
# UNIVERSIDAD DE LAMBAYEQUE

## FACULTAD DE CIENCIAS DE INGENIERÍA

### ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

**TESIS**

**MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN S.R.L.**

**PRESENTADA PARA OBTENER EL TÍTULO DE INGENIERO DE SISTEMAS**

**Autores**
**BACH. VÁSQUEZ ZEVALLOS, JOSÉ LUIS**
**BACH. DELGADO SAAVEDRA, MARTHA MELLISSA**

**Asesor**
**Ing. Cumpa Vásquez Jorge Tomás**

**Línea de investigación**
**Gestión de Infraestructura de TI**

**Chiclayo, Perú**
**2019**

**FIRMA DEL ASESOR Y JURADO**

Ing. Jorge Tomás Cumpa Vásquez
ASESOR

Mg. Enrique Santos Nauca Torres
PRESIDENTE

Mg. Cilenny Cayotopa Ylatoma
SECRETARIO

Ing. Jorge Tomás Cumpa Vásquez
VOCAL

## Dedicatoria

*El presente trabajo va dedicado principalmente a Dios por darme las fuerzas para lograr todas mis metas y objetivos.*
*A mi madre por ser mi motivación y la persona más importante, por demostrarme su amor y apoyo incondicional.*
*A mi padre por ser un gran amigo y estar presente en mi educación.*
*Y mi hermano por ser mi ángel que donde quiera que este guía y cuida mis pasos.*

*Martha Mellissa*

*Esta tesis está dedicada a:*
*A mis padres quienes, con su esfuerzo, paciencia y sobre todo con su amor que me han permitido poder cumplir el sueño de ser un profesional.*
*A mis hermanas por su cariño y apoyo incondicional durante todo este camino a mi sueño y especialmente a mi hermanita Greicy Briset que desde el cielo cuida de mí.*
*Finalmente, a mis sobrinos que son un motivo para seguir adelante.*

*José Luis*

## Agradecimiento

*Agradezco a Dios por siempre guiarme y bendecirme, a mis padres por el apoyo incondicional y estar presente en esta etapa importante de mi vida por ser los principales motores para salir adelante y superarme.*
*A mi hermano que guía mis pasos.*

*Martha Mellissa*

*Al finalizar este trabajo quiero utilizar este espacio para agradecer a mis Padres que han sabido darme su ejemplo de trabajo y honradez y a mis hermanas por el apoyo en este camino y a mi hermanita que desde el cielo me bendice.*
*A los docentes, y especialmente a los ingenieros por el apoyo y las enseñanzas que me brindaron en este camino.*

*José Luis*

**Resumen**

El presente informe de tesis desarrolló un modelo de sistema de gestión de seguridad de la información aplicada a las pymes en la ciudad de Chiclayo, basado en la norma ISO 27001.

Las Normas ISO no sólo son herramientas al alcance de las grandes empresas, sino que también las medianas o pequeñas empresas pueden conseguir los beneficios que se derivan de su implantación y su mantenimiento. Se trató de adaptar la norma a las pymes, ya que demanda un costo muy elevado implementar el ISO 27001.

Para la obtención de la información se consideró conveniente el uso de las técnicas de recolección de datos tales como las encuestas, para su posterior interpretación; y de esta manera medir la realidad problemática apoyado en el uso de la Norma ISO 27001, lográndose identificar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información de la empresa Berendson Natación S.R.L.

Se propuso una metodología de implementación de la ISO 27001 para que sea aplicada en un modelo de sistemas de gestión de seguridad de la información en la empresa Berendson Natación S.R.L. Se buscó facilitar las tareas que dificultan a la empresa debido a los recursos limitados con los que cuentan en presupuesto, conocimiento y personal.

Palabras clave: Control, Información, Norma ISO 27001, PYMES, Riesgos, Seguridad Informática.

**Abstract**

This thesis report developed a model of the information security management system applied to SMEs in the city of Chiclayo, based on the ISO 27001 standard.

ISO Standards are not only tools available to large companies, but also medium or small companies can achieve the benefits derived from their implementation and maintenance. It was tried to adapt the norm to the SMEs, since it demands a very high cost to implement the ISO 27001.

To obtain the information, the use of data collection techniques such as surveys was considered convenient for subsequent interpretation; and in this way measure the problematic reality supported by the use of ISO 27001, managing to identify deficiencies to improve the levels of security and reliability in the information systems of the company Berendson Natación S.R.L.

An ISO 27001 implementation methodology was proposed to be applied in a model of information security management systems in the company Berendson Natación S.R.L. The aim was to facilitate the tasks that make the company difficult due to the limited resources available to them in terms of budget, knowledge and personnel.

Keywords: Control, Information, ISO 27001 standard, Pyme, Risk, Information Security.

**Índice**

**Índice de tablas**

**Índice de figuras**

## 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 existen varias formas de salvaguardar la información. En el presente proyecto se determina la carencia de seguridad en la información que permita diseñar un modelo adaptado a la norma ISO/IEC 27001 para la protección de los activos de la organización y saber analizar los riesgos y amenazas no solo económicas sino también asegurar la confidencialidad y disponibilidad de la información.

El objetivo general es determinar un modelo basado en la norma ISO/IEC 27001 para mejorar la seguridad informática en la empresa BERENDSON NATACION S.R.L, teniendo como objetivos específicos: diagnosticar la situación actual en la que se encuentra la empresa sobre sus amenazas de protección de sus activos, elaborar el modelo adaptado en base a la norma ISO/IEC 27001, evaluar el resultado obtenido de la implementación del modelo adaptado en base a la norma ya mencionada. Asimismo, la hipótesis consiste en el modelo adaptado de la norma ISO/IEC 27001 mejora la seguridad de los activos de la información en la empresa BERENDSON NATACION S.R.L.

La justificación planteada en la investigación se tiene como ámbitos:

Social: El siguiente proyecto también mejoraría la comunicación entre los trabajadores dentro de la empresa, haciendo que todos participen en funcionamiento del sistema de gestión de seguridad de la información y además permitiendo que los trabajadores tengan un mejor conocimiento. Tecnológico: A través de esta investigación se pretende hacer uso de las tecnologías estrictamente orientadas a la seguridad de los sistemas de información, y la auditoria de los Sistemas de información, generando como consecuencia una mejora en el uso de las aplicaciones con mayor nivel de seguridad en los sistemas de información respectivamente. Científica: Con el desarrollo de este proyecto, se pretende otorgar apoyo a futuras investigaciones relacionadas con los temas de seguridad de la información, y así mismo aportar nuevos conocimientos en el tema y metodologías de trabajos para concretar fines específicos relacionados con el uso de las tecnologías y sistemas de información.

## II.Marco teórico

### 2.1 Antecedentes Bibliográficos

### 2.1.2 Antecedente internacionales

Bastidas,Lopez y Peña(2014), en el proyecto titulado "Análisis *de riesgos y recomendaciones de seguridad de la información al área de información y tecnología del Hospital Susana López de Valencia de la Ciudad de Popayán*", consignó como objetivo principal, el diseño de mejoras a los niveles de seguridad informática con la aplicación del proceso de evaluación y análisis de riesgos de seguridad de la información en la oficina de gestión de sistemas de información y telecomunicaciones del Hospital Susana López de Valencia E.S.E de la ciudad de Popayán, fue una investigación de tipo aplicada. Concluyó, entre otras, que la aplicación de la norma ISO 27001, en procesos sensibles que se manejan en el Hospital se establecen las bases para acreditar la seguridad y disponibilidad de los servicios que ofrece la Institución. La metodología utilizada enmarcada en la norma ISO 27001 para una institución de salud, aportó una substancial contribución con la presente investigación por darle un enfoque orientado a optimizar la protección de información en el campo de la salud.

Molina (2015), en la tesis titulada un "*Plan de Gestión del Riesgo en Tecnología aplicado en la Escuela Superior Politécnica del Litoral*", tuvo como objetivos determinar el alcance del plan de riesgos, definir los activos y amenazas, proponer salvaguardas para minimizar el riesgo y contrastar el riesgo e impacto actual y el residual, la investigación fue de tipo aplicada; una entre varias de las conclusiones se refiere a que la gestión de riesgos en una empresa debería considerarse como un proceso intrínseco, ya que, si no se conoce el riesgo de los activos de información, no se podrá evitar las amenazas y sus consecuencias. El investigador determinó la metodología Magerit para el análisis de riesgo en tecnologías de información, procedimientos que sirvieron para la presente investigación, ya que justamente será el método a utilizar.

Tibaquira (2015), en el proyecto denominado "*Metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en el estándar ISO/IEC 27035 y norma ISO/IEC 27005"*,tuvo como objetivo específico, entre otros, definir la metodología, política y procesos de gestión riesgos teniendo como base la ISO/IEC 27035 para los incidentes de seguridad identificados en la plataforma SIEM (Gestión de incidentes en seguridad de la información) 2014, el tipo de investigación fue aplicada. El investigador concluyó que teniendo como base las normas ISO 27035:2011 e ISO 27005:2008 se logró construir un modelo íntegro que abarca la gestión de

incidentes y la gestión de riesgos asociada a estos incidentes. Esta adopción de un estándar ISO 27005 constituyó un aporte substancial para la presente investigación, en el aspecto de la gestión del riesgo.

Aguirre y Aristizabal (2013), en la tesis titulada "D*iseño sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda ",* explicaron como la aplicación de controles del estándar ISO 27001 permite a la administración el funcionamiento de un sistema de detección de intrusos dentro de un Sistema de gestión de seguridad de la información, la investigación fue de tipo aplicada. Concluyó que toda implementación SGSI se debe establecer en referencia a estándares y mejores prácticas encauzadas a seguridad de la información, basándose en el marco de Cobit y la norma ISO/IEC 27001 y el ISO/IEC 27002 en sus versiones 2015 para determinar el marco de control e implantar los controles pertinentes. Esta investigación contribuyó en la parte de aplicación de controles, ya que el investigador realizó un especial tratamiento del mismo.

### 2.1.2 Antecedentes nacionales

Vilca ( 2017), en la tesis denominada "Sistema *de gestión de la seguridad de la información bajo el ISO 27001 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*", empleó una metodología bajo el enfoque cuantitativo y de tipo aplicativo; ya que 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 sean procesados en el software estadístico SPSS.

Agurto (2017), en la investigación titulada "*Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"*, generó gran cantidad de información la cual está expuesta a deteriorarse, perderse, ser modificada o llegar a manos de la competencia, ya que para la ISO 27001, en toda empresa, el activo fundamental es su información. Se realizaron constantes reuniones con los colaboradores del área de logística e informática y el área QHSE para identificar y valorar los activos de información de los procesos implementados bajo la norma ISO 27001, se utilizaron cuestionarios y listas de cotejo para cada dimensión según la norma ISO 27001, obteniendo resultados que el 58% de fuga de

documentación especializada es de manuales, procedimientos, documentación técnica, por debajo con el 33% otra de la fuga de documentación es por las incidencias en información de carácter personal. En conclusión, luego de realizar dicha investigación se propuso elaborar la propuesta técnica, en la que incluyen los controles de seguridad basada en la norma ISO 27001, acorde con los procesos implementados por el estándar ISO 9001.

Castro (2018), en el proyecto denominado "*Implementación de la NTP ISO/IEC 27001:2014, para mejorar la gestión de la seguridad en los sistemas de información de la Autoridad Portuaria Nacional"*, la cual estuvo dividido en 3 etapas y tuvo como alcance los procesos de REDENAVES, Gestión de Licencias y Gestión de los Sistemas de Información en su sede central ubicado en el Callao. Los resultados que se obtuvieron permitieron determinar de forma real que, al implementar la Norma Técnica Peruana ISO/IEC 27001:2014, se obtuvo un mayor nivel de uso de documentos tales como procedimientos, política y otros, que favorecieron a la institución para descubrir las irregularidades en la seguridad de la información plasmado en varios métodos de seguridad para resguardarla. Así mismo, el Plan de Tratamiento de Riesgos, posibilitó la reducción de los niveles de riesgos de los activos de información, respecto a las amenazas y vulnerabilidades en la institución, esto plasmado en una metodología para mitigarlos a través de actividades y poder minimizar los impactos a los activos de información. Finalmente, con el Plan de Capacitación y Concientización se logró incrementar la conciencia en temas relacionados a seguridad de la información y se impulsó al personal a comprometerse a resguardar su información y mitigar riesgos en favor de la institución.

### 2.1.3 Antecedentes locales

Romero (2018), en la tesis titulada "E*studio para la detección de vulnerabilidades de seguridad del software de la línea de producción de microformas de la Contraloría General de la República del Perú"*, se centró en la exigencia de los controles de la norma técnica peruana NTP-ISO/IEC 27001:2014. Se plantearon los siguientes objetivos, realizar un análisis de la seguridad de información de la línea de producción de microformas de la contraloría general de la república, seleccionar los controles recomendados por la norma técnica peruana NTP ISO/IEC 27001:2014 que servirán para la mitigación de vulnerabilidades de seguridad de información de la línea de producción de microformas de la contraloría general de la república, listar las vulnerabilidades encontradas e identificar las de alto índice de riesgo y el tratamiento que se le deben dar a través de planes de acciones correctivas y preventivas y elaborar un manual de seguridad de la información para la línea de producción de microformas de la

contraloría general de la república. Como estudio realizado se obtuvieron las siguientes conclusiones, se realizó el análisis situacional de la seguridad de la información de la línea de producción de microformas al 100%, considerando la aplicación de la totalidad de controles de la NTP ISO/IEC 27001:2014 en la elaboración de las encuestas, donde cada pregunta se relacionó a un control específico de la norma técnica, se realizó la selección de los controles de la NTP ISO/IEC 27001:2014 para cada una de las vulnerabilidades encontradas, los controles fueron seleccionados en relación a los indicadores de cada vulnerabilidad, Se llevó a cabo la advertencia de 20 vulnerabilidades de seguridad de la información, cada una relacionada a diferentes controles de seguridad de la NTP ISO/IEC 27001:2014 y se realizó la identificación de 15 vulnerabilidades de gravedad e índice de prioridad de riesgo alto, por lo que se implementó planes de acciones preventivas y correctivas para la mitigación de las mismas.

Fernández (2015), en la tesis titulada "*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", se indicó* que la falta de una metodología y de un software adecuado que se ajusten a las exigencias de la Superintendencia de Banca y Seguro en sus normativas Resolución S.B.S N° 2116 -2009 - Reglamento para la Gestión del Riesgo Operacional y Circular Nº G-105-2002 - Riesgos de tecnología de información, constituye la justificación del presente trabajo de tesis. Tuvo como objetivo general, el mejorar la gestión de riesgos de TI en la caja de ahorro y crédito Sipán cumpliendo con las exigencias de la SBS, por medio de la implementación de un modelo de gestión de riesgos basado en las ISO/IEC 27001, ISO 17799, Magerit. Como objetivos específicos planteo, mejorar el procedimiento para definir los riesgos de TI de acuerdo a las categorías de información exigidas por la SBS, Lograr el alineamiento de los procedimientos de evaluación y tratamiento de riesgos de TI al modelo en la gestión de riesgos corporativo, Mejorar el nivel de concientización del personal en relación a la aplicabilidad de los controles de TI, Lograr el cumplimiento total de los requisitos y exigencias mínimas de la normativa de la SBS, en relación a la gestión de riesgos, mejorar el procedimiento para identificar y evaluar las amenazas vulnerabilidades, impactos, frecuencias. Las conclusiones del trabajo de información con la definición de políticas de seguridad de la información, tangibilidades en procedimientos, 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, que se expresa en la disminución de incidencias relacionados con las caídas de las TI que dan

soporte a los principales procesos: créditos y captaciones, Con la correcta identificación de los procesos críticos de La Caja, que ha partido principalmente de los dueños de los procesos, con su correspondiente priorización, se ha logrado identificar la infraestructura de TI más crítica y aplicar las estrategias para su recuperación y continuidad, lo que ha conllevado a disminuir el número de caídas o problemas, El producto tangible de la metodología de gestión de riesgos es la matriz de riesgos y a través de ella se ha logrado disponer de un registro permanentemente y actualizado de los principales activos de TI a proteger, de modo que se garantice la continuidad operativa vía los planes mitigación, de los riesgos inmersos en cada activo. Esto ha permitido una adecuada sinergia con los procedimientos de continuidad del negocio.

## 2.2 Bases teóricas

### 2.2.1 Seguridad de la información

#### 2.2.1.1 Definición seguridad de la información

Moyano y Suarez (2017), en la tesis titulada "*Plan de Implementación de SGSI basado en la norma ISO: 27001 :2013 para la empresa de interfaces y soluciones* ", se informó que la seguridad de la información se consiguió implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles necesitaron ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización.

Business School(2018), en la página "*Seguridad de la información, un conocimiento imprescindible* "se indica que la seguridad de la información engloba un conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución y asegurar que no salgan de ese sistema establecido por la empresa. Principalmente este tipo de sistemas se basan en las nuevas tecnologías, por tanto, la seguridad de la información resguardará los datos que están disponibles en dicho sistema y a los que solo tendrán acceso los usuarios autorizados. Por otro lado, tampoco se podrán hacer modificaciones en la información a no ser que sea de la mano de los usuarios que tengan los permisos correspondientes.

Quincho (2017),en la tesis denominada *"Seguridad de la información, un conocimiento imprescindible"*,se indica que seguridad de la información son todas las medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e Integridad de la misma. Diferenciando el concepto de seguridad de la información con el de

seguridad informática, en que este último sólo se encarga de la seguridad en el medio informático.

La seguridad de información se refiere a la protección de los datos o activos de las empresas que pueden ser en diferentes formatos como correo, papel, audios, etc. al usar la información con fines distintos a la empresa puede traer consecuencias graves para esta; en otras palabras, es un conjunto de medidas que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

**2.2.1.2 Importancia de la seguridad de la información**

Alcantara (2015), en la tesis titulada "*Guía de Implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria Del Norte P.N.P en la ciudad de Chiclayo* "se indica que la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

Crítica: Es indispensable para la operación de la empresa.

Valiosa: Es un activo de la empresa y muy valioso.

Sensible: Debe de ser conocida por las personas autorizadas.

Existen dos palabras muy importantes que son riesgo y seguridad:

Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.

La seguridad de la información es muy importante ya que en los activos de una organización se encuentra la información y para mantener su continuidad y éxito profesional de la empresa es necesario establecer de metodologías, prácticas y procedimientos que buscan proteger al activo con el único fin de minimizar las amenazas y riesgos continuos a los que está expuesta cualquier organización.

**2.2.1.3 Políticas de seguridad de información**

Paula y Rosario (2016), en la tesis titulada "A*nálisis de la gestión de la seguridad de Tecnologías de la Información (Ti), en las pequeñas y medianas empresas De San Francisco De Macorís, República Dominicana"*, indican que el interés debe estar escrito en conjunto con la gerencia o, por lo menos, confirmado por la misma, y explicar cómo la seguridad

informática se alinea con los objetivos de la institución. No tiene que ser un documento amplio, pero sí debe explicar, a grandes rasgos, qué es lo que la empresa espera de la seguridad de su información y cuáles son los datos más importantes a proteger. Por ejemplo: datos de clientes, proveedores, empleados, etc.

### 2.2.2 ISO/IEC 27001

#### 2.2.2.1 Definición de la ISO/IEC 27001

Kosituc (2014) citado en Bermudez .y Bailón .(2015 ), en el proyecto denominado "*Análisis de seguridad Informática seguridad de la información basado en la Norma ISO/IEC 27001 - Sistema de Gestión de Seguridad de Seguridad de la Información dirigido a una empresa de servicios Financieros"* , informan que una norma internacional que detalla lineamento de seguridad de la información de cualquier empresa controles para mejorar continuamente la seguridad física y lógica de la información de posibles robos o daños. La primera versión se publicó en el año 2005 y fue desarrollada en base a la norma británica BS 7799-2.

#### 2.2.2.2 Beneficios de la ISO/IEC 27001

Bermudez y Bailón(2015 en el proyecto denominado "*Análisis de seguridad Informática seguridad de la información basado en la Norma ISO/IEC 27001 - Sistema de Gestión de Seguridad de Seguridad de la Información dirigido a una empresa de servicios Financieros",* indican que permite disminuir posibles riesgos de vulnerabilidades en los sistemas informáticos y en la información en general manejada por el personal de la empresa, además mejora los procesos y servicios prestados, teniendo una mejor organización de los procesos, aumentando de la competividad de la empresa debido a que se demuestra el interés por salvaguardar la integridad, confiabilidad y disponibilidad de la información de los clientes.

#### 2.2.2.3 Estructura de la ISO/IEC 27001

ISOTools(2018),esta pagina titulada "*Software ISO Riesgos y Seguridad*",se desarrolla la estructura de la norma ISO 27001 es:

Objeto y campo de aplicación: La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar Referencias Normativas: Recomienda la consulta de ciertos documentos indispensables para la aplicación de ISO27001 Términos y Definiciones: Describe la terminología aplicable a este estándar Contexto de la Organización: Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI.

Liderazgo: Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma.

Planificación: Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos.

Soporte: En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso.

Operación: Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos.

Evaluación del Desempeño: En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado.

Mejora: Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI.

### 2.2.3 Ponderación de metodologías

En base a esta consideración se ha elegido la metodología Magerit ya que como se observa en la tabla la mayoría de los indicadores son abarcados por esta metodología.

La metodología Magerit es la que mejor se adapta para un análisis de riesgos conocer cuáles son todas las amenazas que afectan a una empresa, para eso se necesita saber en cuales son los activos más importantes en una organización y el nivel de daño de puede ocasionar en ello, también permite elaborar un plan de seguridad para estar preparados frente a cualquier riesgo que se presente en la organización.

Tabla 1.
*Ponderación de metodologías*

| Metodología / Indicadores | Magerit | Mehari | Octave | Ebios | Cramm |
|---|---|---|---|---|---|
| Gestión y análisis de riesgos | **X** | **X** | **X** | | **X** |
| Prepara a las empresas para procesos de evaluación, certificación y auditoria. | **X** | | | | |
| Planificación de la reducción de riesgos | **X** | **X** | **X** | **X** | **X** |
| Capacidad de evaluar y simular los niveles de riesgo derivado de medidas adicionales. | **X** | | | | |
| Instruir al personal responsable de los sistemas de información | **X** | **X** | | | |
| Divide los activos de la organización en varios grupos | **X** | | | | |
| Relación de las amenazas a que están expuestos los activos. | **X** | | | | |

Fuente: Elaboración propia.

### 2.2.4 Metodología Magerit

#### 2.2.4.1 Definición de Magerit

Sandoval (2017) , en la tesis denominada "*Diseño de un plan de seguridad de la informacion para el centro de informatica y telecomunicaciones de la Universidad Nacional de Piura, periodo 2015-2018" indica* que la metodología MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

#### 2.2.4.2 Estructura de Magerit

Alcantara (2015), en la tesis titulada "*Guía de Implementación de la Seguridad Basado en la Norma ISO/IEC 27001, para apoyar la Seguridad en los Sistemas Informáticos de la Comisaria del Norte P.N.P en la Ciudad de Chiclayo*" tiene una estructura adecuada la cual se describirá a continuación como:

El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.

El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.

El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que se vera inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.

El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

#### 2.2.4.3 Objetivos de Magerit

Alcantara (2015), en la tesis titulada "*Guía de Implementación de la Seguridad Basado en la Norma ISO/IEC 27001, para apoyar la Seguridad en los Sistemas Informáticos de la Comisaria del Norte P.N.P en la Ciudad de Chiclayo*" ,explica los distintos objetivos que de la metodología son:

Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:

Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

**2.2.4.4 Fundamentos de Magerit**

Alcantara (2015, en la tesis titulada "*Guía de Implementación de la Seguridad Basado en la Norma ISO/IEC 27001, para apoyar la Seguridad en los Sistemas Informáticos de la Comisaria del Norte P.N.P en la Ciudad de Chiclayo*", informa que puntualmente esta metodología se basa fuertemente en analizar el impacto que puede tener para la empresa la violación de su seguridad, busca la identificación de las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas. Lo interesante de esta metodología, es que presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos.

**2.2.4.5 Ventajas de Magerit**

Alcantara (2015), en la tesis titulada "*Guía de Implementación de la Seguridad Basado en la Norma ISO/IEC 27001, para apoyar la Seguridad en los Sistemas Informáticos de la Comisaria del Norte P.N.P en la Ciudad de Chiclayo*", indica que la metodología Magerit permite saber cuánto valor está en juego en las organizaciones y por ende ayuda a protegerlo. Así mismo conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con esta metodología, se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

**2.2.4.6 Fases de la metodología Magerit**

Incibe (2017), es una página titulada "*Análisis de riesgos en 6 pasos"* y detalla que las fases de análisis de riesgo de la metodología son seis:

Fase 1. Definir el alcance. - es establecer el alcance del estudio.

Fase 2. Identificar los activos. - debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio.

Fase 3. Identificar / seleccionar las amenazas. - identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado.

Fase 4. Identificar vulnerabilidades y salvaguardas. - La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades.

Fase 5. Evaluar el riesgo. - Llegado a este punto disponemos de los siguientes elementos:

- Inventario de activos.
- Conjunto de amenazas a las que está expuesta cada activo.
- Conjunto de vulnerabilidades asociadas a cada activo (si corresponde).
- Conjunto de medidas de seguridad implantadas

Con esta información, encontramos condiciones de calcular el riesgo. Para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos.

Fase 6. Tratar el riesgo. - Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. A la hora de tratar el riesgo, existen cuatro estrategias principales:

- Transferir el riesgo a un tercero. Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
- Eliminar el riesgo. Por ejemplo, eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico que hemos expuesto, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.
- Asumir el riesgo, siempre justificadamente. Por ejemplo, el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.
- Implantar medidas para mitigarlo. Por ejemplo, contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.

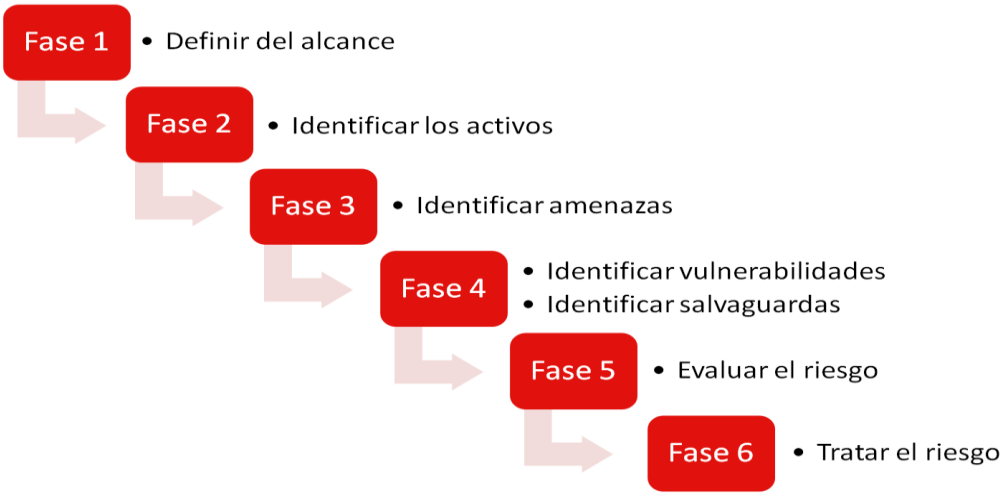



*Figura 1:* Fases de Análisis de riesgos de la metodología magerit.
Fuente: INCIBE (2019)

### 2.2.5 Metodología Mehari

#### 2.2.5.1 Objetivos de mehari

Mogollón (2019), en el proyecto denominado *"Análisis Comparativo: Metodologías de análisis de Riesgos", indica*:

- Método para la evaluación y gestión de riesgos según requerimientos de ISO/IEC 27005:2008.
- Comprende bases de datos de conocimiento, con manuales y guías que describen los diferentes módulos (amenazas, riesgos, vulnerabilidades).
- Modelo de riesgos cualitativo y cuantitativo.
- Capacidad para evaluar y simular los niveles de riesgo derivado de medidas adicionales.

#### 2.2.5.2 Fases de mehari

Mogollón (2019), en el proyecto denominado *"Análisis Comparativo: Metodologías de análisis de Riesgos"* indica:

a. Establecimiento del contexto
b. Tipología y lista de activos principales.
c. Análisis de activos: activos de respaldo y vulnerabilidades intrínsecas.
d. Daños potenciales: lista de posibles escenarios de riesgos.
e. Análisis de amenazas: eventos de iniciación, actores, condiciones específicas.

f. Elementos de reducción de riesgos: servicios de seguridad relevantes, beneficios de los servicios de seguridad.

#### 2.2.5.3 Ventajas de mehari

Mogollón (2019), en el proyecto denominado *"Análisis Comparativo: Metodologías de análisis de Riesgos" ,informa* que una ventaja de esta metodología es:

Usa un modelo de análisis de riesgos cualitativo y cuantitativo.

#### 2.2.5.4 Desventajas de mehari

Mogollón (2019), en el proyecto denominado *"Análisis Comparativo: Metodologías de análisis de Riesgos"* indica que hay tres desventajas de la metodología Mehari:

Sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad, dejando a un lado el no repudio.

La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión de los riesgos.

La estimación del impacto se realiza en el proceso de gestión y evaluación de riesgos.

### 2.2.6 Metodología octave

#### 2.2.6.1 Objetivos de octave

Lara (2014), en su página *Metodología de Evaluación de Riesgos Informáticos* indica los objetivos de la metodología son.

Desmitificar la falsa creencia: La Seguridad Informática es un asunto meramente técnico.

Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos.

#### 2.2.6.2 Fases de la metodología octave

Lara (2014), en su página *Metodología de Evaluación de Riesgos Informáticos* informa que la metodología OCTAVE está compuesta en tres fases:

Visión de organización: Donde se definen los siguientes elementos: activos, vulnerabilidades de organización, amenazas, exigencias de seguridad y normas existentes.

Visión tecnológica: se clasifican en dos componentes o elementos: componentes claves y vulnerabilidades técnicas.

Planificación de las medidas y reducción de los riesgos: se clasifican en los siguientes elementos: evaluación de los riesgos, estrategia de protección, ponderación de los riesgos y plano de reducción de los riesgos.

### 2.2.6.3 Métodos de la metodología octave

Lara (2014), en su página *Metodología de Evaluación de Riesgos Informáticos* indica que existen tres métodos de la metodología octave.

**Método Octave:** Se desarrolló para organizaciones grandes con más de 300 empleados. El método aprovecha el conocimiento de múltiples niveles de la organización, centrándose en:

(1) Identificar los elementos críticos y las amenazas a esos activos.

(2) La identificación de las vulnerabilidades, tanto organizativas y tecnológicas, que exponen a las amenazas, creando un riesgo a la organización.

(3) El desarrollo de una estrategia basada en la protección de prácticas y planes de mitigación de riesgos para apoyar la misión de la organización y las prioridades.

**Método Octave-S:** Se desarrolló pensando en las necesidades de las empresas más pequeñas. Posee los mismos criterios que el método anterior pero adaptado a las limitaciones y restricciones propias del tipo de organización a la que está enfocado. Las principales diferencias entre los dos métodos son:

**Octave-S** requiere un pequeño equipo de 3-5 personas que entienden la amplitud y profundidad de la empresa. Esta versión no comienza con el conocimiento formal sino con la obtención de talleres para recopilar información sobre los elementos importantes, los requisitos de seguridad, las amenazas y las prácticas de seguridad. El supuesto es que el equipo de análisis de esta información ya se conoce.

**Octave-S** incluye sólo una exploración limitada de la infraestructura informática. Las pequeñas empresas con frecuencia externalizan sus procesos de TI por completo y no tienen la capacidad de ejecutar o interpretar los resultados de las herramientas de vulnerabilidad.

**Método Octave** Allegro: Variante del primer método, enfocado a los activos de la información. Consta de las siguientes fases:

Fase 1 - Evaluación de los participantes desarrollando criterios de medición del riesgo con las directrices de la organización: la misión de la organización, los objetivos y los factores críticos de éxito.

Fase 2 – Cada uno de los participantes crean un perfil de los activos críticos de información, que establece límites claros para el activo, identifica sus necesidades de seguridad, e identifica todos sus contenedores.

Fase 3 - Los participantes identifican las amenazas a la información de cada activo en el contexto de sus contenedores.

Fase 4 - Los participantes identifican y analizan los riesgos para los activos de información y empiezan a desarrollar planes de mitigación.

### 2.2.7 Metodología Ebios

#### 2.2.7.1 Definición

Restrepo (2018),en la página titulada "*Metodología Ebios" indica que ebios* es una metodología de análisis y gestión de riesgos de seguridad de sistemas de información que comprende un conjunto de guías y herramientas de código libre, enfocada a gestores del riesgo de TI. Desarrollada en un principio por el gobierno francés.

#### 2.2.7.2 Fases

Restrepo (2018), en la página titulada "*Metodología Ebios"* indica las fases de la Metodología mencionada:

Fase 1. Análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información.

Fases 2 y 3, Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto.

Fases 4 y 5, Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales.

### 2.2.8 Metodología Cramm

#### 2.2.8.1 Objetivos

Raiño (2014), en la página titulada "*CRAMM Metodología de Evaluación y Gestión del riesgo",* informa sobre los objetivos de la metodología.

Conocer una de las metodologías para el análisis de riegos de la información.

Identificar las características de la metodología CRAMM que permite el desarrollo del análisis de riesgos de la información.

Aprender que aplicaciones tiene esta metodología.

Propiedades y más de Cramm.

## 2.3 Definición de términos básicos

### 2.3.1 Vulnerabilidades

Espinoza (2013), en su proyecto titulado "*Análisis y Diseño de un Sistema de Gestión de Seguridad de Información Basado en la Norma Iso/Iec 27001:2005 para una Empresa de Producciónу Comercialización de Productos de Consumo Masivo"* se plante que las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una

organización “Es una debilidad en el sistema, aplicación o infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema”.

### 2.3.2 Controles

Espinoza (2013), en su proyecto titulado “*Análisis y Diseño de un Sistema de Gestión de Seguridad de Información Basado en la Norma Iso/Iec 27001:2005 para una Empresa de Producciόny Comercialización de Productos de Consumo Masivo”, indica* que las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos proveen cierto grado de certeza de que se alcanzaran los objetivos del negocio. Existen varias formas de establecer controles sobre riesgos organizacionales. La siguiente es la presentada por.

Disuasivos: su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto. Por ejemplo: cámaras de vigilancia.

Preventivos: detectan problemas antes que ocurran por medio de monitoreo constante. Por ejemplo: políticas de contratación.

Detectives: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren. Por ejemplo: Uso de antivirus.

Correctivos: minimizan el impacto de una amenaza ya consumada. Por ejemplo: Planes de contingencia. Propios de cada área administrativa y operativa de las organizaciones.

### 2.3.3 Activos

Espinoza (2013), en su proyecto titulado “*Análisis y Diseño de un Sistema de Gestión de Seguridad de Información Basado en la Norma Iso/Iec 27001:2005 para una Empresa de Producciόny Comercialización de Productos de Consumo Masivo”,se plantea que los* activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, necesarios para que la organización funcione y alcance los objetivos que propone su dirección.

Los activos son bienes o servicios que dispone una empresa pudiendo ser tangibles como algún equipo informático o intangible como por ejemplo servicios prestados.

## 2.4 Hipótesis

### 2.4.1 Formulación de hipótesis

El modelo adaptado de la norma ISO/IEC 27001 mejora la seguridad de los activos de la información en la empresa BERENDSON NATACION S.R.L.

## III. Materiales y métodos

### 3.1 Variables y operacionalización

#### 3.1.1 Variable independiente

El modelo adaptado de la norma ISO 27001 a la empresa BERENDSON NATACION S.R.L.

#### 3.1.2 Variable dependiente

Disposición de un marco normativo para gestión de seguridad

#### 3.1.3 Operacionalización de variable

Tabla 2.

*Operacionalización de variable dependiente.*

| | VARIABLE | DIMENSIÓN | INDICADORES | ÍTEMS | TECNICAS | INSTRUMENTO |
|---|---|---|---|---|---|---|
| D E P E N D I E N T E | Disposición de un marco normativo para gestión de seguridad. | Seguridad | Preguntar si la disposición de un marco normativo es adecuada para la seguridad de la empresa BERENDSON NATACION S.R.L. | En medio donde se alojan los backup de los servidores ¿En qué estado se encuentran?<br>El sistema de control para el ingreso a esta área se define como.<br>Como se define los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores.<br>El antivirus instalado en los equipos de cómputo de la empresa se puede definir como:<br>El nivel de protección brinda el antivirus instalado en los equipos de computo<br>Como se define la restricción a paginas no permitidas en la empresa | Entrevista<br>Encuesta | Cuestionario |
| | | Riesgo | Evaluar en cuánto disminuyo el nivel de riego de pérdida y robo de información | Que conocimientos posee con respecto a la seguridad de la información.<br>Que conocimientos tiene sobre las normas que establece de seguridad de la información.<br>Cuál es su conocimiento sobre Norma ISO/27001.<br>Que conocimiento tiene sobre la ley de protección de datos.<br>Como se define el password para ingreso al sistema<br>El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema. | | |

Fuente: Elaboración propia.

### 3.2 Tipos de estudio y diseño de investigación

#### 3.2.1 Tipo de estudio

El tipo de estudio del presente proyecto es una investigación aplicada que implica la implementación de un modelo 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

### 3.3. Población y muestra de estudio

#### 3.3.1 Población

En la empresa BERENDSON NATACION S.R.L. Se realizó un estudio que consistió en analizar el funcionamiento y se encontraron con 3 computadoras registradas que son empleadas para el respaldo de activos.

#### 3.3.2 Muestra

La selección de la muestra se basa en el total de la población de la empresa BERENDSON NATACION S.R.L.

### 3.4 Método, técnicas e instrumentos de recolección de datos

Las siguientes técnicas de recolección de datos que se utilizarán para el desarrollo del presente proyecto son:

Tecnicas de Recolección de Datos (2018), detalla sobre la observación que es una técnica útil para el analista en su proceso de investigación, consiste en observar a las personas cuando efectúan su trabajo. La observación es una técnica de observación de hechos durante la cual el analista participa activamente actúa como espectador de las actividades llevadas a cabo por una persona para conocer mejor su sistema. El propósito de la observación es múltiple, permite al analista determinar que se está haciendo, como se está haciendo, quien lo hace, cuando se lleva a cabo, cuánto tiempo toma, donde se hace y porque se hace.

Tecnicas de Recolección de Datos(2018), informa que una encuesta es un conjunto de preguntas normalizadas dirigidas a una muestra representativa de la población o instituciones, con el fin de conocer estados de opinión o hechos específicos. La intención de la encuesta no es describir los individuos particulares quienes, por azar, son parte de la muestra sino obtener un perfil compuesto de la población. Una encuesta recoge información de una muestra. Una muestra es usualmente sólo una porción de la población bajo estudio.

Tecnicas de Recolección de Datos(2018), indica que una entrevista es una conversación dirigida, con un propósito específico y que usa un formato de preguntas y respuestas. Se establece así un diálogo, pero un diálogo peculiar, asimétrico, donde una de las partes busca recoger informaciones y la otra se presenta como fuente de estas informaciones. Una entrevista

es un dialogo en el que la persona (entrevistador), generalmente un periodista hace una serie de preguntas a otra persona (entrevistado), con el fin de conocer mejor sus ideas, sus sentimientos su forma de actuar.

**3.5 Procesamiento de datos y análisis estadístico**

En el proyecto de investigación se procederá a informar de que manera la norma ISO/IES 27001 permite a la empresa BERENDSON NATACION S.R.L disponer de un marco normativo para la gestión de seguridad.

Para el reciente estudio se utilizará las técnicas de encuesta y entrevista que tiene como instrumento el cuestionario, que estará dirigida a la empresa BERENDSON NATACION S.R.L que resulten seleccionados en la muestra del estudio.

Las encuestas realizadas a la empresa BERENDSON NATACION S.R.L se usarán la herramienta de Excel lo cual servirá para tabular información cuantitativa y cualitativa.

## IV. Resultados

### 4.1. Diagnosticar la situación actual en la que se encuentra la empresa sobre sus amenazas de protección de sus activos.

Para diagnosticar la situación actual que tiene la empresa BERENDSON NATACION S.R.L sobre sus amenazas de protección de sus activos se realizó una encuesta y entrevista:

#### 4.1.1 Entrevista

Se realizaron las entrevistas al personal que labora en la empresa BERENDSON NATACION S.R.L específicamente del área de gerencia , administración y atención al cliente las cuales constaron con un total de 07 preguntas para obtener datos sobre los niveles de riegos , amenazas y de seguridad que hay en las activos de la empresa y los desastres que se puedan ocasionar en ella , cada cuanto tiempo se realiza los backups y que estrategias se tendrían en cuenta para proteger y garantizar las seguridad en los activos.

Una vez culminada la entrevista se procedió al análisis de las respuestas dadas por el personal y se obtuvo que el personal entrevistado carece de conocimiento y de una area especifica que brinde las capacitaciones sobre los puntos ya mencionados, esto puede traer dificultades a la empresa al momento de proteger a los activos de la empresa por eso mismo se aceptó que se implementar el modelo adaptado de la norma ISO IEC/27001.

#### 4.1.2 Encuesta

Se realizó a los trabajadores de las áreas de Gerencia, Administración, y atención al cliente para poder obtener el nivel de conocimiento que tienen sobre seguridad de información y la Norma ISO/IEC 27001, también para conocer en qué estado se encuentra la empresa respecto a la amenazas y vulnerabilidades de los activos.

Tabla 3.
*Conocimiento con respecto a la seguridad de información.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 1 | 25% |
| Bueno | 3 | 75% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

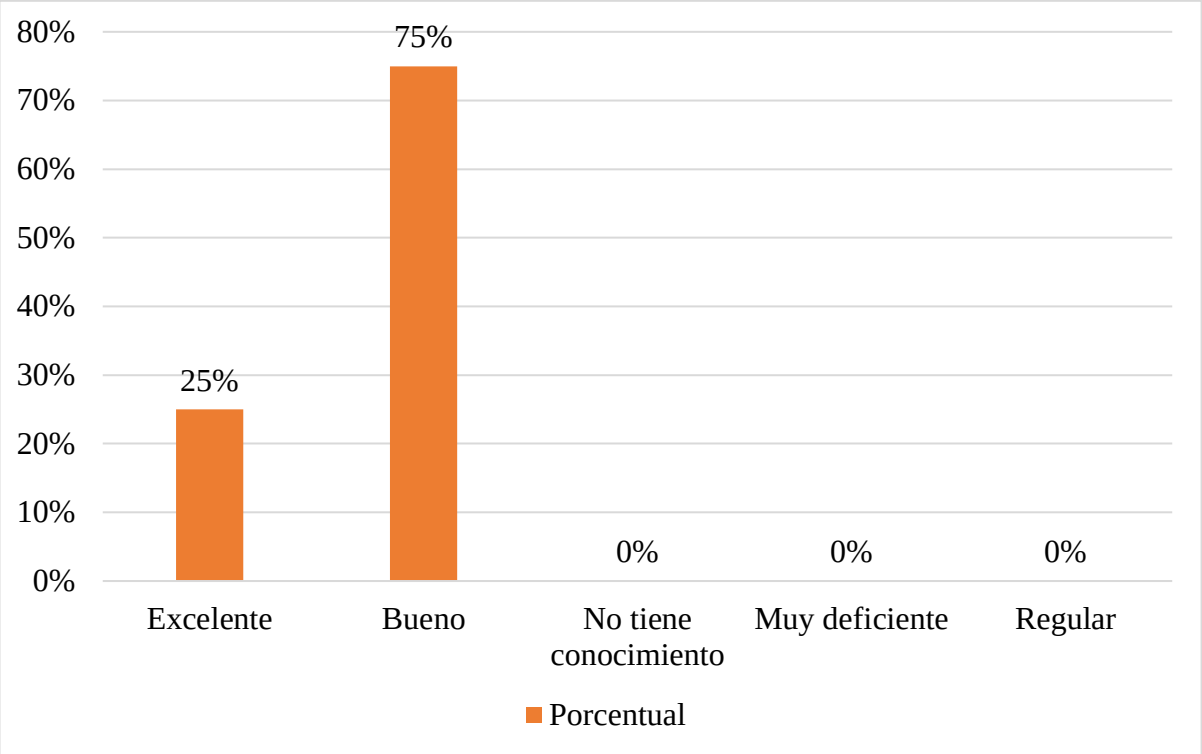



*Figura 2:*Nivel de Conocimiento sobre seguridad de la información
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa

**Análisis:** En relación a la tabla y figura 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.

Tabla 4.
*Conocimiento sobre las Normas de Seguridad de Información.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 3 | 75% |
| No tiene conocimiento | 1 | 25% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

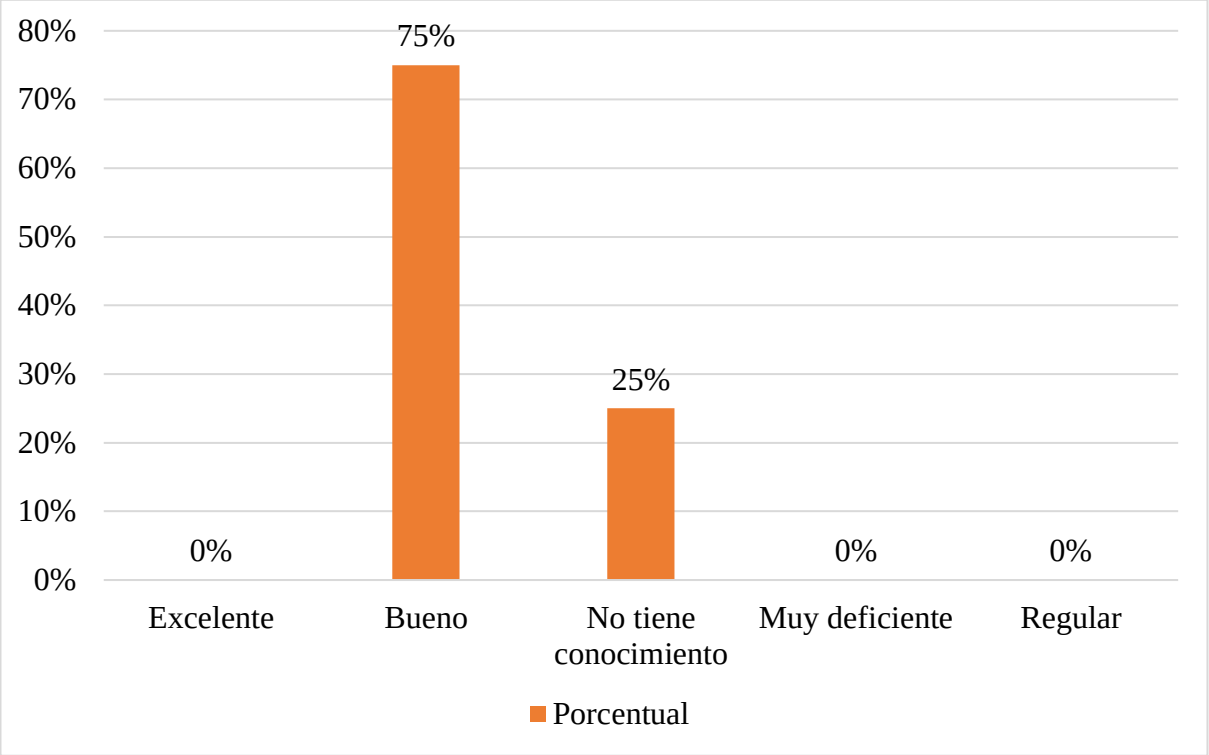



*Figura 3:* Conocimiento sobre las Normas de Seguridad de Información.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura 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.

Tabla 5.
*Nivel de conocimiento sobre la norma ISO/IEC 27001.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 0 | 0% |
| No tiene conocimiento | 3 | 75% |
| Muy deficiente | 0 | 0% |
| Regular | 1 | 25% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

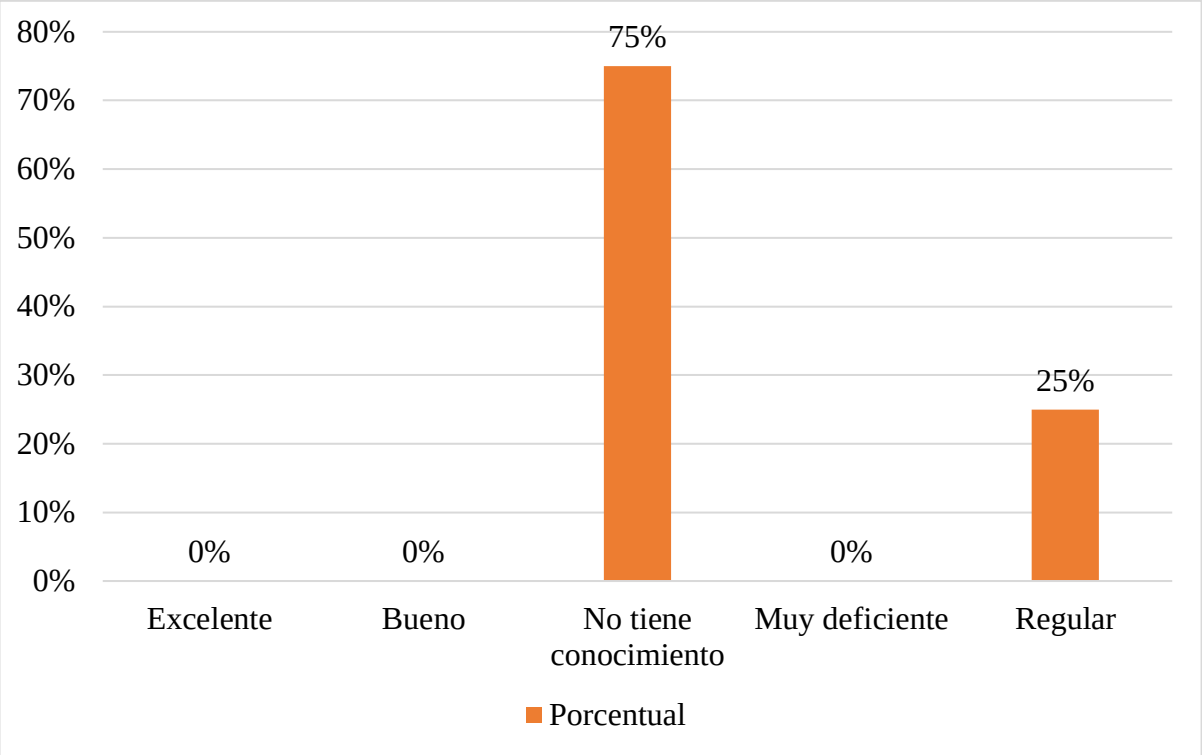



*Figura 4:*Conocimiento sobre la Norma ISO/IEC 27001.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura 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.

Tabla 6.
*Conocimiento sobre la ley de Protección de Datos.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 0 | 0% |
| No tiene conocimiento | 2 | 50% |
| Muy deficiente | 0 | 0% |
| Regular | 2 | 50% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

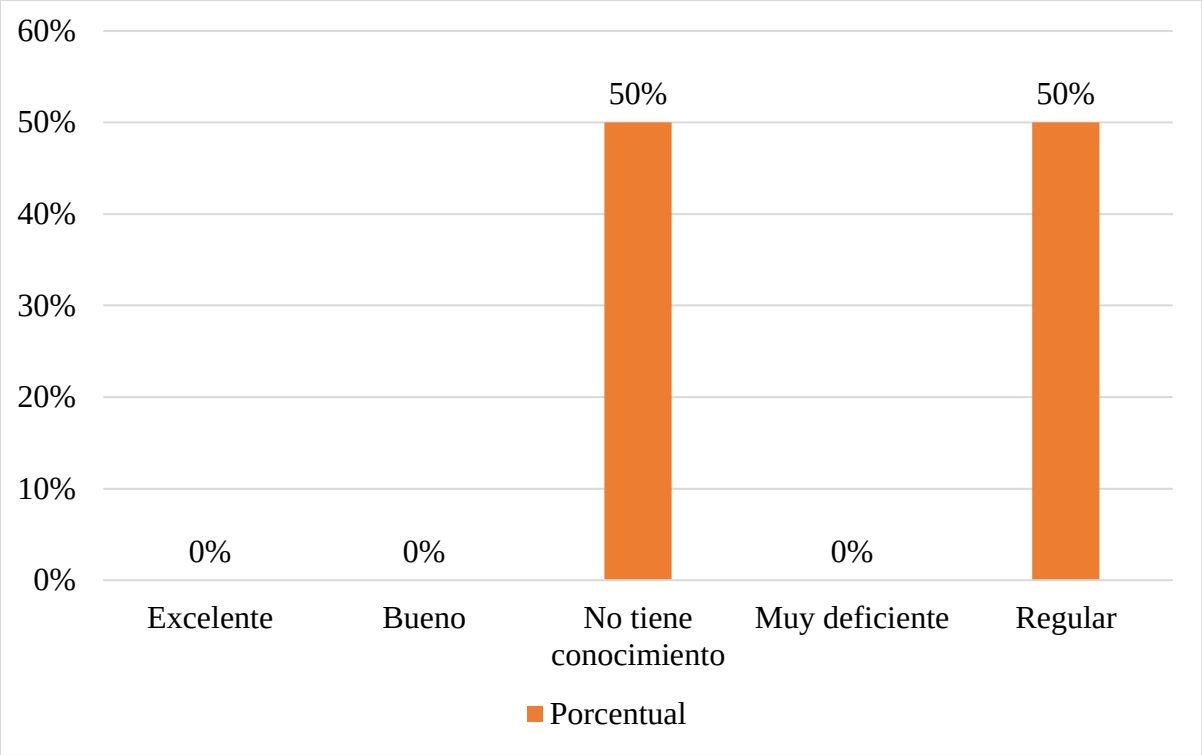



*Figura 5:* Conocimiento sobre la Ley de Protección de Datos.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 50% de los encuestados considera que no tiene conocimiento sobre la Ley de Protección de datos a diferencia que de un porcentaje 50 % menciono que tiene un conocimiento regular.

Tabla 7.
*Nivel de conocimiento sobre el estado de los Backups.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 1 | 25% |
| No tiene conocimiento | 2 | 50% |
| Muy deficiente | 1 | 25% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

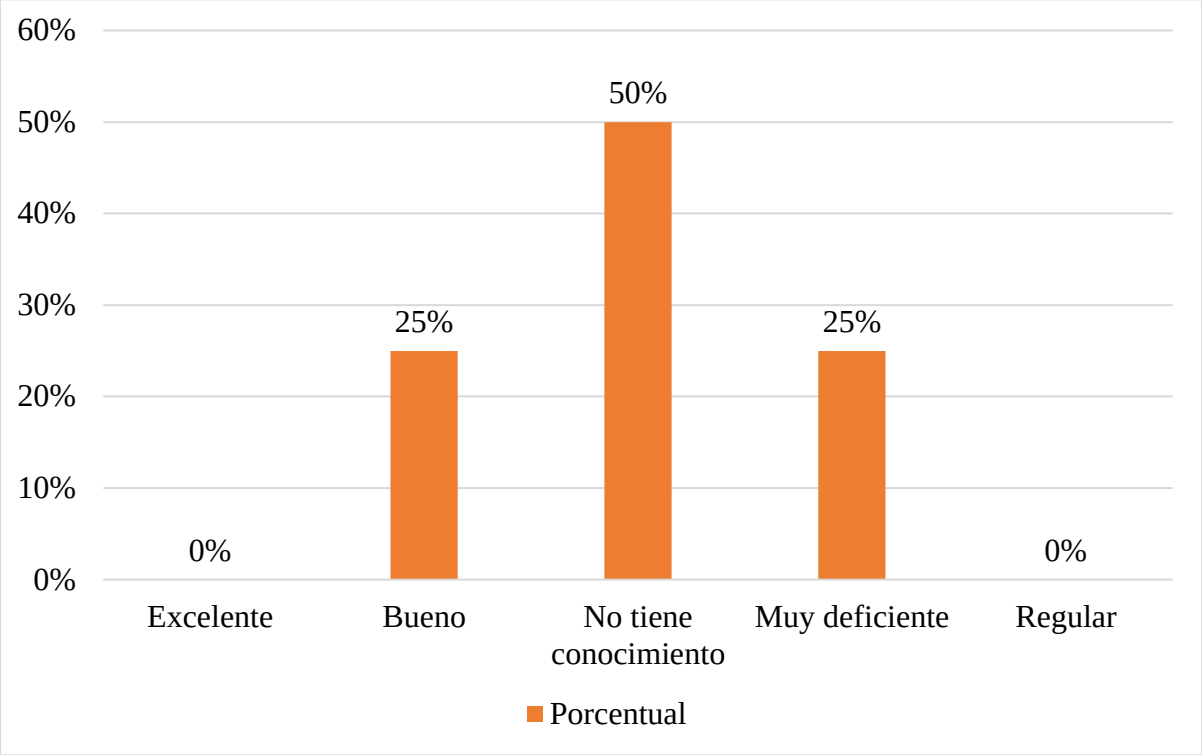



*Figura 6:* Nivel de conocimiento sobre el estado de los Backups.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 25% de los encuestados considera al nivel de conocimiento sobre el estado de los Backups como bueno, a diferencia de otro porcentaje 25% considera como muy deficiente y un 50% considera que no tiene conocimiento.

Tabla 8.
*Nivel de seguridad de los sistemas de control.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 2 | 50% |
| No tiene conocimiento | 1 | 25% |
| Muy deficiente | 1 | 25% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

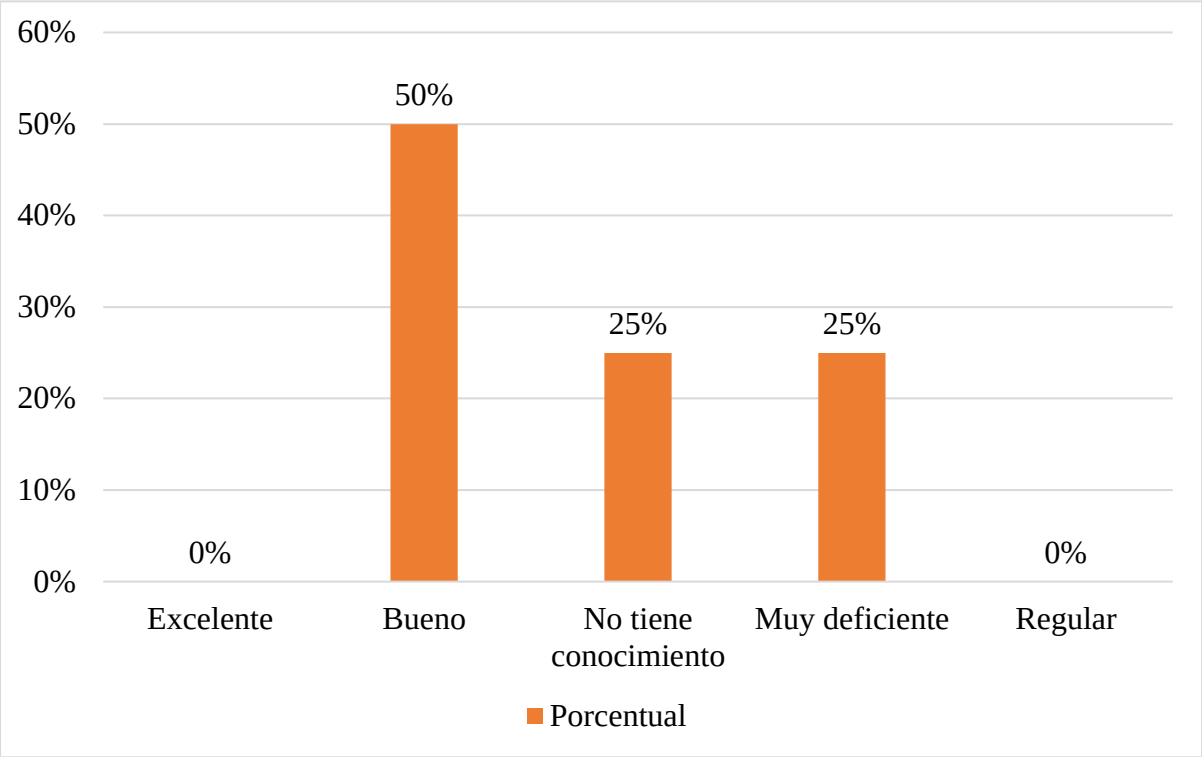



*Figura 7:* Calificación del sistema de control.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura 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.

Tabla 9.
*Nivel de seguridad que tienen los servidores.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 3 | 75% |
| No tiene conocimiento | 1 | 25% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

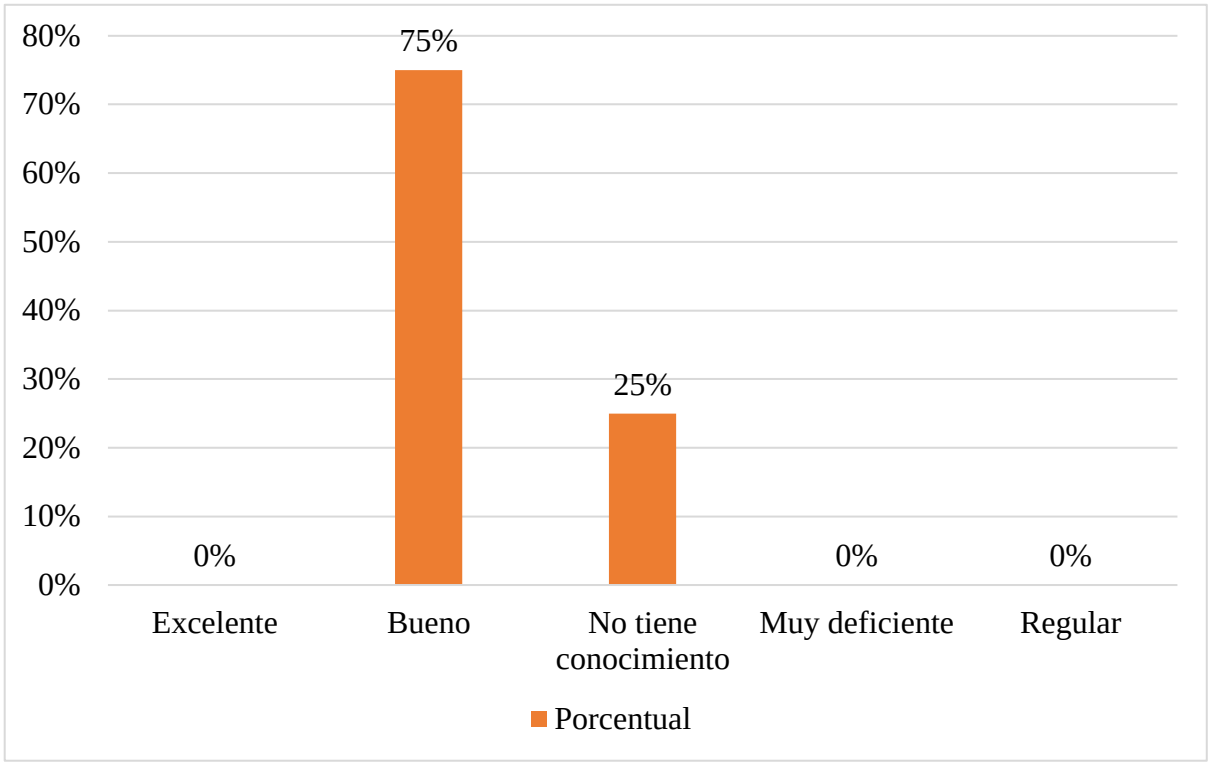



*Figura 8:* Nivel de seguridad que tienen los servidores.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura 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.

Tabla 10.
*Nivel de calificación del antivirus.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 2 | 50% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 1 | 25% |
| Regular | 1 | 25% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

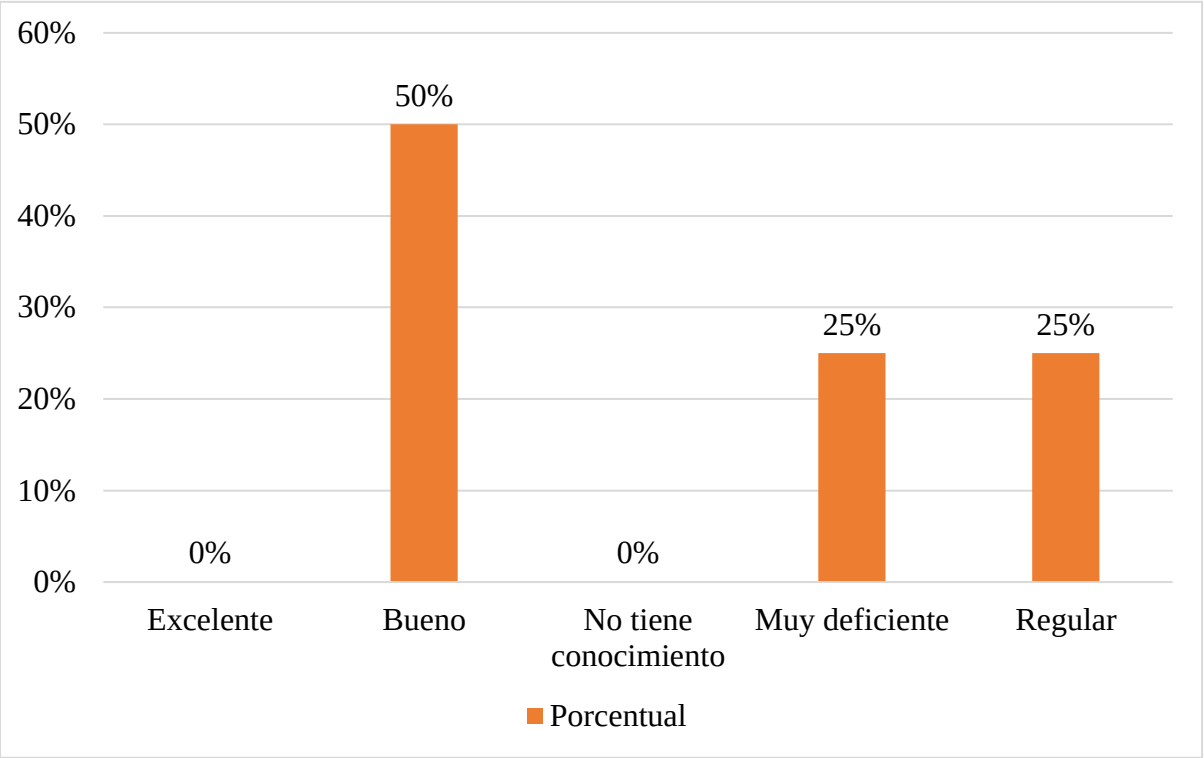



*Figura 9:* Nivel de calificación del antivirus
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa

**Análisis:** En relación a la tabla y figura 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.

Tabla 11.
*Nivel de protección que ofrece el antivirus.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 1 | 25% |
| Bueno | 3 | 75% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

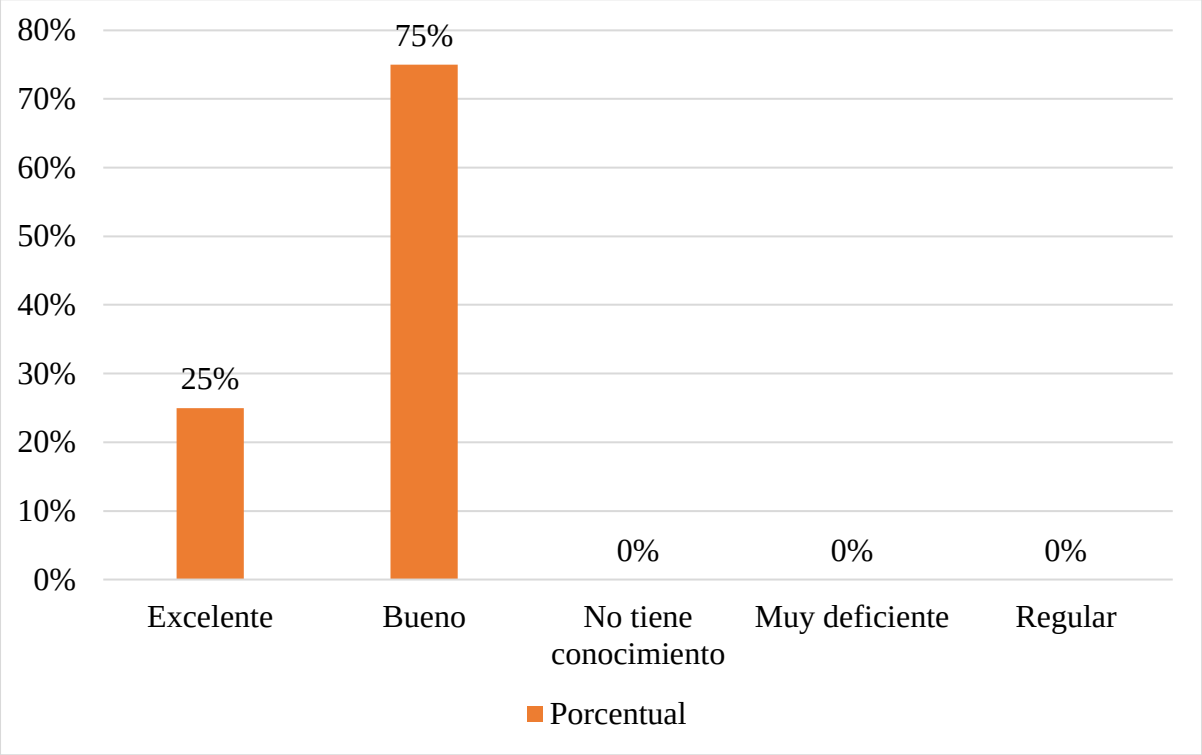



*Figura 10:* Nivel de protección que ofrece el antivirus
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa

**Análisis:** En relación a la tabla y figura se observa que el 75% de los encuestados considera bueno el conocimiento sobre el nivel de protección que ofrece el antivirus a diferencia que un menor porcentaje 25% menciono que tiene un conocimiento excelente.

Tabla 12.
*Nivel de Restricción de Páginas.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 1 | 25% |
| Bueno | 1 | 25% |
| No tiene conocimiento | 1 | 25% |
| Muy deficiente | 1 | 25% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

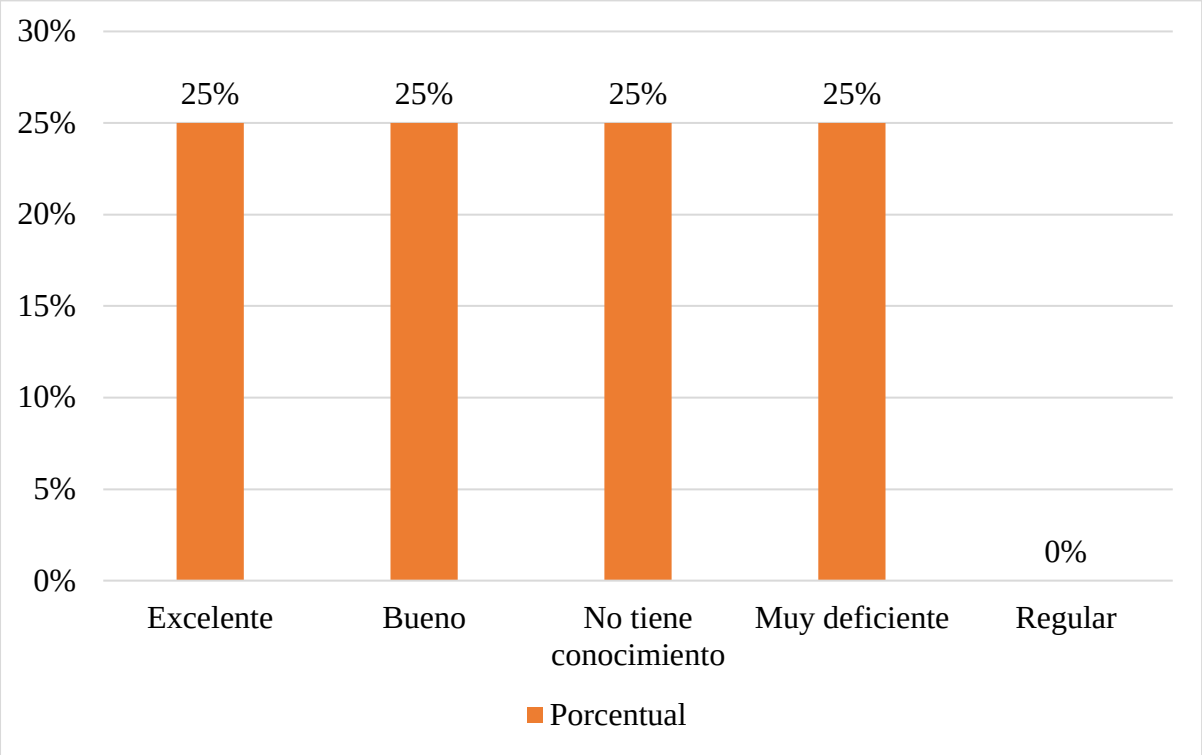



*Figura 11:* Nivel de Restricción de Páginas.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 25% de los encuestados considera sobre el nivel de protección de las paginas como bueno, muy deficiente, no tiene conocimiento y excelente.

Tabla 13.
*Calificación sobre el Nivel de Password para el ingresas a los sistemas.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 2 | 50% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 2 | 50% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

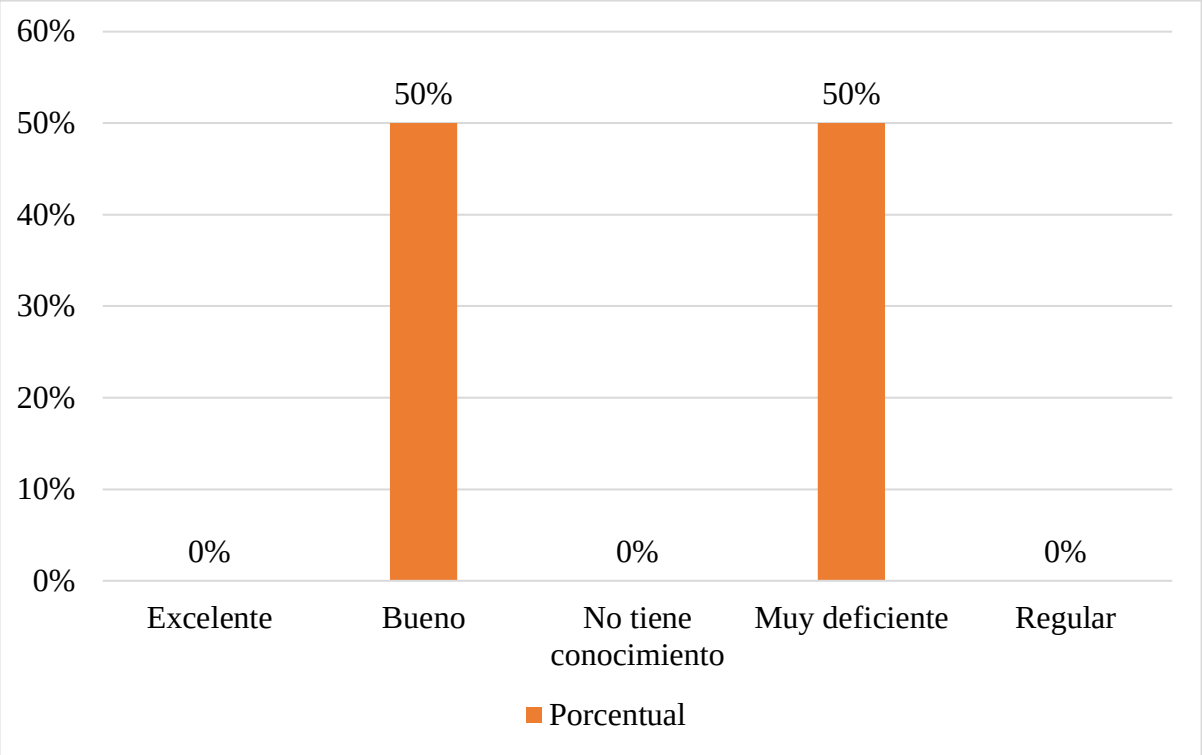



*Figura 12:* Calificación sobre el Nivel de Password para el ingresas a los sistemas.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 50% de los encuestados considera Nivel de Password para el ingresas a los sistemas como bueno, y el otro 50% lo considera como muy deficiente.

Tabla 14.

*El nivel de seguridad cumple con los parámetros establecidos para el ingreso a los sistemas.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 2 | 50% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 1 | 25% |
| Regular | 1 | 25% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

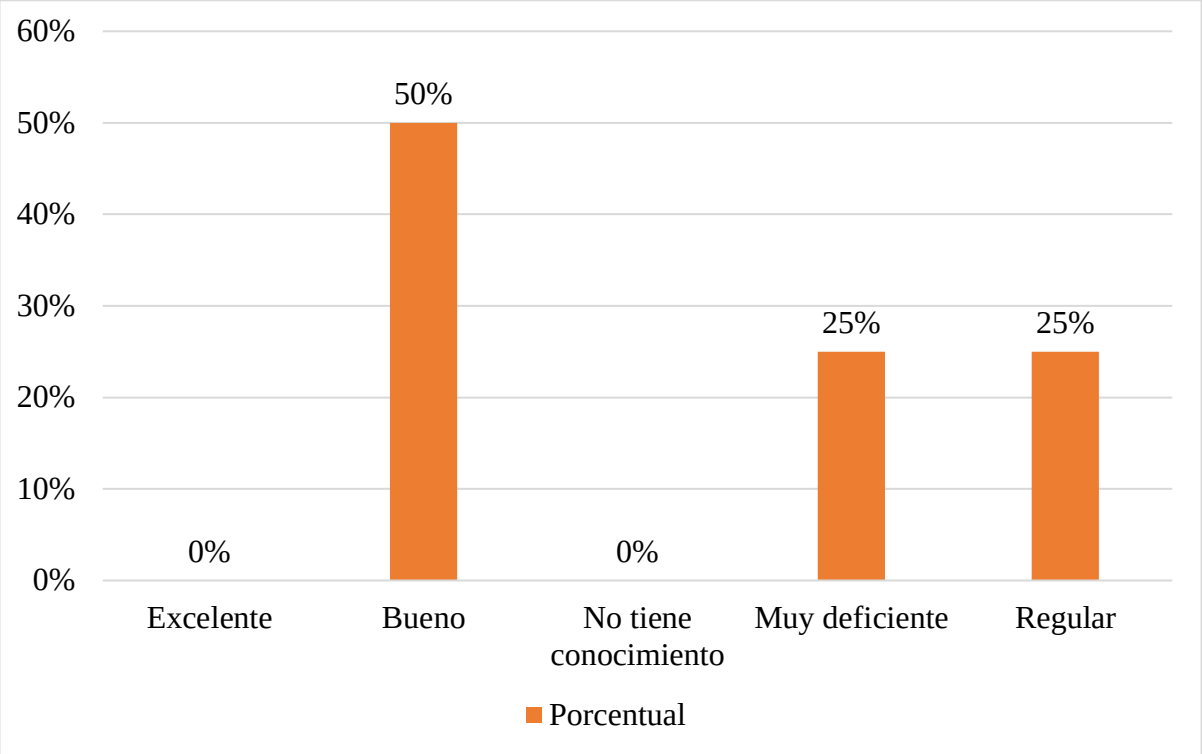



*Figura 13:* El nivel de seguridad cumple con los parámetros establecidos para el ingreso a los sistemas.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 50% de los encuestados considera sobre el nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema como bueno, a diferencia de un 25% considera como muy deficiente y regular.

## 4.2. Elaborar el modelo adaptado en base a la norma ISO/IEC 27001

La elaboración de un modelo adaptado en base a la norma ISO/IEC 27001 permitirá proteger todos los activos importantes de la empresa ya sea datos económicos o activos de información.


ISO 27001

# MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001, PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN S.R.L.

# BERENDSON NATACIÓN S.R.L


*Figura 14:* Logo de la empresa.
Fuente: Berendson Natación S.R.L.

**Objetivos del proyecto y plan director**

Implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 que permita brindar a los clientes confianza .cumpliendo con la transparencia de datos y garantizando la implementación de controles eficientes capaces de proteger los activos de la empresa Berendson Natación S.R.L y así alcanzar el objetivo visional del cual es Ser la academia líder en el deporte de la Natación dentro del norte del país, demostrando ética y responsabilidad social en la formación de profesionales en el deporte.

Objetivo principal de este documento es identificar las amenazas que están afectando, establecer las políticas de seguridad, describir roles y responsabilidades relacionadas con el Sistema de Gestión de Seguridad de la Información de la Empresa Berendson Natación S.R.L y así poder definir, implementar, dirigir y mantener un plan de tratamiento de riesgos de los activos de la organización.

Proteger los activos de Berendson Natación S.R.L manteniendo la integridad, confidencialidad, eficiencia de la empresa, clientes y proveedores.

Identificar las amenazas para la empresa como el robo y alteración de los datos que puedan afectar la imagen de la empresa para establecer controles que minimicen los riesgos.

Establecer los roles y responsabilidad en el interior de la empresa para la Seguridad de la información.

Implementar y mantener una cultura en análisis e identificación de amenazas y riegos orientada a la seguridad de Información de la empresa Berendson Natación S.R.L

Identificar, reportar, registrar y reducir las fallas, problemas o diferentes eventos que puedan alterar la seguridad que tiene la empresa y así poder mantener una mejora en los procesos.

Apoyar las pruebas del plan de continuidad para reducir y eliminar los riesgos.

**Gestión de roles y responsabilidades**

Las responsabilidades del sistema de gestión están a cargo de:

Administrador:

- ✓ Ser consultado para verificar y elaborar de las políticas generales y específicas de la empresa.
- ✓ Es la persona responsable de realizar la revisión de las políticas de seguridad de información.
- ✓ Apoyar la capacitación y entrenamiento requerido para que los trabajadores cumplan con el SGSI.
- ✓ Encargado de resguardar los activos de información.

- ✓ Encargada de realizar el proceso de compras y debe garantizar el tratamiento de la seguridad de información que se establece con los proveedores.
- ✓ Encargado de realizar las actividades necesarias durante y después de la contratación de los trabajadores.
- ✓ Permitir el acceso de datos.

Atención al cliente:

- ✓ Esta encargada de acceder a cierta información de la empresa para poder atender las dudas y reclamos de los clientes
- ✓ Tienen como función resguardar información.
- ✓ Tiene permisos para acceder a cierta parte de la información de la empresa

Encargado de ISO:

- ✓ Es el encargado de gestionar adecuadamente los accesos a los sistemas de información de la empresa.
- ✓ Encargado de realizar las políticas generales y específicas de seguridad
- ✓ Encargado de resguardar los activos de información
- ✓ Encargada de capacitar a los trabajadores de las distintas áreas de la empresa

**Fases de un sistema de gestión de la seguridad de información**

Para realizar la implementación de un MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001, se debe aplicar el ciclo de un Sistema de Gestión de Seguridad de la Información PDCA O PHVA.

1. PLANIFICAR O PLAN: se establece el Sistema de Gestión de Seguridad de la Información.
2. HACER O DO: se implementa el SGSI.
3. VERIFICAR O CHECK: se revisa el Sistema de Gestión de Seguridad de la Información.
4. ACTUAR O ACT: mantener y mejorar el SGSI.

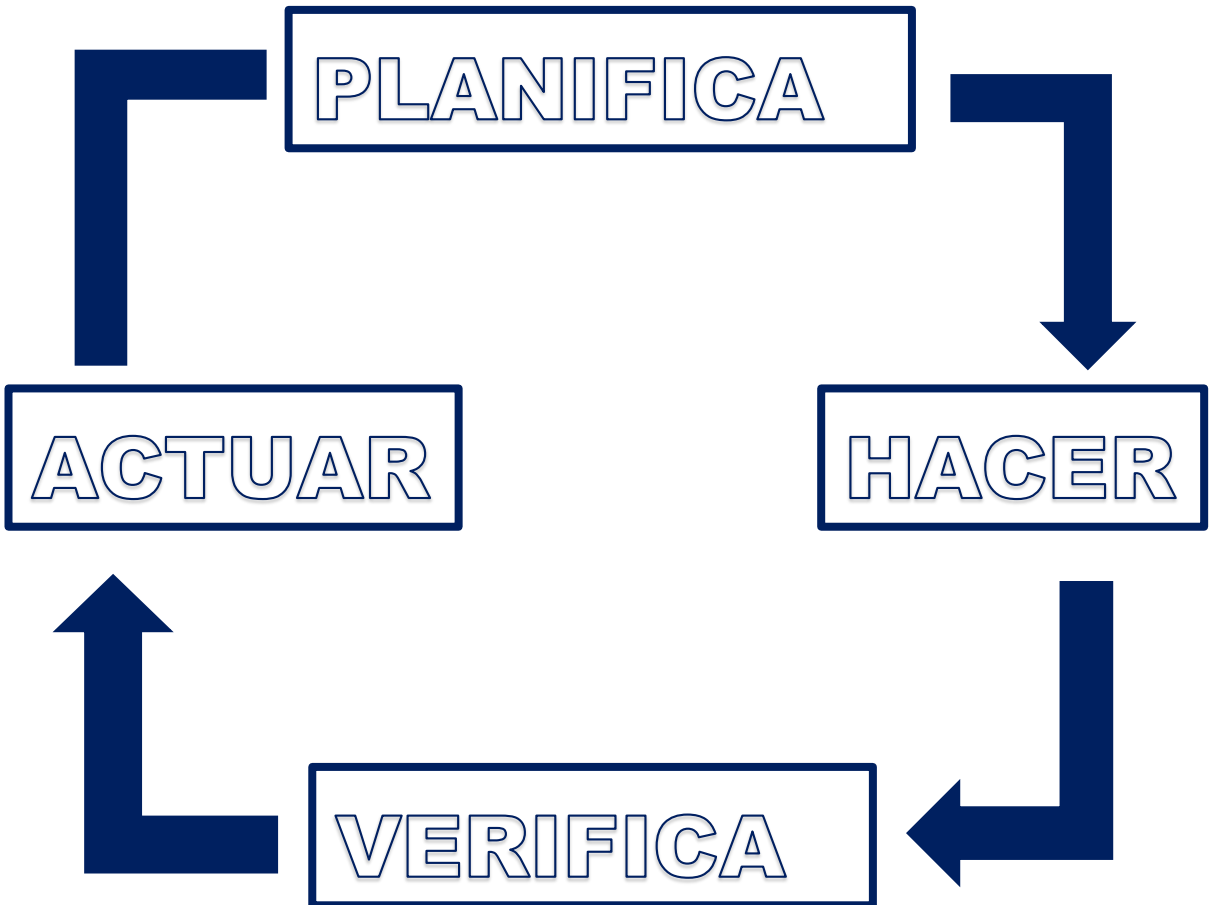



*Figura 15:* Fases de un SGSI.
Fuente: Elaboración propia.

## I. Introducción

En la actualidad donde los activos de cada organización o empresa están vulnerables a cualquier ataque informático, modificaciones, fraudes y robos de información se propuso realizar un Modelo de Seguridad Informática aplicando la Norma ISO/IEC 27001, para proteger los activos de la información en la empresa Berendson Natación S.R.L., con la finalidad de garantizar una mejor protección a la empresa asegurando la integridad, confidencialidad y disponibilidad de la misma para eso se debe aplicar el ciclo de un Sistema de Gestión de Seguridad de la Información PDCA O PHVA.

Con este Modelo de Seguridad Informática aplicando la Norma ISO/IEC 27001 se busca conocer el estado actual de la empresa con respecto a la seguridad de los activos, para esto se realiza la identificación de los activos que tienen las áreas describiendo a cada uno sus características, valor, su impacto que tienen en la organización.

Se realiza una descripción de la empresa detallando su misión, visión y organigrama actual, los objetivos del modelo, las políticas de seguridad generales y específicas de las áreas involucradas, las responsabilidades que recaen en los encargados de las áreas, las sanciones pertinentes en caso de faltas por parte del personal.

Se implementa una metodología para el análisis y tratamiento de los riesgos la cual será la metodología magerit v3, se define las dimensiones, el valor cualitativo y cuantitativo con el que se califica los activos de las áreas específicas de la empresa Berendson Natación S.R.L.

Se analiza todas las amenazas que tiene la empresa y en base a ello se plantea un tratamiento de riesgo, un plan de capacitación para mejorar las fallas existentes y para que los trabajadores de la empresa Berendson Natación S.R.L. tengan un mejor conocimiento de los riesgos están expuestos los activos de la empresa.

Se realiza una auditoria para verificar si está cumpliendo con los objetivos, políticas planteadas en la empresa y así obtener mejores resultados y conocimientos para la seguridad informática que se tiene en la empresa.

## II.Situación actual

### 2.1 Misión

Somos una academia que busca difundir la práctica del deporte, proponiendo una innovadora filosofía de servicio que asegure el desarrollo integral y mejora de la calidad de vida de nuestros clientes.

### 2.2 Visión

Ser la academia líder en el deporte de la Natación dentro del norte del país, demostrando ética y responsabilidad social en la formación de profesionales en el deporte.

### 2.3. Estructura organizacional

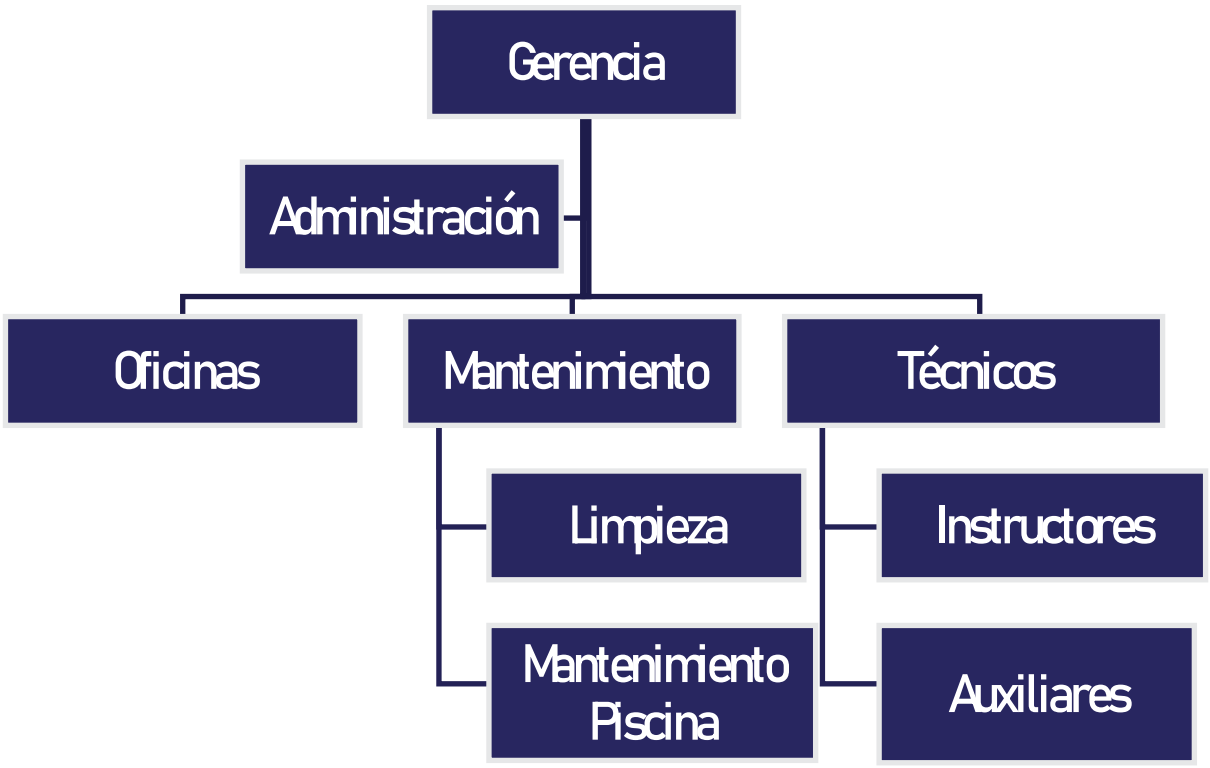



*Figura 16:* Organigrama de Berendson Natación S.R.L.
Fuente: Datos obtenidos en la encuesta aplicada al encargado del área de administración.

## III.Fases

### 3.1 Planificar

#### 3.1.1 Alcance sistema de gestión de seguridad de información

Para la empresa Berendson Natación S.R.L el alcance de un Sistema de Gestión de Seguridad de la Información es uno de los puntos más importantes ya que deben ser los más precisos y que englobe a toda la organización, teniendo en cuenta las reuniones que se tuvo con el encargado de la empresa se definió:

- ✓ Todos los activos de información ya sea en formato electrónico o físico.
- ✓ Las áreas más importantes para proteger los activos son Administración y Atención al cliente.
- ✓ Toda la información generada desde que se inició Berendson Natación S.R.L.
- ✓ La información de clientes, empleados y proveedores.

#### 3.1.2 Políticas de seguridad

##### 3.1.2.1 Políticas generales

En la empresa Berendson se busca que todos sus trabajadores 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.

### 3.1.2.2 Políticas especificas

**Administración**

Se definen las estrategias de la empresa Berenson Natación S.R.L., contrataciones, pagos a personal y de analizar los procesos, entradas y salidas para poder ofrecer mejoras a la empresa

- ✓ 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

**Atención al cliente**

Es el área que procura una verdadera vinculación con las necesidades o requerimientos de los clientes y usuarios. Una empresa exitosa conoce sus clientes, atiende sus requerimientos y necesidades

Es el servicio que la empresa Berendson Natación S.R.L. ofrece a sus clientes para comunicarse directamente con ellos. En caso que estos necesiten manifestar reclamos, sugerencias, solicitar información adicional

- ✓ 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.

### 3.1.3 Sanciones

El cumplimiento de las políticas en la empresa Berendson Natación S.R.L. deben ser obligatorios por los trabajadores, de lo contrario serán sancionados por no respetar e incumplir con las políticas ya establecidas.

Tabla 15.
*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.

### 3.1.4 Metodología de análisis de riesgos

El objetivo de este modelo basado en la norma ISO/IEC 27001 es lograr un plan de Tratamiento para los riesgos de los activos de la empresa Berendson Natación S.R.L., para llevar a cabo este plan se va a utilizar la metodología Magerit la cual cuenta con diferentes fases:

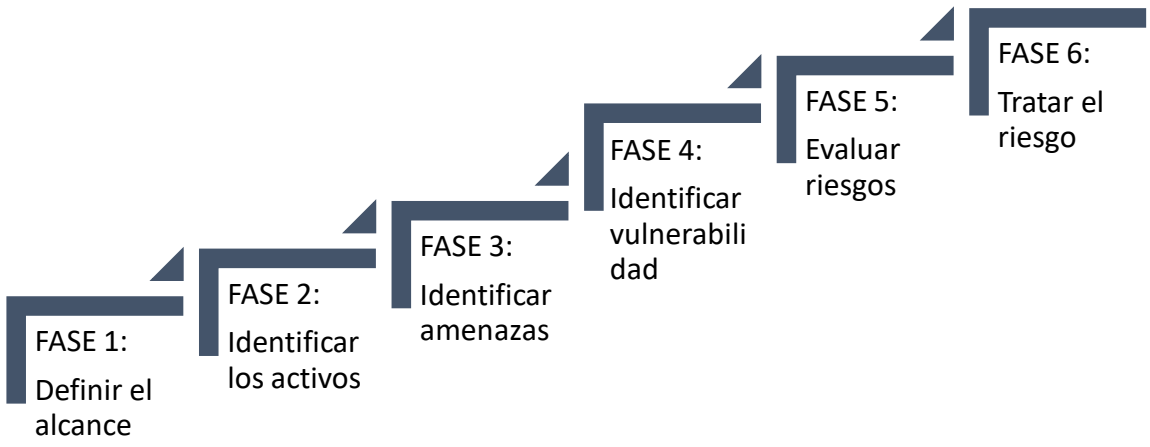



*Figura 17:* Fases de la metodología
Fuente: Elaboración propia

### 3.1.5 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 16.
*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: Analisis de Riesgos en Sistemas( 2019).

Los activos se pueden medir en las siguientes dimensiones.

Tabla 17.
*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 18.
*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.

### 3.1.6 Análisis de riesgos o amenazas

El objetivo es conocer el nivel de exposición de los activos de información que tienen frente a las amenazas, es decir conocer los riesgos a los que está expuesta la empresa Berendson Natación S.R.L

Un riesgo se puede identificar de diferentes maneras:

Tabla 19.
*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 fabrica 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.

Permite estimar la magnitud de los riesgos a lo que está expuesta la organización. La materialización de una amenaza consta de dos elementos: probabilidad e impacto, esto determina el nivel del riesgo.

De acuerdo a la probabilidad se determinó:

Tabla 20.
*Valoración de activos según la probabilidad.*

| Escala de Valoración | Valoración | Descripción |
|---|---|---|
| 3 | ALTO | La amenaza se puede materializar mínimo una vez al mes |
| 2 | MEDIO | La amenaza se puede materializar a lo sumo una vez en el semestre |
| 1 | BAJO | La amenaza se puede materializar a lo sumo una vez al año |

Fuente: Moyano y Suárez(2017).

Según el impacto se determinan los siguientes criterios de valoración.

Tabla 21.
*Valoración de activos según el impacto*.

| Escala de Valoración | Valoración | Descripción |
|---|---|---|
| 3 | ALTO | La ocurrencia del evento tiene impacto a nivel de confidencialidad, integridad y/o disponibilidad de la información poniendo en riesgo la reputación de la empresa. |
| 2 | MEDIO | La ocurrencia del evento tiene impacto a nivel de confidencialidad, integridad y/o disponibilidad de la información poniendo en riesgo la reputación de la empresa. |
| 1 | BAJO | La ocurrencia del evento no tiene consecuencias relevantes para la organización. |

Fuente: Moyano y Suárez (2017).

Por la combinación probabilidad – impacto se define el mapa de riesgo que se presenta a continuación, los números en el interior de las celdas son calculados por la multiplicación de la probabilidad por el impacto. Indican junto con los tonos de colores la criticidad del riesgo.

Tabla 22.
*Valoración de activos probabilidad-impacto.*

| **Mapa de riesgo** | | | | |
|---|---|---|---|---|
| PROBABILIDAD | 3. Alta | 3 | 6 | 9 |
| | 2. Media | 2 | 4 | 6 |
| | 1. Baja | 1 | 2 | 3 |
| | | 1.Bajo | 2.Media | 3.Alta |
| | | IMPACTO | | |

Fuente: Moyano y Suárez(2017).

A continuación, se presentan las vulnerabilidades identificadas.

- ✓ Cultura de Seguridad de la Información: Se evidencia una carencia generalizada por los siguientes aspectos.
- ✓ Los trabajadores de la empresa Berendson Natación S.R.L. no cuentan con un conocimiento bueno en cuanto a la identificación de las incidencias de seguridad de los activos.
- ✓ No cuentan con el personal adecuado para realizar capacitaciones y las soluciones adecuadas sobre la seguridad de la información.
- ✓ No existen políticas de seguridad que ayuden a mejores la protección de los activos y que se especifiquen los roles, las responsabilidades y las sanciones adecuadas.
- ✓ No existe una restricción a los sistemas de la empresa.
- ✓ No se cuenta con el hardware adecuado para la protección de la información.
- ✓ No se cuenta con un área específica de sistemas e informática para que pueda implementar nuevos métodos de seguridad informática.

### 3.1.7 Valoración de activos

Tabla 23.
*Valoración de activos.*

| Tipo | Activo | Código | Descripción | Dimensión | | | | | Valor |
|---|---|---|---|---|---|---|---|---|---|
| | | | | I | C | D | A | T | |
| Software | Sistema Operativo | AS_001 | Windows 10 Pro. Windows 10 Home Single Lenguage. | 6 | 6 | 8 | 7 | 6 | **7** |
| | Suite Ofimática | AS_002 | Office 2016 (Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Access) | 6 | 6 | 7 | 8 | 7 | **7** |
| | Antivirus | AS_003 | ESET NOD32 | 6 | 6 | 6 | 6 | 4 | **6** |
| Hardware | Laptops | AH_001 | ASUSTek – Intel(R) Pentium Silver N500 CPU @ 1.10 GHZ, RAM 4 GB – 64 Bits. HP – Intel(R) Core i3-7020U CPU @ 2.30 GHz, RAM 4 GB – 64 Bits. | 8 | 8 | 7 | 8 | 7 | **6** |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Impresora | AH_002 | - Brother DCP-T310 | 6 | 4 | 6 | 4 | 5 | 5 |
| | Smartphone | AH_003 | XIAOMI REDMI 6A Mediatek Helio A22 quad-core 12 nm 2 GHz - 2 GB RAM - Android 8.1 Oreo + MIUI 9 | 6 | 8 | 4 | 4 | 4 | 5 |
| | USB (Universal Serial Bus | AH_004 | DataTraveler 100 G3 32 GB. SanDisk cruzer force 16 GB. | 6 | 4 | 8 | 5 | 6 | 6 |
| | Router | AH_005 | Mitrastar DSL-2401HNA-T1CC | 6 | 5 | 7 | 6 | 5 | 6 |
| | Teléfono | AH_006 | Motorola - Teléfono Inalambrico AURI2020-2 2.4Ghz – Negro | 7 | 7 | 8 | 7 | 7 | 6 |
| Información | Datos e información | AI_001 | Documentos almacenados en papel (boletas, boletas de ventas, registros de clientes, carnet, egresos, etc.) | 4 | 4 | 6 | 4 | 5 | 5 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | AI_002 | Documentos digitales. | 5 | 5 | 6 | 5 | 6 | 5 |
| | | AI_003 | Archivos (imágenes, videos, etc.) | 5 | 5 | 6 | 5 | 6 | 5 |
| equipamiento auxliar | Extintor de fuego | EAI_001 | 6 extintores de polvo químico seco presurizado. | 5 | 4 | 5 | 3 | 5 | 4 |
| | Detectores de humo | EAI_002 | 4 detectores Sd-4wp Mircom X | 3 | 4 | 6 | 4 | 5 | 4 |
| | Alarma | EAI_002 | Alarma Mircom model MS-401U | 4 | 5 | 7 | 7 | 6 | 5 |
| personas | Personal de oficina | PI_001 | 4 personas que laboran en el área. | 5 | 5 | 5 | 5 | 5 | 5 |

Fuente: Elaboración propia.

### 3.2 Hacer

#### 3.2.1 Plan de tratamiento de riesgos

Se establece un plan de tratamiento en la empresa Berendson Natación S.R.L., con el objetivo de determinar la importancia y el impacto del riesgo y para eso se opta por una de las siguientes formas de mitigar.

Tabla 24.

*Plan de Tratamiento de riesgo.*

| 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.

### 3.2.2 Plan de capacitación

Tabla 25.

*Plan de capacitación 1.*

| | |
|---|---|
| | **CAPACITACIÓN DE SEGURIDAD INFORMÁTICA** |
| **Fecha Inicio:** | **Hora Inicio:** |
| **Fecha Fin:** | **Hora Fin:** |

**Objetivos:**

**Objetivos generales:**

- Preparar al personal para la ejecución eficientes 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:** | **Capacitadores:** |
|---|---|
| - Metodología de exposición.<br>- Presentación de casos sobre SI. | - Delgado Saavedra Martha Mellissa<br>- Vasquez Zevallos José Luis |

| **Contenido:** | **Materiales:** |
|---|---|
| - ISO/IEC 20001.<br>- Seguridad de la información. | - Proyector<br>- Afiches, tríptico<br>- Laptop<br>- Lapiceros |

Fuente: Elaboración propia.

**ISO/IEC 27001**

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

¿Qué entendemos por información en iso 27001?

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada.

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

**Seguridad de la información**

El Sistema de Gestión de Seguridad de la Información ISO/IEC 27001 persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada.

Los términos seguridad de la información, seguridad informática y garantía de la información son utilizados con bastante frecuencia. El significado de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización.

Entre dichos términos existen pequeñas diferencias, dichas diferencias proceden del enfoque que le dé, las metodologías usadas y las zonas de concentración.

La Seguridad de la Información, según ISO/IEC 27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: Electrónico, papel, etc.

Tabla 26.

*Plan de capacitación 2.*

**CAPACITACIÓN DE ACCESOS A LA INFORMACIÓN**

| | |
|---|---|
| **Fecha Inicio:** | **Hora Inicio:** |
| **Fecha Fin:** | **Hora Fin:** |

**Objetivos:**

**Objetivos generales:**

- Preparar al personal para la ejecución eficientes 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:
- Control de accesos.
- Protección de datos.

Materiales:
- Proyector
- Afiches, tríptico
- Laptop
- Lapiceros
- Encuestas

Fuente: Elaboración propia.

**Control de accesos**

El control de acceso es una actividad técnica que tiene relación con la apertura de cuentas, contraseñas y cosas parecidas. El control de acceso incluye todas estas cosas, pero el control de acceso no comienza como algo técnico. Es una decisión de negocios.

Se debe establecer una política de control de acceso, y definir qué usuarios tendrán acceso a las redes y servicios. Esto supone que se deben establecer las reglas en primer lugar, y entonces dar permiso a los usuarios. Se pueden configurar las reglas de acceso de diferentes formas. Por regla general existen dos enfoques: Se definen perfiles de usuario y en función de cada puesto se asignan perfiles de usuario correspondiente

Gestión de acceso de usuario, las cosas comienzan a ponerse más técnicas. Se debe definir cómo se necesitan los usuarios que se registran en su sistema, cómo se les asigna el acceso y cómo se gestionan todos los datos de autentificación. Tiene que hacerse cargo de algunas cosas de la empresa, es decir, si necesita permitir el acceso. Para ello será necesario definir quién puede aprobar dicha excepción de acceso a los usuarios. Lo que se suele hacer es que las organizaciones definen perfiles de usuario y en su caso el acceso debe ser aprobado por el encargado. Se trata como un acceso privilegiado y el propietario del activo debe aprobar la excepción.

Responsabilidades del usuario, se requiere que se defina cómo los usuarios deben mantener su información secreta. Esto se hace de forma general mediante los documentos de política de uso aceptable. Se deben definir las siguientes reglas:

Protección de datos

El Reglamento General de Protección de Datos es cada vez más severo. Las organizaciones que manejan datos personales deben adaptar sus operaciones a los nuevos requisitos para evitar problema con los clientes y las autoridades, pueden hacerlo con la norma ISO 27001.

En lo que respecta a los servicios de infraestructura de la nube, el esfuerzo puede ayudar a los proveedores y a los clientes. En este artículo queremos generar una visión amplia del Código CISPE de Conducta, la forma en que puede ayudar a asegurar el procesamiento de datos personales que se realiza según el Reglamento General de Protección de Datos.

**3.3 Verificar**

**3.3.1 Revisión del Sistema de gestión de seguridad de la información**

La revisión de un sistema de gestión de seguridad de información que realiza la dirección de la organización en este caso el área de administración de la empresa Berendson Natación S.R.L.

Esta revisión le permite a la empresa analizar en que aspectos de mejorar para así cumplir con los objetivos de la organización

Sugerencias por parte de los demás trabajadores para mejorar las políticas y vulnerabilidades que persisten en la empresa.

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.

### 3.3.2 Auditorías internas

Consiste las políticas y procedimientos establecidos en la empresa para proteger su activo, minimizar riesgos, incrementar la eficacia de los procesos operativos y optimizar el negocio.

La persona adecuada o asignada para realizar las auditorías internas en una organización debe tener conocimiento sobre la norma ISO/IEC 27001 para así comprobar que los controles y procedimientos de seguridad sean los adecuados al momento de implementar el modelo.
El auditor responsable debe llevar a cabo las siguientes actividades:

- Una auditoría interna se debe hacer en base a un plan previamente redactado y diseñado, en función de las políticas y procedimientos de la empresa
- Realizar un control de inventarios de los bienes de la empresa
- Descripción de la auditoria, sus objetivos, alcance fechas fases y áreas auditadas
- Vigilancia del cumplimiento de las recomendaciones determinadas en informes y auditorías
- Conclusiones de la auditorias
- Informe sobre fallos e inconformidad por parte de los trabajadores de la empresa
- Evidencias de las irregularidades existentes.

## 3.4 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.

### 4.3 Evaluar el resultado obtenido de la implementación del modelo adaptado en base a la norma ya mencionada.

Tabla 27.

*Conocimiento con respecto a la seguridad de información después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 1 | 25% |
| Bueno | 3 | 75% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

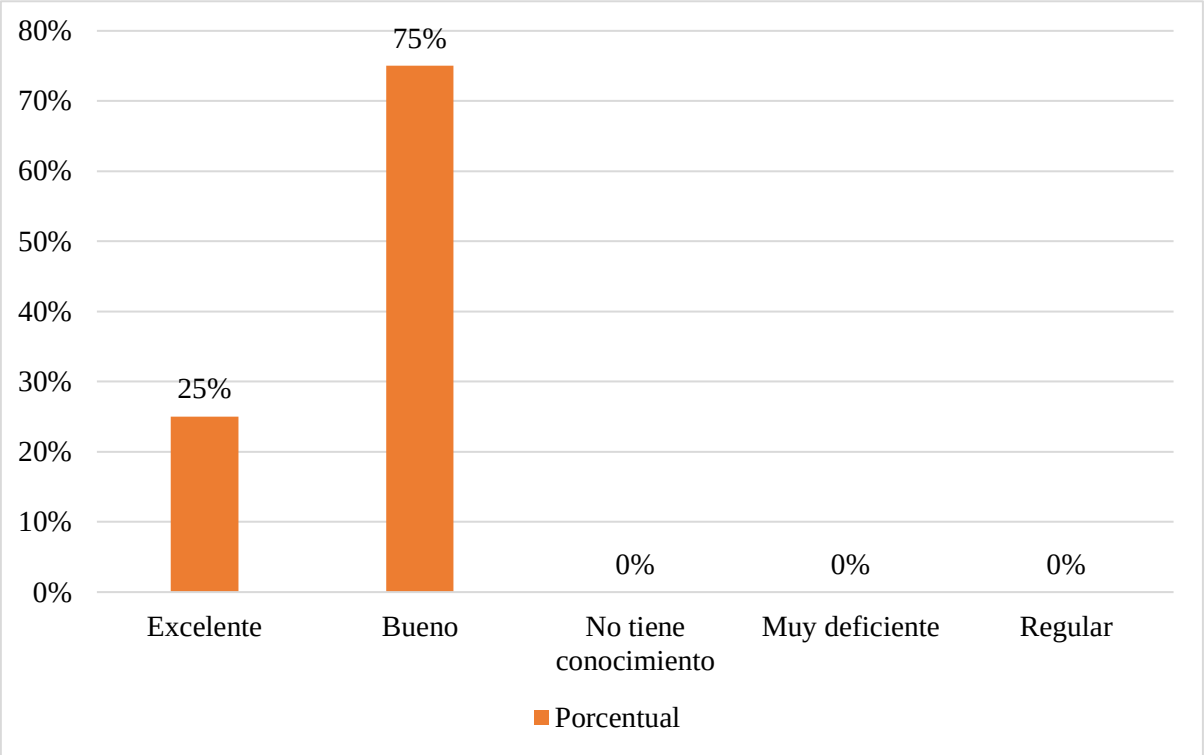



*Figura 18:* Nivel de Conocimiento sobre seguridad de la información después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura 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.

Tabla 28.

*Conocimiento sobre las Normas de Seguridad de Información después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 2 | 50% |
| Bueno | 2 | 50% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

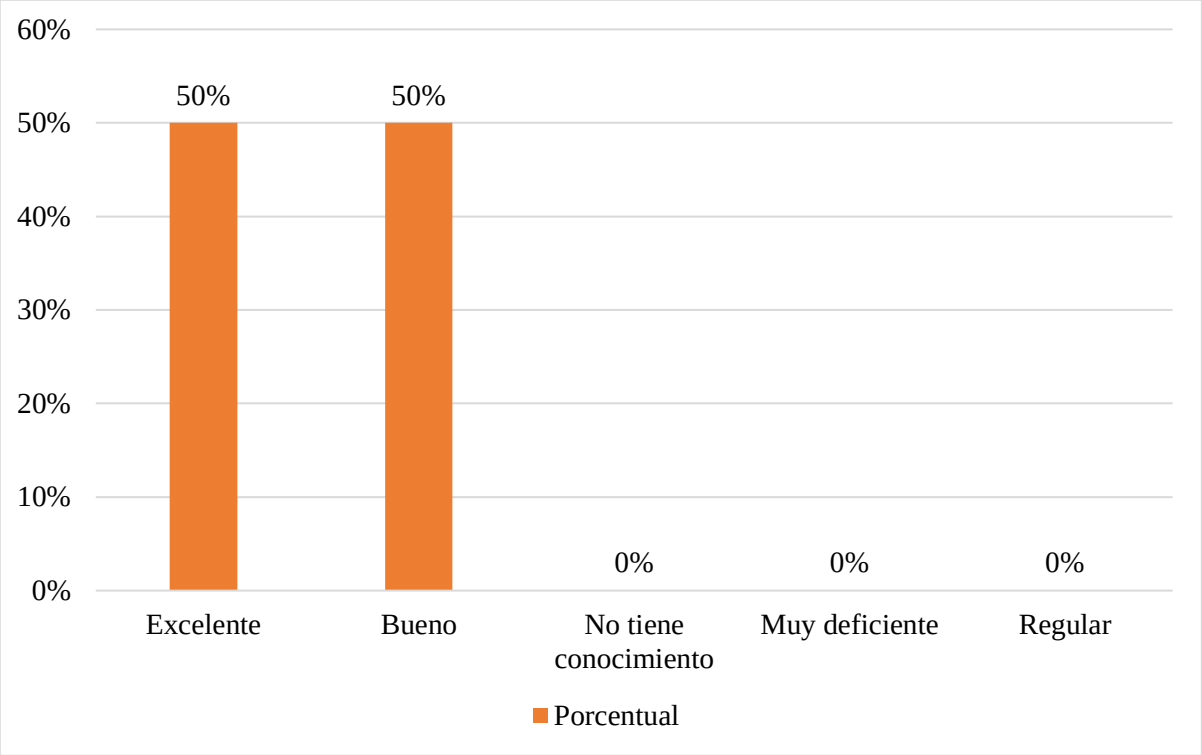



*Figura 19:* Conocimiento sobre las Normas de Seguridad de Información después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 50% de los encuestados considera que tiene un excelente conocimiento sobre las normas que establece de seguridad de la información a diferencia que un porcentaje 50 % menciono que tiene un conocimiento bueno.

Tabla 29.
*Nivel de conocimiento sobre la norma ISO/IEC 27001 después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 4 | 100% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

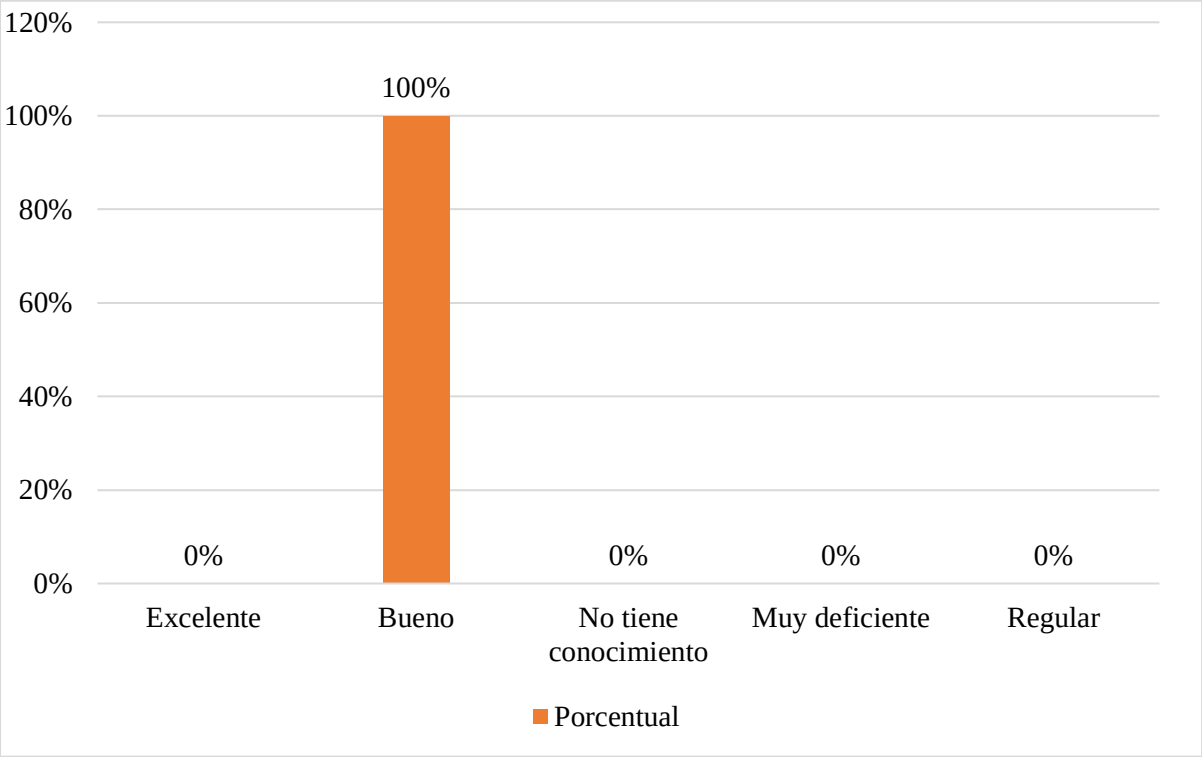



*Figura 20:* Conocimiento sobre la Norma ISO/IEC 27001 después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 100% de los encuestados considera que tiene un conocimiento bueno sobre la norma ISO/IEC 27001.

Tabla 30.
*Conocimiento sobre la ley de Protección de Datos después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 1 | 25% |
| Bueno | 3 | 75% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

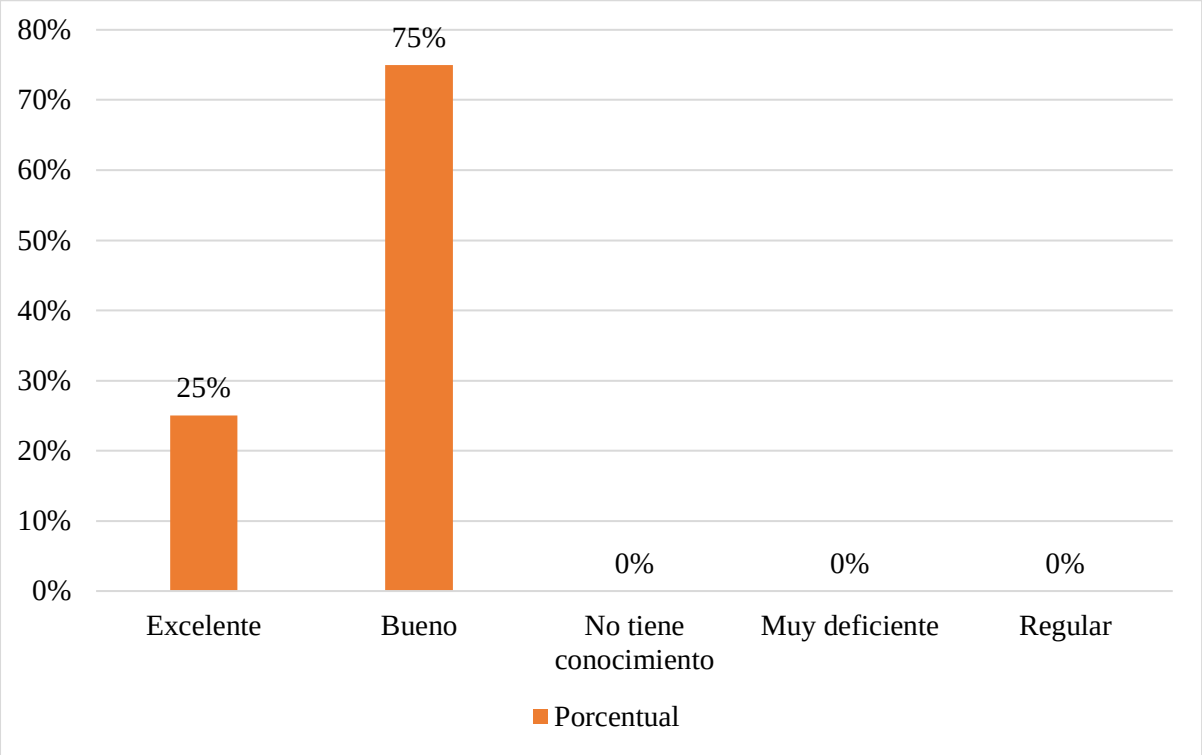



*Figura 21:* Conocimiento sobre la Ley de Protección de Datos después de la capacitación
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa

**Análisis:** En relación a la tabla y figura se observa que el 75% de los encuestados considera que tiene un conocimiento bueno sobre la Ley de Protección de datos a diferencia que de un porcentaje 25 % menciono que tiene un excelente.

Tabla 31.
*Nivel de conocimiento sobre el estado de los Backups después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 4 | 100% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

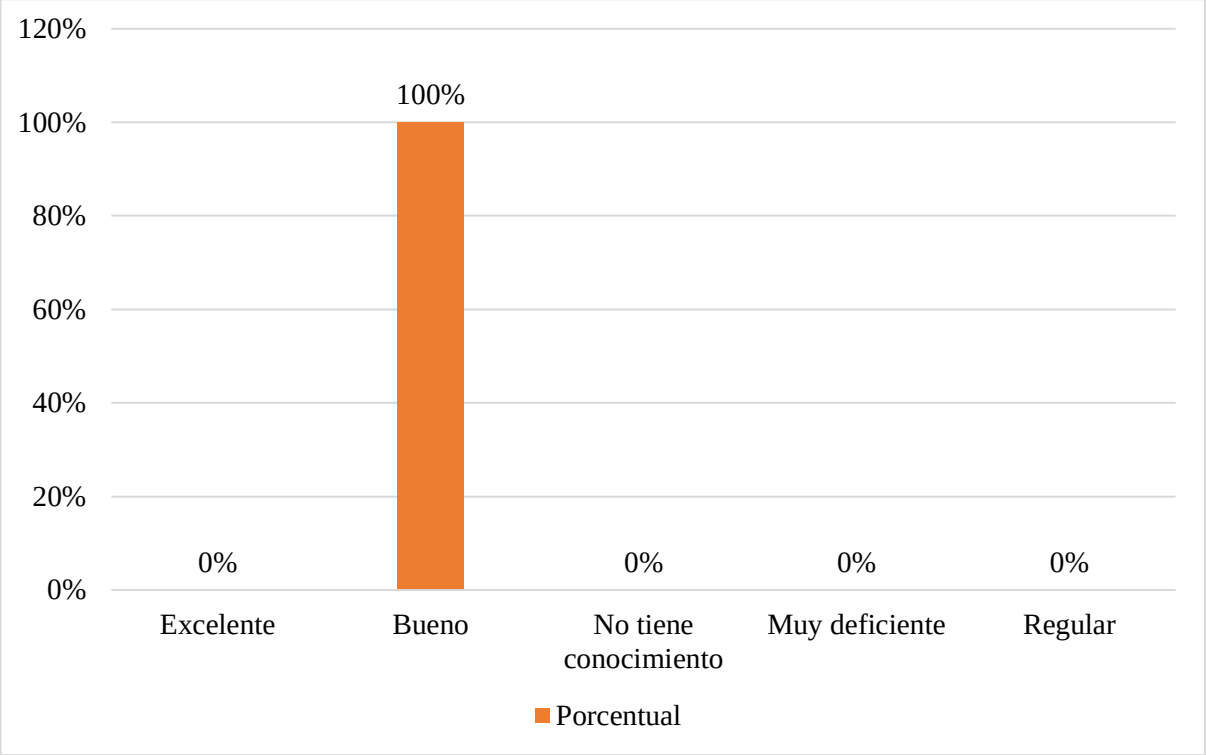



*Figura 22:* Nivel de conocimiento sobre el estado de los Backups después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 100% de los encuestados considera al nivel de conocimiento sobre el estado de los Backups como bueno.

Tabla 32.

*Nivel de seguridad de los sistemas de control después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 2 | 50% |
| Bueno | 2 | 50% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 0 | 0% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

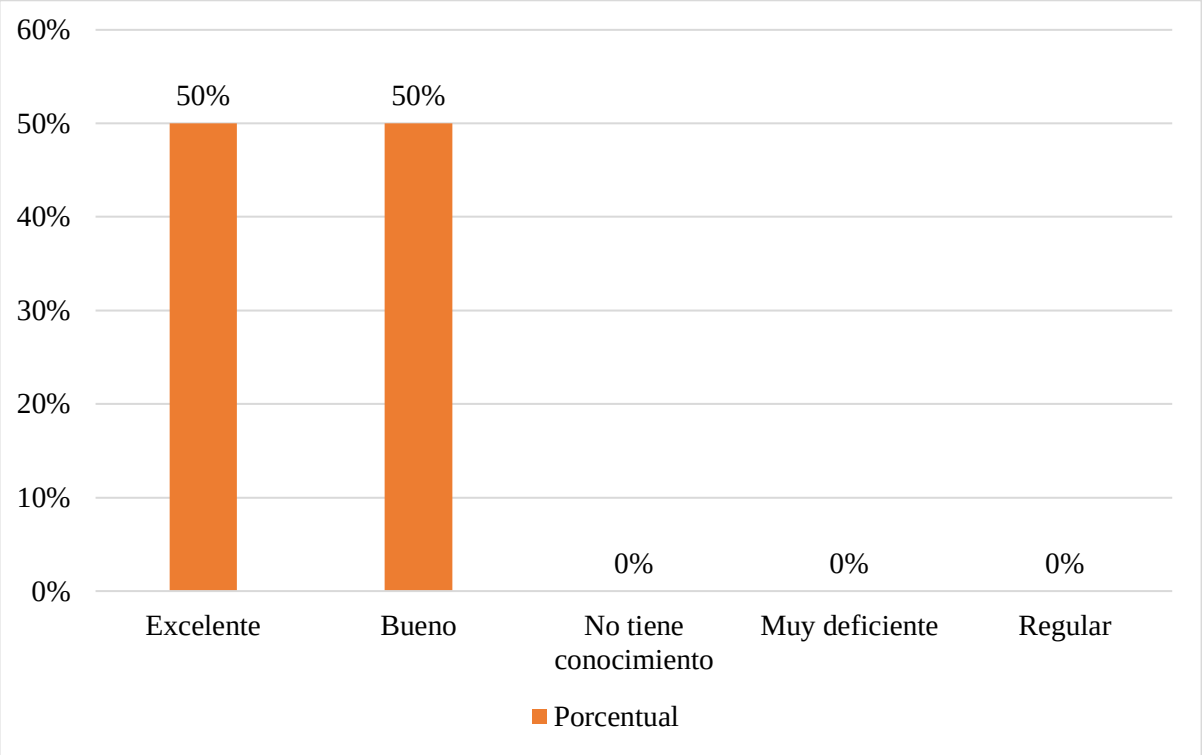



*Figura 23:* Calificación del sistema de control después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura 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 50 % que considera como excelente.

Tabla 33.
*Nivel de seguridad que tienen los servidores después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 1 | 25% |
| Bueno | 2 | 50% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 1 | 25% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

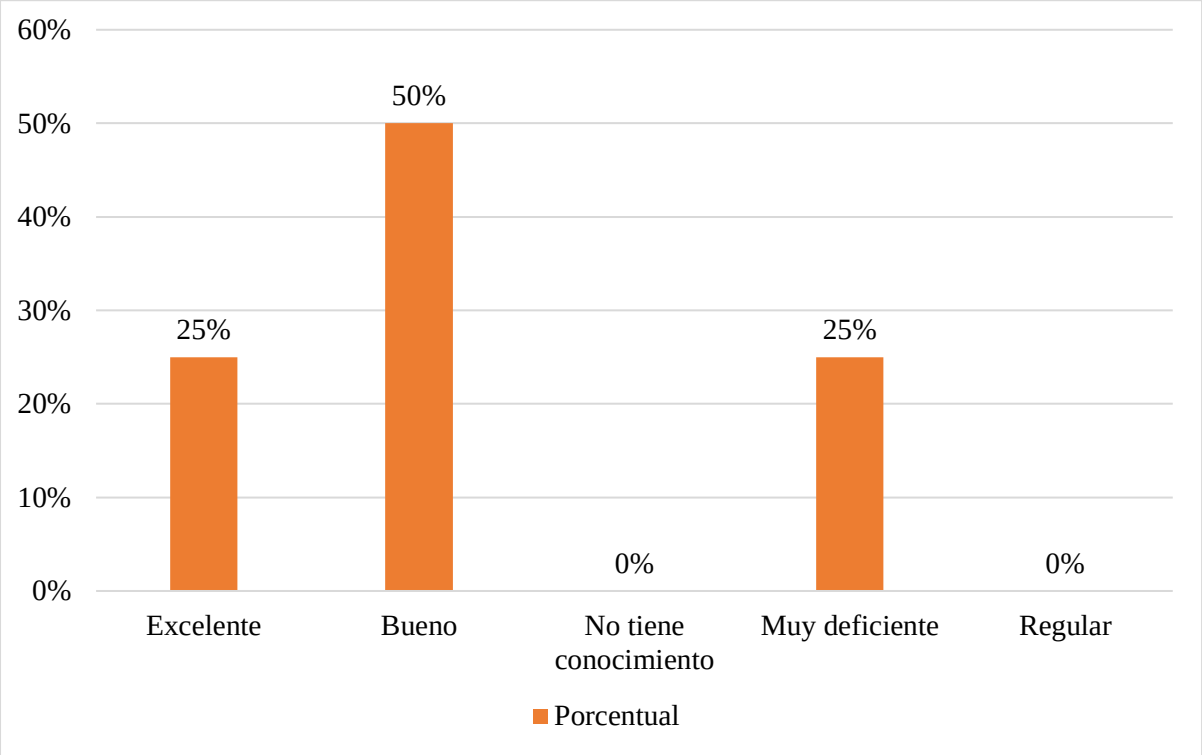



*Figura 24:* Nivel de seguridad que tienen los servidores después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 50% de los encuestados considera como bueno el conocimiento sobre el nivel de seguridad que tienen los servidores a diferencia que un menor porcentaje 25 % considero como excelente y muy deficiente el conocimiento que tiene.

Tabla 34.
Nivel de calificación del antivirus después de la capacitación.

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 3 | 75% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 1 | 25% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

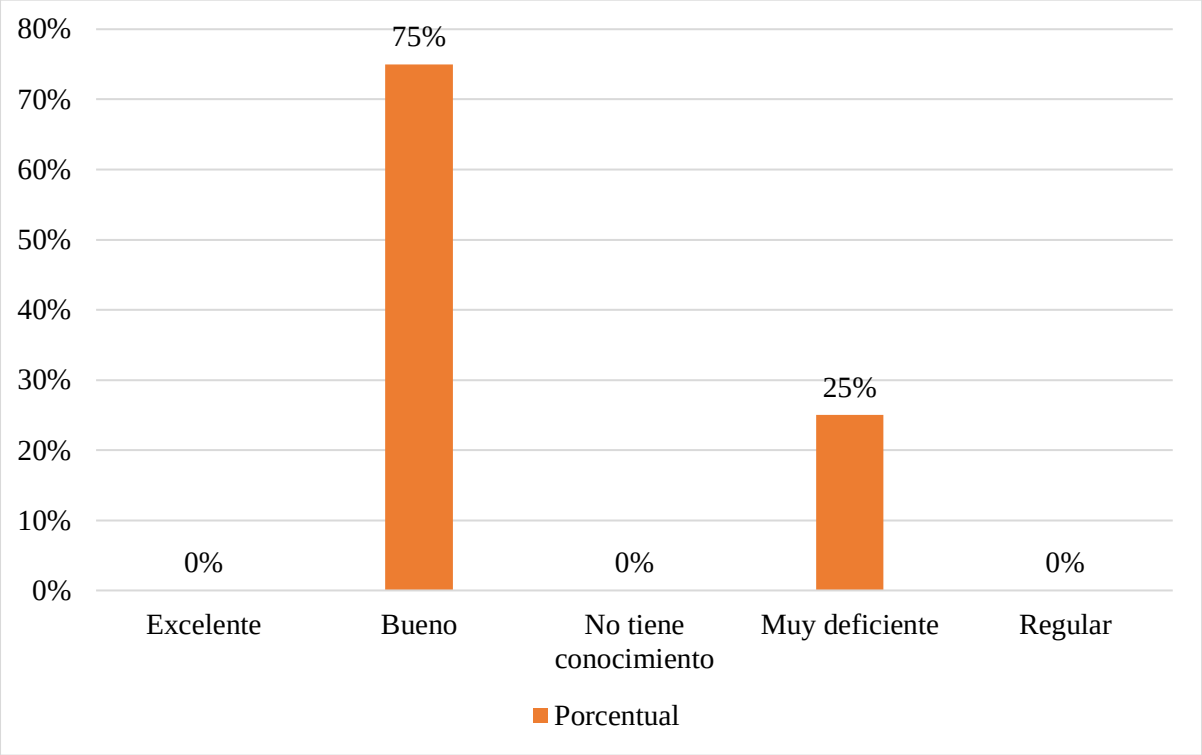



*Figura 25:* Nivel de calificación del antivirus después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 75% de los encuestados considera al nivel de conocimiento sobre la calificación del antivirus como bueno, y un 25 % lo considera como muy deficiente.

Tabla 35.
*Nivel de protección que ofrece el antivirus después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 3 | 75% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 1 | 25% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

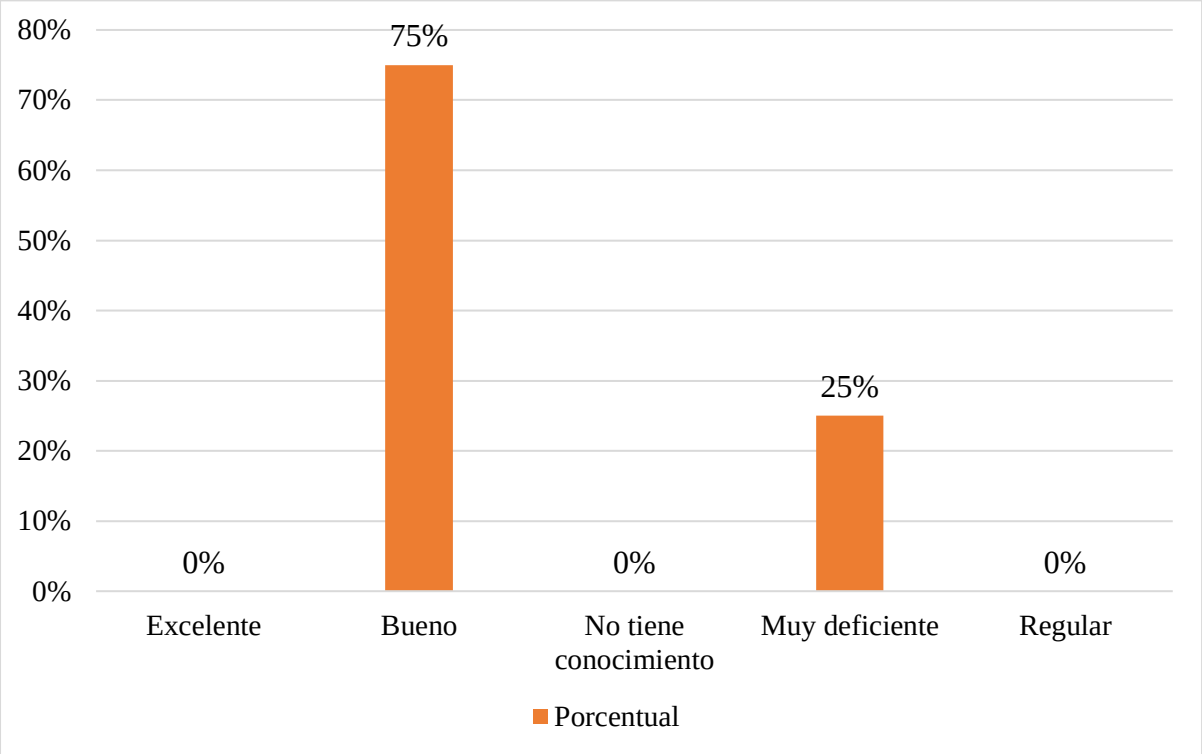



*Figura 26:* Nivel de protección que ofrece el antivirus de la capacitación después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 75% de los encuestados considera bueno el conocimiento sobre el nivel de protección que ofrece el antivirus a diferencia que un menor porcentaje 25% menciono que tiene un conocimiento muy deficiente.

Tabla 36.
*Nivel de Restricción de Páginas después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 1 | 25% |
| Bueno | 1 | 25% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 2 | 50% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

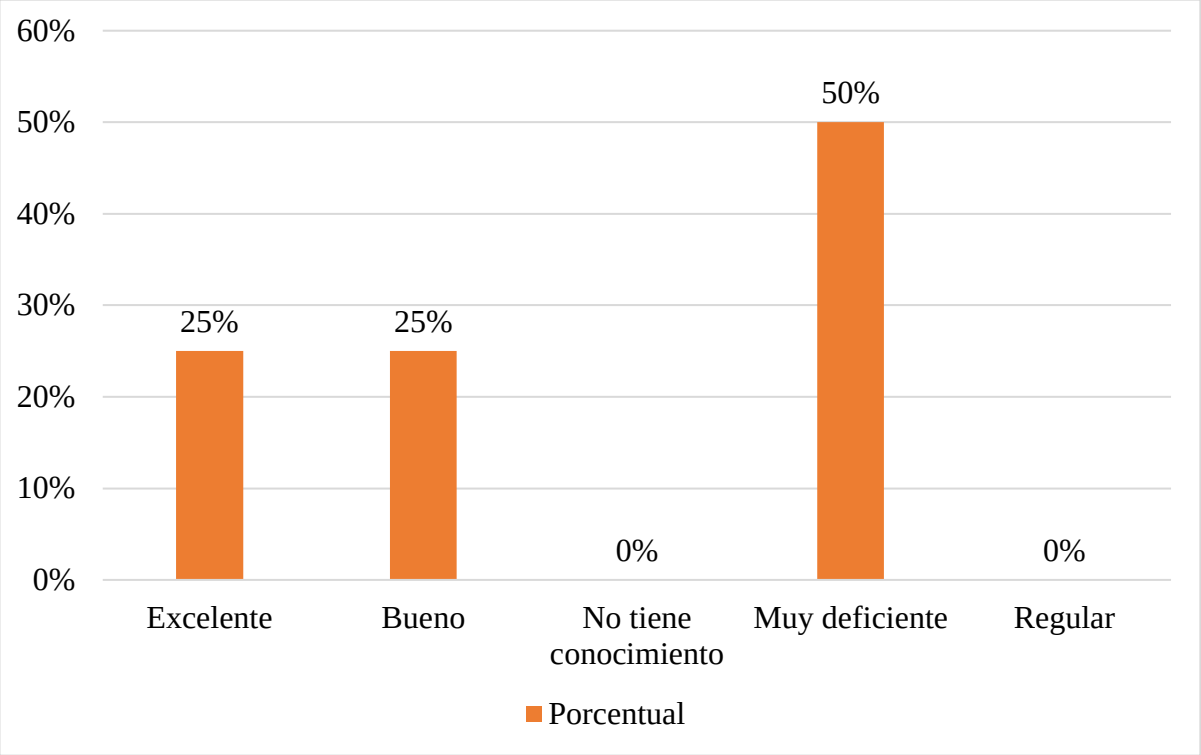



*Figura 27*: Nivel de Restricción de Páginas después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 50% de los encuestados considera sobre el nivel de protección de las paginas como muy deficiente y 25% lo considera como bueno y excelente.

Tabla 37.
*Calificación sobre el Nivel de Password para el ingresas a los sistemas después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 1 | 25% |
| No tiene conocimiento | 0 | 0% |
| Muy deficiente | 3 | 75% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

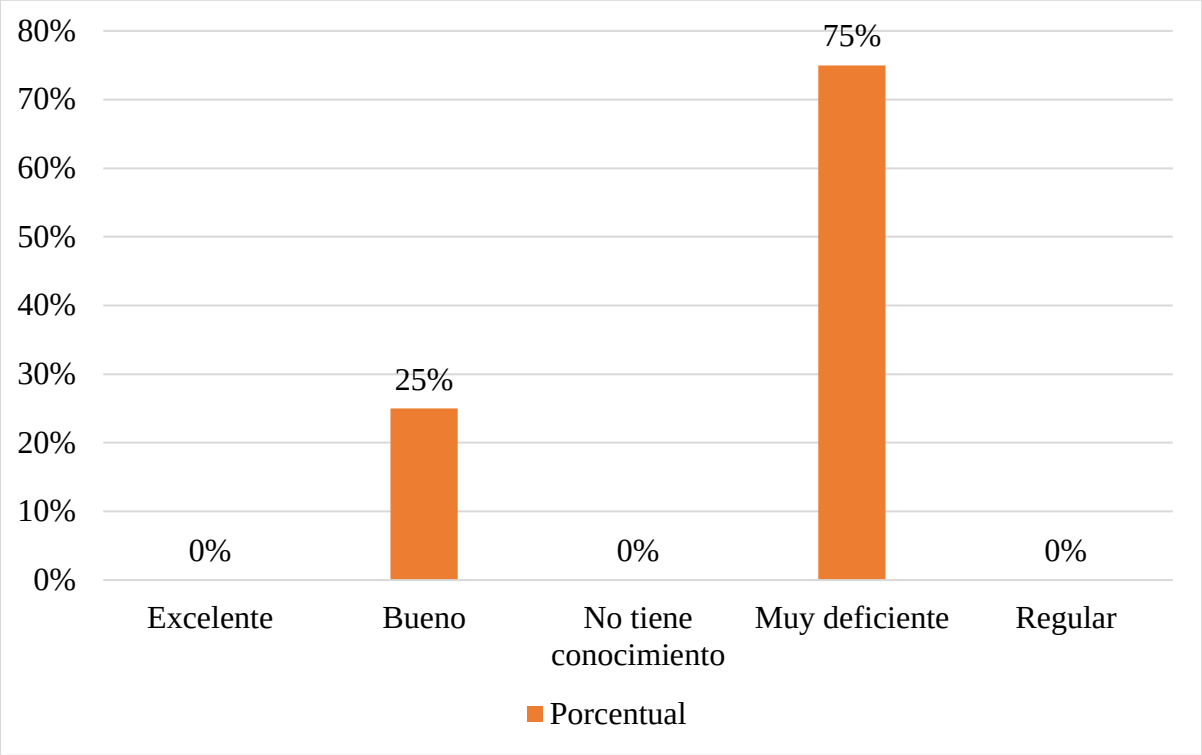



*Figura 28:* Calificación sobre el Nivel de Password para el ingresas a los sistemas después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 75% de los encuestados considera Nivel de Password para el ingresas a los sistemas como muy deficiente, y el otro 25% lo considera como bueno.

Tabla 38.
*El nivel de seguridad cumple con los parámetros establecidos para el ingreso a los sistemas después de la capacitación.*

| Indicadores | Frecuencia | Porcentual |
|---|---|---|
| Excelente | 0 | 0% |
| Bueno | 1 | 25% |
| No tiene conocimiento | 1 | 25% |
| Muy deficiente | 2 | 50% |
| Regular | 0 | 0% |
| **Total** | 4 | 100% |

Fuente: Elaboración propia.

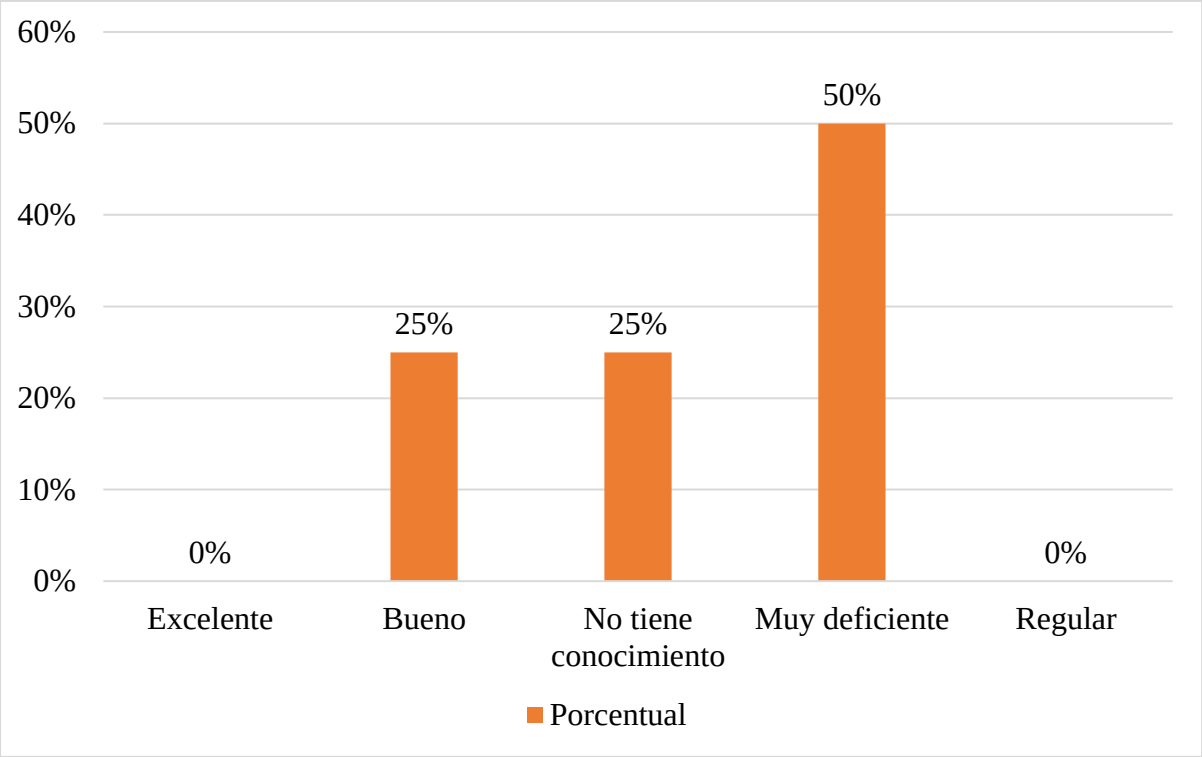



*Figura 29:* El nivel de seguridad cumple con los parámetros establecidos para el ingreso a los sistemas después de la capacitación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En relación a la tabla y figura se observa que el 50% de los encuestados considera sobre el nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema como muy deficiente, a diferencia de un 25% considera como muy bueno y no tiene conocimiento.

**Comparación del antes y después de la capacitación.**

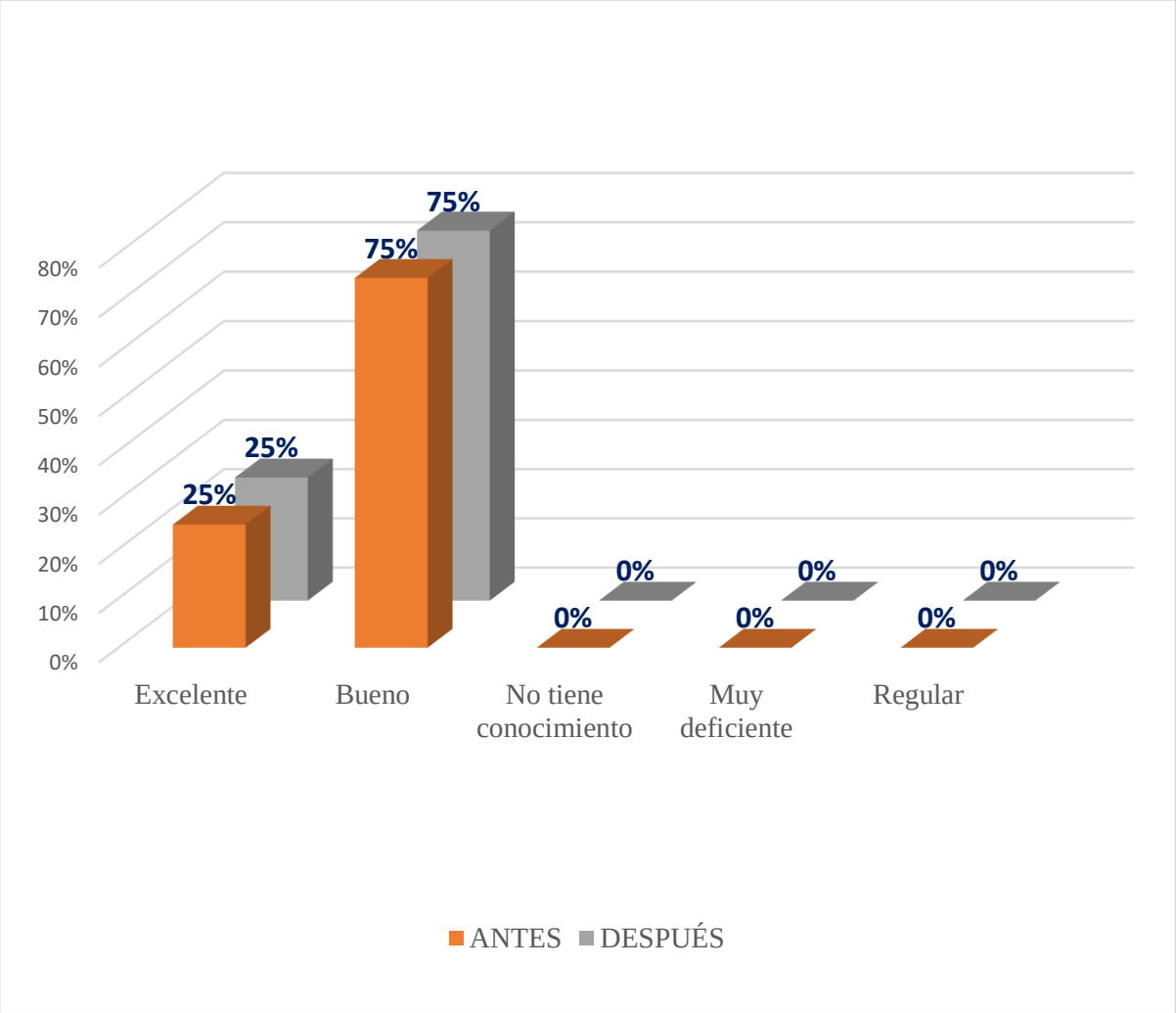



*Figura 30:* Nivel de Conocimiento sobre Seguridad de la Información-Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En la figura se observa que después de la capacitación se ha mantenido los conocimientos sobre el nivel de conocimiento sobre seguridad de la información.

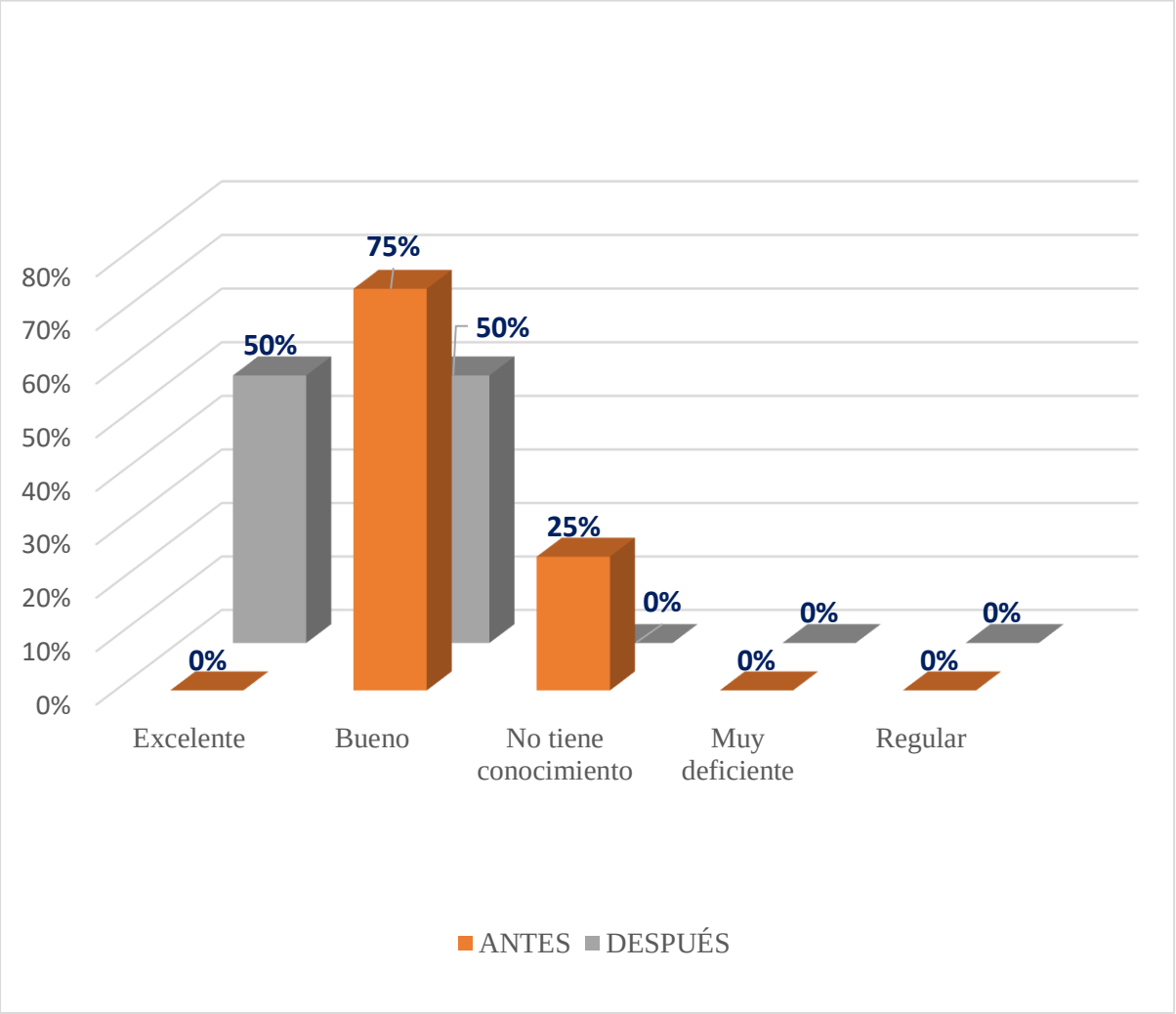



*Figura 31*: Conocimiento sobre las Normas de Seguridad de Información – Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En la figura se observa que después de la capacitación el 25% de la población ha variado a un 50% de conocimiento excelente.

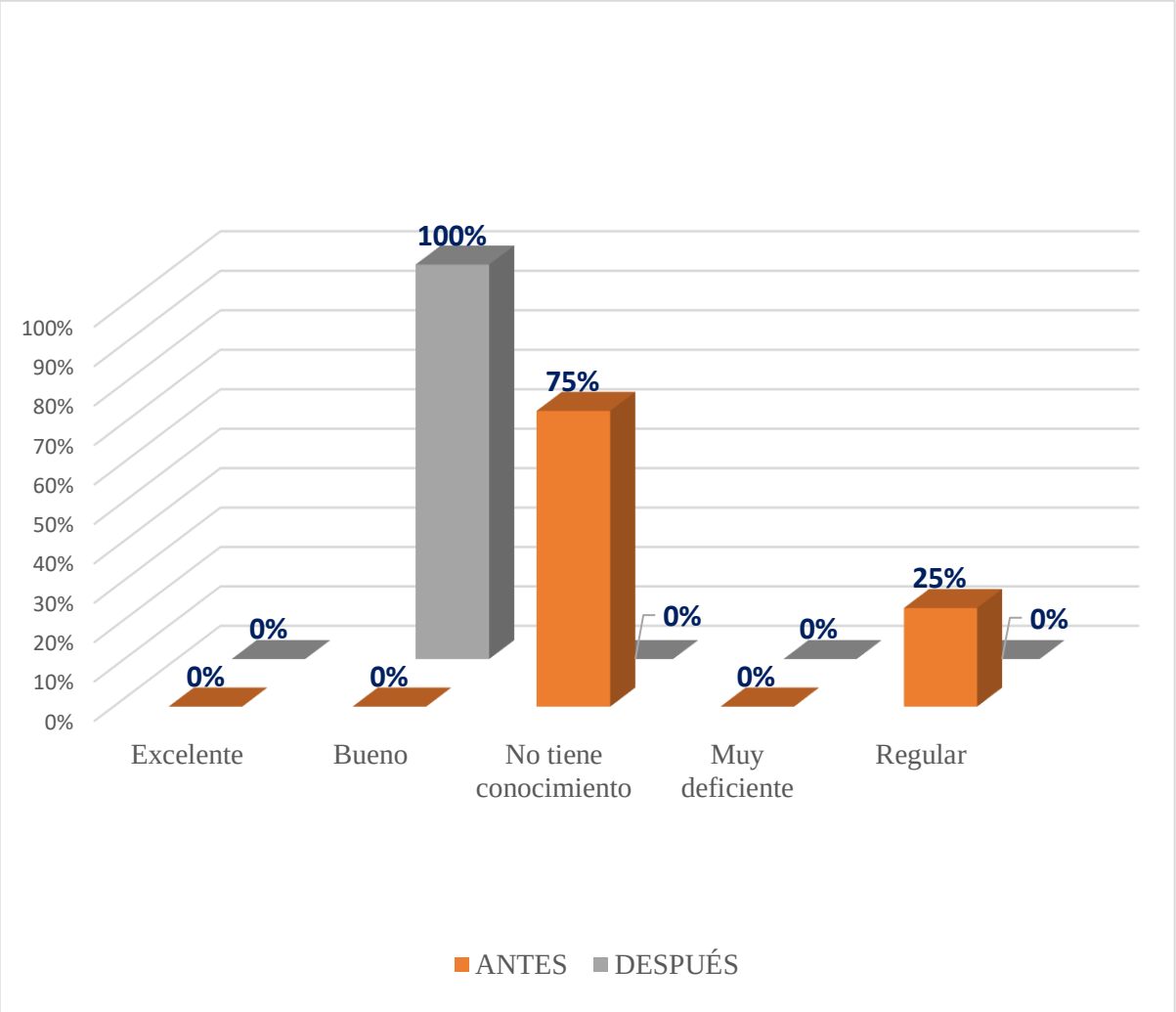



*Figura 32*: Conocimiento sobre la Norma ISO/IEC 27001-Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento son bajos y en las barras gris corresponde a después de capacitación donde se ve un aumento de conocimiento con 100% sobre la norma ISO/IEC 27001.

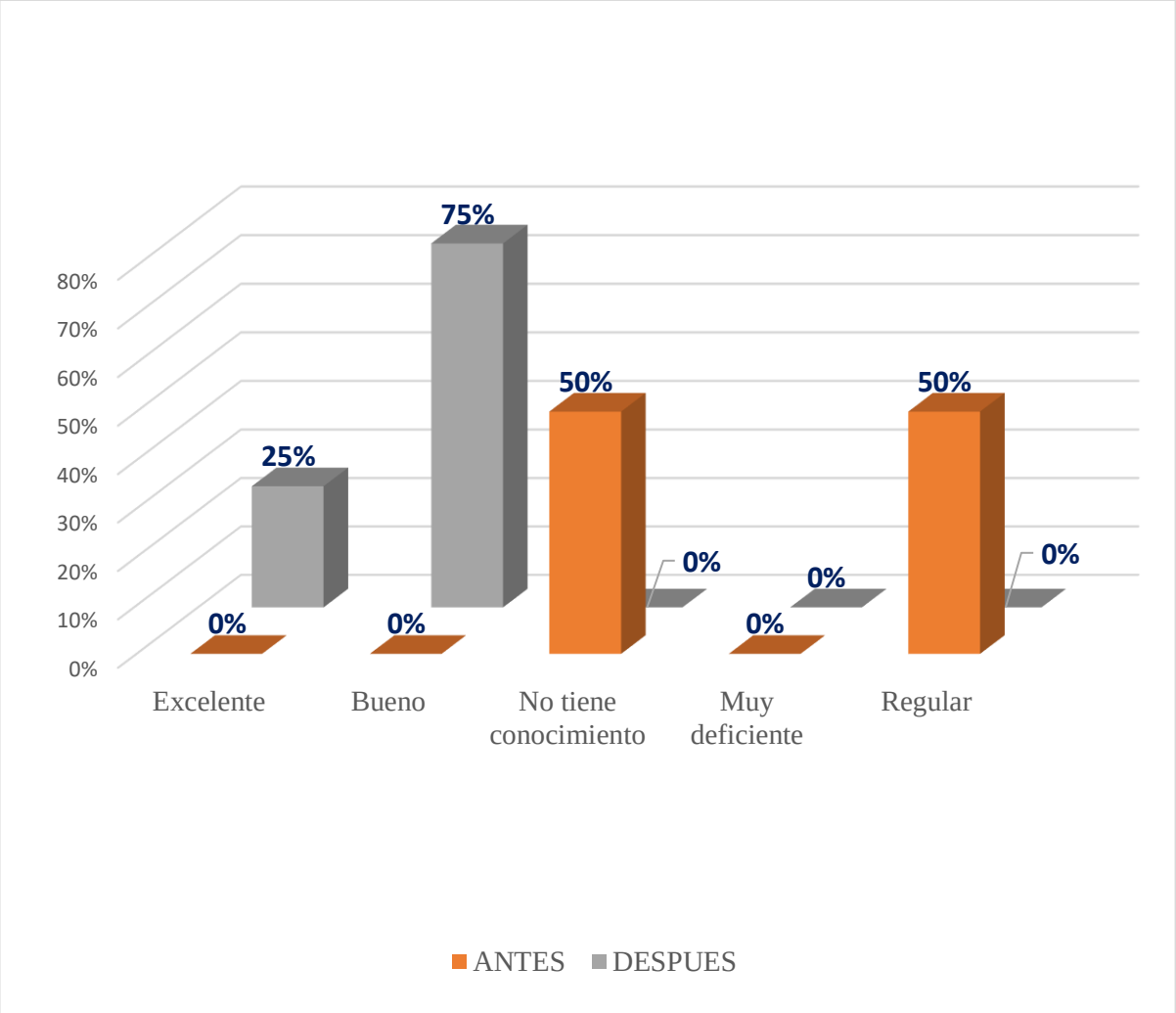



*Figura 33:* Conocimiento sobre la Ley de Protección de Datos-Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento son en no tiene conocimiento y regular son del 50% para cada uno y las barras de grises corresponden a después de la capacitación donde se ve un aumento en el nivel excelente a un 25% y en bueno a un 75% sobre la ley de protección de datos.

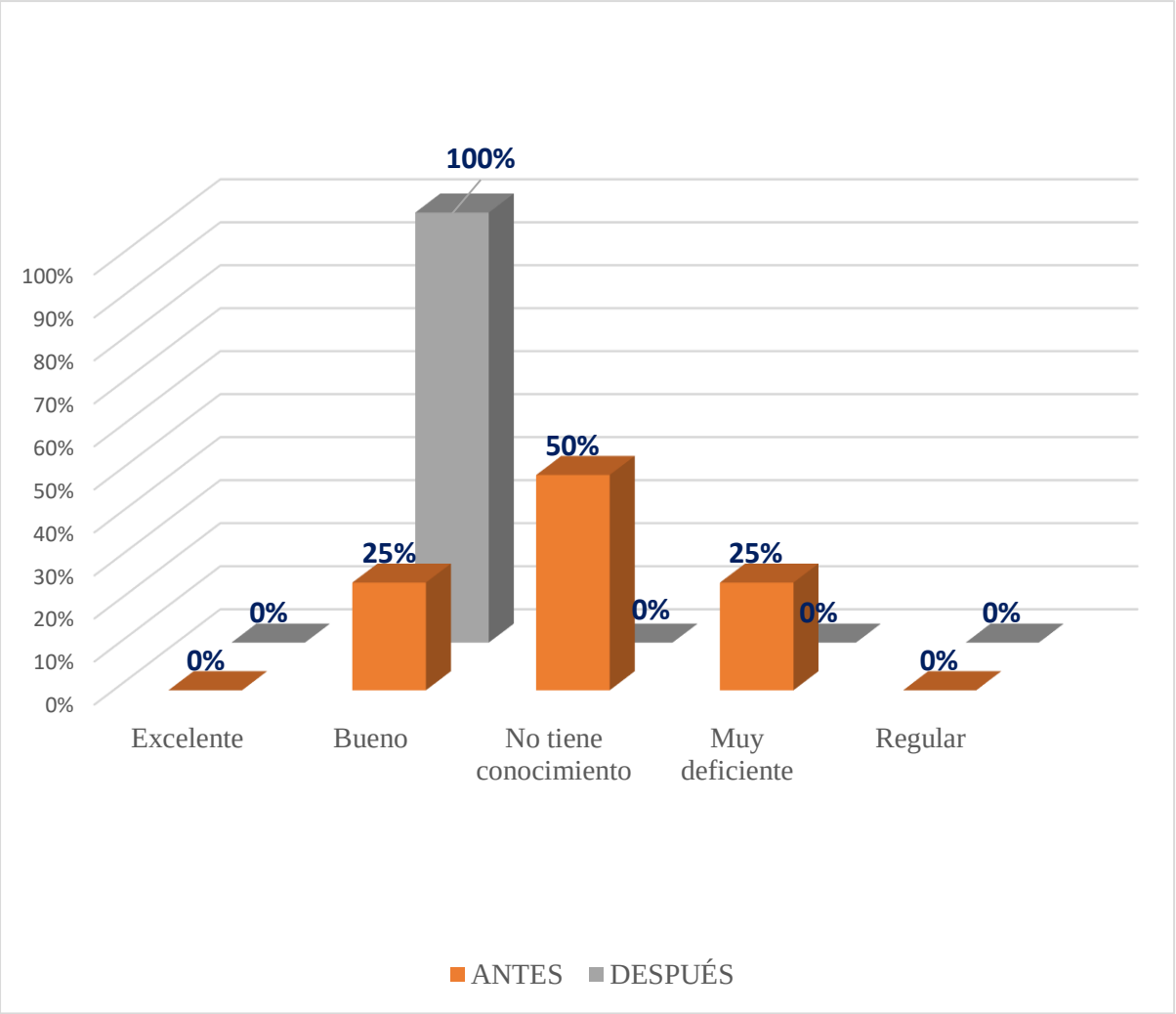



*Figura 34:* Estado de los medios donde se alojan los backups de los servidores – Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento del nivel bueno estaban en un 25%, no tiene conocimiento un 50% y muy deficiente en un 50% para cada uno y las barras de grises corresponden a después de la capacitación donde se ve un aumento en el nivel bueno a un 100% sobre el estado de los medios donde se alojan los backups de los servidores.

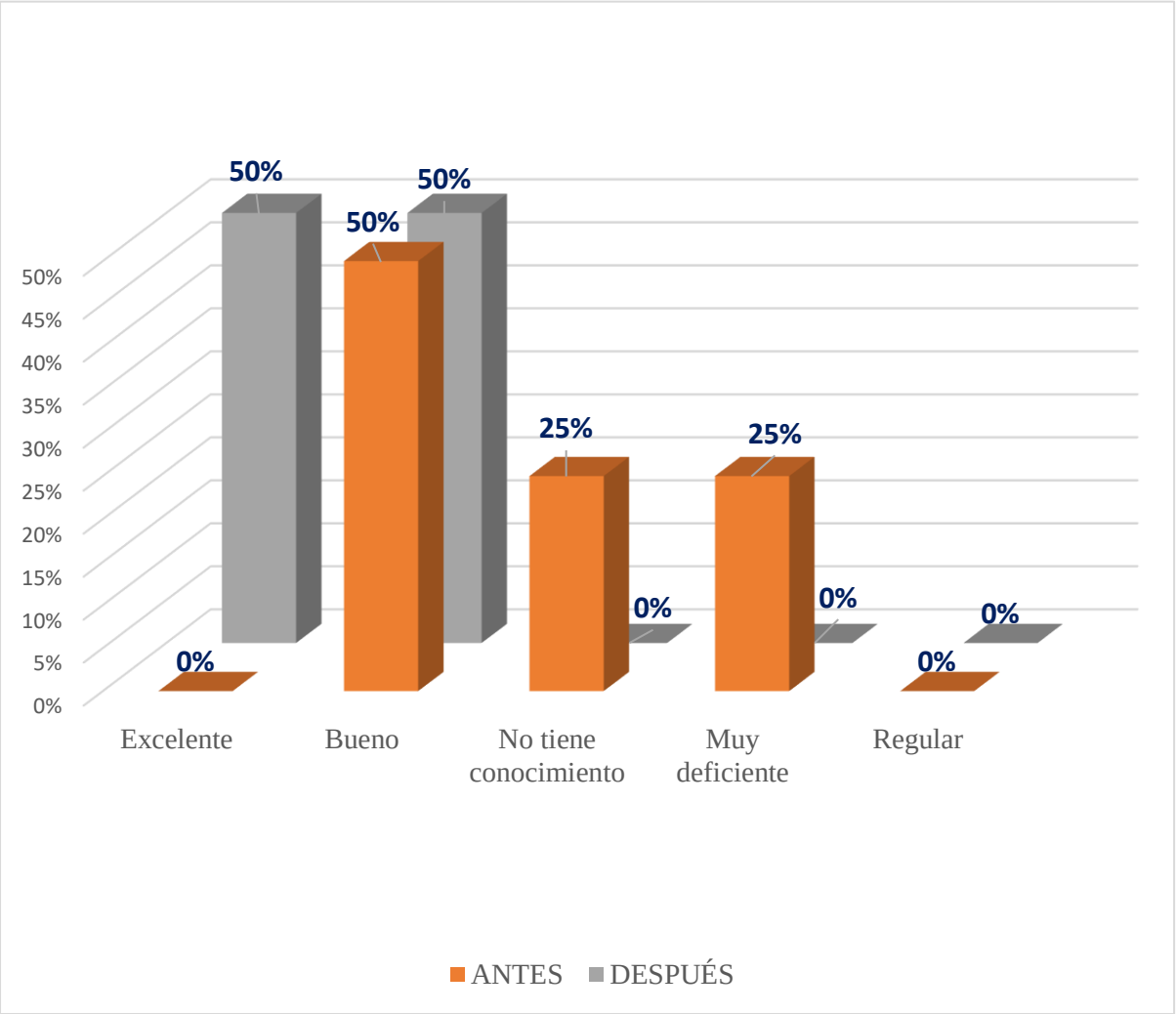
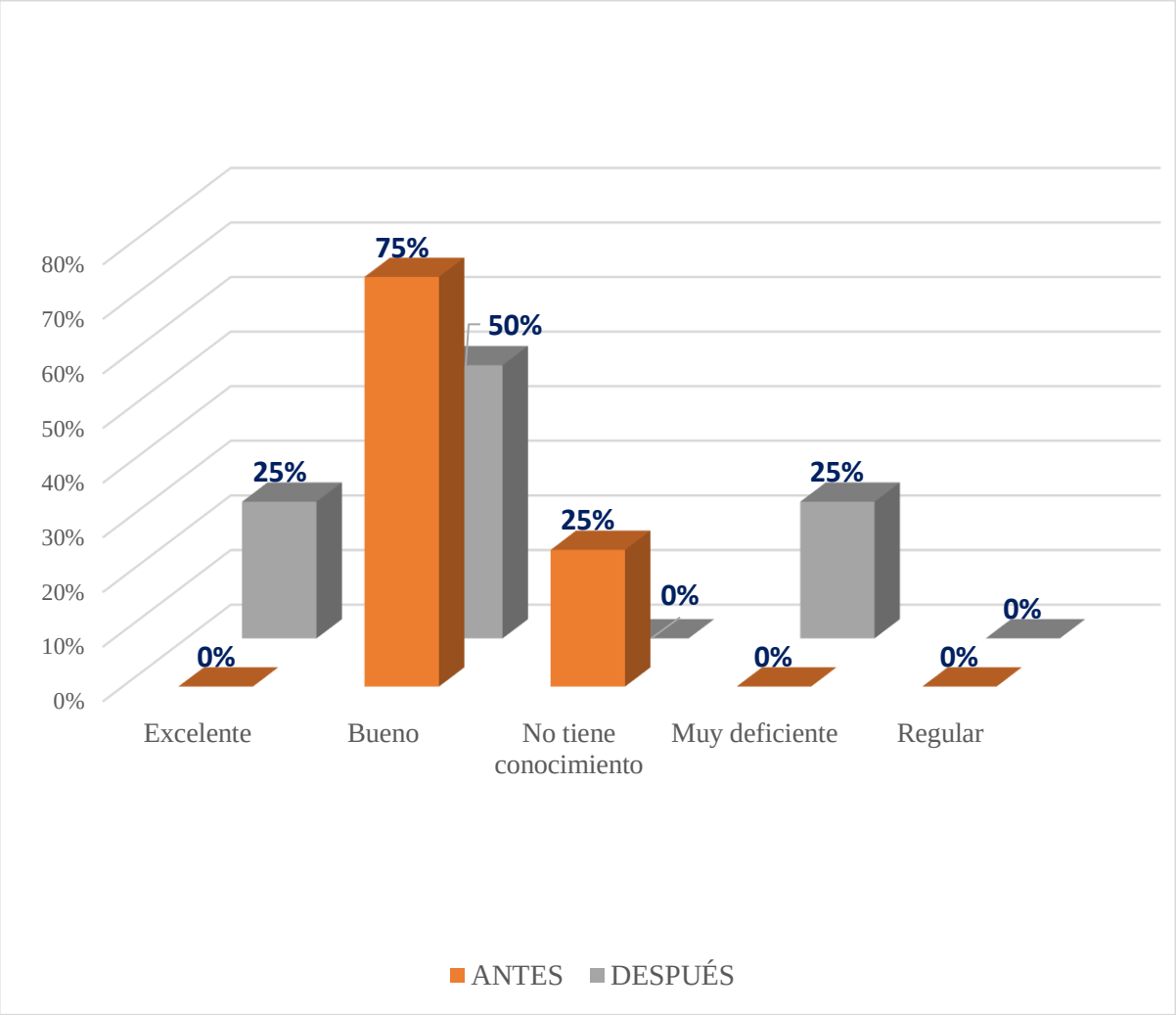



*Figura 35:* Calificación del sistema de control – Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento del nivel bueno estaban en un 50%, no tiene conocimiento un 25% y muy deficiente en un 25% para cada uno y las barras de grises corresponden a después de la capacitación donde se ve un aumento en el nivel excelente a un 50% y en el nivel bueno a un 50% sobre Calificación del sistema de control.




F*igura 36:* Definición del Ingreso a los servidores -Comparación
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento del nivel bueno estaban en un 75%, no tiene conocimiento un 25% para cada uno y las barras de grises corresponden a después de la capacitación donde se ve un aumento en el nivel excelente a un 25%, nivel bueno a un 50% y en muy deficiente en un 25% sobre Definición del Ingreso a los servidores.

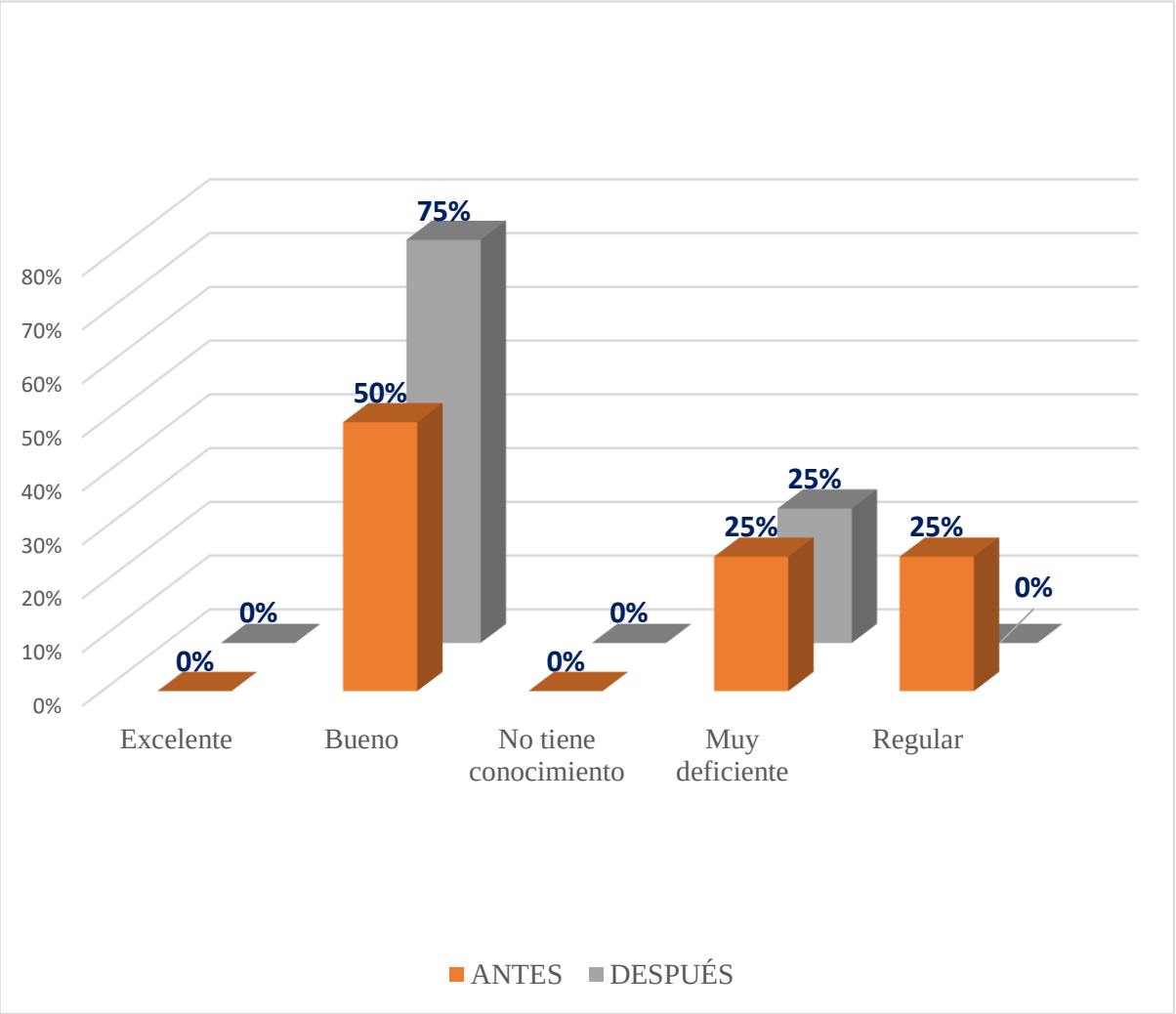



*Figura 37:* Nivel de antivirus-Comparación
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento del nivel bueno estaban en un 50%, muy deficiente era de un 25% y regular de un 25% para cada uno y las barras de grises corresponden a después de la capacitación donde se ve un aumento en el nivel bueno a un 75% sobre Nivel de antivirus.

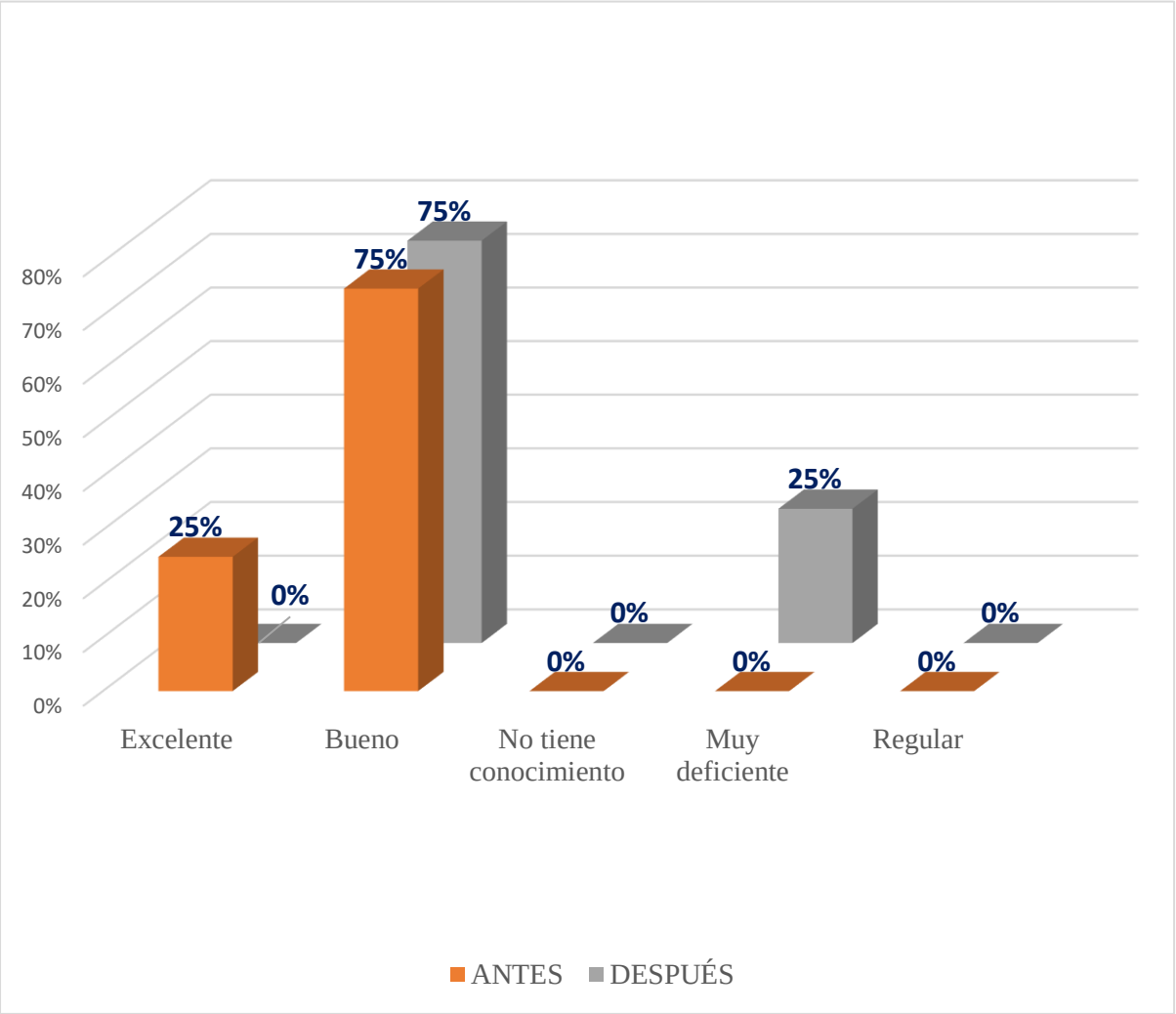



*Figura 38:* Nivel de protección de antivirus-Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento del nivel excelente estaban en un 25%, bueno en un 50% para cada uno y las barras de grises corresponden a después de la capacitación donde se ve un aumento en el nivel bueno a un 75% y muy deficiente en un 25% sobre Nivel de protección de antivirus.

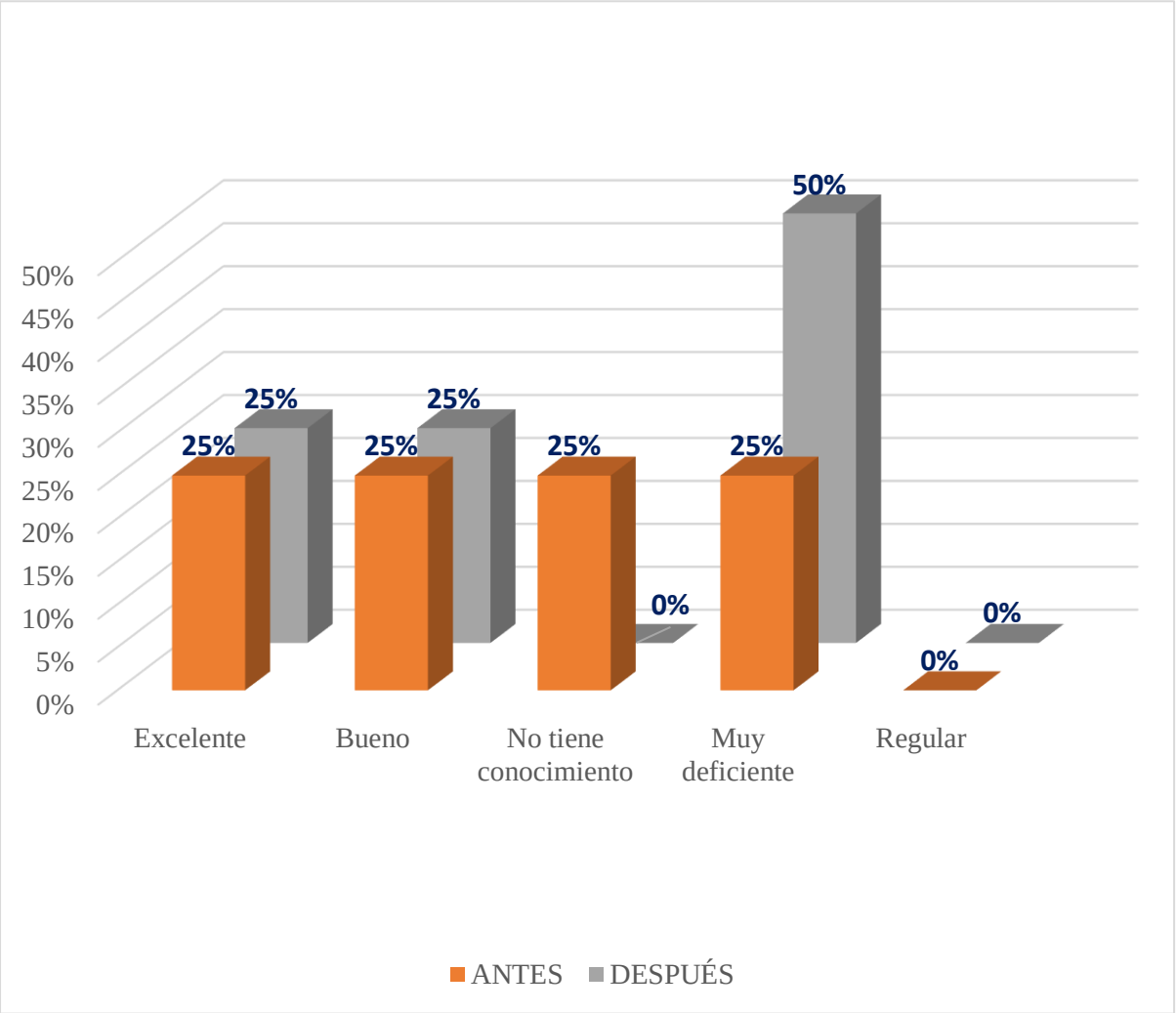



*Figura 39:* Restricción de páginas -Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento del nivel excelente estaban en un 25%, bueno en un 25%, no tiene conocimiento en un 25% y muy deficiente en un 25% para cada uno y las barras de grises corresponden a después de la capacitación donde se ve un aumento en el nivel muy deficiente a un 50% sobre Restricción de páginas.

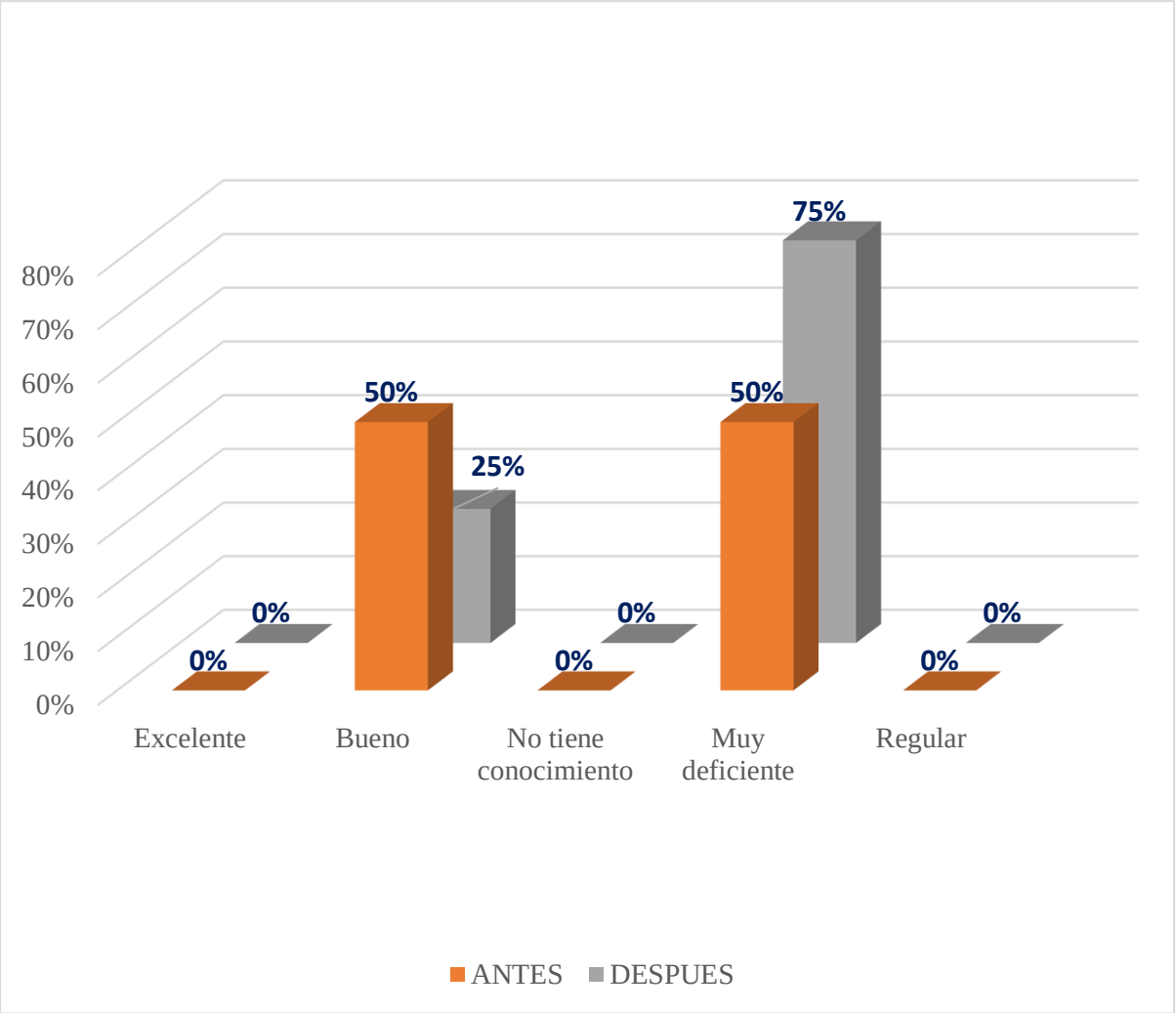



*Figura 40:* Definición de password-Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento del nivel bueno son en un 50%, muy deficiente en un 50% para cada uno y las barras de grises corresponden a después de la capacitación donde se ve un aumento en el nivel bueno a un 25% y en muy deficiente en un 75% sobre Definición de password.

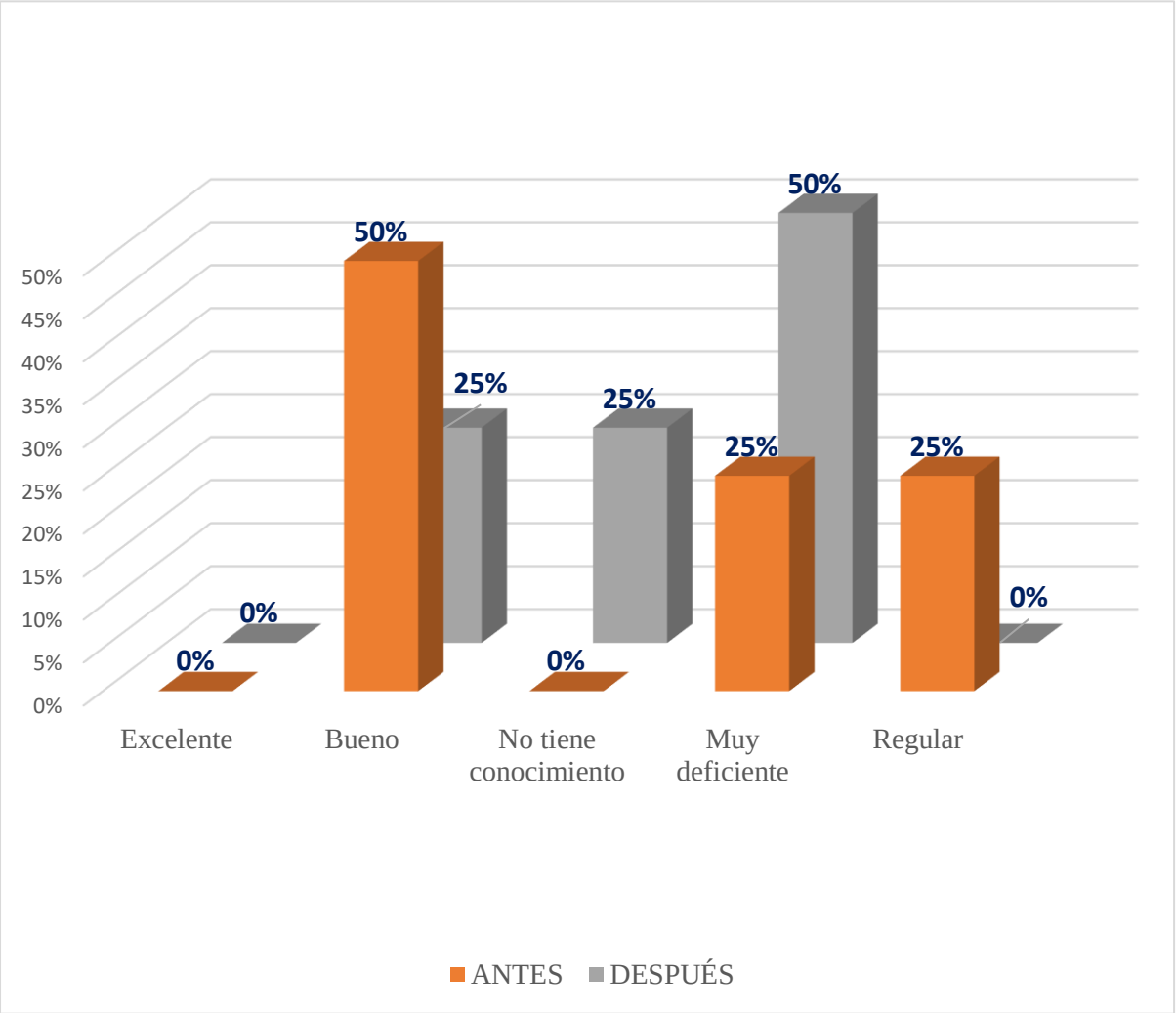



*Figura 41:* Nivel de seguridad al ingreso de sistemas-Comparación.
Fuente: Datos obtenidos en la encuesta aplicada a las áreas de la empresa.

**Análisis:** En el grafico se observa las barras anaranjadas que corresponden al antes de la capacitación donde los niveles de conocimiento del nivel bueno son en un 50%, muy deficiente en un 25% y regular en un 25% para cada uno y las barras de grises corresponden a después de la capacitación donde se ve un aumento en el nivel bueno a un 250% , muy deficiente en un 25% y en no tiene conocimiento en un 25% sobre Nivel de seguridad al ingreso de sistemas.

## V. Discusión

De acuerdo con el objetivo específico D*iagnosticar la situación actual en la que se encuentra la empresa sobre sus amenazas de protección de sus activos*, entre el personal que labora en Berenson S.R..L, se evidenció que en la tabla 8 y figura 7 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 trabajadores de Berendson S.R.L. Estos resultados son similares a los obtenidos en Moyano & Suarez, (2017), en la tesis para optar el título de ingeniero telemático *"Plan de implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y Soluciones" Bogotá – 2017,* en el cual se registró que respecto a la seguridad física y ambiental se ve que en la escala *Buena* un 50%, seguido de *No tiene conocimiento* 30% y finalmente un 20% *Regular.* Esto indica que las empresas no llegan a darle la importancia correspondiente a los asuntos de seguridad de la información.

Según el objetivo específico *Evaluar el resultado obtenido de la implementación del modelo adaptado en base a la norma ISO/IEC 27001,* en la figura 32 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 para optar el título de ingeniero de sistemas e informática "*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*" Huánuco – 2017, en la cual se registró después de la realización de una capacitación donde al realizar una pregunta sobre el conocimiento de las políticas de seguridad de información que se aplica en su área de trabajo, (antes 33 personas desconocían las políticas de seguridad, después 33 personas están más informados sobre las políticas de seguridad), 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.

## VI. Conclusiones

Al momento de realizar el diagnostico en la empresa Berendson Natación S.R.L. se obtuvo que los trabajadores 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. Los trabajadores 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.

## VII. 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 perdidas de información y económicas y se puedan hacer las copias de seguridad cada cierto tiempo.

## VIII. Referencias bibliográficas


Aguirre, J.;Aristizabal, C. (2013). *Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda.* (Proyecto de grado), Universidad Tecnológica de Pereira, Pereira. Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

Agurto, M. (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*. (Tesis para obtener el titulo profesional de ingeniero de sistemas), Universidad de Cesar Vallejo, Piura. Obtenido de http://repositorio.ucv.edu.pe/handle/UCV/11917?show=full

Alcantara, J. (2015). *Guía De Implementación De La Seguridad Basado En La Norma ISO/IEC 27001, Para Apoyar La Seguridad En Los Sistemas Informáticos De La Comisaria Del Norte P.N.P En La Ciudad De Chiclayo.* (Tesis Para Optar El Título De Ingeniero De Sistemas Y Computación ), Universidad Católica Santo Toribio De Mogrovejo, Chiclayo. Obtenido de http://tesis.usat.edu.pe/bitstream/20.500.12423/539/1/TL_Alcantara_Flores_JulioCesar.pdf

Analisis de Riesgos en Sistemas. (2019). Analisis 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

Bastidas, H.;Lopez, I.;Peña, H. (2014). *Análisis de riesgos y recomendaciones de seguridad de la información al aréa de información y tecnología del hospital Susana López de Valencia de la ciudad de Popayán.* (Trabajo de especialización en Seguridad Informatica), Universidad Nacional Abierta y a Distancia, Bogotá. Obtenido de https://repository.unad.edu.co/handle/10596/2668

Bermudez, K.;Bailón, E. (2015). *Analisis De Seguridad Informática Y Seguridad De La Información Basado En La Norma ISO/IEC 27001 - Sistema De Gestión De Seguridad De Seguridad De La Información Dirigido A Una Empresa De Servicios Financieros.* (Obtener El Titulo De Ingeniero De Sistemas), Universidad Poltécnica Salesiana Sede Guayaquil, Guayaquil. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf

Business School. (2018). *Business School*. Obtenido de Business School: https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-de-la-informacion-un-conocimiento-imprescindible?fbclid=IwAR2HbEnVWeXgBf5lGPHOxc4kAzqmP2FNo6P_cNP6CSffvxaeTq9GlNo2hxA

Castro, J. (2018). *Implementación de la NTP ISO/IEC 27001:2014 para mejorarla gestión de seguridad es los sistemas de informacion de la autoridad portuaria nacional.* (Para obtener el título de ingeniero de sistemas), Universidad Autonoma del Perú, Lima, Perú. Obtenido de

http://repositorio.autonoma.edu.pe/bitstream/AUTONOMA/587/1/Castro%20Siguas%20Joshimar.pdf

Espinoza, H. (2013). *Análisis Y Diseño De Un Sistema De Gestión De Seguridad De Información Basado En La Norma Iso/Iec 27001:2005 Para Una Empresa De Producciónу Comercialización De Productos De Consumo Masivo.* Pontifica Universidad Catolica Del Peru. Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/4957/ESPINOZA_HANS_ANALISIS_SISTEMA_GESTION_SEGURIDAD_INFORMACION_ISO_IEC%2027001_2005_COMERCIALIZACION_PRODUCTOS_CONSUMO_MASIVO.pdf?sequence=1&isAllowed=y

Fernámdez , 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.* (Para optar el título de ingeniero de sistemas y computación) , Chiclayo. Obtenido de http://tesis.usat.edu.pe/bitstream/20.500.12423/540/1/TL_FernandezFernandezDamaris.pdf

INCIBE. (2019). Analisis de riesgos en 6 pasos . Obtenido de https://www.incibe.es/en/node/2789

Incibe. (2017). *Incibe*. Obtenido de Incibe: https://www.incibe.es/en/node/2789

ISOTools. (2018). *ISOTools*. Obtenido de ISOTools: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Lara,C. (2014). *Metodología de Evaluación de Riesgos Informáticos*. Obtenido de Metodología de Evaluación de Riesgos Informáticos: http://metodologiaoctave.blogspot.com/2014/03/metodologia-octave.html

Mogollón, A. (2019). *Análisis Comparativo: Metodologías de análisis de Riesgos.* (Diplomado Seguridad de la Información), Universidad Centroccidental "Lisandro Alvarado" Decanato de Ciencias y Tecnología, Venezuela. Obtenido de https://es.scribd.com/document/392217869/Analisis-Comparativo-Metodolo-pdf

Molano, R. (2017). Estrategia para Implementar un Sistema de Gestión de da Seguridad de da Información basada en la Norma ISO 27001 en el Área de ti para la Empresa Market Mix. *(Para obtener el título de Especialista en Auditoria de Sistemas)*. Bogotá D.C. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/15240/1/Esp%20Auditoria%20de%20sistemas.pdf

Molina, M. (2015). *Propuesta de un Plan de Gestión de un Plan de Gestión de Riesgo en Tecnología aplicado en la Escuela Superior Politécnica del Litoral.* (Tesis Titulo de Máster), Universidad Politécnica de Madrid, España. Obtenido de http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Moyano, L.;Suarez, Y. (2017). *Plan de Implementación de SGSI badaso en la norma ISO: 27001 :2013 para la empresa de interfaces y soluciones* . (Optar El Titulo De Ingenieria

En Telematica), Universidad Distrital Francisco Jose De Caldas, Bogota,D.C. Obtenido de http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

Paula, R.;Rosario, M. (2016). *Análisis De La Gestión De La Seguridad De Tecnologías De La Información (Ti), en las Pequeñas Y Medianas Empresas De San Francisco De Macorís, República Dominicana, Año 2014.* (Titulo Para Optar Maestria Profesionalizante En Auditoria Y Seguridad Informatica), Universidad Autonoma Santo Domingo, San Francisco De Macorì. Obtenido de https://es.slideshare.net/ramonpaula08/tesis-sobre-el-analisis-de-la-gestion-de-seguridad-de-ti-en-las-pymes-de-la-ciudad-de-sfm-ao-2014

Quincho, M. (2017). *Diseño De Un Sistema De Gestión De Seguridad De Lainformación Bajo La Ntp Iso/Iec 27001:2014 Para La Municipalidad Provincial De Huamanga, 2016.* (Para optar el título profesional de Ingeniero Informático), Universidad Nacional De San Cristóbal De Huamanga, Ayacucho. Obtenido de http://repositorio.unsch.edu.pe/bitstream/handle/UNSCH/1751/TESIS%20SIS48_Cce.pdf?sequence=1&isAllowed=y

Raiño, K. (2014). *Prezi*. Obtenido de Prezi: https://prezi.com/ngl5q3q8050-/cramm-metodologia-de-evaluacion-y-gestion-del-riesgo/?fbclid=IwAR177dY2rD2zMua5ICNMkO8C-Y2RAtKlfByayEQwyINz7-6WhNaJkkL7Lgo

Restrepo, D. (2018). *Prezi*. Obtenido de Prezi: https://prezi.com/p/sccr7ktzwcry/metodologia-ebios/

Romero, A. (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.* (Para optar el título profesional de ingeniero de sistemas), 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

Sandoval, J. (2017). Diseño de un Plan De Seguridad de la Informacion para el Centro De Informatica Y Telecomunicacionesde la Universidad Nacional De Piura, periodo 2015-2018. *(Para optar el Título de Ingeniero Informático).* Universidad Nacional de Piura, Piura. Obtenido de http://repositorio.unp.edu.pe/bitstream/handle/UNP/1165/IND-SAN-QUI-17.pdf?sequence=1&isAllowed=y

Tecnicas de Recolección de Datos. (2018). *Tecnicas de Recolección de Datos.* Obtenido de Tecnicas de Recolección de Datos: https://gabriellebet.files.wordpress.com/2013/01/tecnicas-de-recoleccic3b3n4.pdf

*Tecon*. (2019). Obtenido de https://www.tecon.es/la-seguridad-de-la-informacion/

Tibaquira, Y. (2015). *Metología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en el estándar ISO/IEC 27035 y norma ISO/IEC 27005.* (Titulo de especialista en Seguridad

Informática), Universidad Nacional Abierta y a Distancia, Bogotá. Obtenido de http://mendillo.info/seguridad/tesis/Tibaquira.pdf

Vilca, E. (2017). *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 obtener el título prodesional de ingeniero de sistemas e informática), Universidad de Huánuco, Huánuco, Perú. Obtenido de http://repositorio.udh.edu.pe/bitstream/handle/123456789/809/T_047_43087253_T.pdf?sequence=1&isAllowed=y

## IX. Anexos

Anexo 1. Encuesta.

**Encuesta**

**ÁREA DE TI PARA LA EMPRESA BERENDSON NATACION S.R.L.**

**UNIVERSIDAD DE LAMBAYEQUE ENCUESTA**

**Objetivo:** Determinar el nivel de seguridad de información Basada en las normas ISO 27001 en la empresa "BERENDSON NATACIÓN S.R.L." para seleccionar la mejor estrategia a seguir.

**Proceso de confiabilidad:** se protege los datos personales de los encuestados

| DATOS DEMOGRÁFICOS |
|---|
| Cargo _____ Antigüedad en la empresa |
| Nivel de educación: Técnico ☐ Tecnólogo ☐ Profesional ☐ Otros ☐ |

Marque con una x en las casillas correspondiente la opción que considere pertinente

[E]excelente (5) [B] Bueno (4) [NT] No tiene Conocimiento (3) [MD] Muy deficiente (2) [R] regular (1)

| Datos de los Indicadores | | | | | | |
|---|---|---|---|---|---|---|
| **Categoría/Indicadores** | | **E (5)** | **B (4)** | **NT (3)** | **MD (2)** | **R (1)** |
| 1. Conocimiento en seguridad de la información | | | | | | |
| 1.1 | La empresa ha impartido la capacitación adecuada en cuento normas de seguridad de la información teniendo en cuenta lo siguiente | | | | | |
| 1.1.1 | Posee conocimientos con respecto a la seguridad de la información | | | | | |
| 1.1.2 | Tiene conocimientos sobre las normas que establece de seguridad de la información | | | | | |
| 1.2 | Conocimiento de la normatividad | | | | | |
| 1.2.1 | Tiene conocimiento sobre Norma ISO/27001 | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1.2.2 | Tiene conocimiento tiene sobre la ley de protección de datos | | | | | |
| 2. Técnicas para la protección de datos y seguridad de la información | | | | | | |
| 2.1 | Para la protección de la información se debe tener en cuenta lo siguiente | | | | | |
| 2.1.2 | El medio donde se alojan los backup de los servidores ¿En qué estado se encuentran? | | | | | |
| 2.2 | Acceso a el área de servidores o backup | | | | | |
| 2.2.1 | El sistema de control para el ingreso a esta área se define como: | | | | | |
| 2.2.2 | Como se define los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores | | | | | |
| 3. Aplicaciones de herramientas para la protección de datos y seguridad de la información | | | | | | |
| 3.1 | Herramientas para la protección de datos y seguridad de la información | | | | | |
| 3.1.1 | El antivirus instalado en los equipos de cómputo de la empresa se puede definir como: | | | | | |
| 3.1.2 | El nivel de protección brinda el antivirus instalado en los equipos de computo | | | | | |
| 3.1.3 | Como se define la restricción a paginas no permitidas en la empresa | | | | | |
| 3.2 | Estrategia para la protección de la información | | | | | |
| 3.2.1 | Como se define el password para ingreso al sistema | | | | | |
| 3.2.2 | El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema | | | | | |

Fuente: Molano (2017).

Anexo 2. Validación de encuestas.

Resultado de la validación de encuesta por: Mg. Nauca Torres Enrique Santos.

VALIDACIÓN DEL INSTRUMENTO

CUESTIONARIO ENCUESTA – COLABORADORES

MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001, PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN S.R.L

Responsables: Delgado Saavedra Martha Mellissa
Vásquez Zevallos José Luis

Indicación: Señor(a) especializado(a) le pido su colaboración para que luego de un riguroso análisis de los ítems del cuestionario de la encuesta, que le mostramos marque con un aspa en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional demostrando si cuenta o no cuenta con los requisitos mínimos de formulación para su posterior aplicación.

Nota: Para cada pregunta se considere un puntaje del 1 a 5:

| 1.Insatisfecho | 2.Mejorable | 3.Satisfecho | 4.Bueno | 5.Excelente |
|---|---|---|---|---|

| N° | ITEMS | PUNTAJE | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Conocimiento en seguridad de la información | | | | | | |
| La empresa ha impartido la capacitación adecuada en cuento normas de seguridad de la información teniendo en cuenta lo siguiente | | | | | | |
| 1 | Posee conocimiento con respecto a la seguridad de la información | | | | | X |
| 2 | Tiene conocimientos sobre las normas que establece de seguridad de la información | | | | | X |
| Conocimiento de la normatividad | | | | | | |
| 3 | Tiene conocimiento sobre Norma ISO/27001 | | | | | X |
| 4 | Tiene conocimiento sobre la ley de protección de datos | | | | | X |
| Técnicas para la protección de datos y seguridad de la información | | | | | | |
| Para la protección de la información se debe tener en cuenta lo siguiente | | | | | | |
| 7 | El medio donde se alojan los backup de los servidores ,en qué estado se encuentran | | | | | X |
| Acceso a el área de servidores o backup | | | | | | |
| 8 | Como define el sistemas de control para el ingreso a esta área. | | | | | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9 | Como define los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores. | | | | | X |
| Aplicaciones de herramientas para la protección de datos y seguridad de la información | | | | | | |
| Herramientas para la protección de datos y seguridad de la información | | | | | | |
| 10 | Como define el antivirus instalado en los equipos de cómputo de la empresa. | | | | | X |
| 11 | El nivel de protección brinda el antivirus instalado en los equipos de computo | | | | | X |
| 12 | Cómo se define la restricción a páginas no permitidas en la empresa | | | | | X |
| Estrategia para la protección de la información | | | | | | |
| 13 | Cómo se define el password para ingreso al sistemas | | | | | X |
| 14 | El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema | | | | | X |

Recomendaciones:

| | |
|---|---|
| Apellidos y nombres | NANCY TORRES ENRIQUE SANTOS |
| Título y/o grado académico | INGENIERO DE SISTEMAS Y COMPUTACIÓN MAGISTER EN DIRECCIÓN Y GESTIÓN DE EMPRESAS |

FIRMA

Resultado de la validación de encuesta por: Ing. Castillo Zumarán Segundo José.

VALIDACIÓN DEL INSTRUMENTO

CUESTIONARIO ENCUESTA – COLABORADORES

MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001, PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN S.R.L

Responsables: Delgado Saavedra Martha Mellissa
Vásquez Zevallos José Luis

Indicación: Señor(a) especializado(a) le pido su colaboración para que luego de un riguroso análisis de los ítems del cuestionario de la encuesta, que le mostramos marque con un aspa en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional demostrando si cuenta o no cuenta con los requisitos mínimos de formulación para su posterior aplicación.

Nota: Para cada pregunta se considere un puntaje del 1 a 5:

| 1.Insatisfecho | 2.Mejorable | 3.Satisfecho | 4.Bueno | 5.Excelente |
|---|---|---|---|---|

| N° | ITEMS | PUNTAJE | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Conocimiento en seguridad de la información | | | | | | |
| La empresa ha impartido la capacitación adecuada en cuento normas de seguridad de la información teniendo en cuenta lo siguiente | | | | | | |
| 1 | Posee conocimiento con respecto a la seguridad de la información | | | | X | |
| 2 | Tiene conocimientos sobre las normas que establece de seguridad de la información | | | | X | |
| Conocimiento de la normatividad | | | | | | |
| 3 | Tiene conocimiento sobre Norma ISO/27001 | | | | X | |
| 4 | Tiene conocimiento sobre la ley de protección de datos | | | | X | |
| Técnicas para la protección de datos y seguridad de la información | | | | | | |
| Para la protección de la información se debe tener en cuenta lo siguiente | | | | | | |
| 7 | El medio donde se alojan los backup de los servidores ,en qué estado se encuentran | | | | X | |
| Acceso a el área de servidores o backup | | | | | | |
| 8 | Como define el sistemas de control para el ingreso a esta área. | | | | X | |

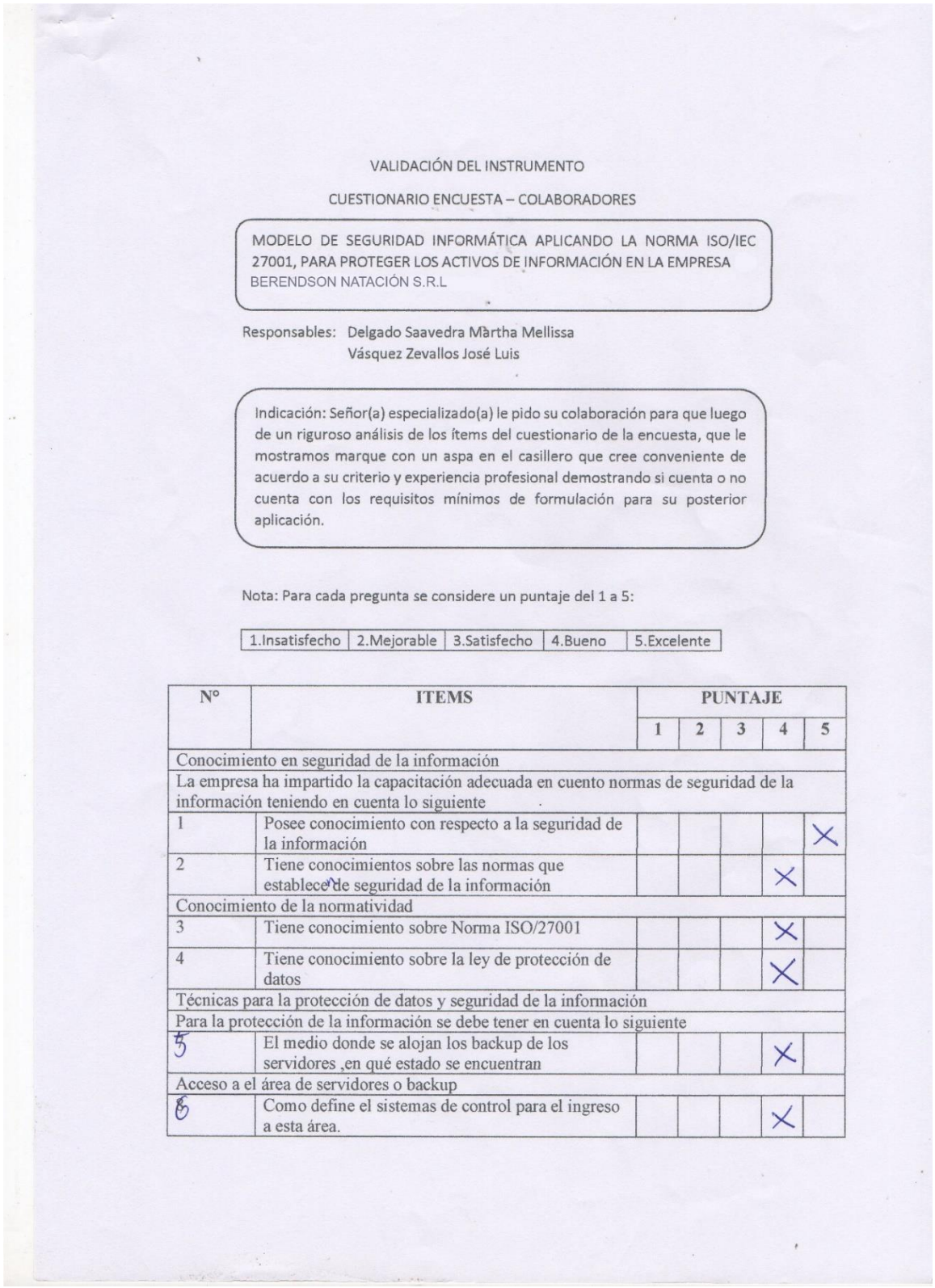
| | | | | | | |
|---|---|---|---|---|---|---|
| 9 | Como define los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores. | | | | X | |
| Aplicaciones de herramientas para la protección de datos y seguridad de la información | | | | | | |
| Herramientas para la protección de datos y seguridad de la información | | | | | | |
| 10 | Como define el antivirus instalado en los equipos de cómputo de la empresa. | | | | X | |
| 11 | El nivel de protección brinda el antiyirus instalado en los equipos de computo | | | | X | |
| 12 | Cómo se define la restricción a páginas no permitidas en la empresa | | | | X | |
| Estrategia para la protección de la información | | | | | | |
| 13 | Cómo se define el password para ingreso al sistemas | | | X | | |
| 14 | El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema | | | X | | |

Recomendaciones:

| | |
|---|---|
| Apellidos y nombres | Castillo Zumaran Segundo Jose |
| Título y/o grado académico | Ing. de Sistemas |

FIRMA

Resultado de la validación de encuesta por: Ing. Bances Santamaria María Violeta.



VALIDACIÓN DEL INSTRUMENTO

CUESTIONARIO ENCUESTA – COLABORADORES

MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001, PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN S.R.L

Responsables: Delgado Saavedra Màrtha Mellissa
Vásquez Zevallos José Luis

Indicación: Señor(a) especializado(a) le pido su colaboración para que luego de un riguroso análisis de los ítems del cuestionario de la encuesta, que le mostramos marque con un aspa en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional demostrando si cuenta o no cuenta con los requisitos mínimos de formulación para su posterior aplicación.

Nota: Para cada pregunta se considere un puntaje del 1 a 5:

| 1.Insatisfecho | 2.Mejorable | 3.Satisfecho | 4.Bueno | 5.Excelente |
|---|---|---|---|---|

| N° | ITEMS | PUNTAJE | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Conocimiento en seguridad de la información | | | | | | |
| La empresa ha impartido la capacitación adecuada en cuento normas de seguridad de la información teniendo en cuenta lo siguiente | | | | | | |
| 1 | Posee conocimiento con respecto a la seguridad de la información | | | | | X |
| 2 | Tiene conocimientos sobre las normas que establece de seguridad de la información | | | | X | |
| Conocimiento de la normatividad | | | | | | |
| 3 | Tiene conocimiento sobre Norma ISO/27001 | | | | X | |
| 4 | Tiene conocimiento sobre la ley de protección de datos | | | | X | |
| Técnicas para la protección de datos y seguridad de la información | | | | | | |
| Para la protección de la información se debe tener en cuenta lo siguiente | | | | | | |
| 5 | El medio donde se alojan los backup de los servidores ,en qué estado se encuentran | | | | X | |
| Acceso a el área de servidores o backup | | | | | | |
| 6 | Como define el sistemas de control para el ingreso a esta área. | | | | X | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9<br>8 - | Como define los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores. | | | | X | |
| Aplicaciones de herramientas para la protección de datos y seguridad de la información | | | | | | |
| Herramientas para la protección de datos y seguridad de la información | | | | | | |
| 09 | Como define el antivirus instalado en los equipos de cómputo de la empresa. | | | | X | |
| 10 | El nivel de protección brinda el antivirus instalado en los equipos de computo | | X | | | |
| 11 | Cómo se define la restricción a páginas no permitidas en la empresa | | | X | | |
| Estrategia para la protección de la información | | | | | | |
| 12 | Cómo se define el password para ingreso al sistemas | | X | | | |
| 13 | El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema | | X | | | |

Recomendaciones:

Se sugiere Mejorar las Preguntas 10, 12 y 13 de acuerdo a lo señalado durante la Validación del instrumento.

| | |
|---|---|
| Apellidos y nombres | Bances Santamaria Maria Violeta |
| Título y/o grado académico | Ingeniera de Sistemas |

FIRMA

Anexo 3. Formato de entrevista.

**ENTREVISTA**

**ÁREA DE TI PARA LA EMPRESA BERENDSON NATACION S.R.L.**

**UNIVERSIDAD DE LAMBAYEQUE ENTREVISTA**

**Objetivo:** Determinar el nivel de seguridad de la información Basada en las normas ISO 27001 en la empresa "BERENDSON NATACIÓN S.R.L." para seleccionar la mejor estrategia a seguir.

1. ¿Qué tan importantes cree Ud. que sean los mecanismos de seguridad en las aplicaciones informáticas que usa la empresa?
2. ¿Conoce de niveles y riesgos en el uso y funcionamiento de las aplicaciones con las que cuenta la empresa?
3. ¿Realizan sistemáticamente copias de seguridad o buckups como medida de protección y seguridad en los datos o la información que se maneja en la empresa?
4. ¿Cuál es el tipo de amenaza que se detecta con mayor frecuencia en su organización?
5. ¿Cómo maneja la empresa los desastres que afecten a los centros de datos o a las conexiones?
6. ¿Cómo asegura la seguridad del software? y ¿qué software permanece bajo su responsabilidad?
7. ¿Qué estrategias de seguridad conoce que se pueden tomar en cuenta para proteger y garantizar la seguridad en las aplicaciones y la información?

Anexo 4. Entrevista realizada al administrador de Berendson Natación S.R.L

**Anexo B**

**ENTREVISTA**

**ÁREA DE TI PARA LA EMPRESA BERENDSON NATACION S.R.L.**

**UNIVERSIDAD DE LAMBAYEQUE ENTREVISTA**

**Objetivo:** Determinar el nivel de seguridad de la información Basada en las normas ISO 27001 en la empresa "BERENDSON NATACION S.R.L." para seleccionar la mejor estrategia a seguir.

1. ¿Qué tan importantes cree Ud. que sean los mecanismos de seguridad en las aplicaciones informáticas que usa la empresa?
2. ¿Conoce de niveles y riesgos en el uso y funcionamiento de las aplicaciones con las que cuenta la empresa?
3. ¿Realizan sistemáticamente copias de seguridad o backups como medida de protección y seguridad en los datos o la información que se maneja en la empresa?
4. ¿Cuál es el tipo de amenaza que se detecta con mayor frecuencia en su organización?
5. ¿Cómo maneja la empresa los desastres que afecten a los centros de datos o a las conexiones?
6. ¿Cómo asegura la seguridad del software? y ¿qué software permanece bajo su responsabilidad?
7. ¿Qué estrategias de seguridad conoce que se pueden tomar en cuenta para proteger y garantizar la seguridad en las aplicaciones y la información?

Anexo 5. Entrevista realizada al personal del área de atención al cliente

**Anexo B**

**ENTREVISTA**

**ÁREA DE TI PARA LA EMPRESA BERENDSON NATACION S.R.L.**

**UNIVERSIDAD DE LAMBAYEQUE ENTREVISTA**

**Objetivo:** Determinar el nivel de seguridad de la información Basada en las normas ISO 27001 en la empresa "BERENDSON NATACION S.R.L." para seleccionar la mejor estrategia a seguir.

1. ¿Qué tan importantes cree Ud. que sean los mecanismos de seguridad en las aplicaciones informáticas que usa la empresa?
2. ¿Conoce de niveles y riesgos en el uso y funcionamiento de las aplicaciones con las que cuenta la empresa?
3. ¿Realizan sistemáticamente copias de seguridad o backups como medida de protección y seguridad en los datos o la información que se maneja en la empresa?
4. ¿Cuál es el tipo de amenaza que se detecta con mayor frecuencia en su organización?
5. ¿Cómo maneja la empresa los desastres que afecten a los centros de datos o a las conexiones?
6. ¿Cómo asegura la seguridad del software? y ¿qué software permanece bajo su responsabilidad?
7. ¿Qué estrategias de seguridad conoce que se pueden tomar en cuenta para proteger y garantizar la seguridad en las aplicaciones y la información?

Anexo 6. Entrevista realizada al personal del área de atención al cliente

**Anexo B**

**ENTREVISTA**

**ÁREA DE TI PARA LA EMPRESA BERENDSON NATACION S.R.L.**

**UNIVERSIDAD DE LAMBAYEQUE ENTREVISTA**

**Objetivo:** Determinar el nivel de seguridad de la información Basada en las normas ISO 27001 en la empresa "BERENDSON NATACIÓN S.R.L."" para seleccionar la mejor estrategia a seguir.

1. ¿Qué tan importantes cree Ud. que sean los mecanismos de seguridad en las aplicaciones informáticas que usa la empresa?
2. ¿Conoce de niveles y riesgos én el uso y funcionamiento de las aplicaciones con las que cuenta la empresa?
3. ¿Realizan sistemáticamente copias de seguridad o buckups como medida de protección y seguridad en los datos o la información que se maneja en la empresa?
4. ¿Cuál es el tipo de amenaza que se detecta con mayor frecuencia en su organización?
5. ¿Cómo maneja la empresa los desastres que afecten a los centros de datos o a las conexiones?
6. ¿Cómo asegura la seguridad del software? y ¿qué software permanece bajo su responsabilidad?
7. ¿Qué estrategias de seguridad conoce que se pueden tomar en cuenta para proteger y garantizar la seguridad en las aplicaciones y la información?

Anexo 7. Entrevista realizada al personal del área de atención al cliente

**Anexo B**

**ENTREVISTA**

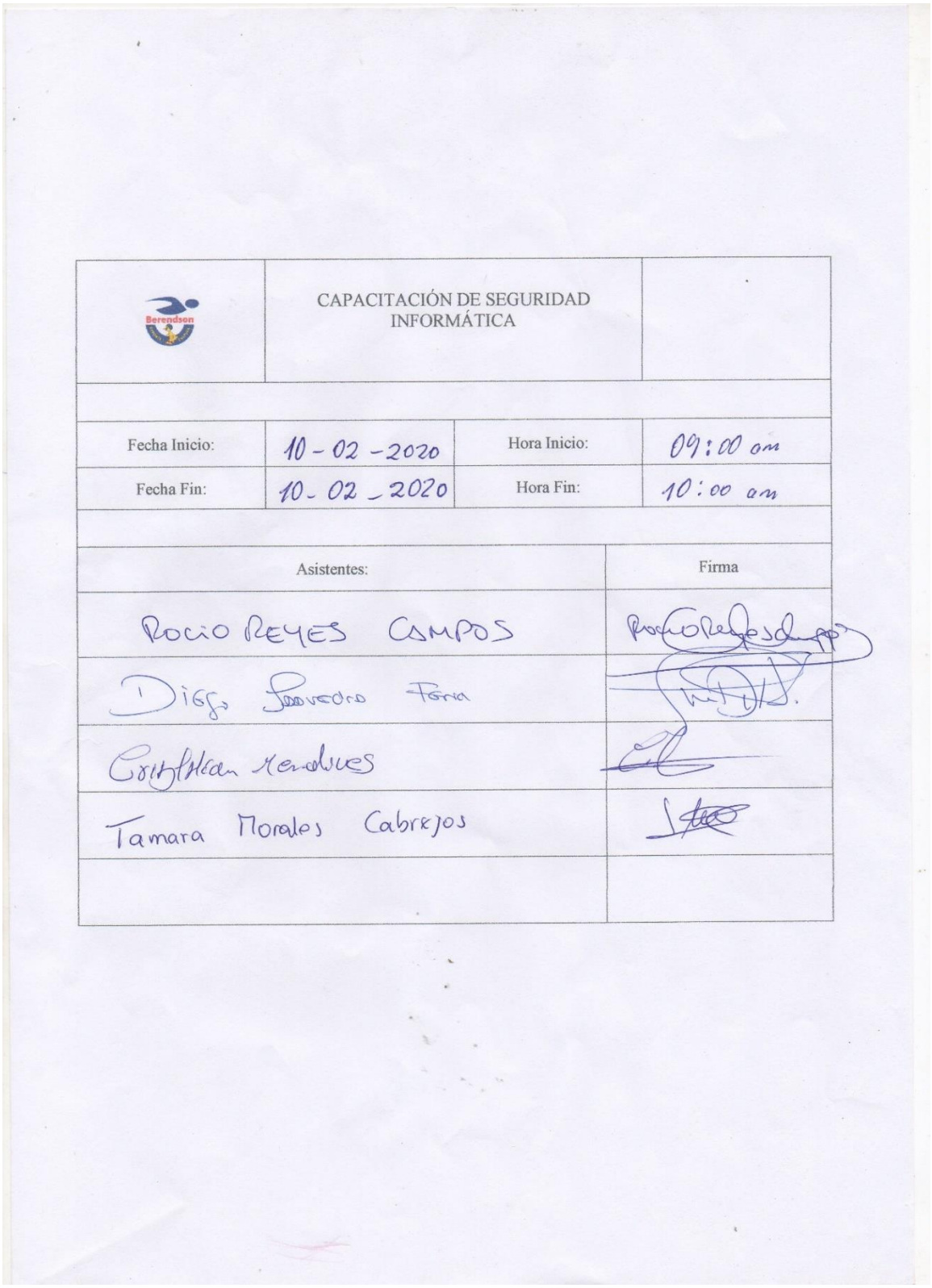
**ÁREA DE TI PARA LA EMPRESA BERENDSON NATACION S.R.L.**

**UNIVERSIDAD DE LAMBAYEQUE ENTREVISTA**

**Objetivo:** Determinar el nivel de seguridad de la información Basada en las normas ISO 27001 en la empresa "BERENDSON NATACIÓN S.R.L."" para seleccionar la mejor estrategia a seguir.

1. ¿Qué tan importantes cree Ud. que sean los mecanismos de seguridad en las aplicaciones informáticas que usa la empresa?
2. ¿Conoce de niveles y riesgos en el uso y funcionamiento de las aplicaciones con las que cuenta la empresa?
3. ¿Realizan sistemáticamente copias de seguridad o buckups como medida de protección y seguridad en los datos o la información que se maneja en la empresa?
4. ¿Cuál es el tipo de amenaza que se detecta con mayor frecuencia en su organización?
5. ¿Cómo maneja la empresa los desastres que afecten a los centros de datos o a las conexiones?
6. ¿Cómo asegura la seguridad del software? y ¿qué software permanece bajo su responsabilidad?
7. ¿Qué estrategias de seguridad conoce que se pueden tomar en cuenta para proteger y garantizar la seguridad en las aplicaciones y la información?

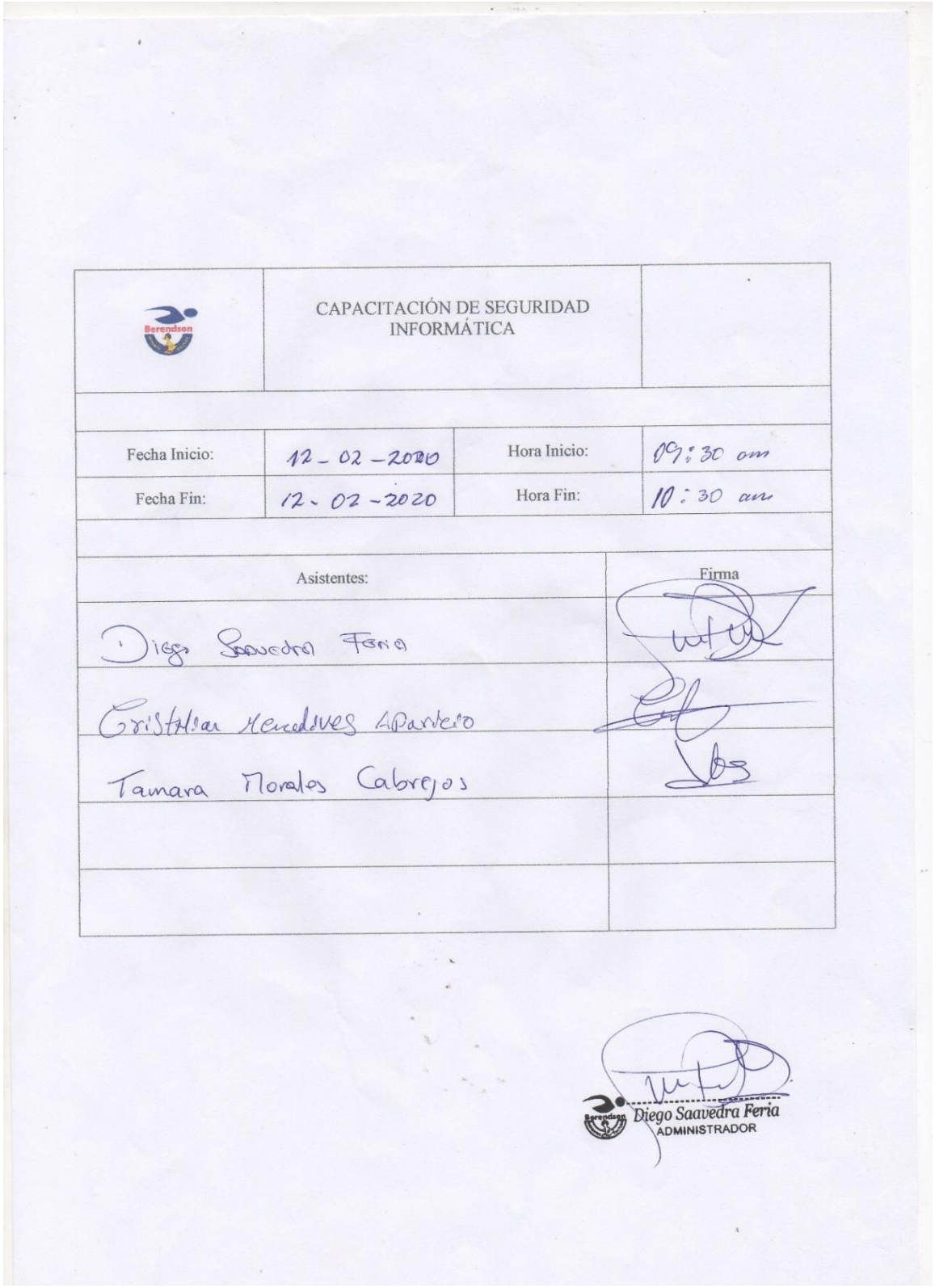
Anexo 8. Firmas de los asistentes de la primera capacitación sobre seguridad informática.



| | CAPACITACIÓN DE SEGURIDAD INFORMÁTICA | | |
|---|---|---|---|
| Fecha Inicio: | 10-02-2020 | Hora Inicio: | 09:00 am |
| Fecha Fin: | 10-02-2020 | Hora Fin: | 10:00 am |

| Asistentes: | Firma |
|---|---|
| ROCIO REYES CAMPOS | |
| Diego Saavedra Feria | |
| Cristhian Mendoles | |
| Tamara Morales Cabrejos | |
| | |

Anexo 9. Firmas de los asistentes de la segunda capacitación sobre seguridad informática.



| | CAPACITACIÓN DE SEGURIDAD INFORMÁTICA | | |
|---|---|---|---|
| Fecha Inicio: | 12-02-2020 | Hora Inicio: | 09:30 am |
| Fecha Fin: | 12-02-2020 | Hora Fin: | 10:30 am |

| Asistentes: | Firma |
|---|---|
| Diego Saavedra Feria | |
| Cristhian Mendoves Aparicio | |
| Tamara Morales Cabrejos | |
| | |
| | |

Diego Saavedra Feria
ADMINISTRADOR

*Figura 42*: Realización de encuesta y entrevista.
Fuente: Fotos obtenidos en la encuesta aplicada a las áreas de la empresa.

*Figura 43:* Realización de encuesta y entrevista.
Fuente: Fotos obtenidos en la encuesta aplicada a las áreas de la empresa.

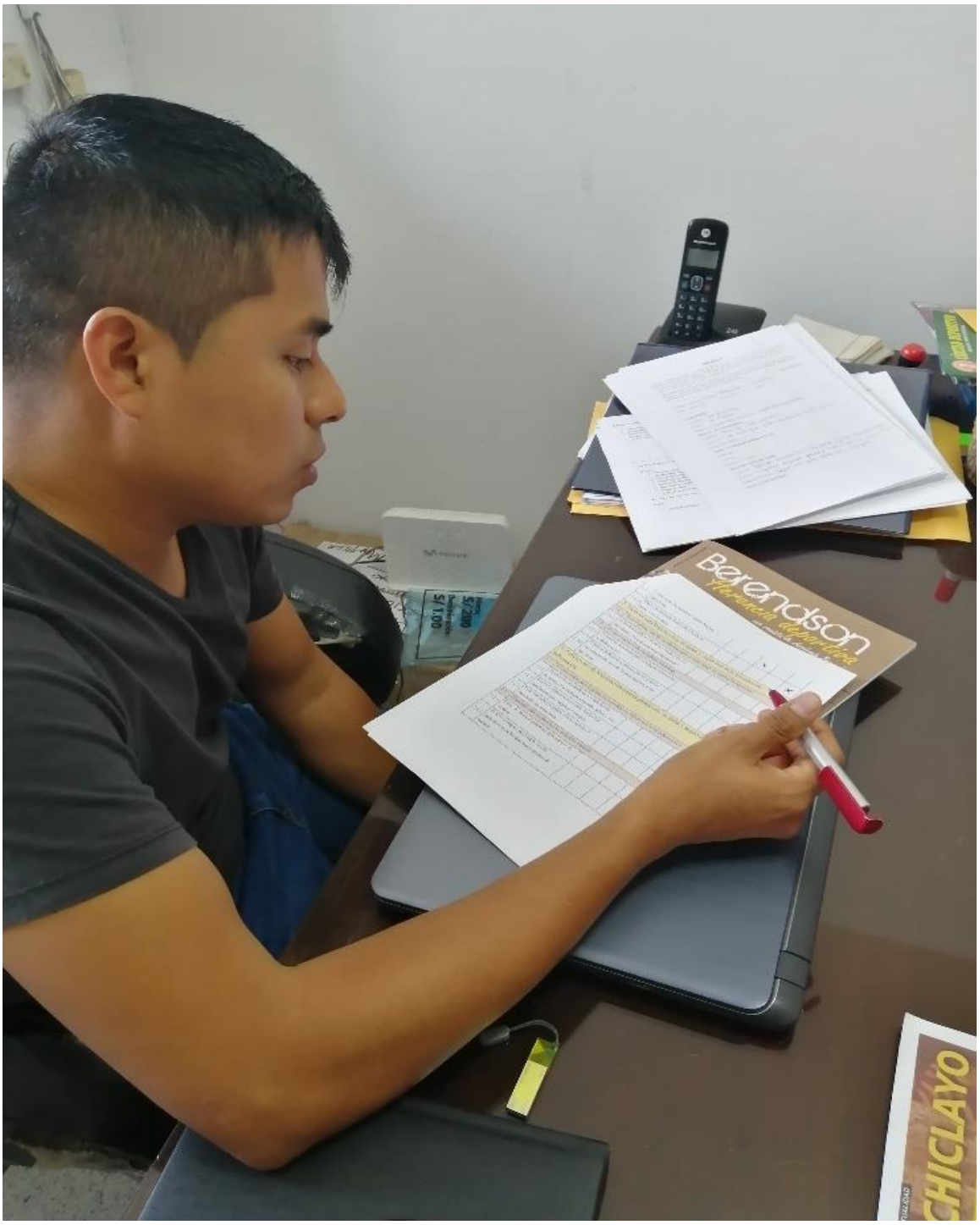



*Figura 44:* Realización de encuesta y entrevista.
Fuente: Fotos obtenidos en la encuesta aplicada a las áreas de la empresa.

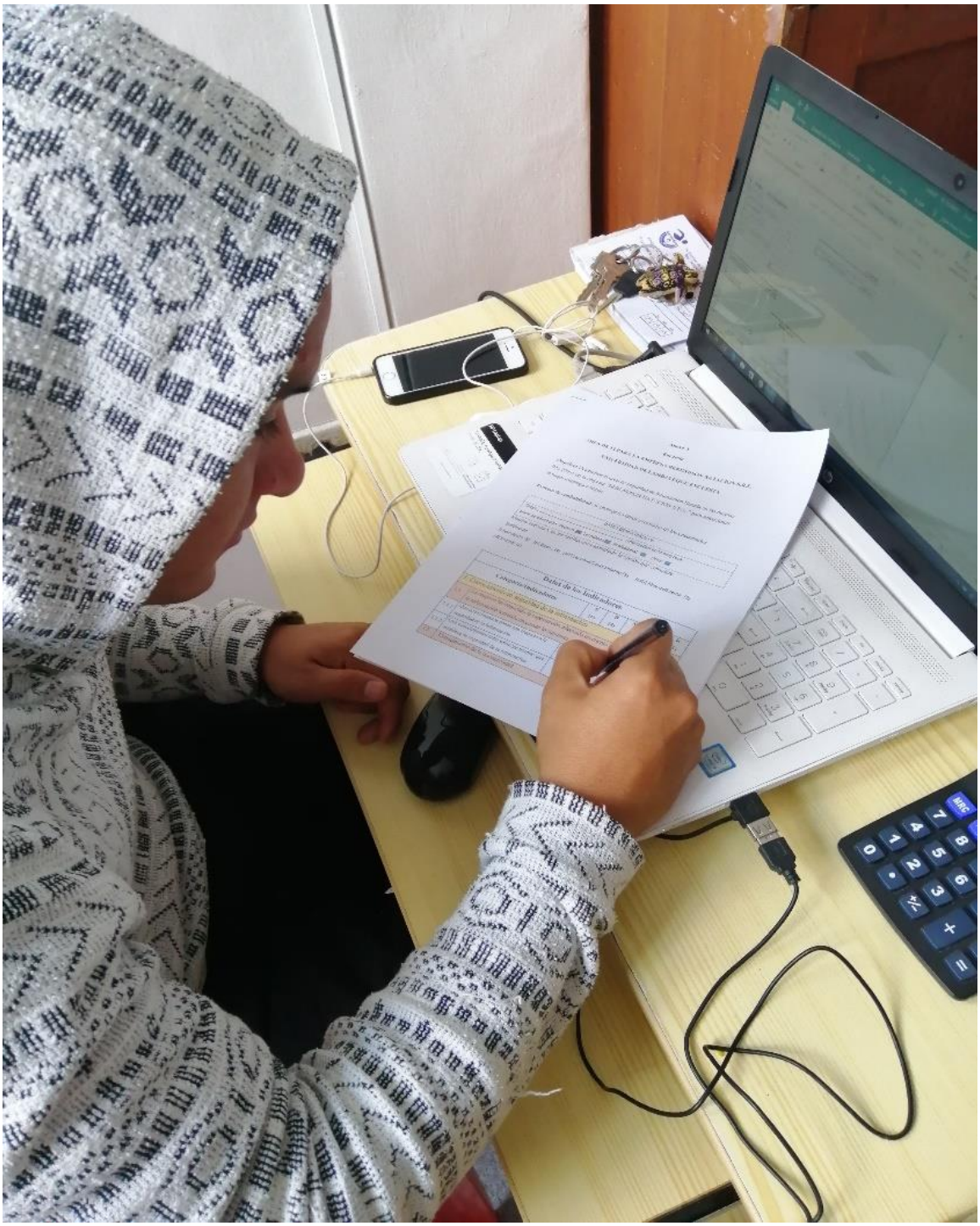


*Figura 45:* Realización de encuesta y entrevista

Fuente: Fotos obtenidos en la encuesta aplicada a las áreas de la empresa


*Figura 46:* Capacitación a Berendson Natación S.R.L.
Fuente: Fotos obtenidos en la encuesta aplicada a las áreas de la empresa

*Figura 47:* Capacitación al encargado del área de administración
Fuente: Fotos obtenidos en la encuesta aplicada a las áreas de la empresa

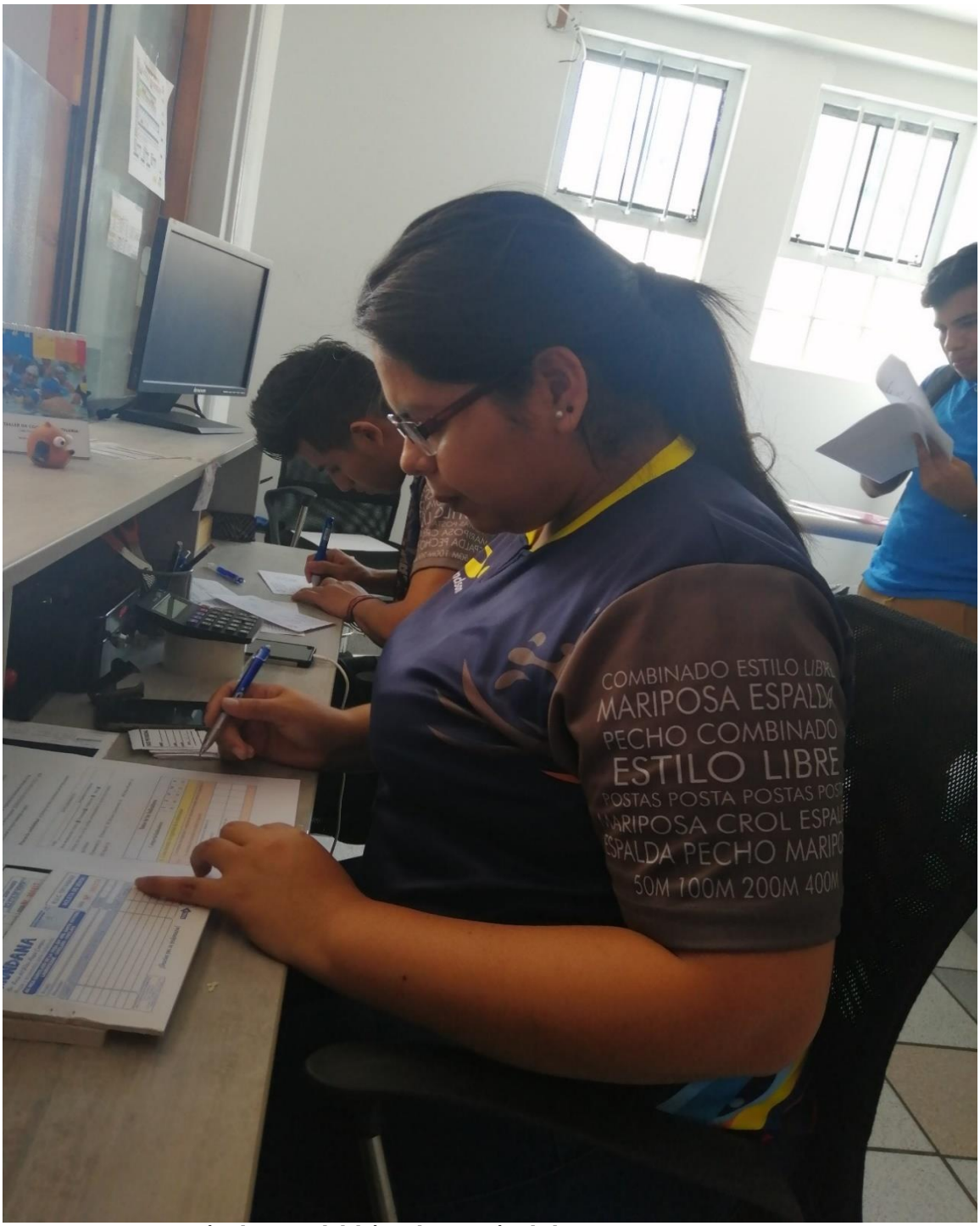



*Figura 48:* Capacitación al personal del área de atención al cliente, 1.
Fuente: Fotos obtenidos en la encuesta aplicada a las áreas de la empresa.

*Figura 49:* Capacitación al personal del área de atención al cliente, 2.
Fuente: Fotos obtenidos en la encuesta aplicada a las áreas de la empresa.


*Figura 50:* Capacitación al personal del área de atención al cliente, 3
Fuente: Fotos obtenidos en la encuesta aplicada a las áreas de la empresa.

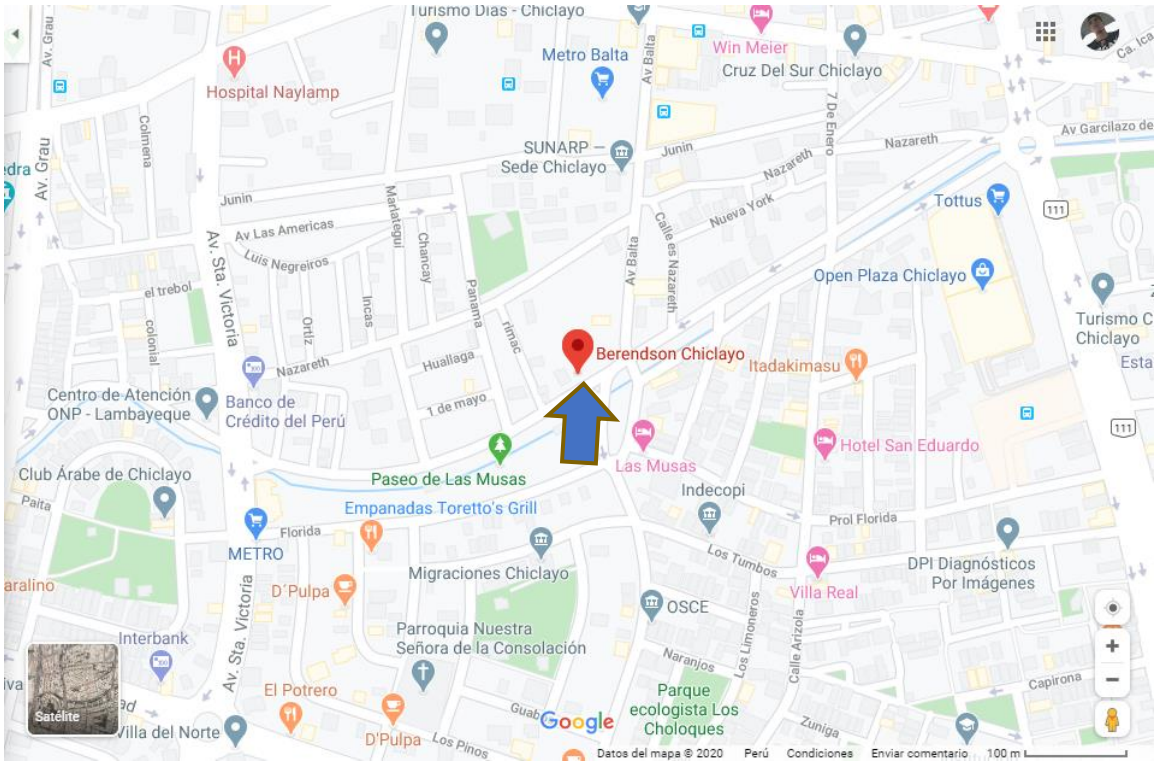



*Figura 52:* Ubicación de Berendson Natación S.R.L.
Fuente: Google Earth.

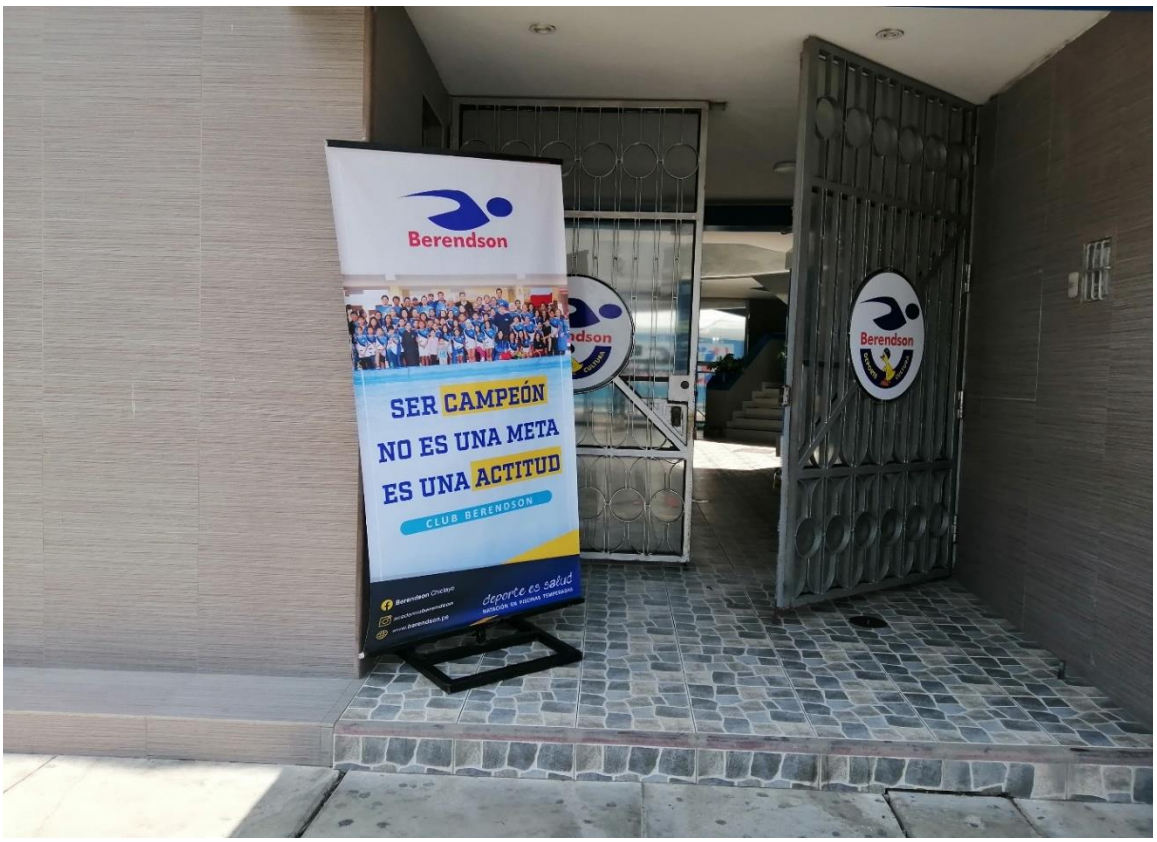



*Figura 51:* Entrada a Berendson Natación S.R.L.
Fuente: Elaboración propia.