SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001 PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

COMPUTER SECURITY APPLYING THE ISO / IEC 27001 STANDARD FOR THE PROTECTION OF INFORMATION ASSETS

Delgado Saavedra Martha Mellissa. [1]
Vásquez Zevallos José Luis. [2]
Nauca Torres Enrique Santos.[3]

Fecha Recepción: 13 DIC 2020
Fecha Aceptación: 16 DIC2020

Resumen

Hoy en día las organizaciones están propensos a delincuentes informáticos y a la vez los sabotajes por parte de sus colaboradores, es por ello que la presente investigación tiene como propósito direccionar la protección de activos de información de una empresa privada mediante la seguridad informática aplicando la Norma ISO/IEC 27001, de tipo de estudio aplicado , con diseño no experimental, con una población y muestra se usó técnicas como encuesta ,entrevista y observación, por otro lado se aplicó la metodología Magerit para el análisis de los riesgos o amenazas que padece la empresa permitiendo capacitar a los colaboradores y así logrando un cambio favorable de 0% a 25% de excelente respecto al nivel de conocimiento de la norma ya mencionada. Por último, se estableció políticas de seguridad y sanciones si se incumplen las normas ya establecidas.

Palabras clave: Norma ISO/IEC 27001, Magerit, metodología, activos

Abstract

Today organizations are prone to computer criminals and at the same time sabotage by their collaborators, that is why the present investigation aims to direct the protection of information assets of a private company through computer security applying the ISO Standard / IEC 27001, applied study type, with non-experimental design, with a population and sample, techniques such as survey, interview and observation were used, on the other hand, the Magerit methodology was applied to analyze the risks or threats suffered by the company allowing to train employees and thus achieving a favorable change from 0% to 25% of excellent with respect to the level of knowledge of the aforementioned standard. Finally, security policies and sanctions were established if the rules already established are breached.

Keywords: ISO / IEC 27001 standard, Magerit, methodology, assets

I. Introducción

Hoy en día la seguridad de la información se ha convertido en el activo más importante para las empresas y por ende hay que tener en cuenta que las vulnerabilidades aumentan y los ciberataques son más frecuentes debido a ello es que en la actualidad ya existe varias formas de salvaguardar la información. La seguridad de información abarca un conjunto de técnicas y medidas para vigilar todos los datos que se maneja y asegurarse que no escape del sistema establecido por la empresa. Según Romero (2018) nos informa que seleccionar los controles recomendados por la norma técnica peruana NTP ISO/IEC 27001:2014 servirán para las vulnerabilidades encontradas e identificar las de alto índice de riesgo y el tratamiento que se le

[1] Ingeniero de Sistemas – Universidad de Lambayeque - ds.melisza@gmail.com
[2] Ingeniero de Sistemas – Universidad de Lambayeque - 21luisvz@gmail.com
[3] Ingeniero de Sistemas y Computación - Universidad de Lambayeque – snauca@gmail.com -
https://orcid.org/0000-0002-5052-1723

deben dar a través de planes de acciones correctivas y preventivas. Por otro lado Fernández (2015) nos informa en que la definición de políticas de seguridad de la información, reglamentos y controles debidamente formalizados, se ha logrado establecer un nivel de conocimiento, concientización y cultura en el personal de La Caja orientado hacia el control y la seguridad de la información. Por lo tanto, el diseñar un modelo adaptado a la norma ISO/IEC 27001 para la protección de los activos de una organización responderá a la siguiente formulación ¿De qué manera la norma ISO/IEC 27001 le permite a una empresa privada disponer de un marco normativo para la gestión de seguridad?, En la empresa investigada

Se evidencio en que no cuenta con un modelo adaptado en base a la norma ISO/IEC 27001, es por ello con la propuesta mejorará la comunicación entre los trabajadores dentro de la empresa, ya que se pretende solucionar un problema en la organización orientada al nivel de seguridad en el uso de sus sistemas de información que manejan en sus actividades, generando como consecuencia una mejora en el uso de las aplicaciones y mayores niveles de seguridad en los sistemas de información respectivamente. Se justificó en lo tecnológico lo cual se direcciona a la seguridad de los sistemas de información, como también auditoria ya que se pretende solucionar un problema en la organización orientada al nivel de seguridad en el uso de sus sistemas de información

II. Métodos y Materiales

Se basó en un método deductivo e inductivo, tipo de estudio aplicada, es decir implica la implementación de mecanismos de seguridad informática por parte de los investigadores, orientado a mejorar la falta de seguridad de la información siendo este uno de los activos más importantes, para lo cual se aplicará la norma ISO 27001 y asimismo de diseño no experimental. La población y muestra conformada por los colaboradores y los activos de información de una empresa privada. Las técnicas para la recopilación de información cuantitativa y cualitativa fueron las encuestas, observación y entrevista.

III. Resultados

Análisis de la situación actual del nivel de conocimiento de los colaboradores

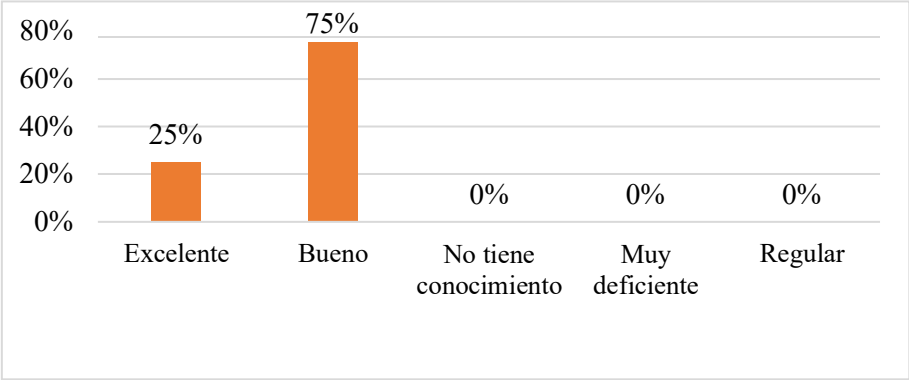

Figura 1. Nivel de Conocimiento sobre seguridad de la información Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa

Análisis e interpretación

En la figura 1, se observa que el 75% de los encuestados considera al nivel de seguridad de información como bueno, a diferencia que un menor porcentaje 25 % menciono que tiene un conocimiento excelente. Es decir existe un buen nivel de conocimiento sobre la importancia en la seguridad de la información organizacional.

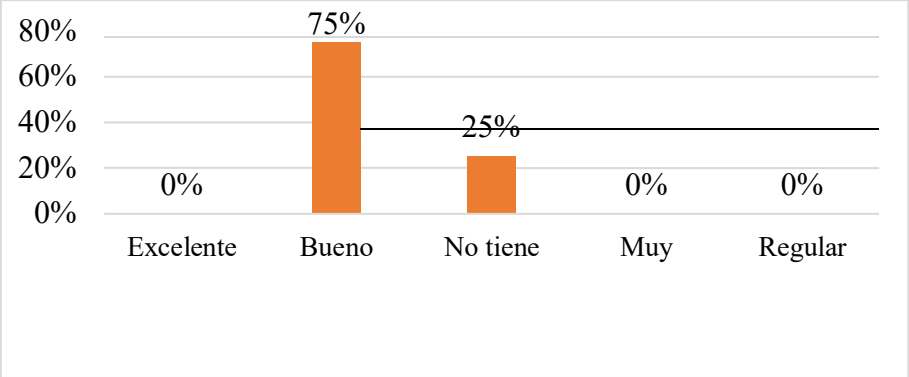

Figura 2. Conocimiento sobre las Normas de Seguridad de Información.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

Análisis e interpretación

En la figura 2 se observa que el 25% de los encuestados considera que no tiene conocimiento sobre las normas que establece de seguridad de la información a diferencia que un mayor porcentaje 75 % menciono que tiene un conocimiento bueno.

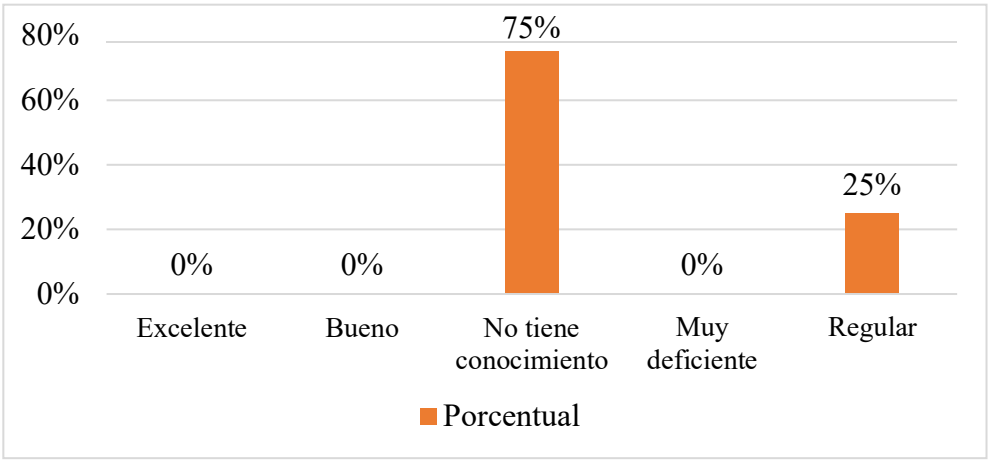

Figura 3. Conocimiento sobre la Norma ISO/IEC 27001.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

Análisis e interpretación

En la figura 3 se observa que el 75% de los encuestados considera que no tiene conocimiento sobre la norma ISO/IEC 27001, a diferencia que un menor porcentaje 25% menciono que tiene un conocimiento regular.

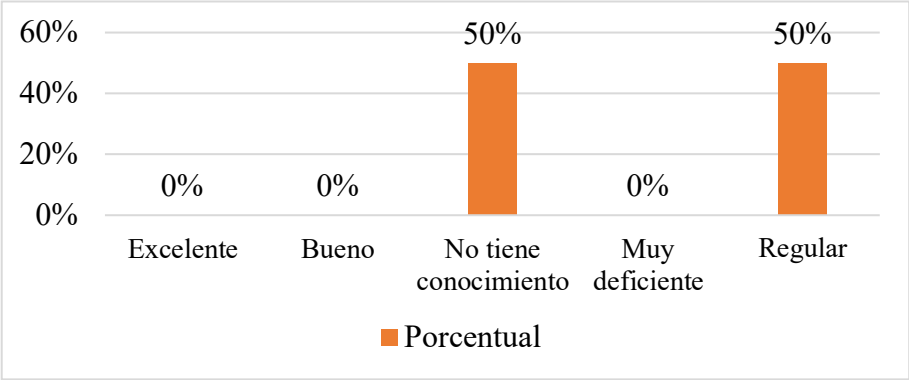

Figura 4. Conocimiento sobre la Ley de Protección de Datos.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

Análisis e interpretación

En la figura 4, se observa que el 50% de los encuestados considera que no tiene conocimiento sobre la Ley de Protección de datos a diferencia un 50 % menciono que tiene un conocimiento regular. Es una evidencia que conlleva a realizar mecanismos para la seguridad de los activos de información, y en primera instancia socializar la ley de protección de datos.

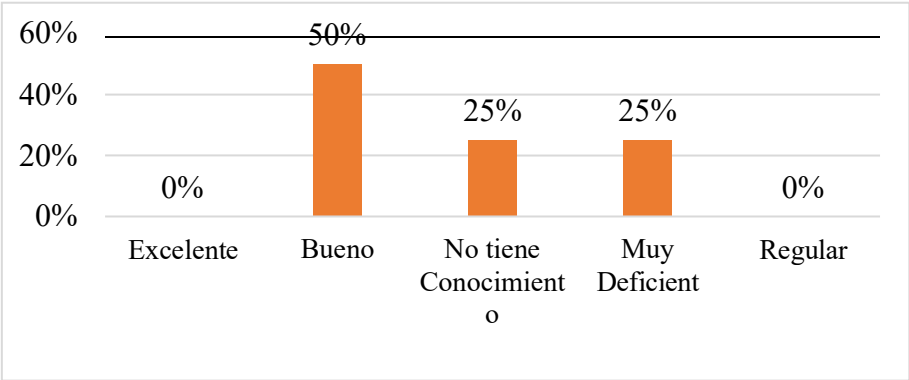

Figura 5. Calificación del sistema de control.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

Análisis e interpretación

En la figura 5, se observa que el 50% de los encuestados considera al nivel de conocimiento sobre la seguridad de los sistemas de control como bueno, a diferencia de un 25 % que considera como muy deficiente y no tiene conocimiento.

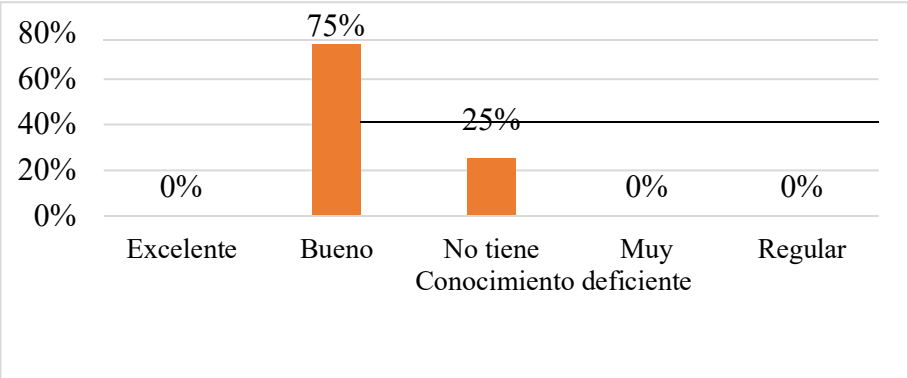

Figura 6. Nivel de seguridad que tienen los servidores.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

Análisis e interpretación

En la figura 6, se observa que el 75% de los encuestados considera como bueno el conocimiento sobre el nivel de seguridad que tienen los servidores a diferencia que un menor porcentaje 25 % menciono que no tiene conocimiento.

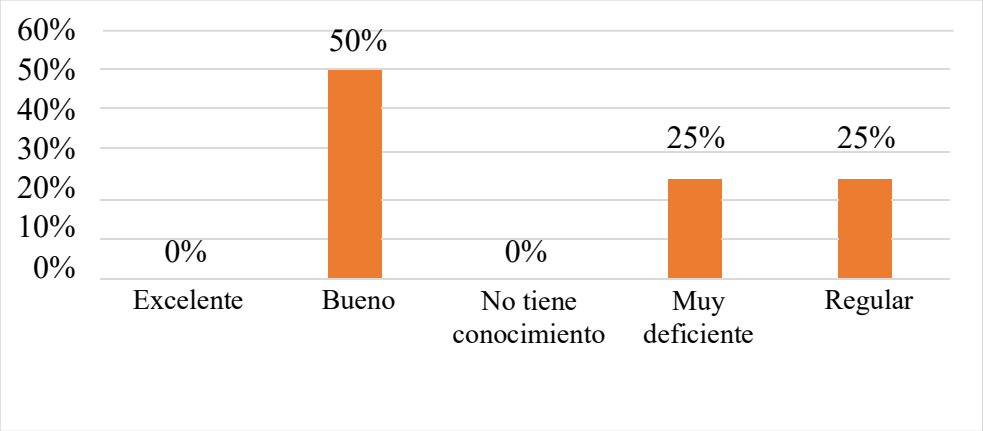

Figura 7. Nivel de calificación del antivirus
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa

Análisis e interpretación

En la figura 7, se observa que el 50% de los encuestados considera al nivel de conocimiento sobre la calificación del antivirus como bueno, y un 25 % lo considera como muy deficiente y regular. Es por ello se plasmara mecanismos de seguridad para contrarrestar o mitigar las vulnerabilidades y de esta manera tener una información segura.

Mecanismos de seguridad informática

Aumentar la seguridad de la empresa

Para el modelo adaptado en base a la norma ISO/IEC 27001 en la empresa Berendson Natación S.R.L se realizará el análisis de riesgos de acuerdo a la metodología magerit que consta de 6 fases:

El diseño del modelo consta de los siguientes puntos:

- Definir el alcance
- Identificar los activos
- Identificar las amenazas y
- Identificar las vulnerabilidades
- Evaluar el riesgo
- Tratar el riesgo

Planificar

Políticas de seguridad

Políticas generales

En la empresa privada en estudio busca que todos sus colaboradores conozcan el marco normativo con el que la organización cuenta. Estas políticas permiten que sus trabajadores fomenten el trabajo en equipo para seguir cumpliendo con los objetivos de la empresa y de cómo se van a llevar las actividades.

-El acceso no autorizado a los sistemas

- Toda la información debe contar con copias de respaldo para garantizar su seguridad
- Suministrar la información a quien no tiene derecho a conocerla
- Usar, ocultar o hacer pública la información para obtener beneficio propio o de terceros
- No utilizar software sin licencia
- Modificar o sustraer algunos equipos importantes de la empresa
- Violar cualquier ley o regulación nacional respecto al uso de sistemas de información
- La empresa cumplirá los requisitos acordados con los clientes
- Debe existir comunicación dentro de la organización
- Aseguras la confianza y transparencia dentro de la empresa
- Toda modificación en la estructura orgánica deber ser aceptada y aprobada por el Administrador.

Políticas específicas

Área Administración

- Evaluar proyectos financieros que garanticen el crecimiento
- Llevar un inventario de todos los activos del área
- El acceso a la información secreta se debe otorgar únicamente a personas específicas.
- Toda la información del área debe ser confiable. disponible, efectiva.
- Realizar copiad de seguridad semanalmente
- No visitar sitios web que no se han permitido en la empresa

Área Atención al cliente

- No proporcionar datos de los clientes a terceras personas
- Realizar copiad de seguridad semanalmente
- No realizar falsificación de los datos de los clientes
- Definir responsabilidades para la seguridad de datos
- Cambiar claves de acceso cada cierto tiempo.

Sanciones

El cumplimiento de las políticas en la empresa y deben ser obligatorios por los colaboradores, de lo contrario serán sancionados por no respetar e incumplir con las políticas ya establecidas.

Tabla 1.

Tabla de sanciones.

Nivel	Cantidad de días	Descuento
Leve	5 días	5% sueldo
Grave	10 días	10% sueldo
Muy Grave	20 días	20% sueldo

Fuente: Elaboración propia.

Identificar los activos

Se requiere realizar un inventario de los activos que se encuentran en la empresa. Los activos son todos los componentes que forman parte del sistema de información, estos son (software, hardware, datos, servicios, comunicaciones, recursos administrativos, recursos humanos, etc.). La identificación de activos se realiza de acuerdo a la metodología Magerit v3.

Tabla 2.
Descripción de activos.

Activos	Descripción
Datos	Materializan la información.
Servicios auxiliares	Se necesitan para poder organizar el sistema.
Software	Las aplicaciones informáticas que permiten manejar los datos.
Hardware	Los equipos informáticos que permiten hospedar datos, aplicaciones y servicios.
Soportes de información	Son dispositivos de almacenamiento de datos.
Equipamiento auxiliar	Complementa el material informático.
Redes de comunicaciones	Permiten intercambiar datos.
Instalaciones	Acogen equipos informáticos y de comunicaciones.
Personas	Son las personas explotan u operan todos los elementos anteriormente citados

Fuente: Análisis de Riesgos en Sistemas (2019).

Los activos se pueden medir en las siguientes dimensiones.

Tabla 3.
Dimensiones de los activos.

Dimensión	Abreviatura	Descripción
Integridad	I	Mantenimiento de las características de los datos y evitar la manipulación de estos.
Confidencialidad	C	Que la información llegue solamente a las personas autorizadas y así no pueda ocasionar daños que afecten a la empresa
Disponibilidad	D	Disposición de los servicios a ser usados estén disponibles para cuando sea necesario.
Autenticidad	A	La entidad u organización garantiza la fuente de la que proceden los datos
Trazabilidad del uso de servicio y de acceso a datos	TS	Se determina quién y en qué momento realizó algún movimiento u operación

Fuente: Elaboración propia.

Los activos se pueden medir en los siguientes valores:

Tabla 4.*Tipos de Valoración de los activos.*

Valor cuantitativo (V.A)	Valor cualitativo (V.B)
0-2	Despreciable
3-5	Bajo
6-8	Medio
9-10	Alto

Fuente: Elaboración propia

Análisis de riesgos o amenazas

Tabla 5.
Descripción de tipos de amenazas

Tipo de amenaza	Descripción
Origen Natural e Industrial	Hay accidentes naturales como los terremotos e inundaciones, accidentes industriales como la contaminación, fallos eléctricos.
Defectos de las aplicaciones y los equipos	Existen fallas técnicas o problemas de fábrica en los equipos ya sea defectos en sus diseños o en alguna pieza que puede traer como consecuencias negativas para el desarrollo de la empresa.
Causadas formas accidentales	Las personas que tienen acceso al sistema pues cometer errores u ocasionar problemas no intencionados.
Causadas formas deliberadas	Las personas que tienen acceso al sistema de información pueden ser ocasionar problemas intencionados como los ataques informáticos; y así beneficiarse indebidamente, o con el objetivo de causar daños y perjuicios a los propietarios.

Fuente: Elaboración propia.

Plan de tratamiento de riesgos
Tabla 6.
Plan de Tratamiento de Riesgos

Forma	Descripción
REDUCIR EL RIESGO	La empresa u organización opta por la implementación de medidas de seguridad como sensores de movimiento, de fuego y de humo en caso de incendios, instalación de firewall, cámaras de vigilancia.
COMPARTIR O TRANFERIR EL RIESGO	La empresa busca a terceros o contrata una entidad que asuma el compromiso de velar por la integridad y seguridad de la información.
ELIMINAR EL RIESGO	Se elimina el incidente o riesgo que este impidiendo el buen funcionamiento de la organización
ACEPTAR EL RIESGO	Cuando se decide convivir con el riego que afecta a la empresa ya que las acciones a tomar tienen un costo demasiado alto y conviene minimizarlas poco a poco.

Fuente: Elaboración propia

Plan de capacitación

Tabla 7.
Plan de capacitación 1 y 2

CAPACITACIÓN DE SEGURIDAD INFORMÁTICA	
Objetivos: Objetivos generales: Preparar al personal para la ejecución eficiente de sus responsabilidades en el manejo de información. Concientizar al personal sobre los peligros que causa la falta de seguridad de información en la empresa. Objetivos específicos: Actualizar y ampliar los conocimientos requeridos en seguridad de la información. Contribuir a elevar y mantener un buen nivel de eficiencia individual y rendimiento colectivo en base a la seguridad de información. Ayudar en la preparación de personal calificado, acorde con los planes, objetivos y requerimientos de la empresa.	
Estrategias: - Metodología de exposición. - Presentación de casos sobre SI.	Capacitadores: - Delgado Saavedra Martha Mellissa - Vasquez Zevallos José Luis
Contenido: - ISO/IEC 20001. - Seguridad de la información. - Control de accesos. - Protección de datos.	Materiales: - Proyector - Afiches, tríptico - Laptop - Lapiceros

Fuente: Elaboración propia.

Verificar
Revisión del Sistema de gestión de seguridad de la información

- Informes sobre la situación actual de la empresa.
- Verificas si las nomas o políticas establecidas se están cumpliendo adecuadamente.
- Actualizar los planes de seguridad.
- Registrar los posibles eventos que afecten a la empresa.

Actuar
Se implementan las medidas correctivas y los planes de mejora obtenidos de la verificación de SGSI:

- Mantener y mejorar cada cierto tiempo el SGSI.

- Evaluar la efectividad de los planes de mejora de sistema de gestión de seguridad de la información.
- Comunicar las acciones de mejoras a las partes interesadas que son los miembros de las áreas de atención al cliente y administración.
- En las diferentes áreas realizar un documento de seguridad donde se detallen y especifiquen que requisitos debe de seguir la empresa para proteger sus activos de información.

IV. Discusión

En el diagnóstico de la situación actual en la que se encuentra la empresa sobre sus amenazas de protección de sus activos, el nivel de conocimiento referente al nivel de seguridad de los sistemas de control, en una escala de Bueno en un 50% de los trabajadores, seguido de un No tiene conocimiento 25% y finalmente Muy deficiente en un 25% de los colaboradores. Estos resultados son similares a los obtenidos en Moyano y Suarez, (2017), en la tesis "*Plan de implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y Soluciones"*, concluye en que las empresas no llegan a darle la importancia correspondiente a los asuntos de seguridad de la información.

Sobre la evaluación del resultado obtenido de la implementación de la propuesta en base a la norma ISO/IEC 27001, referente a la comparación de antes y después de la capacitación brindada sobre el conocimiento de la norma ISO/IEC 27001, en una escala de Excelente (antes 0%, después 25%) y Bueno (antes 0%, después 75%) entre el personal de la empresa, estos resultados son similares a los obtenidos en Vilca, (2017), en la 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"*, esto quiere decir que la implementación de la norma ISO/IEC 27001 ayuda mucho a las empresa en lo que tiene que ver respecto a la protección de los activos de información con la ayuda de sus trabajadores bien capacitados e informados sobre la misma.

V. Conclusiones

Al momento de realizar el diagnostico en la empresa, se obtuvo que los colaboradores tienen un grado de conocimiento regular en cuanto a la protección de los activos de toda organización y que no existen restricciones áreas de personal no autorizado y eso hace que la pérdida o los robos de información sean más rápidos. Además manifestaron que no están capacitados en cuanto a normas existentes que ayuden a mejorar las condiciones de seguridad informáticas, los registros de clientes se realiza todo manual por ende no se realizan copias de seguridad en caso de alguna amenaza o riesgo.

Al implementar el modelo adaptado en base a la norma ISO/IEC 27001 se estableció políticas de seguridad que ayudaron a mejorar la falta de seguridad que había en a la empresa, e establecieron sanciones se incumplan las normas establecidas, se identificaron los activos que tienen mayor probabilidad de sufrir alguna amenaza.

Al finalizar la evaluación luego de realizar las capacitaciones correspondientes al personal que labora en la empresa se obtuvo que su nivel de conocimiento sobre la falta de seguridad y la ley de protección de datos, la norma ISO/IEC 27001 mejoraron ya que se le informo de que trata cada punto mencionado y se le hizo recomendaciones pertinentes para seguir mejorando la seguridad ya establecida.

VI. Recomendaciones

Implementar un área de sistemas e informática que pueda continuar con la seguridad e incluso mejorarla

Seguir capacitando a los trabajadores ya que cada día salen nuevas formas de cómo proteger los activos de la empresa y de las normas o actualizaciones que puedan existir relacionadas a la seguridad informática.

Implementar un software para evitar los registros manuales y perdidos de información y económicos y se puedan hacer las copias de seguridad cada cierto tiempo.

VII. Referencias

Análisis de Riesgos en Sistemas. (2019). Análisis de Riesgos en Sistemas. Obtenido de http://cursos.aiu.edu/AN%C3%81LISIS%20DE%20RIESGOS%20EN%20SISTEMAS/Sesi%C3%B3n%202/PDF/metodo%20de%20analisis%20de%20riesgos%201.pdf

Augurto, M. A. (2017). Diagnostico de los activos de información de los procesos Implementados por el estandar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001. Piura. Obtenido de http://repositorio.ucv.edu.pe/handle/20.500.12692/11917

Fernández, D. (2015). Modelo de gestión de riesgos de TI de acuerdo con las exigencias de la SBS, basados en las ISO/IEC 27001, ISO/IEC 17799, Magerit para la Caja de Ahorro y Créditos SIPAN SA. Chiclayo. Obtenido de http://tesis.usat.edu.pe/bitstream/20.500.12423/540/1/TL_FernandezFernandezDamaris.pdf

Olaza, H. D. (2017). Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el área de configuración y activos del Ministerio de Educación - Sede Centromin. Universidad César Vallejo, Lima. Obtenido de http://repositorio.ucv.edu.pe/bitstream/handle/UCV/9927/Olaza_AHD.pdf?sequence=1&isAllowed=y

Romero, A. D. (2018). Estudio para detectar vulnerabilidades en la seguridad del software de la línea de producción de microformas basada en la norma técnica peruana NTP ISO/IEC 27001:2014; casode estudio contraloría general de la república del Perú. Universidad de Señor de Sipan, Chiclayo. Obtenido de http://repositorio.uss.edu.pe/bitstream/handle/uss/5410/Romero%20Mas%2c%20Armando%20Demetrio.pdf?sequence=1&isAllowed=y