UNIVERSIDAD DE HUÁNUCO

Facultad de Ingeniería

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS:

“DISEÑO E IMPLEMENTACIÓN DE UN SGSI ISO 27001 PARA LA MEJORA DE LA SEGURIDAD DEL AREA DE RECURSOS HUMANOS DE LA EMPRESA GEOSURVEY DE LA CIUDAD DE LIMA.”

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

Autor:

VILCA MOSQUERA, Ehytel Celestino

Asesor:

Mg. LOPÉZ DE LA CRUZ, Edgardo Cristiam Ivan

Huánuco- Perú

2017

DEDICATORIA

A mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación para hacer de mí una mejor persona.

Ehytel

AGRADECIMIENTOS

A la Universidad de Huánuco, a mi honorable Facultad de Ingeniería y a todos los Docentes que a lo largo de mi formación académica me impartieron sus conocimientos en el campo de la ingeniería y en otras áreas que corresponden a mi profesión.

Al asesor de tesis Ing. Cristiam López de la Cruz, por la acertada orientación en la realización de esta tesis.

Ehytel

INDICE

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

RESUMEN

La presente Tesis tuvo como finalidad de implementar un sistema de gestión de la seguridad de la información bajo el ISO 27002 para mejorar la seguridad en cuanto al uso de los activos y tecnologías de la información en la empresa Geosurvey de la ciudad de Lima en el año 2016.

La metodología a emplearse fue bajo el enfoque cuantitativo, y de tipo aplicativo; porque se utilizó la tecnología para la solución de un problema, así mismo se empleó el diseño pre experimental de pre y post test se llevó a cabo un experimento en condiciones controladas. Tanto la población como la muestra estuvo conformada por 33 trabajadores siendo no probabilística, se tomaron en cuenta todos los trabajadores de las diferentes áreas de la empresa. Para la recolección de datos se utilizó el cuestionario como técnica y el cuestionario de encuesta como instrumento para luego los datos ser procesados en el software estadístico SPSS.

Se empleó las cuatro fases PDCA del ISO 27002, que permitió el diagnóstico de la gestión de riesgos de la empresa, la elaboración de la política se seguridad y así también el sistema de gestión de incidentes para poder controlar y mejorar la seguridad de la información de la empresa.

Palabras Clave: SGSI, Gestión de riesgos, gestión de incidencias, política de seguridad de la información.

ABSTRACT

The purpose of this thesis was to implement an information security management system under ISO 27002 to improve security in the use of assets and information technologies in the Geosurvey company of the city of Lima in the year 2016.

The methodology to be used was under the quantitative approach, and of the application type; because the technology was used for the solution of a problem, likewise the pre-experimental design of pre and post test was used, an experiment was carried out under controlled conditions. Both the population and the sample consisted of 33 workers being non-probabilistic, all workers from different areas of the company were taken into account. For data collection, the questionnaire was used as a technique and the survey questionnaire as an instrument for later data to be processed in the statistical software SPSS. The four PDCA phases of ISO 27002 were used, which allowed the diagnosis of the risk management of the company, the elaboration of the security policy and also the incident management system to be able to control and improve the security of the information of the company.

Keywords: SGSI, risk management, incident management, information security policy.

INTRODUCCIÓN

La investigación se realizó en base a la demanda de un estudio preliminar del diagnóstico o situación actual del desempeño de los procesos de la empresa Geosurvey de la ciudad de Lima.

El presente estudio de investigación se centra en el problema de la falta de un sistema de seguridad de la información que permita asegurar la confidencialidad, integridad y disponibilidad de la los activos de la empresa, y estos activos se traducen en la información, la infraestructura tecnológica y el personal con el que cuenta dicha empresa; dentro de estos activos se ha enfocado en el uso correcto y resguardo de las tecnologías de la información y comunicación. Ante la inexistencia de este sistema que desencadenan problemas como por ejemplo las pérdidas de equipos, de información importante desde las computadoras personales de cada área, el desconocimiento de una política de seguridad en cuanto al manejo de las situaciones que podrían suscitarse dentro de la empresa al momento de poner en riesgo a los activos, así mismo de no saber que pueden y no pueden hacer los trabajadores en relación al uso de las tecnologías de la información y comunicación.

Ante el presente problema se formuló la siguiente pregunta: ¿De qué forma la implementación del Sistema de Gestión de la Seguridad de la información mejorará la seguridad de la empresa GEOSURVEY S.A?, ante la pregunta se afirma con el objetivo: Determinar la mejora de implementar un sistema de gestión de seguridad de la información para la seguridad de la empresa GEOSURVEY S.A; de esta forma la investigación se centró en la implementación de un sistema de gestión de la seguridad de la información que permitió controlar y asegurar los activos de la empresa mediante la gestión de riesgos, la implantación de políticas de seguridad y el control de incidentes mediante un sistema de gestión de incidencias y así poder llevar a cabo el ciclo PDCA que significa la planeación, el hacer, el verificar y monitorear la seguridad de la empresa, tanto la población como la muestra que fue de 33 trabajadores asignados a diferentes áreas de la empresa, se utilizó el

cuestionario de encuesta como instrumento para recabar información por parte de los trabajadores en cuanto a la mejora de las actividades relacionadas al uso de las tecnologías de información y comunicación mediante el Sistema de Gestión de seguridad de la información ya implementando.

Con respecto a la limitación principal fue de tipo geográfica, ya que la empresa se encuentra situada en la ciudad de lima, y el estudio correspondiente se hizo en el mes de enero del 2017, con algunos datos que no se pudo recabar o afianzar se tuvo que realizar de forma virtual mediante el uso de la video conferencia.

Finalmente, el estudio de investigación fue exitoso ya que se otorgó a la empresa un documento esencial para el manejo y control de los activos e información de la empresa, dicho documento está compuesto por otros documentos más que conjuntamente el resultado final es el Sistema de Gestión de la seguridad de la información.

CAPITULO I: PROBLEMA DE INVESTIGACIÓN

1.1 Descripción del problema

Una norma o estándar, es un conjunto de reglas y procedimientos que nos guían y nos indican de cómo deben hacerse las cosas en cada situación de los procesos o actividades de una organización.

Las normas ISO surgen para estandarizar la gran cantidad de normas sobre gestión de calidad y seguridad en las organizaciones. Los organismos de normalización de cada país producen normas que resultan del consenso entre representantes del estado y de la industria.

Estamos en la era de información, y por ende el activo más valioso que hoy en día posee las diferentes empresas, es la información y parece ser que cada vez más sufre grandes amenazas en cuanto a su confidencialidad, integridad y disponibilidad, de igual forma la información es vital para el éxito y sobrevivencia de las empresas en cualquier mercado. Con todo esto todo parece indicar que uno de los principales objetivos de toda organización es el aseguramiento de dicha información, así como también de los sistemas que la procesan.

Para que se pueda llevar a cabo una correcta gestión de la seguridad de la información dentro de las organizaciones, es necesario implantar un sistema de gestión de la seguridad de la información que aborde esta tarea de una forma metódica y lógica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. Para lograr estos objetivos, existen organizaciones o entes especializados en redactar estándares necesarios y especiales para el resguardo y seguridad de la información, los estándares correspondientes se encuentran en la norma ISO 27001 y 27002.

El estándar 27001 ha sido preparado para proporcionar y promover un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información. La adopción

de este estándar diseño e implementación debe ser tomada en cuenta como una decisión estratégica para la organización.

La empresa GEOSURVEY.SA ubicada en la Av. Aviación #2836 en el distrito de San Borja, Lima; empresa dedicada a la Geodesia, Topografía, Batimetría, Fotogrametría, Gestión ambiental, Consultoría y Asesoría en procedimientos mineros y auditoria y fiscalización; en el transcurso del desarrollo de las actividades diarias se ha encontrado operaciones ilícitas por parte de los trabajadores con respecto al uso de la información que posee la empresa, así como también el mal uso de los recursos informáticos que posee la empresa, esto ha ocasionado la informalidad en cuanto al control del personal y de los activos de la empresa, conllevando así mismo a la perdida de algunos activos y a la fuga de información sensible desde la empresa hacia el exterior llegando a manos de la competencia. Esto ha ocasionado la falta de compromiso por parte del personal con el buen y correcto proceder de los objetivos que tiene la empresa, por lo tanto, desprestigiando el nombre de la empresa y perjudicando la cartera de clientes de la misma.

En tal sentido la junta directiva mediante consejería externa ha tomado la decisión de implementar un sistema de gestión de seguridad de la información con respecto a los recursos humanos y materiales debido a que regirían lineamientos que permitirán reclutar personal calificado de acuerdo al rol a desempeñar. La empresa maneja información de vital importancia para sus clientes, la cual se considera delicada y no se puede arriesgar a incorporar personal que pueda hacer mal uso, voluntaria o involuntariamente, de ésta. GEOSURVEY S.A considera que una selección adecuada de su personal evitara problemas a futuro con el mismo. Además, cree que aplicar un sistema de gestión de seguridad de la información agregaría confiabilidad al desarrollo de sus actividades. La empresa desea ser pionera en la implementación de dicho sistema, ya que dentro de su mercado es muy escaso el conocimiento del tema.

Por lo tanto, el objetivo de desarrollar un sistema de gestión de seguridad de la información para la organización es disminuir el número de amenazas que, aprovechando cualquier vulnerabilidad existente, pueden someter a activos de información a diversas formas de fraude, sabotaje o vandalismo. Las amenazas que pueden considerarse de mayor relevancia en la institución son los virus informáticos, la violación de la privacidad de los empleados, los empleados deshonestos, intercepción de transmisión de datos o comunicaciones y/o fallas técnicas de manera voluntaria o involuntariamente.

La importancia de realizar el análisis referente a la gestión de la seguridad de las áreas de la empresa, radica en conocer el manejo de la información correspondiente a cada área y su flujo dentro de la empresa. De esta manera, se establece que personas conocen o manejan que información y se establecen los procedimientos a seguir para resguardar dicha información. Al implementar estos procedimientos se deben realizar controles u observaciones de su funcionamiento dentro del área dispuesta, los cuales permitirán desarrollar cambios en los mismos.

1.2 Formulación del problema

Problema General

¿De qué forma la implementación del Sistema de Gestión de la Seguridad de la información mejorará la seguridad del área de recursos humanos de la empresa GEOSURVEY SA?

Problemas Específicos

¿De qué forma se podrá optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa GEOSURVEY SA?

¿De qué forma se podrá optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa GEOSURVEY SA?

1.3 Objetivo General

Determinar la mejora de implementar un sistema de gestión de seguridad de la información para la seguridad del área de recursos humanos de la empresa GEOSURVEY S.A

1.4 Objetivos Específicos

- Optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa
- Optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa

1.5 Justificación de la investigación

- ✓ **Justificación Teórica:**

  Se justifica la investigación a nivel teórica por el desarrollo del documento del Sistema de Gestión de Seguridad de la Información la cual permitirá poseer las políticas de seguridad para así poder cumplirlas en el ámbito laboral de la empresa.

- ✓ **Justificación Práctica:**

  Por medio del presente estudio se podrá utilizar el SGSI como marco normativo para poder realizar todas las actividades relacionadas al uso de las tecnologías de la información y comunicación dentro de la Empresa.

- ✓ **Justificación Metodológica:**

  La implementación de la investigación se realiza utilizando la metodología PDCA basada en el ISO 27002 para poder diseñar e implementar un Sistema de Gestión de Seguridad de la Información.

1.6 Limitaciones de la investigación

Las limitaciones encontradas para realizar el presente estudio de investigación fueron:

- El lugar donde se realizaran la investigación, recojo de datos y la aplicación de la prueba es distante por estar en otra ciudad en este caso en Lima, por lo tanto se tendrá que realizar algunos viajes para poder realizar lo programado.
- Para una buena recolección de información, previamente se debe concientizar a los trabajadores del área de recursos humanos de la empresa en cuanto a los aspectos teóricos y técnicos de un SGSI.
- En cuanto a la metodología empleada bajo el ISO 27002, solo se han utilizado algunos controles.
- Las fases de un SGSI son: plan, hacer, verificar y actuar, en este caso con respecto al desarrollo del SGSI se tiene: en cuanto al análisis de riesgos está considerado en la fase Plan, la asignación de los 133 controles para cada análisis de riesgo se considera dentro de la etapa Hacer y la Gestión de incidentes y el plan de mejora continua lo consideramos dentro de la fase Verificar, por lo tanto, la investigación cubre solo las 3 primeras fases del SGSI.

1.7 Viabilidad de la investigación

El proyecto de investigación es viable por las siguientes razones:

- **Viabilidad Técnica.**

  El viable desde un punto de vista técnico, ya que se dispone de los recursos físicos y lógicos necesarios para el desarrollo de la investigación. En este caso se cuenta con la metodología y todos con controladores planteados por el ISO 27002 que nos permitirá elaborar el Sistema de Gestión de Seguridad de la Información.

- **Viabilidad socio-económica.**

  Los gastos que se realizaran durante el proceso del estudio de la investigación, están considerandos dentro del presupuesto. También se cuenta con los recursos físicos necesarios para la recolección, procesamiento y presentación de la información relacionada al estudio de investigación, así como también la persona adecuada para realizar la investigación en este caso el investigador conjuntamente con el asesor

- **Viabilidad Institucional.**

  Se cuenta con el apoyo del personal directivo de la empresa en cuanto a la recolección de la información, del análisis, del diseño y de la implementación del SGSI.

CAPITULO II: MARCO TEÓRICO

2.1 Antecedentes de la Investigación

A. A nivel Internacional:

- (Pallas Mega, 2009) Metodología de Implantación de un SGSI en un grupo empresarial jerárquico para optar el Título de Ingeniero Informático. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son los siguientes:

  Un grupo empresarial, con una estructura de relación jerárquica o de subordinación, requiere de una metodología que permita gestionar la seguridad de la información atendiendo este aspecto estructural y jerárquico, con criterios alineados a la estrategia empresarial, y además de cooperación en todas las etapas del ciclo PHVA (PDCA), pero a su vez con la flexibilidad y agilidad operativa suficiente para alcanzar los niveles de seguridad necesarios y específicos a cada empresa, respetando los lineamientos corporativos. Este trabajo aporta una metodología con esta concepción de enfoque global y sistémico, atendiendo a la pertenencia de la empresa a un grupo empresarial, y a su vez pragmático, a los efectos que la misma sea, no sólo viable, sino conveniente y efectiva, dando una estructura u organigrama para lograr la coordinación necesaria y especificando los procedimientos que deben cumplirse en cada fase, promoviendo no sólo la reutilización y coherencia integral de la seguridad sino también fomentando la sinergia entre las empresas del grupo.

  Un producto parcial y homónimo de este trabajo de tesis, se ha constituido en una ponencia en el marco del “V Congreso Iberoamericano de Seguridad Informática (CIBSI’09)” en Montevideo, Uruguay, en noviembre de 2009. En referencia a la estrategia de análisis y gestión de riesgos así como de planificación, implementación y seguimiento del SGSI, proponemos un enfoque mixto, de dirección centralizada pero con la autonomía necesaria a nivel de cada dominio y cada

empresa, fundamentalmente en la gestión de controles y en la percepción del impacto de los riesgos locales. Esto permitirá aunar criterios y optimizar recursos cuando los riesgos deban afrontarse en forma conjunta.

- (J., 2013) Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda. Para optar el Título de Ingeniero Informático. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son los siguientes:

  Se puede concluir que actualmente se vive en una época en la que la información y los datos poseen una importancia decisiva en la gran mayoría de organizaciones, convirtiéndose así en su activo más importante. Por ejemplo, en caso de una emergencia, una catástrofe natural y se llegara a caer la instalación de la organización; se puede volver a reconstruir. En cambio, si llegamos a perder la información de la organización, es muy probable que no podamos volver a recuperarla si no se tienen las consideraciones debidas, con lo que es probable que la empresa deje de operar. Cabe resaltar que partiendo de esta premisa, es importante contar con un Sistema de Gestión de Seguridad de la Información para poder asegurar, a un nivel aceptable, la información, de la organización empresarial La Ofrenda S.A, la cual es colombiana, dado que se trata de una organización dedicada a satisfacer integralmente las necesidades de la población en servicios funerarios, parques cementerios y cremación; es una organización, poder cumplir con las regulaciones de la ISO 27002. En este documento se consideraron los procesos que tiene el grupo empresarial La Ofrenda S.A, pero es importante considerar siempre que el SGSI debe estar enfocado en las necesidades del negocio. Es decir, si la organización considera un 80 proceso en particular como crítico, se deben implementar controles necesarios para asegurar el mismo. Es de opinar que una vez identificados los riesgos, se procede a desarrollar los controles para el SGSI. Antes que nada,

es indispensable obtener el apoyo de la alta gerencia haciéndoles entender la importancia que tiene la seguridad de la información en toda la organización. Con el apoyo de la alta gerencia, podemos asegurar que el personal de la organización va a seguir las políticas y procedimientos de seguridad de información que se vayan a publicar como parte del SGSI, así como los controles, lineamientos, estándares, entre otros que se puedan definir.

B. A nivel Nacional:

- (Aguirre Mollehuanca, 2014) Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A. Para optar el Título de Ingeniero Informático. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son los siguientes: Es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas. Existe una clara necesidad en la organización de contratar personal especializado para dar soporte a los procesos involucrados en el SGSI, debido a que los recursos actuales no se dan abasto para atender los requerimientos de los usuarios lo cual en muchos casos se ha utilizado como excusa para realizar actos que afectan la seguridad de la información como el préstamo de credenciales de usuarios, uso de un correo para varias personas o la dejadez en la generación de respaldos de información del área. Es necesario mejorar la comunicación con el área de logística para acelerar los procesos de compra de

aquellos activos que nos ayudaran en el tratamiento de riesgos detectados, especialmente, si estos riesgos son considerados altos o graves por la organización.

- (Aliaga Flores, 2013) Diseño de un sistema de gestión de seguridad de información para un instituto educativo. Para optar por el Título de Ingeniero Informático. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son los siguientes: Conforme a las observaciones, si bien los controles ayudan a mitigar o reducir algún riesgo identificado, algunos de estos no aplican a la realidad del instituto educativo en particular por diversos factores. Estos factores son importantes que se detallen dentro de la justificación de la aplicabilidad de dichos controles, la cual se especifica dentro del documento de la Declaración de Aplicabilidad que es un entregable de la presente tesis. Finalmente, cabe resaltar que, si no se cuenta con el apoyo de la alta gerencia de la institución educativa, no se contara con el soporte necesario para lograr los objetivos del SGSI. Asimismo, si el personal de la organización no sigue las políticas y lineamientos propuestos por la alta gerencia siguiendo dicho SGSI, no se obtendrá el nivel adecuado de seguridad en los flujos de información de los distintos procesos del instituto educativo. En conjunto con las personas, la información es el activo más importante que tiene cualquier organización. La falta de controles y políticas enfocadas a su seguridad puede traer consecuencias graves para el cumplimiento de los objetivos de negocio e incluso, pérdidas más graves de lo que la organización supone. No hay un interés adecuado con respecto a la seguridad de información dentro de las instituciones educativas, partiendo desde la alta gerencia hasta los mismos departamentos de TI. Dicha falta de interés se muestra claramente en la falta de políticas, normas y controles dentro del instituto educativo y en la falta de concientización del personal del mismo con respecto a la seguridad de la información.

- (Ampuero Chang, 2011) Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. Para optar por el Título de Ingeniero Informático. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son los siguientes: El desarrollo del BIA es importante para el posterior análisis de riesgos. En él se identifican los riesgos asociados a los distintos procesos y la criticidad de los mismos, así como los recursos afectados en caso de un incidente de seguridad. El

  BIA también se utiliza como insumo para el desarrollo del plan de continuidad de negocios, que no ha sido parte del alcance de la tesis, y que va a ayudar a identificar aquellos recursos que se deben de recuperar para que el proceso se encuentre operativo una vez más. Una vez que desarrollamos el BIA, es necesario realizar un análisis de los riesgos identificados. Para ello, se puede establecer un comité, formado por personas que cuenten con la experiencia y el conocimiento necesario

  del negocio, que ayude a identificar los riesgos que afectan a la compañía. La participación de diferentes personas dentro de la compañía en el comité va a permitir identificar mejor los riesgos. Para esto, es importante que sean personas que tengan un conocimiento amplio sobre los distintos procesos de la compañía o sean especialistas sobre procesos específicos. Una vez identificados los riesgos, se procede a desarrollar los controles para el SGSI. Antes que nada, es indispensable obtener el apoyo de la alta gerencia haciéndoles entender la importancia que tiene la seguridad de la información en toda compañía. Con el apoyo de la alta gerencia, podemos asegurar que el personal de la compañía va a seguir las políticas y procedimientos de seguridad de información que se vayan a publicar como parte del SGSI, así como los controles, lineamientos, estándares, entre otros que se puedan definir.

- (Justino Salinas, 2015) Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO 27001. Para optar por el Título de Ingeniera Informática. Los puntos más resaltantes que se pueden rescatar de este trabajo de tesis son los siguientes: Es necesario establecer una Política de Seguridad de Información que contenga los lineamientos para una eficiente administración de la información con el fin de garantizar la seguridad de los sistemas que satisfaga el requerimiento del negocio y de mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad. Asimismo, la Alta Dirección debe difundir esta política, conocer y dar a conocer a todo el personal que labora en la empresa, de igual manera, el personal es responsable de conocer y cumplir con lo que se especifica.

  En vista de las amenazas, tanto externas como internas, a las que se ve expuesta la inmobiliaria, es necesario establecer roles y responsabilidades dentro de la organización relacionados a Seguridad de Información, para garantizar el cumplimiento de las políticas de seguridad de Información, así como el monitoreo y seguimiento de los riesgos de información. Actualmente, de acuerdo al análisis de riesgos, el status de la seguridad en la inmobiliaria se encuentra a un nivel bajo, esto es porque hay una gran cantidad de riesgos que se consideran como NO aceptables y no tienen controles asociados para mitigarlos es decir se están aceptando riesgos que posiblemente se materialicen en cualquier momento y esto genere pérdidas directas al negocio. Finalmente, al no contar con una regulación específica que exija tomar un modelo de Seguridad de información en la inmobiliaria, ésta deberá trabajar especialmente en el aspecto de cultura de seguridad a todo nivel, pues es necesario concientizar a todo el personal para llevar a cabo el SGSI.

C. A nivel Local:

Habiendo revisado las fuentes bibliográficas y tesis de la localidad de la ciudad de Huánuco en sus respectivas universidades, no se encontró trabajo de investigación parecido o relacionado al presente.

2.2 Bases Teóricas

Seguridad de Información: Es la protección de la confidencialidad, integridad y disponibilidad de la información; es decir, es asegurarse que esta sea accesible solo a las personas autorizadas, sea exacta sin modificaciones no deseadas y que sea accesible a los usuarios cuando lo requieran

Política de Seguridad de Información: (Peltier, 2005), Las políticas de seguridad de información son aquellas normas que se establecen para guiar a los miembros de la organización a resguardar correctamente la seguridad de la información. Peltier, en su libro “Information Security Fundamentals”, considera a las políticas de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos menciona que estas cumplen con 2 roles importantes, un rol interno y otro externo.

- Rol Interno: Ya que se menciona a cada uno de los miembros de la organización que se espera que realicen y como se evaluará el trabajo realizado.
- Rol Externo: Ya que sirve para mostrarle al mundo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo.

ISO: (Wikipedia, 2016), La Organización Internacional de Normalización (del nombre original en inglés, International Organization for Standardization, conocida por las siglas ISO) es una organización para la creación de

estándares internacionales compuesta por diversas organizaciones nacionales de estandarización.

Fundada el 23 de febrero de 1947, la organización promueve el uso de estándares propietarios, industriales y comerciales a nivel mundial. Su sede está en Ginebra, Suiza y hasta el 2015 trabajaba en 196 países. Fue una de las primeras organizaciones a las que se le concedió estatus consultivo general en el Consejo Económico y Social de las Naciones Unidas.

ISO, la Organización Internacional de Estandarización, es una organización independiente y no-gubernamental formada por las organizaciones de estandarización de sus 164 países miembros. Es el mayor desarrollador mundial de estándares internacionales voluntarios y facilita el comercio mundial al proporcionar estándares comunes entre países. Se han establecido cerca de veinte mil estándares cubriendo desde productos manufacturados y tecnología a seguridad alimenticia, agricultura y sanidad.

El uso de estándares facilita la creación de productos y servicios que sean seguros, fiables y de calidad. Los estándares ayudan a los negocios a aumentar la productividad a la vez que minimizan los errores y el gasto. Al permitir comparar directamente productos de diferentes fabricantes, facilita que nuevas compañías puedan entrar en nuevos mercados y ayudar en el desarrollo de un comercio global con bases justas. Los estándares también sirven para proteger a los consumidores y usuarios finales de productos y servicios, asegurando que los productos certificados se ajusten a los mínimos estandarizados internacionalmente.

ISO/IEC 27000: (Organization, 2012), Es una norma internacional que busca dar información general sobre los sistemas de gestión de seguridad de información, así como definir algunos términos que son usados por todos los estándares de la familia 27000. A diferencia de las otras normas de esta familia, esta es de libre distribución y se caracteriza por brindar un listado de las normas mencionadas:

- ISO/IEC 27001: El estándar principal de la familia, brinda los requerimientos para el desarrollo y operación de SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información. Se puede confirmar la eficacia de la implementación del SGSI mediante una auditoria o certificación
- ISO/IEC 27002: Este estándar brinda la guía de implementación de la lista de las mejores prácticas y los más aceptados objetivos de control presentados como anexo en la ISO/IEC 27001, con el objetivo de facilitar la elección de controles para asegurar la seguridad de los activos de información.
- ISO/IEC 27003: Este estándar brinda información y una guía práctica para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI según lo establecido por la ISO/IEC 27001.
- ISO/IEC 27004: Este estándar provee guías prácticas para el uso de métricas que evalúen la efectividad, objetivos de control y controles usados en un SGSI.
- ISO/IEC 27005: Este estándar provee una guía para la gestión de los riesgos de seguridad de información según los requerimientos establecidos por la ISO/IEC 27001.
- ISO/IEC 27006: Este estándar se complementa con el ISO/IEC 17021 y brinda los requerimientos necesarios para la acreditación de la certificación de una organización que certifique los SGSI según la ISO/IEC 27001.
- ISO/IEC 27007: Provee una guía para conducir una auditoria de un SGSI así como las competencias necesarias de los auditores de sistemas de gestión de seguridad complementando la ISO/IEC 19011
- ISO/IEC TR 27008: Es un reporte técnico que brinda una guía para la revisión de la implementación de los controles del SGSI.
- ISO/IEC 27010: Provee una guía para gestionar la seguridad de la información en caso la organización intercambie o comparta información importante, ya sea que pertenezca al sector público o privado, que lo haga nacional o internacionalmente, o en el mismo sector u otros sectores del mercado en el que opera.

- ISO/IEC 27011: Provee una guía para apoyar la implementación de un SGSI en una empresa de telecomunicaciones.
- ISO/IEC 27013: Brinda una guía para la implementación integrada del ISO/IEC 27001 y el ISO/IEC 20000 (gestión de servicios de TI), ya sea implementándolos al mismo tiempo o uno después de otro.
- ISO/IEC 27014: Brinda una guía para conocer los principios y procesos del gobierno de la seguridad de la información, que busca que las organizaciones puedan evaluar, dirigir y monitorear la gestión de la seguridad de la información.
- ISO/IEC TR 27015: Sirve como complemento a las normas de la familia ISO/IEC 27000 para la implementación, mantenimiento y mejora del SGSI en empresas que provean servicios financieros.

- ISO/IEC TR 27016: Es un reporte técnico que brinda una metodología que permite a las organizaciones saber cómo valorar adecuadamente los activos de información identificados, los riesgos potenciales a los activos, apreciar el valor de los controles que protegen a estos activos y determinar el nivel óptimo de recursos que deben ser usados para asegurarlos.
- ISO/IEC 27799:2008: Brinda una guía para apoyar la implementación de un SGSI en las empresas de salud con la adaptación del ISO/IEC 27002 según los requerimientos de este sector.

Sistema de Gestión de Seguridad de la Información: (Asociación Española para la Calidad, 2012), Este sistema se fundamenta en la norma UNE-ISO/IEC 27001:2007, es parte del sistema gerencial general, está basado en un enfoque de riesgo comercial para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de información; sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o ciclo Deming, o más conocido como PDCA (Plan-Do-Check-Act), asimismo se tiene su fundamento en la norma UNE-ISO/IEC 27002:2009 que recoge una lista de controles necesarios para lograr los objetivos de

seguridad de información. El SGSI está diseñado para asegurar una selección de controles de seguridad que protejan los activos de información y den confianza a las partes interesadas. El diseño e implementación del SGSI de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización. Se espera que éstos y sus sistemas de soporte cambien a lo largo del tiempo, así como las situaciones simples requieran soluciones SGSI simples.

Riesgo: (HALVORSON, 2008), Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad. Existe 3 naturalezas del riesgo, estos son los riesgos estratégicos, tácticos y operacionales.

Los riesgos estratégicos son los que pueden estar ligados a la seguridad de la información; sin embargo, se encuentran más orientados a los riesgos de las ganancias y reputación de la organización, ya que se derivan de decisiones estratégicas que han sido tomadas o serán tomadas en la organización.

Los riesgos tácticos son los asociados a los sistemas que vigilan la identificación, control y monitoreo de los riesgos que afectan a la información, son aquellos que afectan indirectamente a la información.

Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías).

Para poder identificar el potencial daño o perdida debido a un riesgo los dueños de los activos pueden responder estas cuatro preguntas:

- ¿Qué puede suceder? (¿Cuál es la amenaza?)
- ¿Qué tan malo puede ser? (¿Cuál es el impacto?)
- ¿Qué tan seguido puede suceder? (¿Cuál es la frecuencia?)
- ¿Qué tan ciertas son las respuestas de las tres primeras preguntas? (¿Cuál es el grado de confianza?)

Administrar Riesgos

Es el uso de la información para estimar el impacto de los riesgos e identificar sus causas, de esta manera se pueden tomar medidas anticipadas ante un incidente.

Control

Los controles son medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales. "Una de las clasificaciones más generalizadas es:

- Preventivos: Reducen las vulnerabilidades.
- Detectivos: Descubren amenazas o escenarios previos a ellas permitiendo activar otros controles.
- Correctivos: Contrarrestan el impacto de la ocurrencia de una amenaza.
- Disuasivos: Reducen la probabilidad de ocurrencia de las amenazas.

SGSI, (ISO 27000, 2005): SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos. El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles.

Documentos de Nivel 1

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Documentos de Nivel 2

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
- Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

- Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.
- Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Control de la documentación

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.

- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

2.3 Definiciones conceptuales

CHECKLIST: Las “listas de control”, “listas de chequeo”, “check-lists” u “hojas de verificación”, son formatos creados para realizar actividades repetitivas, controlar el cumplimiento de una lista de requisitos o recolectar datos ordenadamente y de forma sistemática. Se usan para hacer comprobaciones sistemáticas de actividades o productos asegurándose de que el trabajador o inspector no se olvida de nada importante.

CONFIDENCIALIDAD: Confidencialidad es la cualidad de confidencial (que se dice o hace en confianza y con seguridad recíproca entre dos o más individuos). Se trata de una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas.

DISPONIBILIDAD: la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios.

IMPACTO: Impresión o efecto intenso producido en una persona por una acción o suceso

INTEGRIDAD: Integridad deriva del adjetivo integer, que significa intacto, entero, no tocado o no alcanzado por un mal. Observando las raíces de este adjetivo, este se compone del vocablo in-, que significa no, y otro término de la misma raíz del verbo tangere, que significa tocar o alcanzar, por lo tanto, la integridad es la pureza original y sin contacto o contaminación con un mal o un daño, ya sea físico o moral.

ISO: Es la Organización Internacional para la Estandarización, que regula una serie de normas para fabricación, comercio y comunicación, en todas las ramas industriales.

OUTSOURCING: Outsourcing es un término inglés muy utilizado en el idioma español, pero que no forma parte del diccionario de la Real Academia Española (RAE). Su vocablo equivalente es subcontratación, el contrato que una empresa realiza a otra para que ésta lleve a cabo determinadas tareas que, originalmente, estaban en manos de la primera.

PDCA: El Ciclo PDCA es la sistemática más usada para implantar un sistema de mejora continua.

RIESGO: Es un término proveniente del italiano, idioma que, a su vez, lo adoptó de una palabra del árabe clásico que podría traducirse como “lo que depara la providencia”. El término hace referencia a la proximidad o contingencia de un posible daño.

SGSI: SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

SOA: Se trata de un documento que enlista 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)

VULNERABILIDAD: Vulnerabilidad es la cualidad de vulnerable (que es susceptible de ser lastimado o herido ya sea física o moralmente). El

concepto puede aplicarse a una persona o a un grupo social según su capacidad para prevenir, resistir y sobreponerse de un impacto.

2.4 Hipótesis

Hipótesis General

La implementación del Sistema de Gestión de la Seguridad de la información mejorará la seguridad de la empresa GEOSURVEY S.A.

Hipótesis Específicas

H1: La implementación del Sistema de Gestión de la Seguridad de la información optimizará los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa GEOSURVEY S.A.

H2: La implementación del Sistema de Gestión de la Seguridad de la información optimizará los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa GEOSURVEY S.A.

2.5 Variables

2.5.1 Variable Dependiente

Y: Seguridad en la empresa GEOSURVEY S.A.

2.5.2 Variable Independiente

X: Sistema de Gestión de la Seguridad de la Información

2.6 Operacionalización de Variables

VARIABLES	DIMENSIONES	INDICADORES
Dependiente Seguridad de la empresa GEOSURVEY	*Seguridad con respecto al uso de la información*	• Copias de respaldo de la información • Cifrado de la información • Política de seguridad • Registro de incidentes • Control de acceso a la red
	Seguridad con respecto al uso de los equipos	• Control de acceso a los equipos • Plan de mantenimiento de equipos • Control de inventario de equipos • Control de préstamo de equipos

CAPITULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Tipo de Investigación

3.1.1. Enfoque

El presente estudio de investigación tiene el enfoque cuantitativo ya que según el Doctor Hernández Sampieri en su libro de Metodología de la investigación (2010). Explica que dicho enfoque presenta, un conjunto de procesos, es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos “brincar o eludir” pasos,3 el orden es riguroso, aunque, desde luego, podemos redefinir alguna fase. Parte de una idea, que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica.

3.1.2. Alcance

Esta investigación por su naturaleza es de nivel aplicativo, ya que el objetivo de la investigación es supervisar el monitoreo del proceso o de la intervención que se realiza sobre la población con la finalidad

de mejorar sus condiciones, en este caso mejorar la seguridad en el área de recursos humanos de la Empresa GEOSURVEY.

3.1.3. Diseño

El diseño que presenta el estudio de investigación es el pre experimental de pre y post prueba en el grupo de la investigación, teniendo en cuenta el siguiente diseño:

G O1 X O2

Dónde:

G = Grupo de investigación (áreas de la empresa)
X = Aplicación (SGSI)
O_1 = Pre Observación
O_2 = Post Observación

3.2 Población y Muestra

Con respeto a la población seria considerar a los integrantes del órgano administrativo y operativo de la empresa, en este caso se consideraría a todos aquellos como la muestra representativa ya que la cantidad de trabajadores por área es mínima.

AREA	CANTIDAD
Gerencia General	1
Gerencia Administrativa	2
Área de Contabilidad	1
Área de Marketing y Publicidad	3
Área de ventas.	3
Gerencia Operativa	5
Área de Medio Ambiente y Seguridad	8
Área de Topografía	10
TOTAL	**33**

3.3 Técnicas es instrumentos de recolección de datos

En este estudio de investigación se utilizará el cuestionario de encuesta como principal técnica de recolección de datos, con el propósito de recolectar toda la información de los trabajadores de las diferentes áreas de la empresa GEOSURVEY S.A, relevante con respecto a la seguridad de la información de dicha empresa.

3.4 Técnicas para el procesamiento y análisis de la información

Para realizar la presentación de los datos procedentes del instrumento de recolección, se va emplear la estadística descriptiva, para ello, se va emplear el paquete informático SPSS, para poder procesar y mostrar los resultados de la investigación por medio de los cuadros y gráficos estadísticos.

CAPITULO IV

RESULTADOS

A continuación, se presenta la información descriptiva, para luego presentarse la contrastación de las hipótesis.

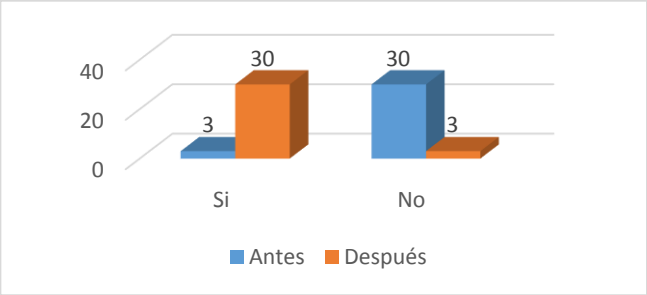
4.1 PROCESAMIENTO DE DATOS

Tabla 4. 1 *Comparación Antes – Después acerca del conocimiento de las políticas de seguridad de información que se aplican en su área de trabajo*

	Antes		Después	
	f	%	f	%
Si	3	9.1	30	90.9
No	30	90.9	3	9.1
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 1 *Comparación Antes – Después acerca del conocimiento de las políticas de seguridad de información que se aplican en su área de trabajo*.



Fuente: Instrumento de medición documental aplicado a la población de estudio

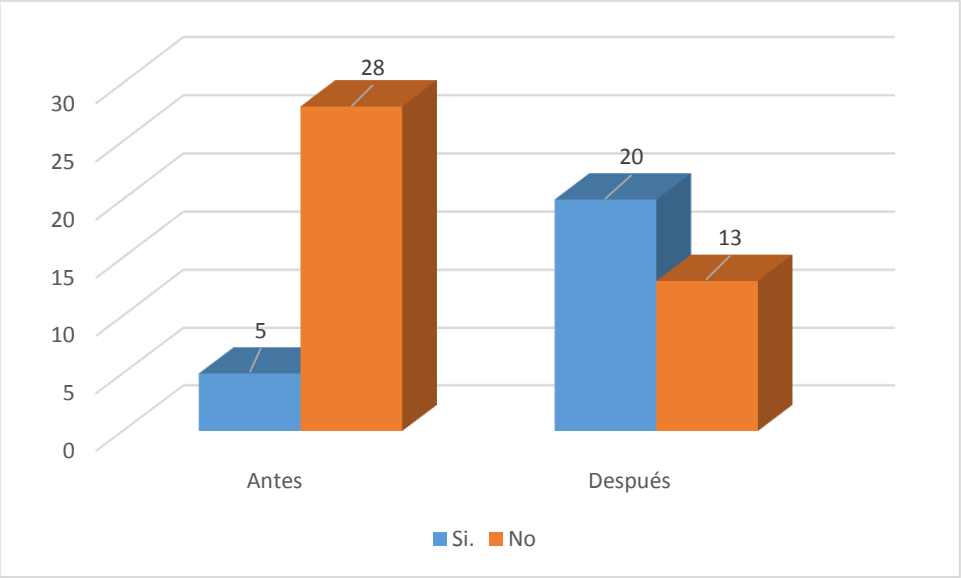
En la tabla y gráfico anterior se observa que la mayoría de los encuestados antes de la intervención desconocían las políticas de seguridad de la información, lo cual se revierte luego de la intervención.

Tabla 4. 2 *Comparación Antes – Después respecto a si se da un mantenimiento periódico de la computadora*.

	Antes		Después	
	f	%	f	%
Si.	5	15.2	20	60.6
No	28	84.8	13	39.4
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 2 *Comparación Antes – Después respecto a si se da un mantenimiento periódico de la computadora.*



Fuente: Instrumento de medición documental aplicado a la población de estudio

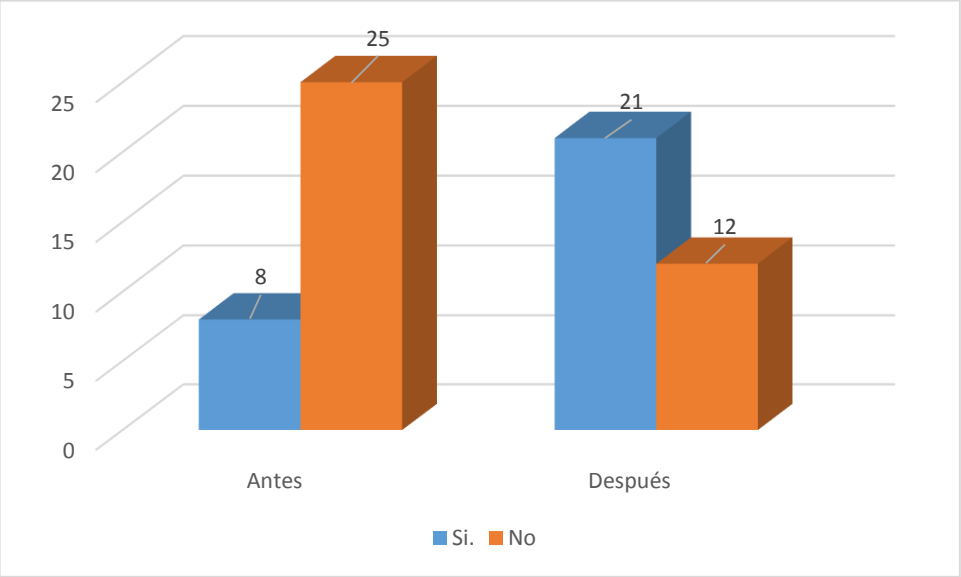
En la tabla y gráfico anterior se observa que las computadoras no recibìan un mantenimiento periódico antes de la intervención, cambiando esta situación luego de la intervención.

Tabla 4. 3 *Comparación Antes – Después respecto a la realización de copias de seguridad de las labores diarias*.

	Antes		Después	
	f	%	f	%
Si.	8	24.2	21	63.6
No	25	75.8	12	36.4
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 3 *Comparación Antes – Después respecto a la realización de copias de seguridad de las labores diarias.*



Fuente: Instrumento de medición documental aplicado a la población de estudio

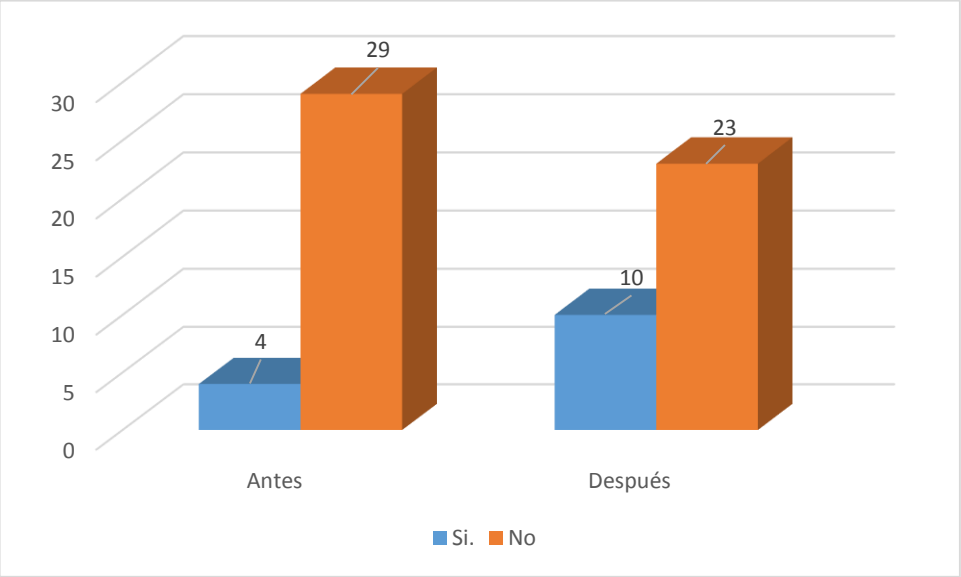
En la tabla y gráfico anterior se observa que la mayoría (75.8%) de los encuestados no solía realizar copias de seguridad de sus labores diarias, sin embargo, esto cambia luego de la intervención (63.6%).

Tabla 4. 4 *Comparación Antes – Después respecto al uso de mecanismo cifrado para su memoria USB*

	Antes		Después	
	f	%	f	%
Si.	4	12.1	10	30.3
No	29	87.9	23	69.7
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 4 *Comparación Antes – Después respecto al uso de mecanismo cifrado para su memoria USB*.



Fuente: Instrumento de medición documental aplicado a la población de estudio

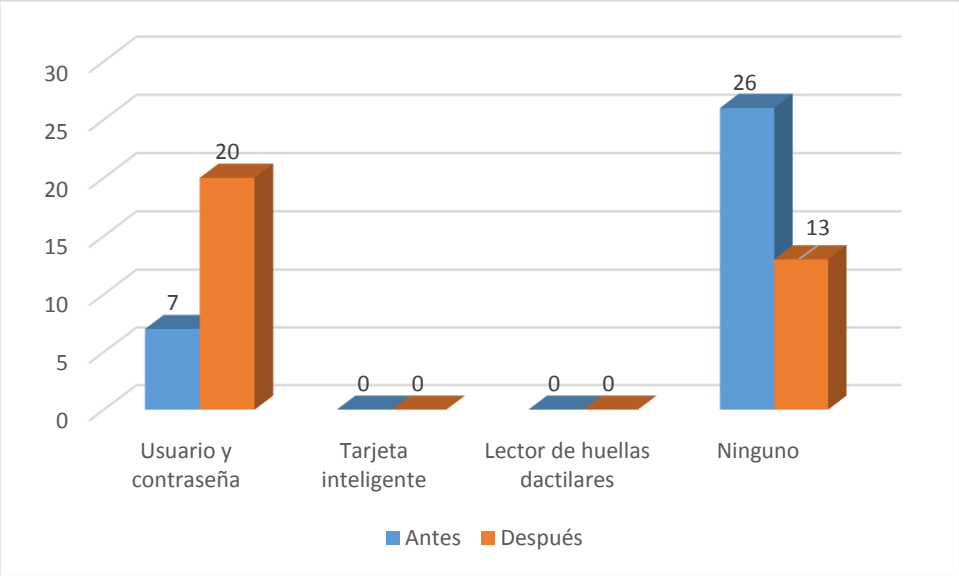
En la tabla y gráfico anterior se observa que era escaso (12.1%) el uso de un mecanismo cifrado para su memoria USB, sin embargo, luego de la intervención hay un incremento del mismo (30.3%)

Tabla 4. 5 *Comparación Antes – Después respecto al mecanismo de control de acceso que se usa al momento de ingresar a la computadora.*

	Antes		Después	
	f	%	f	%
Usuario y contraseña	7	21.2	20	60.6
Tarjeta inteligente	0	0.0	0	0.0
Lector de huellas dactilares	0	0.0	0	0.0
Ninguno	26	78.8	13	33.4
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 5 *Comparación Antes – Después respecto al mecanismo de control de acceso que se usa al momento de ingresar a la computadora.*



Fuente: Instrumento de medición documental aplicado a la población de estudio

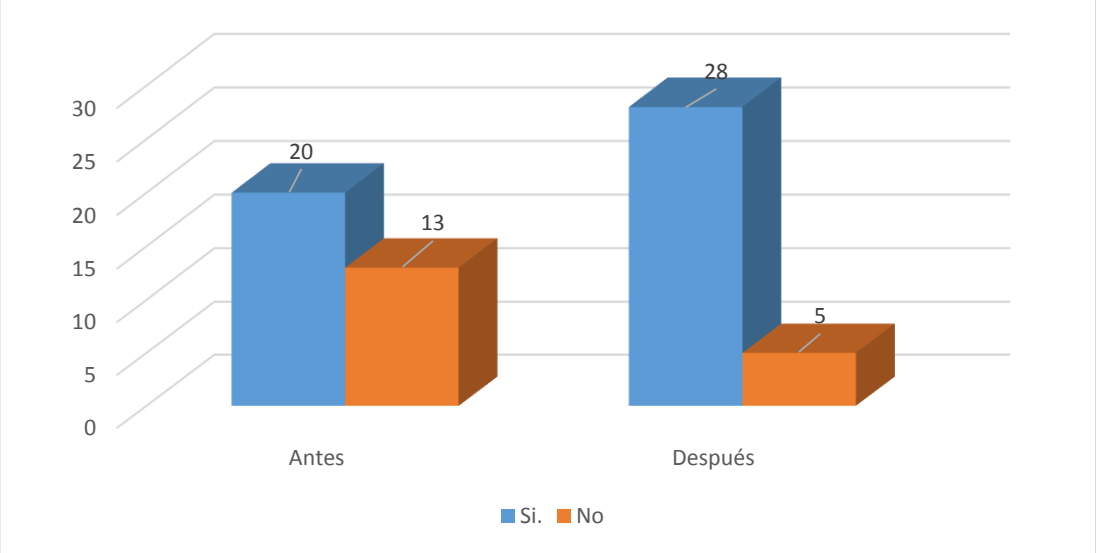
En la tabla y gráfico anterior se observa que ha habido un incremento (de 21.2% a 60.6%) respecto al uso de un mecanismo de control de acceso al ingresar a la computadora, respecto a la evaluación inicial que se hizo previo a la intervención.

Tabla 4. 6 *Comparación Antes – Después respecto al conocimiento sobre el plan de inventario de equipos.*

	Antes		Después	
	f	%	f	%
Si.	3	9.1	28	84.8
No	30	90.9	5	5.2
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 6 *Comparación Antes – Después respecto al conocimiento sobre el plan de inventario de equipos*.



Fuente: Instrumento de medición documental aplicado a la población de estudio

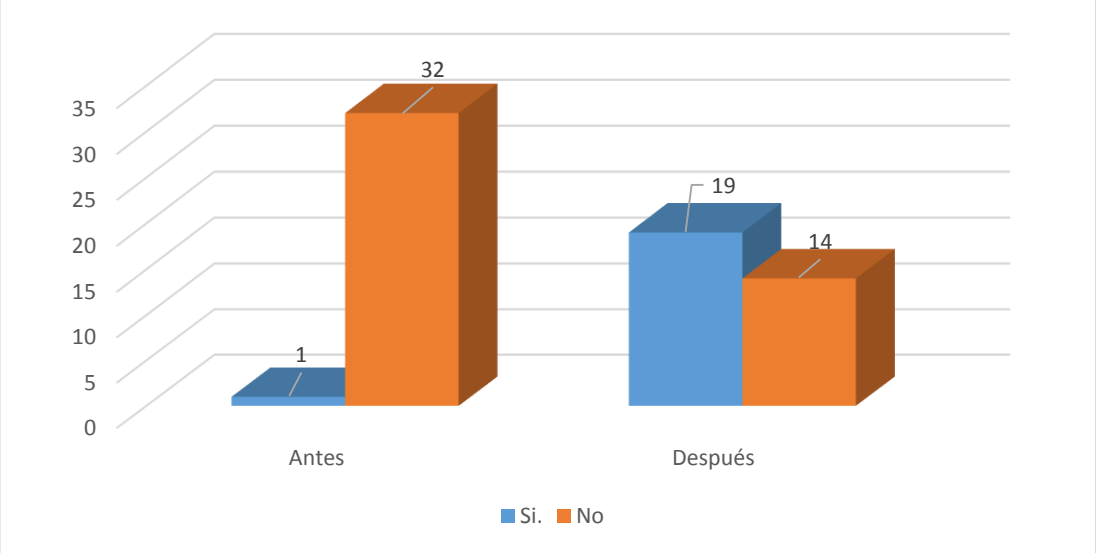
En la tabla y gráfico anterior se observa solo una minoría (9.1%) de la población estudiada tenía conocimiento sobre el plan de inventario de equipos. Sin embargo, esto se revierte luego de la intervención, pues se incrementa al 84.8%

Tabla 4. 7 *Comparación Antes – Después respecto al conocimiento sobre el control de registro de incidentes.*

	Antes		Después	
	f	%	f	%
Si.	1	3.0	19	57.6
No	32	97.0	14	42.4
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 7 *Comparación Antes – Después respecto al conocimiento sobre el control de registro de incidentes*.



Fuente: Instrumento de medición documental aplicado a la población de estudio

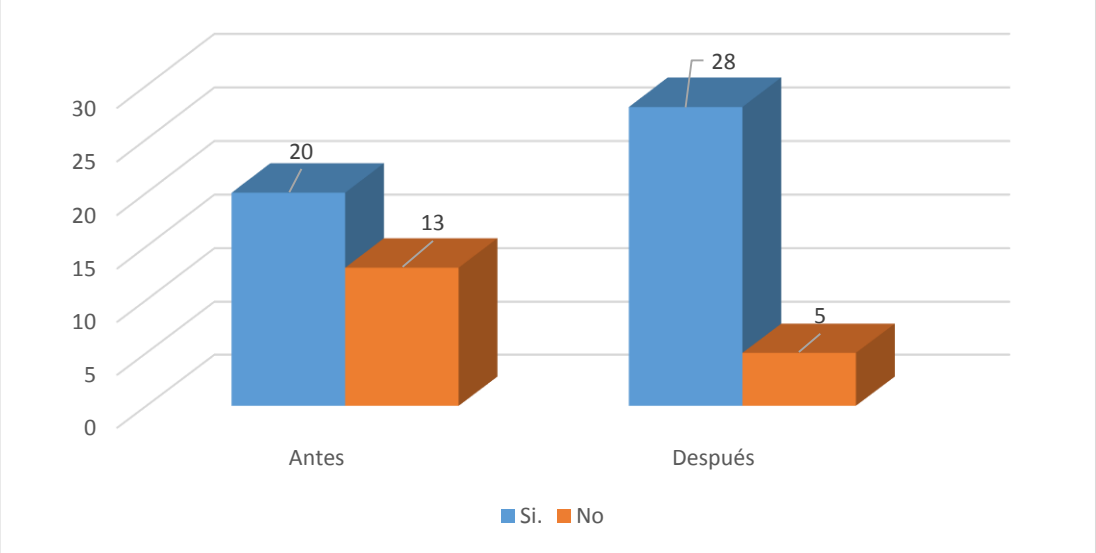
En la tabla y gráfico anterior se observa que la gran mayoría de la población en estudio (97%) desconocía sobre el control de registro de incidentes, pero luego de la intervención hubo una reducción de este porcentaje (42.4%), lo cual es un indicador favorable del estudio.

Tabla 4. 8 *Comparación Antes – Después respecto al conocimiento del control de préstamo de equipos*

	Antes		Después	
	f	%	f	%
Si.	20	60.6	28	84.8
No	13	39.4	5	15.2
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 8 Comparación Antes – Después respecto al conocimiento del control de préstamo de equipos



Fuente: Instrumento de medición documental aplicado a la población de estudio

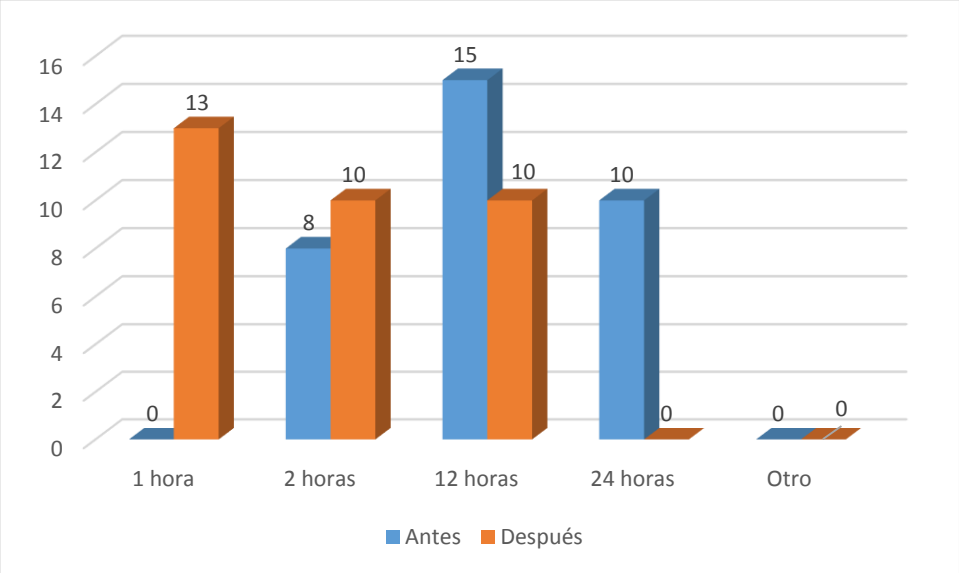
En la tabla y gráfico anterior se observa que se dio una mejora en cuanto al conocimiento que se tenía respecto al control de préstamo de equipos, de 60.6% a 84.8%, lo cual es un indicativo positivo de la efectividad de la intervención.

Tabla 4. 9 *Comparación Antes – Después respecto al tiempo que se demoran en arreglar daños en la computadora.*

	Antes		Después	
	f	%	f	%
1 hora	0	0.0	13	39.4
2 horas	8	24.2	10	30.3
12 horas	15	45.5	10	30.3
24 horas	10	30.3	0	0.0
Otro	0	0.0	0	0.0
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 9 *Comparación Antes – Después respecto al tiempo que se demoran en arreglar daños en la computadora.*



Fuente: Instrumento de medición documental aplicado a la población de estudio

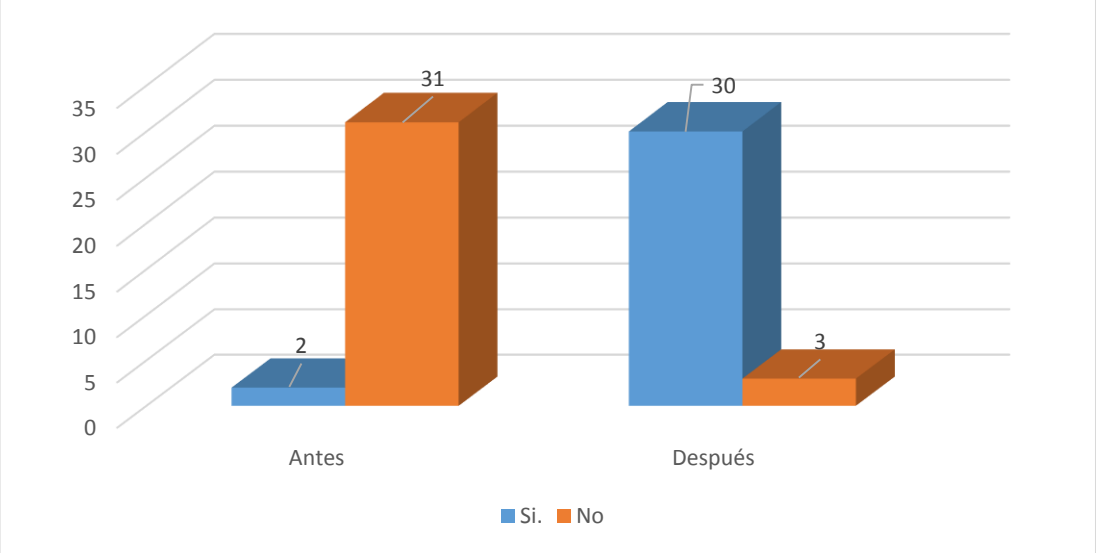
En la tabla y gráfico anterior se observa que se dio una mejora en cuanto al tiempo que se usa para arreglar daños en la computadora, se aprecia que en el 69.7% de los casos, este arreglo se da en hasta 2 horas.

Tabla 4. 10 *Comparación Antes – Después respecto si apaga o bloquea la computadora al salir a almorzar*

	Antes		Después	
	f	%	f	%
Si.	2	6.1	30	90.1
No	31	93.9	3	9.9
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 10 *Comparación Antes – Después respecto si apaga o bloquea la computadora al salir a almorzar*



Fuente: Instrumento de medición documental aplicado a la población de estudio

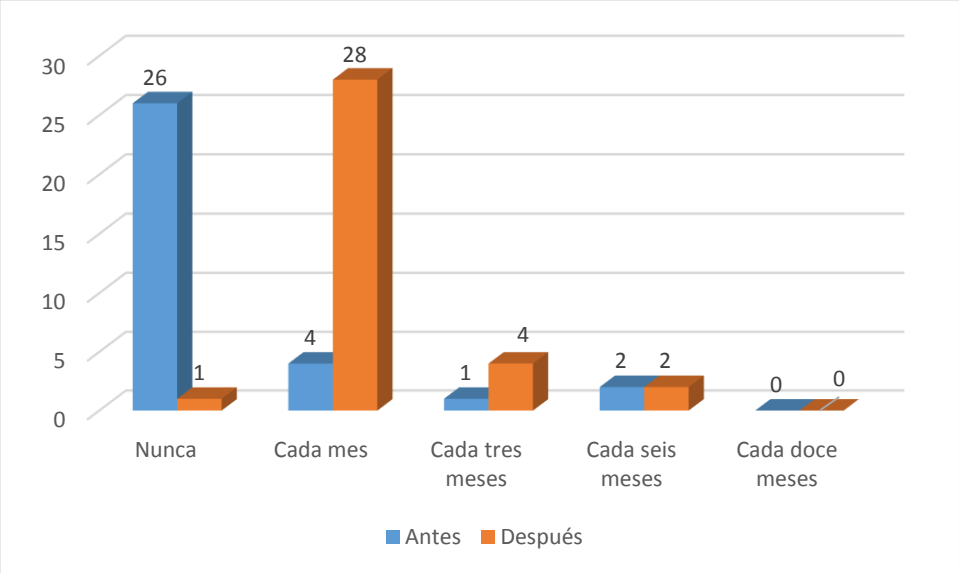
En la tabla y gráfico anterior se observa que la mayoría de los integrantes de la población en estudio no apagaba o bloqueaba su computadora al salir a almorzar, lo cual es revertido al terminar la intervención.

Tabla 4. 11 *Comparación Antes – Después respecto a la frecuencia con la que se cambia la contraseña del equipo.*

	Antes		Después	
	f	%	f	%
Nunca	26	78.8	1	3.0
Cada mes	4	12.1	28	84.8
Cada tres meses	1	3.0	4	12.1
Cada seis meses	2	6.1	2	6.1
Cada doce meses	0	0.0	0	0.0
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 11 *Comparación Antes – Después respecto a la frecuencia con la que se cambia la contraseña del equipo.*



Fuente: Instrumento de medición documental aplicado a la población de estudio

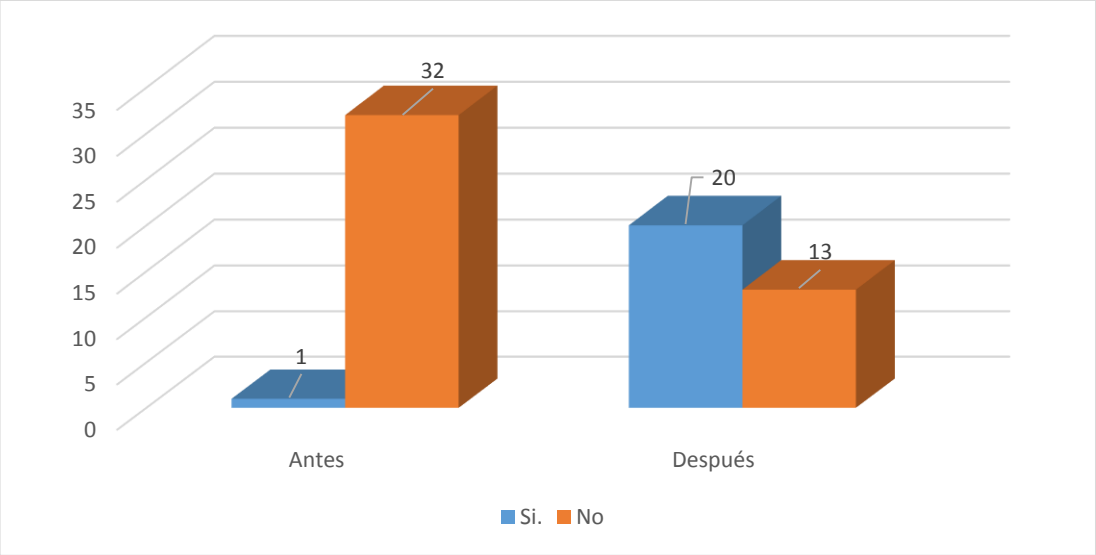
En la tabla y gráfico anterior se observa que antes de la intervención, la mayoría de los integrantes de la población en estudio, no cambiaban su contraseña; luego de la intervención, la mayoría empezó a hacerlo cada mes.

Tabla 4. 12 *Comparación Antes – Después respecto a si usan la misma contraseña para todos los servicios que frecuentan en Internet (Facebook, Correo, etc.)*

	Antes		Después	
	f	%	f	%
Si.	29	87.9	5	15.2
No	4	12.1	28	84.8
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 12 *Comparación Antes – Después respecto a si usan la misma contraseña para todos los servicios que frecuentan en Internet (Facebook, Correo, etc.)*



Fuente: Instrumento de medición documental aplicado a la población de estudio

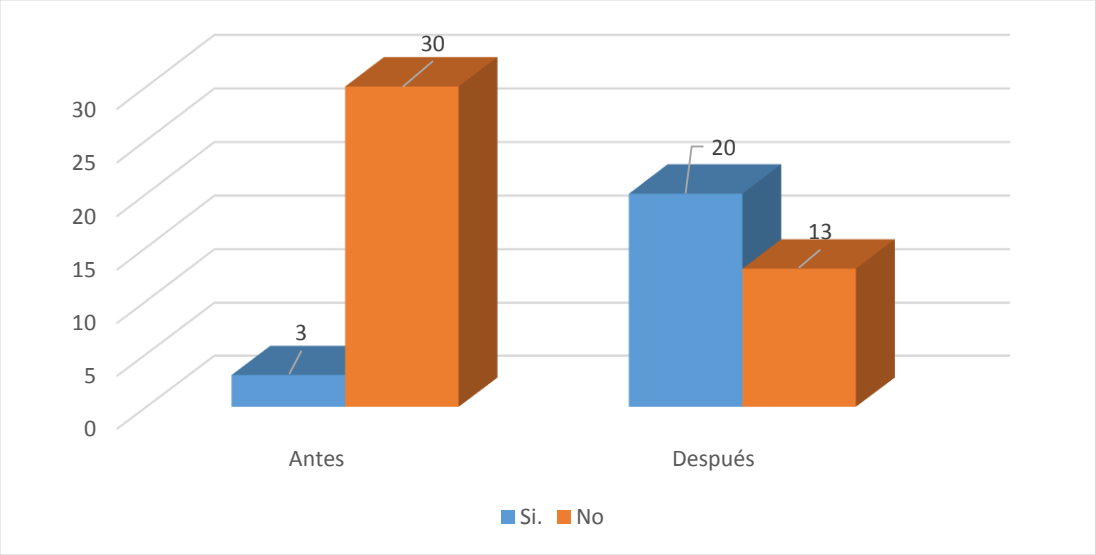
En la tabla y gráfico anterior observamos que la mayoría (87.9%) de los encuestados, solìan usar la misma contraseña para los otros servicios en Internet que frecuentaban, lo cual se revierte después de la intervención.

Tabla 4. 13 *Comparación Antes – Después respecto a si tienen restricción para ingresar a Internet.*

	Antes		Después	
	f	%	f	%
Si.	3	9.1	20	60.6
No	30	90.9	13	39.4
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 13 *Comparación Antes – Después respecto a si tienen restricción para ingresar a Internet.*



Fuente: Instrumento de medición documental aplicado a la población de estudio

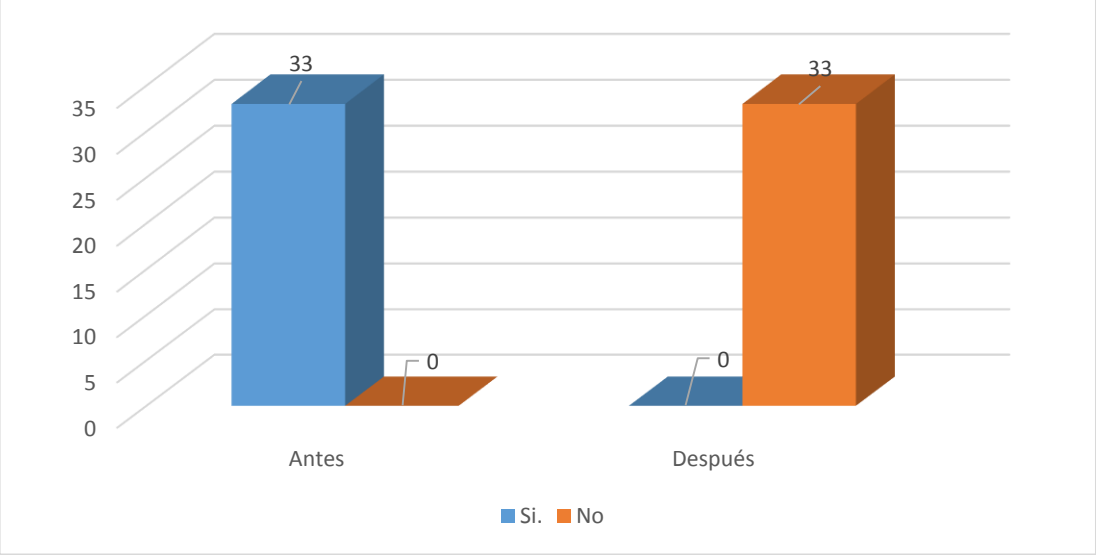
En la tabla y gráfico anterior se observa que el acceso a Internet no es algo restringido para la población en estudio previo a la intervención, luego de ella, existe mayor restricción al ingreso a Internet.

Tabla 4. 14 *Comparación Antes – Después respecto al mecanismo de control que se aplica al momento de acceder a recursos compartidos en la red*

	Antes		Después	
	f	%	f	%
Ninguno	33	100.0	0	0.0
Nombre de usuario y contraseña	0	0.0	33	100.0
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 14 *Comparación Antes – Después respecto al mecanismo de control que se aplica al momento de acceder a recursos compartidos en la red*



Fuente: Instrumento de medición documental aplicado a la población de estudio

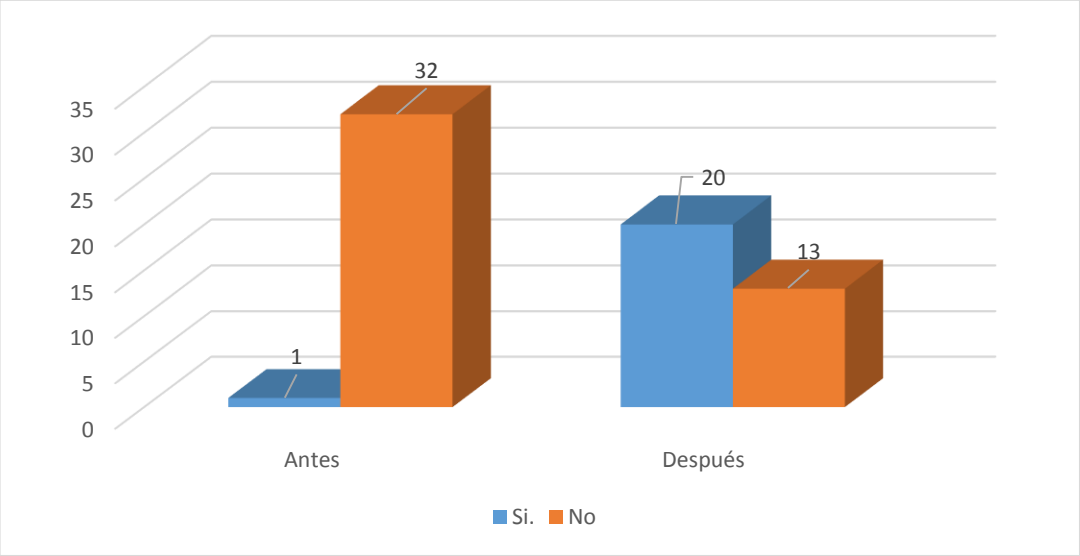
En la tabla y gráfico anterior se revierte totalmente respecto al mecanismo de control que se aplica al momento de acceder a recursos compartidos en la red, existiendo una mejora del 100%

Tabla 4. 15 *Comparación Antes – Después respecto a si se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información de la empresa*

	Antes		Después	
	f	%	f	%
Si.	1	3.0	20	60.6
No	32	97.0	13	39.4
Total	33	100.0	33	100.0

Fuente: Instrumento de medición documental aplicado a la población de estudio

Ilustración 4. 15 *Comparación Antes – Después respecto a si se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información de la empresa*



Fuente: Instrumento de medición documental aplicado a la población de estudio

En la tabla y gráfico anterior se observa que se empezó a llevar un mejor registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información de la empresa después de la intervención.

4.2 CONTRASTACION DE HIPOTESIS Y PRUEBA DE HIPOTESIS

Prueba de hipótesis Comparación antes – después: Optimización de los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa

Se ha evaluado la optimización de los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa GEOSURVEY S.A de la ciudad de Lima

El ritual de la significancia estadística

1	**Plantear Hipótesis** Ho: La implementación del Sistema de Gestión de la Seguridad de la información no optimiza los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa GEOSURVEY S.A. H1: La implementación del Sistema de Gestión de la Seguridad de la información optimiza los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa GEOSURVEY S.A.
2	**Establecer un nivel de significancia** Nivel de Significancia (alfa) α = 5% = 0.05
3	**Seleccionar procedimiento estadístico:** Rangos de Wilcoxon
4	**Valor de P=** 7,4356E-7 = 0.0% **Lectura del p-valor:** Con una probabilidad de error del 0.0% la implementación del Sistema de Gestión de la Seguridad de la información optimiza los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa GEOSURVEY S.A.
5	**Toma de decisiones** La implementación del Sistema de Gestión de la Seguridad de la información optimiza los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa GEOSURVEY S.A.

Interpretación

Se logró una optimización en los procesos de capacitación y formación de seguridad en cuanto al uso de la información en la empresa GEOSURVEY tras la intervención.

Prueba de hipótesis Comparación antes – después: Optimización de los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa

Se ha evaluado la Optimización de los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa

El ritual de la significancia estadística

1	**Plantear Hipótesis** Ho: La implementación del Sistema de Gestión de la Seguridad de la información no optimiza los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa GEOSURVEY S.A. H1: La implementación del Sistema de Gestión de la Seguridad de la información optimiza los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa GEOSURVEY S.A.
2	**Establecer un nivel de significancia** Nivel de Significancia (alfa) α = 5% = 0.05
3	**Seleccionar procedimiento estadístico:** Rangos de Wilcoxon
4	**Valor de P=** 4,3091E-7 = 0.0% **Lectura del p-valor:** Con una probabilidad de error del 0.0% la implementación del Sistema de Gestión de la Seguridad de la información optimiza los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa GEOSURVEY S.A.
5	**Toma de decisiones** La implementación del Sistema de Gestión de la Seguridad de la información optimiza los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa GEOSURVEY S.A.

Interpretación

Se logró una optimización en los procesos de capacitación y formación de seguridad en cuanto al uso de los equipos en la empresa GEOSURVEY tras la intervención.

Prueba de hipótesis Comparación antes – después: Mejora del sistema de gestión de seguridad de la información en el área de Recursos Humanos de la empresa GEOSURVEY S.A

Se ha evaluado la mejora del sistema de gestión de seguridad de la información en el área de Recursos Humanos de la empresa GEOSURVEY S.A

El ritual de la significancia estadística

1	**Plantear Hipótesis** Ho: La implementación del Sistema de Gestión de la Seguridad de la información no mejora la labor del área de recursos humanos de la empresa GEOSURVEY S.A. H1: La implementación del Sistema de Gestión de la Seguridad de la información mejora la labor del área de recursos humanos de la empresa GEOSURVEY S.A.
2	**Establecer un nivel de significancia** Nivel de Significancia (alfa) α = 5% = 0.05
3	**Seleccionar procedimiento estadístico:** Rangos de Wilcoxon
4	**Valor de P=** 4,8758E-7= 0.0% **Lectura del p-valor:** Con una probabilidad de error del 0.0% La implementación del Sistema de Gestión de la Seguridad de la información mejora la labor del área de recursos humanos de la empresa GEOSURVEY S.A.
5	**Toma de decisiones** La implementación del Sistema de Gestión de la Seguridad de la información mejora la labor del área de recursos humanos de la empresa GEOSURVEY S.A

Interpretación

La intervención en la empresa GEOSURVEY resultó en una mejora del sistema de gestión de seguridad de la información en su área de Recursos Humanos

CAPÍTULO V

DISCUSIÓN DE RESULTADOS

En esta sección del informe final de la investigación se da a conocer la discusión, interpretación, y explicación del resultado de la aplicación del Sistema de Gestión de Seguridad de la información a la empresa Geosurvey de la ciudad de Lima.

El conocimiento sobre las políticas de seguridad en la empresa era mínimo antes de la aplicación, un 9.1% de la población solo tenía referencia de algunas normas laborales en cuanto al uso de los activos de la empresa, específicamente a las tecnologías de la información y comunicación, estas normas solo han sido mencionadas por los jefes de área o el gerente de la empresa pero mas no habían sido plasmadas en un documento; ya posteriormente a la aplicación del SGSI se obtuvo que un 90,0% de la población ya tenía de conocimiento la existencia de una política de seguridad y que en si era un documento al cual se podía consultar ya que se realizaron reuniones de capacitación para dar a conocer todas las normas inmersas en la política de seguridad.

En la fase previa a la aplicación de la investigación no se contaba con un plan de mantenimiento de equipos, este plan también inmerso dentro de la política de seguridad, esto también género que el 84.8% de los trabajadores hayan contestado negativamente en cuanto al mantenimiento periódico de la computadora, esto es porque previa a la aplicación no se contaba con un plan de mantenimiento es así que las maquinas funcionaban expuestos a riesgos, incluso infectadas, con el software desactualizado y parte de hardware dañado u obsoleto, esto dificultaba la labores diarias de los trabajadores en cuanto al uso de los equipos, es por eso que luego de haber realizado la implementación del SGSI, se determinó los riesgos y se pudo aplicar los controles necesarios para minimizar cada riesgo valorado, es así como el 60.6% de los trabajadores afirmaron que si recibían el mantenimiento preventivo y correctivo a tiempo de la máquinas asignadas, esto gracias al conocimiento del plan de mantenimiento al personal indicado de las tareas de soporte y mantenimiento.

También con la aplicación del SGSI se puedo lograr que el 63.6% de los trabajadores hagan las copias de seguridad constantemente de la información que manejaban, se logró así que del total que 21 trabajadores hacían copias de seguridad de su información en contraste de los 8 restantes que por motivos ajenos de las capacitaciones no pudieron recibir la información adecuada para realizar el procedimiento de resguardo, pero esto se subsana al momento de transferir el conocimiento entre ellos y hacerlos partícipes de dicho procedimiento.

El mayor temor de las empresas es la perdida de información sensible por parte de sus propios trabajadores, es así que antes de la solución del problema los trabajadores extraviaban sus dispositivos de almacenamiento extraíbles, como consecuencia información sensible llegaba a manos desconocidas, es por eso que el 87.9% de los trabajadores no aplicaban técnicas de cifrados para sus dispositivos, creando una vulnerabilidad de perdida de información, por lo tanto una vez aplicado la solución, el SGSI, solo decremento a un 69.7% la cantidad total de trabajadores que no aplicaban dicho mecanismo, es así que solo se pudo capacitar a 10 trabajadores para que puedan realizar el proceso de encriptado del dispositivo esto se entiende que 10 de ellos solo manejan información sensible de su área correspondiente.

En relación a los controles de acceso para poder acceder al computador, solo el 21.2% de los trabajadores configuraron en sus máquinas el ingreso al sistema con usuario y contraseña, esto es que antes la inexistencia de la política de seguridad solo ese porcentaje lo hacía por conocimiento, el resto simplemente por desinformación, ya después de haber realizado la implementación de la política de seguridad y las correspondientes capacitaciones, el 60,6% ya contaba con sus equipos seguros al momento de accederlos mediante el uso del control de acceso usando un nombre de usuario y contraseña.

Cuando se suscitan los incidentes que ponen en riesgo a los activos de la empresa, simplemente no se llevaba la cuenta de esto ni se registraban antes de la implementación del SGSI, es por eso que solo el 3% afirmo que en cierta forma conocía de la existencia de un sistema de gestión de incidentes mientras el que después de la implementación se dio a conocer el sistema de gestión de

incidentes el cual estaba disponible para cualquier trabajador para que registre en cualquier momento el incidente suscitado, dando a un total del 57.6% de los trabajadores ya con el conocimiento de la existencia de dicho sistema. Esto también influyo que los trabajadores el 84% de ellos conocían del documento para realizar el préstamo de equipos cada vez que salía a campo.

En cuanto a las medidas correctivas ante de la implementación del sistema los trabajadores del área de soporte se demoraban entre 12 a 24 horas para solucionar un problema esto es un total del 75.8% de los trabajadores que dieron esa información, mientras que después de la aplicación el tiempo promedio era entre 1 y 2 horas como máximo, esto reflejado en el 69.7% de las respuestas de los trabajadores en la encuesta.

También se logró que los trabajadores tomen conciencia de que tan importante es dejar bloqueado el equipo antes de salir o irse a almorzar o hacer alguna diligencia, de los cuales se logró que el 90% de ellos realizaba el bloqueo de sus equipos al retirarse, mientras que antes de la implantación del sistema solo el 6.1% lo hacía.

Un aspecto muy importante también fue el de haber concientizado a los trabajadores que cada mes deberían cambiar sus contraseñas de los servicios en red utilizados, es así que los resultados nos muestran un 84.8% de los trabajadores lo hacían mensualmente el cambio de sus contraseñas en contraposición al 78.8% previo a la aplicación del sistema que nunca lo hacían. Así mismo esto influyo también a que los trabajadores utilicen diferentes contraseñas para diferentes servicios y no solo una contraseña general para todos los servicios, y los resultados reflejan que solo el 15.2% de los encuestados tomo conciencia y usaba contraseñas diferentes para cada servicio.

Las políticas de seguridad y a la aplicación de los controles del ISO 27002 también ayudo a incrementar la productividad de los trabajadores por medio de la restricción de sitio web de ocio en los cuales la mayoría entretenía su tiempo laboral dejando de lados sus actividades diarias, es así que en la encuesta se obtuvo que el 60.6% de los trabajadores tenían restricción al momento de acceder a páginas distractoras como redes sociales y juegos en línea.

El acceso a los recursos conectados en red después de la implementación del SGSI, se logró que el 100% de los trabajadores accedan a la red mediante el ingreso de un nombre de usuario y contraseña, anteriormente a esto no se contaba con dicha protección.

Finalmente podríamos afirmar en base a la contratación de hipótesis que se logró una optimización en los procesos de capacitación y formación de seguridad en cuanto al uso de la información, el uso de los equipos en la empresa tras la intervención concluyendo que la intervención en la empresa GEOSURVEY resultó en una mejora del sistema de gestión de seguridad de la información en su área de Recursos Humanos.

CONCLUSIONES

- ✓ Optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa.

- ✓ Optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa.

- ✓ Se logró una optimización en los procesos de capacitación y formación de seguridad en cuanto al uso de la información en la empresa GEOSURVEY tras la intervención.

- ✓ Se logró una optimización en los procesos de capacitación y formación de seguridad en cuanto al uso de los equipos en la empresa GEOSURVEY tras la intervención.

- ✓ La intervención en la empresa GEOSURVEY resultó en una mejora del sistema de gestión de seguridad de la información en su área de Recursos Humanos

RECOMENDACIONES

- ✓ Se recomienda al personal directivo continuar con los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa.

- ✓ Realizar continuos talleres de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa.

- ✓ Continuar con la concientización hacia los trabajadores la importancia de la información como activo dentro de la empresa.

- ✓ Realizar continuamente la fase ACT, del SGSI, esto es actuar siempre mantener actualizados los planes y registrar siempre las incidencias suscitadas.

- ✓ Perseguir a futuro la acreditación por la empresa certificadora y lograr el la certificación ISO 27001 y 27002

REFERENCIAS BIBLIOGRÁFICAS

Aguirre Mollehuanca, D. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.*

Aliaga Flores, L. (2013). *Diseño de un sistema de gestión de seguridad de información para un instituto educativo. .*

Ampuero Chang, C. (2011). *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros.*

Asociación Española para la Calidad, A. (2012). *La norma ISO 27001. Seguridad de la información. Garantía de confidencialidad, integridad y disponibilidad de la información.* España: Revista Calidad.

Bunge, M. (1999). *Diccionario de filosofía.* México: Ibidem.

HALVORSON, N. (2008). *Information Risk Management: A Process Approach to Risk Diagnosis and Treatment.* USA: Auerbach Publications.

ISO 27000. (2005). *El portal de ISO 27001 en Español.* Obtenido de http://www.iso27000.es/download/doc_sgsi_all.pdf

J., A. C. (2013). *Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda.*

Justino Salinas, Z. (2015). *Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO 27001.*

Organization, I. S. (2012). *IEC 27000.* Second Edition.

Pallas Mega, G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.*

Peltier, T. R. (2005). *Information Security Fundamentals.* USA: Auerbach Publications.

Real Academia, E. (2014). *Diccionario de la lengua española.* España: Espasa.

ANEXOS

FORMULARIO DE APLICABILIDAD DEL SGSI

Instrucciones: Debe responder las preguntas de manera honesta y responsable. Sus respuestas deben ser claras y concisas.

1. ¿Conoce las políticas de Seguridad de Información que se aplican en su área de trabajo?
   ☐ Si

   ☐ No

2. ¿Su computadora recibe mantenimiento de manera periódica?

   ☐ Si

   ☐ No

3. ¿Realiza copias de información de su labor diaria?

   ☐ Si

   ☐ No

4. ¿Utiliza mecanismo de cifrado para su memoria USB?

   ☐ Si

   ☐ No

5. ¿Qué mecanismo de control de acceso se aplica al momento de ingresar a la computadora?

   ☐ Ingreso de nombre de usuario y contraseña

   ☐ Tarjeta inteligente

   ☐ Lector de huellas dactilares

   ☐ Ninguno

6. ¿Tiene conocimiento sobre el plan de inventario de equipos?

   ☐ Si

   ☐ No

7. ¿Tiene conocimiento sobre el control registros de incidentes?

   ☐ Si

   ☐ No

8. ¿Tiene conocimiento sobre el control de préstamos de equipos?

   ☐ Si

   ☐ No

9. ¿En caso de daño de su computadora, que tiempo se demoran en arreglarlo?

   ☐ 1 hora

   ☐ 2 horas

   ☐ 12 horas

   ☐ 24 horas

   ☐ Otros

10. ¿Ud. apaga o bloque su computadora cuando se va almorzar?

    ☐ Si

    ☐ No

11. ¿Con que frecuencia cambia su contraseña del equipo?

    ☐ Nunca

    ☐ Cada mes

    ☐ Cada 3 meses

    ☐ Cada 6 meses

☐ Cada 12 meses

12. ¿Utiliza la misma contraseña para todos los servicios que usa en Internet (Facebook, Correo, etc.)?

☐ Si

☐ No

13. ¿Tiene alguna restricción para ingresar a los servicios de Internet?

☐ Si

☐ No

14. ¿Qué mecanismo de control se aplica al momento de acceder a recursos compartidos en la red?

☐ Ninguno

☐ Nombre de usuario y contraseña

15. ¿Se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información de la empresa?

☐ Si

☐ No

DISEÑO E IMPLEMENTACIÓN DE UN SGSI ISO 27001 PARA LA MEJORA DE LA SEGURIDAD DEL AREA DE RECURSOS HUMANOS DE LA EMPRESA GEOSURVEY DE LA CIUDAD DE LIMA

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
Problema General ¿De qué forma la implementación del Sistema de Gestión de la Seguridad del área de recursos humanos de la información mejorará la seguridad de la empresa GEOSURVEY S.A.?	**Objetivo General** Determinar la mejora de implementar un sistema de gestión de seguridad de la información en la seguridad del área de recursos humanos de la empresa GEOSURVEY S.A.	**Hipótesis General** La implementación del Sistema de Gestión de la Seguridad de la información mejorará la seguridad del área de recursos humanos de la empresa GEOSURVEY S.A.	**Dependiente** Seguridad de Área de recursos humanos	***Seguridad con respecto al uso de la información***	**Copias de respaldo de la información** **Cifrado de la información** **Política de seguridad** **Registro de incidentes** **Control de acceso a la red**	**Enfoque:** Cuantitativo **Tipo:** Aplicativo **Diseño:** Pre-Experimental
				Seguridad con respecto al uso de los equipos	**Control de acceso a los equipos** **Plan de mantenimiento de equipos** **Control de inventario de equipos** **Control de préstamo de equipos**	
Problema Específico **P.E 01:** ¿De qué forma se podrá optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa GEOSURVEY SA? **P.E 02:** ¿De qué forma se podrá optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa GEOSURVEY SA?	**Objetivos Específico** **O.E.1:** Optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa. **O.E.2:** Optimizar los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa. .	**Hipótesis Especifica** **H1:** La implementación del Sistema de Gestión de la Seguridad de la información optimizará los procesos de capacitación y de formación de la seguridad en cuanto al uso de la información de la empresa GEOSURVEY S.A. **H2:** La implementación del Sistema de Gestión de la Seguridad de la información optimizará los procesos de capacitación y de formación de la seguridad en cuanto al uso de los equipos de la empresa GEOSURVEY S.A.	**Independiente** SGSI ISO 27002	.		**Esquema del Diseño:** G: O1 X O2 •Donde: G= Grupo de investigación (Trabajadores del área de recursos humanos) X= Aplicación de la variable O1, O2, = Medición de Observación

UNIVERSIDAD DE HUANUCO

Facultad de Ingeniería

P.A. DE INGENIERÍA DE SISTEMAS E INFORMATICA

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO (A) DE SISTEMAS E INFORMÁTICA

En la ciudad de Huánuco, siendo las 17:10 horas del día 19 del mes de DICIEMBRE del año 2017, en el Auditorio de la Facultad de Ingeniería, en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, se reunieron el **Jurado Calificador** integrado por los docentes:

HECTOR RAUL ZACARIAS VENTURA (Presidente)

PAOLO EDVER SOLIS JARA. (Secretario)

JOSE ANTONIO NUÑEZ VICENTE (Vocal)

Nombrados mediante la Resolución N° 835 - 2017 - D - FI - UDH, para evaluar la **Tesis** intitulada:

"DISEÑO E IMPLEMENTACION DE UN SISTEMA GESTON DE SEGURIDAD DE LA INFORMACIÓN ISO 27001 PARA LA MEJORA DE LA SEGURIDAD DEL AREA DE RECURSOS HUMANOS DE LA EMPRESA BIOSURVEY DE LA CIUDAD DE LIMA.",

presentada por el (la) Bachiller EHYTEL CELESTINO VILCA MOSQUERA para optar el Título Profesional de Ingeniero (a) de Sistemas e Informática.

Dicho acto de sustentación se desarrolló en dos etapas: exposición y absolución de preguntas: precediéndose luego a la evaluación por parte de los miembros del Jurado.

Habiendo absuelto las objeciones que le fueron formuladas por los miembros del Jurado y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo (a) APROBADO por UNANIMIDAD con el calificativo cuantitativo de 12 y cualitativo de SUFICIENTE (Art. 47)

Siendo las 18:15 horas del día 19 del mes de DICIEMBRE del año 2017, los miembros del Jurado Calificador firman la presente Acta en señal de conformidad.

Presidente

Secretario

Vocal