras de ser "Alguien en la vida", de que uno de la familia tiene que ser el ejemplo y motivación de las siguientes generaciones.

Gracias a mi tutor Ing. Dennis Chicaiza por compartir su conocimiento y don de persona durante mi vida académica en la universidad y especialmente en este trabajo.

Christian Damian Torres Chango

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

En la actualidad, es muy importante considerar que la información es una prioridad para cualquier institución u organización. Dentro de estas entidades, la información conjuntamente con los sistemas informáticos y procesos, forman activos muy importantes. La confidencialidad, disponibilidad e integridad de la información deben ser garantizadas, para mantener niveles de conformidad, competitividad e imagen empresarial.

Conforme avanza las Tecnologías de la información (TI), existe un incremento de incidentes informáticos siendo que los activos de información cada vez están más expuestos a niveles de amenazas elevadas. Estos incidentes se aprovechan de las vulnerabilidades existentes en los activos de información, afectando no solo a los procesos, si no a la continuidad operativa del negocio.

En el presente proyecto de investigación, el principal objetivo es la implementación de un modelo estructurado de carácter preventivo Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO 27001:2013, para la realización de un plan de seguridad informática en la empresa privada Megaprofer S.A. La importancia radica en la información que maneja la empresa, entre ellos las políticas de seguridad, sistemas de control de acceso, administración de activos, seguridad de los recursos humanos, entre otros.

A partir de esto, se proponen nuevas políticas de seguridad coherentes y enmarcadas dentro de los límites de cumplimiento institucional, para el establecimiento, implantación, mantenimiento y mejora que ofrece un SGSI, mediante un proceso de mejora continua.

ABSTRACT

At present, it is very important to consider that information is a priority for any institution or organization. Within these entities, the information together with the computer systems and processes, form very important assets. The confidentiality, availability and integrity of the information must be guaranteed, to maintain levels of conformity, competitiveness and business image.

As Information Technology (IT) progresses, there is an increase in computer incidents, and information assets are increasingly exposed to high threat levels. These incidents take advantage of existing vulnerabilities in information assets, affecting not only the processes, but also the operational continuity of the business.

In the present research project, the main objective is the implementation of a structured preventive structured model Information Security Management System (ISMS), based on ISO 27001: 2013, for the realization of a computer security plan in the private company Megaprofer SA The importance lies in the information handled by the company, including security policies, access control systems, asset management, human resources security, among others.

From this, new coherent security policies are proposed and framed within the limits of institutional compliance, for the establishment, implementation, maintenance and improvement offered by an ISMS, through a process of continuous improvement.

INTRODUCCIÓN

El desarrollo del informe final del presente trabajo de investigación denominado "PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A.", se encuentra dividido en capítulos que se detallan a continuación:

En el Capítulo I del presente proyecto, se describe las problemáticas que se presentan en la falta de políticas, procedimientos, control de accesos, administración de activos. Ya que todo ello engloba la seguridad de la información, al momento de realizar un test sobre los procesos de seguridad.

En el Capítulo II se hace mención a los antecedentes investigativos relacionados a estudios aplicados sobre seguridad de la información. Mediante la implementación del SGSI con la norma ISO 27001:2013. Aportando al planteamiento de una propuesta para dar solución al problema detallado en el Capítulo I.

A continuación, del marco teórico el Capítulo III detalla los diferentes tipos de modalidades de investigación a utilizarse. Especificando el método de recolección de la información para el desarrollo del presente proyecto. Por último, se presenta un listado de las diferentes actividades necesarias para cumplir con los objetivos planteados.

En el Capítulo IV se describe el desarrollo de la propuesta llevando a cabo las actividades detalladas en el capítulo anterior.

Finalmente, en el Capítulo V se redactan las conclusiones y recomendaciones obtenidas del presente proyecto de investigación.

Como punto final, se encuentran los anexos correspondientes al trabajo de investigación

CAPÍTULO I

El problema

1.1 Tema

"PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A."

1.2 Planteamiento del problema

A nivel internacional, las organizaciones presentan grandes volúmenes de información que los ha llevado hacia el éxito. En todos los continentes existen los denominados Hackers, que no son más que piratas de la informática. Ellos hacen el uso de la sabiduría en el área tecnológica, lo cual les permite hacer delitos informáticos, extrayendo la mayor cantidad posible de información confidencial que reside en una empresa [1].

Las amenazas de hurto de información y/o activos en empresas ya sean públicas o privadas aumentan constantemente, de manera que estas pueden ser causados por herramientas informáticas o pueden ser provocados por acto voluntario de un individuo, dado que ninguna protección es infalible. Debido a ello, a nivel internacional, las organizaciones buscan soluciones eficientes en el campo de la seguridad informática [1].

De los países a nivel internacional atentados por el cibercrimen, Colombia se involucra en esta calamidad basado en el desarrollo de una encuesta del año 2012 sobre fraudes informáticos. El laboratorio de investigación digital mexicano MaTTica quién ejecutó la encuesta, logró evidenciar un 19% de las empresas que residen en tierras colombianas son víctimas del robo de información. En base al estudio realizado las

compañías se ponen por encima de la media mundial en el tema de la delincuencia informática [2].

La policía nacional de Colombia en el año 2011 entrega información acerca de las empresas que fueron víctimas de ataques, donde existieron pérdidas de 6,6 millones de pesos, dando a conocer que la mayoría de ataques son a las medianas empresas que cuentan un número menor a 250 empleados. Por tal acontecimiento, en la actualidad las empresas pequeñas y medianas se enfrentan a probabilidades altas en el robo de información [2].

En la cuidad de Ambato-Ecuador, en la empresa privada Megaprofer S.A (encargada de la comercialización de productos ferreteros a nivel Nacional), se encontró problemas en la gestión de seguridad de la información y activos. La falta de políticas adecuadas, procedimientos y controles en los procesos son evidentes, en consecuencia, los usuarios no toman el mínimo cuidado por cumplir normativas de la institución.

La empresa cuenta con acontecimientos en la pérdida de la información, debido a un malware la cual que se desconoció su origen. Las políticas de seguridad en la empresa no siguen un proceso de verificación, revisión y mejora para que todo el personal tenga la obligación o prioridad de cumplimiento, dentro de todo ámbito laborable en Megaprofer S.A Ambato.

1.3 Delimitación

De contenidos:

Área académica: Administrativas Informáticas.

Línea de investigación: Normas y Estándares.

Sublíneas de investigación: Seguridad de Unidades Informáticas.

Delimitación espacial: El presente proyecto de investigación se desarrolló en el área de TICS Megaprofer S.A de la cuidad de Ambato (Plan de Seguridad Informática para la protección de la seguridad de la información y activos de la Empresa).

Delimitación temporal: La presente investigación se ha desarrollado en el período académico septiembre 2019 – febrero 2020 de acuerdo a lo establecido en el Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

1.4 Justificación

El departamento de TICS es uno de los pilares fundamentales de la empresa Megaprofer S.A, debido a que se involucra en el área tecnológica, sistemas informáticos, equipamiento, adicional se encarga principalmente de la telecomunicaciones y procesamiento de datos, entonces tienden a participar con diferentes procesos, como recursos humanos, compras, ventas, facturación entre otros, obteniendo la mayor fuente de información.

En la entidad hay que analizar muchos aspectos en cuanto a seguridad, generalmente dentro del área de TICS y seguridad física ya que no cuentan con una correcta gestión en la seguridad de la información y activos, obteniendo problemas en el incumplimiento de las políticas, perdida de conectividad hacia internet, apagones de energía eléctrica, fallos en el sistema ERP, entre otros. En base a los riesgos que presenta la empresa, da paso a la implementación de una norma que pueda integrar parámetros de seguridad, que ayudara a proteger cualquier amenaza que ponga en peligro o riesgo los activos de información y/o evitar una inestabilidad en el ámbito laboral.

Megaprofer S.A posee información sensible que debe ser resguardado, para ello la norma ISO 27001 propone un plan de seguridad en el área informática. El objetivo de la propuesta es la implementación de un SGSI con la finalidad de mejorar la gestión en la seguridad, alineado los procesos de negocio de la entidad.

Se ha seleccionado la norma ISO 27001 por la amplia aceptación que tiene el marco de referencia en cuanto a la gestión de seguridad, una característica de mayor importancia radica en que se puede adaptar a las necesidades de la empresa sin importar el tamaño. La norma se encargará de la preservación de confidencialidad, integridad y disponibilidad de la información y activos que posee la institución.

1.5 Objetivos

1.5.1 Objetivo General:

Elaborar una propuesta de plan de seguridad informática utilizando la norma ISO 27001 en la empresa Megaprofer S.A.

1.5.2 Objetivos Específicos:

- Estudiar el proceso de verificación del cumplimiento de políticas ya establecidas dentro de la empresa.
- Realizar el diagnóstico de la seguridad de la información del Departamento de TICS de la empresa Megaprofer S.A.
- Integrar los beneficios que ofrece la norma 27001 para la protección ante cualquier amenaza que pueda poner en peligro o riesgo a la empresa.
- Elaborar un plan de seguridad informática para aplicarse en la empresa Megaprofer S.A.

CAPÍTULO II

Marco teórico

2.1 Antecedentes Investigativos

Al desarrollar una investigación de tipo bibliográfica se hallaron los siguientes resultados:

En la investigación realizada por Tania Verónica Guachi Aucapiña, sobre "Norma de seguridad informática ISO 27001 hacia la mejora de la confidencialidad, disponibilidad e integridad que posee los sistemas de la Cooperativa de Ahorro y Crédito San Francisco Limitada en el departamento de Sistemas". Plantea que conforme avanza las tecnologías de la información y la relación que tiene esta con el

negocio que realizan las organizaciones, están en crecimiento tanto las amenazas y vulnerabilidades. En vista de aquello, es motivo de vital importancia proteger los activos de información que posee una entidad por más simple que esta sea, ya que debe radicar la confidencialidad, disponibilidad e integridad de la información mediante una buena implementación de la gestión de riesgos, logrando identificar aquellos activos más vulnerables [3].

Uno de los pilares fundamentales de la entidad San Francisco es el departamento de sistemas, ya que es una organización financiera que opera y gestionan información muy importante de los usuarios. Es fundamental garantizar la seguridad y confiabilidad de los datos de cada usuario que se encuentran en la cooperativa y a los que se integren, esto se logra con el uso de normas que ayudan a manejar y mantener los activos de información [3].

Para la implementación de un SGSI basado en la norma internacional ISO 27001 en la versión que se mantiene actual desde el 2013, se reúne los recursos necesarios para ser ejecutada, ya que por medio de la mencionada norma se escogerá los controles adecuados acorde a las necesidades de la organización. Se pretende proteger todos los activos que se mantiene en el alcance de la norma, con la finalidad de otorgar confianza a las partes interesadas, ya que el sistema será capaz ser implantado, supervisado, mantenido y mejorado en el tiempo [4].

El proyecto de investigación para la generación de las "Políticas de seguridad en los activos de información guiada por la norma ISO 27002 para la DITIC de la Universidad Técnica de Ambato", se tiene diseñado la selección de los controles adecuados para la implantación en la infraestructura mencionada, llevando a cabo la parte tecnológica y a la vez las políticas serán mantenibles para que siempre garanticen la seguridad los activos de información [4].

La versión 2013 de la norma ISO 27002 ayuda a la protección de los activos de información, mediante la implementación de las políticas de seguridad, con ello se evitan accesos no autorizados por usuarios o terceras personas. Se evitará daños físicos y ambientales, entre otros beneficios que se encuentran en la ejecución de los controles, para ello se realiza un análisis de requerimientos en la DITIC UTA y conocer la situación actual, mediante la ayuda de un método tecnológico que son las entrevistas, que fue aplicada al director del área [4].

Una vez realiza la encuesta y tener conocimiento dela situación actual del área se empieza a desarrollar las políticas de seguridad de la información basada en la norma mencionada en su versión actual, cabe recalcar que mediante la implantación de las políticas no es suficiente para que se obtenga una certificación en seguridad de la información, ya que esa norma solo es un conjunto de buenas prácticas en la que prevalece la protección de los activos de información, la misma que en cualquier entidad es de vital importancia. Se generan políticas de control de acceso, recursos humanos, seguridad física y ambiental, continuidad del negocio, cumplimientos entre otros, acorde a la necesidad de la organización [4].

Castro Núñez Diana Margoth, Noviembre 2012 en su investigación realizada sobre una auditoria, para Optimizar el Manejo de la Información y Equipamiento Informático en el MIES INFA Tungurahua, obtiene que la investigación realizada surge de las diferentes falencias que posee la institución a nivel informático, donde hoy en día se maneja la información confidencial, ya que en cada momento los avances del desarrollo de nuevas ideas especializadas en el área de informática van en un constante aumento a nivel internacional [5].
La lentitud en sus ordenadores, la proliferación de virus, el innecesario software instalado y no utilizados por parte de los funcionarios ha sido un detonante para tomar una medida a través de la aplicación de una auditoria Informática, de esta manera tener conocimiento que es lo que está sucediendo en la institución como evitar y qué medidas tomar. La auditoría Informática tiene como fin recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo de una entidad, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización [5].

Pico Llerena Elsa Maribel, en el Análisis de los fraudes informáticos y su incidencia en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo, La investigación realizada surge a raíz de que en todo el ámbito financiero se ha venido dando un incremento considerable en los casos de fraudes informáticos, hecho que ha generado gran preocupación debido a la importancia de la información generada dentro de estas dependencias. Sin embargo, el erradicar este tipo de actos delictivos se torna en un hecho imposible, más no la posibilidad de prevenirlo

y con ello disminuir su impacto en la sociedad. Es por ello que el realizar un análisis de esta actividad ilícita es un hecho primordial, ya que en muchas ocasiones es realizada con gran facilidad, aprovechando el desconocimiento de las personas, la ingenuidad al entregar información personal o los deseos de beneficiarse económicamente [6].

La guía preventiva de seguridad servirá como herramienta para orientar a los usuarios respecto a medidas de seguridad que deben llevarse a cabo para disminuir la posibilidad de ser víctimas de algún tipo de fraude informático, con lo cual se vería beneficiada la institución financiera como sus respectivos clientes, pues evitaremos que se sigan dando pérdidas económicas, lógicas, daños físicos o incluso la pérdida de prestigio y credibilidad de la entidad [6].

2.2 Fundamentación Filosófica

La investigación está relacionada hacia un enfoque de análisis de vulnerabilidades existentes dentro de la entidad, ejecución de un análisis profundo en cuanto a la seguridad los activos e información confidencial para buscar la implantación de un Sistema de Gestión de la Seguridad de la Información en la empresa, con el objetivo de obtener la certificación o simplemente como mejores prácticas para perfeccionar aspectos de seguridad en la empresa.

2.3 Fundamentación Legal

La norma ISO 27001 basada en la seguridad de la información, auxilia a las empresas en el cumplimiento de los requisitos legales que están sujetas a los reglamentos contractuales de seguridad de la información que deben encontrarse explícitamente definidos, documentados y mantenerse actualizados en cada Sistema de Gestión de Seguridad de la Información.

2.4 Fundamentación Teórica

2.4.1 Seguridad

El tema de seguridad se nos viene a la mente ausencia de riesgos o a la confianza en algo o en alguien, pero este factor puede tomarse de diversos sentidos según el área o campo en el que haga referencia la seguridad, sin embargo en cualquiera que este se

encuentre se encargará de evaluar, estudiar y gestionar los riesgos en la que esta se encuentra sometida [7].

En general la información hoy en día uno de los activos más importantes de las organizaciones o entidades, la cual debe protegerse debido a las amenazas que se presentan conforme avanza la tecnología, ya que están sometidos cada vez a amenazas más elevadas hacia la información y todos los soportes con las que se sustentan una entidad, con ello estamos hablando del pilar de funcionamiento de las compañías como son los sistemas y redes [8].

Las clásicas amenazas: fraude, espionaje, sabotaje, vandalismo, fuego, inundaciones, entre otros.

¿Qué es información?

Conjunto de datos organizados en poder de una entidad que poseen valor para la misma.

La información puede estar:

- ✓ En medios escritos.
- ✓ Contenida en imágenes.
- ✓ Medios de expresión oral.
- ✓ Por medio de impresiones en papel.
- ✓ Con tecnología de almacenamiento electrónico.
- ✓ En medios de proyección.
- ✓ Contenida en fax o email.
- ✓ Visualizada y comunicado en reuniones.
- ✓ Entre conversaciones presenciales o digitales.
- ✓ Almacenada en la nube.

2.4.2 Seguridad de la información

Fundamentalmente la seguridad de la información se encarga de la protección de confidencialidad, integridad y disponibilidad de la información, así como de los sistemas integrados en su tratamiento de información dentro de una entidad [9].

Para proteger la información usamos medidas preventivas que abarca la seguridad de la información sobre los activos con la finalidad de que la información sea resguardada en las organizaciones.

La seguridad de la información es un concepto asociado a la certeza, falta de riesgo o contingencia. Se entiende como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se comprende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen [10].

2.4.3 Tipos de Seguridad

Activa

"Es la encargada de que los sistemas informáticos padezcan algún daño, un ejemplo en los ordenadores sería que se usen contraseñas para proteger los datos que esté almacenada, pero se pueden aplicar otras acciones como encriptar datos, usar software de seguridad como los antivirus o establecer contraseñas seguras [11]."

Pasiva

"La seguridad pasiva es aquella que se encarga de minimizar los efectos o desastres que se originan en un accidente, un ejemplo podría ser el malware hacia los sistemas informáticos y una acción para ello sería la realización de copias de seguridad [11]."

2.4.4 Riesgos

En los riesgos existe un factor de incertidumbre asociado con la probabilidad de que aparezcan las amenazas. Es decir que la amenaza solo se puede predecir dentro de ciertos límites [12].

Un incidente no deseado presenta tres componentes amenaza, vulnerabilidad e impacto. Las vulnerabilidades indican la debilidad del activo que puede ser aprovechada por una amenaza [12].

Estos riesgos se contrarrestan con la implantación de controles, es decir medidas que se deben llevar a cabo para cumplir con dicho objetivo.

MAGERIT es la metodología basada en el análisis y gestión de riesgos de las tecnologías de la información, esta técnica de trabaja conjuntamente con los activos y

sistemas de información. MAGERIT da a conocer cuando un activo se encuentra expuesta ante amenazas, con la finalidad de ser protegidos. Los riesgos a los que están sometidos los elementos de una entidad son muy elevados, pero la metodología ayuda a creación de una correcta gestión de riesgos.

Metodología para le gestión de riesgos:

- Identificación de activos
- Tasación de activos
- Identificación de amenazas
- Probabilidad de ocurrencia
- Identificación de vulnerabilidades

MAGERIT toma en cuenta tres aspectos claves para la gestión de riesgos

a) Submodelo de elementos
    - Activos
    - Amenazas
    - Vulnerabilidades
    - Impactos
    - Riesgos
    - Salvaguardas
b) Submodelo de eventos
    - Vista estética relacional
    - Vista dinámica de tipo organizativo
    - Vista dinámica de tipo físico
c) Submodelo de procesos
    - Planificación del proyecto de riesgos
    - Análisis de riesgos
    - Gestión de riesgos
    - Selección de salvaguardas

Para gestión de riesgos la metodología se basa en el siguiente proceso:

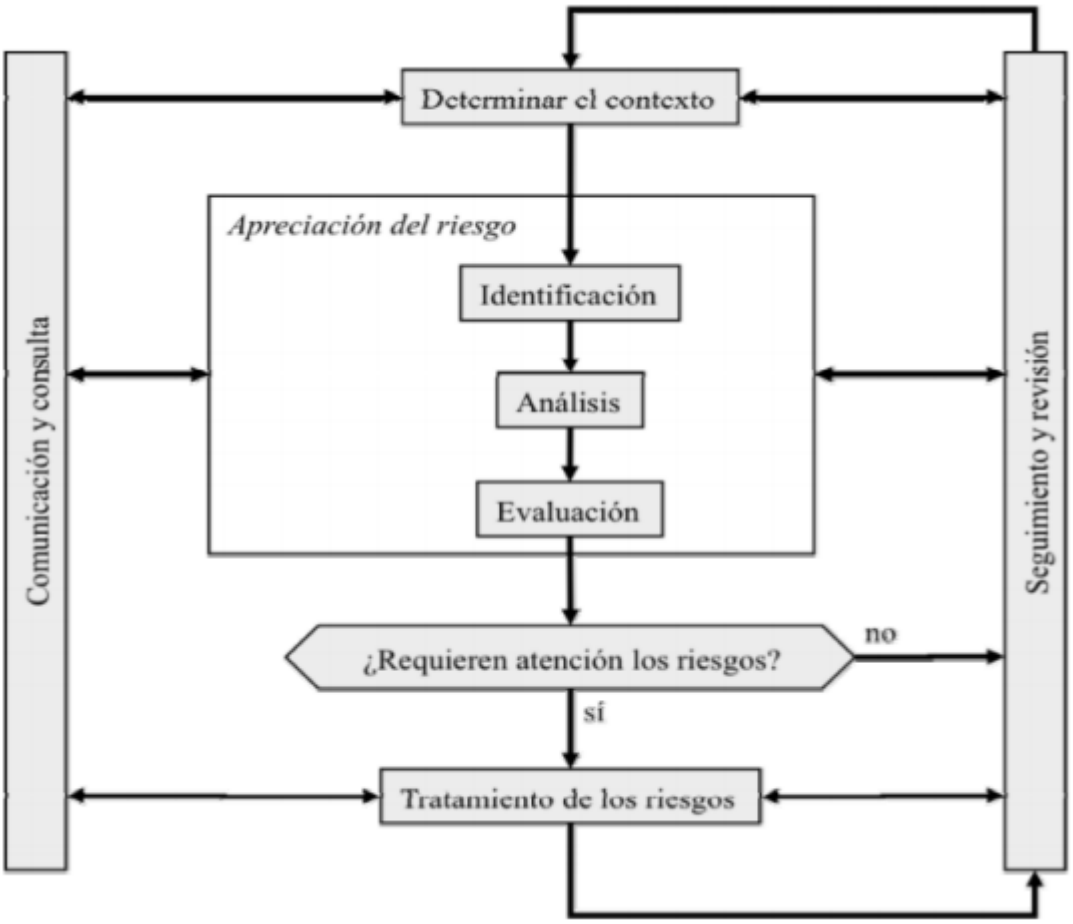

Fig. 1: Proceso para la gestión de riesgos.
Fuente: [13]

2.4.5 Las amenazas a los activos de información

En la actualidad, las empresas se enfrentan a numerosos riesgos e inseguridades procedentes de focos diversos. Esto quiere decir que los activos de información de las empresas, uno de sus valores más importantes se encuentra ligados o asociados a riesgos y amenazas que explotan una amplia tipología de vulnerabilidades.

2.4.6 SGSI

Esto se refiere a un Sistemas de Gestión de la Seguridad de la Información por sus siglas SGSI en español y en el idioma inglés es entendido como Information Security Management System por sus siglas ISMS.

Con la norma estándar ISO 27001, el Sistema de Gestión de la Seguridad de la Información se enfoca en la preservación de la confidencialidad, disponibilidad e integridad a todos los activos de información dentro de la organización [14].

El Sistema de Gestión de Seguridad de la Información es el principal concepto sobre la cual se conforma la norma [9].

La secretaria nacional de administración pública, considerando que las TIC son herramientas imprescindibles para el desempeño institucional e interinstitucional, y como respuesta a la necesidad gestionar de forma eficiente y eficaz la seguridad de la información en las entidades públicas, emitió los acuerdos ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011 respectivamente, mediante los cuales creo la comisión para la seguridad informática y de las tecnologías de la información y comunicación [15].

Evolución

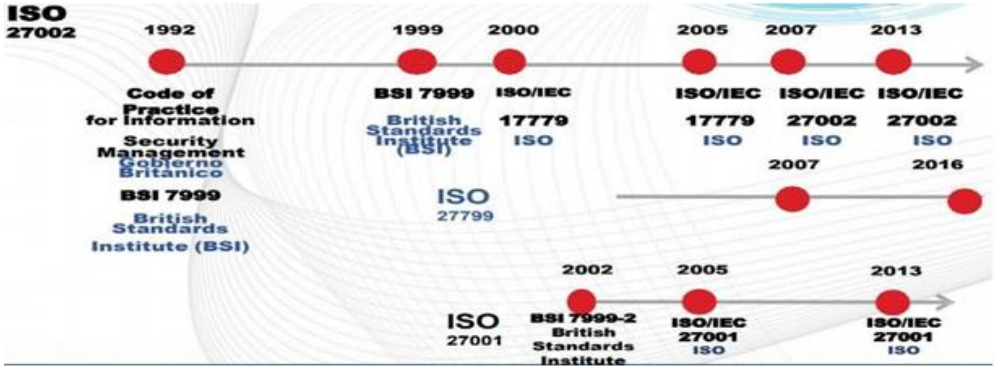

Fig. 2: Evolución ISO 27000.

Fuente: [15].

Beneficios de implantación de un SGSI

- ✓ Estructura e inversiones adecuadas, costo correcto
- ✓ Control y clasificación de activos
- ✓ Dirección de operaciones y comunicaciones
- ✓ Política de Seguridad
- ✓ Evaluación de riesgos internos y a terceros
- ✓ Gestión de las personas: Seguridad del personal
- ✓ Desarrollo y mantenimiento de sistemas
- ✓ Dirección de Planes de Contingencia

- ✓ Cumplimiento con la legislación

2.4.7 ISO 27001, El estándar de seguridad de la información

Un SGSI no solo requiere de su implementación sino también de un mantenimiento y mejora de las medidas de seguridad, es por ello que la norma ISO 27001 otorga una solución de mejora continua con la evaluación de los riesgos en los activos de información y con un objetivo es cuál es la protección y defensa de los mismos [16].

ISO 27001 es un sistema que tiene un enfoque basado en el ciclo de mejora continua o de Deming. Dicho ciclo consiste como ya sabemos, en Planificar-Hacer- Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act) [16].

Incidentes de la Seguridad

Fig. 3: Incidentes de la Seguridad.
Fuente: [17].

2.4.8 ISO 27001

En relación con la seguridad de la información existen normas ligadas a la misma, pero la norma ISO 27001 es factor principal con relación a las demás ya que esta implementa un SGSI certificable en cuando a la seguridad de los activos de información [18].

Generalmente se eligen las áreas más críticas o vulnerables en materia de gestión de la información. Luego de definido el alcance, se debe formular y divulgar una política de la gestión de la seguridad de la información que establezca los lineamientos generales que la organización debe tener en cuenta frente a los riesgos de la información, considerando en ello los requisitos legales, contractuales y propios de la empresa [18].

El eje central de la planificación del SGSI consiste en identificar los riesgos de la información, en relación con las posibles amenazas y los puntos vulnerables de la organización en cuanto a la confiabilidad, seguridad y disponibilidad de la información.

A partir de la identificación de estos riesgos, y de su análisis y valoración, se definirán los planes de control o tratamiento de riesgo. Incluye también la documentación y la aplicación de los procedimientos necesarios para aplicar tales controles, así como la formación y la concienciación de los empleados respecto a la seguridad de la información y los controles que se han de aplicar [18].

La verificación incluye la medición del desempeño del SGSI, la evaluación de los riesgos y la eficacia de los controles implementados, la realización de auditorías internas al sistema y la recisión del mismo por parte de la dirección [18].

Áreas o Dominios de Seguridad de la ISO/IEC 27001 [19]**.**

- **A 5:** Políticas de seguridad de la Información.
- **A 6:** Organización de la seguridad de la información.
- **A 7:** Seguridad de los Recursos Humanos.
- **A 8:** Gestión de recursos.
- **A 9:** Control de Acceso.
- **A 10:** Criptografía.
- **A 11:** Seguridad física y ambiental.
- **A 12:** Seguridad Operacional.
- **A 13:** Seguridad de las Comunicaciones.
- **A 14:** Adquisición, desarrollo y mantenimiento de Sistemas.
- **A 15:** Relaciones con los proveedores.
- **A 16:** Gestión de Incidentes en Seguridad de la Información.

- **A 17:** Aspectos de Seguridad de la Información para la gestión de la continuidad del negocio.
- **Anexo 18:** Cumplimiento.

2.4.9 Etapas de la seguridad de la información

Todo sistema de gestión de seguridad se basa en el conocido ciclo de DEMING (PDCA). Es una estrategia de mejora continua de la calidad la cual se basa en cuatro fases: planear, hacer, verificar y actuar. La estructura completa se puede observar en la figura:

Fig. 4: Ciclo DEMING PDCA.
Fuente: [20].

a) Planificación. - La dirección toma conciencia de la situación actual real mediante la recolección y análisis de datos.

b) Hacer. - Consiste en la implementación de procesos a partir del análisis y planificación previos.

c) Verificar. - Consiste en la monitorización y evaluación de los procesos y de los resultados, relacionándolos con los objetivos y especificaciones planteados inicialmente.

d) Actuar. - Se realizan las correcciones necesarias y se realiza la estandarización de los cambios con el propósito de garantizar el mejoramiento continuo de los procesos.

2.4.10 Normas ISO 27000

El Sistema de Gestión de Seguridad de la información son requisitos de especificación que denomina la familia de normas ISO 27000 [21].

Para que la seguridad de la información sea llevada a cabo en una organización se basa en un marco de estandarización que consiste en un conjunto de normas las cuales se presenta a continuación [21]:

- Sistema de gestión de la seguridad de la información.
- Valoración de riesgos.
- Controles ISO 2013.

En un Sistema de Gestión de Seguridad de la Información los activos de información deben centrarse en tres aspectos fundamentales [21]:

- Confidencialidad.
- Integridad.
- Disponibilidad.

2.4.11 Fases de un SGSI basado en la norma ISO 27001

Un SGSI completo basado en la norma estándar ISO 27001 debe basarse en diferentes fases los cuales son los siguientes:

1. Análisis y evaluación de riesgos.
2. Implementación de controles
3. Definición de un plan de tratamiento de los riesgos o esquema de mejora
4. Alcance de la gestión
5. Contexto de organización
6. Partes interesadas
7. Fijación y medición de objetivos
8. Proceso documental
9. Auditorías internas y externas

2.4.12 Ventajas de implantar un SGSI basado en la ISO 27001 [22]

- ✓ Garantiza la confidencialidad, integridad y disponibilidad de los activos información relevantes [22].
- ✓ Reducir la incertidumbre por el conocimiento de los riesgos e impactos asociados [22].

- ✓ Mejorar continuamente la gestión de la seguridad de la información [22].
- ✓ En las organizaciones garantizan la continuidad del negocio [22].
- ✓ Incremento de la confianza de las partes interesadas [22].
- ✓ Cumple con la legislación vigente que es referente a la seguridad de la información [22].
- ✓ En lo empresarial mejora la implicación y participación del personal en la gestión de la seguridad [22].
- ✓ Integración con otros sistemas de gestión como las normas ISO 9001, ISO14001, OHSAS 18001, entre otros [22].
- ✓ Capacidad de mejora de procesos y servicios prestados [22].

2.5 Propuesta de solución

La siguiente investigación plantea la implementación de un SGSI basado en la norma ISO/IEC 27001 en su versión actual, por medio de una planificación estructurada que servirá como plan de acción para el mejoramiento de la seguridad de la información y activos con la finalidad de alcanzar una eficiencia óptima integrando nuevas actividades como políticas, resguardo de información y la protección de la información. A partir de la implementación se plantea la automatización de los procesos de seguridad existentes en la empresa Comercializadora, reduciendo riesgos de pérdida de información y activos.

CAPÍTULO III

Metodología

3.1 Enfoque

La presente investigación se basa en un enfoque cualitativo ya que se requiere la recolección de la información para tener un análisis completo de la actual situación de la empresa.

3.2 Modalidad de la investigación

La presente investigación se fundamenta dentro del paradigma crítico propositivo porque se realiza la investigación de todas las causas y factores del problema en la empresa privada Megaprofer S.A, donde se pretende solucionar los problemas de seguridad de la información.

3.2.1 Modalidad de Campo

Esta modalidad es aplicada ya que será necesario acudir al lugar donde se suscitan los hechos con la finalidad de obtener información en relación al proyecto de investigación que será desarrollada.

Para la recolección de la información se utilizarán técnicas como entrevistas, encuestas y la observación en el lugar de los hechos.

3.2.2 Modalidad Bibliográfica o Documentada

Se considera esta modalidad ya que se recurre a diferentes fuentes obtenidas de libros, artículos científicos, tesis desarrolladas en diferentes Universidades del País para profundizar enfoques con respecto al tema de la investigación que abarca el término de la seguridad de la información.

3.2.3 Modalidad Aplicada

Por la utilización de los conocimientos adquiridos sobre gestión de calidad de la información que se enmarco en Normas ISO y otros conocimientos obtenidos a lo largo de la carrera universitaria.

3.3 Población y muestra

3.3.1 Población

Para la presente investigación se tomó como población al personal integrado por cuatro personas en el departamento de Tics de la empresa privada Megaprofer S.A.

3.3.2 Muestra

No es necesario realizar un muestreo debido a que la población es reducida y se puede acceder a ella sin restricciones. Por tanto, la muestra viene a ser la misma población definida anteriormente.

Tabla 1: Personal TICS.
Fuente: Elaborado por el investigador.

Cargo	Cantidad
Jefe de Sistemas	1
Asistente de Sistemas	2
Pasantes Asistente de Sistemas	1
Total	4

3.4 Recolección de la Información

Para la recolección de la información se realizó una entrevista y encuesta al personal de TICS para determinar casos en los que se no se apliquen controles o procedimiento que conlleva con los activos de seguridad de la información, también evaluar el cumplimento de las políticas de seguridad de la información que actualmente emplean en la empresa y a la vez la utilización de medios electrónicos relacionado con la temática propuesta, con el objetivo de tener la información fundamental para el proyecto de investigación.

Para la realización de la entrevista se utilizó cuestionarios de evaluación que fueron elaborados en base a los estándares de seguridad informática, dirigida al departamento de TICS con la finalidad de conocer las actividades que se realizan a diario de manera que no se omita ningún aspecto de la relevante en la investigación.

De igual manera se realizó una observación de campo debido a que fue necesario una inspección para conocer los activos que posee la empresa y la arquitectura de los sistemas informáticos que se manejan, a fin de verificar cómo se lleva a cabo la seguridad de la información, así como la protección de los activos pertenecientes a la empresa.

Además, se buscó en internet información adicional de documentos técnicos, tesis, libros, todo esto para alcanzar los objetivos planteados, así como también la respectiva observación en el departamento de TICS.

3.4.1 Matriz de Entrevista

Tabla 2: Seguridad y Norma ISO 27001.
Fuente: Elaborado por el investigador.

Categorías / Indicadores	Observaciones
Seguridad y Norma ISO 27001	
1. ¿Qué conocimientos posee con respecto a la seguridad de la información?	Con relación a la seguridad de la información se tiene un conocimiento suficiente.
2. ¿Qué conocimientos tiene sobre las normas que establecen la Seguridad de la información?	Con respecto a las normas de seguridad de la información el conocimiento es parcialmente suficiente.
3. ¿Cuál es su conocimiento sobre Normas ISO 27001?	El conocimiento con respecto a la norma ISO 27001 es insuficiente.
4. ¿Qué conocimiento tiene sobre la ley de protección de datos?	No tiene conocimientos sobre la ley de protección de datos.
5. ¿Los equipos de cómputo tienen licenciamiento vigente?	Los equipos de cómputo no cuentan con licenciamiento vigente.
6. ¿Qué nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema?	El nivel de seguridad para el ingreso al sistema tiene un nivel medio.
7. ¿Está disponible en su totalidad todo tipo de información necesaria para todos los usuarios de los sistemas autorizados?	Toda la información para los usuarios del sistema es redundante.

8. ¿Existe información que se filtra hacia fuera del departamento?	Se filtra información (activos, activos informáticos …).
9. ¿Los procesos que se manejan actualmente poseen una documentación detallada y disponible en cualquier momento?	Los procesos se manejan de una forma documentada con disponibilidad en cualquier momento.
10. ¿Se aplican actualmente políticas de seguridad para gestionar la información? Enúncielas.	Inexistencia de políticas de seguridad para gestionar la información.
11. ¿Se realiza gestión de riesgos en cuanto a la seguridad de la información?	No se realizan gestión de riesgos en cuanto a la seguridad de la información.

Usuarios

Tabla 3: Usuarios.
Fuente: Elaborado por el investigador.

1. ¿Existe una sola persona encargada para la creación de usuarios?	Sola una persona es la encargada de la creación de usuarios.
2. ¿Existe algún registro de los usuarios creados?	No existe un registro completo de los usuarios creados.
3. ¿Los usuarios que se encuentran en período de vacaciones o que ya no laboran en la empresa son bloqueados?	A los usuarios que se encuentran en período de vacaciones no se les bloquea y a los usuarios que ya no laboran se hace un seguimiento para ser bloqueados.
4. ¿Se debe solicitar permisos para la creación de usuarios?	Es de carácter obligatorio solicitar permiso para la creación de usuarios.
5. ¿Las claves creadas tienen caducidad?	Existe un tiempo estimado para que las claves creadas tengan caducidad.

6. ¿Están definidas responsabilidades del usuario en cuanto al uso adecuado de los recursos?	Las responsabilidades en cuanto al uso adecuado de recursos se le otorga al usuario.
7. ¿Existe un control sobre el acceso no autorizado al usuario, con la finalidad de proteger el equipamiento y sistemas que se manejan en la empresa?	Inexistencia del control de acceso no autorizado.

Autentificación

Tabla 4: Autentificación.
Fuente: Elaborado por el investigador.

1. ¿El password es genérico para todos los usuarios creados?	Cuando se crea una cuenta en un determinado sistema para el usuario su contraseña como primer ingreso es genérico.
2. ¿Está definido el tamaño y definición del password?	El password es por afinidad del usuario.
3. ¿El ingreso de clave errado bloquea al usuario?	Luego de 3 intentos el usuario es bloqueado.
4. ¿Los usuarios pueden ingresar a sistema través de cualquier equipo?	En ocasiones se necesita que los usuarios complementen su trabajo desde otro lugar que no sea la empresa.
5. ¿Se puede ingresar a través de otro equipo de cómputo si el usuario ya está en uso?	Se puede ingresar desde varios equipos.

Autorización

Tabla 5: Autorización.
Fuente: Elaborado por el investigador.

1. ¿Los usuarios creados tienen permiso para realizar cualquier clase de consulta, modificación o alteración de la base de datos?	Los usuarios no tienen ninguna clase de permiso para alterar la BDD.
2. ¿Están definidos los permisos para cada usuario?	Aún no se tiene bien definidos el control sobre los permisos para cada usuario.
3. ¿Existe autorización para el cambio de usuario o password?	No, ya que es responsabilidad del usuario realizar cambios de contraseñas.
4. ¿Está permitido el acceso a páginas que no son de orden institucional?	No, se tiene controlado por Lista de Control de Acceso (ACL) el acceso a la Web
5. ¿Se puede hacer uso de celular o cualquier medio de almacenamiento durante la jornada laboral?	Si, las políticas de la empresa no consideran dicho tema.

Administración Sistemas

Tabla 6: Administración Sistemas.
Fuente: Elaborado por el investigador.

1. ¿El administrador puede realizar cambios en la Base de Datos (BDD)?	Si, si se requiere bajo autorización.
2. ¿La sesión de los usuarios permanece activa durante tiempos prolongados cuando no hay uso del sistema?	No, en los sistemas se encuentra configurada la expiración de las sesiones.
3. ¿Existen controles para el acceso a los backups por parte del	No se tiene personal en el área de Base de Datos.

	Administrador de base de datos (DBA)?	
4.	¿Los usuarios pueden extraer información a través de dispositivos externos?	No, tenemos un sistema de bloqueo contra dispositivos extraíbles.
5.	¿Existe algún registro o documento de las personas autorizadas para realizar respaldos de los sistemas?	Si, en nuestro proceso está documentado las personas responsables.
6.	¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación? Si…. De qué manera se lo ha realizado; No…. ¿Por qué?	No se han realizado ya que no se ha tenido conocimiento del tema.
7.	¿Se realizan tareas de monitoreo a los sistemas de información que se manejan?	En los sistemas controlados por la empresa si se realiza en otros el proveedor nos ayuda a controlar.

Equipos Informáticos

Tabla 7: Equipos Informáticos.
Fuente: Elaborado por el investigador.

1.	¿Los equipos tienen capacidad de memoria suficiente para la ejecución de programas y aplicaciones necesarias para ejecutarse correctamente?	Si, antes de otorgar un equipo se hace un análisis para realizar la compra.
2.	¿Todos los procesos en cuanto a los equipos se encuentran documentados?	Si, al tener certificación BASC nos obliga a tener los procedimientos para el resguardo de los activos fijos.
3.	¿Se realiza un mantenimiento periódico de los equipos de la empresa?	Sí, pero no se tiene un cronograma de mantenimiento de equipos.

4. ¿Los usuarios pueden destapar o abrir los equipos de cómputo asignados?	No, se les ha comunicado que ellos no tienen autorización solo personal técnico autorizado.

Pistas de Auditoría

Tabla 8: Pistas de Auditoría.
Fuente: Elaborado por el investigador.

1. ¿Los proxys están definidos?	Si, se tiene un servidor dedicado.
2. ¿Se actualizan documentos para el registro de o actualización de la información?	Si, el personal tiene la responsabilidad de registrar diariamente registros o actualizaciones.
3. ¿Qué mecanismo, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y de comunicación?	Ninguno, no se ha considerado dicho tema.

Activos fijos

Tabla 9: Activos fijos.
Fuente: Elaborado por el investigador.

1. ¿Los registros de activos fijos contienen la suficiente información y detalle, según la necesidad de la empresa?	Si, se trata de tener la información del activo para identificarlo de mejor manera.
2. ¿Qué tipo de políticas o reglas se aplican al momento de la autorización de activos fijos para: retirar, destruir, ¿adquirir o vender?	No se tiene políticas o procesos.

3. ¿Se hace periódicamente un inventario físico o digital de los activos fijos donde se consta su existencia y su estado?	No se ha realizado.
4. ¿Las personas que tienen a su cuidado el activo fijo otorgado por la empresa, están obligadas a reportar cualquier cambio existente como: daños, golpes, traspasos, problemas con el software, ¿etc.?	Si, al capacitarlos se les comunica que los activos fijos con defectos o daños sean reportados a Tic para su reposición.
5. ¿La venta de activos fijos del departamento de TICS requiere la autorización previa de los directivos?	Si, Gerencia General nos sumilla y autoriza la baja de activos
6. ¿Se tiene información sistematizada y actualizada de inventario de activos fijos de la empresa?	No existe personal a cargo para realizar dicho acto, pero si se lo realiza cada cierto tiempo.
7. ¿El inventario esta degradado por áreas?	Sí, se tiene segmentado para un mejor control.
8. ¿Se han definido procedimientos específicos para: (¿Registro de activos, Resguardos, Altas, Bajas, Transferencias, ¿Toma física de inventarios?	Se tiene un proceso para el manejo de activos, pero no para bajas y tomas físicas de inventario.
9. ¿Se cuenta con una base de datos o programas computarizados del inventario de los activos fijos?	No, únicamente se controla en una hoja de cálculo.
10. ¿Se lleva un registro actualizado de los ingresos de activos de los proveedores?	Inexistente el control interno ya que nos apoyamos con contabilidad.

11. ¿Existe el personal idóneo para controlar los activos fijos?	Si, el personal está capacitado y tiene las aptitudes necesarias.
12. ¿Es necesaria la implantación de un proceso adecuado para el control de los activos fijos?	Si ya que se debe tener un control de cada activo fijo.

3.4.2 Evaluación de la entrevista aplicada

Con la respectiva entrevista realizada al Ingeniero Paul Montesdeoca del departamento de sistemas puede evaluar los siguiente:

Se aplican ciertas políticas para gestionar la información, pero estas son hasta cierto punto básicas, como la gestión de usuarios, limitación en cuanto al uso de internet …, las cuales no son suficientes para garantizar que la información esté asegurada.

Ha ocurrido problemas internos con correos mal intencionados que contienen archivos adjuntos con el objetivo de borrar la información, siendo un problema muy perjudicial y como factor la gestión de contraseñas no seguras.

No existe un documento formal donde consten responsabilidades de los funcionarios respecto a los equipos, es decir no están definidas formalmente. Únicamente se socializa a aquellos funcionarios que tienen cierta responsabilidad de algún recurso lo cual no es aconsejable.

Existe un punto positivo de control de acceso de los usuarios hacia el equipamiento de la institución, ya en cierta medida el mismo se encuentran protegido por contraseña contra usuarios mal intencionados.

En cuanto a la seguridad física, la ubicación de la data center no cumple con las especificaciones de seguridad, en consecuencia, se tiene un control incorrecto de acceso para el personal no autorizado, el acceso a este medio se debería llevar a cabo de una documentación detallada donde consten registros de ingreso y salida de personal.

No existe un cronograma de mantenimiento para los equipos que utilizan los usuarios, actualmente solo manejan un plan básico de mantenimiento.

No existe un plan de contingencia ante caídas de los sistemas que manejan.

No existe plan de contingencia cuando se quedan sin conexión de internet.

No se realiza una gestión de riesgos ante las eventualidades como robos o ataques de la información que manejan por parte de personas malintencionadas.

3.4.3 Encuesta

Para realizar el procesamiento de la encuesta se basó en la escala de Likert, con el objetivo de medir actitudes y opiniones con un mayor grado de especificidad, con la ayuda de una gama de opciones ya que es una de las maneras más confiables para medir opiniones, percepciones y comportamientos [23].

Cada pregunta cuenta con una valoración que se especifica a continuación:

Tabla 10: Valoraciones encuesta.
Fuente: Elaborado por el investigador.

Observación	Abreviación	Valoración
Excelente	E	5
Bueno	B	4
Regular	R	3
Muy deficiente	MD	2
No tiene conocimientos	NT	1

3.4.4 Tabulación de Resultados

3.4.5 Conocimiento en la Seguridad de la Información.

Considerando que el departamento de TICS cuenta con cuatro integrantes en el área, tres de ellos de planta y uno como pasante, se realizó la encuesta a los integrantes mencionados.

Tabla 11: Conocimiento en la seguridad de la información.
Fuente: Elaborado por el investigador.

Conocimiento en la Seguridad de la Información	E	B	R	MD	NT
En cuanto a la seguridad de la información usted tiene un conocimiento	0	2	1	1	0
Usted tiene conocimientos sobre las normas que integran la seguridad de la información	0	2	1	0	1

Mediante las capacitaciones otorgadas en la entidad sobre la seguridad de la información, que nivel de conocimiento ha desarrollado	0	0	0	3	1
Dado que se hayan desarrollado auditorias sobre la seguridad de la información, mediante ese proceso en qué estado se encuentra la seguridad en la entidad	0	0	2	1	1
Cuál es su conocimiento sobre la norma ISO 27001	0	1	2	1	0
Qué conocimiento tiene sobre la ley de protección de datos	0	1	1	2	0
Total:	0%	25%	29%	33%	13%

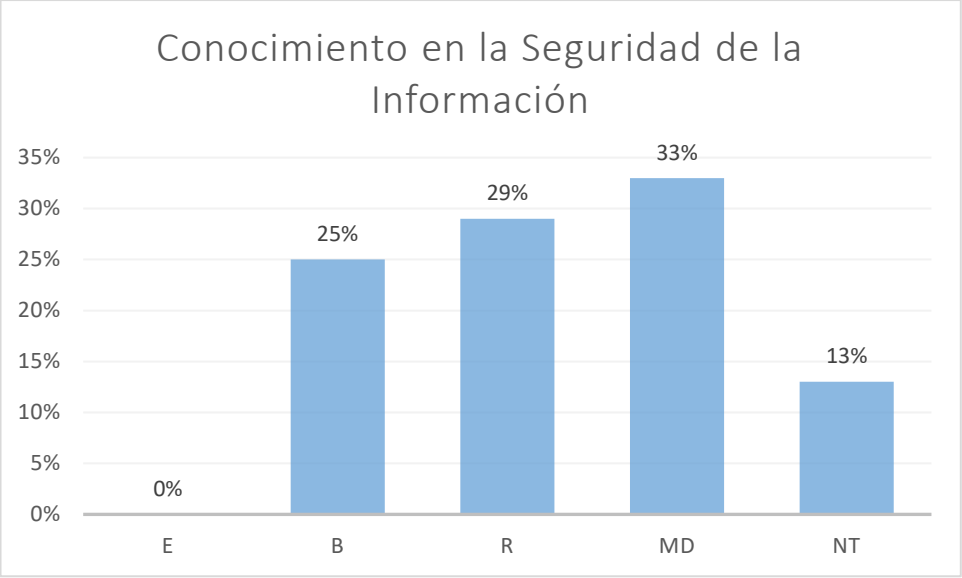

Fig. 5: Porcentaje de conocimiento en la seguridad de la información.
Fuente: Elaborado por el investigador.

Interpretación: de acuerdo con las encuestas realizadas al personal en el área de TICS, se logra evidenciar que el 0% su conocimiento es excelente, el 25 % su conocimiento es bueno, el 29% el conocimiento es regular, el 33% su conocimiento es muy deficiente y el 13% no tiene conocimiento.

Análisis: se puede definir que la mayoría del personal esto es 77% que labora en el área de TICS tiene unos niveles de conocimiento regular de seguridad de la

información, o no los tiene, es de suma importancia establecer tareas o actividades que conlleven a que el personal nivele los conocimientos de seguridad informática.

3.4.6 Conocimiento en procedimientos para la defensa y seguridad de la información.

Tabla 12: Procedimientos para la defensa y seguridad de la información.
Fuente: Elaborado por el investigador.

Procedimientos para la defensa y seguridad de la información	E	B	R	MD	NT
El medio donde se alojan los backups de los servidores ¿En qué estado se encuentra?	0	2	1	0	1
Los datos que se verifican después de realizadas las copias de seguridad se catalogan como	2	1	0	1	0
El sistema de control para el ingreso a esta área se define como:	0	0	3	1	0
Como se define las pistas dejadas al ingresar a esta área	0	3	1	0	0
Como se definen los controles que se ejerce a los usuarios del área de TICS para ingresar a los servidores	0	2	1	0	1
En qué estado se dispone los servidores alternos que tiene la entidad en caso de un fallo en los servidores principales	0	0	0	3	1
Total:	8%	33%	25%	21%	13%

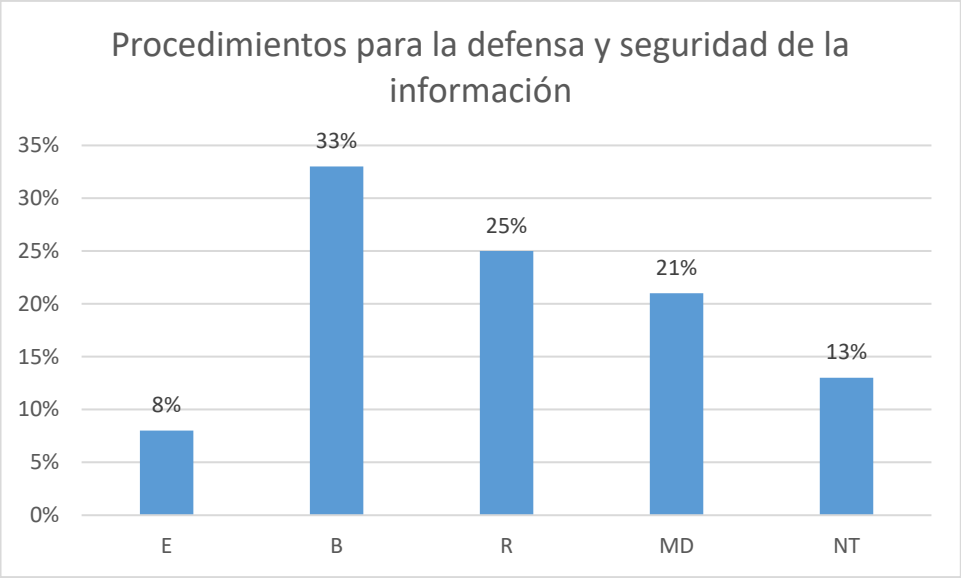

Fig. 6: Porcentaje de conocimiento en los procedimientos para la defensa y seguridad de la información.

Fuente: Elaborado por el investigador.

Interpretación: de acuerdo con las encuestas realizadas al personal en el área de TICS, se logra evidenciar que el 8% su conocimiento es excelente, el 33 % su conocimiento es bueno, el 25% el conocimiento es regular, el 21% su conocimiento es muy deficiente y el 13% no tiene conocimiento.

Análisis: se puede definir que la mayoría del personal esto es 33 % que labora en el área de TICS tiene unos niveles de conocimiento de los procedimientos para la defensa y seguridad de la información en un buen conocimiento, pero supera el 50% por lo que es necesario implementar una estrategia que permitan reducir los riesgos que pongan en peligro la disponibilidad, la integridad y confidencialidad de la información en la empresa Megaprofer S.A.

3.4.7 Aplicación de herramientas para la protección de datos y seguridad de la información.

Tabla 13: Aplicación de herramientas para la protección de datos y la seguridad de la información.

Fuente: Elaborado por el investigador.

Aplicación de herramientas para la protección de datos y la seguridad de la información	E	B	R	MD	NT
El antivirus instalado en los equipos de cómputo de la empresa se puede definir como:	0	1	2	0	1
El nivel de protección brinda el antivirus instalado en los equipos de computo	0	1	2	1	0

Como se define la restricción a paginas no permitidas en la empresa Megaprofer S.A.	1	2	0	0	1
Los equipos de cómputo tienen licenciamiento vigente	0	0	2	0	2
Como se define el password para el ingreso al sistema	0	1	2	0	1
El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema	0	1	2	0	1
Total:	4%	25%	42%	4%	25%

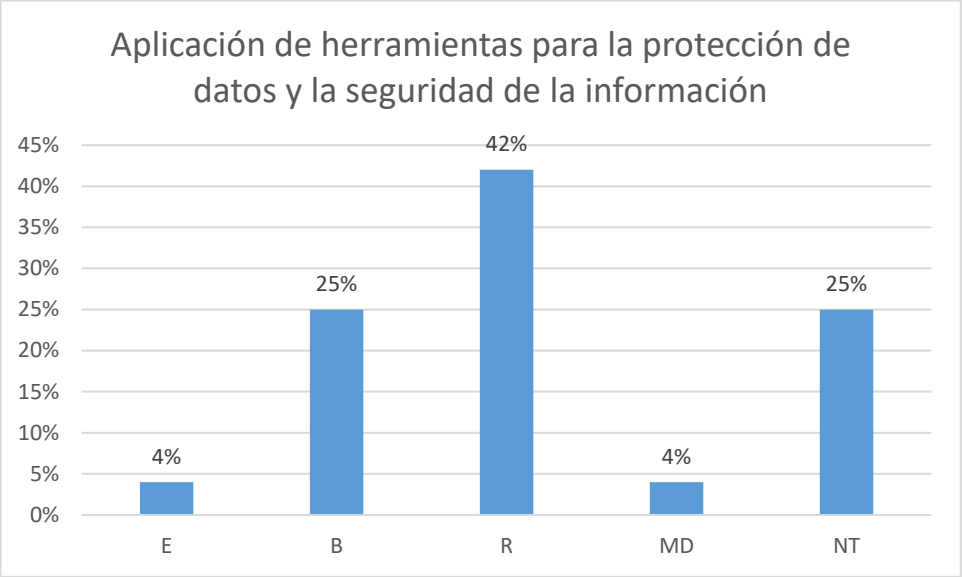

Fig. 7: Porcentaje de conocimiento en la aplicación de herramientas para la protección de datos y seguridad de la información.

Fuente: Elaborado por el investigador.

Interpretación: de acuerdo con las encuestas realizadas al personal en el área de TICS, se logra evidenciar que el 4% su conocimiento es excelente, el 25 % su conocimiento es bueno, el 42% tiene un conocimiento regular, el 4% su conocimiento es muy deficiente y el 25% no tiene conocimiento,

Análisis: en este ítem se evidencia que el índice de des favorabilidad hacía los conocimientos de la aplicación de las herramientas para la protección de datos y seguridad de la información que tiene un índice alto de conocimiento regular y consecuentemente que no se tiene conocimiento siendo un riesgo para la seguridad de

la información ya que se presentan porcentajes muy bajos en personal que tiene conocimientos excelentes y buenos, es indispensable realizar la implementación de la metodología seleccionada para cumplir con las tareas y actividades que esta señala.

3.4.8 Acceso al área de servidores o Data Center

Tabla 14: Acceso al área de servidores o Data Center.

Fuente: Elaborado por el investigador.

Acceso al área de servidores o Data Center	E	B	R	MD	NT
Mediante las normativas de seguridad de la información en los servidores que son el diseño y ubicación de los mismos que estado dispone	0	0	3	0	1
En caso de que se suscite una emergencia y este ponga en riesgo la información el plan de contingencia en qué nivel se encuentra para actuar ante la eventualidad	0	0	2	1	1
En el ingreso al área de las cámaras, registros, bitácoras, backus entre otros, la seguridad se define como	0	2	1	1	0
En qué estado se dispone los servidores alternos que tiene la entidad en caso de un fallo en los servidores principales	0	0	0	0	4
En los servidores donde se almacenan los backups, en cuanto a su seguridad como lo define	0	0	2	1	1
Total:	0%	10%	40%	15%	35%

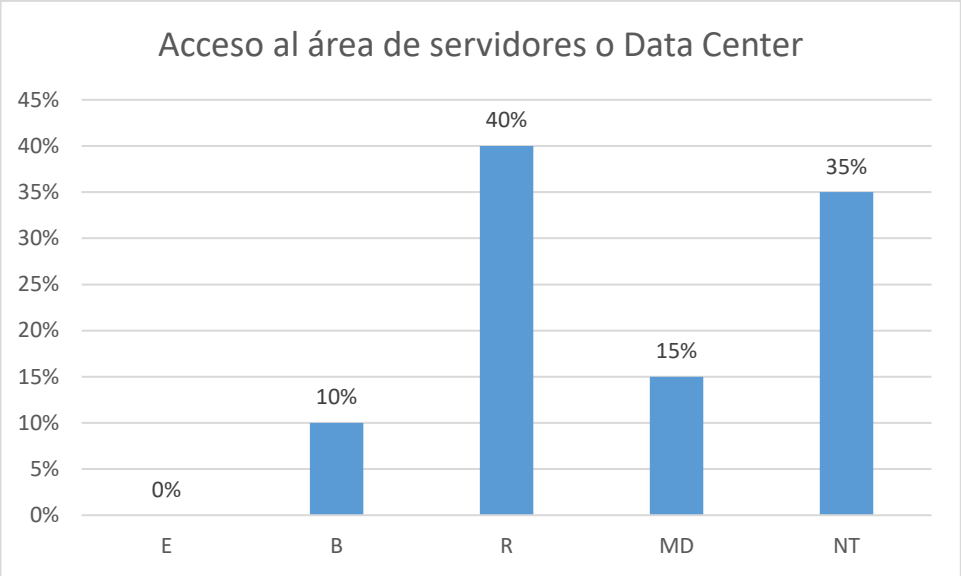

Fig. 8: Porcentaje de conocimiento en el acceso al área de servidores o Data Center.
Fuente: Elaborado por el investigador.

Interpretación: de acuerdo a las encuestas realizadas al personal de TICS, se logra evidenciar que el 10% su conocimiento es bueno, el 40% es regular, el 15% su conocimiento es muy deficiente y el 35% no tiene conocimiento, en este ítem se evidencia que existe un porcentaje alto en que su conocimiento es regular en base al acceso al área de servidores o Data Center dejando un riesgo para la seguridad de la información.

Análisis: Es importante que se tomen medidas para establecer un control que sea favorable en cuanto a los archivos backups y así garantizar un buen estado hacia los servidores, ante los fallos que puedan evidenciarse en los servidores la entidad no cuenta con equipos alternos.

3.5 Procesamiento y análisis de datos

Para el procesamiento de la información se realizará las siguientes actividades:

- Recolección de la información de las encuestas y entrevistas aplicadas.
- Recolección de la información mediante la investigación en documentos físicos y virtuales referentes al tema.
- Análisis de los datos.
- Lectura de artículos relacionados con la investigación presentada.
- Redactar evaluaciones de los resultados.

- Establecimiento conclusiones y recomendaciones.

La información que se recolectó por medio de la encuesta fue procesada mediante el uso de herramientas informáticas, con el fin de elaborar gráficos que ayuden a la interpretación en cuanto a los conocimientos en la seguridad de la información y las normas que lo establecen.

Al llevar a cabo el procesamiento y análisis de datos, se busca organizar la información para conocer la situación actual de la entidad, para poder integrar los beneficios que ofrece el SGSI basado en la norma ISO 27001, sustentando dentro del marco teórico.

3.6 Desarrollo del proyecto

Mediante la metodología en cascada se desarrolla el siguiente proyecto de investigación, ya que para implementar un SGSI basado en la norma estándar ISO 27001 es necesario aplicar diferentes etapas para lograr la eficiencia en la seguridad de la información y activos la cual se basa en un proceso sistémico. El modelo en cascada ayudará a que el inicio de cada etapa deba esperar la culminación de la fase anterior, con la finalidad de que cuando se produzcan fallas en los procesos este conduzca a la mejora de las mismas.

CAPÍTULO IV

Desarrollo del proyecto

4.1 Análisis de Requerimientos

4.1.1 Análisis de la situación actual

El punto principal que debemos tener en cuenta para el desarrollo del proyecto de investigación es determinar la situación actual de la empresa Megaprofer S.A con respecto a la seguridad de la información.

Con la ayuda de la recolección de la información detallados en el capítulo 3, a fin de obtener toda información relevante y tener un previo conocimiento sobre la gestión de seguridad empresarial y personal, es evidente que el departamento no se centra en la implementación de buenas prácticas para el cumplimiento de las políticas establecidas dentro de la organización, es decir no tienen implementado un SGSI basado en la norma ISO 27001 para gestionar adecuadamente la información que se lleva a cabo cotidianamente en la entidad.

Antes de llevar a cabo la implementación del sistema de gestión de seguridad, es importante aclarar que no necesariamente se asocia el término “sistema” con la implementación o desarrollo de una aplicación informática. De forma general el término sistema hace relación a un conjunto de normas y procedimientos relacionados entre sí para contribuir a la consecución de un objetivo.

4.1.2 Seguridad de la información en el departamento de TICS

La situación actual en base a los cumplimientos de políticas establecidas en la empresa Megaprofer S.A, en cuanto a la protección de los activos de información según la ISO 27001 en el departamento de TICS, da a conocer que no siguen un proceso de verificación del cumplimiento de políticas, esto se puede evidenciar con las técnicas de recolección de la información presentados en el capítulo 3, adicional se pueden visualizar los cumplimientos en manera gráfica y porcentual en la sección 4.4.6.

Debido a la falta de interés por parte de la alta gerencia evidenciados en el capítulo 3 en cuanto a la seguridad de la información en el área de TICS, se planteara una matriz FODA, con el objetivo de relacionar las Fortalezas, Oportunidades, Debilidades y Amenazas que ayuden a la visualización del impacto que pueden tener las amenazas y debilidades en la seguridad de los activos de información, con ello se toma en cuenta las fortalezas y oportunidades que posee el departamento de TICS para que se implemente la seguridad de la información mediante la norma ISO 27001 y que tenga el apoyo por parte de la administración autoritaria.

4.2 Matriz FODA

Se realiza el análisis de la matriz FODA dando a conocer las Fortalezas, Oportunidades, Debilidades y las Amenazas que se están presentando en el área de TICS de la empresa Megaprofer S.A de acuerdo a la información recolectada en el trabajo de campo.

Tabla 15: Matriz FODA.
Fuente: Elaborado por el investigador.

FORTALEZAS	OPORTUNIDADES
• Se tienen proveedores de servicios alterno que facilita la continuidad del negocio en caso de algún inconveniente que se presente. • Políticas internas de seguridad para usuarios e información en base a la norma internacional BASC. • Cuenta con el área de soporte técnico dentro de la empresa y no depende de terceros. • Los password protegen el ingreso de usuarios no autorizados para	• Contar con el presupuesto para la compra e innovación de las herramientas para tener una mejor seguridad de la información. • Otorgar un plan para la mejora en cuanto a la seguridad de la información. • Enfoque en la seguridad de la información para la adquisición de nuevas tecnologías. • En cuanto a la seguridad de la información dar capacitaciones a todo el personal de la entidad.

el uso de los equipos de la compañía. • La empresa reconoce el valor de los datos priorizados	• Implementación de la norma ISO 27001
DEBILIDADES	AMENAZAS
• La empresa cuanta no cuenta con servidor alterno, no continuidad operativa. • El personal no cuenta con licencias de software, solo usuarios específicos cuentan con licencia vigente. • No se tiene un amplio conocimiento sobre la seguridad de la información. • El acceso al área de servidores no se encuentra bien protegida**.** • No cuenta con políticas estandarizadas internacionalmente. • Inexistencia de planes de contingencia en caso de pérdida de información. • Falta capacitación con respecto a seguridad de la información. • Falta de apoyo en el proceso de TICS.	• El antivirus utilizado no brinda una seguridad optima. • Pérdida de información por no revisar las copias de seguridad después de que se ejecuten • No cuenta con la implementación de firewall, equipos vulnerables en la red. • Personal incapaz de seguir lineamientos planteados por la norma BASC. • Software no confiable (Atix ERP) sistema con errores. • Falta de espacio físico para realizar tareas eficientes dentro del proceso de TICS. • Pérdidas financieras debido a las sanciones impuestas por la ley. • Afectación a la integridad de los datos por accesos permitidos no controlados.

4.3 Conclusiones y Recomendaciones situación actual de la empresa

4.3.1 Conclusiones

- El personal del departamento de TICS no posee un alto conocimiento en base a la seguridad de la información, de acuerdo a la evaluación de Conocimiento en Seguridad de la Información, Procedimientos para la defensa y seguridad de la información y aplicación de Herramientas para la Protección de datos y Seguridad de la Información, así como también servidores de backups.
- La infraestructura de la organización se encuentra divida por procesos, gracias a ello se pudo conocer las actividades que se desarrollan dentro de cada una de ellas, se determinan las falencias en el departamento de TICS mediante la seguridad en el hardware y software, infraestructura, soporte a usuarios.
- La empresa privada Megaprofer S.A ha sufrido acontecimientos de pérdida de información debido a la falta de políticas de seguridad que sigan una normatividad adecuada, llegando hasta tener problemas en ataques informáticos.
- Megaprofer S.A una organización dedicada a la comercialización ferretera con alto porcentaje de progresión en el mercado, no se ha enfocado en la seguridad de la información a pesar que la entidad actualmente cuenta con los recursos necesarios para implementar una ISO referente a la seguridad de los activos de información.
- En base a la normatividad BASC el departamento de TICS ha empleado políticas en cuanto a la seguridad, estas están expuestas hacia todo el personal pero que no son llevados a cabo eficientemente provocando que la información sea hurtada.

4.3.2 Recomendaciones

- Implementar un plan de seguridad hacia todos los activos de información que agregan valor a la empresa, basándose en normas de seguridad como la ISO 27001 que genera un procedimiento sistemático para aplicar controles adecuados en los activos.
- Tener a un personal encargado específicamente de la seguridad informática para cada uno de los procesos, con el objetivo de dar el correcto seguimiento a

las políticas establecidas y generar nuevos controles a los activos de información relevantes.

- Desarrollar lo más pronto posible políticas y controles adecuadas en base a la normatividad ISO 27001, con el fin de minimizar riesgos en los activos de información y fortalecer la gestión de seguridad de la empresa.
- Elaborar una correcta gestión de riesgos en base a una metodología, la cual ayudará a encontrar amenazas en los activos de información de una manera eficiente para establecer medidas de seguridad y que estas sean capaces de responder ante cualquier incidente.
- Efectuar programas de capacitaciones a todo el personal en general acerca de la importancia de seguir un lineamiento de normativas de seguridad de la información.

4.4 Implementación SGSI

Se presenta el SGSI basado en la norma internacional ISO 27001 en su versión actual año 2013. Un modelo sistémico de carácter preventivo en cuanto a la seguridad de la información brindando confidencialidad, integridad y disponibilidad, dando respuesta a los riesgos que se enfrentan los activos y que estos sean gestionados para que sean minimizados mediante la aplicación de controles adecuados.

El sistema de Gestión de Seguridad propuesto consta de las siguientes etapas:

- Definir el alcance, políticas del SGSI y objetivos.
- Identificar los riesgos sobre los activos definidos en el alcance del SGSI.
- Analizar las probabilidades e impactos de los riesgos sobre los activos identificados bajo el alcance y calcular los niveles de riesgo, aplicando la metodología MAGERIT.
- Implementar controles sobre los activos, basado en un plan de tratamiento de riesgo.
- Asegurar la creación de procedimientos para el monitoreo y revisión del SGSI.

4.4.1 Alcance

Para definir el alcance que tendrá la implementación del SGSI, se basará en los procesos definidos en el Anexo A, y sistemas de información existentes en la entidad

ya que todo ello engloba actividades como soporte, comerciales, compras, ventas, financieras..., que marcan valor sensible para la entidad.

La definición anterior nos agrega valor en la declaración de la aplicabilidad la cual no existe en la organización.

Se deberán evaluar los procesos considerados en el alcance y en cuanto a la norma estándar ISO 27001:

- Se toma en cuenta la gestión de activos fijos existentes en la organización en base a un a gestión adecuando de los riesgos y que tan vulnerable se encuentre, así como también la gestión de responsabilidades y usos apropiados de los activos.
- Seguridad física, debido a los controles que no son aplicados correctamente y que en consecuencia llevaría a un empleado o tercero tener acceso a un recurso físico o lógico que la organización posea.
- Gestión de accesos, debido a la falta de controles y requisitos aplicables a la misma, es uno de los factores relevantes ya que con ello se garantiza la continuidad de sus actividades brindando disponibilidad en todo momento de la información.
- Recursos Humanos, uno de los procesos que posee activos de información valiosos para la entidad en donde se deben aplicar controles que protejan la información en todo momento.
- Equipos físicos, que se apliquen controles que abarquen el mantenimiento ya sea preventivo como correctivo, para un rendimiento eficiente y que se pueda conservar la integridad del hardware y software.

Este alcance ha sido desarrollado mediante la norma ISO 27001 y por un integrante del departamento de TICS, ya que mediante su ayuda se lleva a cabo el SGSI que tendrá valor en el área de sistemas para la verificación de las etapas que se han establecido.

4.4.2 Política de Seguridad del SGSI

Para la implementación del Sistema de Gestión de la Seguridad de la Información se establece la siguiente política, la cual se encuentra alineada con el contexto de

seguridad de la información y la entidad, donde se tiene lugar la implementación y el mantenimiento del SGSI.

"Promover prácticas de seguridad de la información, con el fin de garantizar la calidad y excelencia en el tratamiento de la información, permitiendo asegurar la continuidad de los procesos de la empresa Megaprofer S.A. a través de un Sistema de Gestión de Seguridad de la Información que constituye el marco de referencia para lograr la consecución de este compromiso, garantizando confidencialidad, integridad y disponibilidad de la información."

Objetivos: con la finalidad de llevar a cabo la política establecida para la organización se establecen los siguientes:

- Considerar la seguridad de la información como un proceso de mejora continua, que permita alcanzar niveles de seguridad cada vez más avanzados.
- Generar una adecuada gestión de riesgos que puedan detectar las vulnerabilidades posibles en los activos de información.
- Definir, desarrollar e implementar los controles de seguridad organizativos que resulten necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en la empresa Megaprofer S.A.
- Monitorear el SGSI para garantizar la integridad de la información.

4.4.3 Gestión de Riesgos

Para la gestión de los riesgos es importante evaluar el impacto de los mismos que tendrá para la empresa, en el cual teniendo en consideración las posibles consecuencias que afecten los procesos que se ejecutan y más en los que manejan la información de mayor importancia.

El propósito de este proceso es determinar si un cierto riesgo es aceptable o de otra manera buscar y aplicar un método adecuado para mitigarlo.

Para la ejecución de esta sección, se ha definido una metodología con la cual se realizará el análisis y evaluación de riesgos. El método consiste en un análisis cualitativo de los activos más relevantes que pertenecen a la empresa, posterior la identificación de las amenazas relacionadas con ellos y su probabilidad de ocurrencia;

en base a esto, se describen las vulnerabilidades que podrían hacer que dichas amenazas se cumplan.

A continuación, se muestra un diagrama de la metodología a utilizar:

Fig. 9: Metodología para la gestión de riesgos.
Fuente: Elaborado por el investigador.

a) Identificación de activos:

Todos los activos que la empresa dispone, tienen un valor significativo porque contienen y la vez trabaja con la información, por lo tanto, es esencial proporcionar una protección adecuada.

Después de identificar todos los activos, se los evalúa para administrar aquellos que se consideran "más relevantes" en términos del desarrollo de las actividades por parte del personal de la empresa, según el nivel de participación con respecto a la confidencialidad, integridad y disponibilidad de la información.

b) Al tener identificado los activos considerados de "mayor relevancia", se determinan tanto las amenazas como las vulnerabilidades, entonces en base a esto, se determina el nivel de impacto en los activos de la empresa.
c) Posteriormente, procedemos a evaluar y determinar la probabilidad real de ocurrencia de dicha amenaza, teniendo en cuenta las consecuencias y el impacto que tendrán si llegan a cumplirse, lo que implica un riesgo relacionado con la confidencialidad, integridad y disponibilidad de la información.
d) Finalmente, el valor de riesgo se obtiene de acuerdo a la tabla establecida para estimar la frecuencia de ocurrencia de la amenaza.

- Inventario de Activos Informáticos

Para llegar al objetivo que es la implementación del SGSI es importante cumplir con el análisis y la gestión de riesgos de los activos vinculados a la información, que la empresa dispone y que son partícipes en cada uno de los procesos.

METODOLOGÍA MAGERIT

Esta metodología dedicada al análisis y gestión de riesgos, mediante un método sistémico que analiza las tecnologías de información y comunicación, en cuanto a riesgos para establecer controles adecuados que sean capaces de minimizar todos aquellos riesgos a los que se expone los activos de información. [24].

La metodología MAGERIT identifica las amenazas o vulnerabilidades mediante una escala a las que expone los activos de información que pueden llegar a tener un impacto negativo para las organizaciones, con ello busca aplicar medidas apropiadas para que las amenazas o vulnerabilidades no sean aprovechaba [24].

El uso de esta metodológica es eficiente ya que su enfoque es a los activos más relevantes de la empresa todos aquellos que se relacionan con los activos de información.

MAGERIT persigue los siguientes objetivos:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de gestionarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.

- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

Para un mejor análisis, se va a trabajar por agrupaciones los activos acordes con la metodología MAGERIT el cual está enfocado en la gestión de los riesgos.

Tabla 16: Tipos de activos según MAGERIT.
Fuente: Elaborado por el investigador.

Activos	Descripción
Instalaciones [L]	Lugares donde se hospedan los sistemas de información y comunicaciones.
Hardware [HW]	Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
Software [SW]	Tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de servicios.
Datos[D]	La información que permite a la organización prestar sus servicios.
Redes de comunicaciones [COM]	Son los medios de transporte que llevan datos de un sitio a otro. Se incluyen tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
Equipamiento Auxiliar [AUX]	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con éstos.
Personal [P]	Personas relacionadas con los sistemas de información.
Soportes de información [M]	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

- Identificación de Activos Informáticos

Tabla 17: Identificación de activos.
Fuente: Elaborado por el investigador.

Tipo de Activo Descripción	ID	ACTIVO
	L1	Data Center
	L2	Salas de Reuniones
	L3	Instalaciones Gerenciales

Instalaciones [L]	L4	Instalaciones Administrativas
	L5	Plantas de Producción
	L6	Bodegas
	L7	Seguridad Física
	L8	Recepción
Hardware [HW]	HW1	Servidor de aplicaciones
	HW2	Servidor de Bases de Datos
	HW3	Servidor Telefonía
	HW4	Servidor de almacenamiento
	HW5	Servidor Web
	HW6	Servidor de Dominio
	HW7	Computadores de Escritorio
	HW8	Computadores portátiles
	HW9	Impresoras
	HW10	Switch
	HW11	Router
	HW12	Access Point
Software [SW]	SW1	Windows Server
	SW2	Microsoft Office
	SW3	Sistema Operativo Windows
	SW4	Atix ERP
	SW8	Antivirus
	SW9	Sistemas propios de producción
Datos[D]	D1	Bases de Datos Empleados
	D2	Bases de Datos Producción
	D3	Bases de Datos Clientes
	D4	Bases de Datos Proveedores, Empresarios
	D5	Backus generadas de Bases de datos
	D6	Bases de Datos Correos empresarial
	D7	Respaldo de Aplicaciones
	D8	Centro de proceso de Datos
	COM1	Acceso a internet

Redes de comunicaciones [COM]	COM2	Líneas Telefónicas
	COM3	Fax
	COM4	Acceso Inalámbrico
Servicios (S)	S1	Backups de usuarios
	S2	Video vigilancia
	S3	Virtualización
	S4	Correo electrónico empresarial
Equipamiento Auxiliar	AUXI	Sistema Eléctrico General
		Aire Acondicionado (Data Center)
		Sistema de Detección de incendios
		Sistema de primeros Auxilios
		Fibra óptica
		Cableado estructurado
		Ups Principal
Personal [P]	P1	Gerencias
	P2	Jefaturas
	P3	Coordinadores
	P4	Analistas
	P5	Directores
	P6	Soporte técnico
	P7	Servicios generales
	P8	Área de Recursos Humanos
	P9	Vendedores
	P10	Asistentes
	P11	Recepcionistas
	P12	Auxiliares
	P13	Personal General
Soportes de información [M]	M1	Discos Duros Backups
	M2	USB

Para identificar los riesgos en los activos de información, cada uno de los activos se evalúa de acuerdo con el nivel de Confidencialidad, Disponibilidad e Integridad que proporcionan para garantizar la información en un rango entre 1 a 5 llevados a cabo con el departamento de sistemas con el Ing. Mario Perez, donde se detallan los siguientes niveles:

Niveles (C, D, I)	ID
Extrema	5
Alta	4
Media	3
Baja	2
Muy Baja	1

Tabla 18: Identificación de riesgos.
Fuente: Elaborado por el investigador.

ACTIVO	Confidencialidad	Disponibilidad	Integridad	Total
Data Center	4	4	4	4
Salas de Reuniones	2	3	2	2
Instalaciones Gerenciales	3	3	2	3
Instalaciones Administrativas	3	3	2	3
Plantas de Producción	2	3	2	2
Bodegas	3	4	3	3
Seguridad Física	4	4	4	4
Recepción	1	1	2	1
Servidor de aplicaciones	4	4	3	4
Servidor de Bases de Datos	4	4	4	4
Servidor Telefonía	4	3	4	4
Servidor de almacenamiento	3	3	3	3

Servidor Web	4	4	3	4
Servidor de Dominio	4	3	3	3
Computadores de Escritorio	4	4	3	4
Computadores portátiles	3	4	3	3
Impresoras	4	3	2	3
Switch	3	4	3	3
Router	4	4	3	4
Access Point	4	4	3	4
Windows Server	3	4	3	3
Microsoft Office	3	4	3	3
Sistema Operativo Windows	4	4	3	4
Atix ERP	4	4	4	4
Antivirus	3	4	3	3
Sistemas propios de producción	5	5	5	5
Bases de Datos Empleados	5	5	5	5
Bases de Datos Producción	5	5	5	5
Bases de Datos Clientes	5	5	5	5
Bases de Datos Proveedores	4	4	5	4
Backups generadas de Bases de datos	3	3	3	3
Bases de Datos Correos empresarial	3	2	3	3
Respaldo de Aplicaciones	3	3	3	3

Centro de proceso de Datos	4	4	4	4
Acceso a internet	5	5	3	4
Líneas Telefónicas	4	4	2	3
Fax	3	2	2	2
Acceso Inalámbrico	3	4	4	4
Backups de usuarios	2	2	2	2
Video vigilancia	4	4	4	4
Virtualización	4	4	3	4
Correo electrónico empresarial	5	5	5	5
Sistema Eléctrico General	4	4	3	4
Aire Acondicionado (Data Center)	4	4	4	4
Sistema de Detección de incendios	4	3	3	3
Sistema de primeros Auxilios	3	3	3	3
Fibra óptica	5	5	5	5
Cableado estructurado	4	4	4	4
Ups Principal	4	5	4	4
Gerencias	4	3	4	4
Jefaturas	2	3	2	2
Coordinadores	3	2	2	2
Analistas	1	3	2	2
Directores	2	2	2	2
Soporte técnico	3	2	2	2
Servicios generales	3	2	2	2
Área de Talento Humano	4	3	4	4
Vendedores	2	3	2	2

Asistentes	2	3	2	2
Recepcionistas	4	3	2	3
Auxiliares	2	3	2	2
Personal General	2	2	2	2
Discos Duros Backups	4	3	3	3
USB	2	4	3	3

A partir de la tabla anterior se determinan aquellos activos cuyo valor es mayor o igual a 3 para realizar la evaluación de riesgos.

Tabla 19: Activos de mayor relevancia.
Fuente: Elaborado por el investigador.

ACTIVO	Total
Data Center	4
Instalaciones Gerenciales	3
Instalaciones Administrativas	3
Bodega	3
Seguridad Física	4
Servidor de aplicaciones	4
Servidor de Bases de Datos	4
Servidor Telefonía	4
Servidor de almacenamiento	3
Servidor Web	4
Servidor de Dominio	3
Computadores de Escritorio	4
Computadores portátiles	3
Impresoras	3
Switch	3
Router	4
Access Point	4
Windows Server	3
Microsoft Office	3
Sistema Operativo Windows	4

Atix	4
Antivirus	3
Sistemas propios de producción	5
Bases de Datos Empleados	5
Bases de Datos Producción	5
Bases de Datos Clientes	5
Bases de Datos Proveedores	4
Backups generadas de Bases de datos	3
Bases de Datos Correos empresarial	3
Respaldo de Aplicaciones	3
Acceso a internet	4
Líneas Telefónicas	3
Acceso Inalámbrico	4
Video vigilancia	4
Virtualización	4
Correo electrónico empresarial	5
Sistema Eléctrico General	4
Aire Acondicionado (Data Center)	4
Sistema de Detección de incendios	3
Sistema de primeros Auxilios	3
Fibra óptica	5
Cableado estructurado	4
Ups Principal	4
Gerencias	4
Área Talento Humano	4
Recepcionista	3
Discos Duros Backups	3
USB	3

Tabla 20: Catálogo de amenazas según MAGERIT.
Fuente: Elaborado por el investigador.

Tipo de Activo Descripción	ID	Amenazas
Desastres Naturales [N]	N1	Fuego
	N2	Daños por agua
	N3	Tormenta Eléctrica
	N4	Terremoto
Origen Industrial [I]	I1	Fuego
	I2	Daños por agua
	I3	Sobrecarga eléctrica
	I4	Explosión
	I5	Derrumbe
	I6	Contaminación mecánica
	I7	Contaminación electromagnética
	I8	Avería de origen física o lógica
	I9	Corte eléctrico
	I10	Condiciones inadecuadas de temperatura y/o humedad
	I11	Fallo del servicio de comunicaciones
	I12	Interrupción de otros servicios y suministros esenciales
	I13	Degradación de los soportes de almacenamiento de la información
	I14	Emanaciones electromagnéticas
Errores y fallos no intencionados [E]	E1	Errores de usuarios
	E2	Errores de los técnicos de TI
	E3	Errores de los administradores de sitio
	E4	Errores de monitorización (log)
	E5	Errores de configuración
	E6	Deficiencias en la organización
	E7	Difusión de software dañino

	E8	Errores de [re-]encaminamiento
	E9	Errores de secuencia
	E10	Escapes de información
	E11	Alteración accidental de la información
	E12	Destrucción de información
	E13	Fugas de información
	E14	Vulnerabilidad de los programas (software)
	E15	Errores de mantenimiento / actualización de programas (software)
	E16	Errores de mantenimiento / actualización de equipos (hardware)
	E17	Caída del sistema por agotamiento de recursos
	E18	Pérdida de equipos
	E19	Indisponibilidad del personal
Ataques intencionados [A]	A1	Manipulación de los registros de actividad (log)
	A2	Manipulación de la configuración
	A3	Suplantación de la identidad del usuario
	A4	Abuso de privilegios de acceso
	A5	Uso no previsto
	A6	Difusión de software dañino
	A7	[Re-]encaminamiento de mensajes
	A8	Alteración de secuencia
	A9	Acceso no autorizado
	A10	Análisis de tráfico
	A11	Repudio
	A12	Interceptación de información (escucha)
	A13	Modificación deliberada de la información
	A14	Destrucción de información
	A15	Divulgación de información
	A16	Manipulación de programas
	A17	Manipulación de los equipos
	A18	Denegación de servicio

	A19	Robo
	A20	Ataque destructivo
	A21	Ocupación enemiga
	A22	Indisponibilidad del personal
	A23	Extorsión
	A24	Ingeniería social

Para estimar la vulnerabilidad, es necesario estimar la frecuencia de ocurrencia de amenazas en una escala de tiempo.

Tabla 21: Categorías de frecuencias de amenazas.
Fuente: Elaborado por el investigador.

Vulnerabilidad	ID	Rango
Extrema Frecuencia	MA	1 vez al día
Alta Frecuencia	A	1 vez cada 2 semanas
Frecuencia Media	M	1 vez cada 2 meses
Baja Frecuencia	B	1 vez cada 6 meses
Muy Baja Frecuencia	MB	1 vez al año

Para la valoración del impacto con respecto a la frecuencia de una amenaza se basará en la siguiente tabla y así determinar un valor en las dimensiones aplicadas:

Tabla 22: Valoración de impacto de una amenaza.
Fuente: Elaborado por el investigador.

Impacto	ID	Valor
Muy Alto	MA	Valor > 95%
Alto	A	75%<Valor>95%
Medio	M	50%<Valor>75%
Bajo	B	30%<Valor>50%
Muy Bajo	MB	10%<Valor>30%

A continuación, se muestra una tabla de resumen del análisis de amenazas de la empresa Megaprofer S.A, se puede ver que para cada amenaza que afecta a un activo, se analiza la frecuencia con la que puede ocurrir, así como su impacto en las diferentes dimensiones de seguridad del activo.

Tabla 23: Análisis de amenazas.
Fuente: Elaborado por el investigador.

Grupo	Amenaza	Activo afectado	Frecuencia	% Impacto - Dimensiones		
				C	D	I
Desastres Naturales [N]	Fuego [N1]	Hardware [HW]	MB		100	
		Instalaciones [L]	MB		100	
		Red de Comunicaciones [COM]	MB		100	
		Equipamiento Auxiliar [AUX]	MB		75	
	Daños por agua [N2]	Hardware [HW]	MB		75	
		Instalaciones [L]	MB		75	
		Red de Comunicaciones [COM]	MB		75	
		Equipamiento Auxiliar [AUX]	MB		75	
	Tormenta Eléctrica [N3]	Hardware [HW]	MB		75	
		Red de Comunicaciones [COM]	MB		50	
		Equipamiento Auxiliar [AUX]	MB		50	
	Terremoto [N4]	Instalaciones [L]	MB		100	
		Hardware [HW]	MB		75	

		Equipamiento Auxiliar [AUX]	MB		75	
De origen industrial [I]	Fuego [I1]	Hardware [HW]	MB		100	
		Instalaciones [L]	MB		100	
		Red de Comunicaciones [COM]	MB		100	
		Equipamiento Auxiliar [AUX]	MB		100	
	Daños por agua [I2]	Hardware [HW]	MB		75	
		Instalaciones [L]	MB		75	
		Red de Comunicaciones [COM]	MB		75	
		Equipamiento Auxiliar [AUX]	MB		75	
	Sobrecarga eléctrica [I3]	Hardware [HW]	B		75	
		Red de Comunicaciones [COM]	B		50	
		Equipamiento Auxiliar [AUX]	B		50	
	Explosión [I4]	Hardware [HW]	MB		100	
		Instalaciones [L]	MB		100	
		Red de Comunicaciones [COM]	MB		100	
		Equipamiento Auxiliar [AUX]	MB		100	
	Derrumbe [I5]	Hardware [HW]	MB		75	
		Instalaciones [L]	MB		100	

		Red de Comunicaciones [COM]	MB		60	
		Equipamiento Auxiliar [AUX]	MB		60	
	Contaminación mecánica [I6]	Hardware [HW]	MB		50	
		Equipamiento Auxiliar [AUX]	MB		50	
	Contaminación electromagnética [I7]	Red de Comunicaciones [COM]	MB		75	
		Hardware [HW]	MB		75	
		Datos [D]	MB		75	
		Equipamiento Auxiliar [AUX]	MB		775	
	Avería de origen física o lógica [I8]	Red de Comunicaciones [COM]	M		75	
		Hardware [HW]	M		75	
		Equipamiento Auxiliar [AUX]	M		40	
		Instalaciones [L]	B		20	
		Software [SW]	M		75	
		Servicios [S]	M		80	
		Datos [D]	B		30	
	Corte eléctrico [I9]	Hardware [HW]	B		100	
		Red de Comunicaciones [COM]	B		100	
		Equipamiento Auxiliar [AUX]	B		100	
		Hardware [HW]	B		60	

	Condiciones inadecuadas de temperatura y/o humedad [I10]	Red de Comunicaciones [COM]	B		60	
		Equipamiento Auxiliar [AUX]	B		60	
	Fallo del servicio de comunicaciones [I11]	Acceso a Internet Principal Oficinas [COM]	M		100	
		Acceso a Internet Secundario Oficinas [COM]	M		100	
		Acceso a Internet en Plantas [COM]	M		100	
		Líneas Móviles [COM]	M		100	
		Línea voz fija principal oficinas [COM]	M		100	
		Línea voz fija secundaria oficinas [COM]	M		100	
		Línea voz fija Plantas oficinas [COM]	M		100	
		Acceso de Voz Fijo [COM]	M		100	
		Acceso a Internet Plantas [COM]	M		100	

		Servicios [S]	M		100	
	Interrupción de otros servicios y suministros esenciales [I12]	Sistema de climatización CPD	B		60	
		Sistema de alimentación Ininterrumpida	B		30	
	Degradación de los soportes de almacenamiento de la información [I13]	Servidores [HW]	MB		75	
		Cabina de Almacenamiento [HW 11]	MB		100	
		PC'S [HW]	B		10	
	Emanaciones electromagnéticas [I14]	Instalaciones [L]	MB		20	20
		Hardware [HW]	MB		50	50
		Equipamiento Auxiliar [AUX]	MB		20	20
	Errores de usuarios [E1]	Instalaciones [L]	M	20	10	50
		PC'S [HW]	M	20	50	20
		Móviles [HW]	M	20	50	20
		Datos [D]	M	75	75	40
	Errores de los técnicos de TI [E2]	Instalaciones [L]	M	20	50	20
		Hardware [HW]	M	20	75	20
		Software [SW]	M	20	75	20
		Datos [D]	M	20	75	20
		Equipamiento Auxiliar [AUX]	M		75	
		Servicios [S]	M		80	
	Errores de monitorización [E4]	Datos [D]	M		75	
		Hardware [HW]	B		50	

Errores y fallos no intencionados [E]	Errores de configuración [E5]	Software [SW]	B		50	
		Datos [D]	B		50	
		Equipamiento Auxiliar [AUX]	B		50	
	Deficiencias en la organización [E6]	Personal [P]	M	50	75	30
		Datos [D]	M	50	75	30
		Instalaciones [L]	M	50	75	30
		Servicios [S]	M	50	75	30
	Difusión de Software dañino [E7]	Software [SW]	B	75	75	75
		Datos [D]	B	50	50	50
	Errores de [re-]encaminamiento [E8]	Servicios [S]	MB	50	75	
		Red de Comunicaciones [COM]	MB	40	75	
		Software [SW]	B		100	
	Errores de secuencia [E9]	Servicios [S]	MB	50	75	
		Red de Comunicaciones [COM]	MB	50	75	
		Software [SW]	B	50	75	
	Escapes de información [E10]	Servicios [S]	MB	50		
		Software [SW]	B	50		
		Datos [D]	B	100		
	Alteración accidental de la información [E11]	Datos [D]	M			75
	Destrucción de información [E12]	Datos [D]			100	
		Servicios [S]	MB	30		

	Fugas de información [E13]	Software [SW]	B	65		
		Datos [D]	B	100		
	Vulnerabilidad de los programas (software) [E14]	Software [SW]	M	75	75	20
		Datos [D]	M	75	75	20
	Errores de mantenimiento / actualización de programas (software) [E15]	Software [SW]	B		75	50
	Errores de mantenimiento / actualización de equipos (hardware) [E16]	Hardware [HW]	B		75	
	Caída del sistema por agotamiento de recursos [E17]	Servicios [S]	MB		100	
		Red de Comunicaciones [COM]	MB		100	
	Pérdida de equipos [E18]	PCS	B	50	100	
		Móviles	M			
	Indisponibilidad del personal [E19]	Personal [P]	A		100	
	Manipulación de los registros de actividad (log) [A1]	Datos [D]	MB			
		Servicios [S]	MB			
	Manipulación de la configuración [A2]	Datos [D]	MB	75		75
		Servicios [S]	MB	75		75

Ataques intencionados [A]	Suplantación de la identidad del usuario [A3]	Software [SW]	B	100		80
		Datos [D]	B	100		80
		Red de Comunicaciones [COM]	B	75		75
		Servicios [S]	B	75		75
	Abuso de privilegios de acceso [A4]	Instalaciones [L]	B	75	50	50
		Software [SW]	B	75	50	50
		Red de Comunicaciones [COM]	B	75	50	50
		Servicios [S]	B	75	50	50
	Uso no previsto [A5]	Instalaciones [L]	MB	25	25	25
		Software [SW]	MB	25	25	25
		Red de Comunicaciones [COM]	MB	25	25	25
		Servicios [S]	MB	25	25	25
		Hardware [HW]	MB	25	25	25
	Difusión de software dañino [A6]	Software [SW]	B	75	75	20
		Datos [D]	B	75	75	20
	[Re-]encaminamiento de mensajes [A7]	Red de Comunicaciones [COM]	MB	50	75	
		Software [SW]	MB	50	75	
		Servicios [S]	MB	50	75	
	Alteración de secuencia [A8]	Servicios [S]	MB	50	75	
		Red de Comunicaciones [COM]	MB	50		
		Software [SW]	B	50	75	

	Acceso no autorizado [A9]	Servicios [S]	B	75	75	50
		Red de Comunicaciones [COM]	B	30	75	30
		Software [SW]	B	75	50	75
		Hardware [HW]	MB		50	
		Datos [D]	B	100	100	100
		Equipamiento Auxiliar [AUX]	B		50	
		Instalaciones [L]	B	20	20	20
	Análisis de tráfico [A10]	Datos [D]	MB	50		
	Repudio [A11]	Servicios [S]	MB			
	Interceptación de información (escucha) [A12]	Datos [D]	B	100		
	Modificación deliberada de la información [A13]	Datos [D]	B			100
		Software [SW]	B			100
	Destrucción de información [A14]	Datos [D]	B		100	
		Software [SW]	B		100	
	Divulgación de información [A15]	Datos [D]	B	100		
		Software [SW]	B	100		
	Manipulación de programas [A16]	Software [SW]	B		100	
	Manipulación de los equipos [A17]	Hardware [HW]	B		100	
		Servicios [S]	B		100	

	Denegación de servicio [A18]	Red de Comunicaciones [COM]	B		100	
	Robo [A19]	Hardware [HW]	B		75	
		Equipamiento Auxiliar [AUX]	MB		75	
		Datos [D]	MB	100	100	
		Software [SW]	MB	100	75	
	Ataque destructivo [A20]	Instalaciones [L]	MB		100	
		Hardware [HW]	MB		100	
		Software [SW]	MB		100	
		Equipamiento Auxiliar [AUX]	MB		100	
		Red de Comunicaciones [COM]	MB		100	
		Servicios [S]	MB		100	
		Datos [D]	MB		100	
	Ocupación enemiga [A21]	Instalaciones [L]	MB	20	100	
		Hardware [HW]	MB	20	100	
		Software [SW]	MB	75	100	
		Equipamiento Auxiliar [AUX]	MB	20	100	
		Red de Comunicaciones [COM]	MB	30	100	
		Servicios [S]	MB	80	100	
		Datos [D]	MB	100	100	
	Indisponibilidad del personal [A22]	Personal [P]	M		100	
	Extorsión [A23]	Personal [P]	B	25	25	25

	Ingeniería social [A24]	Personal [P]	B	25	25	25

Luego de realizar el análisis y evaluación de riesgo de los principales activos de la institución identificando además las amenazas con su probabilidad de ocurrencia, se pueden determinar aquellos con mayor probabilidad de afectación, ya sea por motivo de daños, ataques, vulnerabilidades entre otros.

4.4.4 Selección de objetivos de control

El siguiente paso para el desarrollo del SGSI es relacionar los controles definidos por la norma ISO 27001 con los activos de mayor valoración en cuanto al factor riesgo reflejados en las tablas anteriores.

La norma ISO 27002 se ha tomado como referencia para una ampliación de las prácticas para implementar los controles [25].

Las siguientes son los 14 anexos o dominios que conforman el estándar ISO27001 [25]:

- **Anexo 5:** Políticas de seguridad.
- **Anexo 6:** Aspectos organizativos de la Seguridad de la Información.
- **Anexo 7:** Seguridad ligada a los Recursos Humanos.
- **Anexo 8:** Gestión de Activos.
- **Anexo 9:** Control de Accesos.
- **Anexo 10:** Cifrado.
- **Anexo 11:** Seguridad física y ambiental.
- **Anexo 12:** Seguridad en la Operativa.
- **Anexo 13:** Seguridad de las Telecomunicaciones.
- **Anexo 14:** Adquisición, desarrollo y mantenimiento de los Sistemas de Información.
- **Anexo 15:** Relaciones con Suministradores.
- **Anexo 16:** Gestión de Incidentes en Seguridad de la Información.

- **Anexo 17:** Aspectos de Seguridad de la Información en la gestión de continuidad del negocio.
- **Anexo 18:** Cumplimiento.

A continuación, en la columna "Objetivo de control" de la siguiente tabla, contiene el dominio relacionado con la posible amenaza de cada activo informático detallado:

Tabla 24: Selección de objetivos de control.

Fuente: Elaborado por el investigador.

Tipo de Activo	Amenaza	Probabilidad de ocurrencia	Objetivos de Control	Controles de la norma ISO 27001
Hardware	A. Fuego	MB	A5.1 Directrices de gestión de la seguridad de la información A8.1 Responsabilidad sobre los activos A9.2 Gestión de acceso de usuario A11.1 Áreas seguras A11.2 Seguridad de los equipos A16.1 Gestión de incidentes de seguridad de la información y mejoras	A11.1.1 Perímetro de seguridad física (A, B, C, D) A11.1.3 Protección contra las amenazas externas y ambientales (A, B, C, D) A8.1.3 Uso aceptable de los activos (E, K) A11.2.4 Mantenimiento de los equipos (E, K) A11.2.2 Instalaciones de suministro (F) A5.1.1 Políticas para la seguridad de la información (G) A8.1.2 Propiedad de los activos (H, L) A9.2.3 Gestión de privilegios de acceso (I, J) A16.1.1 Responsabilidades y procedimientos (M)
	B. Erupción Volcánica	MB		
	C. Terremoto	MB		
	D. Daños por Agua	MB		
	E. Avería de origen físico o lógico	MB		
	F. Corte de suministro eléctrico	B		
	G. Errores de Administrador	B		
	H. Pérdida de equipos	MB		
	I. Abuso de privilegios de acceso	MB		
	J. Acceso no autorizado	MB		
	K. Manipulación de los equipos	MB		
	L. Robo	MB		
	M. Ataque destructivo	MB		
Software	A. Avería de origen físico o lógico	B	A5.1 Directrices de gestión de la seguridad de la información A8.1 Responsabilidad sobre los activos A9.2 Gestión de acceso de usuario A9.4 Control de acceso a sistemas y aplicaciones A12.2 Protección contra el software malicioso (malware)	A8.1.3 Uso aceptable de los activos (A) A5.1.1 Políticas para la seguridad de la información (B, C, E, N) A12.2. 1 controles contra el código malicioso (D) A9.4.1 Restricción del acceso a la información (F, G) A12.6.1 Gestión de las vulnerabilidades técnicas (H, I, M)
	B. Errores de usuarios	A		
	C. Errores de administrador	B		
	D. Difusión de Software dañino	B		
	E. Alteración accidental de la información	MB		
	F. Destrucción de información	MB		
	G. Fugas de información	MB		

	H. Vulnerabilidades de los programas (software)	MB	A12.6 Gestión de la vulnerabilidad técnica	A9.4.2 Procedimientos seguros de inicio de sesión (J) A9.2.3 Gestión de privilegios de acceso (K, L)
	I. Errores de mantenimiento/actualización de programas (software)	A		
	J. Suplantación de la identidad del usuario	MB		
	K. Abuso de privilegios de acceso	MB		
	L. Acceso no autorizado	MB		
	M. Manipulación de programas	MB		
	N. Divulgación de información	MB		
Redes de comunicación	A. Erupción Volcánica	MB	A5.1 Directrices de gestión de la seguridad de la información A9.2 Gestión de acceso de usuario A9.4 Control de acceso a sistemas y aplicaciones A11.2 Seguridad de los equipos A13.1 Gestión de la seguridad de las redes A13.2 Intercambio de información	A11.2.1 Emplazamiento y protección de equipos (A, B) A11.2.3 Seguridad del cableado (B) A5.1.1 Políticas para la seguridad de la información (D, K) A13.1.1 Controles de red (D) A9.4.1 Restricción del acceso a la información (E, F) A9.4.2 Procedimientos seguros de inicio de sesión (G) A9.2.3 Gestión de privilegios de acceso (H, I) A13.1.2 Seguridad de los servicios de red (J) A13.2.4 Acuerdos de confidencialidad o no revelación (K)
	B. Terremoto	MB		
	C. Fallo de servicios de comunicaciones	B		
	D. Alteración accidental de la información	MB		
	E. Destrucción de la información	MB		
	F. Fugas de información	B		
	G. Suplantación de la identidad del usuario	MB		
	H. Abuso de privilegios de acceso	MB		
	I. Acceso no autorizado	MB		
	J. Análisis de tráfico	MB		
	K. Divulgación de información	MB		
Servicios	A. Errores de los Usuarios	M	A5.1 Directrices de gestión de la seguridad de la información A9.2 Gestión de acceso de usuario A9.4 Control de acceso a sistemas y aplicaciones	A5.1.1 Políticas para la seguridad de la información (A, B, C, I) A9.4.1 Restricción del acceso a la información (D, E) A9.4.2 Procedimientos seguros de inicio de sesión (F) A9.2.3 Gestión de privilegios de acceso (G, H)
	B. Errores del administrador	M		
	C. Alteración accidental de la información	B		
	D. Destrucción de la información	MB		
	E. Fugas de información	M		

	F. Suplantación de identidad del usuario	B		
	G. Abuso de privilegios de acceso	B		
	H. Acceso no autorizado	B		
	I. Divulgación de información	M		
Equipamiento Auxiliar	A. Fuego	MB	A5.1 Directrices de gestión de la seguridad de la información A8.1 Responsabilidad sobre los activos A9.2 Gestión de acceso de usuario A11.1 Áreas seguras A11.2 Seguridad de los equipos A16.1 Gestión de incidentes de seguridad de la información y mejoras	A11.1.1 Perímetro de seguridad física (A, B, C, D) A11.1.3 Protección contra las amenazas externas y ambientales (A, B, C, D) A8.1.3 Uso aceptable de los activos (E, I) A11.2.4 Mantenimiento de los equipos (E, I) A11.2.2 Instalaciones de suministro (F) A8.1.2 Propiedad de los activos (G, J) A9.2.3 Gestión de privilegios de acceso (H) A16.1.1 Responsabilidades y procedimientos (K)
	B. Erupción Volcánica	M		
	C. Terremoto	MB		
	D. Daños por Agua	MB		
	E. Avería de origen físico o lógico	B		
	F. Corte de suministro eléctrico	B		
	G. Pérdida de equipos	MB		
	H. Acceso no autorizado	MB		
	I. Manipulación de los equipos	B		
	J. Robo	MB		
	K. Ataque destructivo	MB		
Personal	A. Fugas de información	MB	A5.1 Directrices de gestión de la seguridad de la información A7.1 Antes del empleo A7.2 Durante el empleo	A5.1.1 Políticas para la seguridad de la información (A) A7.1.2 Términos y condiciones del empleo (B) A7.2.1 Responsabilidades de gestión (B) A7.2.3 Proceso disciplinario (C, D)
	B. Indisponibilidad del personal	B		
	C. Extorsión	MB		
	D. Ingeniería social (picaresca)	MB		
Soportes de información	A. Fuego	MB	A5.1 Directrices de gestión de la seguridad de la información A8.1 Responsabilidad sobre los activos A9.2 Gestión de acceso de usuario A9.4 Control de acceso a sistemas y aplicaciones	A11.1.1 Perímetro de seguridad física (A, B) A11.1.3 Protección contra las amenazas externas y ambientales (A, B) A8.1.3 Uso aceptable de los activos (C, M) A11.2.4 Mantenimiento de los equipos (C, M) A11.2.2 Instalaciones de suministro (D)
	B. Daños por agua	MB		
	C. Avería de origen físico o lógico	MB		
	D. Corte de suministro eléctrico	B		
	E. Errores de los usuarios	MB		

	F. Errores del administrador	MB	A11.1 Áreas seguras A11.2 Seguridad de los equipos A16.1 Gestión de incidentes de seguridad de la información y mejoras	A5.1.1 Políticas para la seguridad de la información (E, F, G, L) A9.4.1 Restricción del acceso a la información (H, I) A8.1.2 Propiedad de los activos (J, N) A9.2.3 Gestión de privilegios de acceso (K) A16.1.1 Responsabilidades y procedimientos (O)
	G. Alteración accidental de la información	MB		
	H. Destrucción de información	MB		
	I. Fugas de información	MB		
	J. Pérdida de equipos	MB		
	K. Acceso no autorizado	MB		
	L. Divulgación de información	MB		
	M. Manipulación de los equipos	MB		
	N. Robo	MB		
	O. Ataque Destructivo	MB		

4.4.5 Declaración de Aplicabilidad

Para mantener el registro y control de las medidas de seguridad aplicadas se desarrolló la declaración de aplicabilidad (SOA) en la Tabla 25: Aplicabilidad de controles, que se trata de un documento que en lista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001 (un conjunto de 114 controles agrupados en 35 objetivos de control, en la versión de 2013 de esta norma de seguridad) [26].

El anexo A suele ser utilizado como una referencia para la implementación de medidas de protección de la información, con eso se detallan y se verifican los controles relevantes para su aplicabilidad a la situación actual de la empresa Megaprofer S.A., respaldada por la norma ISO/IEC 27002 [26].

El proceso consiste en enumerar los controles de seguridad que son factibles de implementar en la empresa, así como la justificación de aquellos que no lo son. La declaración de aplicabilidad incluye:

- El dominio o control de la norma ISO 27001.
- Los objetivos de control, así como los controles que se llevan a cabo o se implementan.
- Los objetivos de control seleccionados y su justificación.
- Los objetivos de control que se han excluido y la justificación para tomar tal decisión.

La persona encargada de revisar y aprobar la declaración de aplicabilidad es encargada del seguimiento a la seguridad de la información en el departamento de TICS, Ing. Mario Pérez.

Tabla 25: Aplicabilidad de controles.
Fuente: Elaborado por el investigador.

ISO/IEC 27002:2013	Aplicable	No Aplicable	Justificación
5. POLÍTICAS DE SEGURIDAD.			
5.1 Directrices de la Dirección en seguridad de la información.			
5.1.1 Conjunto de políticas para la seguridad de la información.	X		Es de vital importancia que exista un conjunto de políticas para asegurar la información y que pueda ser comunicado a todo el personal de la entidad.
5.1.2 Revisión de las políticas para la seguridad de la información.	X		Es necesario que periódicamente se haga una revisión de las políticas integradas con la finalidad de garantizar la eficacia de las mismas.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.			
6.1 Organización interna.			
6.1.1 Asignación de responsabilidades para la seguridad de la información.	X		Se debe gestionar adecuadamente la seguridad de la información definiendo responsabilidades por parte de la gerencia.
6.1.2 Segregación de tareas.	X		Es imprescindible que se lleve a cabo la gestión de la seguridad en base a las competencias por

			departamentos que posee la institución y asignar un personal adecuado.
6.1.3 Contacto con las autoridades.	X		Periódicamente se debe mantener contacto con el departamento de TICS ya que ellos gestionaran la seguridad de la información con el fin de monitorizar y regular los procesos que se lleven a cabo.
6.1.4 Contacto con grupos de interés especial.	X		Se debe compartir información con grupos de interés para tener mejor tratamiento del riesgo en cuanto a la seguridad de la información.
6.1.5 Seguridad de la información en la gestión de proyectos.	X		Es necesario identificar y abordar los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos.
6.2 Dispositivos para movilidad y teletrabajo.			
6.2.1 Política de uso de dispositivos para movilidad.	X		Es necesario definir controles y normativas respecto al uso que se le den a los dispositivos para la movilidad.
6.2.2 Teletrabajo.	X		Es necesario definir controles y normativas respecto al teletrabajo que se realiza en un ámbito diferente a la oficina.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.			

7.1 Antes de la contratación.			
7.1.1 Investigación de antecedentes.	X		Es necesario que se investigue los antecedentes penales al aspirante en el proceso de contratación.
7.1.2 Términos y condiciones de contratación.	X		En el proceso de contratación se debe dar a conocer normativas y políticas que el aspirante deberá acatar.
7.2 Durante la contratación.			
7.2.1 Responsabilidades de gestión.	X		Debe existir un programa de concientización / educación sobre la seguridad de la información dirigido a la gerencia para el conocimiento y la capacitación apropiados específicamente sobre su riesgo clave de información y roles.
7.2.2 Concienciación, educación y capacitación en seguridad de la información	X		Es necesario un programa estructurado de sensibilización y capacitación sobre seguridad de la información para todos los tipos de trabajadores.
7.2.3 Proceso disciplinario.	X		Se debe explicar al aspirante el proceso de disciplina que debe cumplir en el área de trabajo para evitar violaciones a la privacidad, piratería informática, fraude y espionaje industrial.
7.3 Cese o cambio de puesto de trabajo.			

7.3.1 Cese o cambio de puesto de trabajo.	X		Antes del contrato es importante mencionar políticas sobre el derecho que se le otorga en la empresa que sean claras para el cese o cambio del lugar de trabajo con la finalidad de que a futuro no existan inconvenientes.
8. GESTIÓN DE ACTIVOS.			
8.1 Responsabilidad sobre los activos.			
8.1.1 Inventario de activos.	X		Todos los activos deben estar identificados y a partir de ello mantener un inventario actualizado de los mismos.
8.1.2 Propiedad de los activos.	X		El departamento de TICS tiene a su cargo la responsabilidad de los activos informáticos por lo que debe llevar un control adecuado de los mismos.
8.1.3 Uso aceptable de los activos.	X		Es importante existencia de los controles sobre los activos para promulgar el correcto uso de los recursos y por ende de la información.
8.1.4 Devolución de activos.	X		Debe existir un procedimiento automatizado para recuperar los activos tras una baja o despido y así garantizar que no haya desvíos.

8.2 Clasificación de la información.			
8.2.1 Clasificación de la información.	X		Es importante contar con políticas de revisión, estándares, procedimientos, directrices y registros asociados relacionados con la clasificación de la información obteniendo los requisitos de confidencialidad, integridad y disponibilidad con conocimiento al personal.
8.2.2 Etiquetado y manipulado de la información.	X		Mediante el proceso de etiquetado para la información física debe estar sincronizado a la clasificación de la información.
8.2.3 Manipulación de activos.	X		Se debe establecer medidas de control que verifiquen que solo el personal autorizado pueda manipular la información de los activos.
8.3 Manejo de los soportes de almacenamiento.			
8.3.1 Gestión de soportes extraíbles.	X		Se debe contar con controles apropiados para el registro de medios extraíbles, etiquetados y clasificados de forma adecuada para mantener la confidencialidad de los datos almacenados.

8.3.2 Eliminación de soportes.	X		El proceso de eliminación de soporte debe estar ligado a una autoridad quien autorice el acto, documentando la aprobación del mismo.
8.3.3 Soportes físicos en tránsito.	X		Es de necesario cumplir con los controles se seguridad para que el transporte o el servicio de mensajería sean confiables.
9. CONTROL DE ACCESOS.			
9.1 Requisitos de negocio para el control de accesos.			
9.1.1 Política de control de accesos.	X		Es necesario tener las políticas de control de acceso documentado y aprobado por el que gestiona la información.
9.1.2 Control de acceso a las redes y servicios asociados.	X		La seguridad en el acceso VPN debe ser supervisado, controlados y autorizados para evitar el hurto de información.
9.2 Gestión de acceso de usuario.			
9.2.1 Gestión de altas/bajas en el registro de usuarios.	X		Es importante que los usuarios tengas un ID único para facilidad de gestionar cualquier acontecimiento y se pueda resolver de manera adecuada.

9.2.2 Gestión de los derechos de acceso asignados a usuarios.	X		El control de acceso a los usuarios debe garantizar que se concede de acuerdo a las políticas de control de acceso y segregación de las funciones.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	X		Debe existir un proceso para realizar revisiones más frecuentes y periódicas de las cuentas privilegiadas con el fin de monitorizar actividades ejecutadas.
9.2.4 Gestión de información confidencial de autenticación de usuarios.	X		Se debe gestionar correctamente controles técnicos para la identidad de los usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.	X		Debe existir una revisión periódica y documentada de los derechos de acceso de los usuarios en sistemas y aplicaciones.
9.2.6 Retirada o adaptación de los derechos de acceso	X		Debe tomarse como medidas de prevención, los retiros de privilegios en acceso de información y contraseñas a los usuarios que se le sea terminado el contrato.
9.3 Responsabilidades del usuario.			
9.3.1 Uso de información confidencial para la autenticación.	X		Es necesario que exista un factor de aseguramiento de la confidencialidad de las credenciales de autentificación.
9.4 Control de acceso a sistemas y aplicaciones.			

9.4.1 Restricción del acceso a la información.	X		Debe existir accesos adecuados para el control de usuarios de forma individual para restringir a personas ajenas a la empresa.
9.4.2 Procedimientos seguros de inicio de sesión.	X		Debe existir una pantalla de advertencia de inicio de sesión para disuadir el acceso no autorizado.
9.4.3 Gestión de contraseñas de usuario.	X		Los sistemas deben requerir que las contraseñas se establezcan bajo políticas y estándares corporativos de manera que se almacenen de forma segura (cifrada).
9.4.4 Uso de herramientas de administración de sistemas.	X		Debe existir una persona encargada que controle los servicios privilegiados bajo condiciones con verificación de acuerdo a sus roles y responsabilidades.
9.4.5 Control de acceso al código fuente de los programas.	X		El almacenamiento del código fuente debe mantenerse en un controlador de versiones de forma segura para un monitoreo consecuente de quien realice diferentes actividades dentro de ella.
10. CIFRADO.			
10.1 Controles criptográficos.			

10.1.1 Política de uso de los controles criptográficos.	X		Debe existir una política que cubra el uso de controles criptográficos, así como la información debe ser protegida a través de la criptografía. Uso de cifrado para información almacenada o transferida.
10.1.2 Gestión de claves.	X		Proteger el equipo utilizado para generar, almacenar y archivar claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.			
11.1 Áreas seguras.			
11.1.1 Perímetro de seguridad física.	X		Se deben establecer perímetros de seguridad para proteger aquellas áreas con equipamiento importante o con instalaciones donde se procesa información.
11.1.2 Controles físicos de entrada.	X		Para evitar mal uso del equipamiento es importante que se definan controles de entrada para asegurar el acceso de solo personal autorizado.
11.1.3 Seguridad de oficinas, despachos y recursos.	X		Debe existir procedimientos para mantener la confidencialidad e integridad en las diferentes áreas.
11.1.4 Protección contra las amenazas externas y ambientales.	X		Debe existir un plan de gestión de riesgos ante eventualidades externas como sismos, incendios,

			ataques ..., para evitar el daño de equipos y mucho menos la pérdida de información.
11.1.5 El trabajo en áreas seguras.	X		Se debe realizar verificaciones en los puestos de trabajos y tener en cuenta que no pueden utilizar cualquier mecanismo de grabación.
11.1.6 Áreas de acceso público, carga y descarga.	X		Debe existir procedimientos para la carga y descarga de mercadería.
11.2 Seguridad de los equipos.			
11.2.1 Emplazamiento y protección de equipos.	X		Una correcta ubicación de los equipos disminuirá el riesgo de amenazas y peligros ambientales para los equipos.
11.2.2 Instalaciones de suministro.	X		El sistema de UPS debe proporcionar una potencia adecuada, confiable y de alta calidad que sea monitoreada periódicamente con la finalidad de que abarquen todos los equipos esenciales durante un período de tiempo suficiente que se produzca un acontecimiento de falla eléctrica.

11.2.3 Seguridad del cableado.	X		Se debe proteger el cableado de energía y comunicaciones para evitar tanto daños como interferencias.
11.2.4 Mantenimiento de los equipos.	X		Programar un mantenimiento periódico de los equipos a fin de mantener la disponibilidad de la información y evitar daños futuros que puedan ocasionar pérdida de información.
11.2.5 Salida de activos fuera de las dependencias de la empresa.	X		Debe existir reglas de uso para los equipos fueras de las instalaciones, así también contar con una aprobación apropiada que sea documentada.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	X		Deben existir políticas de uso aceptable y compromiso del empleado cumpliendo requisitos de seguridad y obligaciones para uso de los equipos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	X		Para prevenir la revelación de la información en la reasignación o eliminación de equipos, será necesario realizar un respaldo o borrado seguro de la información.

11.2.8 Equipo informático de usuario desatendido.	X		Debe existir un tiempo adecuado para establecer en estado de suspensión cuando el usuario está en inactividad.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	X		Es importante que exista políticas, nomas, procedimientos y directrices para mantener las zonas de trabajo limpias y despejadas.
12. SEGURIDAD EN LA OPERATIVA.			
12.1 Responsabilidades y procedimientos de operación.			
12.1.1 Documentación de procedimientos de operación.	X		Se deben documentar los procedimientos operativos y ponerlos a disposición de los demás.
12.1.2 Gestión de cambios.	X		Es de importancia la existencia de un plan de control para gestionar los cambios en sistemas operacionales.
12.1.3 Gestión de capacidades.	X		Para alcanzar un nivel óptimo respecto a la productividad de los sistemas es importante que se realice un seguimiento continuo del uso de recursos pata tomar medidas correctivas si fuese necesario.
12.1.4 Separación de entornos de desarrollo, prueba y producción.		X	No aplica, debido a que la empresa no se desarrolla ningún tipo de sistema.

12.2 Protección contra código malicioso.			
12.2.1 Controles contra el código malicioso.	X		Es vital para garantizar la integridad de la información que se establezcan mecanismos o herramientas de detección de ataques y código malicioso.
12.3 Copias de seguridad.			
12.3.1 Copias de seguridad de la información.	X		Con la realización de copias de seguridad de la información se garantiza que la información esté disponible a todo momento especialmente en caso de que ocurran incidentes que la comprometan.
12.4 Registro de actividad y supervisión.			
12.4.1 Registro y gestión de eventos de actividad.	X		Es importante registrar los problemas que ocurren relacionados con la seguridad de la información a fin de analizarlos y brindar soluciones más eficaces
12.4.2 Protección de los registros de información.	X		Debe existir un área donde se resguarden archivos de importancia para la empresa con la finalidad de accesos no autorizados.
12.4.3 Registros de actividad del administrador y operador del sistema.			Debe existir un control de las actividades del administrador y operador del sistema para llevar un registro y poder ser revisado periódicamente.

12.4.4 Sincronización de relojes.	X		Es vital que exista políticas, arquitecturas o procedimientos relativos a la sincronización del reloj del todos los sistemas.
12.5 Control del software en explotación.			
12.5.1 Instalación del software en sistemas en producción.	X		Es necesario políticas de instalación de software para que asegurar que sea probado, aprobado, permitido y mantenido en la producción teniendo soporte en los diferentes ordenadores existentes en la empresa.
12.6 Gestión de la vulnerabilidad técnica.			
12.6.1 Gestión de las vulnerabilidades técnicas.	X		Al obtener oportunamente información de ataques o vulnerabilidades el departamento de TICS está en la capacidad de tomar las medidas correctivas apropiadas.
12.6.2 Restricciones en la instalación de software.	X		La instalación de software está limitada al personal autorizado que ejecuta la acción adecuada.
12.7 Consideraciones de las auditorías de los sistemas de información.			
12.7.1 Controles de auditoría de los sistemas de información.	X		Es necesario que exista una política que requiera auditorias de seguridad de la información para

			garantizar la confidencialidad de la información, para ello debe tener herramientas de auditoria controladas.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.			
13.1 Gestión de la seguridad en las redes.			
13.1.1 Controles de red.	X		Es importante que la separación de la administración de las operaciones de sistemas y la de infraestructura de red para monitoreo de las conexiones que se realizan en ella y garantizar la integridad y confidencialidad de la información.
13.1.2 Mecanismos de seguridad asociados a servicios en red.	X		Debe existir revisiones periódicas de las configuraciones de red y que se puedan emplear de manera eficiente mecanismos de autentificación y cifrado de tráfico en la red.
13.1.3 Segregación de redes.	X		Es necesario políticas de segmentación de red basada en la clasificación, los niveles de confianza, dominios para obtener una buena organización.
13.2 Intercambio de información con partes externas.			

13.2.1 Políticas y procedimientos de intercambio de información.		X	No aplica, la información se maneja explícitamente de manera interna. No existe motivo alguno para compartirla con terceras personas.
13.2.2 Acuerdos de intercambio.		X	No aplica, la información se maneja explícitamente de manera interna.
13.2.3 Mensajería electrónica.	X		Toda información relacionada con los procesos internos pasa por servidores de mensajería que el departamento de TICS tiene configuradas, por lo que es indispensable asegurar la integridad de la misma.
13.2.4 Acuerdos de confidencialidad y secreto.	X		Es importante documentar acuerdos de confidencialidad de la información con lo cual se garantiza la no divulgación y por tanto el uso inadecuado de la misma.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.			
14.1 Requisitos de seguridad de los sistemas de información.			
14.1.1 Análisis y especificación de los requisitos de seguridad.	X		Se deben regir en las políticas, procedimientos y registros relacionados con el análisis de requisitos de seguridad para la adquisición de sistemas y software.

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.		X	No aplica, la empresa no ejecuta el comercio electrónico debido a eso no genera transacciones electrónicas.
14.1.3 Protección de las transacciones por redes telemáticas.		X	No aplica, la empresa no ejecuta el comercio electrónico debido a eso no genera transacciones electrónicas.
14.2 Seguridad en los procesos de desarrollo y soporte.			
14.2.1 Política de desarrollo seguro de software.		X	No aplica, debido a que la empresa no desarrolla ningún tipo de software.
14.2.2 Procedimientos de control de cambios en los sistemas.		X	No aplica, debido a que la empresa no desarrolla ningún tipo de software.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.		X	No aplica, debido a que la empresa no desarrolla ningún tipo de software.
14.2.4 Restricciones a los cambios en los paquetes de software.		X	No aplica, debido a que la empresa no desarrolla ningún tipo de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.		X	No aplica, debido a que la empresa no desarrolla ningún tipo de software.

14.2.6 Seguridad en entornos de desarrollo.		X	No aplica, debido a que la empresa no desarrolla ningún tipo de software.
14.2.7 Externalización del desarrollo de software.		X	No aplica, debido a que la empresa no desarrolla ningún tipo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.		X	No aplica, debido a que la empresa no desarrolla ningún tipo de software.
14.2.9 Pruebas de aceptación.		X	No aplica, debido a que la empresa no desarrolla ningún tipo de software.
14.3 Datos de prueba.			
14.3.1 Protección de los datos utilizados en pruebas.	X		Es de vital importancia mantener una discreción por parte del personal encargado de las pruebas y garantizar la confidencialidad de la información.
15. RELACIONES CON SUMINISTRADORES.			
15.1 Seguridad de la información en las relaciones con suministradores.			
15.1.1 Política de seguridad de la información para suministradores.	X		Se debe contar con políticas, procesos, prácticas y registros relacionados con la gestión de relaciones con suministradores que se involucran servicios de TICS.

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	X		Los acuerdos que se produzcan con los suministradores es necesario documentarlos para tener una validez y compromiso de ambas partes.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	X		Es importante que exista una validación de los requisitos de seguridad de los productos o servicios adquiridos y tener un control de rastreo del origen del producto o servicio.
15.2 Gestión de la prestación del servicio por suministradores.			
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	X		El departamento de TICS debe monitorizar los servicios prestados por terceros para evitar el riesgo de información.
15.2.2 Gestión de cambios en los servicios prestados por terceros.	X		Los cambios en los servicios prestados por terceros con el hecho de estar ligados con la información deben ser tomadas por parte de la gerencia.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.			
16.1 Gestión de incidentes de seguridad de la información y mejoras.			

16.1.1 Responsabilidades y procedimientos.	X		Es necesario establecer responsabilidades para garantizar una respuesta eficaz e inmediata a un determinado problema de seguridad que se pronuncie.
16.1.2 Notificación de los eventos de seguridad de la información.	X		Al momento de una ocurrencia de cualquier eventualidad, la notificación del problema al departamento de TICS permitirá brindar una solución inmediata.
16.1.3 Notificación de puntos débiles de la seguridad.	X		Es vital que existan mecanismos de notificación de puntos débiles en la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	X		Con la clasificación de incidentes de seguridad permitirá dar una solución eficaz a aquellos con mayor afectación para la empresa.
16.1.5 Respuesta a los incidentes de seguridad.	X		Mediante el plan de contingencia se debe evaluar el manejo de incidentes que se puedan pronunciar.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	X		Con la documentación de los incidentes producidas se pueden identificar incidentes de impacto con el fin de evitar recurrencias.
16.1.7 Recopilación de evidencias.	X		Con la recolección de evidencias de los incidentes hace de forma competente a la empresa o terceros

			capacitarse en área con procesos y herramientas adecuadas.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.			
17.1 Continuidad de la seguridad de la información.			
17.1.1 Planificación de la continuidad de la seguridad de la información.	X		Para garantizar la continuidad de la seguridad de la información la empresa realice una planificación de las actividades empresariales, documentar los procesos y controles que permitan solucionar inconvenientes en un futuro cercano.
17.1.2 Implantación de la continuidad de la seguridad de la información.	X		En la continuidad de la seguridad de información debe ser implementado de forma que se puedan restaurar los servicio tras una interrupción y sean adecuados em sitios de recuperación de desastres remotos.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	X		Debe existir un método de pruebas del plan de continuidad dando resultados reales.
17.2 Redundancias.			

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	X		Se den identificar los requisitos de disponibilidad de servicios para mantener un continuo procesamiento de Información con capacidades de recuperación.
18. CUMPLIMIENTO.			
18.1 Cumplimiento de los requisitos legales y contractuales.			
18.1.1 Identificación de la legislación aplicable.	X		Deben existir políticas acerca del cumplimiento garantizado de requisitos legales manteniendo un registro de cumplimiento de todas las obligaciones, expectativa legales, reglamentarias y contractuales.
18.1.2 Derechos de propiedad intelectual (DPI).	X		Es necesario establecer políticas y procedimientos relativos a la adquisición, el uso y licencias de propiedad intelectual, gestión de licencias y cumplimiento.
18.1.3 Protección de los registros de la organización.	X		Deben promoverse buenas prácticas respecto a la protección por pérdida, destrucción, amenaza …, de registros importantes de la institución.
18.1.4 Protección de datos y privacidad de la información personal.	X		Debe existir un mecanismo para instruir al personal en el manejo de información debido a que por ética se

			debe garantizar la privacidad y la protección de la información de carácter personal.
18.1.5 Regulación de los controles criptográficos.	X		Debe existir una política que cubra actividades relacionadas con importación/exportación de material criptográfico, con requisitos legales y reglamentarios.
18.2 Revisiones de la seguridad de la información.			
18.2.1 Revisión independiente de la seguridad de la información.	X		Es necesario revisar de manera individual políticas, objetivos de control y demás procesos de seguridad de forma periódica.
18.2.2 Cumplimiento de las políticas y normas de seguridad.	X		El departamento de TICS deberá asignar un responsable en el área de seguridad de información que deberá revisar periódicamente el cumplimiento de políticas, procesos, normas y demás mecanismos de seguridad implementados.
18.2.3 Comprobación del cumplimiento técnico.	X		Para una mejor administración en la gestión de seguridad es preciso la realización de una auditoría interna para garantizar que se cumplen adecuadamente los procesos de seguridad.

4.4.6 Cumplimiento de los controles en base a la norma ISO 27001.

Dado la declaración de la aplicabilidad realizada conforme a la empresa Megaprofer S.A, se determina el nivel de cumplimiento de los 14 Anexos presentados anteriormente con sus respectivos dominios y objetivos de control, a fin de elaborar la propuesta de mejora de los controles de mayor relevancia que integra la norma internacional ISO/IEC 27001 para la entidad, analizando cada control con el encargado del seguimiento al proceso de la implementación de la norma, se determina el porcentaje del cumplimiento de cada uno de los controles planteados.

Anexo 5: Políticas de seguridad.

5.1 Directrices de la Dirección en seguridad de la información.

5.1.1 Conjunto de políticas para la seguridad de la información.

El departamento de TICS no cuenta con un documento formal que especifique las políticas de seguridad de la información para que sean expuestas a la institución, dentro de la entidad los procesos son llevados a cabo sin un lineamiento establecido, se aplican ciertas normatividades de BASC para que se lleve a cabo un conjunto de políticas las cuales no garantizan la seguridad de la información.

Es necesario que se documenten políticas de seguridad factibles que sean de carácter obligatorias para todo el personal de Megaprofer sin excepción alguna, ya que todos son participes en ella y debe existir sanciones aquel que incumpla las políticas que se hayan expuesto de forma transparente.

5.1.2 Revisión de las políticas para la seguridad de la información.

El conjunto de políticas establecidas es fundamental para la seguridad de la información, pese a ello se lleva a cabo en diferentes escenarios, no mantienen un plan periódico para que el departamento de TICS este comprometido a realizar revisiones y actualizaciones con el fin de determinar su efectividad, autorización, cumplimiento y distribución la cual garantice la seguridad de la información en los procesos que se llevan cotidianamente en la organización.

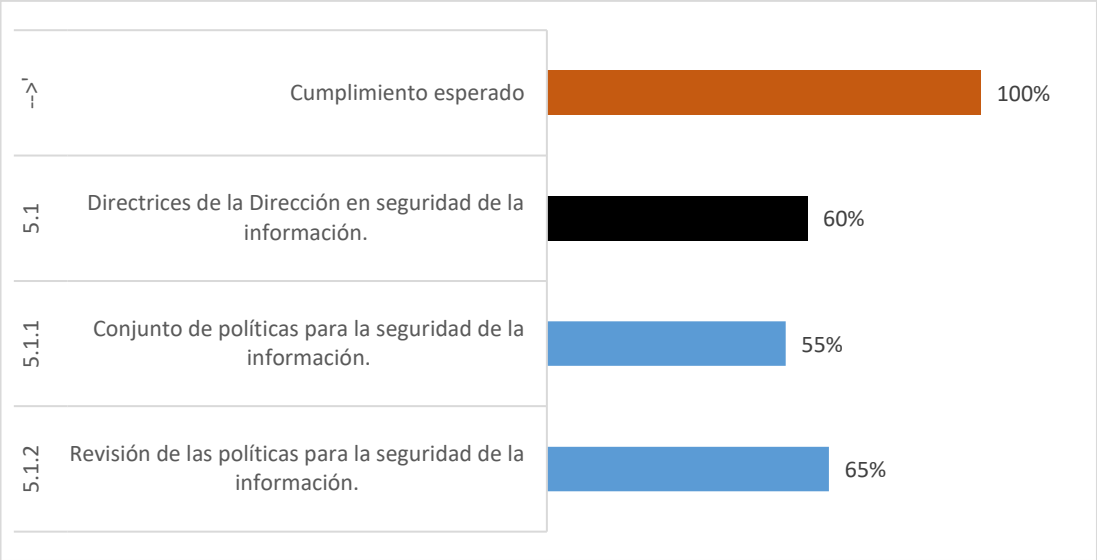

Fig. 10: Cumplimiento políticas de seguridad.
Fuente: Elaborado por el investigador.

Interpretación: En la gráfica se puede observar que un 55% de control del conjunto de políticas para la seguridad se aplican, mientras que el control de las revisiones de las políticas para la seguridad de la información tiene un cumplimiento del 65% ya que no se puede dar un seguimiento por falta de un plan periódico de revisiones.

Anexo 6: Aspectos organizativos de la Seguridad de la Información.

6.1 Organización interna.

6.1.1 Asignación de responsabilidades para la seguridad de la información.

En el departamento de TICS la asignación de responsabilidades para la seguridad de la información es de manera ineficiente, ya que no cuenta con el personal suficiente y adecuado para ejecutar el cargo, por ende, no brinda el suficiente énfasis a la seguridad y riesgo de la información, ante cualquier eventualidad en la seguridad de la información todo el personal de sistemas es responsable.

Existe poco control y monitoreo de los procesos que se realizan en la entidad, una desventaja es que el personal en los diferentes procesos no tiene conocimiento con quien comunicarse ante cualquier suceso que pueda ocurrir con respecto a la seguridad de la información, debido a que no se tiene a un personal asignado.

Un factor negativo que tiene el departamento de sistemas es que tiene un poco apoyo por parte de la administración gerencial, contando con bajos recursos para gestionar las actividades de seguridad y riesgo de la información.

6.1.2 Segregación de tareas.

No existe un control adecuado para las responsabilidades de segregación de tareas, a falta de políticas que lo cubran para la toma de decisiones con respecto a las segregaciones, se lleva un control simple de acuerdo a los conocimientos y competencias donde se asignan diferentes tareas que estén en la capacidad de ser ejecutados.

La segregación se debe manejar con una matriz RACI, conocida como una matriz de responsabilidades que sirve para establecer responsabilidades de cada actor que sea participe en una tarea.

6.1.3 Contacto con las autoridades.

Para salvaguardar la información que se maneja en la institución, el departamento de TICS es el encargado de dar una solución a dicho acontecimiento que comprometa la seguridad interna, por lo que si cumplen con este control ya que cuando se dan este tipo de eventos acuden a gerencia, el área de TICS es el encargado de la solución inmediata manteniendo comunicación del evento.

6.1.4 Contacto con grupos de interés especial.

Este control no se cumple debido a que no mantienen contacto con grupos de interés especial donde compartan amenazas, tecnologías de seguridad, buenas prácticas…, que ayuden a la seguridad de la información.

6.1.5 Seguridad de la información en la gestión de proyectos.

Para abordar los riesgos de la información y los requisitos de seguridad en todas las etapas de todos los proyectos no lo acatan de forma correcta, ya que la mayor parte de ellas se lo dejan a personas quienes brindan los proyectos que se relacionan con la información, cambios / mejoras en los sistemas, aplicaciones y procesos existentes. Las etapas de los proyectos no incluyen actividades apropiadas.

6.2 Dispositivos para movilidad y teletrabajo.

6.2.1 Política de uso de dispositivos para movilidad.

Par la movilidad de los dispositivos no se ha establecido políticas, pero el personal de sistemas en la inducción que se le da al personal al integrarse a la empresa de forma verbal da a conocer los reglamentos que debe cumplir con los dispositivos de movilidad, y a su vez para verificar la integridad de la información y actualizaciones de los programas del equipo se realiza una conexión remota.

6.2.2 Teletrabajo.

No existen controles de seguridad eficaces para el teletrabajo, ya que se puede ejecutar desde cualquier lugar donde el personal tenga acceso al medio, no tienen definido autentificaciones adecuadas del usuario al equipo de conexión y no realizan monitoreos para que la información se mantenga con integridad y sea confidencial.

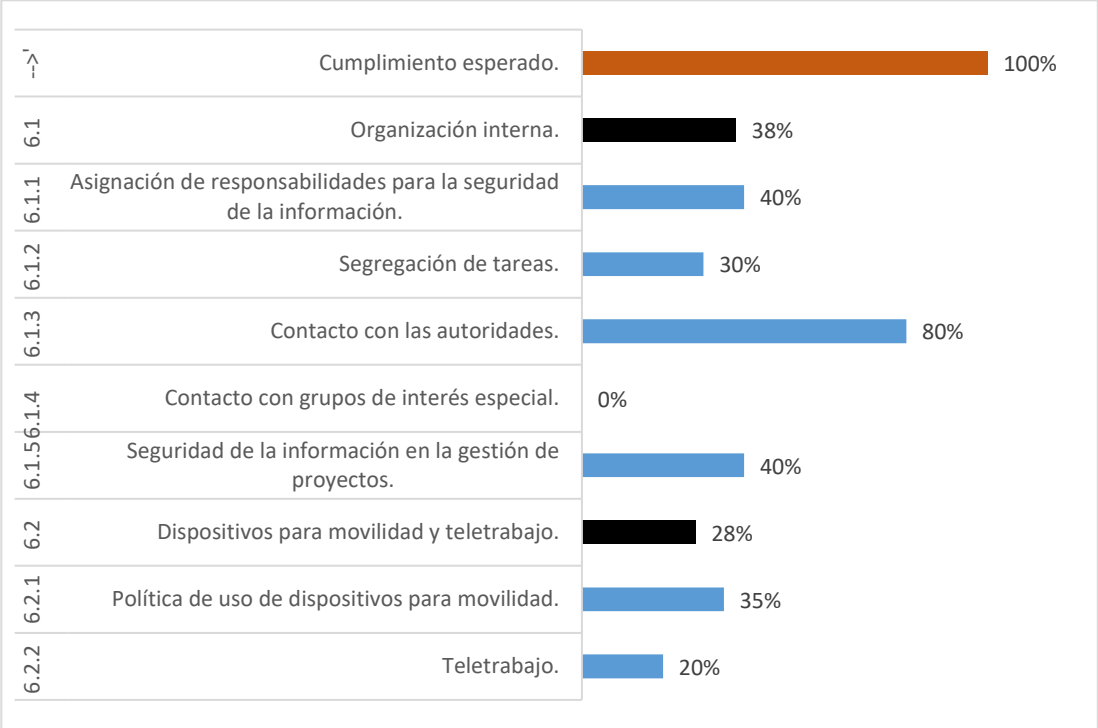

Fig. 11: Cumplimiento aspectos organizativos de la seguridad de la información.
Fuente: Elaborado por el investigador.

Interpretación: de acuerdo a la gráfica relacionada con los aspectos organizativos de la seguridad de la información se puede observar que existe menos del 50% del cumplimento siendo solo un 80% de cumplimiento en el control contacto con las

autoridades y obteniendo un 0% del cumplimiento del contacto con grupos de interés.

En los dispositivos para la movilidad y el teletrabajo se evidencia un 28% del cumplimiento debido a la falta de políticas que cubren a los controles siendo un factor importante para que los controles de cumplan de manera eficiente.

Anexo 7: Seguridad ligada a los Recursos Humanos.

7.1 Antes de la contratación.

7.1.1 Investigación de antecedentes.

Antes de la contratación de un aspirante a la empresa, el departamento de Talento Humano tiene definidos políticas basadas en la investigación de antecedentes del personal aspirante a puesto en la empresa, se realizan un análisis del perfil laboral que por parte de la empresa se le envía a que sea llenado y enviado a un integrante de TTHH, así es como identifican experiencia, conocimientos, referencias…, para aplicar al cargo que requiere la entidad.

7.1.2 Términos y condiciones de contratación.

De manera verbal el encargado de la contratación de personal, miembro del departamento de Talento Humano conjuntamente con un integrante del del departamento de TICS son los encargados de difundir claramente los términos y condiciones que tengan que ver con el riesgo de la información, a fin de mantener la información de manera confidencial.

7.2 Durante la contratación.

7.2.1 Responsabilidades de gestión.

El departamento de TICS proporciona los equipos y claves de acceso a los sistemas que van a manejar los empleados que inician su labor en el cargo designado, el proceso es documentado mediante un acta de entrega-recepción a la vez dando una clara explicación sobre el uso adecuado de los activos de información que se entregan o que ellos van a manipular, así como el uso adecuado de las contraseñas.

7.2.2 Concienciación, educación y capacitación en seguridad de la información.

La seguridad de la información es primordial en cualquier aspecto, el departamento de TICS informa a todos los empleados la importancia de cumplir las políticas de la seguridad de la información que se tienen establecidas con la normatividad BASC, la importancia de notificar cualquier problema que se suscite es fundamental por más mínima que sea y que ponga en riesgo la información.

7.2.3 Proceso disciplinario.

Para este control se ayuda en las políticas establecidas en los contratos, pero no se tiene un documento formal que contenga procedimientos a seguir contra los incidentes para el procedimiento disciplinario de la seguridad de la información.

7.3 Cese o cambio de puesto de trabajo.

7.3.1 Cese o cambio de puesto de trabajo.

Para este control la institución con la ayuda del departamento de Talento Humano se tiene cumplimiento adecuado, debido a que el personal que cesa o cambia en sus funciones deja legalizada toda la documentación, procesos, archivos, devolución de activos antes de su retirada de acuerdo a los lineamientos que tiene la entidad.

Se pudo evidenciar que la persona sustituta al puesto de trabajo del cesante no tiene una correcta inducción para tener continuidad en seguir las actividades a su cargo, dado que el personal saliente no guía o capacita sobre las funciones que ejecutaba.

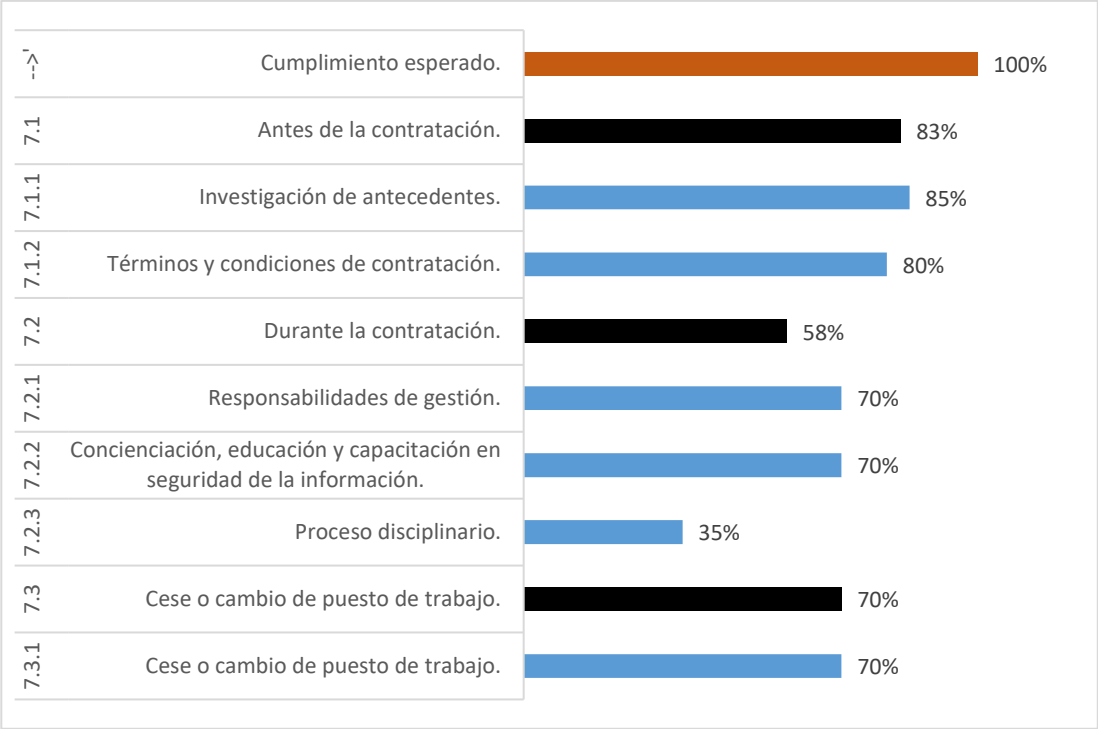

Fig. 12: Cumplimiento seguridad ligada a los recursos humanos.
Fuente: Elaborado por el investigador.

Interpretación: En el cuadro referente a los controles relacionados con la Seguridad ligada a los Recursos Humanos, se puede observar que los controles con mayor índice de cumplimiento son "investigación de antecedentes" y "términos y condiciones de contratación" con un porcentaje promedio del 83%. Los demás controles tienen un índice aceptable a excepción del "proceso disciplinario", cuyo cumplimiento es 35%.

Anexo 8: Gestión de Activos.

8.1 Responsabilidad sobre los activos.

8.1.1 Inventario de activos.

El inventario de activos que posee la entidad se lleva a cabo en el departamento de TICS, quienes están encargados del registro de cada activo existente en todos los procesos de la entidad, se realiza la transición de los activos al personal que ingrese a la empresa y para quienes ya no forman parte de ella, llevando un control documentado por un miembro del área de sistemas.

La responsabilidad de los activos informáticos recae al personal a quien se le entrega y se notifica verbalmente que un activo determinado queda a su debido

cargo bajo los lineamientos de entrega de los mismos, siendo así que el departamento de TICS no tenga custodia sobre todos los quipos informáticos que se encuentran en el interior de la institución.

8.1.2 Propiedad de los activos.

Los bienes son propiedad de la empresa Megaprofer S.A, debido a que son adquiridos con el presupuesto de la institución conforme a las necesidades de cada proceso interno o externo.

El departamento de TICS es el encargado del proceso de responsabilidades sobre los bienes informáticos de la organización, gestionan el cuidado de los mismos mediante aspectos legales que se designan como custodios al personal en el momento de entrega o al momento que ingresa a la empresa.

8.1.3 Uso aceptable de los activos.

Dado la existencia de políticas para el uso adecuado de los activos y gestión de la información que se maneja, se debe garantizar que los empleados de la institución acojan y cumplan responsablemente con dichas normativas expuestas.

Se pudo tener conocimiento de que los bienes son manejados inadecuadamente, de manera que los parámetros y límites con respecto a uso de los mismos no son acatados en un porcentaje aceptable, teniendo casos como los siguientes:

- Las responsabilidades de bloqueo de equipos, no dejar visible la información que manipulan los usuarios al momento de abandonar el puesto de trabajo, estos ítems no son llevadas a cabo adecuadamente.
- El uso de internet ya sea alámbrica o inalámbricamente son utilizados a cierto punto irresponsablemente, ya que tienden a acceder a redes sociales u otro tipo de información.

8.1.4 Devolución de activos.

En este control para la devolución de activos de los empleados o terceros que hayan finalizado su labor en la empresa, se tienen en cuenta el estado del activo siguiendo el cumplimiento de las clausuras de devolución de activos físicos y/o electrónicos que se dieron a conocer al personal antes de realizar la entrega.

8.2 Clasificación de la información.

8.2.1 Clasificación de la información.

La clasificación de la información física o digital está dada según su área es decir según su departamento que tiene la empresa, todos los departamentos tienen procedimientos para acceder a su respectiva información otorgada por el departamento de sistemas, pero no se tiene un control para que la información no sea alterada o eliminada ya sea de manera perjudicial o accidental.

8.2.2 Etiquetado y manipulado de la información

La información ya sea digital o físico se encuentra identificado de acuerdo con las áreas que maneja la empresa, se tienen etiquetado los activos de información con la finalidad de que sea manipulado correctamente por los integrantes de los diferentes departamentos.

8.2.3 Manipulación de activos.

Para manipular correctamente la información y tener manejo eficiente, procesamiento y almacenamiento de los mismos, se tienen clasificados por áreas, configurado por restricciones de acceso ya que un departamento no puede tener acceso a la información de otro, para ello también es importante el etiquetado de la información de acuerdo a los procesos.

8.3 Manejo de los soportes de almacenamiento.

8.3.1 Gestión de soportes extraíbles.

El personal tiene conocimiento del uso de soportes extraíbles, debido a que son un punto muy importante en la seguridad de la información, para su respectivo uso se tiene que tener autorización del departamento de TICS que son los encargados de la confidencialidad de los datos que se almacenan en los ordenadores y medios extraíbles, ellos proporcionan el desbloqueo de puertos para que el medio extraíble pueda ser usado.

8.3.2 Eliminación de soportes.

No se tienen establecidos procedimiento de borrado seguro de los soportes cuando hayan finalizado su ciclo vida, solo se borra información de acuerdo al estado del

activo y tiempo de que disponga algún integrante de área de TICS, con esto existe riesgo de información dado que el activo que no agrega valor es dado de baja y un miembro de la empresa o un tercero puede recuperar información confidencial mediante programas que existen para recuperar datos.

8.3.3 Soportes físicos en tránsito.

Para el transporte a otras ubicaciones de soportes físicos se tienen registros y autorización por el departamento de TICS, además de ello se aplican cintas de seguridad embaladas en el soporte que va a ser trasladado y seguimiento del mismo verificando la recepción por el destino.

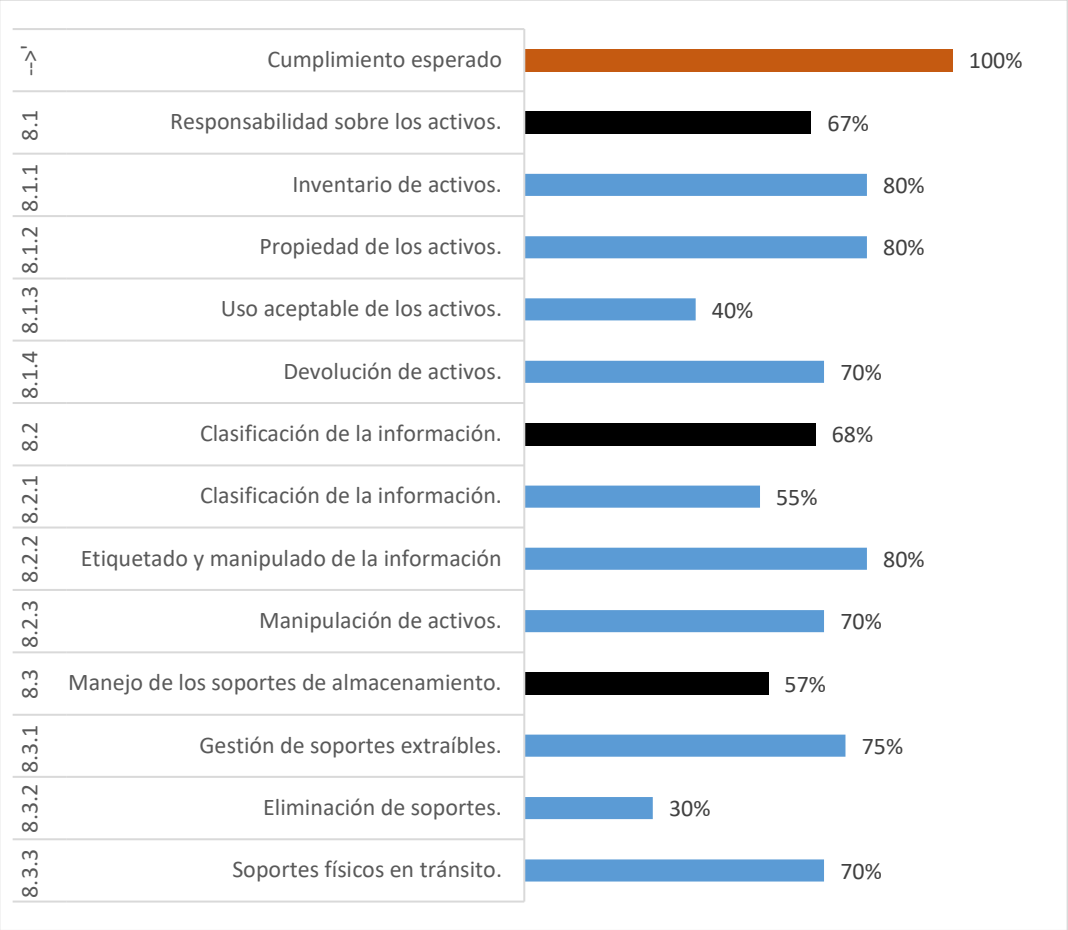

Fig. 13: Cumplimiento gestión de activos.
Fuente: Elaborado por el investigador.

Interpretación: En la figura referente a la Gestión de Activos, se puede percibir que el control con mayor porcentaje de cumplimiento es "Inventario de Activos, Propiedad de activos, Etiquetado y manipulado de la información" con un 80% del cumplimiento, al contrario del control "Eliminación de soportes" que necesitan aplicar controles para

su eficiencia en el cumplimiento y relacionado con los demás controles tienen que ser mejorados.

Anexo 9: Control de Accesos.

9.1 Requisitos de negocio para el control de accesos.

9.1.1 Política de control de accesos.

Para gestionar el control de accesos no cuentan con políticas establecidas, pero se aplican ciertos procedimientos que ayudan a llevar a cabo este control, por ejemplo, el empleado no tiene acceso a un ordenador que no se encuentre bajo su cargo ni mucho menos acceder a los sistemas que maneja la empresa si no cuenta con los permisos para hacerlo. Este proceso se lo controla mediante la asignación de claves las cuales son otorgadas por departamento de TICS.

Es necesario mantener un documento que se verifique el cumplimiento periódico cuando se cree las políticas para el control de acceso y no poner en riesgo los activos de información.

9.1.2 Control de acceso a las redes y servicios asociados.

El departamento de TICS restringe el acceso al personal hacia los sitios web que no son autorizados y que no sean seguros, además servicios que no son necesarios para el desarrollo y cumplimiento de las actividades laborales, también mantienen requisitos de autentificación para el acceso a las redes.

El personal de sistemas tiene privilegios para acceder a la configuración de la red, por tanto, restringe el uso del Wifi a personas no autorizadas, pero para los que tienen acceso no cuenta con supervisión de a qué información pueden ingresar.

9.2 Gestión de acceso de usuario.

9.2.1 Gestión de altas/bajas en el registro de usuarios.

Para la gestión de los registros y bajas de usuarios en la empresa el departamento de TICS es el encargado de administrar las mismas.

En la creación y/o eliminación de usuarios en los sistemas que utilizan la organización, los jefes de cada área son los encargados de solicitar al

departamento de sistemas la creación y asignación de una cuenta para el empleado que se encuentra en su proceso.

Para la gestión de usuarios en los ordenadores el personal de TICS es el encargado de crear o modificar el usuario en el ordenador con sus respectivas credenciales.

El problema percibido es que no tienen una revisión periódica para identificar y deshabilitar usuarios redundantes, usuarios que no se encuentran activos, además de ello cuando un usuario ya no labora en la empresa no es eliminada inmediatamente.

9.2.2 Gestión de los derechos de acceso asignados a usuarios.

No se tiene un control eficiente donde garanticen que se asignen permisos conforme a las necesidades que el usuario requiera para realizar sus actividades, ya que solo se le crea el usuario en un sistema determinado sin aplicar controles que gestionen si la cuenta creada tenga permisos solo para realizar las actividades que estén a cargo en un área específica.

9.2.3 Gestión de los derechos de acceso con privilegios especiales.

De igual manera no se tiene aplicado este control de forma eficiente ya que no se encuentran definidas políticas de acceso con privilegios especiales, solo asignan privilegios según sus intereses, pero debido a la falta de documentación de accesos no se percatan si tienen accesos privilegiados algunos usuarios.

9.2.4 Gestión de información confidencial de autenticación de usuarios.

El departamento de TICS emite de manera verbal en las que menciona sobre la confidencialidad de las contraseñas para la autentificación de los usuarios dentro de la empresa, también da a conocer que el cambio de contraseña es importante después de que se le entregue una contraseña genérica que sea temporal.

Un problema detectado es que no el usuario no recibe capacitación o indicaciones sobre la creación de las contraseñas lo cual genera un riesgo en la seguridad de las mismas.

9.2.5 Revisión de los derechos de acceso de los usuarios.

Los derechos de acceso comunes o privilegiados de los usuarios no son revisados y documentados en los sistemas y aplicaciones, en consecuencia, un usuario normal podría tener accesos a derechos que solo las jefaturas o personal autorizado deban tenerlo, es importante que se lleve a cabo procedimientos para hacer revisiones periódicas.

9.2.6 Retirada o adaptación de los derechos de acceso.

Este control se da cuando existen cambios en los puestos de trabajo o algún miembro sujeto a la empresa finaliza su cargo o trabajo, pero no existe un proceso documentado para realizar la actividad y el cumplimiento de este apartado no es de manera eficiente ya que existen inconvenientes en administrar las cuentas de usuario.

9.3 Responsabilidades del usuario.

9.3.1 Uso de información confidencial para la autenticación.

El departamento de TICS emite al personal de la empresa la importancia del uso confidencial para la autentificación con varios parámetros (la no divulgación, que sean contraseñas seguras, fácil de recordar…) pero esto de igual forma no tiene un cumplimiento eficiente ya que solo son mensajes informativos más no existe un control formalizado.

9.4 Control de acceso a sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información.

La información tanto de los sistemas y aplicaciones que la empresa maneja tienen restricciones de escritura y lectura en base a las actividades que se necesita desarrollar son asignadas a los usuarios, la información se oculta para los usuarios comunes mediante la administración en los sistemas.

9.4.2 Procedimientos seguros de inicio de sesión.

Para el inicio de sesión en los sistemas y aplicaciones existentes se establecen mediante su nombre inicial seguido de un punto y su apellido paterno, los sistemas tienen advertencias que sirven de ayuda en el inicio de sesión, una vez que el

sistema haya validado las credenciales ingresa al sistema caso contrario tienen un bloqueo y para esos casos el usuario debe dirigirse al departamento de sistemas para su desbloqueo.

9.4.3 Gestión de contraseñas de usuario.

Los sistemas y aplicaciones no son manejados mediante contraseñas establecidas en las políticas y estándares corporativos ya que no se ha generado estos controles, pero se ha informado a los usuarios por el departamento de TICS que coloquen una contraseña segura y fácil de recordar.

9.4.4 Uso de herramientas de administración de sistemas.

No existe una persona encargada para controlar los servicios privilegiados, el personal que requiera que en los sistemas tengan privilegios de administración, se les da acceso bajo condiciones y según las actividades que tenga que cumplir, la segregación de tareas en el departamento de TICS es complicada debido a que no existe el personal suficiente para ello, lo cual no les permite tener a un integrante encargado a disposición de llevar a cabo la gestión de accesos privilegiados.

9.4.5 Control de acceso al código fuente de los programas

Algunos sistemas eran desarrollados por los integrantes del departamento de TICS, pero no se seguía una normativa ya que ellos lo realizaban a su manera ya sea con controlador de versiones o sin ella y solo ellos tenían acceso al código por tanto la modificación, compilación y publicación del código fuente dependía solo de ellos.

Fig. 14: Cumplimiento controles de acceso.

Fuente: Elaborado por el investigador.

Interpretación: En la gráfica se observa que el control relacionado con los controles de acceso no tiene un cumplimiento aceptable ya que están por debajo del 50% del cumplimiento dando a conocer que se tienen que hacer mejoras de todos los controles asociados a este anexo.

Anexo 10: Cifrado.

10.1 Política de uso de controles criptográficos: el departamento de TICS no tiene establecido políticas para el uso de controles criptográficos.

10.2 Gestión de claves: el departamento de TICS es el encargado de la gestión de claves, y se llevan a cabo actividades como generación de diferentes claves para sistemas y aplicaciones, no aplicación de claves débiles, backups de respaldo entre otros…, debido a estos parámetros se tiene un cumplimiento de 50%, en cuanto a los objetivos de control.

Recomendación: Este documento contiene las normas de seguridad criptográfica aplicables a los sistemas de información que ofrecen apoyo a procedimientos académicos y de gestión electrónicos de la Universitat Oberta de Catalunya (UOC) [27].

Anexo 11: Seguridad física y ambiental.

11.1 Áreas seguras.

11.1.1 Perímetro de seguridad física.

La empresa Megaprofer S.A se encuentra ubicada en Huachi Belén en las afueras del centro de la cuidad de Ambato, donde no existen edificios anexados a la institución, pero siendo una zona poblada, cuentan con cámaras de seguridad para monitoreo dentro de la entidad y contando con los servicios de guardianía tanto en el día como en la noche para salvaguardar los bienes de la empresa.

El techo exterior, las paredes y el suelo son de construcción sólida, las puertas y ventanas tienen cerraduras y se encuentran en buen estado.

Se pudo evidenciar que no se tiene definidos perímetros de seguridad en oficinas, redes informáticas, archivos…, un factor a favor es que los procesos están divididos es decir que no son compartidos y los profesionales no pueden tener acceso fácil a los diferentes procesos sin que se percaten los pertenecientes a dicho departamento.

11.1.2 Controles físicos de entrada.

El control de acceso a la empresa es controlado por el guardia de seguridad para que no existan intrusos en la empresa, para el control del personal que labora en la institución se lo hace mediante una credencial que lo identifica y además de

manera obligatoria tienen que registrarse en el biométrico, mientras que para las personas que no son parte de la institución se verifica y retiene su cedula de identidad para su posible ingreso y se lleva a cabo un registro de visitas.

Ante una eventualidad de pérdida o daño de algún activo institucional externo por parte de quienes ingresan a la empresa, la guardianía es el encargado de notificar a las autoridades la situación siendo el responsable de las instalaciones externas de la institución.

Cuando alguien desea salir de la empresa el guardia se encarga de hacer una revisión física y a la vez registra ingresos y salidas de todo personal entrante y saliente de la organización.

La empresa realiza contantemente movimiento de material ferretero ya sea mercadería para bodega o despacho, para ello se lleva a cabo un registro de movimiento de material que mantiene conjuntamente el área de facturación electrónica como la guardianía, con ello se encarga de la verificación del movimiento y de su registro.

11.1.3 Seguridad de oficinas, despachos y recursos.

Los accesos de entrada y salida de las diferentes áreas existentes se controlan mediante cámaras de seguridad que son monitoreados por el departamento de TICS, por medio de ella se puede evitar posibles riesgos de la información, pero no toman énfasis los activos de información almacenados por parte de los usuarios.

11.1.4 Protección contra las amenazas externas y ambientales.

El departamento de Seguridad Física se ha encargado de lineamientos para la protección de las amenazas externas y ambientales como las siguientes:

La empresa Megaprofer cuenta con señaléticas informativas en zonas visibles, con el objetivo ante cualquier eventualidad el personal y terceras personas que se encuentren dentro de la institución tengan conocimiento a qué lugar dirigirse.

Tienen definidos vías de evacuación que para un mejor conocimiento de ellas se realizan simulacros, pero no periódicamente.

En caso de incendios se tiene implementado una alarma anti incendio que en caso de producirse dicha eventualidad, la alama es ejecutada e inmediatamente todos los que se encuentren en la institución deben retirarse inmediatamente de la zona de peligro y encaminare al punto de encuentro seguro.

Para las protecciones contra el fuego se tienen extintores ubicadas en zonas estratégicas de la empresa, en planta situadas en cada piso y al alcance de quien lo requiera en su momento.

Para la detección de intrusos se tiene un mecanismo de sensor de movimientos y a la vez se ayudan mediante cámaras de seguridad.

El área considerada como segura no son tan eficientes al momento de ocurrir una emergencia, ya que estos se encuentran en una zona que se circula por medio de paredes elevadas y está junto a la bodega, la zona segura se encuentra con material ferretero.

No existen facilidades de evacuación para personas con discapacidad, actualmente la empresa cuenta con tres pisos en la matriz y es dificultoso la evacuación en la ocurrencia de una emergencia.

11.1.5 El trabajo en áreas seguras.

Para contribuir con la seguridad de la información el departamento de TICS manifiesta que al final del día sean verifican las oficinas, las salas de informática y otros lugares donde se hayan realizado actividades, se tiene controles de acceso físico mediante cámaras para ingreso a los diferentes procesos, se prohíbe el uso de equipos fotográficos, video, audio u otro tipo de grabación en las áreas de trabajo.

11.1.6 Áreas de acceso público, carga y descarga.

Las entregas de carga y descarga se lo realizan por la puerta principal manteniendo control de acceso y limitado a personal autorizado, el horario para realizar esta actividad frecuentemente se lo realiza por las noches para que no afecte a las personas quienes ingresan y salen de la empresa.

El área de logística es el encargado de verificar que el material recibido coincide con un número de pedido autorizado, se registran los detalles de la recepción de

material según las políticas y procedimientos de adquisición, conjuntamente realizan el respectivo inventario de la mercadería.

11.2 Seguridad de los equipos.

11.2.1 Emplazamiento y protección de equipos.

Para los equipos relacionado con el área de TICS no se encuentran en áreas adecuadamente protegidas, un ejemplo son los servidores que anteriormente no contaba con una instalación en un cuarto independiente protegido contra la humedad y el calor, estuvo situada junto a los baños estando a visualización de quienes ingresaban a los servicios higiénicos, pero actualmente se tuvo conciencia de riesgo que presentaba al estar situados en esos lugares por tanto se construyó un cuarto independiente pero esta se encuentra interno al departamento de TICS y no se construyó de acuerdo a las normativas de seguridad de la información para el diseño y ubicación.

Tienen en cuenta los controles medioambientales para la protección de equipos y evitar daños, se tienen establecidos UPS contra la protección de energía eléctrica, en algunos procesos se manejan mediante zonas estratégicas de ubicación de equipos para que las pantallas no sean visualizadas fácilmente.

11.2.2 Instalaciones de suministro.

En los departamentos y otras áreas donde se encuentren con equipos electrónicos se cuenta con sistemas UPS que poseen una potencia adecuada para abarcar los equipos en un período de tiempo suficiente que necesita el empleado para resguardar sus actividades dado un acontecimiento de falla eléctrica.

Se pudo evidenciar que no existen un plan de mantenimiento para los UPS de acuerdo a las especificaciones de los fabricantes.

Un problema con respecto a los UPS es que como ya se mencionó que no se tiene un plan de mantenimiento en consecuencia existen fallos de que el sistema de UPS se encuentra defectuoso o que prácticamente dejo de funcionar, cabe mencionar que existen algunos ordenadores no cuentan con UPS lo cual estos inconvenientes afectan a la integridad física de los equipos ante una suscitación de corte de suministro eléctrico.

11.2.3 Seguridad del cableado.

Para el cableado de red se utiliza cable UTP categoría 5e y 6 con conectores RJ45 en los puntos donde se requieren conexión, para el cableado se encuentra distribuido por canaletas que lo separan del suministro eléctrico en los diferentes procesos y áreas requeridas, pero el estado de las canaletas en su totalidad no es eficiente ya que existen lugares donde las canaletas están en estado defectuoso mostrando los cables de datos y siendo visible por los usuarios, con la creación de un cuarto para los servidores se puede controlar el acceso al cableado.

11.2.4 Mantenimiento de los equipos.

Se tuvo conocimiento de que no existe un plan programado para realizar mantenimiento a los ordenadores, el mantenimiento se da cuando los ordenadores presentan alguna falla o por alguna razón no tienen un correcto funcionamiento y/o ha pasado un período largo donde no se ha realizado mantenimientos, el encargado de realizar los mantenimientos es el personal de TICS o un tercero cuando se suscite hacer un mantenimiento global de todos los ordenadores existentes.

Existen registros de los mantenimientos realizados a los equipos tecnológicos que se llevan a cabo físicamente en una carpeta situada en un estante del departamento de sistemas.

Un miembro del departamento de TICS manifestó que no se tiene un plan de mantenimiento debido a que no existe el personal suficiente en el área por múltiples ocupaciones que realizan interna y externamente para la empresa.

11.2.5 Salida de activos fuera de las dependencias de la empresa.

Todos los activos que dan valor a la empresa Megaprofer S.A están a cargo del departamento de TICS quienes son los que deben administrar de forma eficiente el control apropiado de los mismos.

El área de sistemas para la salida de activos fuera de la dependencia de la institución cuenta con actas de entrega / recepción la cual contienen firmas de autorización y entrega al responsable.

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.

No existe una política de uso aceptable que cubra los requisitos de seguridad y obligaciones con respecto al uso de dispositivos móviles o portátiles que se dan utilidad fuera de la organización, pero se toman en cuenta documentos donde el activo se le entrega con fines de mantener la información confidencial y mencionando que existen aspectos legales si la información es compartida.

11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.

El departamento de TICS es el encargado de administrar si se reasigna o elimina los equipos de almacenamiento tanto internos como externos que manejan las instalaciones de la empresa.

Para la reasignación de equipos de almacenamiento tanto interno como externo se tiene el siguiente proceso:

- Un miembro del área realiza una verificación al medio de almacenamiento con el objetivo de percibir el estado actual.
- Se realiza un respaldo de la información útil y se elimina toda información mediante un formateo y mantenimiento preventivo del activo informático.
- El equipo es reasignado de acuerdo a las características que posee.

Para la eliminación de equipos de almacenamiento tanto interno como externo se tiene el siguiente proceso:

- Un miembro del área realiza una verificación al medio de almacenamiento con el objetivo de percibir su estado actual.
- Si el activo se encuentra funcional pero ya no otorga el correcto funcionamiento se le hace un respaldo de la información útil y luego se le ejecuta un borrado de la toda información.
- Si el activo ya ha cumplido con su vida útil se continua con el proceso de eliminación.

Todo el proceso mencionado para la reasignación y eliminación del activo informático son llevados a cabo con registros, pero no se realizan informes.

11.2.8 Equipo informático de usuario desatendido.

El proceso para que las PCS y portátiles que no estén en uso se lo hacen mediante un tiempo de 5 minutos dado ese intervalo la maquina es bloqueada con contraseña que sabe solo el propietario de ese ordenador, en cuanto a sistemas y otros dispositivos no cumplen con este control y no se tiene un seguimiento de las mismas.

11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

En este control solo se ha aplicado de manera informativa por parte del departamento de TICS, pero no con el uso de políticas que ayuden al cumplimiento de las mismas obteniendo inconvenientes de mal uso de activos de información, puesto de trabajo en desorden y con facilidad de visualización de la información que se maneja en casa área de trabajo.

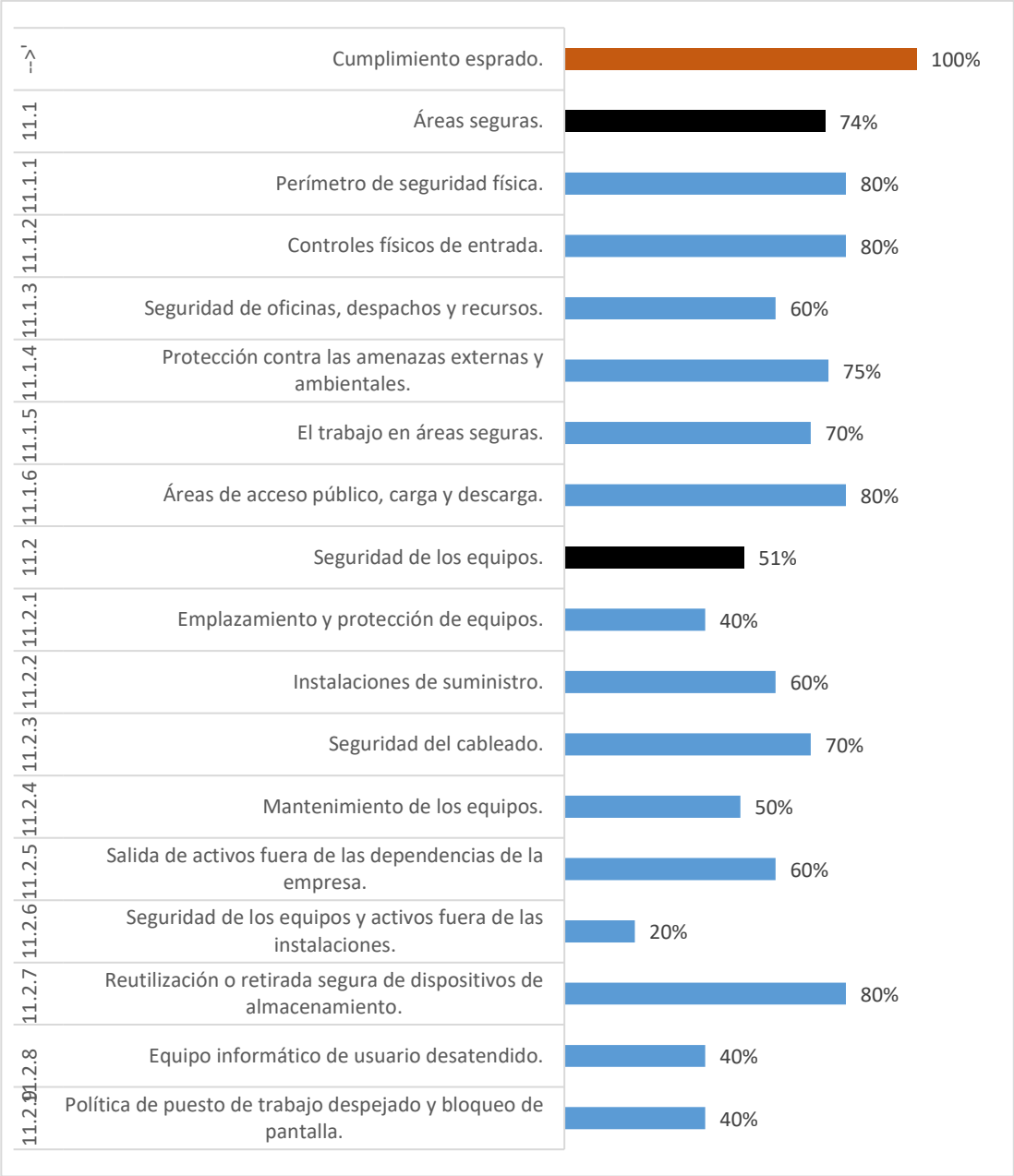

Fig. 15: Cumplimiento seguridad física y ambiental.

Fuente: Elaborado por el investigador.

Interpretación: En la gráfica anterior se puede apreciar el porcentaje de cumplimientos de los controles referentes a la seguridad física y ambiental, donde la ubicación y protección de los equipos son los tópicos donde el departamento de tecnología debe hacer mayor énfasis en cuanto a su cuidado y aplicación, en cuanto a la seguridad física se puede observar que existe un cumplimiento aceptable pero que se puede mejorar.

Los controles donde es necesario mejorar el índice de cumplimientos son en la seguridad en los equipos, políticas de uso de trabajo despejado, usuario desatendido y mantenimiento de los equipos. Éste último debido a la falta de un cronograma de planificaciones periódicas.

Anexo 12: Seguridad en la Operativa.

12.1 Responsabilidades y procedimientos de operación.

12.1.1 Documentación de procedimientos de operación.

Un problema que se tiene es que no existe documentación para los procesos relacionados con la seguridad de la información, únicamente se realizan socializaciones para dar a conocer a los empleados de determinados procesos la forma de llevarlos a cabo, por lo que la mayoría de veces genera dependencia para el departamento de sistemas debido la ocurrencia de imprevistos o sucesos inesperados.

12.1.2 Gestión de cambios.

Para la gestión de cambios en los sistemas operacionales deben ser solicitados al departamento de TICS, ellos son los que gestionan una autorización por parte de la gerencia con un previo estudio para que se dé el acto ya sea referente a hardware o software.

No cuentan con un registro documentado que conlleve los cambios efectuados, no se toma importancia la evaluación de riesgos asociados a los cambios que se puedan efectuar.

12.1.3 Gestión de capacidades.

La gestión de la capacidad para gestionar las tecnologías de la información se aplica mediante el seguimiento de uso de recursos y una previa planificación de mejoras cuando sea necesario para que así la capacidad de los sistemas de TICS cumpla los requisitos presentes y futuros de la organización con unos costes asumibles.

Las métricas relevantes para la gestión de capacidades incluyen (uso de la CPU, almacenamiento, capacidad de la red, demanda de RAM, la capacidad de aire acondicionado, espacio de rack…).

El problema detectado es que no se realizan registros de la gestión de capacidades, ya que no cuentan con el establecimiento de políticas eficientes que ayuden a que se aplique correctamente este control.

12.2 Protección contra código malicioso.

12.2.1 Controles contra el código malicioso.

Se basan en anuncios periódicos informativos y control por medio de antivirus que se aplica para contrarrestar los códigos maliciosos, pero esto no es un tanto seguro ya que los antivirus no cuentan con licenciamiento y una previa actualización de ellas para que brinde una alta capacidad en la seguridad.

No existen controles establecidos para que los usuarios que utilizan los ordenadores utilicen la herramienta anti malware al momento de introducir sus medios de almacenamiento.

Debido a que no se toman medidas adecuadas para identificar ni contrarrestar códigos maliciosos existe un alto riesgo en el robo de la información.

12.3 Copias de seguridad.

12.3.1 Copias de seguridad de la información.

El respaldo de la información si es llevada a cabo, pero no conjuntamente en base políticas para que se realicen backups de los datos relevantes que generen riesgo en la información.

El respaldo de la información se lo hace mediante una programación diaria, realizado por el Ingeniero Mario Pérez quien es el encargado de realizar la actividad y adicional la documentación.

Las copias de seguridad se almacenan en ubicaciones inadecuadas, generando riesgos de acceso indebido.

12.4 Registro de actividad y supervisión.

12.4.1 Registro y gestión de eventos de actividad.

Para este control no se tienen políticas establecidas o procedimientos para gestionar los eventos que ocurran en los sistemas de información, debido a ello ante la ocurrencia de problemas el área de TICS brinda soluciones en base a las herramientas que dispone, una de ellas es la revisión de los logs donde se pueden visualizar los errores que se hayan producido.

12.4.2 Protección de los registros de información.

No existen controles establecidos, ni se aplican procedimientos para salvaguardar la información, debido a esto siempre va a existir riesgo de que ocurran alteraciones o pérdida de la misma.

12.4.3 Registros de actividad del administrador y operador del sistema.

A causa del personal limitado y la ejecución de diferentes actividades que tienen que cubrir el departamento de TICS, no existen responsabilidades para el control administrado de usuarios comunes y privilegiados.

12.4.4 Sincronización de relojes.

El departamento de TICS ejecuta arquitecturas o procedimientos relativos a la sincronización del reloj, pero no mediante referencias como reloj automático, GPS, NTP …, por consecuencia no se tienen un cumplimiento eficiente.

12.5 Control del software en explotación.

12.5.1 Instalación del software en sistemas en producción.

El departamento de TICS por medio de procedimientos mas no políticas establecidas, realizan instalaciones de software en cualquier dispositivo dentro de la empresa, cabe recalcar que el software solo está permitido su instalación por el departamento de sistemas dado que no se manejan por medio de una autorización gerencial.

El software instalado es probado para su correcto funcionamiento en portátiles, servidores, base de datos…, se tiene en cuenta la instalación de software con soporte. Existen procedimientos para que el software sea instalado solo el personal de sistemas, ya que se rigen en los conocimientos que poseen.

12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Gestión de las vulnerabilidades técnicas.

Este control en la empresa es ineficiente ya que no tienen políticas ni procedimientos donde se realicen escaneos periódicos de vulnerabilidades técnicas, un factor principal en desventaja en este control es que no se tiene implementado gestión de riesgos ya que por medio de ella se puede establecer los controles adecuados para la seguridad de cualquier activo de información.

12.6.2 Restricciones en la instalación de software.

Todos los ordenadores tienen dos usuarios el administrador y el usuario normal, mediante esto se controla la no instalación de software que no sea autorizado, ya que se restringe por medio de una clave que solo el administrador conoce, además de ello el departamento de TICS es el encargado de socializar e indicar al personal que se prohíbe instalar software sin autorización del área.

Para que el usuario pueda instalar un software que en su ordenador debido a que tenga que trabajar con ello, se debe solicitar al departamento de TICS su instalación.

12.7 Consideraciones de las auditorías de los sistemas de información.

12.7.1 Controles de auditoría de los sistemas de información.

Este control no se cumple debido a que la empresa no mantiene una auditoria de seguridad de la información.

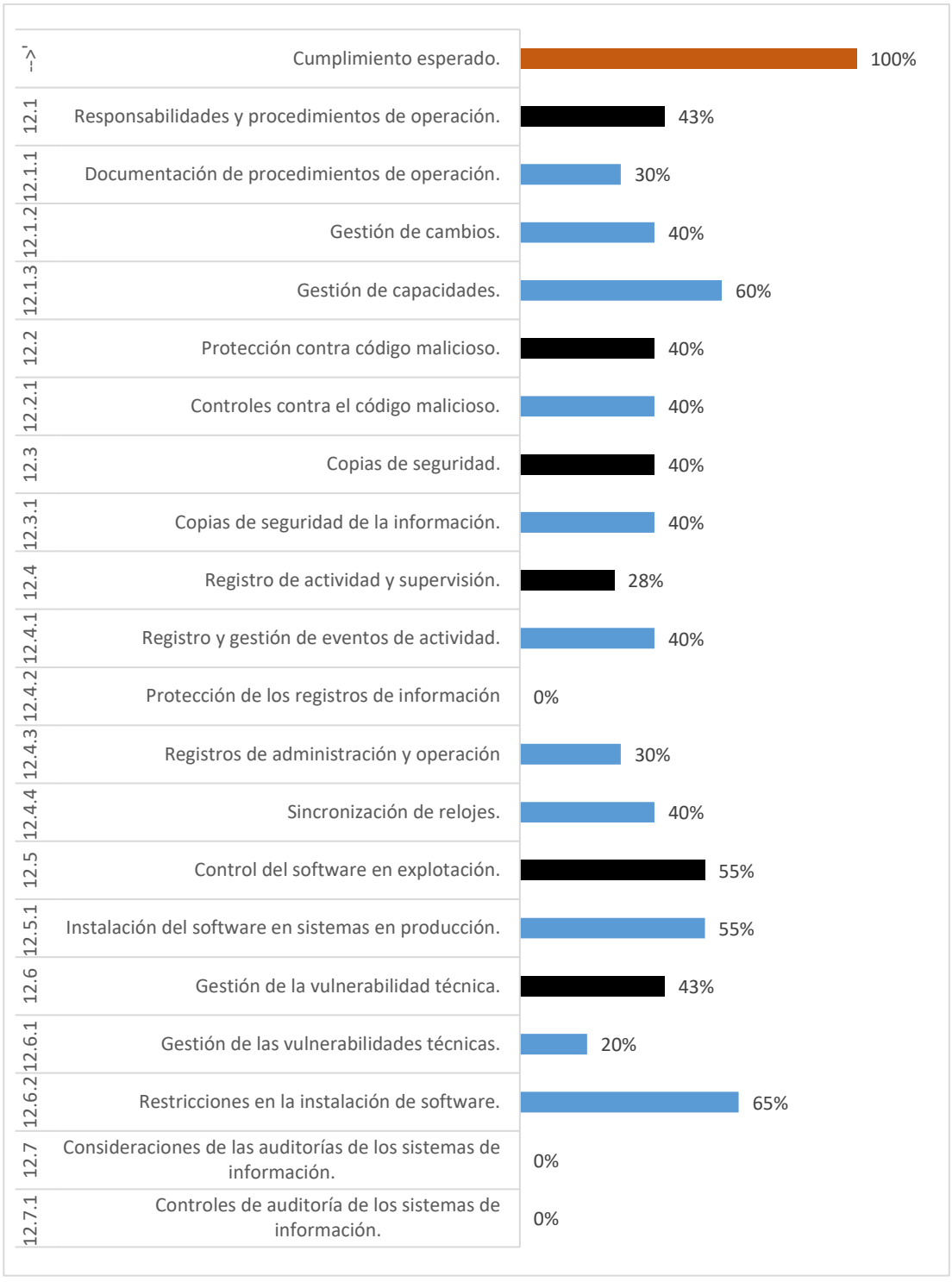

Fig. 16: Cumplimiento seguridad en la operativa.
Fuente: Elaborado por el investigador.

Interpretación: En la figura referente a la seguridad en la operativa, se detallan los porcentajes muy bajos de los controles que conforman el mismo, siendo el punto crítico el considerar auditorias en los sistemas de información, además de la protección de los registros de protección. En general el dominio en cuestión

tiene un nivel sumamente bajo en cuanto a cumplimiento por lo que se deberán tomar las medidas correctivas apropiadas. El único apartado que deja cierto grado de satisfacción son las restricciones para la instalación de software.

Anexo 13: Seguridad de las Telecomunicaciones.

13.1 Gestión de la seguridad en las redes.

13.1.1 Controles de red.

No llevan a cabo controles precisos en la red, siendo que está expuesto a sufrir alteraciones provocando robo de la información, existen uno cuantos controles, por ejemplo, autentificación para los todos los accesos a la red de la empresa.

13.1.2 Mecanismos de seguridad asociados a servicios en red.

Ente control es altamente bajo ya que no gestionan, clasifican y protegen los servicios de red de forma adecuada, tampoco existe un monitoreo, no mantienen una auditoria. Existen ciertos mecanismos como la autentificación en la red, revisiones de las configuraciones de la red, entre otros, pero que no son suficientes para un cumplimiento aceptable.

13.1.3 Segregación de redes.

No existe una política definida sobre la segmentación de red, pero su distribución está clasificada de acuerdo a los procesos de la empresa. No se lleva a cabo la segmentación de red lógica.

13.2 Intercambio de información con partes externas.

13.2.1 Políticas y procedimientos de intercambio de información.

Para este control no existe un establecimiento de políticas o procedimientos que ayuden en el cumplimiento del mismo, pero la mayor parte donde intercambian información son a los clientes que posee la empresa, para ello utilizan medios de transmisión autorizados por el departamento de TICS.

13.2.2 Acuerdos de intercambio.

Para este control no se ha establecido acuerdos de intercambio de la información, lo cual viene a ser un riesgo para quienes intercambian datos de la empresa, se emplea controles para el uso, protección y acceso a la información.

13.2.3 Mensajería electrónica.

El departamento de TICS es el encargado de la mensajería electrónica para toda la organización, lo administra mediante políticas que no son eficientes al no poseen una política de mensajería que cubra controles de intercambio de datos por comunicación de red, incluyendo correo electrónico y FTP / SFTP entre otras normativas que se deberían cumplir.

13.2.4 Acuerdos de confidencialidad y secreto.

La manipulación de la información debe ser confidencial entre las personas que intervengan en la manipulación de la información, a la vez estableciendo sanciones. Este control no es efectivo ya que no se tienen establecidos acuerdos de intercambio de la información.

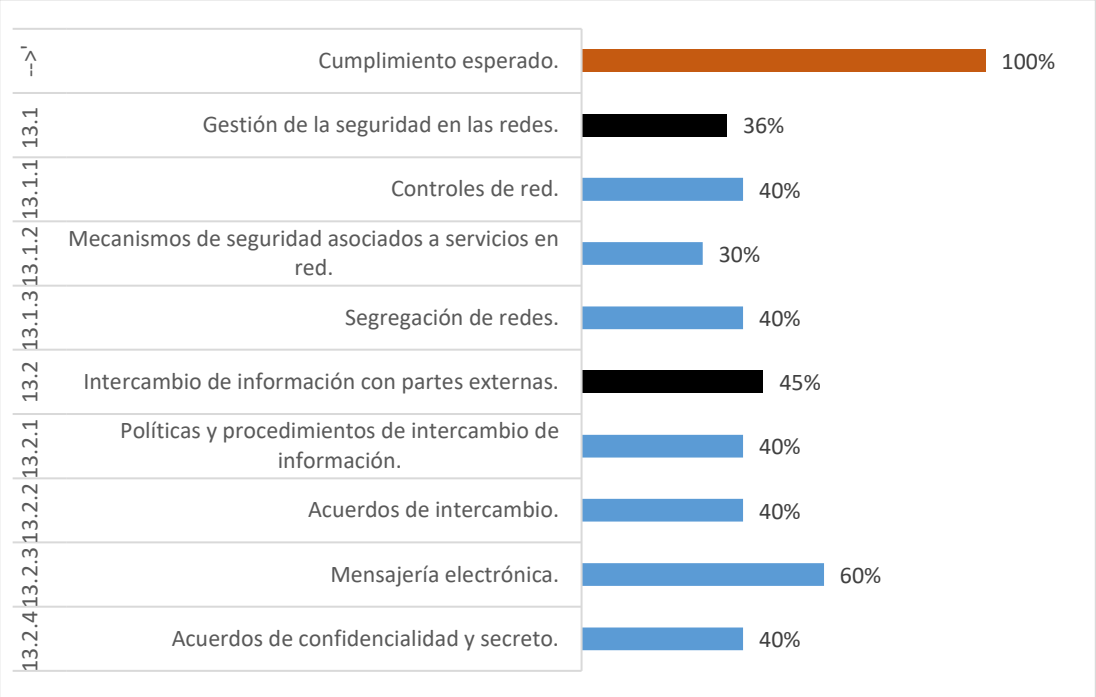

Fig. 17: Cumplimiento seguridad de las telecomunicaciones.
Fuente: Elaborado por el investigador.

Interpretación: Como se observa en la gráfica anterior, la mayoría de controles tiene un cumplimiento no aceptable con un porcentaje menor al 50%, excepto el

control relacionado a la mensajería electrónica cuyo índice de cumplimiento es 60% y está por encima de los demás controles por consecuente hay que tomar medidas correctivas en relación a todos estos controles.

Anexo 14: Adquisición, desarrollo y mantenimiento de los Sistemas de Información.

14.1 Requisitos de seguridad de los sistemas de información.

14.1.1 Análisis y especificación de los requisitos de seguridad.

Al adquirir un software se tienen en cuenta los requisitos para la seguridad de la información en base a las características y funcionalidades que posea el sistema, se establecen requisitos de seguridad, accesos al sistema, que se pueda mantener y mejorar a futuro.

14.3 Datos de prueba.

14.3.1 Protección de los datos utilizados en pruebas.

Al momento de ejecutar nuevos sistemas en producción, no se efectúan pruebas de seguridad en la red, tampoco se tiene un proceso de implementación, solo tienen en cuenta la funcionalidad del sistema y como se hace la utilización de recursos del software.

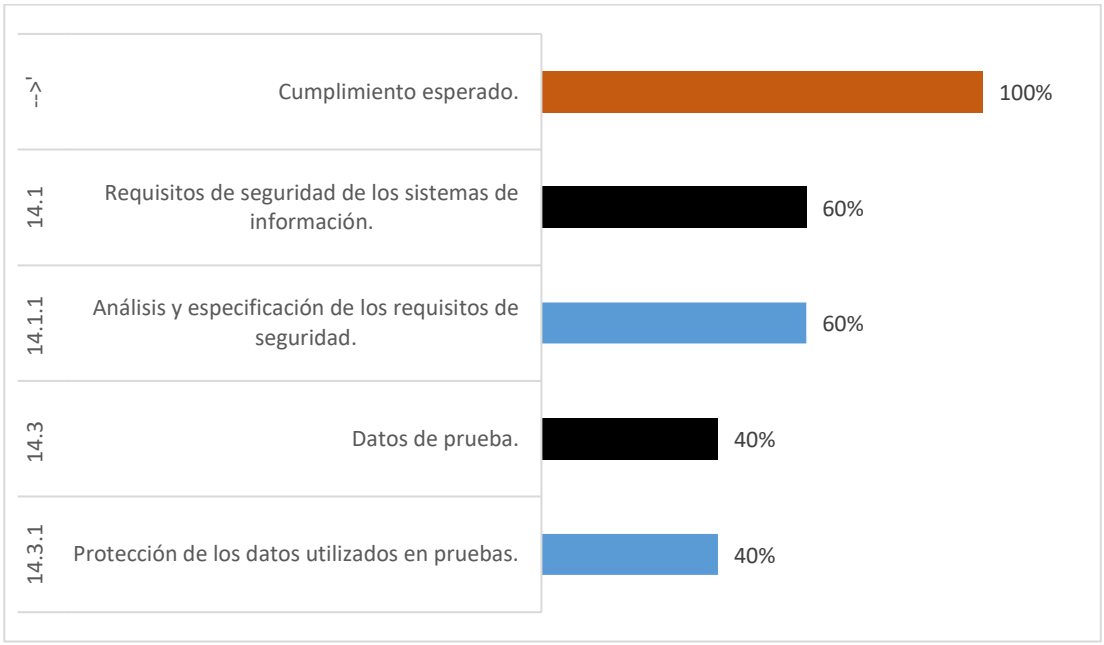

Fig. 18: Cumplimiento adquisición, desarrollo y mantenimiento de los sistemas de información.
Fuente: Elaborado por el investigador.

Interpretación: en la gráfica se puede observar que en la Adquisición, desarrollo y mantenimiento de los Sistemas de Información existe un control que no es aplicable (Desarrollo de sistemas informáticos), el control de "Requisitos de seguridad en los sistemas de información" tenemos un cumplimiento no satisfactorio con un porcentaje del 60% y el control "Datos de prueba" con un bajo porcentaje requiriendo que se apliquen medidas correctivas en los controles.

Anexo 15: Relaciones con Suministradores.

15.1 Seguridad de la información en las relaciones con suministradores

15.1.1 Política de seguridad de la información para suministradores.

No existen políticas acerca de los procesos relacionados con la gestión de relaciones con proveedores, pero se realizan controles de acceso a la información, limitaciones de acceso solo a la información que sea necesaria, estableciendo condiciones de seguridad.

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.

No se tiene un tratamiento de riesgo adecuado entre los proveedores, pero manejan cláusulas de confidencialidad generados por el departamento de sistemas y acordadas al momento de la adquisición de un producto o servicio.

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

El departamento de TICS quien se encarga de gestionar a los suministradores, por tal razón toma en cuenta aspectos relevantes como:

- Tener un control se seguridad sobre los proveedores gestionados.
- Veracidad de confianza en los proveedores.
- Rastrean el origen de los proveedores
- Toman en cuenta el control de seguridad de sus propios productos o servicios.

15.2 Gestión de la prestación del servicio por suministradores.

15.2.1 Supervisión y revisión de los servicios prestados por terceros.

Un integrante de área de sistemas es quien controla el servicio prestado por terceros, a fin de realizar monitoreos y revisiones de los mismos, también al proveedor terciario se le da a conocer cláusulas de penalización en cuanto al riesgo de la información, establecen reuniones para hacer revisiones del servicio con la finalidad de que el trabajo sea eficiente.

Un problema detectado es que no se generan informes al momento de culminación del servicio, no toman en cuenta los riesgos que se pueden originar y esto es debido a que no se tiene implantado una gestión de riesgos.

15.2.2 Gestión de cambios en los servicios prestados por terceros.

Para le gestión de cambios en los servicios prestados por terceros, se tiene en cuenta la confidencialidad de la información con el objetivo de que no ocurran riesgos en los activos de información.

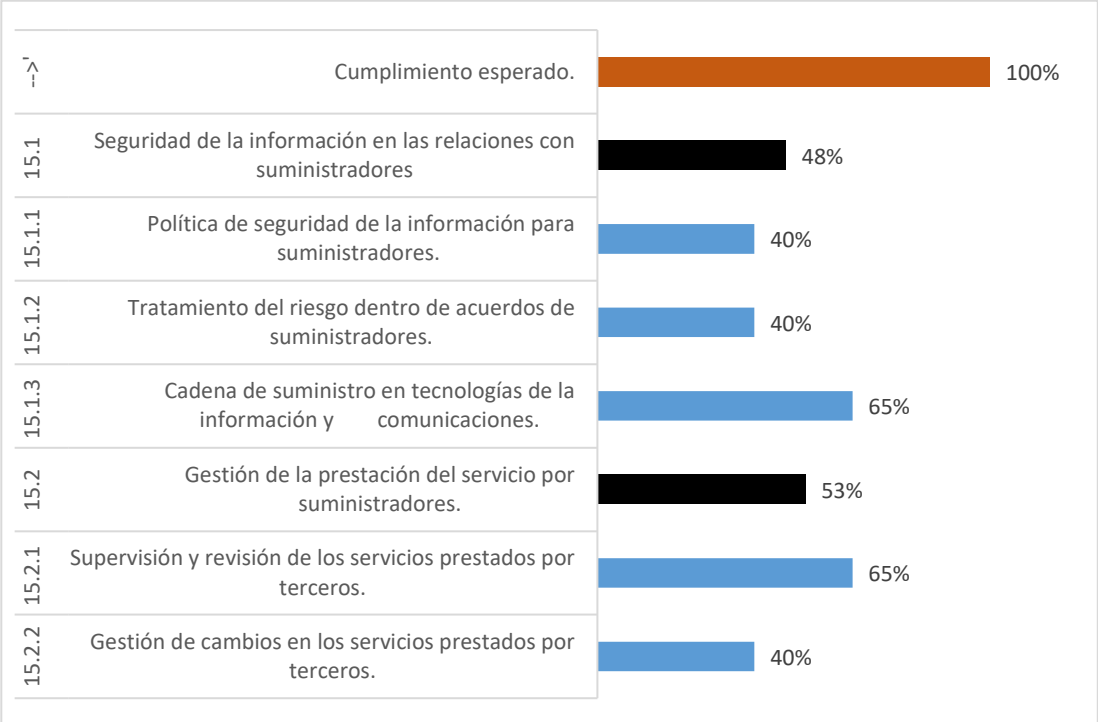

Fig. 19: Cumplimiento relaciones con suministradores.
Fuente: Elaborado por el investigador.

Interpretación: La gráfica anterior plasma la relación con suministradores, en promedio los controles que conforman el dominio "Seguridad de la información en las relaciones con los suministradores" tienen un porcentaje de cumplimiento por debajo del 50% y un cumplimiento medio en la "Gestión de la prestación del

servicio por suministradores" lo cual requiere que la aplicabilidad sea mejorada de todos los controles.

Anexo 16: Gestión de Incidentes en Seguridad de la Información.

16.1 Gestión de incidentes de seguridad de la información y mejoras.

16.1.1 Responsabilidades y procedimientos.

Para gestionar incidentes y mejoras de la seguridad de la información el departamento de TICS es el encargado de dar solución aquellos problemas que estén relacionados en el área de tecnología, pero no se tiene establecido procedimientos y responsables del área de sistemas para aplicar medidas de seguridad.

16.1.2 Notificación de los eventos de seguridad de la información.

El problema en este control es que no existe una política definida para la notificación de los eventos de seguridad de la información, únicamente se socializa por parte del departamento de TICS, exponen la importancia que tiene el reporte ante cualquier problema que se suscite relacionado con riesgo de información, ya sea en su lugar de trabajo o en los diferentes procesos que tiene la empresa.

16.1.3 Notificación de puntos débiles de la seguridad.

Debido al control anterior no se cuenta con políticas que ayuden en la notificación de la seguridad de la información, por tal motivo los empleados no tienen una obligación contractual para informar cualquier incidente y por tanto es difícil encontrar puntos débiles en la seguridad, el área de sistemas socializa compartir cualquier evento que ponga en riesgo la información.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.

Para la valoración de los eventos de seguridad, se socializa al personal que notifiquen incidentes sobre la seguridad de la información, posterior a ello se

realiza una evaluación dependiendo del tipo de incidente, para el soporte toman en cuenta al personal calificado para ejecutar una acción sobre los acontecimientos.

16.1.5 Respuesta a los incidentes de seguridad.

El departamento de TICS es el encargado de dar respuesta a los incidentes de seguridad que puedan ocurrir, mediante la comunicación del mismo se realizan actividades como:

- Verificación del incidente ocurrido.
- Intervención de los integrantes del área de sistemas con conocimientos apropiados para solventar el evento.
- Comunicación del evento a una autoridad superior Jefaturas o Gerencias.
- Solución al incidente aplicando métodos necesarios.

16.1.6 Aprendizaje de los incidentes de seguridad de la información.

Existen eventualidades en el área de sistemas donde si ha ocurrido incidentes en la seguridad de la información, para ello investigan a profundidad con el objetivo de poder evaluar el riesgo al cual haya sido expuesto los activos de información, a fin de estar preparados para que no vuelva a ocurrir el mismo incidente y así no estar vulnerables a ataques por los delincuentes informáticos.

En este control se encontró problemas, no se tienen registrados los incidentes ocurridos y pese a ello no concientizan sobre lo importante que es tener una gestión de riesgos o insistir en tomar capacitaciones relacionadas a la seguridad de los activos de información.

16.1.7 Recopilación de evidencias.

Para este control los integrantes quienes intervienen al momento de solventar los ataques informáticos, ejecutan sus propios conocimientos y mecanismos con ello verifican y obtienen evidencias sobre los incidentes que puedan ocurrir.

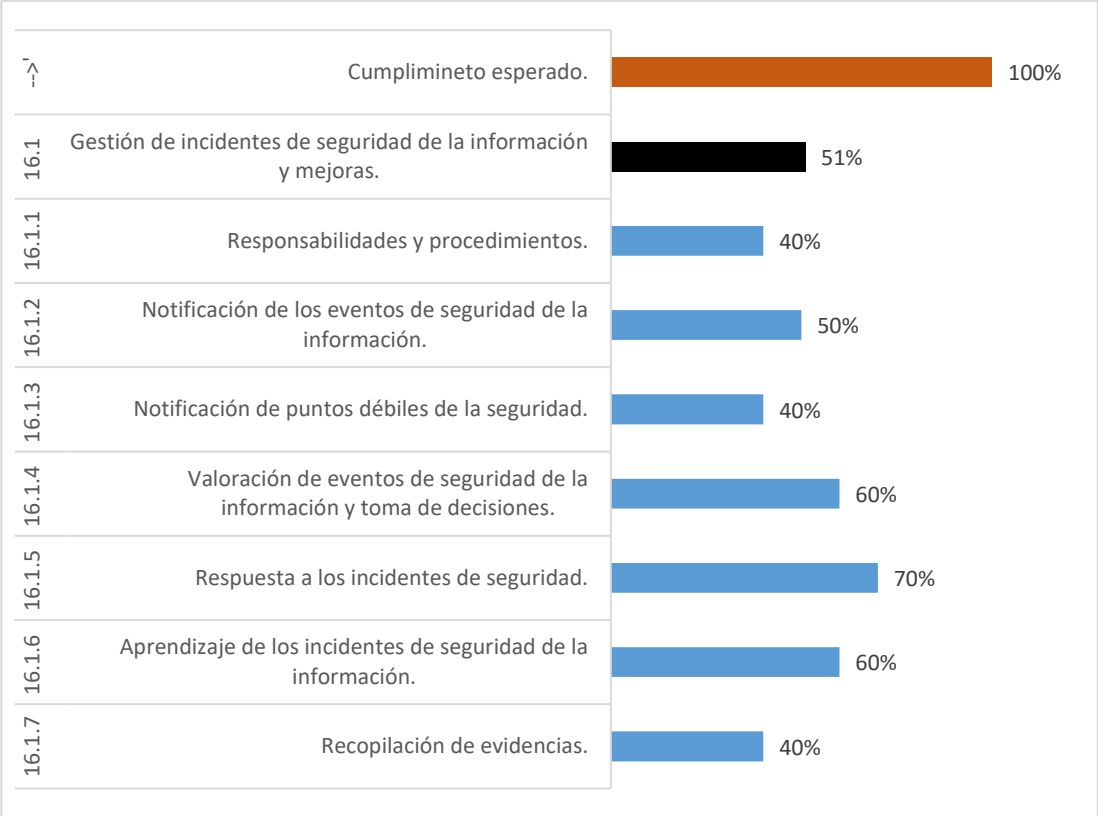

Fig. 20: Cumplimiento gestión de incidentes en la seguridad de la información.
Fuente: Elaborado por el investigador.

Interpretación: En la gráfica expuesta se puede apreciar los porcentajes de cumplimiento de los controles referentes a la Gestión de incidentes en la Seguridad de la Información, donde la respuesta a los incidentes de la seguridad de la información, valoración de eventos para la toma de decisiones y aprendizaje de los eventos ocurridos son los tópicos donde el departamento de tecnología hace mayor control en cuanto a los demás controles se necesitan aplicar medidas correctivas.

Anexo 17: Aspectos de Seguridad de la Información en la gestión de continuidad del negocio.

17.1 Continuidad de la seguridad de la información

17.1.1 Planificación de la continuidad de la seguridad de la información.

No existen planes de contingencia para ningún tipo eventos que pueda ocurrir, por tanto, este control no posee cumplimientos.

17.1.2 Implantación de la continuidad de la seguridad de la información.

Este control no tiene cumplimientos ya que no tienen planificado la continuidad de la seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

Este apartado también no es cumplible debido a que no existe una gestión para la continuidad de la seguridad de la información, por tanto, no se puede hacer verificación, revisión y pruebas.

17.2 Redundancias.

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

Existe la disponibilidad de instalación para el procesamiento de la información definiendo la capacidad del rendimiento, fiabilidad e implementando controles de seguridad de la información.

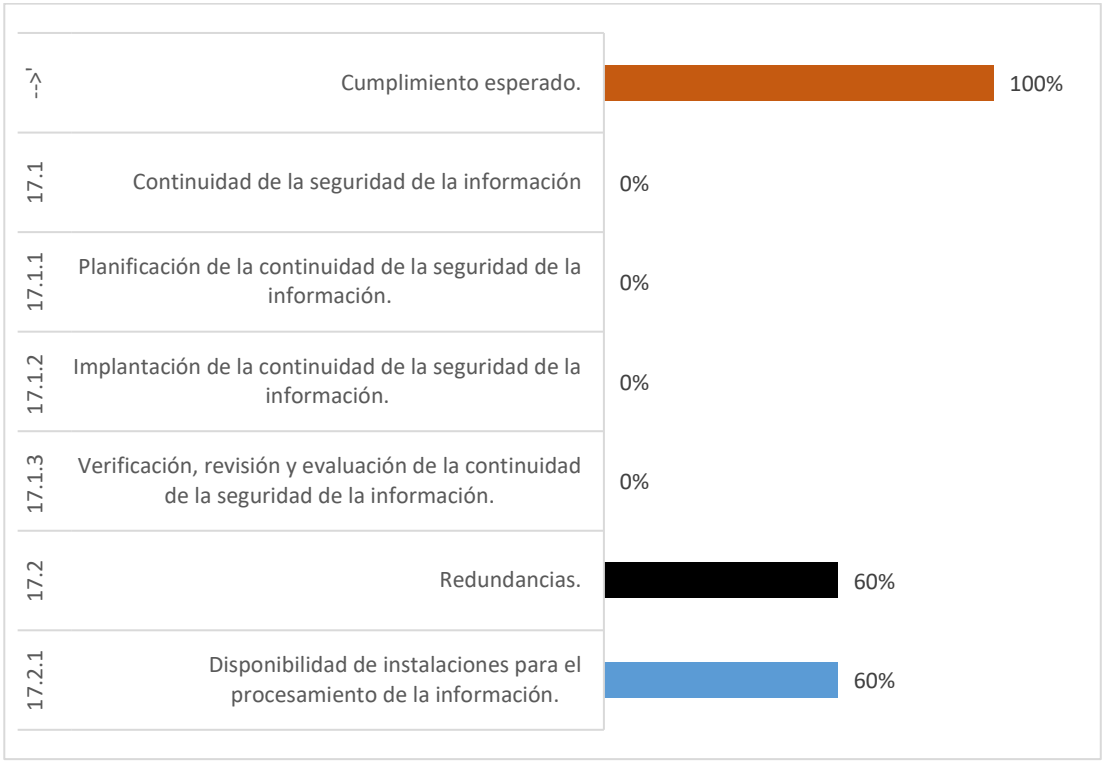

Fig. 21: Cumplimiento aspectos de seguridad de la información en la gestión de continuidad del negocio.

Fuente: Elaborado por el investigador.

Interpretación: En la gráfica anterior se observa que el control relacionado con la Aspectos de Seguridad de la Información en la gestión de continuidad del negocio se expone de forma crítica, obviamente es necesaria la aplicación de lineamientos para su funcionamiento óptimo y mejoras en el control que tiene un cumplimiento poco aceptable.

Anexo 18: Cumplimiento.

18.1 Cumplimiento de los requisitos legales y contractuales.

18.1.1 Identificación de la legislación aplicable.

La empresa no tiene políticas sobre el cumplimiento de requisitos legales como es la Ley Orgánica de Protección de Datos (LOPD), Reglamento General de Protección de Datos (GDPR)…, la protección de los datos personales de todo el personal sujeto a la empresa se lo realizar mediante reglamentos generados por el departamento de sistemas dando a conocer controles sobre cómo manejar sus datos personales.

18.1.2 Derechos de propiedad intelectual (DPI).

El uso de software está basado en los derechos de propiedad intelectual mediante procedimientos en la adquisición, el uso legal y aseguramiento la no violación de los derechos de autor.

18.1.3 Protección de los registros de la organización.

Mediante el departamento de TICS se protege los registros de la entidad, pero no se toma en cuenta requisitos legales. El área de sistemas es el encargado de evitar borrado, falsificaciones o accesos no autorizados.

18.1.4 Protección de datos y privacidad de la información personal.

El departamento es el responsable para la gestión de protección de datos y privacidad de la información personal, el área de sistemas socializa que la información de cada usuario debe ser procesada de manera segura en medios de almacenamiento donde existan controles de seguridad con el objetivo de mantener la confidencialidad e integridad, a la vez socializar con todo el personal sombre la

privacidad de sus datos personales e informarle que sus datos se encuentran de manera segura.

18.2 Revisiones de la seguridad de la información.

18.2.1 Revisión independiente de la seguridad de la información.

La seguridad de la información es revisada por terceros que son profesionales en la seguridad de la información, ellos realizan revisiones de las políticas o procedimientos existentes en la empresa, se basan en la documentación de los mismos, buscando la garantía de que el personal este en la obligación de acatar cada una de las normativas generadas.

El problema en este control es que no toman en cuenta la elaboración de la gestión de riesgos para detectar vulnerabilidades en los activos de información, en consecuencia, no se tienen implementadas políticas o procedimientos adecuados donde se puedan cumplir a cabalidad normativas.

18.2.2 Cumplimiento de las políticas y normas de seguridad.

El cumplimiento de políticas y nomas de seguridad es llevado a cabo por el departamento de TICS, quien conjuntamente con ayuda de los líderes de los diferentes procesos existentes están en la responsabilidad de socializar sobre la importancia de la seguridad de la información y que se ejecuten políticas y nomas que simplifiquen riesgos en los activos de información, pero no son llevados a cabo eficientemente.

18.2.3 Comprobación del cumplimiento técnico.

No existe una programación periódica para escaneos de vulnerabilidades en la red y pruebas de pentesting, pero si existe la ejecución de las mismas, estas actividades son ejecutadas por los integrantes del departamento de TICS quienes son seleccionados en base a sus conocimientos, el seleccionado establece un análisis previo a la obtención de resultados y establece prioridades para la toma de decisiones correctivas.

Un problema detectado es el tratamiento ante vulnerabilidades encontradas debido a no poseer una gestión de riesgos, la cual ayude a seleccionar el mejor mecanismo

para mitigar o eliminar vulnerabilidades, las medidas tomadas no son eficientes ni confiables.

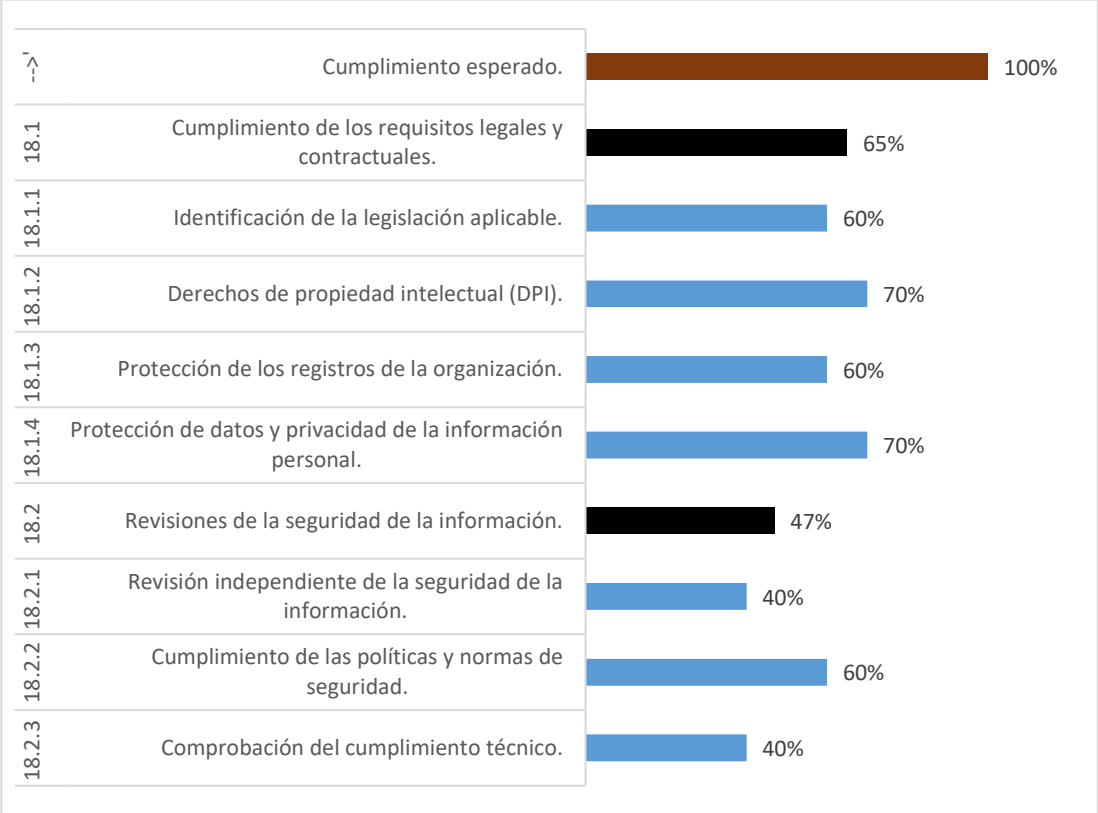

Fig. 22: Cumplimiento técnico.
Fuente: Elaborado por el investigador.

Interpretación: En la figura referente al anexo del Cumplimiento, se puede percibir que el control "Cumplimiento de los requisitos legales y contractuales" posee un mayor porcentaje de cumplimiento mientras que no se enfocan en realizar revisiones en la seguridad de la información.

4.5 Planteamiento de políticas en base a la norma ISO 27001

Mediante la implementación de la norma ISO 27001, se realizó un análisis de la seguridad de la información en base a los procedimientos planteados, como gestión de riesgos, aplicabilidad, controles, entre otros, dándonos a conocer un nivel bajo de la seguridad de la información que posee en los diferentes procesos tanto operativas como comerciales que se llevan cabo en la empresa Megaprofer S.A.

Dado que la seguridad de la información es importante en todos los procesos y áreas de la institución, se tiene que establecer políticas en base a la seguridad de la información que se encuentre dentro de los límites de la empresa, para minimizar vulnerabilidades que pongan en riesgo la información.

Establecimiento de políticas de Seguridad de la Información en base a los controles indagados de la norma ISO 27001, cubriendo necesidades como seguridad organizacional, lógica, física y legal en la entidad.

Política de Seguridad de la información

A partir de la implementación del Sistema de Gestión de Seguridad de la Información y como factor principal la gestión de riesgos, el personal de TICS se compromete a salvaguardar la información, detectando las vulnerabilidades en todos los procesos con la finalidad de proteger los activos de información contra amenazas que puedan existir. El área de sistemas establece estrategias basadas en las mejores prácticas y controles, el cumplimiento de los requisitos legales, gestión de incidentes y el compromiso de toda la empresa en general.

Políticas de seguridad para la Gestión de Activos

Objetivo: implantar responsabilidades para el respectivo uso y manejo los activos de información otorgados.

Descripción: mediante la generación de inventarios de los activos de información se aplican procedimientos como identificación, protección, proceso de gestión documental, designación de equipos y responsables para administrar los activos.

Responsable: departamento de TICS.

Aplicabilidad: departamento de TICS encargado de la seguridad de la información.

Aprobación: gerencia, TICS.

Directrices

- Actualización periódica del inventario y su revisión por las autoridades gerenciales.

- En cada proceso existente en la entidad, habrá un responsable de los activos de mayor relevancia y que a su vez deberá mantener un documento actualizado de los mismos para una mejor gestión.
- Cada sucursal de la organización debe tener a un integrante responsable quien realice la revisión del inventario de los activos.
- La responsabilidad y custodia de los activos, recaerá al funcionario a quien se le haga la entrega para que realice sus actividades en beneficio de la empresa.
- Mantener información detallada del inventario por parte del personal encargado y siendo evaluadas mediante los aspectos de confidencialidad, integridad y disponibilidad y a la vez presentar inconsistencias detectadas.
- Bajo ningún criterio los custodios de los activos, podrán realizar actividades que están prohibidas a ser ejecutadas.
- Para realizar el inventario se deben aplicar procedimientos como identificación, valoración y clasificación de los activos de información.
- Realizar acuerdos de confidencialidad en cuanto a la utilización de los activos, otorgados por la entidad para su beneficio.

Políticas de seguridad para Dispositivos Móviles.

Objetivo: garantizar que los dispositivos móviles fuera de la organización brinden seguridad en la información.

Descripción: fuera de las instalaciones de la empresa el uso de equipos como portátiles y móvil será restringido, autorizados por parte gerencia y en conjunto con el departamento de TICS para que no exista riesgo en la seguridad de la información.

Responsable: departamento de TICS.

Aplicabilidad: todo el personal de la empresa.

Aprobación: gerencia, TICS.

Directrices

Para el correcto uso de los activos de información en movimiento y con la finalidad de mantener la seguridad que es suministrada dentro de la empresa se establece los siguientes procedimientos:

- Se debe requerir usuario y contraseña para el acceso a los dispositivos móviles.
- El acceso a la red de la empresa deberá ser mediante túneles SSL o VPN por medio de dispositivos autorizados.
- En los dispositivos móviles que se hayan instalado un software debe tener su respectiva licencia y autorizado por autoridades.
- Mediante las herramientas que proporcione el departamento de TICS la información dentro de los dispositivos móviles debe ser cifrada y monitoreada.
- Emplear condiciones de seguridad y autorización para el acceso remoto hacia los dispositivos.
- La conexión debe ser en redes confiables que sean de carácter privado para evitar cualquier amenaza que puede existir en las redes públicas.
- No almacenar información de la empresa en los dispositivos móviles en caso de que este no pertenezca a la empresa.
- La responsabilidad del uso de los dispositivos asignados recaerá sobre empleados.

Políticas de seguridad para Recursos Humanos

Objetivo: garantizar que el personal que va a ser contratado cumpla con las políticas de seguridad de la información en la empresa.

Descripción: para la organización los recursos humanos vienen a ser uno de los activos más importantes debido a que por medio de ella se adquiere empleados que deben ser capaces de regirse a las políticas de la empresa requiriendo de su compromiso en la seguridad de la información.

Responsable: departamento de Talento Humano

Aplicabilidad: Talento Humano de la institución.

Aprobación: gerencia, TICS, Talento Humano.

Directrices

- Empleados, personal externo o cualquiera que tenga vinculación con la entidad debe hacer los trámites y gestiones necesarios para la declaración de confidencialidad y compromiso con la seguridad de la información.
- En el proceso de selección del personal TTHH debe confirmar la veracidad de la información mediante la revisión del perfil que se encuentra en las hojas de vida perteneciente al postulante al puesto solicitado antes de su integración al proceso.
- El personal ya sea externo, tercero o contratista que estén ligados a la empresa deben hacer los trámites y gestiones necesarios para la declaración de confidencialidad y compromiso con la seguridad de la información y será parte integral del contrato o un acuerdo en cooperación que se debe mantener junto a las hojas de vida que gestiona TTHH.
- En el contrato se establece el proceso infracciones disciplinarias.

Políticas de Seguridad para Control de Accesos.

Objetivo: establecimiento de controles adecuados para el acceso a la información evitando acceso no autorizado.

Descripción: para el control de acceso a la información se establecen en los sistemas, recursos tecnológicos, medios de acceso al internet entre otros, el control de los usuarios lo lleva a cabo el departamento de TICS como pueden ser creación de usuarios, roles y permisos necesarios para ejecutar sus actividades.

Responsable: departamento de TICS.

Aplicabilidad: personal del departamento de TICS.

Aprobación: gerencia, TICS.

Directrices

- Los sistemas de información que tiene la empresa deben estar integrados al SID (Sistema de Identificación Digital).

- Los usuarios a través de roles que se administran en el sistema con los privilegios otorgados a cada usuario de los diferentes procesos tendrán su respectivo acceso a la información correspondiente.
- Para el acceso físico o digital de la información se tendrá en cuenta la clasificación y el manejo de la información por procesos.

Políticas para Escritorio y Pantalla limpias.

Objetivo: reducir la exposición de la información en los puestos de trabajo evitando mantener activos de información sobre los escritorios y equipos de cómputo.

Descripción: controlar activos de información en los lugares de trabajo reduciendo riesgos de visualización, manipulación o perdida de la información.

Responsable: departamento de TICS.

Aplicabilidad: todo el personal de la organización.

Aprobación: gerencia, TICS.

Directrices

- Bloqueo de sesión del ordenador cuando esté en inactividad.
- Configurar el protector de pantallas en base a un tiempo predeterminado.
- Todo archivo de información que se lleve a cabo manejarlos mediante procedimientos de protección contra personal no autorizado.
- Fuera del horario de trabajo colocar los activos de información en los cajones con llaves.
- No tener accesos directos hacia los archivos de información en los escritorios de los ordenadores.
- Proteger puntos de recepción, impresoras, fotocopias que puedan afectar en la seguridad de la información.
- Retiro inmediato de información que se ha enviado a imprimir.

Políticas para la protección contra Código Malicioso.

Objetivo: defender a los ordenadores contra infecciones en programas que puedan contener códigos maliciosos evitando el riesgo en la operatividad de la empresa.

Descripción: prevenir infecciones en todos los ordenadores que manipulan los empelados evitando malicias como troyanos, gusanos entre otros virus que puedan afectar la confidencialidad, integridad o disponibilidad de la información.

Responsable: departamento de TICS.

Aplicabilidad: departamento de TICS encargado de la seguridad de la información.

Aprobación: gerencia, TICS.

Directrices

- Capacitación a todo el personal sobre los códigos maliciosos, así como el tratamiento de ellos.
- En programas, archivos recibidos, medios de almacenamiento… verificar que no exista presencia de virus.
- Revisión periódica de los sistemas de información verificando que los archivos no hayan sufrido pérdidas de integridad.
- Intercambio de información a través de archivos planos no permitidos.
- En los equipos de cómputo se prohíbe la compartición de carpetas.
- Prohibición de software no autorizado por el departamento de TICS.
- Actualizar los sistemas a la última versión para mejorar la seguridad de la información.
- Como medida preventiva instalar antispyware para examinación de ordenadores y medios informáticos como medida preventiva.

Políticas de seguridad para las Relaciones con los Proveedores.

Objetivo: revisar los servicios de contrato del personal externo con la finalidad de que cumplan las políticas de la seguridad de la información.

Descripción: Establecer mecanismos para el control de las relaciones con los proveedores de bienes o servicios, se debe garantizar el cumplimiento de las políticas de seguridad de la información mediante firmas de contrato, acuerdos o convenios.

Responsable: departamento de Talento Humano.

Aplicabilidad: proveedores, contratistas o personal externo.

Aprobación: gerencia, TICS, Talento Humano.

Directrices

- Mediante un procedimiento se deberá otorgar acceso a la información bajo los términos de gestión documental, procedimientos asociados y bajo deber de reserva.
- Realizar una evaluación del riesgo antes de permitir el acceso y/o entrega de los activos de información a un tercero.
- Definir de forma clara los contratos con acuerdos de niveles de servicio que deben ser contemplados como una de las especificaciones técnicas.
- Definir una persona responsable que se haga cargo de la supervisión del personal tercero, contratistas y personal externo que ejecuten actividades dentro de a la organización.
- El personal externo debe someterse a un estudio de confiabilidad, credibilidad y confianza para el acceso a la información.
- Para el compromiso de la seguridad de la información con los contratistas o terceros se debe firmar la declaración de confidencialidad y compromiso con los activos de información y un acuerdo para la revelación de la misma bajo deber de reserva.

Política de seguridad para la Gestión de Incidentes.

Objetivo: ofrecer una respuesta rápida a los incidentes de la seguridad informática y a todo el personal de a la organización.

Descripción: mediante procedimientos adecuados ante incidentes se pretende otorgar más atención e investigación de las eventualidades que puedan surgir velando por la prevención de la misma.

Responsable: departamento de TICS.

Aplicabilidad: departamento de TICS encargado de la seguridad informática y a todo el personal de la organización.

Aprobación: gerencia, TICS.

Directrices

- Los incidentes que ocurran deben ser registrados por el personal encargado de la seguridad informática para tener un tratamiento eficaz la gestión de incidentes.
- Los diferentes eventos en contra de la seguridad de la información deben ser manejados con una asesoría de un experto en el área.
- Las diferentes sucursales que posee la entidad deben reportar de manera obligatoria cualquier incidente que se genere para que el personal encargado de a la seguridad efectúe el respectivo análisis.
- Tener documentados todos los incidentes en general denominado atención a incidentes.

Políticas de seguridad para la Continuidad del Negocio.

Objetivo: determinar vulnerabilidades o amenazas que puedan ocasionar la suspensión de las actividades o procesos que afecten la operatividad de la organización.

Descripción: mediante procedimientos adecuados identificar el impacto de los incidentes que amenazan las actividades cotidianas que lleva en la empresa y respuestas de recuperación.

Responsable: departamento de TICS y Seguridad Física.

Aplicabilidad: departamento de TICS encargado de la seguridad de la información.

Aprobación: gerencia, TICS, Seguridad Física.

Directrices

- Realizar planes de contingencia frente a los incidentes que puedan ocurrir para garantizar la continuidad del negocio hasta que se restablezcan los servicios en la matriz.
- Evaluación de los riesgos ante incidentes para determinar el impacto en la continuidad de los procesos.
- Determinar controles preventivos en contra de las eventualidades de incidentes que se presenten.

- Generar un plan estratégico para el enfoque con la que se abordará la continuidad del negocio en la organización.

Política de seguridad para la Gestión de Contraseñas.

Objetivo: establecer contraseñas seguras para acceso a los sistemas de información que maneja la organización.

Descripción: gestiona miento de contraseñas seguras para la creación y acceso seguro a los sistemas de información que posee la empresa.

Responsable: departamento de TICS.

Aplicabilidad: departamento de TICS encargado de la seguridad de la información.

Aprobación: gerencia, TICS.

Directrices

- Requerir a todo el personal que se generen contraseñas de calidad.
- Otorgar contraseñas temporales para inicio por primera vez a los sistemas de información.
- Cambio de contraseñas en un período determinado.
- En los sistemas impedir el uso de contraseñas ya usadas anteriormente.
- Evitar la visualización de contraseñas al momento de inicio de sesiones.

Política de seguridad para la Clasificación de la Información.

Objetivo: clasificar la información que se generar en los diferentes procesos de la organización para un acceso eficaz al momento de requerir información.

Descripción: clasificación de la información mediante los procedimientos adecuados que ayuden a mantener la información por cada proceso existente en la organización y así tener una disponibilidad eficiente.

Responsable: todos los procesos.

Aplicabilidad: departamento de TICS y personal en general

Aprobación: gerencia, TICS.

Directrices

La clasificación de la información es vital para la disponibilidad de ello, por ese motivo se clasifica de la siguiente manera:

Ultrasecreta: aquella información a la realización de una actividad o planes que la alta dirección plantee en la empresa ya sea interna o externa, ya que este tipo de información puede estar relacionadas con otras empresas, convenios, acuerdos…, siendo afectada los intereses de la empresa.

Secreta: aquella información adecuada u oportuna de actividades o planes que maneje internamente o externamente la empresa, siendo afectados las relaciones con otras empresas, prestigio o poner en peligro la organización.

Reservada: aquella información que pone en manos el aumento de amenazas actuales o potenciales de la entidad, siendo perjudicial en los intereses o prestigio de la organización.

Confidencial: aquella información cuyo contenido solo le interesa a quien vaya dirigida, la afectación de esta puede ocasionar perjuicios a una sede o persona.

Interna: aquella información que manejan los empleados, la mala utilización de la misma como divulgación, destrucción, alteración …, podría resultar pérdidas importantes para la empresa.

Pública: aquella información entregada o que su publicación está basada sin restricciones siendo que esta no tenga ningún impacto negativo para para la organización.

Política de seguridad para la Seguridad Física.

Objetivo: resguardo del equipamiento físico de la institución, provocado interna o externamente por personas mal intencionadas o en el caso de existir desastres naturales afectando a la integridad de los mismos.

Descripción: protección de los activos que contienen información o que puedan ocasionar inconvenientes en la operatividad, mediante los procedimientos adecuados que ayuden a mantener la integridad en cada proceso.

Responsable: departamento de Seguridad Física y Sistemas.

Aplicabilidad: departamento de Seguridad Física.

Aprobación: gerencia, TICS, Seguridad Física.

Directrices

ÁREAS SEGURAS:

Tener a un personal encargado en el monitoreo de las condicione ambientales, como estas pueden ser corrientes de aire, humedad, iluminación, temperatura…, con la finalidad de garantizar las estaciones de trabajo y el equipamiento.

De acuerdo a la infraestructura de la entidad, en cada piso deberá existir herramientas auxiliares como extintores, botiquín, lámparas, alarmas de seguridad…, para proteger la integridad tanto de los equipos como de los funcionarios.

La seguridad afueras de la entidad, se llevará a cabo por el guardia de seguridad que integra Megaprofer S.A.

El guardia de seguridad es el responsable de salvaguardar los activos e instalaciones al interior de la institución, quien ingresara una hora antes de la jornada normal y verificara el estado de la infraestructura y sus recursos. En caso de que existan incidentes, el guardia tiene la obligación de repórtalo al jefe se Seguridad Física.

CONTROLES FÍSICOS DE INGRESO

Todo el personal que ingrese a la entidad, deberá ser identificado por medio de credenciales a los funcionarios y cedula de identidad a personas que no dormán parte de la empresa. Además, el personal que ejerce sus actividades en la entidad, deberá registrarse en el biométrico con el objetico de evitar el ingreso a terceras personas.

En las zonas de alto riesgo, solo el personal autorizado estará en derecho para el ingreso.

El ingreso a los servidores está prohibido para las personas que no estén autorizadas, dado algún requerimiento para que el cuarto de servidores reciba visitas, únicamente los integrantes del departamento de TICS tienen la custodia de aceptar o denegar la petición.

En la bodega donde se encuentra la mercadería, solo se permite el acceso al personal que cumpla con los requisitos de autorización y utilización de cashaco de seguridad.

SEGURIDAD EN LOS EQUIPOS

Literalmente se prohíbe la manipulación física de los activos que posee la entidad, los únicos que tienen permiso para dicha acción, son los integrantes del departamento de sistemas.

El data center contiene uno de los activos de mayor relevancia (SERVIDORES), de acuerdo a los requisitos para su ubicación, deben estar situadas en una zona aislada y segura, fuera de oficinas y departamentos, para evitar manipulación de usuarios no deseados o peligros ambientales.

MANTENIMIENTO DE EQUIPOS

Periódicamente se llevará a cabo el mantenimiento preventivo y correctivo de todos los equipos, con la finalidad de prevenir fallos y problemas que pongan en peligro la continuidad operacional.

Para los daños o fallos que presenten los equipos, el departamento de TICS esta en la obligación da dar solución en un lapso de tiempo mínimo, para asegurar la continuidad de las actividades funcionarias.

Los funcionarios están restringidos para intervenir de manera lógica o física en los equipos, ellos tienen la obligación de realizar el respectivo reporte al departamento de sistemas para la solución inmediata.

INSTALACIONES DE SUMINISTRO

Para las instalaciones de equipos en general, se tomará en cuenta los perímetros de seguridad, a fin de proteger instalaciones como eléctrico, telefónico, cableado entre otros.

Los tipos de cableados estarán aislados unos entre otros, es decir que el cableado de red estará separado físicamente del cableado telefónico y/o corriente eléctrica, a fin de evitar interferencias.

Todos los equipos deberán estar situados donde exista una correcta instalación de energía eléctrica, la cual contenga un UPS para garantizar la integridad del equipo y a la vez la información que este almacenada.

SEGURIDAD EN LA ELIMINACIÓN O REUTILIZACIÓN DE EQUIPOS

Cuando un equipo haya cumplido con su vida útil, el departamento de TICS es el encargado de realizar un informe dirigido a la gerencia, y continuar a la eliminación del activo.

Si el equipo dado la revisión por un integrante del área de sistemas, tiene el caso que aún puede agregar valor en alguna otra actividad, se procede al formateo y reasignación del mismo.

En el caso de que se apruebe el informe de eliminación de equipos, se procederá al envió hacia las bodegas a cargo de personal de limpieza. Posterior, se efectúa el envío hacia una entidad recicladora.

SEGURIDAD DE LOS EQUIPOS HACIA FUERA DE LAS INSTALACIONES

El departamento de TICS es el encargado de todo equipamiento saliente de la institución, debido a ello deben mantener un informe detallado del estado y la información que almacena en activo.

Si el equipamiento presenta inconvenientes fuera de las instalaciones, el departamento de sistemas está en la obligación de dar una solución adecuada. En el caso de que el problema sea grave se deberá tener asistencia personal de un integrante del área tecnológica.

SANCIONES POR INCUMPLIMIENTO DE POLÍTICAS PLANTEADAS

Objetivo: prevenir toda acción que pongan en riesgo la preservación de la confidencialidad, disponibilidad e integridad de la información, por incumplimiento de las políticas establecidas.

Descripción: aplicación de sanciones por incumplimiento de obligaciones que se llevan a cabo en la organización, con la finalidad de inhibir o disuadir acciones futuras. Tendrá como inicio la notificación y terminará con sancionas severas, de acuerdo al daño que se trata de eludir.

Responsable: departamento de TICS.

Aplicabilidad: toda persona que tenga vínculo con la empresa.

Aprobación: jefe del departamento de TICS.

Vigencia: estas sanciones internas comenzarán a regir desde la aplicación de la norma ISO 27001, actividad en que es aprobado por la alta Gerencia de la empresa privada Megaprofer S.A.

Conocimiento y difusión: la entidad con la ayuda del personal capacitado, dará a conocer y difundirá las sanciones internas al acto de incumplimiento, a todo el personal en general.

ITEMS. -

Las sanciones por incumplimiento y/o divulgación de la información confidencial sea de forma oral, escrita o gráfica, de cualquier fuente de información, será aplicada una sanción dependiendo de la gravedad del asunto, la cual se describen a continuación:

A) El incumplimiento de las políticas de carácter leve, tendrá como un aviso de forma escrita, con la finalidad de notificarle que ha cometido un acto no deseado y estará sujeto a amonestaciones, suspensión de empleo y sueldo de 5 días laborables.
B) En el caso de presentar un incumplimiento grave o recurrencia de incumplimientos leves, se le notificará por escrito y se dará aviso a las altas gerencias, dado el respectivo conocimiento a las autoridades, se inhabilitarán asensos en área de trabajo, así como suspensión de empleo y sueldo hasta un lapso de 6 meses.
C) En el caso de presentar un incumplimiento muy grave, tendrá como consecuencia el despido inmediato, demanda ante la ley bajo los requerimientos de la empresa que se detallan a continuación:
    - La pena privativa de libertad de un año dada a la persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio [27].

- La pena privativa de libertad de uno a tres años dada a la persona que ocasione la alteración, manipulación, modificación de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de comunicación [27].
- La pena privativa de libertad de uno a dos años dada a la persona que provoque la inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes [27].
- La pena privativa de libertad de uno a tres años dada a la persona que revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, ¡telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas [27].
- La pena privativa de libertad de un año dada a la persona que provoque la modificación del sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder [27].
- La pena privativa de libertad de uno a dos años dada a la persona que ocasione la alteración, manipulación o modificación del funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero [27].
- La pena privativa de libertad de uno a dos años dada a la persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen [27].
- La pena privativa de libertad de un año dada a la persona que realice la intercepción, escucha, desviación, grabación u observación, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema

informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible [27].

4.6 Socialización de las políticas propuestas

Se analizan las políticas planteadas para los diferentes escenarios de la empresa privada Megaprofer S.A, para ello se realiza la evaluación del nivel grado de confidencialidad, disponibilidad e integridad que tuvo en la implementación del Sistema de Gestión de Seguridad de información, presentada en la sección 4.7 Resultados de la aplicación SGSI basado en la norma ISO 27001:2013.

4.7 Resultados de la aplicación del plan de seguridad informática

Para la evaluación del impacto al implementar el plan de seguridad informática basado en la norma ISO 27001:2013, se hizo el uso de una encuesta en el departamento de sistemas de la empresa privada Megaprofer S.A. En la aplicación de cada una de las etapas de la norma, se llega a la evaluación de los tres pilares principales confidencialidad, integridad y disponibilidad de la información.

Con la ayuda de la recolección de la información, que se planteó en el capítulo 3, se hace uso de la encuesta Anexo C, antes de la aplicación del plan de seguridad informática, con la finalidad de conocer la situación anterior de la organización presentados en la sección 4.1.1 Situación actual de la empresa y 4.3 conclusiones y recomendaciones. Posteriormente, se realiza otra encuesta Anexo D, a partir de la aplicación de la norma ISO 27001. Para conocer la situación actual con el uso del SGSI basado en la norma.

El presente tema de investigación hace uso del paradigma Crítico-Positivo, debido al diagnóstico y el análisis de a la situación actual de la empresa. A partir de ello se plantea una solución alternativa para la seguridad de los activos que posee la entidad.

Población y Muestra

Se toma como referencia la población y muestra detallado en el capítulo 3, sección 3.3, donde se da a conocer lo ítems mencionados.

Los resultados obtenidos se detallan a continuación:

Número de encuestados N =4

Disponibilidad

Preguntas disponibilidad PD = 9 Numero encuestados N = 4 Total votos = 36

Integridad

Preguntas integridad PD = 9 Numero encuestados N = 4 Total votos = 36

Confidencialidad

Preguntas confidencialidad PD = 7 Numero encuestados N = 4 Total votos = 28

Tabla 26:Valores numéricas de las encuestas.
Fuente: Elaborado por el investigador.

Indicador	Pregunta	Antes			#Encuestados
		Si	No	Parcial	
Disponibilidad	P1	3	0	1	4
	P3	3	0	1	
	P7	2	1	1	
	P8	4	0	0	
	P11	3	0	1	
	P12	3	0	1	
	P13	4	0	0	
	P14	3	0	1	
	P15	3	1	0	
Total, disponibilidad		28	2	6	36
	P4	4	0	0	
	P5	3	1	0	
	P6	2	1	1	

Integridad	P7	2	1	1	4
	P9	4	0	0	
	P11	3	0	1	
	P12	3	0	1	
	P14	3	0	1	
	P15	3	0	1	
Total, integridad		27	3	6	36
Confidencialidad	P2	4	0	0	4
	P7	2	1	1	
	P10	2	1	1	
	P12	3	0	1	
	P13	4	0	0	
	P14	3	0	1	
	P15	3	0	1	
Total, confidencialidad		21	2	5	28

Se presenta la siguiente tabla, en valores porcentuales basados en la encuesta presentada en la tabla 26.

Tabla 27: Valores porcentuales de las encuestas.
Fuente: Elaborado por el investigador.

Indicador / Pregunta		Antes			%
		Si	No	Parcial	
	P1	75	0	25	100
	P3	75	0	25	100
	P7	50	25	25	100
	P8	100	0	0	100

Disponibilidad	P11	75	0	25	100
	P12	75	0	25	100
	P13	100	0	0	100
	P14	75	0	25	100
	P15	75	25	0	100
Total, disponibilidad		77,8	5,6	16,6	100
Integridad	P4	100	0	0	100
	P5	75	25	0	100
	P6	50	25	25	100
	P7	50	25	25	100
	P9	100	0	0	100
	P11	75	0	25	100
	P12	75	0	25	100
	P14	75	0	25	100
	P15	75	0	25	100
Total, integridad		75	8,3	16,7	100
Confidencialidad	P2	100	0	0	100
	P7	50	25	25	100
	P10	50	25	25	100
	P12	75	0	25	100
	P13	100	0	0	100
	P14	75	0	25	100
	P15	75	0	25	100
Total, confidencialidad		75	7,14	17,86	100
TOTAL		**75,9**	**7,05**	**17,05**	**100**

Análisis de los resultados en base a los indicadores Disponibilidad, Integridad y Confidencialidad

DISPONIBILIDAD:

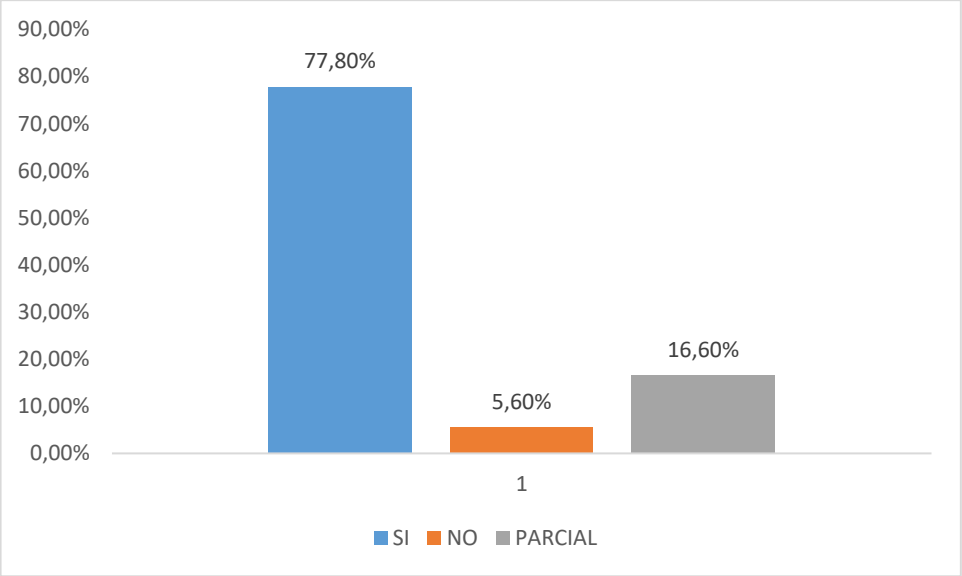

Fig. 23: Resultados indicador disponibilidad.
Fuente: Elaborado por investigador.

Interpretación: en base al indicador de disponibilidad, se puede visualizar que existe un alto porcentaje de incremento. Ya que el 77,80% de los encuestados afirma que la información está disponible en todo momento.

INTEGRIDAD:

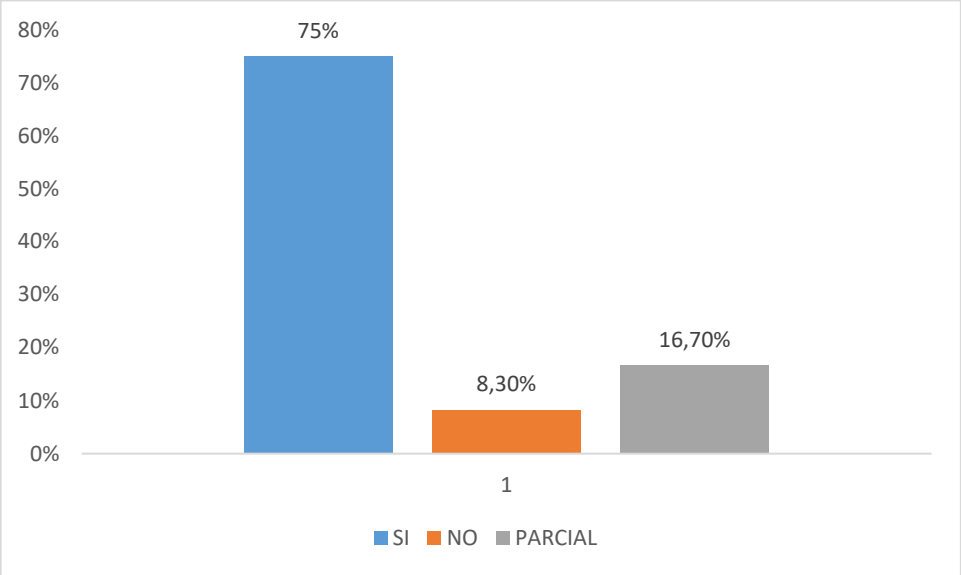

Fig. 24: Resultados indicador integridad.
Fuente: Elaborado por investigador.

Interpretación: de acuerdo al indicador de integridad, existe un incremento en la seguridad de la información, con el 75% en mantener la gestión adecuada para que los activos no sean manipulados.

CONFIDENCIALIDAD:

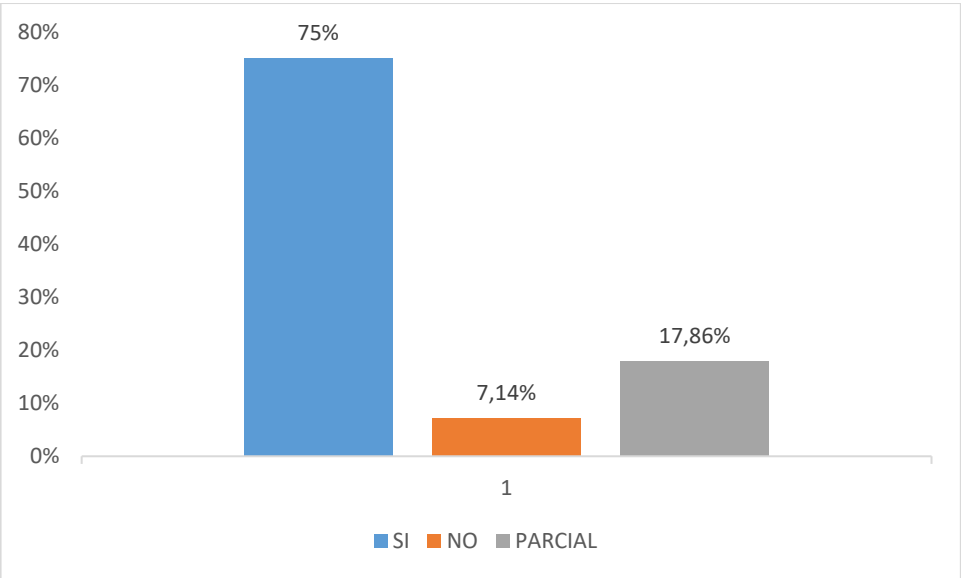

Fig. 25: Resultados indicador confidencialidad.
Fuente: Elaborado por investigador.

Interpretación: en la figura expuesta, el indicador de confidencialidad también forma parte de un incremento satisfactorio, El 75% afirma que los activos de información se dirigen solo hacia las personas a quien vayan dirigidas. A la vez que no existe salida de información que sea perjudicial para la organización.

Con la visualización de los resultados obtenidos, mediante la encuesta que se presenta en las tablas. Se puede observar que la implantación del SGSI en base a la norma ISO 27001, ha tenido una favorable gestión de mejora. Para que el Sistema de Gestión de Seguridad de la Información, no quede en términos de implementación, se plantea un procedimiento para el monitoreo y revisión del SGSI.

4.8 Procedimiento para el monitoreo y revisión del SGSI.

Se debe llevar un monitoreo y revisión del plan de seguridad informática basado en la norma internacional ISO 27001 expuesta, esto debe ser en base a una programación periódica que garantice en todo momento los tres aspectos importantes de la norma las cuales son confidencialidad, integridad y disponibilidad de los activos de información.

La empresa privada Megaprofer S.A está en su derecho de implementar este procedimiento para mejorar constantemente la eficiencia y productividad en cuanto a la seguridad de la información.

Para la monitorización y revisiones se establece un tiempo acorde a las actividades que se desarrollan en el departamento de TICS, para lo cual se establecen las siguientes etapas:

- Fecha de monitorización y revisiones: es necesario definir la fecha al cabo de la acción de monitoreo y las revisiones que se den.
- Origen de la acción: se debe tener en cuenta en donde se lleva a cabo la acción ya que la empresa está dividida por procesos.
- Descripción de la acción: se debe justificar la acción donde se detalle el estado del monitoreo y revisiones dando a conocer el cumplimiento de la seguridad de la información.
- Plan de mejora: se llevan a cabo toma decisiones para la ejecución de controles que ayuden a la evolución de las políticas o procedimientos.

- Seguimiento: es necesario para la definición de períodos de monitoreo y revisiones con el objetivo de verificar el cumplimiento eficaz del SGSI en la entidad.

CAPÍTULO V

Conclusiones y Recomendaciones

5.1 Conclusiones

Mediante el desarrollo del plan de implementación de la norma actual ISO 27001, ayudo a realizar la propuesta de un Sistema de gestión de Seguridad de la Información para la empresa Megaprofer S.A, aplicando controles adecuados en cuanto a la seguridad de la información.

La entidad no cuenta con procedimientos eficientes para salvaguardar la información, los diferentes procesos llevan a cabo ciertas políticas no eficaces que no ayudan al cumplimiento aceptable que puedan garantizar la confidencialidad, integridad y disponibilidad de la información.

Se toma conciencia sobre la importancia que tiene la seguridad de la información en la actualidad, dándonos a conocer que en una institución es fundamental contar un Sistema de Gestión de la Seguridad de la información aplicado mediante la norma internacional ISO 27001, para la ayuda de un análisis profundo del estado en la gestión de seguridad, la cual también permite evolucionar en el tratamiento de los riesgos de la seguridad de los activos de información.

Es de vital importancia contar con una matriz de riesgos, la cual ayude a identificar las vulnerabilidades existentes en los activos de información. Con el modelo SGSI que se integra bajo la norma ISO 27001, se tiene un procedimiento continuo en la gestión de la seguridad, que pueda ser capaz de mitigar o eliminar riesgos de información.

Con la elaboración del análisis de riesgos en base a la metodología MAGERIT permitió identificar la probabilidad e impacto de riesgos a los que se pueden enfrentar los activos de información, para poder emplear los controles necesarios que nos brinda la norma aplicada y así poder prevenirlos.

Con la ayuda de una segunda encuesta se pudo visualizar el impacto tuvo la implementación del SGSI, se pude apreciar que la preservación de la confidencialidad, disponibilidad e integridad tuvieron un impacto favorable.

La mejora continua del SGSI basada en la norma ISO 27001 es de vital importancia, para ello se creó procedimientos donde se realizarán monitoreos y revisiones que cubran incidentes, revisiones por parte de la gerencia y a la vez su estudio para toma de decisiones y aplicar medidas correctivas ante nuevos desafíos de amenazas en los activos de información.

5.2 Recomendaciones

La seguridad de la información es un pilar muy importante hoy en día para todo tipo de entidades, es importante que Megaprofer S.A despierte el interés y compromiso por parte de la alta dirección, con a fin de brindar apoyo al departamento de TICS, aportando los recursos necesarios para que así se lleven a cabo la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en su totalidad.

En el departamento de TICS se debe desarrollar un comité de seguridad y nombrar a una persona responsable que se encargue de gestionar la seguridad de la información, dando un seguimiento en el cumplimiento de las políticas de seguridad y controles, para un manejo eficiente de los activos de información de la organización.

Contratar un personal en el área de sistemas con el conocimiento y competencias necesarias para llevar a cabo la seguridad de la información y con eso evitar consultorías externas.

Dar seguimiento a las políticas de seguridad propuestas, para minimizar riesgos en los activos de información y a la vez fortalecer los cumplimientos en los controles que maneja la norma actual ISO 27001.

De acuerdo a la clasificación de la información establecer perfiles de acceso a cada usuario, a fin de mantener una confidencialidad eficaz.

Realizar capacitaciones a todo el personal con el objetivo de concientizar el impacto que tiene la seguridad de la información en la institución.

BIBLIOGRAFÍA

[1] U. I. d. Valencia, «¿Qué es la seguridad informática y cómo puede ayudarme?,» Ciencia y Tecnología, 21 Marzo 2018. [En línea]. Available: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/. [Último acceso: 17 Mayo 2018].

[2] E. T. Colombia, «El 31 por ciento de los ataques informáticos en Colombia apuntan a las pyme.,» http://www.eltiempo.com/, 8 Mayo 2013. [En línea]. Available: https://mattica.com/colombia-dos-de-cada-10-empresas-victimas-de-robo-de-datos/. [Último acceso: 10 octubre 2018].

[3] T. V. Guachi Aucapiña, «Norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el departamento de sistemas de la Cooperativa de ahorro y crédito San Francisco LTDA,» Julio 2012. [En línea]. Available: http://repo.uta.edu.ec/bitstream/123456789/2361/1/Tesis_t715si.pdf. [Último acceso: 25 octubre 2018].

[4] E. M. Torres Nuñez, «Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato,» Julio 2015. [En línea]. Available: http://repositorio.uta.edu.ec/jspui/bitstream/123456789/13057/1/Tesis_t1030si.pdf. [Último acceso: 25 Octubre 2018].

[5] . D. . M. Castro Núñez, «Auditoría Informática para optimizar el manejo de la información y equipamiento informático en el MIES INFA Tungurahua.,» Noviembre 2012. [En línea]. Available: http://repositorio.uta.edu.ec/bitstream/123456789/2901/1/Tesis_t765si.pdf. [Último acceso: 25 octubre 2018].

[6] E. P. Urrutia Urrutia y . E. M. Pico Llerena, «Análisis de los fraudes informáticos y su incidencia en el acceso a la información en la Cooperativa de Ahorro y Crédito San Francisco Ltda. Agencia Pelileo,» noviembre 2012. [En línea]. Available: http://repositorio.uta.edu.ec/jspui/handle/123456789/2899. [Último acceso: 25 octubre 2018].

[7] M. E. Raffino, «¿Qué es Seguridad?,» 5 septiembre 2017. [En línea]. Available: https://concepto.de/seguridad/.

[8] M. RUBÉN GARCÍA , «Análisis de situación ISO 27001 en las organizaciones.,» ISO 27001:2013, 11 Junio 2016. [En línea]. Available: https://www.eoi.es/blogs/ciberseguridad/2016/06/11/analisis-de-situacion-iso27001-en-las-organizaciones-3/.

[9] R. GARCÍA MORENO, «ANÁLISIS DE SITUACIÓN ISO27001 EN LAS ORGANIZACIONES,» 11 junio 2016. [En línea]. Available: https://www.eoi.es/blogs/ciberseguridad/2016/06/11/analisis-de-situacion-iso27001-en-las-organizaciones-3/.

[10] Á. García, «¿Qué es la Seguridad Informática?,» 9 enero 2015. [En línea]. Available: http://www.integracanarias.com/blog/35-seguridad-informatica-que-es#targetText=No%20debes%20confundir%20Seguridad%20Inform%C3%A1tica,e%20integridad%20de%20la%20misma.. [Último acceso: 4 noviembre 2018].

[11] N. Flores García, J. Santaeufemia Delgado y S. Valera Rodríguez, «Seguridad activa y pasiva,» 2014. [En línea]. Available:

https://sites.google.com/site/seguridadinformaticasjn/seguridad-activa-y-pasiva. [Último acceso: 4 noviembre 2018].

[12] P. Sullivan, «Gestión de riesgos de seguridad de la información,» 26 noviembre 2016. [En línea]. Available: https://searchdatacenter.techtarget.com/es/consejo/Gestion-de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes.

[13] M. Á. Amutio Gómez, «MAGERIT versión 3,» [En línea]. Available: https://administracionelectronica.gob.es/ctt/magerit#.Xe6qT-hKjIU.

[14] L. L. CORDOBA ARAUJO y W. C. DELGADO TRUJILO, «DISEÑO DE LAS POLÍTICAS DE CONTROL DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA SEDE CENTRAL DE LA GOBERNACIÓN DEL PUTUMAYO (MOCOA),» 2016. [En línea]. Available: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/8511/3/1124848759.pdf.

[15] M. J. Buigues, «Iso 27001 interpretación introducción,» 18 junio 2015. [En línea]. Available: https://es.slideshare.net/mariajosebuigues3/iso-27001-interpretacin-introduccin.

[16] p. p. e. p. SGSI, «La norma ISO 27001 y la mejora continua en la gestión de seguridad de la información,» 13 mayo 2016. [En línea]. Available: https://www.esan.edu.pe/apuntes-empresariales/2016/05/norma-iso-27001-mejora-continua-en-la-gestion-de-seguridad-informacion/. [Último acceso: 4 diciembre 2018].

[17] A. T. Alarcon, C. M. Gonzales y A. F. Lara, «Sistemas de Gestión de Calidad,» 22 mayo 2015. [En línea]. Available: https://www.emaze.com/@ALFOZITZ.

[18] www.ISO27001.es, «Sistema de Gestión de la Seguridad de la,» 2 octubre 2014. [En línea]. Available: http://www.iso27000.es/download/doc_sgsi_all.pdf.

[19] U. b. e. p. I. Excellence, «Dominios ISO 27001:2013: Motivos para conocer mejor la nueva norma,» Blog especializado en Sistemas de Gestión, 20 abril

2017. [En línea]. Available: https://www.pmg-ssi.com/2017/04/dominios-iso-27001-2013/.

[20] W. . A. GAVIRIA ÁLVAREZ, «Políticas de seguridad de la información empresa caso de estudio, en la sede Medellín de la ISO 27001 2013.,» 27 septiembre 2017. [En línea]. Available: https://webcache.googleusercontent.com/search?q=cache:kCZykJySbCcJ:https://repository.unad.edu.co/bitstream/10596/13274/1/71768559.pdf+&cd=1&hl=es-419&ct=clnk&gl=ec. [Último acceso: 15 diciembre 2018].

[21] G. R. Baena, R. V. Mendoza Méndez y E. . d. Joel Coronado, «IMPORTANCIA DE LA NORMA ISO/EIC 27000 EN LA IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN,» 23 mayo 2019. [En línea]. Available: https://www.eumed.net/rev/ce/2019/2/norma-iso-eic.html.

[22] F. E. SANCHEZ ARDILA, «PLAN DE IMPLEMENTACIÓN DE LA ISO/IEC 27001:2013, EN LA FUNDACIÓN UNIVERSITARIA SAN MATEO,» junio 2018. [En línea]. Available: https://docplayer.es/108672966-Plan-de-implementacion-de-la-iso-iec-27001-2013-en-la-fundacion-universitaria-san-mateo.html.

[23] C. LikedIn, «Conoce una de las maneras más confiables para medir opiniones, percepciones y comportamientos, y cómo puedes aplicarla en tu próxima encuesta.,» [En línea]. Available: https://es.surveymonkey.com/mp/likert-scale/.

[24] L. L. CORDOBA ARAUJO y W. C. DELGADO TRUJILO , «EL ANÁLISIS DE RIEGOS METODOLOGIA MAGERIT,» 2016. [En línea]. Available: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/8511/3/1124848759.pdf. [Último acceso: 15 marzo 2019].

[25] E. p. d. I. 2. e. Español, «Portal de soluciones técnicas y organizativas de referencia a los CONTROLES DE ISO/IEC 27002,» 13 enero 2018. [En línea]. Available: http://iso27000.es/iso27002.html. [Último acceso: 23 junio 2019].

[26] M. Á. Mendoza , «¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve?,» 1 abril 2015. [En línea]. Available: https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/. [Último acceso: 25 junio 2019].

[27] U. O. d. Catalunya, «Política de seguridad criptográfica de la Universitat Oberta de Catalunya,» [En línea]. Available: https://www.uoc.edu/portal/_resources/ES/documents/seu-electronica/Politica_Seguretat_Criptogrxfica_UOC-cat_ES.pdf.

[28] R. E. VALENTE CONYA, «PROPUESTA DE UNA METODOLOGÍA DE DETECCIÓN Y RESPUESTA A VULNERABILIDADES PARA MEJORAR LA SEGURIDAD EN LA RED DE DATOS. CASO PRÁCTICO: INTRANET DE LA ORGANIZACIÓN NO GUBERNAMENTAL WORLD VISION ECUADOR,» octubre 2018. [En línea]. Available: http://dspace.espoch.edu.ec/bitstream/123456789/9056/1/20T01085.pdf. [Último acceso: 10 diciembre 2019].

[29] B. e. e. S. d. gestión, «¿Cuáles son los retos a los que se enfrente un director de seguridad de la información?,» ISO 27001:2013, 26 octubre 2017. [En línea]. Available: https://www.pmg-ssi.com/2017/10/retos-director-seguridad-de-la-informacion/.

ANEXOS

Anexo A.- PROCESOS EXISTENTES EN MEGAPROFER S.A

Index of /SISTEMASDEGESTION/PROCEDIMIENTOS/NUEVOS

Name	Last modified	Size	Description
Parent Directory		-	
ADMINISTRACIÓN DE PEDIDOS/	21-Nov-2018 17:07	-	
DESPACHO Y DISTRIBUCIÓN/	21-Nov-2018 17:07	-	
GESTIÓN ADMINISTRATIVA/	21-Nov-2018 17:07	-	
GESTIÓN DE COMPRAS/	21-Nov-2018 17:07	-	
GESTIÓN DE CONTABILIDAD/	21-Nov-2018 17:07	-	
GESTIÓN DE POSVENTA/	21-Nov-2018 17:07	-	
GESTIÓN DE TALENTO HUMANO/	21-Nov-2018 17:07	-	
Manual de Control y Seguridad MEGAPROFER S.A/	21-Nov-2018 17:07	-	
PLANIFICACIÓN ESTRATÉGICA/	21-Nov-2018 17:07	-	
PROCESOS DE CONTABILIDAD/	21-Nov-2018 17:07	-	
SEGURIDAD Y SALUD OCUPACIONAL, SEGURIDAD FÍSICA/	21-Nov-2018 17:07	-	
SISTEMAS DE GESTIÓN/	21-Nov-2018 17:07	-	
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN/	21-Nov-2018 17:07	-	

Anexo B.- Entrevista Personal TICS

"PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A."

UNIVERSIDAD TÉCNICA DE AMBATO

ENTREVISTA PARA EL PERSONAL DEL DEPARTAMENTO DE TICS

Objetivo: Determinar el nivel protección de seguridad de la información y activos en el área de TICS basada en la norma ISO 27001 en la empresa Megaprofer S.A, para seleccionar la mejor estrategia a seguir.

Datos demográficos

Nombre: Paúl Montesdeoca

Cargo: Asistente de Tics

Antigüedad en la empresa: 5 años

Nivel de Educación: Técnico __ Tecnológico __ Profesional _x_ Otros __

Categorías / Indicadores	Observaciones
Seguridad y Norma ISO 27001	
12. ¿Qué conocimientos posee con respecto a la seguridad de la información?	
13. ¿Qué conocimientos tiene sobre las normas que establecen la Seguridad de la información?	
14. ¿Cuál es su conocimiento sobre Normas ISO 27001?	
15. ¿Qué conocimiento tiene sobre la ley de protección de datos?	
16. ¿Los equipos de cómputo tienen licenciamiento vigente?	
17. ¿Qué nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema?	
18. ¿Está disponible en su totalidad todo tipo de información necesaria para todos los usuarios de los sistemas autorizados?	
19. ¿Existe información que se filtra hacia fuera del departamento?	
20. ¿Los procesos que se manejan actualmente poseen una documentación detallada y disponible en cualquier momento?	

21. ¿Se aplican actualmente políticas de seguridad para gestionar la información? Enúncielas.	
22. ¿Se realiza gestión de riesgos en cuanto a la seguridad de la información?	

Usuarios

8. ¿Existe una sola persona encargada para la creación de usuarios?	
9. ¿Existe algún registro de los usuarios creados?	
10. ¿Los usuarios que se encuentran en período de vacaciones o que ya no laboran en la empresa son bloqueados?	
11. ¿Se debe solicitar permisos para la creación de usuarios?	
12. ¿Las claves creadas tienen caducidad?	
13. ¿Están definidas responsabilidades del usuario en cuanto al uso adecuado de los recursos?	
14. ¿Existe un control sobre el acceso no autorizado al usuario, con la finalidad de proteger el	

equipamiento y sistemas que se manejan en la empresa?	

Autentificación

6. ¿El password es genérico para todos los usuarios creados?	
7. ¿Está definido el tamaño y definición del password?	
8. ¿El ingreso de clave errado bloquea al usuario?	
9. ¿Los usuarios pueden ingresar a sistema través de cualquier equipo?	
10. ¿Se puede ingresar a través de otro equipo de cómputo si el usuario ya está en uso?	

Autorización

6. ¿Los usuarios creados tienen permiso para realizar cualquier clase de consulta, modificación o alteración de la base de datos?	
7. ¿Están definidos los permisos para cada usuario?	
8. ¿Existe autorización para el cambio de usuario o password?	
9. ¿Está permitido el acceso a páginas que no son de orden institucional?	
10. ¿Se puede hacer uso de celular o cualquier medio de	

almacenamiento durante la jornada laboral?	

Administración Sistemas

8. ¿El administrador puede realizar cambios en la Base de Datos (BDD)?	
9. ¿La sesión de los usuarios permanece activa durante tiempos prolongados cuando no hay uso del sistema?	
10. ¿Existen controles para el acceso a los backups por parte del Administrador de base de datos (DBA)?	
11. ¿Los usuarios pueden extraer información a través de dispositivos externos?	
12. ¿Existe algún registro o documento de las personas autorizadas para realizar respaldos de los sistemas?	
13. ¿Han realizado simulacros frente a la caída de los sistemas de información y de comunicación? Si…. De qué manera se lo ha realizado; No…. ¿Por qué?	
14. ¿Se realizan tareas de monitoreo a los sistemas de información que se manejan?	

Equipos Informáticos

5. ¿Los equipos tienen capacidad de memoria suficiente para la ejecución de programas y aplicaciones necesarias para ejecutarse correctamente?	
6. ¿Todos los procesos en cuanto a los equipos se encuentran documentados?	
7. ¿Se realiza un mantenimiento periódico de los equipos de la empresa?	
8. ¿Los usuarios pueden destapar o abrir los equipos de cómputo asignados?	

Pistas de Auditoría

4. ¿Los proxys están definidos?	
5. ¿Se actualizan bitácoras para el registro de o actualización de la información?	
6. ¿Qué mecanismo, técnicas y/o herramientas de seguridad se aplican en los sistemas de información y de comunicación?	

Activos fijos

13. ¿Los registros de activos fijos contienen la suficiente	

información y detalle, según la necesidad de la empresa?	
14. ¿Qué tipo de políticas o reglas se aplican al momento de la autorización de activos fijos para: retirar, destruir, ¿adquirir o vender?	
15. ¿Se hace periódicamente un inventario físico o digital de los activos fijos donde se consta su existencia y su estado?	
16. ¿Las personas que tienen a su cuidado el activo fijo otorgado por la empresa, están obligadas a reportar cualquier cambio existente como: daños, golpes, traspasos, problemas con el software, ¿etc.?	
17. ¿La venta de activos fijos del departamento de TICS requiere la autorización previa de los directivos?	
18. ¿Se tiene información sistematizada y actualizada de inventario de activos fijos de la empresa?	
19. ¿El inventario esta degradado por áreas?	
20. ¿Se han definido procedimientos específicos para: (¿Registro de activos, Resguardos, Altas,	

Bajas, Transferencias, ¿Toma física de inventarios?	
21. ¿Se cuenta con una base de datos o programas computarizados del inventario de los activos fijos?	
22. ¿Se lleva un registro actualizado de los ingresos de activos de los proveedores?	
23. ¿Existe el personal idóneo para controlar los activos fijos?	
24. ¿Es necesaria la implantación de un proceso adecuado para el control de los activos fijos?	

Anexo C.- Encuesta Personal TICS (PRE)

"PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A."

UNIVERSIDAD TÉCNICA DE AMBATO

ENCUESTA PARA EL PERSONAL DEL DEPARTAMENTO DE TICS

Objetivo: determinar el nivel de conocimiento en cuanto a la seguridad de la información y las normas que lo establecen, con el objetico de conocer la situación actual de la entidad.

Datos demográficos

Dirigido: integrantes del departamento de TICS

Cargo: jefe, Asistentes de Tics, Pasante

Antigüedad en la empresa: menor igual a 5 años

Nivel de Educación: Técnico _x_ Tecnológico __ Profesional _x_ Otros __

Conocimiento en la Seguridad de la Información	E	B	R	MD	NT
En cuanto a la seguridad de la información usted tiene un conocimiento					
Usted tiene conocimientos sobre las normas que integran la seguridad de la información					
Mediante las capacitaciones otorgadas en la entidad sobre la seguridad de la información, que nivel de conocimiento ha desarrollado					
Dado que se hayan desarrollado auditorias sobre la seguridad de la información, mediante ese proceso en qué estado se encuentra la seguridad en la entidad					
Cuál es su conocimiento sobre la norma ISO 27001					
Qué conocimiento tiene sobre la ley de protección de datos					
Total:					

Procedimientos para la defensa y seguridad de la información	E	B	R	MD	NT
El medio donde se alojan los backups de los servidores ¿En qué estado se encuentra?					
Los datos que se verifican después de realizadas las copias de seguridad se catalogan como:					
El sistema de control para el ingreso a esta área se define como:					
Como se define las pistas dejadas al ingresar a esta área					

Como se definen los controles que se ejerce a los usuarios del área de TICS para ingresar a los servidores					
En qué estado se dispone los servidores alternos que tiene la entidad en caso de un fallo en los servidores principales					
Total:					

Aplicación de herramientas para la protección de datos y la seguridad de la información	E	B	R	MD	NT
El antivirus instalado en los equipos de cómputo de la empresa se puede definir como:					
El nivel de protección brinda el antivirus instalado en los equipos de computo					
Como se define la restricción a paginas no permitidas en la empresa Megaprofer S.A.					
Los equipos de cómputo tienen licenciamiento vigente					
Como se define el password para el ingreso al sistema					
El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema					
Total:					

Acceso al área de servidores o Data Center	E	B	R	MD	NT
Mediante las normativas de seguridad de la información en los servidores que son el diseño y ubicación de los mismos que estado dispone					
En caso de que se suscite una emergencia y este ponga en riesgo la información el plan de contingencia en qué nivel se encuentra para actuar ante la eventualidad					

En el ingreso al área de las cámaras, registros, bitácoras, backus entre otros, la seguridad se define como					
En qué estado se dispone los servidores alternos que tiene la entidad en caso de un fallo en los servidores principales					
En los servidores donde se almacenan los backups, en cuanto a su seguridad como lo define					
Total:					

Anexo D.- Encuesta Personal TICS (POST)

"PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001, PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DE LA EMPRESA PRIVADA MEGAPROFER S.A."

UNIVERSIDAD TÉCNICA DE AMBATO

ENCUESTA PARA EL PERSONAL DEL DEPARTAMENTO DE TICS

Objetivo: determinar la preservación de la seguridad de la información y activos basada en la norma ISO 27001 en la empresa Megaprofer S.A, que permitan el incremento de la seguridad con ayuda del SGSI implementado.

Datos demográficos

Dirigido: integrantes del departamento de TICS

Cargo: jefe, Asistentes de Tics, Pasante

Antigüedad en la empresa: menor igual a 5 años

Nivel de Educación: Técnico _x_ Tecnológico __ Profesional _x_ Otros __

Categorías / Indicadores	Si	No	Parcial
1. ¿Actualmente, los procesos tienen una documentación formal detallada y disponible en cualquier ámbito?			
2. ¿Existe información que se filtra hacia fuera del departamento?			
3. ¿Para los usuarios en los sistemas autorizados, se encuentra disponible toda información necesaria?			
4. ¿Existen seguridades de ingreso a los sistemas, que manejan los usuarios?			
5. ¿Se tiene planificado el monitoreo periódico de la información almacenada en los sistemas?			
6. ¿Se garantiza el uso adecuado de los dispositivos móviles?			
7. ¿Existen políticas que den respuesta a los incidentes que se presenten?			
8. ¿Existe una persona responsable de realizar backups de la información?			
9. ¿El usuario que necesita instalar un software en su ordenador, presenta autorización por parte de una autoridad?			
10. ¿Existen mecanismos de control para la relación con personal externo que le proveen bienes o servicios?			
11. ¿Los activos fijos se manejan bajo directrices de bloqueo, protección, seguridad, entre otros?			
12. ¿Existen controles ante amenazas que pueden ocasionar interrupciones de los procesos o actividades que afecten el servicio de la empresa?			
13. ¿Existe controles sobre el código malicioso para los equipos de cómputo?			

14. ¿Se aplican actualmente políticas de seguridad para gestionar la información?			
15. ¿Se tiene conocimiento si el departamento de TICS posee una política de seguridad de la información?			