



UNIVERSIDAD DE LAMBAYEQUE

FACULTAD DE CIENCIAS DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TRABAJO DE INVESTIGACIÓN

**DIAGNÓSTICO DE LA SEGURIDAD INFORMÁTICA DE LOS
ACTIVOS DE LA EMPRESA BERENDSON NATACION S.R.L.**

AUTORES

**Delgado Saavedra Martha Mellissa
Vásquez Zevallos José Luis**

**PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR EL GRADO DE
BACHILLER EN INGENIERÍA DE SISTEMAS**

**Chiclayo-Perú
2019**

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 DELGADO SAAVEDRA

Este trabajo de investigación está dedicado 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.

Finalmente, a mis sobrinos que son un motivo para seguir adelante.

JOSE LUIS VÁSQUEZ ZEVALLOS

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 DELGADO SAAVEDR

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.

También quiero agradecer a la Universidad de Lambayeque y a todas las autoridades, por permitirme concluir con una etapa de mi vida.

JOSE LUIS VÁSQUEZ ZEVALLOS

Resumen

El presente trabajo de investigación muestra el desarrollo de un diagnóstico de la seguridad informática de los activos de la empresa Berendson Natación S.R.L., para proteger de la pérdida o deterioro de información, corregir las vulnerabilidades con el fin principal de proponer la elaboración de un modelo de seguridad informática aplicando la norma ISO/IEC 27001 para proteger los activos de información.

La empresa Berendson Natación S.R.L. carece de seguridad informática en sus principales áreas de atención al cliente y administración por lo que se planteó diagnosticar la seguridad informática de los activos de la empresa y así obtener qué nivel de conocimiento que tienen los trabajadores sobre la identificación de los activos y de los riesgos informáticos que existen en la empresa.

Para la obtención de dicha información y recolección de datos se consideró conveniente el uso de las técnicas de recolección de datos tales como las encuestas y entrevistas, como medio para poder extraer la información y su posterior interpretación.

En este trabajo también se propone capacitar a los trabajadores de la empresa sobre las amenazas y riesgos a los que está expuesto los activos de información y crear el área de sistemas e informática para que así monitoree el cumplimiento de las políticas y realice las capacitaciones necesarias.

Como resultado se obtuvo que solo el 33% de los trabajadores de la empresa Berendson Natación S.R.L. conoce algunos riesgos informáticos e identifica los activos existentes.

Palabras claves:

Diagnóstico, Información, Norma ISO 27001, Seguridad, Riesgos, Activo

Indice

Dedicatoria	II
Agradecimiento	III
Resumen.....	IV
I. Problema de investigación	1
II. Marco teórico	2
2.1 Antecedentes bibliográficos	2
2.1.1 Antecedentes internacionales	2
2.1.2 Antecedentes nacionales	3
2.2 Materiales y Métodos.....	4
2.2.1 Variables y operacionalización	4
2.2.1.1 Variable única	4
2.2.1.2 Operacionalización de variables	4
2.2.2 Tipo de estudio y diseño de investigación	6
2.2.2.1 Tipo de estudio.....	6
2.2.3 Población y muestra de estudio.....	6
2.2.3.1 Población.....	6
2.2.3.2 Muestra	6
2.2.3.3 Método, técnicas e instrumentos de recolección de datos	8
2.2.3.4 Procesamiento de datos y análisis estadístico	9
III Resultados	9
IV. Conclusiones.....	24
V. Recomendaciones	24
VI. Referencias bibliográficas.....	25
VII. Anexos.....	27

Índice de tablas

Tabla 1 Operacionalización de variables -----	5
Tabla 2 Clasificación de activos en las áreas -----	6
Tabla 3 Características de activos de las áreas -----	7
Tabla 4 Estado en que se encuentran los backups -----	10
Tabla 5 Ingreso al sistema de control -----	11
Tabla 6 Nivel de seguridad de los servidores -----	12
Tabla 7 Definición de antivirus-----	13
Tabla 8 Nivel de seguridad que brinda el antivirus-----	14
Tabla 9 Nivel de conocimiento sobre seguridad de la información-----	16
Tabla 10 Nivel de conocimiento sobre la Norma que establece a la información-----	17
Tabla 11 Nivel de conocimiento sobre la norma ISO/IEC 27001-----	18
Tabla 12 Nivel de conocimiento sobre la Ley de Protección de dato-----	19
Tabla 13 Definición de la restricción de páginas no permitida en la empresa-----	20
Tabla 14 Definición del nivel de password para el ingreso al sistema-----	21
Tabla 15 Nivel de seguridad para el ingreso al sistema-----	22
Tabla 16 Matriz de consistencia-----	35

Índice de figuras

Figura 1 Estado en que se encuentran los backups	10
Figura 2 ¿Cómo se define el ingreso al sistema de control?.....	11
Figura 3 Nivel de seguridad que tienen los servidores	12
Figura 4 Calificación del antivirus.....	13
Figura 5 Nivel de protección del antivirus.....	14
Figura 6 Porcentaje del nivel de conocimiento con respecto a la seguridad de la información	16
Figura 7 Nivel de conocimiento sobre la norma de seguridad de información	17
Figura 8 Nivel de conocimiento de la Norma ISO/IEC 27001	18
Figura 9 Nivel de conocimiento sobre la Ley de Protección de Datos.....	19
Figura 10 Nivel de restricción de páginas	20
Figura 11 Calificación sobre el Nivel de Password para el ingreso a los sistemas.....	21
Figura 12 El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.....	22
Figura 13 Desarrollo de encuesta a cargo del responsable del área de administración	28
Figura 14 Desarrollo de encuesta a cargo del responsable del área de atención al cliente.....	28
Figura 15 Explicación de la encuesta por parte de los autores	28
Figura 16 Explicación de la encuesta por parte de los autores	28
Figura 17 Desarrollo de encuesta a cargo del responsable del área de atención al cliente.....	28
Figura 18 Validación de encuestas N° 1	28
Figura 19 Validación de encuestas N° 1	28
Figura 20 Validación de encuestas N° 2.....	28
Figura 21 Validación de encuestas N° 2.....	28

I. Problema de investigación

En la actualidad es fundamental que todas las compañías u organizaciones sin importar el rubro al que se dedican cuenten con medidas de seguridad ya que en los últimos años los ciberdelincuentes dedicándose a alterar de manera ilegal a los sistemas para así sustraer, editar, eliminar todos los datos confidenciales o también pueden usar imágenes, cuentas correos electrónicos y redes sociales falsos de las empresas para crear contenido perjudicial.

Por ello las empresas tienen que adaptarse a los avances tecnológicos y mantenerse actualizado, algunas de ellas han tenido que recurrir a ofrecer sus servicios o productos de manera virtual esto obliga que los factores de seguridad, estabilidad y confiabilidad de las plataformas sea un elemento clave a considerar en el desarrollo de las aplicaciones y, por lo tanto, la utilización de herramientas dedicadas a la prevención y detección de fallas de seguridad.

La prevención de los riesgos informáticos en nuestros equipos debe ser uno de los principales objetivos que toda empresa debe plantearse ya que de las medidas de seguridad que se impongan depende la sobrevivencia de ella.

Según Universidad Internacional de Valencia (2018) nos indica que la seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.

El objetivo general de la presente investigación es diagnosticar la seguridad informática de los activos de la empresa Berendson Natación S.R.L teniendo como objetivos específicos: Identificar los activos que existen en la empresa, conocer los riesgos informáticos en la empresa Berendson Natación S.R.L.

El presente trabajo de investigación se determinó la falta de seguridad en la información la cual nos permite realizar un diagnóstico de la seguridad informática de los activos de la empresa Berendson Natación S.R.L. y así tener conocimiento de qué manera se eliminan o disminuyen las amenazas y riesgos que afectan a la empresa; asimismo la hipótesis consistió: si se tiene un diagnóstico adecuada de la seguridad informática, entonces es posible identificar los riesgos de los activos informáticos de la empresa Natación S.R.L.

II. Marco teórico

2.1 Antecedentes bibliográficos

2.1.1 Antecedentes internacionales

Según Bermúdez, K.; Bailón, E. (2015) Esta investigación se elaboró un análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001-sistema de gestión de seguridad de la información dirigido a una empresa en servicios financieros en la ciudad de Guayaquil en el año 2015. Como objetivo principal el estudio de seguridad en los procesos críticos. A través de reuniones, revisión de documentación, consultas, observación, encuestas y ejecución de entrevistas con directivos que poseen un amplio conocimiento del negocio, se logró identificar los riesgos actuales a los que se exponen los datos tanto físicos, lógicos y sistemas de procesamiento de información. Los resultados obtenidos dan a conocer que, para minimizar los riesgos existentes, es necesario implementar controles de seguridad, lo cual ayuda a fortalecer tres aspectos importantes: la confidencialidad, integridad y disponibilidad de la información. Pero los resultados también muestran la importancia del compromiso y trabajo en equipo que debe tener la empresa.

Según Chavez, J.(2016) en su trabajo desarrollado análisis y modelos de datos de redes para seguridad informática en la ciudad de Santiago de Chile en el año 2016 comprende el diseño e implementación de un ambiente de simulación basado en herramientas de código libre para el estudio de una red simplificada de Internet en cuanto a servicios, aplicaciones, flujos y vulnerabilidades de seguridad. Utilizando estas herramientas se estudia el comportamiento de la red durante condiciones de tráfico web normal y durante ataques informáticos definidos, con el objetivo de generar modelos de predicción y detección que permitan detectar la ocurrencia de un ataque informático mientras este está en curso o en el corto plazo, desde su comienzo. Los objetivos específicos que se planteó son los siguientes: Diseñar e implementar una arquitectura de red simplificada y representativa de Internet utilizando GNS3 como software base, Implementar generadores de tráfico web utilizando herramientas de software y un modelo simple propuesto para el comportamiento de los usuarios, Investigar sobre ataques informáticos para ejecutarlos durante las simulaciones, Recolectar datos sobre los flujos de información a través es de los routers para ser analizados posteriormente, Evaluar cualitativamente la factibilidad de usar estas metodologías como alternativa complementaria a los mecanismos tradicionales para la prevención y detección de ataques a un servicio o aplicación web, actuando siempre desde el punto de vista del proveedor

de servicios de Internet. Como conclusión a los objetivos propuestos se puede decir: En primer lugar, se comprueba la factibilidad de montar un ambiente de simulación representativo de una arquitectura de proveedor de servicios de Internet para realizar estudios e investigaciones relacionadas con redes de comunicaciones y seguridad informática, utilizando hardware disponible en un computador personal y software de código libre. Esto permite entregar todo lo necesario para su configuración en cualquiera de los tres grandes sistemas operativos (Windows, Linux y OSX), incluyendo las máquinas virtuales de la arquitectura y un breve manual para su uso en estudios posteriores.

2.1.2 Antecedentes nacionales

Según Calderon, J.(2017) dicha tesis que realizó con nombre aplicación de la herramienta de gestión de riesgos para la seguridad informática del honadomani san Bartolomé en la ciudad de Lima en el año 2019. La presente tesis se realizará en el Hospital Nacional Madre Niño San Bartolomé, con la finalidad de aplicar una herramienta de gestión de riesgos para la seguridad informática. El objetivo principal de esta tesis es determinar la influencia de la aplicación de una herramienta de gestión de riesgos para la seguridad informática del honadomani San Bartolomé. El tipo de investigación es aplicada-no experimental y el diseño de investigación es longitudinal de tendencia. La metodología de desarrollo para la aplicación de la herramienta de gestión de riesgos es Magerit, y como herramienta de trabajo para Magerit se utilizará la matriz de riesgos de Magerit y la ISO/IEC 27001:2013 para la auditoria. Se llego a las siguientes conclusiones En el nivel de cumplimiento de la seguridad lógica para la seguridad informática en el honadomani San Bartolomé, en la medición del PreTest, alcanzó los 42.50% de porcentaje y con la aplicación de la herramienta de gestión de riesgos alcanzo un 74.17%,) En el nivel de cumplimiento de la seguridad Física para la seguridad informática en el honadomani San Bartolomé, en la medición del PreTest, alcanzó los 71.25% de porcentaje y con la aplicación de la herramienta de gestión de riesgos alcanzo un 84.50%.

Según Palomares, M.(2016) dicha tesis se elaboró sistema de seguridad informática para los riesgos en la red de datos de la empresa grupo palomares SAC en la ciudad de Lima en el año 2016. La investigación realizada fue de tipo aplicada, con un diseño experimental de tipo pre experimental. La población estuvo formada por 30 estaciones de trabajo y el muestreo fue no probabilístico, intencional. Se usó como técnica recopilación de datos la observación que hizo uso como instrumento una ficha de observación. El instrumento de recolección de datos fue validado por medio del juicio de expertos con un resultado de opinión de aplicabilidad y la confiabilidad se realizó

mediante la prueba de t student. Los resultados de esta investigación confirman que la implementación del sistema de seguridad informática tuvo un efecto significativo para los riesgos en la red de datos de la empresa; en cuanto al nivel de amenazas detectadas se logró una reducción de 8% y en el nivel de gravedad de impacto se redujo a 4%

Según Chura, E.(2018) dicha tesis se desarrolló un Plan de Seguridad Informática en la Municipalidad Provincial de San Román (Sistema Web) en la ciudad de Juliaca en el año 2018 Para lograr dicho propósito se formuló un objetivo general y dos objetivos específicos para dar a conocer el plan de seguridad informática, y conseguir confidencialidad, integridad y disponibilidad de los datos. Así mismo se realizó el estudio con una población siendo el universo, que es un conjunto de personas y una muestra que se determina a través del método provístico siendo elegido un total de población de forma sistémica. La conclusión del presente trabajo de investigación refiere de acuerdo a los resultados que se han obtenido es con respecto a la percepción de la dimensión de paradigmas con un total de deficiencia de un 99%.

2.2 Materiales y Métodos

2.2.1 Variables y operacionalización

2.2.1.1 Variable única

El diagnóstico de seguridad informática en la empresa Berendson Natación S.R.L

2.2.1.2 Operacionalización de variables

Tabla 1*Operacionalización de variables*

I	VARIABLE	DIMENSIÓN	INDICADORES	TECNICAS	INSTRUMENTO
I	El	SEGURIDAD	Preguntar si el diagnostico de		Cuestionario/ Guía de
N	diagnostico		seguridad informática disminuye los	Encuestas	entrevista
D	de seguridad		riesgos a los que la empresa	Entrevista	
E	informática		Berendson Natación S.R.L se		
P	en la empresa		encuentra expuesta.		
E	Berendson	RIESGO	Evaluar el nivel de riesgo de pérdida		
N	Natación		y robo de información en la empresa		
D	S.R.L		Berendson Natación S.R. L		
I					
E					
N					
T					
E					

Fuente: Elaboración propia

2.2 .2Tipo de estudio y diseño de investigación

2.2.2.1 Tipo de estudio

Según Vásquez, I. (2005) nos dice que un estudio descriptivo sirve para analizar cómo es y cómo se manifiesta un fenómeno y sus componentes. Permiten detallar el fenómeno estudiado básicamente a través de la medición de uno o más de sus atributos.

El tipo de estudio del presente proyecto es una investigación descriptiva que implica la realización de un diagnóstico de seguridad informática en la empresa Berendson Natación S.R.L por parte de los investigadores, orientado a resolver la falta de seguridad en la información siendo este uno de los activos más importantes.

2.2.3 Población y muestra de estudio

2.2.3.1 Población

Según (Toledo, Neftali., 2019) nos informa que la población de una investigación está compuesta por todos los elementos (personas, objetos, organismos, historias clínicas) que participan del fenómeno que fue definido y delimitado en el análisis del problema de investigación.

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

2.2.3.2 Muestra

Según (Toledo, Neftali., 2019) nos indica que una muestra es una parte de la población. La muestra puede ser definida como un subgrupo de la población o universo. Para seleccionar la muestra, primero deben delimitarse las características de la población. La muestra consistió en la misma población.

Tabla 2

Clasificación de activos en las áreas

Área	N^a Computadoras
Administración	01
Atención al cliente	01
Gerencia	01
TOTAL	03

Fuente: Elaboración propia

Tabla 3*Características de activos de las áreas*

ÁREA	ACTIVOS	
Gerencia	Software	- Windows 10 Pro. - Office 2016. - ESET NOD32 (Antivirus).
	Hardware	
	Información	- Documentos almacenados en papel. - Documentos digitales.
	Personal	-01 persona
Administración	Software	- Windows 10 Pro. - Office 2016. - ESET NOD32 (Antivirus).
	Hardware	- ASUSTek – Intel(R) Pentium Silver N500 CPU@ 1.10 GHZ, RAM 4 GB - 64 Bits (Laptop). - XIAOMI REDMI 6A Mediatek Helio A22 quad -core 12 nm 2 GHz – 2 GB RAM – Android 8.1 Oreo + MIUI 9 (Smartphone). - Miltrastar DSL-240HNA-T1CC (Router). - DataTraveler 100 G3–32 GB (USB).
	Información	- Documentos almacenados en papel. - Documentos digitales.
	Personal	- 01 persona
Atención al cliente	Software	- Windows 10 Pro. - Office 2016. - ESET NOD32 (Antivirus).

Hardware	- HP – Intel(R) Core i3-7020U CPU @ 2.30 GHz, RAM 4 GB – 64 Bits. - Brother DCP-7310 (Impresora). - SanDisk cruzer force 16 GB.
Información	- Documentos almacenados en papel. - Documentos digitales.
Personal	- 2 personas.

Fuente: Elaboración propia

2.2.3.3 Método, técnicas e instrumentos de recolección de datos

Las técnicas de recolección de datos que se utilizaran para el desarrollo el presente proyecto son:

Encuesta: Según EncuestaTick., (2019) nos informa que es un estudio en el cual el investigador obtiene los datos a partir de realizar un conjunto de preguntas normalizadas dirigidas a una muestra representativa o al conjunto total de la población estadística en estudio, formada a menudo por personas, empresas o entes institucionales, con el fin de conocer estados de opinión, características o hechos específicos. Se encuestó al personal que labora en las áreas de atención al cliente y administración, permitió la identificación de activos y riesgos informáticos que existen en la empresa Berendson Natación S.R.L., donde se determinó que el personal tiene un conocimiento limitado sobre dichos temas.

Entrevista: Según Significados. (2019) nos indica que es conversación o conferencia que sostienen dos o más personas que se encuentran en el rol de entrevistador y entrevistado con la finalidad de obtener el primero determinada información sobre un asunto o tema que pueda proporcionarle el segundo. Se entrevistó al Gerente de la empresa Berendson Natación S.R.L., la cual nos respondió un total de siete preguntas enfocadas a los objetivos de identificar los activos y riesgos informáticos que existen en la empresa para así obtener datos necesarios para el diagnóstico de seguridad informática en la empresa.

Cuestionario: Deconceptos.com., (2019) nos informa que son una serie de preguntas ordenadas, que buscan obtener información de parte de quien las responde, para servir a quien pregunta o a ambas partes.

2.2.3.4 Procesamiento de datos y análisis estadístico

El trabajo de investigación informara de que manera el Diagnostico de seguridad informática en la empresa Berendson Natación S.R.L. disminuye los riesgos.

Para el reciente estudio se utilizará las técnicas de encuesta, 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.

III Resultados

3.1 Identificar los activos que existen en la empresa definición

Con la identificación de activos en la empresa Berendson Natación S.R.L. Permitió clasificar a que activos se les brinda mayor protección y a cuales no, también nos permite identificar sus características y roles dentro de la empresa.

3.1.1 Encuesta

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

Tabla 4

Estado en que se encuentran los backups

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	1	33%
No tiene conocimiento	1	33%
Muy deficiente	1	33%
Regular	0	0%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

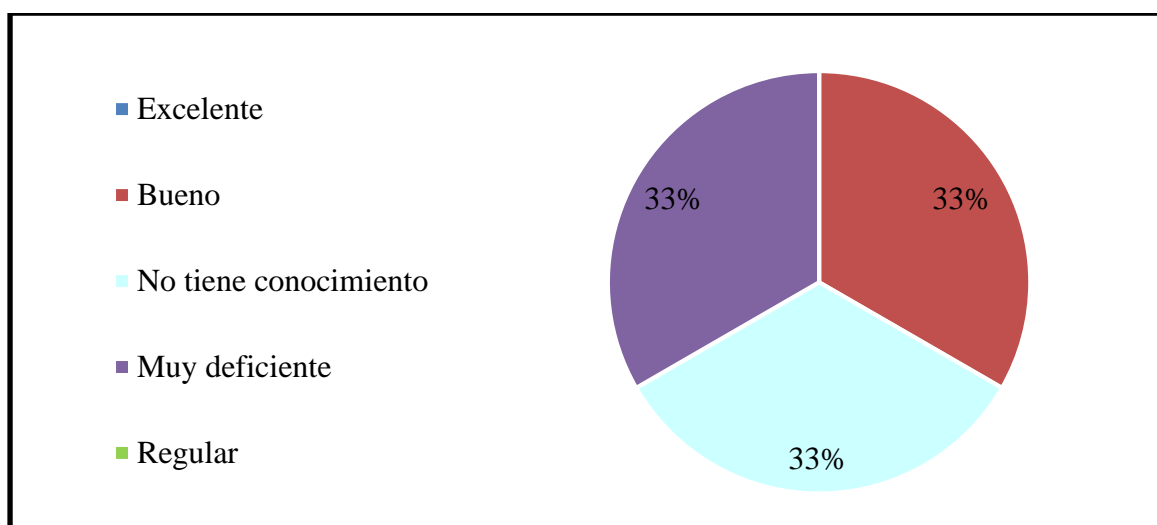


Figura 1 Estado en que se encuentran los backups

Análisis: En relación a la tabla y figura se observa que el 33% de los encuestados considera como bueno, muy deficiente y no tiene conocimiento sobre el nivel de conocimiento del estado de los backup

Tabla 5

Ingreso al sistema de control

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	1	33%
No tiene conocimiento	1	33%
Muy deficiente	1	33%
Regular	0	0%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

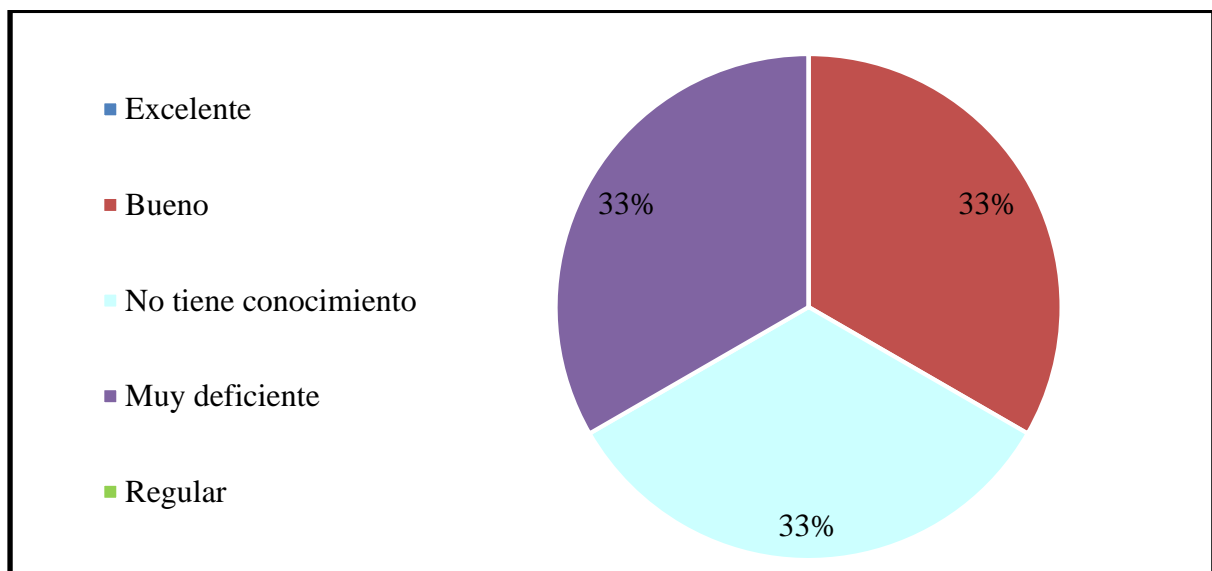


Figura 2 ¿Cómo se define el ingreso al sistema de control?

Análisis: En relación a la tabla y figura se observa que el 33% de los encuestados considera como bueno, muy deficiente y no tiene conocimiento sobre el nivel de seguridad al ingreso de los sistemas de control

Tabla 6

Nivel de seguridad de los servidores

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	2	67%
No tiene conocimiento	1	33%
Muy deficiente	0	0%
Regular	0	0%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

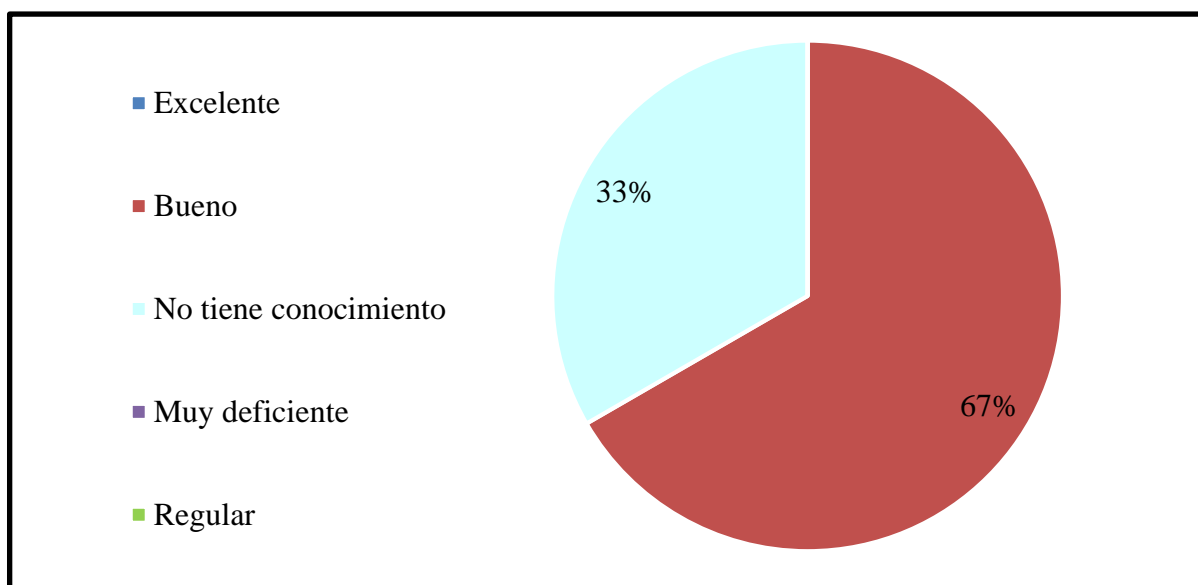


Figura 3 Nivel de seguridad que tienen los servidores

Análisis: En relación a la tabla y figura se observa que el 67% de los encuestados considera como bueno el nivel de seguridad que tienen los servidores, a diferencia que un menor porcentaje 33 % menciona que tiene un conocimiento regular.

Tabla 7

Definición de antivirus

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	1	33%
No tiene conocimiento	0	0%
Muy deficiente	1	33%
Regular	1	33%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

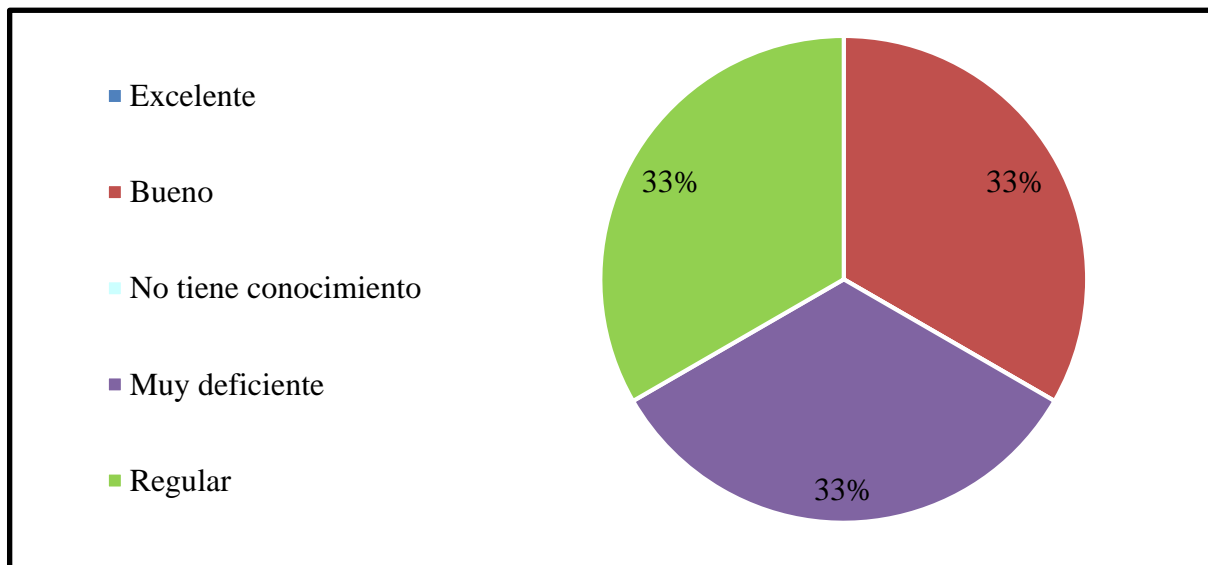


Figura 4 Calificación del antivirus

Análisis: En relación a la tabla y figura se observa que el 33% de los encuestados considera como bueno, muy deficiente y regular sobre la definición del antivirus instalado en los equipos de cómputo de la empresa.

Tabla 8

Nivel de seguridad que brinda el antivirus

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	2	67%
No tiene conocimiento	0	0%
Muy deficiente	0	0%
Regular	1	33%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

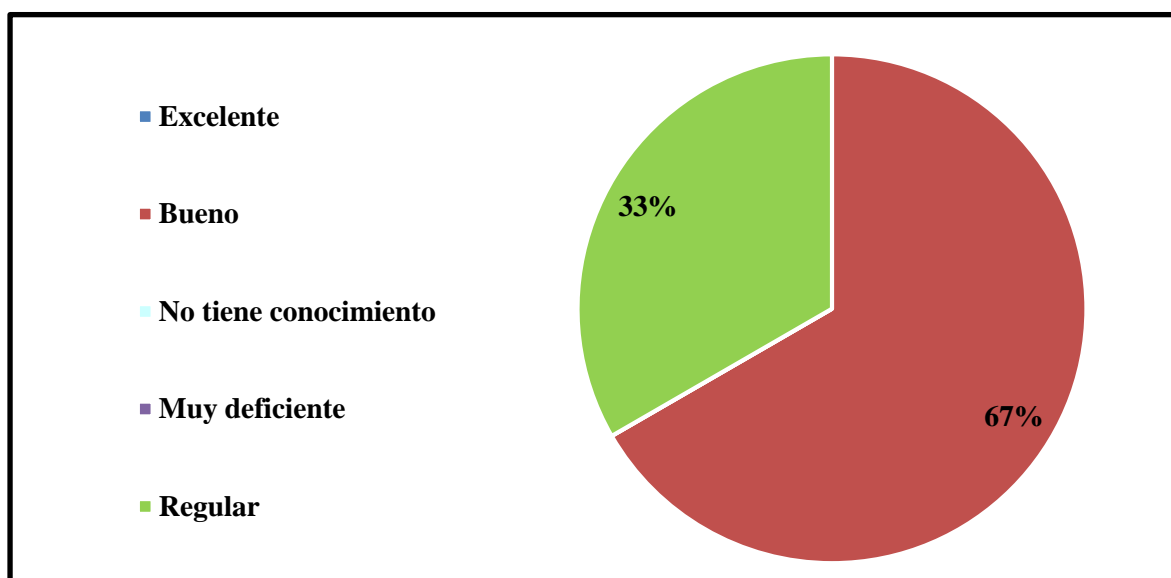


Figura 5 Nivel de protección del antivirus

Análisis: En relación a la tabla y figura se observa que el 67% de los encuestados considera como bueno el nivel de protección que tiene el antivirus, a diferencia que un menor porcentaje 33 % menciona que tiene un conocimiento regular

3.1.2 Entrevista

Se realizó la entrevista al Gerente de la empresa BERENDSON NATACION S.R.L la cual constó de 3 preguntas relacionadas al primer objetivo sobre la identificación de los activos que existen en la empresa y así obtener los datos necesarios.

Nos informó que los trabajadores de la empresa no tienen el conocimiento ni la capacitación adecuada al momento de identificar los activos que se encuentran en sus respectivas áreas.

Se concluyó que el encargado del area de gerencia solo conoce un 33 % sobre la identificación de los activos que existen en la empresa BERENDSON NATACION S.R.L eso puede traer dificultad ya que no se podrá saber cómo y qué proteger de las amenazas de los activos.

3.2 Conocer los riesgos informáticos en la empresa Berendson Natación S.R.L.

3.2.1 Entrevista

Se realizó la entrevista al Gerente de la empresa BERENDSON NATACION S.R.L la cual constó de 4 preguntas relacionadas al segundo objetivo sobre el nivel de conocimiento de los riesgos informáticos que existen en la empresa y así obtener los datos necesarios.

El gerente nos indicó que tanto él como sus trabajadores no conocen los riesgos informática que hay en la actualidad ya que no cuentan con un área específica de sistemas e informática que los pueda capacitar y guiar para disminuir o eliminar la amenazas y riesgos que se presentan en la organización.

Una vez culminada la entrevista se procedió al análisis de las respuestas dadas por él y se obtuvo que hace falta capacitar a los empleados en el tema de los riesgos informáticos e informar sobre las consecuencias puede traer la falta de un diagnóstico de la seguridad informática de los activos de la empresa Berendson Natación S.R.L.

3.2.2 Encuesta

Tabla 9

Nivel de conocimiento sobre seguridad de la información

Indicadores	Frecuencia	Porcentual
Excelente	1	33%
Bueno	1	33%
No tiene conocimiento	1	33%
Muy deficiente	0	0%
Regular	0	0%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

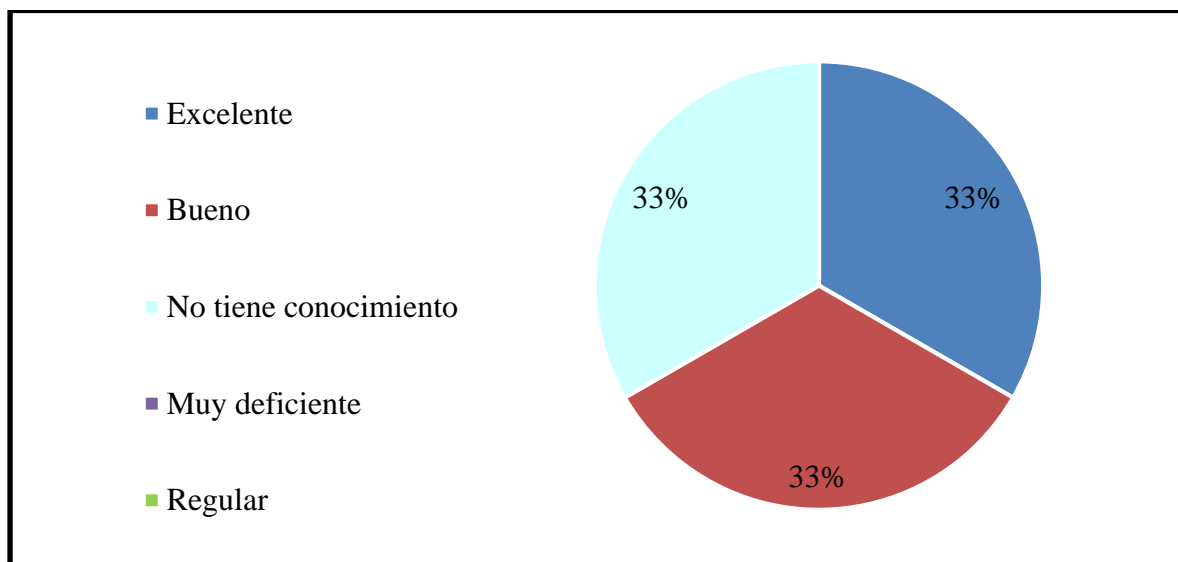


Figura 6 Porcentaje del nivel de conocimiento con respecto a la seguridad de la información

Análisis: En relación a la tabla y figura se observa que el 33% de los encuestados considera al nivel de seguridad de información como bueno, excelente y no tiene conocimiento.

Tabla 10

Nivel de Conocimiento sobre la Norma que establece la Seguridad a La información

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	1	33%
No tiene conocimiento	2	67%
Muy deficiente	0	0%
Regular	0	0%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

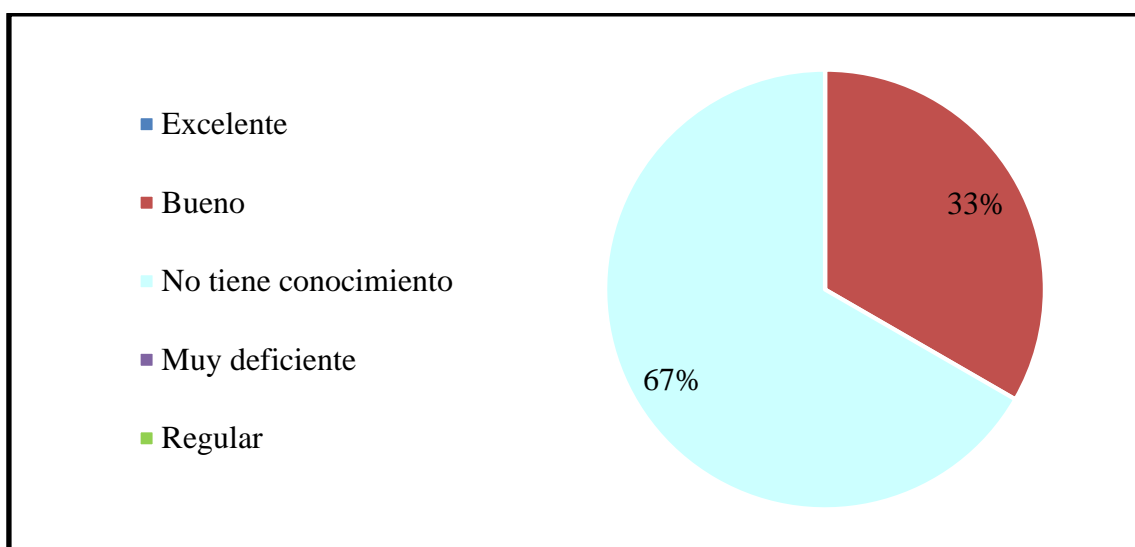


Figura 7 Nivel de conocimiento sobre la norma de seguridad de información

Análisis: En relación a la tabla y figura se observa que el 67% de los encuestados considera que no tiene conocimiento sobre la norma que establece la seguridad de la información, a diferencia que un menor porcentaje 33 % menciono que tiene un conocimiento bueno.

Tabla 11

Nivel de conocimiento sobre la norma ISO/IEC 27001

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	0	0%
No tiene conocimiento	3	100%
Muy deficiente	0	0%
Regular	0	0%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

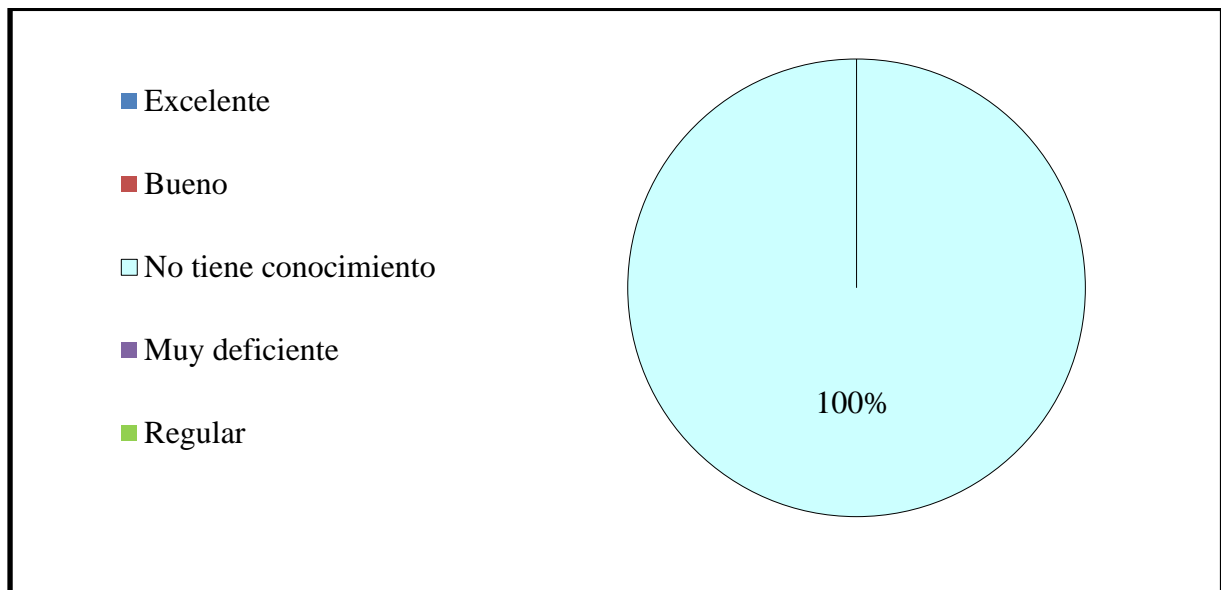


Figura 8 Nivel de conocimiento de la Norma ISO/IEC 27001

Análisis: En relación a la tabla y figura se observa que el 100% de los encuestados considera que no tiene conocimiento sobre la Norma ISO/IEC 27001

Tabla 12

Nivel de conocimiento sobre la Ley de Protección de datos

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	0	0%
No tiene conocimiento	2	67%
Muy deficiente	0	0%
Regular	1	33%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

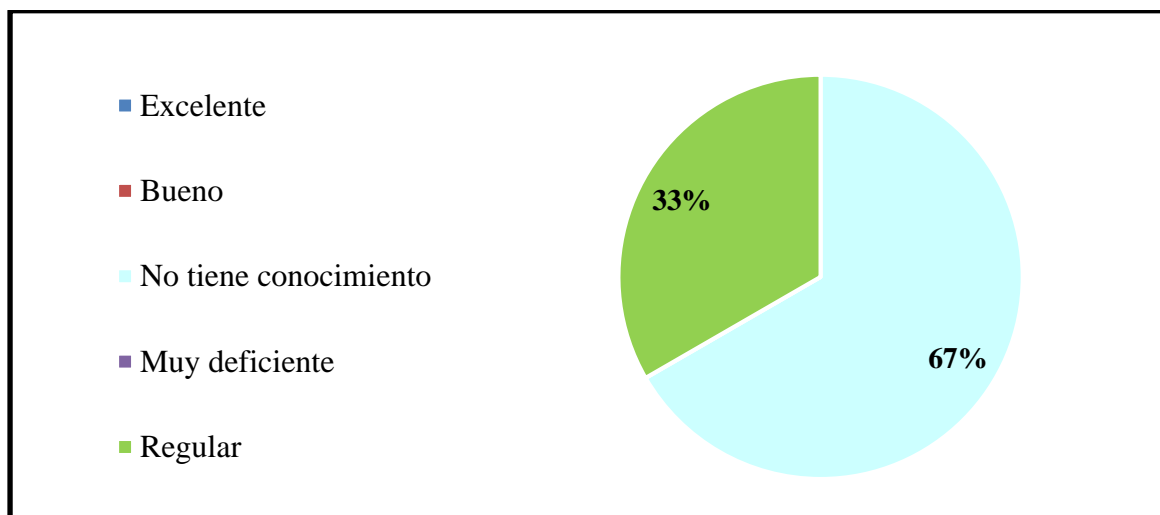


Figura 9 Nivel de conocimiento sobre la Ley de Protección de Datos

Análisis: En relación a la tabla y figura se observa que el 67% de los encuestados considera que no tiene conocimiento sobre la norma de la ley de protección de datos, a diferencia que un menor porcentaje 33 % menciona que tiene un conocimiento regular.

Tabla 13

Definición de la restricción de páginas no permitida en la empresa

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	1	33%
No tiene conocimiento	0	0%
Muy deficiente	1	33%
Regular	1	33%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

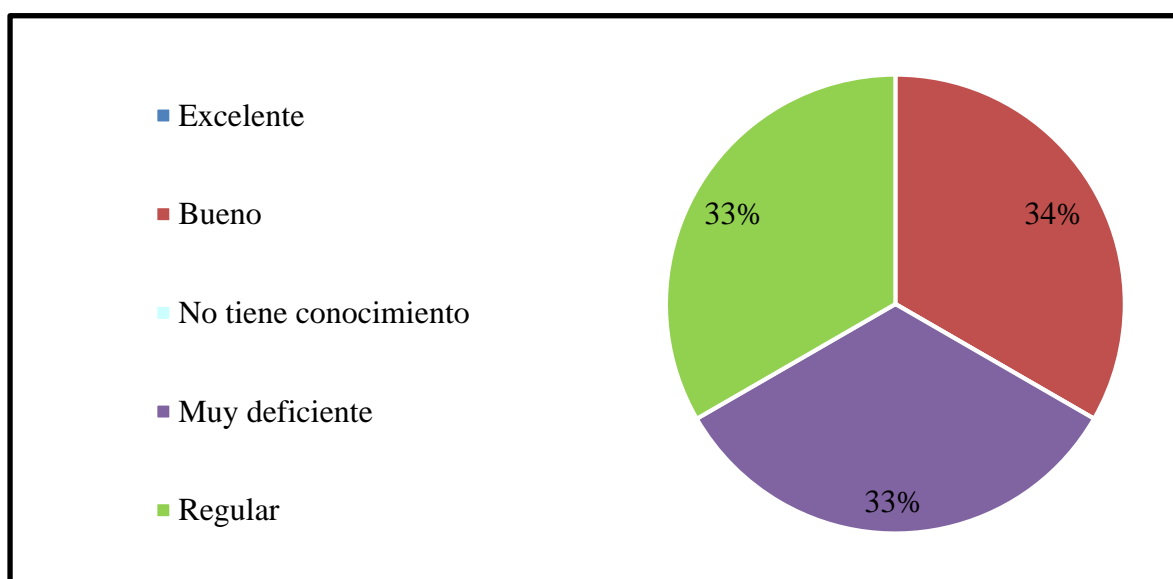


Figura 10 Nivel de restricción de páginas

Análisis: En relación a la tabla y figura se observa que el 33% de los encuestados considera como bueno, muy deficiente y regular sobre la definición de la restricción a páginas no permitidas en la empresa, a diferencia que un menor porcentaje 34 % menciona que tiene un conocimiento bueno

Tabla 14

Definición del nivel de password para el ingreso al sistema

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	1	33%
No tiene conocimiento	1	33%
Muy deficiente	1	33%
Regular	0	0%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

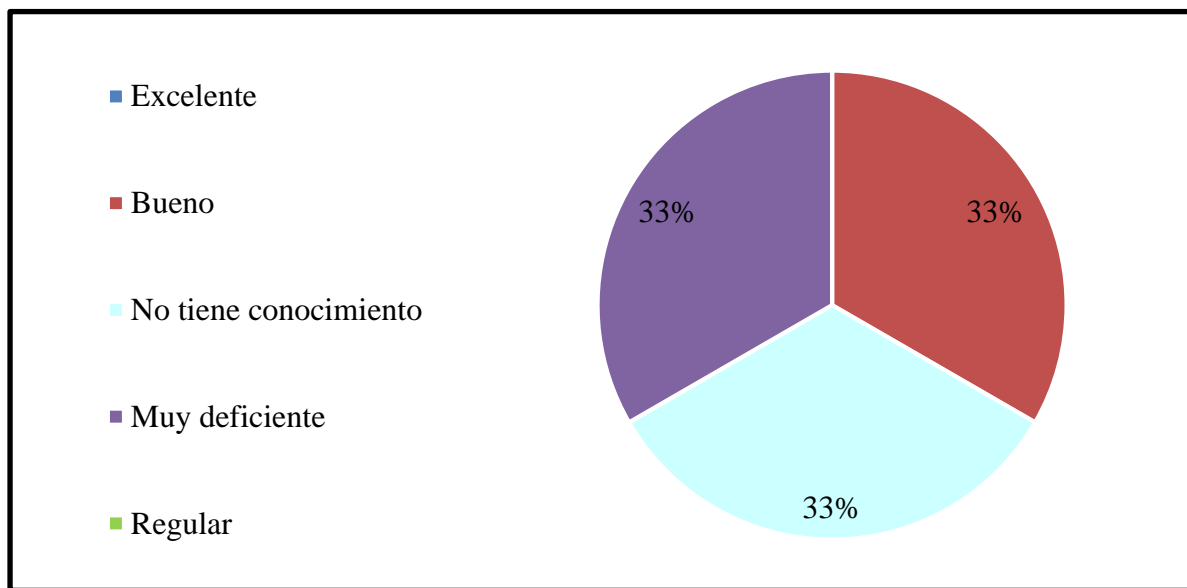


Figura 11 Calificación sobre el Nivel de Password para el ingreses a los sistemas

Análisis: En relación a la tabla y figura se observa que el 33% de los encuestados considera como bueno, no tiene conocimiento y regular sobre la definición del nivel de password para el ingreses a los sistemas

Tabla 15

Nivel de seguridad para el ingreso al sistema

Indicadores	Frecuencia	Porcentual
Excelente	0	0%
Bueno	1	33%
No tiene conocimiento	1	33%
Muy deficiente	1	33%
Regular	0	0%
Total	3	100%

Fuente: Datos obtenidos de la encuesta aplicada a las áreas de la empresa (Elaboración propia)

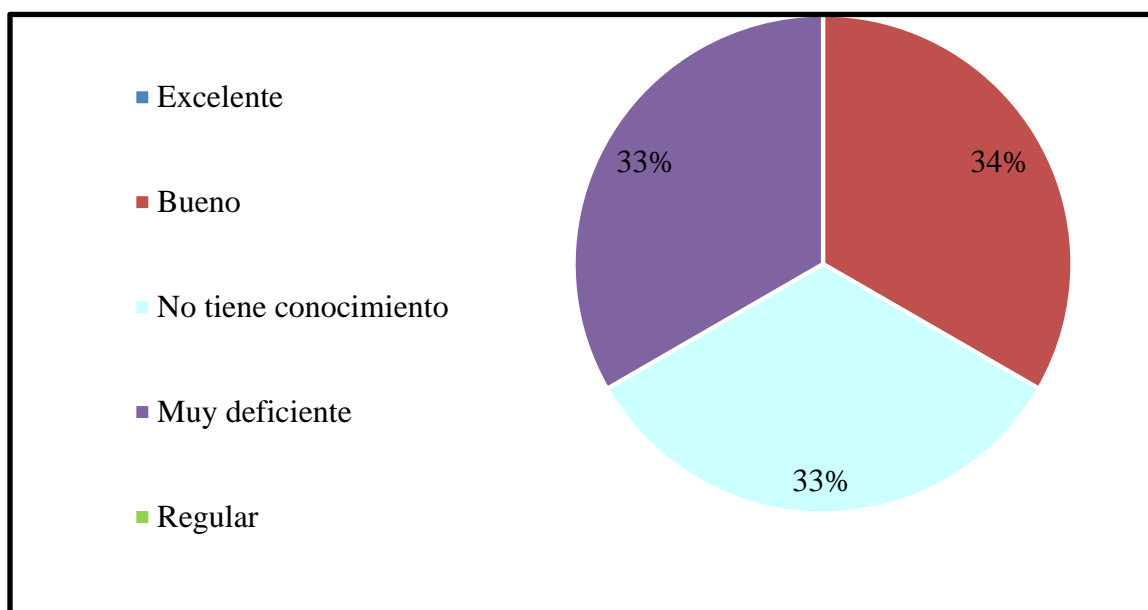


Figura 12 El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema

Análisis: En relación a la tabla y figura se observa que el 33% de los encuestados considera como no tiene conocimiento y muy deficiente sobre la definición del nivel de password para el ingresas a los sistemas, a diferencia que un menor porcentaje 34 % menciono que tiene un conocimiento bueno.

Según Bermúdez, K.; Bailón, E. (2015) el análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001- Sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros, que mediante controles de seguridad se puede mejorar en ámbito financiero ,pues ayudara a prevenir incidentes de seguridad que puedan incurrir en altos costos para la empresa. Esto permite obtener de los sistemas datos claros y precisos minimizando incidentes de seguridad como daños de aplicaciones, equipos tecnológicos, robo o alteración de información.

Según Chavez, J.(2016) nos informa en su análisis y modelos de datos de redes para seguridad informática que comprende el diseño e implementación de un ambiente de simulación basado en herramientas de código libre para el estudio de una red simplificada de Internet en cuanto a servicios, aplicaciones, flujos y vulnerabilidades de seguridad. Utilizando estas herramientas se estudia el comportamiento de la red durante condiciones de tráfico web normal y durante ataques informáticos definidos, con el objetivo de generar modelos de predicción y detección que permitan detectar la ocurrencia de un ataque informático mientras este está en curso o en el corto plazo, desde su comienzo.

El realizar un diagnóstico de la seguridad informática de los activos de la empresa Berendson Natación S.R.L. no solo ayuda a proteger mejor los activos que existen en la organización sino también ayuda económicamente ya que este diagnostico evita perdidas futuras, se determino los riesgos y amenazas que se tienen como estar expuestos a robo o alteración de información , ataques informáticos ,en base a esto se propuso implementar un modelo de seguridad informática aplicando la Norma ISO/IEC 27001 para proteger los activos de información de la empresa incluyendo políticas de seguridad informática que ayuden a mejorar la protección como realizar copias de seguridad cada cierto tiempo o restringir acceso a los sistemas, asignar las responsabilidades a los encargados de las areas , capacitar al personal y sancionar en caso de alguna falta que pueda afectar directamente a la organización . Esto permite mejorar la imagen empresarial de Berendson Natación S.R.L. ya que están preparados para cualquier incidente que pueda ocurrir dentro de la empresa.

Este trabajo nos permitió conocer el nivel de conocimiento que tiene cada trabajador en cuanto a las normas de seguridad informática, la restricción de páginas web, la Ley de Protección de Datos y que medidas se debe tomar al momento de capacitar al personal de la empres Berendson Natación S.R.L.

IV. Conclusiones

- Mediante la encuesta realizada se demuestra que los activos de la empresa Berendson Natación S.R.L. están expuestos a riesgos y amenazas como daños o modificaciones de información, robos, fraudes. Con la elaboración de diagnóstico de la seguridad informática se pretendió que la empresa tome decisiones para prevenir las amenazas a las que están expuesta sus activos y la información que es manejada por los trabajadores.
- Se evaluó el nivel de conocimiento de los trabajadores de la empresa Berendson Natación S.R.L. que se tiene respecto a la seguridad informática, la ley de protección de los datos, la norma ISO/IEC 27001, el nivel de protección que brinda el antivirus, el nivel de seguridad para ingresar a sistema y a los riesgos informativos que tiene la empresa, en el cual solo el 33% de la población tiene un conocimiento muy deficiente respecto a estos puntos ya mencionados.

V. Recomendaciones

- Elaborar un modelo de seguridad informática aplicando la Norma ISO/IEC 27001 para proteger los activos de información de la empresa Berendson Natación S.R.L, que permita incrementar políticas de seguridad para poder disminuir y eliminar los riesgos y amenazas que padece los activos , así ayudar con su protección, realizar auditorías para llevar un mejor control de las normas y estatutos de la empresa a la vez capacitar a los trabajadores sobre riesgos informáticos que tiene la empresa
- Crear el área de sistemas e informática para que así monitoree el cumplimiento de las políticas y realice las capacitaciones necesarias.

VI. Referencias bibliográficas

- Bermúdez, K.; Bailón, E.;. (2015). Analisis en Seguridad Informática y Seguridad de la Información basado en la norma ISO/IEC 27001-Sistema de Gestion de Seguridad de la Información dirigo a una empresa en servicios financieros. (*Trabajo previo para la obtención del titulo de Ingeniero de Sistemas*). Guayaquil. Obtenido de http://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/8572/Burga_gj%20-%20Resumen.pdf?sequence=1&isAllowed=y
- Calderon, J. (2017). Aplicación de la Herramienta de Gestión de Riesgos para la Seguridad Informática del Honadomani San Bartolomé. (*Tesis para Obtener el Título Profesional de Ingeniería de Sistemas*). Lima. Obtenido de http://repositorio.ucv.edu.pe/bitstream/handle/UCV/1879/Calderon_AJJ.pdf?sequence=1&isAllowed=y
- Chavez, J. (2016). Analisis y Modelos de Datos de Redes para Seguridad Informática. (*Optar al Título de Ingeniero Civil Eléctrico*). Santiago de Chile. Obtenido de <http://repositorio.uchile.cl/bitstream/handle/2250/138269/Analisis-y-modelos-de-datos-de-redes-para-seguridad-informatica.pdf?sequence=1&isAllowed=y>
- Chura, E. (2018). Plan de Seguridad Informática en la Municipalidad Provincial de San Román (Sistema Web). (*Optar el Grado Académico de Magíster en Ingeniería de Sistemas*). Juliana. Obtenido de http://repositorio.uancv.edu.pe/bitstream/handle/UANCV/1797/T036_24007013.pdf?sequence=3&isAllowed=y
- Deconceptos.com. (2019). *Deconceptos.com*. Obtenido de Deconceptos.com: <https://deconceptos.com/ciencias-sociales/cuestionario>
- EncuestaTick. (2019). *EncuestaTick*. Obtenido de EncuestaTick: <https://www.portaldeencuestas.com/que-es-una-encuesta.php>
- Palomares, M. (2016). Sistema de Seguridad Informática para los Riesgos en la Red De Datos de la Empresa Grupo Palomares Sac. (*Tesis Para Obtener El Título Profesional De Ingeniería De Sistemas*). Lima. Obtenido de http://repositorio.ucv.edu.pe/bitstream/handle/UCV/22052/Palomares_MMG.pdf?sequence=1&isAllowed=y
- Significados. (2019). *Significados*. Obtenido de Significados: <https://www.significados.com/entrevista/>
- Toledo, Neftali. (2019). *Población y muestra*. Obtenido de <https://core.ac.uk/download/pdf/80531608.pdf>

Universidad Internacional de Valencia;. (2018). *Universidad Internacional de Valencia*.
Obtenido de Universidad Internacional de Valencia:
<https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/>

Vásquez, I. (2005). *Gestiopolis*. Obtenido de Gestiopolis: <https://www.gestiopolis.com/tipos-estudio-metodos-investigacion/>

VII. Anexos

Anexo A

Encuesta

ÁREA DE TI PARA LA EMPRESA BERENDSON NATACIÓN 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 <input type="checkbox"/> Tecnólogo <input type="checkbox"/> Profesional <input type="checkbox"/> Otros <input type="checkbox"/>	

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	Que conocimientos posee con respecto a la seguridad de la información					
1.1.2	Que conocimientos tiene sobre las normas que establece de seguridad de la información					
1.2	Conocimiento de la normatividad					

1.2.1	Cuál es su conocimiento sobre Norma ISO/27001					
1.2.2	Que 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					

Anexo B
ENTREVISTA
ÁREA DE TI PARA LA EMPRESA BERENDSON NATACIÓN 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 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 C
EVIDENCIAS

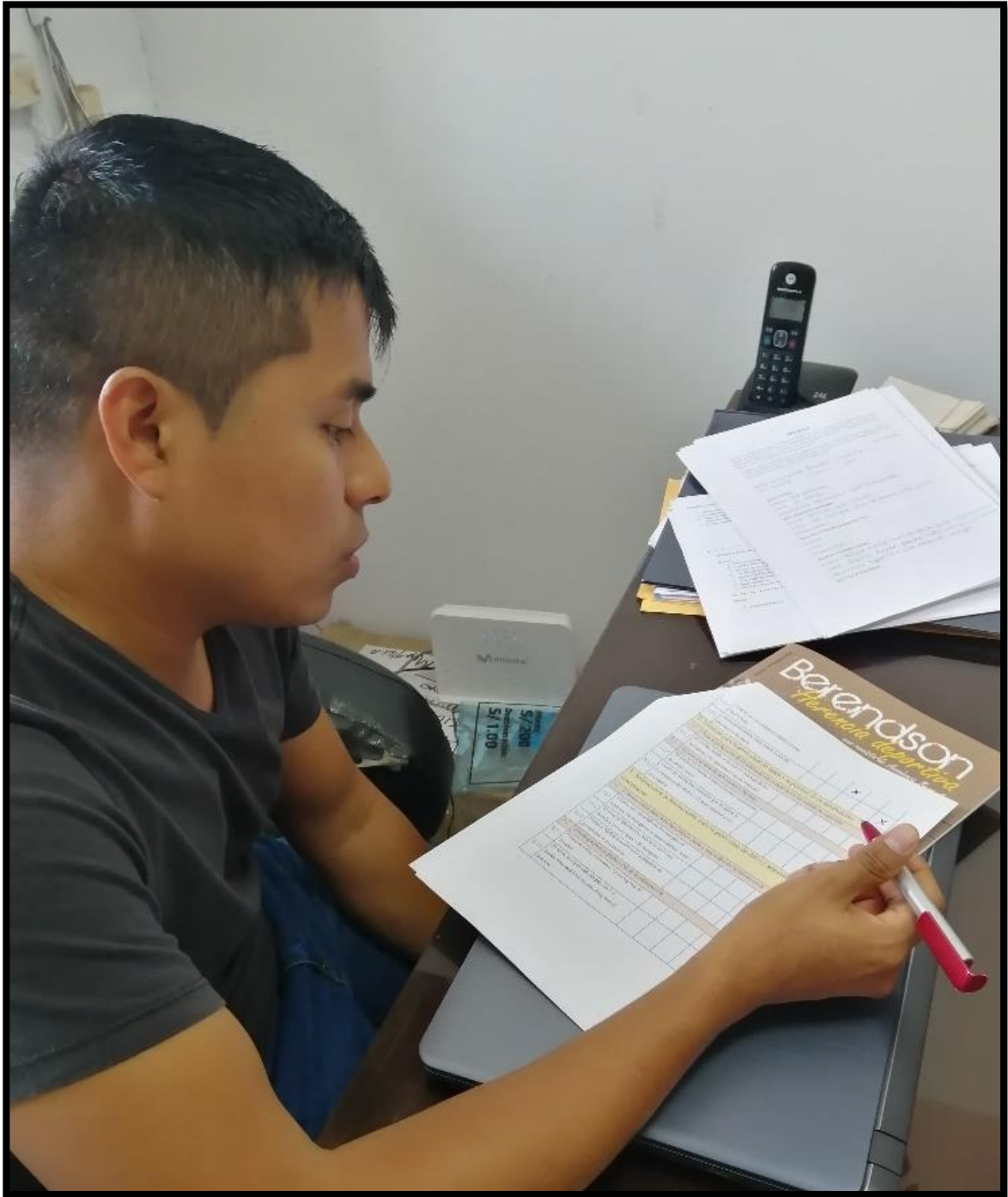


Figura 13 Desarrollo de encuesta a cargo del responsable del área de administración

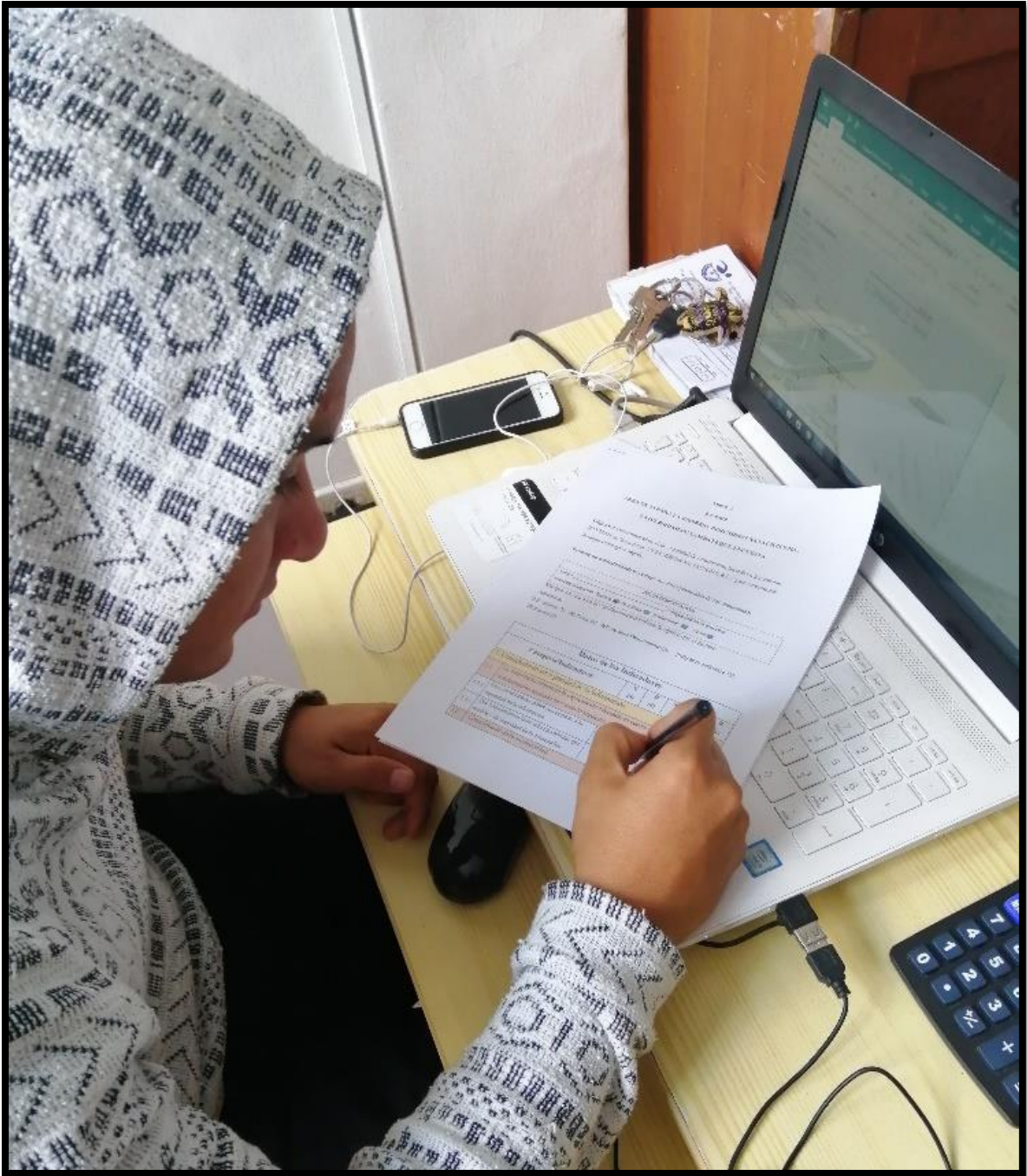


Figura 14 Desarrollo de encuesta a cargo del responsable del área de atención al cliente



Figura 15 Explicación de la encuesta por parte de los autores



Figura 16 Explicación de la encuesta por parte de los autores

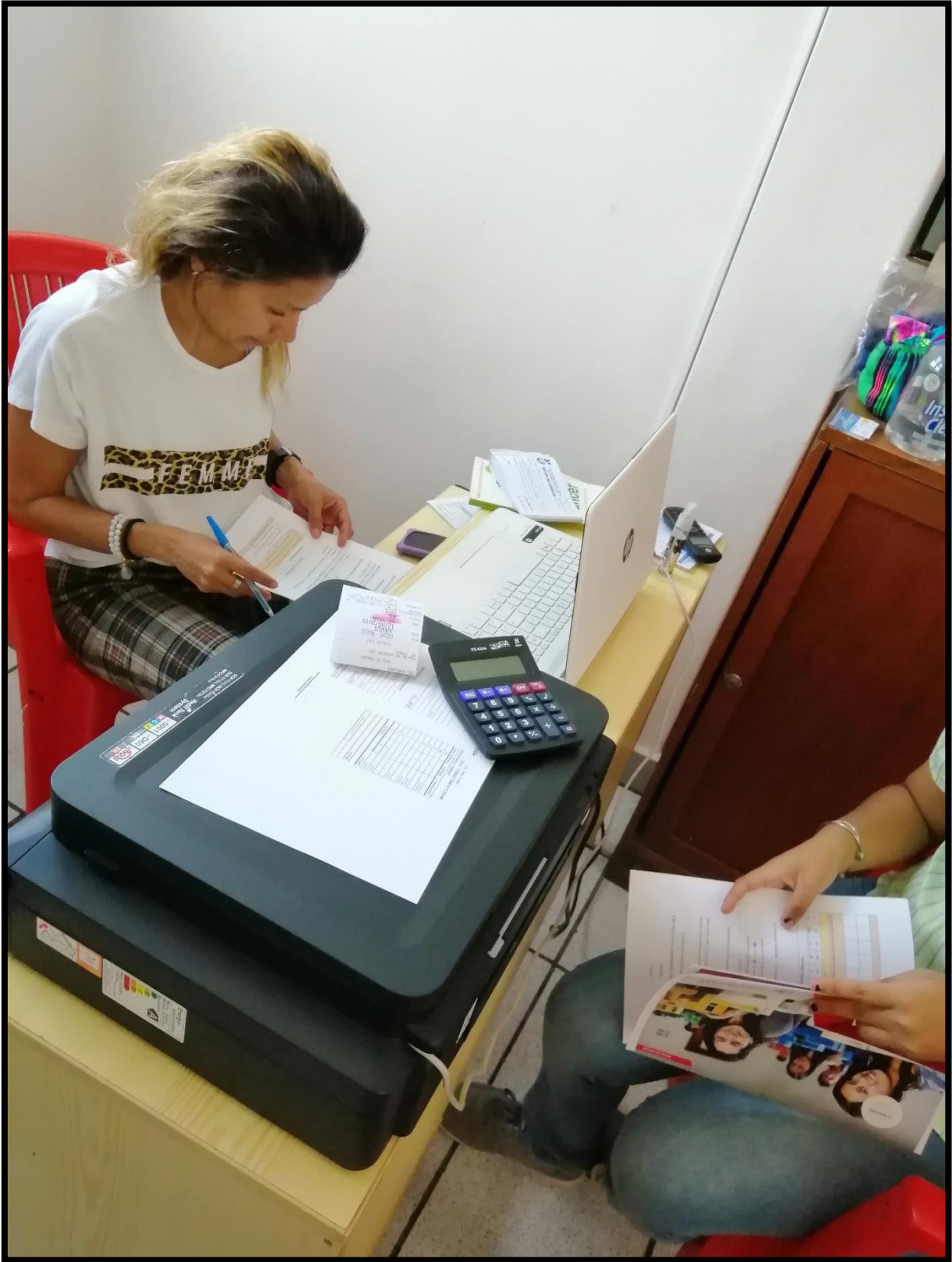


Figura 17 Desarrollo de encuesta a cargo del responsable del área de atención al cliente

Anexo D
MATRIZ DE CONSISTENCIA

Autores:

Delgado Saavedra Martha Mellissa

Vasquez Zevallos José Luis

Asesor:

Ing. Enrique Santos Nauca Torres

Escuela de Ingeniería de Sistemas

Tabla 16 *Matriz de consistencia*

TITULO	PROBLEMA	HIPOTESIS	OBJETIVO	VARIABLES	TIPO DE DISEÑO DE INVESTIGACIÓN	POBLACIÓN Y MUESTRA	TÉCNICA E INSTRUMENTO
Diagnóstico de la seguridad informática de los activos de la empresa Berendson Natación S.R.L.	¿Cuál sería el nivel de seguridad informática en los	Si se tiene un diagnóstico o adecuada de la seguridad	GENERAL Diagnosticar la seguridad informática de los activos de la empresa	Diagnóstico de seguridad informática	Descriptiva	Esta formada por 4 computadoras en las áreas de	Técnica: Encuesta Entrevista Instrumento: Cuestionario

activos de	informática	Berendson	administrac
la	a, entonces	Natación S.R.L.	ión y
empresa	es posible		atención al
Berendso	identificar	ESPECIFICO	cliente de la
n	los riesgos	S	empresa
Natación	de los	-Identificar los	Berendson
S.R.L.?	activos	activos que	Natación
	informática	existen en la	S.R.L.
	os de la	empresa	
	empresa	Berendson	
	Natación	Natación S.R.L.	
	S.R.L.	-Conocer los	
		riesgos	
		informáticos en	
		la empresa	
		Berendson	
		Natación S.R.L.	

Anexo E
VALIDACIÓN DE INSTRUMENTO

CUESTIONARIO ENCUESTA – COLABORADORES

DIAGNÓSTICO DE LA SEGURIDAD INFORMÁTICA DE LOS ACTIVOS DE LA EMPRESA BERENDSON NATACIÓN S.R.L.

RESPONSABLES: Delgado Saavedra Martha Mellissa
Vasquez 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 considera un puntaje del 1 al 5:

La empresa ha impartido la capacitación adecuada en cuanto normas de seguridad de la información teniendo en cuenta lo siguiente					
1.	Posee conocimiento respecto a la seguridad de la información.				
2.	Tiene conocimiento sobre las normas que establece la seguridad de información.				
Conocimiento de la normatividad					
3.	Tiene conocimiento sobre Norma ISO/IEC 27001.				
4.	Tiene conocimiento sobre la ley de protección de datos.				
Técnicas 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 que estados se encuentran.				
Acceso al área de servidores o backup					
6.	Como define el sistema de control para el ingreso a esta área.				

7.	Como se define los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores.					
Aplicaciones de herramientas para la protección de datos y seguridad de la información						
Herramientas para la protección de datos y seguridad de la información						
8.	Como define los antivirus instalados en los equipos de cómputo de la empresa.					
9.	El nivel de protección que brinda el antivirus instalado en los equipos de cómputo.					
10.	Como define la restricción a paginas no permitidas en la empresa.					
Estrategia para la protección de la información						
11.	Como define el password para el acceso al sistema.					
12.	El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.					

RECOMENDACIONES:

Apellidos y Nombres: -----
 Título y/o grado académico: -----

 FIRMA

VALIDACIÓN DE INSTRUMENTO
CUESTIONARIO ENCUESTA – COLABORADORES

**DIAGNÓSTICO DE LA SEGURIDAD INFORMÁTICA DE LOS ACTIVOS DE LA
EMPRESA BERENDSON NATACIÓN S.R.L.**

RESPONSABLES: Delgado Saavedra Martha Mellissa
Vasquez 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 considera un puntaje del 1 al 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 cuanto normas de seguridad de la información teniendo en cuenta lo siguiente						
1.	Posee conocimiento respecto a la seguridad de la información.					X
2.	Tiene conocimiento sobre las normas que establece la seguridad de información.					X
Conocimiento de la normatividad						
3.	Tiene conocimiento sobre Norma ISO/IEC 27001.					X
4.	Tiene conocimiento sobre la ley de protección de datos.					X
Técnicas 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 que estados se encuentran.					X
Acceso al área de servidores o backup						
6.	Como define el sistema de control para el ingreso a esta área.					X
7.	Como se define los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores.					X


Figura 18 Validación de encuestas N° 1

Aplicaciones de herramientas para la protección de datos y seguridad de la información						
Herramientas para la protección de datos y seguridad de la información						
8.	Como define los antivirus instalados en los equipos de cómputo de la empresa.					X
9.	El nivel de protección que brinda el antivirus instalado en los equipos de cómputo.					X
10.	Como define la restricción a paginas no permitidas en la empresa.					X
Estrategia para la protección de la información						
11.	Como define el password para el acceso al sistema.					X
12.	El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.					X

RECOMENDACIONES :

Apellidos y Nombres: CARRA VÁSQUEZ JORGE TOMÁS

Título y/o grado académico: ING. INDUSTRIAL Y SISTEMAS



 FIRMA

Figura 19 Validación de encuestas N° 1

VALIDACIÓN DE INSTRUMENTO
CUESTIONARIO ENCUESTA – COLABORADORES

**DIAGNÓSTICO DE LA SEGURIDAD INFORMÁTICA DE LOS ACTIVOS DE LA
EMPRESA BERENDSON NATACIÓN S.R.L.**

RESPONSABLES: Delgado Saavedra Martha Mellissa
Vasquez 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 considera un puntaje del 1 al 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 respecto a la seguridad de la información.				/	
2.	Tiene conocimiento sobre las normas que establece la seguridad de información.				/	
Conocimiento de la normatividad						
3.	Tiene conocimiento sobre Norma ISO/IEC 27001.				/	
4.	Tiene conocimiento sobre la ley de protección de datos.				/	
Técnicas 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 que estados se encuentran.				/	
Acceso al área de servidores o backup						
6.	Como define el sistema de control para el ingreso a esta área.				/	
7.	Como se define los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores.				/	

Figura 20 Validación de encuestas N° 2

Aplicaciones de herramientas para la protección de datos y seguridad de la información					
Herramientas para la protección de datos y seguridad de la información					
8.	Como define los antivirus instalados en los equipos de cómputo de la empresa.				✓
9.	El nivel de protección que brinda el antivirus instalado en los equipos de cómputo.			✓	
10.	Como define la restricción a paginas no permitidas en la empresa.				✓
Estrategia para la protección de la información					
11.	Como define el password para el acceso al sistema.				✓
12.	El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.			✓	

RECOMENDACIONES:

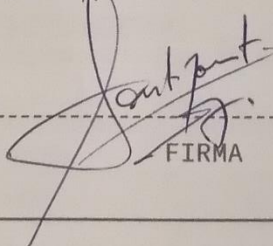
Apellidos y Nombres:	NAUCA TORRES ENRIQUE SANTOS
Título y/o grado académico:	INGENIERO DE SISTEMAS Y COMPUTACIÓN - ASISTENTE EN ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS
	 FIRMA

Figura 21 Validación de encuestas N° 2