UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

"ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL MANEJO DE INFORMACIÓN DE LA DISTRIBUIDORA ALMAPO S.R.L. HUACHO,2016"

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO EN INFORMÁTICA Y DE SISTEMAS

AUTOR
BACH. GONZALES QUINTEROS, YULEICY YAJAIRA

ASESOR:
ING. LARA CARREÑO, MARCO

HUACHO – PERÚ
2016

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

PALABRAS CLAVES

Tema	Seguridad Informática
Especialidad	Gestión

KEY WORDS

Theme	Informatic Security
Especialty	Management

TÍTULO

"ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL MANEJO DE INFORMACIÓN DE LA DISTRIBUIDORA ALMAPO S.R.L. HUACHO, 2016"

RESUMEN

La presente tesis tuvo como finalidad determinar políticas de seguridad informática para el manejo de información de la Distribuidora Almapo S.R.L., Huacho, a través del cual se conocerá las deficiencias en el uso de la información por la falta de controles de seguridad, ya que la información que se procesa diariamente es confidencial y de mucha importancia para la empresa, por ende la información debe ser protegida correctamente.

Para el desarrollo de la investigación se utilizó la Norma ISO/IEC 27001:2013, que es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El tipo de investigación fue aplicada y el nivel de investigación fue descriptivo.

En conclusión, los resultados obtenidos van a permitir evidenciar las vulnerabilidades en el uso de la información y para que estos incidentes no vuelvan a suceder es necesario determinar políticas de seguridad, a través del cual se darán las recomendaciones respectivas y así se logrará mejores resultados.

ABSTRACT

The present thesis aimed to determine computer security policies for the information management of the Distributor Almapo SRL, Huacho, through which it will be known the deficiencies in the use of the information due to the lack of security controls, since the information which is processed on a daily basis is confidential and of great importance to the company, therefore the information must be protected correctly.

For the development of the research, ISO / IEC 27001: 2013 was used, which is an international standard that allows the assurance, confidentiality and integrity of data and information, as well as the systems that process it. The type of research is applied and the level of research was descriptive.

In conclusion, the results obtained will allow to highlight the vulnerabilities in the use of information and for these incidents not to happen again, it is necessary to determine security policies, through which the respective recommendations will be given and thus better results will be achieved.

INTRODUCCIÓN

1.1. Antecedentes y Fundamentación Científica

1.1.1 Antecedentes

Bermúdez y Bailón, (2015) en Guayaquil - Ecuador, realizó un proyecto de investigación denominado, "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", el cual tuvo como finalidad conocer las vulnerabilidades a las que está expuesta la información por la falta de aplicación de controles de seguridad. La investigación tiene un nivel descriptivo y un diseño no experimental. 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. (Bermúdez Molina & Bailón Sánchez, 2015)

Macen (2014) en Asunción - Paraguay, en su tesis de grado denominado, "Políticas De Seguridad De La Información: Realidad De La UTIC Para La Construcción De Políticas De Seguridad De La Información", el cual nació de la necesidad de elaborar políticas de seguridad de la información para el Departamento de Tecnología Informática de la UTIC. Por ello se propuso describir la realidad que presenta la UTIC para la construcción de política de seguridad de la información. Esta investigación tuvo un enfoque cuantitativo, de nivel descriptivo, el diseño es no experimental. El resultado demostró una proporción global con respecto al manejo de la información de manera insegura 55,95 % y una proporción del manejo seguro de 44,05 %. Como

recomendación se presenta el manual de políticas de seguridad de la información para su implementación. (Macen Rojas, 2014)

Galeano y Alzate, (2013) en Pereira - Colombia, realizó su trabajo de grado denominado, "Protocolo De Políticas De Seguridad Informática Para Las Universidades De Risaralda", el cual tuvo como objetivo proponer un protocolo que marque unas pautas claras al momento de implementar la seguridad en las instituciones de educación superior proporcionando una orientación y unas recomendaciones en la elección de herramientas. Como resultado esperado se realizó un protocolo basado en la norma ISO 27000 e ISO 17000, el cual se concluye con la propuesta de un protocolo de seguridad que puede ser aplicado en las instituciones de educación superior el cual permitirá guiar y facilitar su implementación garantizando una disponibilidad, integridad y seguridad de la información en un porcentaje muy alto de aplicación y protección. (Galeano Villa & Alzate Castañeda, 2013)

Henao y Ortiz, (2010) en Pereira - Colombia, en su proyecto de investigación denominado, "Política De Seguridad Informática Para Apostar S.A.", tuvo como objetivo principal y único crear conciencia organizacional, en lo referente a la protección de la información y de los datos. Se establece y se confirma la falta de prácticas seguras en el área informatica y la falta de preocupación por parte de la alta gerencia de las organizaciones para adoptar medidas al respecto. Finalmente, se diseña una propuesta que, puesta en marcha, le ayudará a Apostar S.A. a mejorar su protección frente a riesgos inherentes a su actividad económica y marcará la ruta para iniciar un proyecto estructurado y que abarque todos los niveles de seguridad en la organización. (Henao Acosta & Ortiz Villegas, 2010)

Alcántara (2015) en Chiclayo - Perú, en su tesis de grado denominado, "Guía De Implementación De La Seguridad Basado En La Norma ISO/IEC 27001, Para Apoyar La Seguridad En Los Sistemas Informáticos De La Comisaría Del Norte P.N.P. En La Ciudad De Chiclayo", propone una guía de implementación que apoye a la seguridad de los sistemas de información con la finalidad de medir los riesgos y evaluar los controles en el uso de las tecnologías de información, haciendo uso de técnicas y estrategias de análisis, que permitan una mejor gestión de TI, a disposición de las entidades públicas. El tipo de investigación es tecnológica aplicada. Los resultados esperados fueron que se pudo incrementar el porcentaje de conocimiento por parte del personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la institución, teniendo como resultado personal comprometido con la seguridad en favor de la institución. (Alcántara Flores, 2015)

Yan y Zavala, (2013) en Trujillo - Perú, en su tesis de grado denominado, "Plan De Mejora De La Seguridad De Información Y Continuidad Del Centro De Datos De La Gerencia Regional de Educación La Libertad Aplicando Lineamientos ISO 27001 Y Buenas Prácticas COBIT", tuvo como finalidad elaborar un plan de mejora de seguridad de la información y continuidad del centro de datos, y mostrar los resultados obtenidos de la auditoria de sistemas, utilizando la metodología MAIGTI, el marco de trabajo y las directrices de auditoria propuestas por lineamientos ISO 27001 y buenas practicas COBIT 4.0. Para esta investigación, el nivel fue descriptivo y su diseño fue no experimental. El resultado esperado fue de brindar las recomendaciones necesarias para superar las falencias encontradas según las buenas prácticas y alineamientos por COBIT e ISO/IEC 27001 respectivamente, el cual se

proporcionará el Plan de Mejora para ser evaluado por la institución y así poder implementarlo. (Yan Carranza & Zavala Vasquez, 2013)

1.1.2 Fundamentación Científica

En líneas generales, cuando se decide desarrollar una política de seguridad estamos estableciendo las bases para la gestión de la seguridad de la información que se procesa en nuestros sistemas informáticos, sin embargo, no sólo se establecerá indicaciones técnicas sino también organizativas, relacionadas con recursos humanos o incluso con la seguridad física de nuestras instalaciones.

Las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Un punto fundamental es establecer los requisitos de seguridad de nuestra empresa, desarrollando un conjunto de principios y reglas que resuman como se gestionará la protección de la información del negocio, teniendo unos objetivos básicos que fundamentalmente serán garantizar la confidencialidad, integridad y disponibilidad de los datos.

- **Confidencialidad** es la propiedad de la información, por la que se garantiza que está accesible únicamente al personal autorizado.
- **Integridad** se refiere a la corrección y completitud de los datos.
- **Disponibilidad** es asegurar que los datos sean utilizables cuando estos sean necesitados para las tareas habituales de la organización.

1.2. Justificación De La Investigación

1.2.1. Social

Hoy en día la información es un activo muy importante en toda empresa, que a su vez también es propensa a sufrir daños y alteraciones, por ende es necesario protegerlo de todo tipo de amenazas. Esta investigación, permitirá a la empresa Distribuidora Almapo S.R.L. Huacho, darse cuenta porque es importante contar con políticas de seguridad informática frente a las diferentes vulnerabilidades a las que se vea desafiada la empresa, ya que esta necesita que la información sea manejada siempre de manera íntegra, disponible y confiable. Estas políticas beneficiarán a la empresa brindando recomendaciones y se podrá tomar las acciones preventivas a fin de evitar que la información esté en riesgo perjudicando la continuidad del negocio.

1.2.2. Conocimiento

Para el desarrollo de la investigación se buscó conocimientos selectivos y sistematizados, del cual se utilizó la Norma ISO/IEC 27001:2013, que es un estándar de calidad de seguridad de la información, que ayuda a minimizar los peligros o daños que pueda sufrir la información, frente diferentes incidentes.

A través de sus controles de seguridad nos permitió identificar las diferentes incidencias, de tal manera que así se pueda determinar las políticas de seguridad informática para el adecuado manejo de la información en la empresa. Esta norma es operativamente viable ya que existen modelos realizados en otras empresas.

1.3. Problema

1.3.1. Descripción Del Problema

En la actualidad en muchas empresas, sus negocios se basan exclusivamente en los datos que puedan suministrar de forma veraz y rápida. La gestión de sus operaciones que realiza la Distribuidora Almapo S.R.L Huacho, se llevan a cabo a través de un sistema informático, en el cual está consignado, tanto información de los clientes y de las actividades que se realizan diariamente con referencia a los productos. La empresa mantiene firme sus operaciones, pero a pesar de eso surge la necesidad de gestionar controles de seguridad para garantizar la integridad, disponibilidad y confidencialidad de la misma.

Actualmente en el almacén hay un sistema informático llamado FlexBussiness ERP, en el que se registra todas las entradas, salidas y reportes de los productos. Por el cual se le asignó al colaborador correspondiente un usuario para registrar toda la información en el sistema, este colaborador al momento de filtrar alguna información diferente a su sucursal, tiene acceso libremente sin restricciones, tanto es así que le permite crear un nuevo registro y a la vez eliminar la información que no corresponde a su sucursal, por lo que hasta la actualidad no se ha realizado ninguna acción para que se restringa tal hecho. A veces los colaboradores manejan gran cantidad de información el cual lo dejan libremente a vista y paciencia ya sea de personas internas o ajenas a la empresa, por el cual no comprenden que la información que poseen es bastante sensible a copias, daños o modificaciones. La falta de procedimientos o políticas de seguridad hace que no se tenga un uso adecuado del manejo de la información, permitiendo que esta sea totalmente vulnerable y disponible a cualquier persona.

Se observa que estas dificultades harían que la información sea muy susceptible a cualquier eventualidad, provocando un mal manejo o robo de información a la empresa. Por tal razón la presente investigación pretende aportar una definición clara y así poder establecer políticas de seguridad informática, permitiendo el uso adecuado del manejo de la información, a través de la Norma ISO/IEC 27001:2013.

1.3.2. Formulación Del Problema

¿Cómo establecer políticas de seguridad informática para el manejo de información de la Distribuidora Almapo S.R.L. Huacho, 2016?

1.4. Marco Referencial

1.4.1. Política de Seguridad

Wood (2002), define de diferentes maneras el concepto de política de seguridad, además de entregar procedimientos claros para su elaboración y justifica infaliblemente su importancia a nivel organizacional.

Las políticas son definidas como:

- Instrucciones gerenciales que trazan una dirección predeterminada o describen la manera de manejar un problema o situación.
- Planteamientos de alto nivel que transmiten a los trabajadores la orientación que necesitan para tomar decisiones presentes y futuras.
- Requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro, y en algunos casos fuera, de la organización.

- Son obligatorias y pueden considerarse el equivalente de una ley propia de la organización.

"Aunque nos encantaría que fuese de otra manera, las políticas simplemente no pueden sacarse de un estante, redactarse, aprobarse mediante un fácil proceso burocrático y emitirse, sino que deben adaptarse a las necesidades específicas de cada organización". (Wood, 2002)

Por su parte, Álvarez y Pérez (2004), aseguran que "las políticas de seguridad definen las reglas que la organización espera sean seguidas por sus miembros y las consecuencias derivadas de no cumplirlas. Constituyen la piedra angular para la implantación de la seguridad".

Según la Universidad Nacional de Colombia (2003) "Es importante resaltar que una política de seguridad tiene un ciclo de vida completo mientras está vigente. Este ciclo de vida incluye un esfuerzo de investigación, la labor de escribirla, lograr que las directivas de la organización la acepten, conseguir que sea aprobada, lograr que sea diseminada a través de la empresa, concienciar a los usuarios de la importancia de la política, conseguir que la acaten, hacerle seguimiento, garantizar que esté actualizada y, finalmente, suprimirla cuando haya perdido vigencia. Si no se tiene en cuenta este ciclo de vida se corre el riesgo de desarrollar políticas que sean poco tenidas en cuenta, incompletas, redundantes, sin apoyo por parte de los usuarios y las directivas, superfluas o irrelevantes".

Una política de seguridad es un conjunto de reglas y prácticas que regulan la manera en que se deben dirigir, proteger y distribuir los recursos en una organización para llevar a cabo los objetivos de seguridad informática de la misma.

Una política de seguridad en el ámbito de la criptografía de clave pública o PKI es un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad. Pueden cubrir cualquier cosa desde buenas prácticas para la seguridad de un solo ordenador, reglas de una empresa o edificio, hasta las directrices de seguridad de un país entero. La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad.

Figura N°1. **Políticas de Seguridad**
Fuente: Recuperado de
http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

Definición de Política

Según Herrera (2009), en su Ensayo Filosófico de justificación de la Praxis Política, manifiesta que la política podría ser entendida como la actividad de quienes procuran obtener el poder, retenerlo o ejercitarlo con vistas a un fin que se vincula al bien o con el interés de la generalidad o pueblo.

Proviene del latín politĭcus, que significa «de, para o relacionado con los ciudadanos», es el proceso de tomar decisiones que se aplican a todos los

miembros de un grupo. Según la RAE, la política es el arte, doctrina u opinión referente al gobierno de los Estados.

La política es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos. También puede definirse como una manera de ejercer el poder con la intención de resolver o minimizar el choque entre los intereses encontrados que se producen dentro de una sociedad. La utilización del término ganó popularidad en el siglo V a.c., cuando Aristóteles desarrolló su obra titulada justamente "Política".

Las políticas pueden considerarse como un conjunto de leyes obligatorias propias de una organización, y son dirigidas a un público mayor que las normas pues las políticas proporcionan las instrucciones generales, mientras que las normas indican requisitos técnicos específicos. Las normas, por ejemplo, definirían la cantidad de bits de la llave secreta que se requieren en un algoritmo de cifrado. Por otro lado, las políticas simplemente definirían la necesidad de utilizar un proceso de cifrado autorizado cuando se envíe información confidencial a través de redes públicas, tales como Internet.

Objetivo de una Política de Seguridad

El objetivo de una política de seguridad informática es la de implantar una serie de leyes, normas, estándares y prácticas que garanticen la seguridad, confidencialidad y disponibilidad de la información, y a su vez puedan ser entendidas y ejecutadas por todos aquellos miembros de la organización a las que van dirigidos.

Beneficios de las Política de Seguridad

Las políticas de seguridad informática muchas veces ayudan a tomar decisiones sobre otros tipos de política (propiedad intelectual, destrucción de la información, etc.). También son útiles al tomas decisiones sobre adquisiciones porque algunos equipos o programas no serán aceptables en términos de las políticas mientras que otras la sustentaran.

Las políticas de seguridad informática deben considerarse como un documento de largo plazo, que evolucionan. No contienen asuntos específicos de implementación, pero si asuntos específicos del equipo de cómputo y telecomunicaciones de la organización. Probablemente serán la guía para el diseño de cambios a esos sistemas. El desarrollo e implantación de políticas de seguridad informática es una indicación de que una organización está bien administrada y los auditores lo toman en cuenta en sus evaluaciones. (Beneficios de Politicas de Seguridad)

Principios Fundamentales de las Políticas de Seguridad

Son las ideas principales a partir de las cuales son diseñadas las políticas de seguridad. Los principios fundamentales son: responsabilidad individual, autorización, mínimo privilegio, separación de obligaciones, auditoría y redundancia.

- **Responsabilidad individual**

  Este principio dice que cada elemento humano dentro de la organización es responsable de cada uno de sus actos, aun si tiene o no conciencia de las consecuencias.

- **Autorización**

  Son las reglas explícitas acerca de quién y de qué manera puede utilizar los recursos.

- **Mínimo Privilegio**

  Este principio indica que cada miembro debe estar autorizado a utilizar únicamente los recursos necesarios para llevar a cabo su trabajo. Además de ser una medida de seguridad, también facilita el soporte y mantenimiento de los sistemas.

- **Separación de Obligaciones**

  Las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. Este principio junto con el de mínimo privilegio reducen la posibilidad de ataques a la seguridad, pues los usuarios sólo pueden hacer uso de los recursos relacionados con sus actividades, además de que facilita el monitoreo y vigilancia de usuarios, permitiendo registrar y examinar sus acciones.

- **Auditoría**

  Todas las actividades, sus resultados, gente involucrada en ellos y los recursos requeridos, deben ser monitoreados desde el inicio y hasta después de ser terminado el proceso. Además, es importante considerar que una auditoría informática busca verificar que las actividades que se realizan, así como las herramientas instaladas y su configuración son acordes al esquema de seguridad informática realizado y si éste es conveniente a la seguridad requerida por la empresa

- **Redundancia**

Trata entre otros aspectos sobre las copias de seguridad de la información, las cuales deben ser creadas múltiples veces en lapsos de tiempos frecuentes y almacenados en lugares distintos. Sin embargo, la redundancia como su nombre lo indica, busca "duplicar" y en este sentido se puede decir que a través de los respaldos se duplica información, y lo mismo se puede realizar en diferentes aspectos, como por ejemplo: en cuanto a energía eléctrica, una planta de luz para garantizar que opere en casos de emergencia, servidores de datos que entren en operación cuando el primario sufra una avería, etcétera, de manera tal que la redundancia se considera en aquellos casos o servicios que se vuelven imprescindibles para la empresa y que no pueden suprimirse pase lo que pase.

Figura N°2. **Múltiples Copias de Respaldo**

Fuente: Recuperado de
http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

1.4.2. Seguridad Informática

Según Aguilera (2010) manifiesta que la seguridad informática "Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable." (p.9)

Conjunto de medidas (administrativas, organizativas, físicas, técnicas legales y educativas) dirigidas a prevenir, detectar y responder a las acciones que pongan en riesgo la integridad, confidencialidad y disponibilidad, de la informatización que se procesa, intercambie, reproduzca o conserve a través de las tecnologías de la información.

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Según Canal (2006), la definición de seguridad informática se resume en cinco aspectos que se deben garantizar. Estos son:

- **Confidencialidad:** Consiste en dar acceso a la información sólo a los usuarios autorizados.
- **Control de Accesos:** Consiste en controlar el acceso a recursos de usuario autorizados.
- **Disponibilidad:** Consiste en la posibilidad de acceder a la información o a utilizar un servicio siempre que se necesite.
- **No Repudio:** consiste en la imposibilidad de negar la autoría de un mensaje o información del que alguien es autor.
- **Integridad:** consiste en garantizar que una información o mensaje no han sido manipulados.

Importancia de la Seguridad

El autor Mediavilla (1998) menciona que**:** La seguridad hoy en día es uno de los principales problemas encontrados en el área informática,

cuando se habla de seguridad por lo general se piensa en un término privacidad de la información en el cual se pueden incluir aspectos tales como: contraseñas, accesos a la información, mensajes cifrados y en definitiva, todo lo relacionado con la protección y confiabilidad de los datos. Indica que también se tienen que considerar otros aspectos como son: "la privacidad, la integridad y disponibilidad" (p.15)

Funciones de la Seguridad Informática

Para Mediavilla (1998) Dentro de las funciones que se refieren a la seguridad informática tenemos:

- Planear y establecer estrategias de seguridad informática de acuerdo a lineamientos principios y necesidades institucionales.
- Contar con un sistema de información estadístico para dar seguimiento a los proyectos y planes de acción con el fin de garantizar dentro de la institución su implantación control y seguimiento.
- Definir, elaborar, liberar, difundir y actualizar políticas y normas de seguridad informática que permitan a las áreas de la organización implantar y fortalecer mecanismos de protección de la información.
- Realizar campañas de capacitación, Difusión y concientización que eleven el nivel de recepción, entendimiento y conocimiento del personal en general sobre la materia
- Realizar diagnósticos y evaluaciones de seguridad informática para identificar y minimizar los riesgos en los diferentes niveles funcionales, operativos y de sistema.

- Mantener la actualización sobre los avances tecnológicos en este campo, con el fin fortalecer esquemas de protección en la organización. (p.102, 103).

Tipos de Seguridad

Según Aguilera (2010) menciona dos tipos de seguridad:

- **Activa**

  Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema. Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes.

- **Pasiva**

  Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos. (p.10)

Propiedades de un Sistema de Información Seguro

Según Aguilera (2010) señala que los daños producidos por falta de seguridad pueden causar pérdidas económicas o de credibilidad y prestigio a una organización.

Su origen puede ser:

- **Fortuito.** Errores cometidos accidentalmente por los usuarios, accidentes, cortes de fluido eléctrico, averías del sistema, catástrofes naturales…
- **Fraudulento.** Daños causados por software malicioso, intrusos o por la mala voluntad de algún miembro del personal con acceso al sistema, robo o accidentes provocados.

Se considera seguro un sistema que cumple con las propiedades de integridad, confidencialidad y disponibilidad de la información. Cada una de estas propiedades conlleva la implantación de determinados servicios y mecanismos de seguridad que se estudiarán más adelante.

Integridad

Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que esta se solicita, o dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado. Para evitar este tipo de riesgos se debe dotar al sistema de mecanismos que prevengan y detecten cuándo se produce un fallo de integridad y que puedan tratar y resolver los errores que se han descubierto.

Confidencialidad

La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus Directrices para la Seguridad de los Sistemas de Información define la confidencialidad como «el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada». Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema: quién

puede acceder, a qué parte del sistema, en qué momento y para realizar qué tipo de operaciones.

Disponibilidad

La información ha de estar disponible para los usuarios autorizados cuando la necesiten. Se deben aplicar medidas que protejan la información, así como crear copias de seguridad y mecanismos para restaurar los datos que accidental o intencionadamente se hubiesen dañado o destruido. (p.10 - 11).

La inversión en seguridad informática es un reto para los encargados de este tema en las organizaciones. Surgen preguntas alrededor del tema de presupuesto, impacto y retorno de la inversión que en la actualidad causan revuelo y establecen muchos interrogantes para aquellos que se haya en la tarea de justificar presupuestos de seguridad informática. (p.86). (Marco teorico s,f)

Servicios de Seguridad

Aguilera (2010) menciona los siguientes servicios de seguridad:

- **Integridad**

  Asegura que los datos del sistema no han sido alterados ni cancelados por personas o entidades no autorizadas y que el contenido de los mensajes recibidos es el correcto.

- **Confidencialidad**

  Proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

- **Disponibilidad**

  Permitirá que la información esté disponible cuando lo requieran las entidades autorizadas.

- **Autenticación (o identificación)**

  El sistema debe ser capaz de verificar que un usuario identificado que accede a un sistema o que genera una determinada información es quien dice ser. Solo cuando un usuario o entidad ha sido autenticado, podrá tener autorización de acceso. Se puede exigir autenticación en la entidad de origen de la información, en la de destino o en ambas.

- **No repudio (o irrenunciabilidad)**

  Proporcionará al sistema una serie de evidencias irrefutables de la autoría de un hecho. El no repudio consiste en no poder negar haber emitido una información que sí se emitió y en no poder negar su recepción cuando sí ha sido recibida.

  De esto se deduce que el no repudio puede darse:

  - **En origen.** El emisor no puede negar el envío porque el receptor tiene pruebas certificadas del envío y de la identidad del emisor. Las pruebas son emitidas por el propio emisor.
  - **En destino.** En este caso es el destinatario quien no puede negar haber recibido el envío ya que el emisor tiene pruebas infalsificables del envío y de la identidad del destinatario. Es el receptor quien crea las pruebas.

- **Control de acceso**

  Podrán acceder a los recursos del sistema solamente el personal y usuarios con autorización. (p.18)

Mecanismos de Seguridad

Aguilera (2010) manifiesta que según la función que desempeñen los mecanismos de seguridad pueden clasificarse en:

- **Preventivos:** Actúan antes de que se produzca un ataque. Su misión es evitarlo.
- **Detectores:** Actúan cuando el ataque se ha producido y antes de que cause daños en el sistema.
- **Correctores:** Actúan después de que haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño.

La elección de mecanismos de seguridad depende de cada sistema de información, de su función, de las posibilidades económicas de la organización y de cuáles sean los riesgos a los que esté expuesto el sistema. (p.7)

Enfoque Global de la Seguridad

Aguilera (2010) manifiesta que la información es el núcleo de todo sistema de información. Para proteger sus propiedades de integridad, disponibilidad y confidencialidad es necesario tener en cuenta a los niveles que la rodean para dotarlos de mecanismos y servicios de seguridad.

Desde el exterior hasta llegar a la información, se pueden definir estos niveles:

- La ubicación física. Edificio, planta o habitaciones, por ser el lugar físico en donde se encuentran ubicados los demás niveles.
- El sistema operativo y todo el software, porque gestiona la información.

- La conexión a internet, por ser la vía de contacto entre el sistema de información y el exterior.
- El hardware y los componentes de la red que se encuentran en el interior del entorno físico, porque contienen, soportan y distribuyen la información.
- La información.

Observa la figura siguiente para comprobar que la conexión a internet atraviesa los distintos niveles hasta llegar a la información: En el edificio habrá antenas, cableado en los muros, etc. Entre el hardware contamos con routers, switches, ordenadores, servidores, periféricos, etc. El sistema operativo y el software gestionan los accesos a internet. La información es el bien preciado que no se debe descuidar, pues desde internet solamente se podrá acceder a una parte de ella y siempre que los usuarios tengan autorización. Una vez más aludimos al personal de la empresa que puede actuar en todos los niveles o en parte de ellos y por lo tanto es un factor a tener en cuenta. (p. 20)

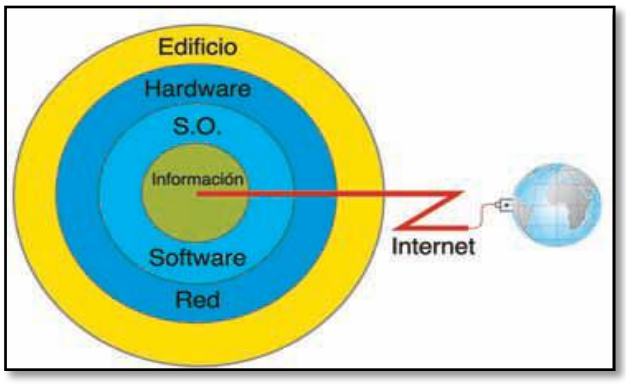

Figura N°3. **Enfoque Global de la Seguridad**

Fuente: Tomado de "Seguridad Informática".
Autor Aguilera López, Purificación

1.5. Hipótesis

En vista de que la investigación tiene un alcance de carácter descriptivo, no es posible plantear una hipótesis debido a que no se intenta correlacionar o explicar causalidad de variables. Por tanto la hipótesis es Implícita.

1.6. Objetivos

1.6.1. Objetivo General

Establecer políticas de seguridad informática para el manejo de información de la Distribuidora Almapo S.R.L. Huacho, a través de la Norma ISO/IEC 27001:2013.

1.6.2. Objetivos Específicos

- Conocer la situación actual en la que se encuentra el manejo de información de la Distribuidora Almapo S.R.L. Huacho, 2016.
- Aplicar la Norma ISO/IEC 27001:2013 para identificar las incidencias de seguridad informática en el manejo de información de la Distribuidora Almapo S.R.L. Huacho, 2016.
- Determinar las políticas de seguridad informática que permitan el manejo adecuado de información de la Distribuidora Almapo S.R.L. Huacho, 2016.

METODOLOGÍA DE TRABAJO

2.1. Tipo y Nivel de Investigación

El tipo de investigación que se realizó es aplicada, porque se caracteriza por su interés en la aplicación, utilización y consecuencias prácticas de los conocimientos, según Zorrilla (1993), y el nivel de investigación es descriptivo, el cual permite observar y describir en todos sus componentes, una realidad; que en este caso es las diferentes incidencias encontradas en el manejo de información de la Distribuidora Almapo S.R.L. Huacho.

2.2. Diseño de Investigación

El diseño de la investigación es no experimental, de carácter descriptivo y de corte transversal. Es no experimental porque trata de observar las características de los hechos, en los cuales no se interviene o manipula deliberadamente los fenómenos de estudio. Es de corte transversal porque se analiza en un periodo de tiempo determinado, en un solo momento.

2.3. Población y Muestra

2.3.1. Población

La población está conformada por 32 colaboradores, distribuidos en las diferentes áreas de: Administración, Almacén, Cómputo, Reparto - Transporte y Ventas, los cuales se detalla a continuación:

Tabla N° 1. **Personal de la empresa por áreas**

ÁREA	CARGO	CANTIDAD
Administración	Administradora	1
Almacén	Encargado de Álmacen	1
	Asistente de Álmacen	1
	Auxiliar de Álmacen	2

Cómputo	Encargado de Cómputo	1
	Asistente de Cómputo	1
	Auxiliar de Cómputo	1
Reparto - Transporte	Encargado de Reparto	1
	Asistente de Reparto	2
	Liquidador	3
	Chofer	4
Ventas	Encargado de Ventas	1
	Supervisor de Ventas	1
	Auxiliar de Ventas	2
	Vendedores Mercado	5
	Vendedores Cobranzas	5
TOTAL		**32**

Fuente: Elaboración Propia

2.3.2. Muestra

La muestra es equivalente a la población.

2.4. Técnicas e Instrumentos de Investigación

Las técnicas e instrumentos de recolección de datos que se utilizaron para el presente proyecto de investigación fueron:

Tabla N° 2. **Técnicas e Instrumentos de Investigación**

TÉCNICAS	INSTRUMENTOS
Observación	Visitas Presenciales a la empresa
Entrevista	Entrevista a la administradora de la empresa
Encuestas	Guía de encuesta dirigida a los colaboradores

Fuente: Elaboración Propia

Se utilizaron fuentes bibliográficas, fuentes con referencias web, libros, textos, revistas, páginas web, artículos online, informes de trabajos, así como también la Norma ISO/IEC 27001:2013, el cual fue de mucha ayuda para nuestra investigación. Se construyeron entrevistas y encuestas, el cual se obtuvo información certera y directa en cuanto a los objetivos específicos planteados del trabajo de investigación. La entrevista y las encuestas se detallan en los anexos.

2.5. Procesamiento y Análisis de la Información

En cuanto al análisis de la información se realizó el levantamiento, clasificación y verificación de la información, tanto en lo observado, como en las encuestas y cuestionario dirigidos a los colaboradores. Para el procesamiento de la información se utilizó el software Microsoft Excel 2010, que es una herramienta ofimática, el cual ayudó en el análisis, tabulación y gráficos de la información, para así obtener los resultados.

2.6. Norma ISO/IEC 27001:2013

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 el 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. (Aspectos Básicos ISO 27001)

ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. La

aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización. (ISO 27001 SGSI)

ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI). (Wikipedia s,f)

Estructura de la norma ISO 27001

- **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. (ISO 27001 SGSI)

Anexo A de la Norma ISO/IEC 27001:2013

El Anexo A de la Norma ISO 27001 es probablemente el anexo más famoso de todas las normas ISO y es porque provee una herramienta esencial para la gestión de la seguridad: una lista de los controles (o medidas) de seguridad que pueden ser usados para mejorar la seguridad de la información. Aquí se describe cada una de las 14 secciones del anexo A:

- **A.5 Políticas de seguridad de la Información** – controles acerca de cómo deben ser escritas y revisadas las políticas.
- **A.6 Organización de la seguridad de la información** – controles acerca de cómo se asignan las responsabilidades; también incluye los controles para los dispositivos móviles y el teletrabajo.
- **A.7 Seguridad de los Recursos Humanos** – controles antes, durante y después de emplear.
- **A.8 Gestión de recursos** – controles acerca de lo relacionado con el inventario de recursos y su uso aceptable, también la clasificación de la información y la gestión de los medios de almacenamiento.
- **A.9 Control de Acceso** – controles para las políticas de control de acceso, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones, y responsabilidades del usuario
- **A.10 Criptografía** – controles relacionados con la gestión de encripción y claves.
- **A.11 Seguridad física y ambiental** – controles que definen áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipos, descarte seguro, políticas de escritorio y pantalla despejadas, etc.

- **A.12 Seguridad Operacional** – muchos de los controles relacionados con la gestión de la producción en TI: gestión de cambios, gestión de capacidad, malware, respaldo, bitácoras, espejos, instalación, vulnerabilidades, etc.
- **A.13 Seguridad de las Comunicaciones** – controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc.
- **A.14 Adquisición, desarrollo y mantenimiento de Sistemas** – controles que definen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte.
- **A.15 Relaciones con los proveedores** – controles acerca de qué incluir en los contratos, y cómo hacer el seguimiento a los proveedores
- **A.16 Gestión de Incidentes en Seguridad de la Información** – controles para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta, y recolección de evidencias.
- **A.17 Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio** – controles que requieren la planificación de la continuidad del negocio, procedimientos, verificación y revisión, y redundancia de TI.
- **A.18 Cumplimiento** – controles que requieren la identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales, y revisiones de la seguridad de la información.

Uno de los grandes mitos acerca de ISO 27001 es que está enfocada en la TI, como se puede ver en las secciones mostradas, esto no es totalmente cierto: no se puede negar que la TI es importante, pero la TI por sí sola no puede proteger la información. La seguridad física, la protección legal, la gestión de recursos humanos, los aspectos organizacionales y todos ellos juntos son requeridos para

asegurar la información. La mejor manera de entender el Anexo A es pensar que es un catálogo de controles de seguridad del que se puede seleccionar los que apliquen a su compañía. (Anexo A Norma ISO 27001:2013)

NTP-ISO/IEC 27001:2014

La presente Norma Técnica peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el sistema 1 o de adopción, durante los meses de abril junio del 2014, utilizando como antecedente a la norma ISO/IEC 27001:2013. No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la información. Requisitos, 2da Edición, el 01 de diciembre del 2014. Esta Norma Técnica Peruana reemplaza a la NTP-ISO/IEC 27001:2008 y es una adopción de la Norma ISO/IEC 27001:2013.

Según la publicación del Diario El Peruano, el día 8 de enero del 2016 con Resolución Ministerial N° 004-2016-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática. Asimismo se ordena la publicación de la misma en el Portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y en el Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) (www.ongei.gob.pe) el mismo día de la publicación de la presente resolución en el Diario Oficial El Peruano. Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2 Edición"; podrán realizar dicha certificación de forma opcional y con recursos propios de cada entidad. (Diario El Peruano)

RESULTADOS

3.1. Resultados de Encuestas

A continuación se muestra gráficamente los resultados de algunas preguntas de la encuesta realizada a los colaboradores:

1. ¿Tiene conocimiento si hay manuales o procedimientos en la empresa aprobados por la gerencia?

Tabla N°3. **Resultados en Porcentaje – Pregunta 1**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	4	13
No	17	53
No Sabe / No Opina	11	34
TOTAL	**32**	**100**

Fuente: Elaboración Propia

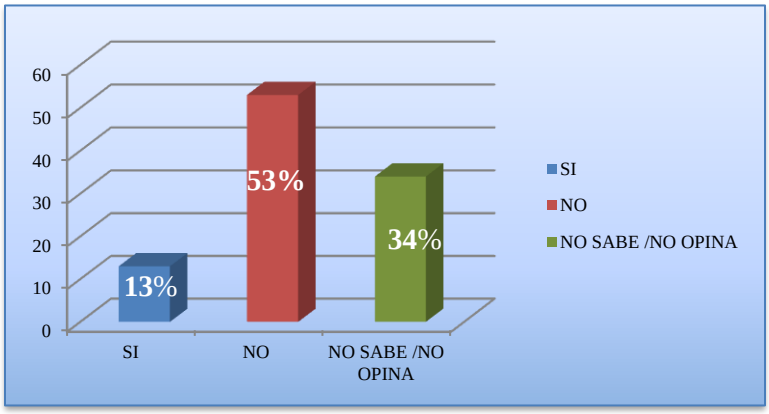

Figura N°4. **Resultados en Barras – Pregunta 1**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 3 y la Figura Nº 4 se observa, que el 13% de colaboradores si tiene conocimiento, asi mismo el 53% de colaboradores indica que no tiene conocimiento alguno, mientras que el 34% de colaboradores

no sabe/ no opina si hay manuales en la empresa. Como se ve la mayoría de los colaboradores desconoce totalmente que haya manuales o procedimientos en la empresa, aprobados por la gerencia.

2. ¿El área donde labora, cuenta con procedimientos, manuales o instructivos establecidos para el manejo de información del sistema?

Tabla N°4. **Resultados en Porcentaje – Pregunta 2**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	2	7
No	19	59
No Sabe / No Opina	11	34
TOTAL	**32**	**100**

Fuente: Elaboración Propia

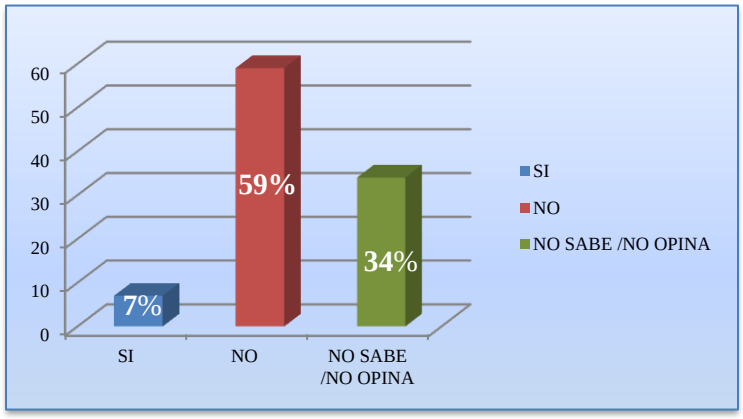

Figura N°5. **Resultados en Barras – Pregunta 2**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 4 y la Figura Nº 5 se observa, que el 7% de colaboradores indica que si hay procedimientos, asi mismo el 59% de colaboradores dice que no hay procedimientos, mientras que el 34% de colaboradores no sabe/ no opina si hay procedimiento alguno. Como se aprecia

la mayoría de los colaboradores afirma que no hay procedimientos establecidos para el manejo de la información en el área que laboran.

3. ¿Existe algún manual de contingencia elaborado y aprobado por la empresa?

Tabla N°5. **Resultados en Porcentaje – Pregunta 3**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	1	3
No	18	56
No Sabe / No Opina	13	41
TOTAL	**32**	**100**

Fuente: Elaboración Propia

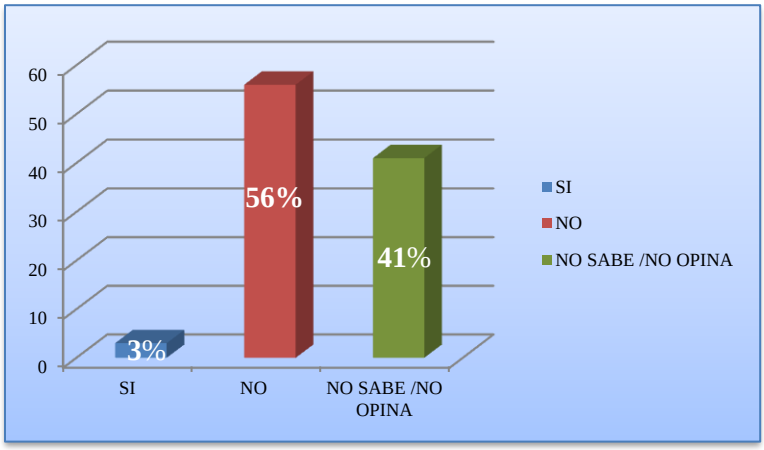

Figura N°6. **Resultados en Barras – Pregunta 3**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 5 y la Figura Nº 6 se observa, que el 3% de colaboradores indica que si hay manual de contingencia, asi mismo el 56% de colaboradores dice que no hay manual alguno, mientras que el 41% de colaboradores no sabe/ no opina si hay manuales de contingencia. Por tanto se puede ver que la mayor parte de los colaboradores señala que no hay manuales de contingencia elaborado y aprobado por la empresa.

4. ¿Se ha implementado alguna política de seguridad para la protección y seguridad de la información?

Tabla N°6. **Resultados en Porcentaje – Pregunta 4**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	3	9
No	20	63
No Sabe / No Opina	9	28
TOTAL	**32**	**100**

Fuente: Elaboración Propia

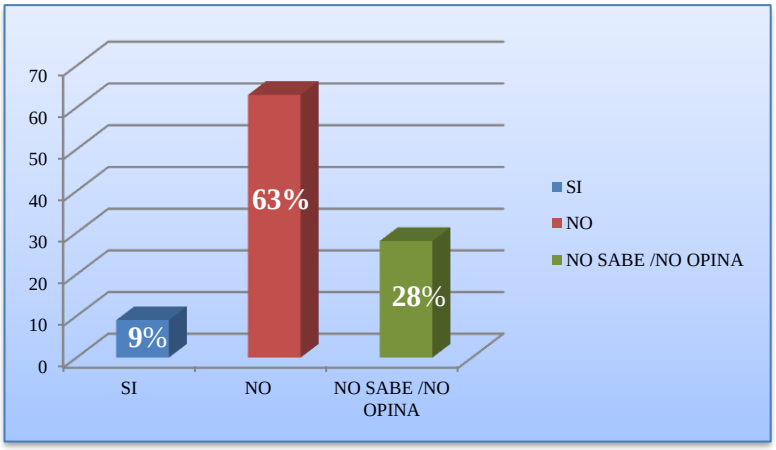

Figura N°7. **Resultados en Barras – Pregunta 4**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 6 y la Figura Nº 7 se observa, que el 9% de colaboradores señala que se ha implementado alguna política de seguridad, el 63% de colaboradores menciona que no hay ninguna implementación de políticas, mientras que el 28% de colaboradores indica que no sabe/ no opina si hay políticas de seguridad implementadas. Por tanto se puede ver que la mayoría de colaboradores señala que no hay políticas de seguridad implementadas para la protección y seguridad de la información.

5. ¿Sabe Usted si la empresa se rige por alguna norma o estándar de calidad para la protección de la información?

Tabla N°7. **Resultados en Porcentaje – Pregunta 5**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	0	0
No	24	75
No Sabe / No Opina	8	25
TOTAL	**32**	**100**

Fuente: Elaboración Propia

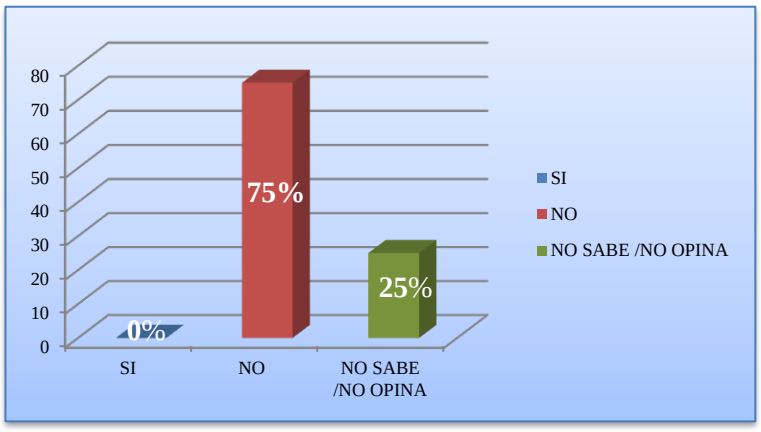

Figura N°8. **Resultados en Barras – Pregunta 5**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 7 y la Figura Nº 8 se observa, que el 75% de colaboradores indica que no sabe si la empresa se rige por normas, mientras que el 25% de colaboradores no sabe/ no opina si la empresa se rige por alguna de ellas. Por lo cual se puede observar que la mayoría de colaboradores señala que no sabe si la empresa se basa en alguna norma o estándar de calidad para la protección de la información.

6. ¿Conoce si en la empresa hay algún encargado sobre la seguridad informática?

Tabla N°8. **Resultados en Porcentaje – Pregunta 6**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	0	0
No	13	41
No Sabe / No Opina	19	59
TOTAL	**32**	**100**

Fuente: Elaboración Propia

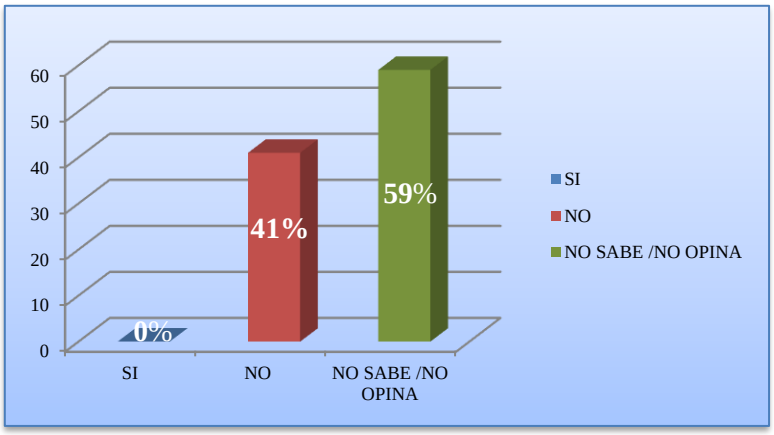

Figura N°9. **Resultados en Barras– Pregunta 6**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 8 y la Figura Nº 9 se observa, que el 41% de colaboradores dice que no hay ningún encargado, mientras que el 59% de colaboradores no sabe / no opina si hay algún encargado. Como se puede ver la mayor parte de los colaboradores afirma que no sabe si hay algún encargado acerca de la seguridad informática en la empresa.

7. ¿Posee Ud. algún conocimiento acerca de la seguridad informática?

***Tabla N° 9*. Resultados en Porcentaje – Pregunta 7**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	6	19
No	26	81
TOTAL	**32**	**100**

Fuente: Elaboración Propia

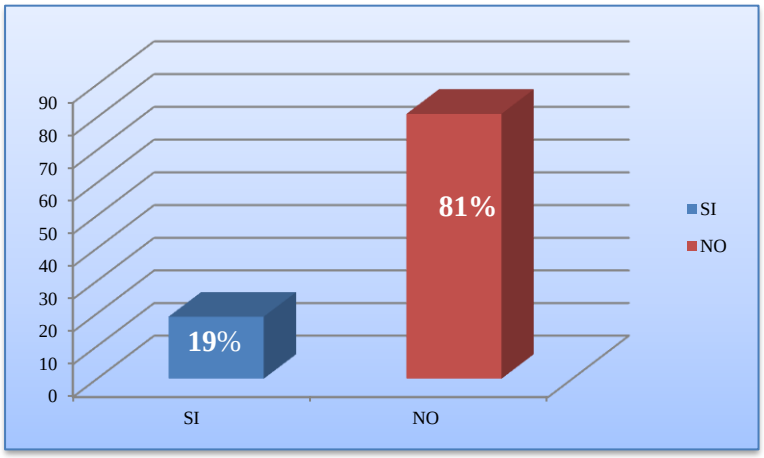

***Figura N°10.* Resultados en Barras – Pregunta 7**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 9 y la Figura Nº 10 se observa, que el 19% de colaboradores indica que si posee conocimiento de seguridad informatica, mientras que el 81% de colaboradores no posee conocimiento en seguridad informática. Como se puede ver la mayoría de colaboradores señala que no posee conocimiento alguno acerca de la seguridad informática, es por eso que ante cualquier incidente no saben como poder resolverlo.

8. ¿Con que frecuencia se presentan dificultades o inconvenientes en el sistema?

Tabla N° 10. **Resultados en Porcentaje – Pregunta 8**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Siempre	19	59
Algunas Veces	10	32
Nunca	3	9
TOTAL	**32**	**100**

Fuente: Elaboración Propia

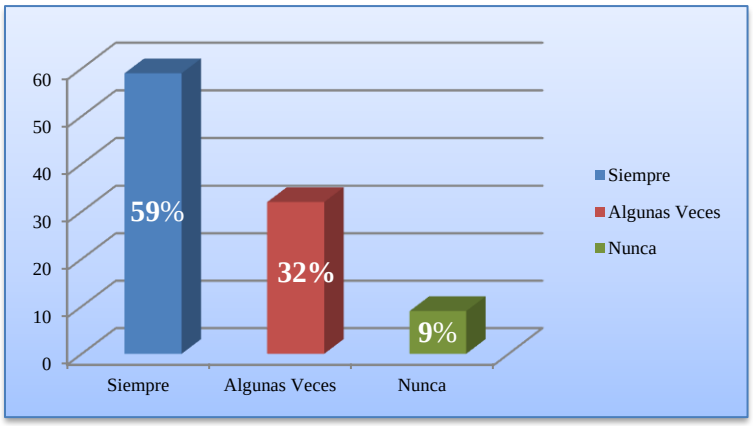

Figura N°11. **Resultados en Barras – Pregunta 8**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 10 y la Figura Nº 11 se observa, que el 59% de colaboradores dice que siempre hay inconvenientes con el sistema, asimismo el 32% de colaboradores indica que solo algunas veces hay inconvenientes, mientras que el 9% de colaboradores indica que nunca se presenta dificultades en el sistema. Como se puede observar la mayoría de los colaboradores afirma que siempre hay inconvenientes o dificultades con el sistema, es por eso que la información no se tiene a tiempo.

9. ¿En cuánto tiempo se resuelve las dificultades presentadas en el sistema?

Tabla N° 11. **Resultados en Porcentaje – Pregunta 9**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Enseguida	4	12
Se espera un poco	8	25
Se demora	20	63
TOTAL	**32**	**100**

Fuente: Elaboración Propia

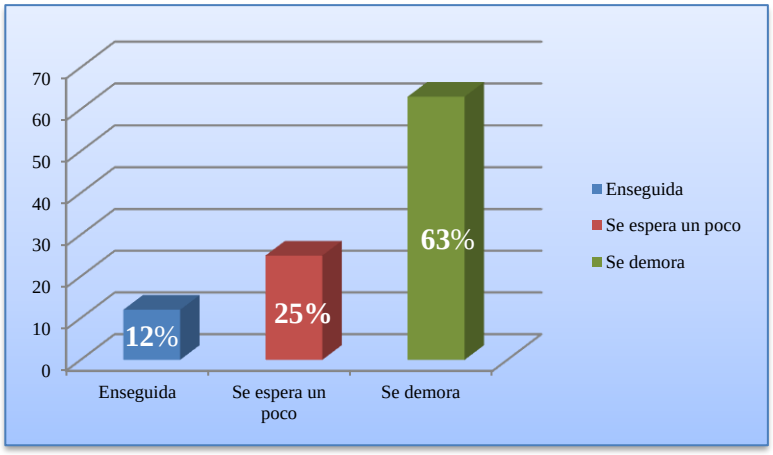

Figura N°12. **Resultados en Barras – Pregunta 9**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 11 y la Figura Nº 12 se observa, que el 12% de colaboradores dice que se resuelve enseguida las dificultades, asimismo el 25% de colaboradores indica que se espera un poco, mientras que el 63% de colaboradores señala que se demoran en solucionarlo. Como se puede observar la mayoría de los colaboradores señala que se demoran para solucionar las dificultades o inconvenientes que se presentan en el sistema.

10. ¿La información que facilita el sistema de almacén es?

Tabla N° 12. **Resultados en Porcentaje – Pregunta 10**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Adecuada	17	53
Correcta	12	38
Confiable	3	9
TOTAL	**32**	**100**

Fuente: Elaboración Propia

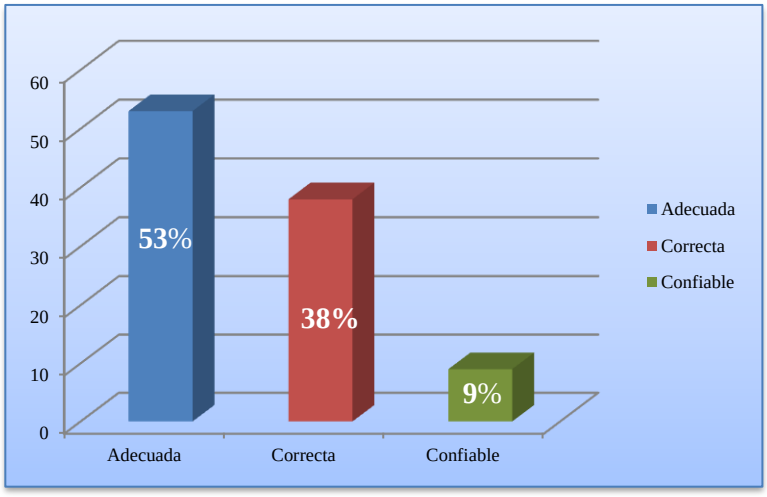

Figura N°13. **Resultados en Barras – Pregunta 10**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 12 y la Figura Nº 13 se observa, que el 53% de colaboradores dice que la información que facilita es adecuada, asimismo el 38% de colaboradores indica que la información es correcta mientras el 9% señala que la información no es tan confiable. Como se puede observar los colaboradores señalan que la información que facilita el sistema es la adecuada, pero a la vez no es tan confiable, ya que se encuentra a disposición de cualquier persona o usuario.

11. ¿El manejo del sistema de almacén es?

Tabla N° 13. **Resultados en Porcentaje – Pregunta 11**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Fácil	16	50
Más o menos	11	34
Difícil	5	16
TOTAL	**32**	**100**

Fuente: Elaboración Propia

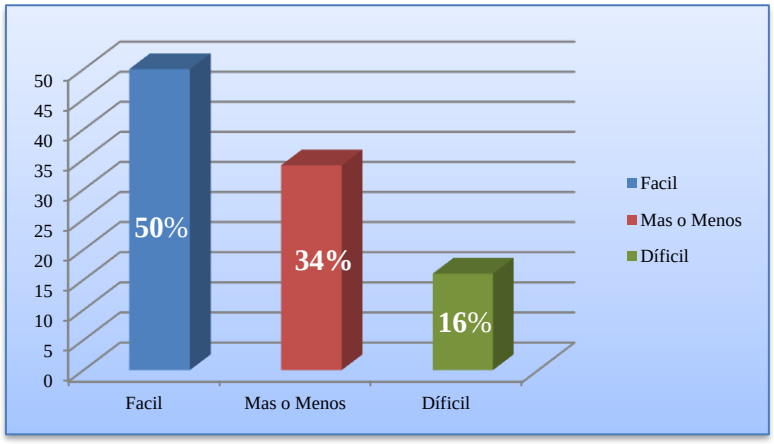

Figura N°14. **Resultados en Barras – Pregunta 11**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 13 y la Figura Nº 14 se observa, que el 50% de colaboradores dice que es fácil de utilizar, asimismo el 34% de colaboradores indica que es más o menos el manejo del sistema, mientras que el 16% de colaboradores indica que es difícil. Como se puede observar la mayoría de los colaboradores señala que el manejo del sistema es fácil de utilizar y un cierto porcentaje indica que no es tan fácil de utilizar por lo cual es necesario realizar capacitaciones constantes.

12. ¿El acceso a la información en el sistema de almacén es?

Tabla N° 14. **Resultados en Porcentaje – Pregunta 12**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Limitado	5	16
En algunos casos	9	28
Libremente accedida	18	56
TOTAL	**32**	**100**

Fuente: Elaboración Propia

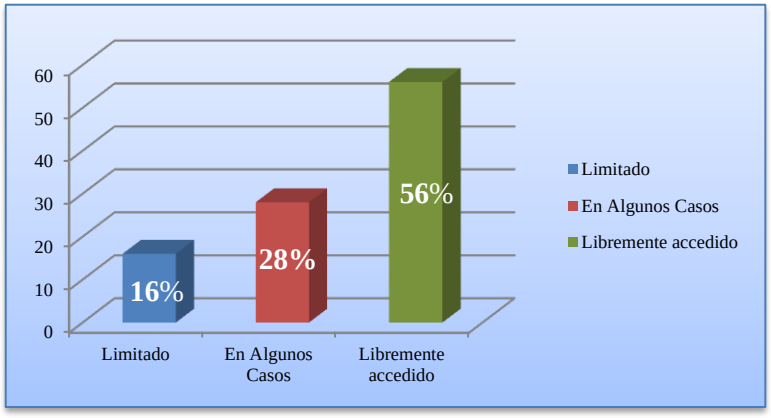

Figura N°15. **Resultados en Barras – Pregunta 12**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 14 y la Figura Nº 15 se observa, que el 16% de colaboradores dice que el acceso de información es limitada, asimismo el 28% de colaboradores indica que solo es en algunos casos, mientras que el 56% de colaboradores indica que es libremente accedida. Como se puede ver gráficamente la mayoría de los colaboradores afirma que la información es libremente accedida y disponible a cualquier colaborador, por ende esto provocaría alguna vulnerabilidad o manejo en la información.

13. ¿Se realizan copias de seguridad sobre la información de la empresa?

Tabla N° 15: **Resultados en Porcentaje – Pregunta 13**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	0	0
No	21	66
No Sabe / No Opina	11	34
TOTAL	**32**	**100**

Fuente: Elaboración Propia

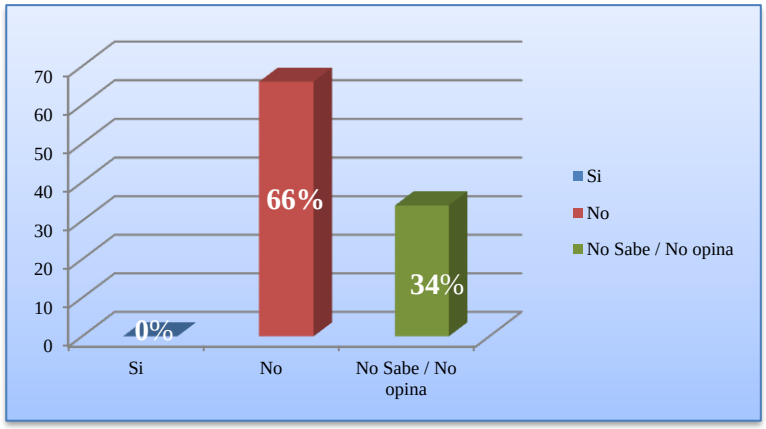

Figura N°16: **Resultados en Barras – Pregunta 13**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 15 y la Figura Nº 16 se observa, que el 66% de colaboradores indica que no se realizan ninguna copia de seguridad acerca de la información, mientras que el 34% de colaboradores señala que no sabe si se realiza copias de seguridad diariamente. Como se puede ver la mayoría de los colaboradores afirma que no se realiza copias de seguridad de información en la empresa.

14. ¿Usted cierra sesión de su computadora, cuando no está trabajando en ella?

Tabla N° 16. **Resultados en Porcentaje – Pregunta 14**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	7	22
No	25	78
TOTAL	**32**	**100**

Fuente: Elaboración Propia

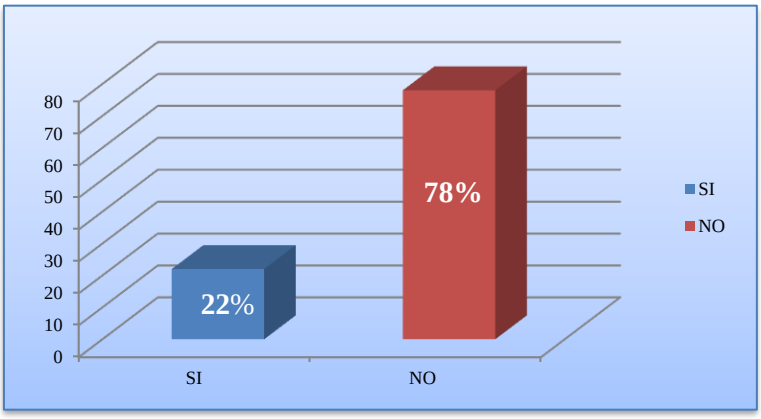

Figura N°17. **Resultados en Barras – Pregunta 14**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 16 y la Figura Nº 17 se observa, que el 22% de colaboradores dice que cierra sesión en su computadora, mientras que el 78% de colaboradores indica que efectivamente no cierra sesión de su computadora, cuando terminan de trabajar en ella. Como se puede observar en su mayoría, los colaboradores señalan que cuando se termina de trabajar no cierran sesión de su computadora, quedando la información a disponibilidad de cualquier persona o usuario.

15. En el tiempo que labora ¿Usted ha recibido alguna capacitación acerca de la seguridad informática y de los sistemas que se maneja en la empresa?

Tabla N° 17. **Resultados en Porcentaje – Pregunta 15**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	5	16
No	27	84
TOTAL	**32**	**100**

Fuente: Elaboración Propia

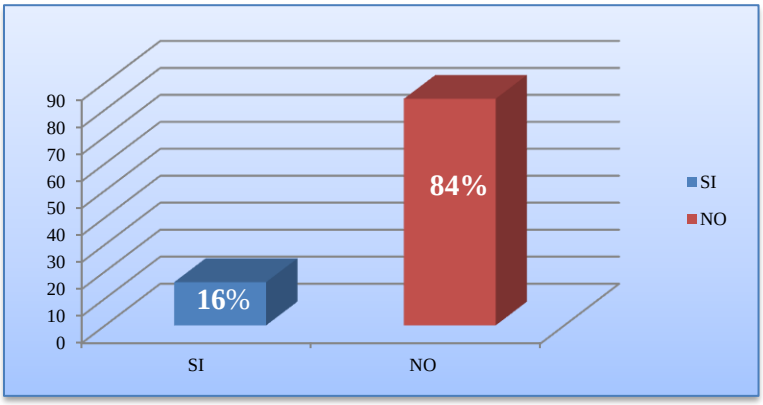

Figura N°18: **Resultados en Barras – Pregunta 15**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 17 y la Figura Nº 18 se observa, que el 16% de colaboradores indica que han recibido capacitaciones acerca de la seguridad informática, mientras el 84% de colaboradores indica que tal capacitación no la tuvieron. Como se puede apreciar, la empresa no realiza ninguna capacitación es por eso que los colaboradores no poseen conocimiento y menos concientización en referencia al uso de la información.

16. ¿Se realizan mantenimiento a las computadoras y sistemas de información?

Tabla N° 18. **Resultados en Porcentaje – Pregunta 16**

DETALLE	COLABORADORES (N°)	PORCENTAJE (%)
Si	2	6
No	12	38
No Sabe / No Opina	18	56
TOTAL	**32**	**100**

Fuente: Elaboración Propia

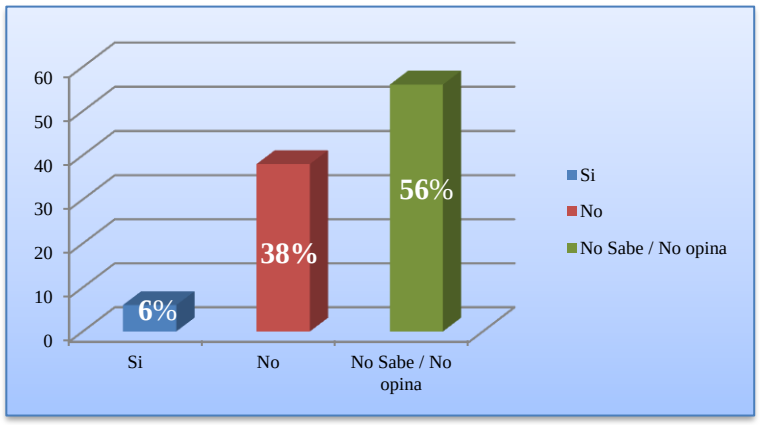

Figura N°19. **Resultados en Barras – Pregunta 16**
Fuente: Elaboración Propia

INTERPRETACIÓN: En la Tabla N° 18 y la Figura Nº 19 se observa, que el 6% de colaboradores señala que se realiza mantenimiento a los equipos, el 38% de colaboradores indica que no se realiza mantenimiento ni a los equipos ni a los sistemas, mientras el 56% de colaboradores no sabe si realiza mantenimiento a los equipos. Por ende, como se puede observar no se tiene en constante mantenimiento los equipos ni los sistemas, ocasionando pérdidas de información e incluso daños en los propios equipos.

3.2. Desarrollo de la Norma ISO/IEC 27001:2013

3.2.1. Etapa de Planificación

3.2.1.1. Descripción de la empresa

Distribuidora Almacenes Populares S.R.LTDA., con nombre comercial Almapo S.R.L. es una empresa peruana del sector económico, reconocida en el mercado, caracterizada por la excelencia en el servicio, que inició sus actividades el 01/01/1989, dedicados al rubro de la venta y distribución de productos en consumo masivo: abarrotes, golosinas, bebidas, etc. Somos competitivos, exitosos, innovadores y con calidad humana, trabajamos unidos como un equipo comprometido para mantener y reforzar este liderazgo.

***Tabla N°19*. Ficha Informativa Almapo S.R.L.**

Razón Social	Almacenes Populares S.R.Ltda.
Nombre Comercial	ALMAPO S.R.L.
Tipo de Empresa	Soc.com.respons. Ltda.
Registro Único de Contribuyente (RUC)	20132345237
Estado	Activo
Inicio de Actividades	01/01/1989
Actividad De Comercio Exterior	Sin Actividad
Actividad Principal	Venta Al Por Mayor De Alimentos, Bebidas Y Tabaco
Dirección Principal Sede Central	Mza. B1 lote. 13 ex. Fundo Larrea (costado de Nicovita - Fabrica Coca Cola) – La Libertad / Trujillo / Moche
Teléfono(s)	200459 - 205635 - 246056 - 607325 – 607326
Correo Electrónico	@almapo.com
Página Web	http://www.almapo.com

Fuente: Recuperado de https://compuempresa.com/info/ almacenes-populares-srltda-20132345237

Registrada en la SUNAT con Ruc número 20132345237, encontrándose como estado de contribuyente Activo y de condición Habido. También se encuentra empadronada en el Registro Nacional de Proveedores.

Tabla N°20. **Códigos Registro Nacional de Proveedores**

CÓDIGO	CAPÍTULO	VIGENCIA	ESTADO
B0033720	Proveedor De Bienes	08/11/2015 - 08/11/2016	Vigente
S0437061	Proveedor De Servicios	08/11/2015 - 08/11/2016	Vigente

Fuente: Recuperado de https://compuempresa.com/info/almacenes-populares-srltda-20132345237

Historia

En el año 1980 el Sr. Bernabé Anticona inició su comercio de abarrotes abriendo una tienda en Otuzco, le fue tan bien que abrió dos tiendas más, lo que le caracterizaba de sus tiendas era, que eran muy grandes y parecían almacenes, fue allí cuando se le ocurrió llamarlas Almacenes Populares. En 1989, los hijos de Bernabé Anticona llevaron a Almacenes Populares a Trujillo y abrieron su primera tienda fue allí cuando vieron q había un buen mercado y pensaron en crear una empresa que la llamaron Almapo S.R.L.

Esta empresa se creó con la finalidad de dedicarse a la compra y venta de golosinas y abarrotes al por mayor y menor a través de sus diferentes locales comerciales. Tiempo más adelante y frente a la difícil situación económica existente, Almapo S.R.L., decide incursionar en el servicio de atención al punto de venta de sus clientes con la finalidad de obtener un medio efectivo para incrementar los niveles de venta de los productos que expandía.

Luego de comprobar la efectividad de este sistema de distribución surge la iniciativa de buscar empresas que comulguen con esta nueva política de ventas para distribución de sus productos, es asi como Almapo S.R.L. obtiene la distribución de productos P&G, Nestlé, Sayón, Clorox, Global Alimentos, etc., marcas que cuentan con un gran respaldo financiero y que brindan a nuestra empresa un importante apoyo profesional y especializado. La empresa Almapo S.R.L. cuenta con más de 26 años de experiencia en el sistema de distribución y venta a nivel horizontal y vertical de productos de consumo masivo.

Misión: *"Ser tu satisfacción"*

Ser la mejor alternativa peruana en satisfacer las necesidades de nuestros clientes, promoviendo el consumo de nuestros productos, basados en la excelencia de los mismos, logrando a la vez solidez de la empresa y el bienestar de sus integrantes.

Visión: *"Ser los mejores"*

Estar en la mente de cada cliente que necesite de nuestros productos y servicios.

Valores

- Calidad De Trabajo
- Respeto
- Responsabilidad
- Vocación De Servicio
- Solidaridad

Esto significa Almapo S.R.L.:

- Para nuestros Clientes: La fuente de abastecimiento más confiable para poder competir en sus respectivos mercados.
- Para nuestros Proveedores: La distribución de sus productos al costo más bajo, en un número elevado de puntos de venta en nuestro territorio.

Almapo S.R.L. al paso del tiempo quiere ser una organización líder a nivel nacional e internacional en distribución, con un portafolio diversificado de productos y marcas de excelente calidad, optimizando e innovando procesos con tecnología de punta, capaz de adaptarse a los cambios para satisfacer de manera oportuna las necesidades de nuestros clientes.

Figura N°20. **ALMAPO S.R.L. Sede Central**
Fuente: Recuperado de http://www.almapo.com

Marcas con las que trabaja ALMAPO S.R.L.

- **Procter & Gamble – P&G**

- **Nestlé Perú SA:**

- **Clorox Perú SA:**

- **Global Alimentos SA:**

Figura N°21. **Marcas de Productos de ALMAPO S.R.L.**
Fuente: Recuperado de http://www.almapo.com

Sucursales / Oficinas

Hasta la fecha Almapo S.R.L. es una de las empresas distribuidoras más nombradas en Trujillo y al norte del Perú, tiene sucursales desde Huacho hasta Piura y aún siguen creciendo. Consta de 9 sucursales a nivel nacional.

- **Sede:** TARAPOTO
  Dirección: Car.Chontamuyo Km 13.5 San Martin - La Banda.
  Teléfono: 976394455
  Email: tarapoto@almapo.com

- **Sede:** CHICLAYO
  Dirección: Car.Chacupe 1 Int 17 Fundo La Linea - Chacupe
  Teléfono: 074-612718
  Email: chiclayo@almapo.com

- **Sede**: CHIMBOTE
  Dirección: Jr. Callao # 475 - AH Miraflores - I Zona - Santa
  Teléfono: 043-350638
  Email: chimbote@almapo.com

- **Sede:** HUACHO
  Dirección: Calle. Juan Velazco Alvarado # 786 - Cruz Blanca
  Teléfono: 01-2327648
  Email: huacho@almapo.com

- **Sede:** HUAMACHUCO

  Dirección: Jr. Bolívar # 1132 - Pueblo Huamachuco

  Teléfono: 94949494

  Email: huamachuco@almapo.com

- **Sede**: JAEN

  Dirección: Jr. Pakamuros # 497 - Cercado

  Teléfono: 976394494

  Email: jaen@almapo.com

- **Sede:** MOYOBAMBA

  Dirección: Jr.20 de Abril Mza C Lte 13 San Martin

  Teléfono: 042-509769

  Email: moyobamba@almapo.com

- **Sede:** CAJAMARCA

  Dirección: Jr. Juan Beato Macías # 1093 - Cercado

  Teléfono: 076-607521

  Email: cajamarca@almapo.com

- **Sede:** CHEPÉN

  Dirección: Calle Trujillo # 913 – Chepén

  Teléfono: 94949494

  Email: chepen@almapo.com

3.2.1.2. Situación Actual de la Empresa

La sucursal analizada para esta investigación es Huacho, el cual dentro de esta sucursal se identificó las vulnerabilidades que afectan la empresa, asimismo también conocer el grado de sensibilización y concientización por parte de los colaboradores, en cuanto a la seguridad y manejo de información. La empresa cuenta con las siguientes áreas: Administración, Almacén, Cómputo, Reparto – Transporte y Ventas.

El área de almacén es considerada soporte fundamental de la empresa, ya que es ahí donde se realiza las diferentes operaciones diarias en el sistema, para el proceso y almacenamiento de información tanto de los clientes como de los productos.

En la empresa se utiliza dos software: el Microsoft Office 2010 (Paquete completo) y Flex Bussiness Erp.

Al realizar las visitas a la empresa se pudo evidenciar que no cuentan con:

- Manual de organización y funciones
- Inventario de Software y Hardware actualizado.
- Relación de usuarios para las aplicaciones que poseen.
- Procedimientos o instructivos ante cualquier incidente.
- Políticas o reglamentos de seguridad para el manejo de la información.

Asimismo la empresa cuenta con los siguientes activos informáticos

Tabla N°21. **Lista de Activos Informáticos**

EQUIPOS	CANTIDAD
Computadoras de escritorio	12
Impresoras (multifuncional y matricial)	6
Modem router	3
Teléfono fijo (empresa)	2
Celulares	18

Fuente: Elaboración Propia

El análisis realizado al manejo de información en la empresa Distribuidora Almapo S.R.L. Huacho, muestra como resultado diferentes incidencias, el cual va en contra de los tres pilares fundamentales de la seguridad: confidencialidad, integridad y disponibilidad.

Según lo observado en las diferentes visitas a la empresa, de la misma forma en las respuestas obtenidas en la entrevista a la administradora y en las encuestas realizadas a los colaboradores de la sucursal el cual están incluidas en el anexo 1, se pudo conocer el estado actual con respecto al manejo de información que realizan los diferentes colaboradores. A continuación se muestra la lista de incidencias encontradas:

Tabla N°22. **Período de incidencia**

PERÍODO DE INCIDENCIA	DESCRIPCIÓN
La Mayoría de veces	Incidentes ocurridos regularmente
Frecuentemente	Incidentes ocurridos casi diariamente
Ocasionalmente	Incidentes ocurridos algunas veces
Casi Nunca	Incidentes ocurridos en un solo momento

Fuente: Elaboración propia

Tabla N°23. **Lista de incidencias encontradas**

N°	INCIDENCIAS ENCONTRADA	PERÍODO DE INCIDENCIA
01	La empresa no realiza capacitaciones constantes a los colaboradores acerca de la seguridad de información.	Frecuentemente
02	La lista de inventario no se encontró actualizada en la empresa.	Frecuentemente
03	Para la asignación de los activos informáticos no se encontró ningún formato donde se asignen los responsables para estos recursos.	Mayoría de veces
04	La información almacenada en un dispositivo es modificada o borrada sin ninguna autorización.	Mayoría de veces
05	La información que se procesa y se obtiene está disponible a todos los colaboradores.	Frecuentemente
06	No se da de baja los usuarios correspondientes a trabajadores que ya no pertenecen a la empresa.	Frecuentemente
07	No realizan copias de respaldo, mucho menos no tienen algún medio físico donde se almacene esta información	Mayoría de veces
08	Las áreas de la empresa son difíciles de ubicar, ya que no se encuentran correctamente señaladas.	Frecuentemente
09	No cuenta con señales de seguridad (prohibido fumar, acceso restringido, etc)	Mayoría de veces
10	Utilizan el internet de forma excesiva con fines extra laborales.	Frecuentemente
11	Las áreas no se encuentran correctamente acondicionadas, frente a alguna amenaza natural u otra incidencia.	Mayoría de veces
12	Los mobiliarios no son adecuados para los equipos y las instalaciones no cuentan con una correcta distribución.	Mayoría de veces
13	El corte de energía provoca que los colaboradores dejen de trabajar y no pueden terminar con sus labores.	Ocasionalmente
14	Los equipos utilizados fuera de la empresa no son devueltos en el tiempo establecido	Frecuentemente
15	En la mayoría de las áreas se encontró los escritorios llenos de papeles y documentación innecesaria.	Mayoría de veces
16	No se encontró un formato donde se registre las diferentes fallas o eventos que se producen en los equipos.	Frecuentemente

17	La información no está segmentada por niveles, por ende los colaboradores tienen acceso fácilmente a cualquier información, asi sea confidencial.	Mayoría de veces
18	Cuando ocurre algún suceso o incidencia referente a la información estos no son reportados a tiempo.	Frecuentemente

Fuente: Elaboración propia

3.2.2. Etapa de Ejecución

3.2.2.1. Evaluación de los Controles de seguridad Norma ISO/IEC 27001:2013

En la Tabla N° 25 se especifica las incidencias encontradas, evaluados bajo los controles de seguridad de la Norma ISO/IEC 27001:2013, asimismo se brinda las recomendaciones respectivas y se describe el nivel de importancia que tiene cada control de seguridad frente a las sucesos encontrados en la empresa, esto permitirá determinar políticas de seguridad informática.

Tabla N°24. **Nivel de Importancia**

NIVEL DE IMPORTANCIA	DESCRIPCIÓN
Alta	Son los controles de seguridad primordiales para la empresa.
Media	Son los controles de seguridad que van ayudar a fortalecer los de nivel de importancia Alta.

Fuente: Tomado de Bermúdez y Bailón (2015) – Modificado por el autor

Tabla N°25. **Cuadro de Incidencias y Recomendaciones**

CUADRO DE INCIDENCIAS Y RECOMENDACIONES					
OBJETIVOS DE CONTROL	**ÁREA RESPONSABLE**	**INCIDENCIA ENCONTRADA**	**RECOMENDACIONES**	**CONTROLES BASADO EN ISO/IEC 27001**	**IMPORTANCIA**
A.5. Políticas de Seguridad de la Información					
A.5.1 Dirección de la Gerencia para la Seguridad de la Información	Administración de la Sucursal.	No se halló ningún manual o instructivo de políticas de seguridad informática	Se debe elaborar un manual o instructivo de políticas de seguridad informática, alineados a las mejores prácticas de seguridad, que sean acordes a las necesidades de la empresa.	A.5.1.1 Políticas de Seguridad de la Información	Alta
			El manual o instructivo de las políticas de seguridad informatica deberá ser puesta en conocimiento a la Gerencia para su aprobación, una vez aprobado se tiene que hacer de conocimiento a todos los colaboradores de la empresa.	A.5.1.2 Revisión de las Políticas para la Seguridad de la Información	Medio
	Todas las áreas	Falta de procedimientos documentados	Es importante que dentro de las oficinas haya un manual donde indique todas las funciones que realizan los colaboradores de la empresa, y así se pueda verificar que se está realizando de forma correcta.	A.5.1.1 Políticas de Seguridad de la Información	Medio

A.6 Organización de la Seguridad de la Información					
A.6.1 Organización Interna	Administración, Recursos Humanos	No se encontró designado ninguna persona Responsable de la Seguridad Informática	Se debe asignar formalmente una persona Responsable, para que sea el encargado de definir y explicar claramente las actividades que se realizarán acerca de la seguridad informática en la empresa.	A.6.1.1 Roles y Responsabilidades para la seguridad de la información	Alta
	Gerencia General, Administración	No se encontró un Equipo de Trabajo que se reúna para tratar acerca de la Seguridad informática	Es importante que se conforme y se asigne un Equipo de Trabajo, para tratar temas sobre la seguridad informatica el cual permita mejorar el manejo de la información.	A.6.1.2 Segregación de Funciones	Alta
	Administración	No se da el apoyo de la administración de la sucursal en cuanto a establecer controles de seguridad	Se debe continuar con la comunicación y el compromiso constante entre la administradora y el gerente general, para que asi se ayude en mejorar la seguridad informatica.	A.6.1.3 Contacto con Autoridades	Alta
	Responsable de Seguridad informática	No hay relación con empresas que hayan afrontado la misma situación referente al tema de seguridad.	Se debe analizar e identificar las empresas que actualmente estén aplicando controles de seguridad, de tal manera que se pueda intercambiar experiencias y opiniones referentes al tema.	A.6.1.4 Contacto con grupos especiales de interés	Media

A.6.2 Dispositivos Móviles y teletrabajo	Administración de la Sucursal.	No se halló ninguna política de seguridad para el uso de dispositivos móviles.	Se recomienda no utilizar ningún dispositivo móvil, para evitar la reproducción de la información fuera de la empresa.	A.6.2.1. Política de Dispositivos Móviles	Alta
A.7 Seguridad de los Recursos Humanos					
A.7.1 Antes del empleo	Recursos Humanos	No se encontró una cláusula en el contrato referente a la seguridad de la información	Se recomienda que en los contratos deba de haber una cláusula que comprometa a los colaboradores a guardar la confidencialidad de la información de la empresa.	A.7.1.2. Términos y condiciones del empleo	Alta
A.7.2 Durante el empleo	Administración de la Sucursal.	No se encontró una adecuada capacitación a los colaboradores acerca de la seguridad de información	Todos los colaboradores deben conocer las políticas de seguridad informatica y no ser ajeno a ellos, concientizando y brindando capacitación constante, de tal manera que ellos vean cuales pueden ser las consecuencias.	A.7.2.2. Conciencia, educación y capacitación sobre seguridad de la información	Alta
	Recursos Humanos, Responsable de Seguridad Informática	No se encontró ningún instructivo o que indique las sanciones en caso de faltas cometidas en la seguridad de información.	Se recomienda que para estos casos, se debe elaborar un procedimiento estableciendo las sanciones que tendrá un colaborador en caso de realizar alguna falta en la seguridad de información	A.7.2.3. Proceso Disciplinario	Alta

A.7.3 Terminación y cambio de empleo	Recursos Humanos	No se encontró ningún formato donde indique que antes de terminar su contrato laboral, deben devolver los activos que se le dio al inicio.	Se debe elaborar un listado donde indique los activos que se le entrega al inicio de sus actividades y que al finalizar debe devolverlos tal y como se le entregaron	A.7.3.1. Terminación o cambio de responsabilidades del empleo	Media
A.8 Gestión de Activos					
A.8.1. Responsabilidad por los activos	Todas las áreas	No se encontró la lista de inventario actualizada de la empresa.	Se recomienda realizar mensualmente el inventario de los equipos y/o dispositivos que hay en las áreas.	A.8.1.1. Inventario de activos	Alta
	Todas las áreas	No se encontró ningún documento formal donde se asigne los responsables para los activos	Se recomienda que al realizar el inventario de los activos, se debe asignar formalmente a los responsables de los mismos por cada área, para que no haya ninguna confusión o pérdida de los mismos.	A.8.1.2. Propiedad de los activos	Alta
	Recursos Humanos	No se encontró ningún formato donde indique que los usuarios externos deben devolver los activos.	Se recomienda realizar un formato para que al término del trabajo los usuarios o clientes externos devuelvan los activos que se les prestó al inicio de sus actividades	A.8.1.4. Retorno de los activos	Media

A.8.2. Clasificación de la información	Administración de la Sucursal	No se encontró ningún documento establecido para la clasificación de la información.	Se debe elaborar un documento de clasificación de información en el cual se establezca que la información es de uso interno, confidencial y propio de la empresa.	A.8.2.1. Clasificación de la Información	Alta
	Administración de la Sucursal	No se encontró ningún documento definido para el etiquetado de la información.	Se debe elaborar un procedimiento para el etiquetado de la información, el cual vaya en concordancia con la empresa.	A.8.2.2. Etiquetado de la Información	Media
A.8.3. Manejo de los Medios	Administración de la Sucursal	La información almacenada en un dispositivo es modificada o borrada sin ningún autorización	Se recomienda que la información que esté almacenada en algún medio o dispositivo referente a la empresa no sea ni reproducida ni modificada ni borrada previa autorización.	A.8.3.1. Gestión de medios removibles A.8.3.2. Disposición de medios	Alta Media
A.9 Control de Acceso					
A.9.1. Requisitos de la empresa para el control de acceso	Cómputo	No se encontró ningún procedimiento o documento cerca de los controles de acceso	Se recomienda elaborar un procedimiento o documento acerca de los controles de acceso en el cual especifique las limitaciones para el uso de la información	A.9.1.1. Política de Control de acceso	Alta

A.9.1. Requisitos de la empresa para el control de acceso	Cómputo	Los usuarios tienen acceso a todos los servicios de red ya sea de trabajo u ocio.	Se recomienda que para evitar eso se debe administrar los servicios de red, permitiendo el acceso solo a sitios autorizados, referentes básicamente al trabajo	A.9.1.2. Acceso a redes y servicios de red	Media
A.9.2. Gestión de acceso de usuario	Administración de la Sucursal Cómputo	No se da de baja los usuarios correspondientes a trabajadores que ya no pertenecen a la empresa, lo siguen teniendo en el sistema	Se recomienda que tanto para el ingreso de un nuevo trabajador este sea registrado, como para el término de su contrato el usuario sea dado de baja totalmente para que así ya no tenga ningún acceso a la empresa	A.9.2.1. Registro y baja de usuarios	Alta
	Administración de la Sucursal Cómputo	La información está disponible a cualquier usuario, ya sea un colaborador o algún administrativo	Se recomienda que la información deba estar disponible para los diferentes cargos, ya que se maneja información confidencial y para eso tiene que haber controles de acceso siendo restringido y controlado para cada cargo.	A.9.2.3. Gestión de derechos de acceso privilegiados A.9.2.4. Gestión de información de autentificación secreta de usuarios	Alta Media
A.9.3. Responsabilidad de los usuarios	Administración de la Sucursal Cómputo	Los colaboradores no son responsables con la información que manejan a diario, ya que no desconocen si es confidencial o no	Se recomienda que los colaboradores sigan las instrucciones que ha dado la empresa con respecto al uso de la información.	A.9.3.1. Uso de Información de autentificación secreta	Alta

A.9.4. Control de acceso a sistema y aplicación	Todas las áreas Administración de la Sucursal	Los colaboradores ingresan a aplicaciones o programas que necesariamente no son del trabajo	Se recomienda que para estos casos haya un procedimiento el cual detalle las restricciones en el acceso a la información en el sistema y en las aplicaciones.	A.9.4.2. Procedimientos de ingreso seguro A.9.4.4. Uso de programas utilitarios privilegiados	Alta Media
A.10 Criptografía					
A.10.1. Controles Criptográficos	Administración de la Sucursal	Las claves o contraseñas no son cambiadas con frecuencia	Se recomienda realizar un instructivo referente a los controles criptográficos, y que a través de este se pueda gestionar de una mejor manera mejor las claves o contraseña para los sistemas.	A.10.1.1. Procedimientos de ingreso seguro A.10.1.2. Gestión de Claves	Alta Media
A.11 Seguridad Física y Ambiental					
A.11.1. Áreas Seguras	Administración de la Sucursal Todas las áreas	Las áreas no están debidamente protegidas, esto ocasiona que cualquier tipo de información esté disponible a los colaboradores	Se recomienda que para proteger las áreas deben realizarse procedimientos el cual permita solo el acceso de la información a personal autorizado. Asimismo colocar señales de seguridad como área restringida, solo personal autorizado, etc, dentro y fuera de cada área.	A.11.1.1. Perímetro de seguridad física A.11.1.2. Control de ingreso físico	Alta Media
	Todas las áreas	Resulta confuso identificar cada área de la empresa	Se recomienda colocar señales el cual identifique a cada área permitiendo a los colaboradores saber dónde se encuentra cada área.	A.11.1.3. Asegurar oficinas, áreas e instalaciones	Alta

A.11.1. Áreas Seguras	Administración de la Sucursal	Algunas veces las cámaras no funcionan, eso perjudica al control diario de la empresa	Se recomienda que la empresa debe monitorear las entradas y salidas del personal, ya sea externo o interno	A.11.1.1. Perímetro de seguridad física	Alta
	Administración de la Sucursal	Los mobiliarios no son adecuados para los equipos, las instalaciones no tienen un diseño adecuado	Se recomienda comprar mobiliarios adecuados para los equipos , tener instalaciones adecuadas contando con señales de seguridad, para proteger de todo tipo de amenazas naturales o externas	A.11.1.4. Protección contra amenazas externas y ambientales	Alta
	Administración de la Sucursal	No se encontró ningún procedimiento referente a las áreas seguras	Se recomienda elaborar un procedimiento o instructivo referente a las áreas seguras y al mantenimiento de los equipos, para que esto ayude a mejorar a la empresa.	A.11.1.1. Perímetro de seguridad física A.11.1.5. Trabajo en áreas seguras A.11.2.1. Emplazamiento y protección de los equipos	Alta Alta Alta
A.11.2. Equipos	Administración de la Sucursal	Los equipos no están debidamente protegidos contra alguna amenaza ambiental; asimismo el mantenimiento de los mismos no suelen realizarlo.	Se recomienda que los equipos deben estar ubicados correctamente y protegidos frente a cualquier amenaza ambiental. El mantenimiento de los equipos debe realizarse cada 3 meses para que esto garantize la disponibilidad e integridad de la información	A.11.2.1. Emplazamiento y protección de los equipos A.11.2.4. Mantenimiento de equipos	Alta Alta

A.11.2. Equipos	Administración de la Sucursal	El corte de energía provoca que los colaboradores dejen de trabajar y no pueden terminar con sus labores.	Para eso se recomienda utilizar un UPS o alimentador de suministro de energía el cual permita que estos cortes de energía se puedan restablecer con el UPS.	A.11.2.2. Servicios de suministro	Alta
	Administración de la Sucursal	Los equipos utilizados fuera de la empresa no son devueltos en el tiempo establecido	Se recomienda que se debe tener un formato para registrar todos los equipos que van a ser utilizados fuera de la empresa, el cual especifique el tiempo de devolución y la condición del equipo. Si es posible realizar no dejar que los equipos salgan de la empresa solo en casos extremos.	A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	Media
	Administración de la Sucursal	En la mayoría de las áreas se encontró los escritorios llenos de papeles y documentación innecesaria.	Se recomienda que los colaboradores no dejen ningún archivo en el escritorio, que esté totalmente limpio; asimismo también la pantalla de la computadora.	A.11.2.9. Política de escritorio limpio y pantalla limpia	Media
A.12 Seguridad de las Operaciones					
A.12.1. Procedimientos y responsabilidad operativas	Cómputo	No se encontró ningún formato referente a copias de respaldo	Se recomienda elaborar y aplicar un formato para el registro de las copias de respaldo que deben ser diariamente para proteger la información de manera íntegra sin alteraciones o daños.	A.12.1.1. Procedimientos operativos documentados	Alta

A.12.2. Protección contra códigos maliciosos	Cómputo	No se encontró ningún control para proteger la información en contra de códigos maliciosos	Se recomienda monitorear los equipos con frecuencia actualizándose el antivirus y concientizando al personal a no descargar información desconocido para evitar peligro y así esta no pueda sufrir daños.	A.12.2.1. Controles contra códigos maliciosos	Media
A.12.3. Respaldo	Cómputo	No realizan copias de respaldo, mucho menos no tienen algún medio físico donde se almacene esta información	Para eso se recomienda se recomienda realizar diariamente copias de respaldo de la información guardándolas en medio físico, permitiendo salvaguardar la información y restablecerla de nuevo.	A.12.3.1. Respaldo de la información	Alta
A.12.4. Registro y Monitoreo	Cómputo	No se encontró un formato donde se registre las diferentes fallas o eventos que se producen en las computadoras	Se recomienda que para estos casos se deba tener un formato el cual se registre diariamente los eventos o fallas que se han presentado en todo el día, y así poder monitorear y resolver las diferentes incidencias.	A.12.4.1. Registro de eventos	Media
	Cómputo	La información consignada en los registros están libremente a sufrir modificaciones y acceder sin ninguna autorización	Se recomienda que la información deba ser manejada en niveles, para así tener un mejor control en cuanto a la integridad y disponibilidad de la misma.	A.12.4.2. Protección de información de registros	Media

A.13 Seguridad de las Comunicaciones					
A.13.1. Gestión de seguridad de la red	Cómputo	La empresa no cuenta con un control para las redes, el cual permita proteger la información	Se recomienda realizar un instructivo en el cual se detalle que las redes deben ser monitoreadas y controladas para el mejor uso de los datos y así poder guardar su confidencialidad.	A.13.1.1. Controles de red	Alta
A.13.2. Transferencia de Información	Cómputo	No se encontró ningún instructivo o procedimiento acerca de la transferencia de la información a empresas externas	Se recomienda que en el instructivo se incorpore sobre el uso de servicios de red; asimismo establecer acuerdos de confidencialidad y no reproducción de la información con empres externas.	A.13.2.1. Políticas y procedimientos de transferencia de la información A.13.2.4. Acuerdos de confidencialidad o no divulgación	Alta Media
A.15 Relaciones con los Proveedores					
A.15.1. Seguridad de la Información en las relaciones con los proveedores	Administración de la Sucursal	No se encontró algún instructivo para el acceso de los activos a los proveedores.	Se recomienda realizar un procedimiento donde se indique que activos pueden ser utilizados por los proveedores, dentro y fuera de la empresa.	A.15.1.1. Políticas y procedimientos de transferencia de la información A.15.1.2. Abordar la seguridad dentro de los acuerdos con proveedores	Alta Media
A.16 Gestión de Incidentes de Seguridad de la Información					
A.16.1. Gestión de incidentes de seguridad de la información y mejoras	Cómputo	No se tiene un instructivo para el manejo de incidentes	Se recomienda que se deba realizar un instructivo para los incidentes, el cual indique las acciones que se debe tomar para estos casos.	A.16.1.1. Responsabilidades y procedimientos	Alta

A.16.1. Gestión de incidentes de seguridad de la información y mejoras	Cómputo	Cuando ocurre algún suceso en la seguridad de la información estos no son reportados	Se recomienda que para estos sucesos los incidentes deban reportarse y a la vez registrarse en un formato, indicando a detalle el incidente ocurrido, para así poder tomar medidas respectivas, de tal forma que no vuelvan a ocurrir estos sucesos.	A.16.1.2. Reporte de eventos de seguridad de la información. A.16.1.3. Reporte de debilidades de seguridad de la información. A.16.1.6. Aprendizaje de los incidentes de seguridad de la información.	Alta Alta Media
	Cómputo	Cuando se presenta un incidente se demoran en poder resolverlo.	Se recomienda que los incidentes presentados se han resueltos de manera oportuna y sean resultados de acuerdo las políticas establecidas.	A.16.1.5. Respuesta a incidentes de seguridad de la información	Alta
A.17 Aspectos de Seguridad de la Información en la Gestión de continuidad del Negocio					
A.17.1. Continuidad de seguridad de la información	Administración de la Sucursal Cómputo	La empresa no cuenta con procedimientos o instructivos acerca de la seguridad de la información	Es importante que la empresa realize procedimientos o instructivos referente a la seguridad de la información, el cual ayude en caso de daños, modificaciones, alteraciones, acceso no autorizado, información alojado en los sistemas del negocio entre otros, de tal manera que no peligre la continuidad del negocio.	A.17.1.1. Planificación de continuidad de seguridad de la información A.17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información	Alta Alta

A.18 Cumplimiento					
A.18.1. Cumplimiento con requisitos legales y contractuales	Administración de la Sucursal Cómputo	No cuentan con normas de seguridad establecidas que eviten la modificación, reproducción y alteración de la información de la empresa el cual no tiene derecho de autor.	Se recomienda establecer políticas y controles de seguridad que permitan evitar el incumplimiento de las leyes del estado sobre el derecho de propiedad intelectual Asimismo se debe cumplir con las políticas de seguridad y los diferentes estándares de calidad para el mejor desempeño de la empresa.	A.18.1.1. Identificación de requisitos contractuales y de legislación aplicables A.18.1.2. Derechos de propiedad intelectual	Alta Alta
A.18.2. Revisiones de seguridad de la información	Administración de la Sucursal	No se realiza seguimiento al manejo de información que posee cada colaborador, por ende se desconoce si cumplen con las medidas respectivas	La administración de la empresa debe monitorear, revisar y cotejar regularmente el manejo de la información con las políticas de seguridad, para verificar si los colaboradores lo están empleando.	A.18.2.2. Cumplimiento de políticas y normas de seguridad	Alta

Fuente: Tomado de Bermúdez y Bailón (2015) – Modificado por el autor

3.2.3. Etapa de Finalización

3.2.3.1. Determinar Políticas de Seguridad

POLÍTICAS DE SEGURIDAD INFORMÁTICA - DISTRIBUIDORA ALMAPO S.R.L. HUACHO

Las políticas de seguridad que se muestran a continuación, están basados en el análisis actual de la empresa, alineado a la Norma ISO/IEC 27001:2013. Estas políticas permiten asegurar el uso y manejo adecuado de la información, ayudando en la continuidad del negocio.

A Nivel Organizacional

- La empresa debe poner en conocimiento de la alta Gerencia los manuales o instructivos que se van a crear a corto plazo de acuerdo a las necesidades de la empresa y así puedan ser aprobados rápidamente para difundirse a todos los colaboradores.
- Se debe elaborar un manual de funciones y responsabilidades a corto plazo donde especifique a los colaboradores que tareas deben realizar.
- Cada área debe tener un procedimiento acerca del manejo de información el cual señale que hacer ante alguna incidencia.
- La empresa debe contar con un colaborador responsable de la seguridad informática, el cual debe estar atento ante cualquier cambio, para que así pueda realizar la actualización en los diferentes manuales o procedimientos.

- En las claúsulas de los contratos laborales deben incluirse un artículo referente a la confidencialidad de la información y las sanciones de las mismas; así mismo crear un formato donde el colaborador se comprometa a esto.
- Al término del contrato laboral se debe crear un formato en el cual detalle todos los equipos informáticos y la devolución de la información que se le entregó al inicio de sus labores.
- La empresa debe comprometerse a realizar capacitaciones trimestralmente a sus colaboradores acerca de la seguridad de la información, para así lograr la concientización y sensibilización en cada uno de ellos.
- Se debe formar un equipo de trabajo para tratar temas de seguridad informática y así poder elaborar nuevos manuales o instructivos, según sus necesidades, para el mejor uso de la información.
- Las áreas deben contar con señalizaciones el cual permita a los colaboradores identificar cada área y asimismo colocar en toda la empresa señales de seguridad como: personal autorizado, área restringida, no fumar entre otros.
- La administración de la sucursal debe monitorear, revisar y cotejar frecuentemente el manejo de la información, para verificar si los colaboradores están correctamente su trabajo.
- Se recomienda que la empresa debe monitorear las entradas y salidas del personal, ya sea externo o interno, registrándolos en un formato respectivo.

- Se debe realizar anualmente una auditoria con referencia a la seguridad informática, ya que eso serviría de mucha ayuda para los colaboradores y para la administración de la sucursal, para así poder saber más fondo cuales son los riesgos y en que se tiene que mejorar en la empresa.
- Se debe mantener actualizado los diferentes procedimientos o instructivos de cada área, para que los colaboradores siempre estén atentos a cualquier eventualidad, cumpliendo de forma organizada y ordenada los procedimientos establecidos.

A Nivel de Software

- Los colaboradores deben cambiar de contraseña de sus diferentes aplicaciones cada 3 meses para evitar el hackeo de sus cuentas.
- No abrir archivos maliciosos, ni hacer clic en enlaces desconocidos, para así evitar problemas en la información y los equipos.
- No utilizar el internet con fines extra laborales, por ende la empresa debe bloquear ciertas páginas web, para así evitar la distracción de los colaboradores y el uso excesivo del internet.
- No descargar archivos como: música, películas u otros archivos no autorizados, el cual no son útiles para las colabores de la empresa.
- Se debe crear un procedimiento donde especifique las prohibiciones que se tienen que tomar en cuenta al momento de procesar o utilizar los sistemas, esto debe ser difundido y publicado en cada área de la empresa.

- La empresa debe realizar copias de respaldo diariamente, esta información debe guardar en un medio físico, para así salvaguardar la confidencialidad, disponibilidad e integridad de los datos.
- Se debe elaborar una lista con los diferentes usuarios que son aplicados en los sistemas, para así poder actualizar trimestralmente y poder eliminar los usuarios que ya no son utilizados.
- La empresa debe administrar de una forma ordenada los controles de acceso, según los niveles de información (confidencialidad); el cual permita clasificarla y etiquetarla dando la disponibilidad de la información según la necesidad delos colaboradores.
- El antivirus de las computadoras deben mantenerse actualizados, para eso se debe monitorear mensualmente, a fin de evitar alguna infiltración de virus en los equipos informáticos
- Se debe monitorear frecuentemente la información que están alojados en los sistemas de información, a fin de evitar daños en las mismas.

A Nivel de Hardware

- Se debe impedir que los colaboradores lleven algún dispositivo u otro equipo informático a la empresa para que no haya ninguna pérdida.

- Los colaboradores deben utilizar correctamente los equipos, manteniéndolos limpios, sin rayas en la pantalla, sin daños; para que así se mantenga en mejor estado.
- Debe realizarse mensualmente el inventario de los recursos informáticos, a fin de tener conocimiento del mismo.
- La empresa debe acondicionar correctamente cada área con señales de seguridad, distribuir los espacios adecuados, así mismo los equipos informáticos y los mobiliarios adecuados para cada uno de ellos, protegiéndolos frente a cualquier incidencia ambiental (polvo, humedad, entre otros).
- Para el corte de energía se debe tener como contingencia un UPS o suministro de energía ininterrumpida, para que así los colaboradores puedan realizar sus tareas sin inconveniente.
- Se debe programar mensualmente un día para el mantenimiento de los equipos informáticos, a fin de evitar daños en los mismos y en la información.
- Se recomienda elaborar un procedimiento o instructivo referente a las áreas seguras y al mantenimiento de los equipos.
- Los incidentes deben reportarse diariamente, resolviéndose de manera oportuna y a la vez registrándose en un formato indicando a detalle el incidente ocurrido, para así tomar las medidas respectivas, de tal forma que no vuelvan a ocurrir.
- Se debe contar con un plan de contingencia frente a desastres naturales, a fin de salvaguardar la información y los diferentes equipos informáticos.

ANÁLISIS Y DISCUSIÓN

En su investigación, Bermúdez y Bailón (2015), resaltan que el uso de controles de seguridad dentro de una empresa permite minimizar aquellas brechas de seguridad que dan paso a la corrupción de la información, por lo cual se está de acuerdo, ya que a través de la Norma ISO/IEC 27001 se tiene una mejor gestión de seguridad de la información, teniendo como objetivo disminuir los riesgos identificados, mediante controles y procedimientos ya establecidos.

Por otro lado, en su tesis Macen (2014), indica que las políticas de seguridad de información ayudan a resguardar las informaciones de las organizaciones, en este sentido se está de acuerdo, asimismo recomienda realizar la elaboración y construcción de un manual ajustado a la realidad de cada empresa, debiéndose evaluar el resultado y su constante actualización.

Por lo consiguiente, en su informe Galeano y Alzate (2013), precisa que la seguridad es muy importante para la evaluación y análisis de riesgos, por ende se plantea la propuesta de un protocolo de seguridad basado en la Norma ISO 27000 y 17000, que puede ser aplicado en las instituciones de educación superior, en tal sentido se está de acuerdo, ya que permitirá guiar y facilitar su implementación garantizando una disponibilidad, integridad y seguridad de la información en un porcentaje muy alto.

Al aplicar en la Distribuidora Almapo S.R.L. , las encuestas a los trabajadores de la empresa y la entrevista a la administradora de la sucursal, los resultados indicaron claramente en un gran porcentaje que tanto los colaboradores y la parte administrativa no consideran de alta importancia la seguridad informática, o no saben sobre el tema, al igual que la importancia que tiene el manejo de información, lo que claramente incrementan los riesgos y posibles amenazas ya estudiadas con anterioridad.

Asimismo se muestra que la empresa anteriormente mencionada, no hace de conocimiento, ni capacita a sus colaboradores por ende ellos son ajenos a este tema, pero esto puede ir mejorando tal como lo argumenta en su trabajo de investigación Henao y Ortiz (2010), que indica que proponer una política de seguridad informática requiere un alto compromiso por parte de la organización, para que se convierta en un proceso exitoso, por el cual se está de acuerdo, ya que el propósito de establecer políticas de seguridad, es para proteger la información y los activos de la organización, además de las responsabilidades que deben asumir todos y cada uno de los empleados mientras permanezcan en la entidad.

Por otra parte Alcántara (2015), señala que al incorporar la norma ISO/IEC 27001, se logra incrementar procedimientos, utilizados en favor de la empresa, en tal sentido, se está de acuerdo, ya que esto va permitir realizar diferentes instructivos o guías, para prevenir y tomar las precauciones necesarias de manera que se disminuya el impacto del incidente, por tanto el personal va estar más orientado y capacitado para realizar sus diferentes labores en la empresa.

Finalmente, Yan y Zavala (2013), indica que en los últimos años todo lo relacionado respecto a seguridad de la información y continuidad de procesos suscita un gran interés, es por ende que las diferentes empresas tanto estatales y privadas están más concientizadas de los riesgos que conlleva, por lo cual, se está de acuerdo, ya que la continuidad del negocio depende de la seguridad y del flujo ininterrumpido de dicha información, es por eso que gracias a los diferentes lineamientos como la Norma ISO/IEC 27001 u otros estándares de calidad, se puede salvaguardar mejor la información .

CONCLUSIONES

- Al analizar la situación actual se concluyó que la mayor incidencia es la falta de normas o políticas de seguridad para el manejo de la información de la Distribuidora Almapo S.R.L. Huacho.
- Se detectó que los colaboradores no tienen claro el concepto de seguridad informática, por consiguiente no lo aplican y por ende esto conlleva a que no dimensionen la importancia del tema y los problemas que pueden ocasionar en el manejo de la información.
- Se concluyó usar los controles de seguridad de la Norma ISO/IEC 27001:2013 como instrumento para identificar las incidencias en la seguridad informática que afectan el manejo de la información de la Distribuidora Almapo S.R.L. Huacho.
- Se determinó las políticas de seguridad informática para el manejo de información de la Distribuidora Almapo S.R.L. Huacho.

RECOMENDACIONES

- Realizar capacitaciones constantes a los colaboradores para que se socializen ampliamente con las políticas de seguridad informática para el manejo de información y no sea nada ajeno a ellos.
- Al evaluar las incidencias encontradas con los controles de seguridad de la Norma ISO/IEC 27001:2013, evidenciaron las deficiencias en el manejo de la información, por ende se recomienda que la empresa debe realizar mensualmente un plan estratégico, para así mantener la información segura.
- Se recomienda documentar y aprobar manuales de usuario, procedimientos o instructivos para las diferentes áreas, salvaguardando la información de las mismas y así poner en conocimiento a los colaboradores.
- Se recomienda usar las políticas de seguridad informática que se ha establecido a través de los controles de la Norma ISO/IEC 27001:2013, como una herramienta, a fin de poder enfrentar cualquier incidente referente al manejo de información de la Distribuidora Almapo S.R.L. Huacho.

AGRADECIMIENTO

En primer lugar agradezco a Dios por todo lo que me ha dado, por ayudarme a lograr cada uno de mis objetivos y por haberme permitido llegar a concluirlos.

A mis Padres y Hermanos, que son mi motivación día con día, quiénes me apoyaron incondicionalmente, que siempre creyeron en mí y que sin ellos nada de esto hubiese sido posible.

A la Universidad San Pedro, quién me acogió a lo largo de mi formación profesional y que me preparo para asumir los nuevos retos del mundo laboral.

A mis Docentes que con profesionalismo y dedicación me brindaron sus conocimientos y experiencias para ser mejores cada día y poder crecer tanto en lo profesional como personal, el cual me ayudó en el desarrollo de la presente tesis.

Finalmente agradecer a todas aquellas personas y amigos que de una u otra forma me ayudaron a lo largo del desarrollo de este proceso.

GONZALES QUINTEROS, YULEICY YAJAIRA

REFERENCIAS BIBLIOGRÁFICAS

Alcántara Flores, J. C. (2015). *Guía de Implementación de la Seguridad Basado en la Norma ISO/IEC 27001, Para Apoyar la Seguridad en los Sistemas Informáticos de la Comisaría del Norte P.N.P. en la Ciudad de Chiclayo.* Chiclayo - Perú: Recuperado de http://tesis.usat.edu.pe/jspui/bitstream/123456789/491/1/TL_Alcantara_Flores_JulioCesar.pdf.

Aguilera López, P. (2010). *Seguridad Informática.* Madrid, España: Editex SA.

Almapo. (s.f.). Recuperado el 25 de Noviembre de 2016, de Almapo: Recuperdo de www.almapo.com

Álvarez, G. , & Pérez, P. (2004). *Seguridad Informática para Empresas y Particulares.* Madrid,España: Mc Graw Hill.

Anexo A Norma ISO 27001:2013. (s.f.). Recuperado el 25 de Noviembre de 2016, de Anexo A Norma ISO 27001:2013: Recuperado de: https://advisera.com/27001academy/es/knowledgebase/resumen-del-anexo-a-de-la-norma-iso-270012013/

Aspectos Básicos ISO 27001 . (s.f.). Recuperado el 25 de Noviembre de 2016, de Aspectos Básicos ISO 27001 : Recuperado de: https://advisera.com/27001academy/es/que-es-iso-27001/

Aula uvs . (s.f.). Recuperado el 25 de Noviembre de 2016, de Aula uvs : Recuperado de http://www.aulauvs.sld.cu

Beneficios de Politicas de Seguridad. (s.f.). Recuperado el 25 de Noviembre de 2016, de Beneficios de Politicas de Seguridad: Recuperdo de: http://www.oas.org/juridico/pdfs/mesicic4_repdom_manTI.pdf

Bermúdez Molina, K. G., & Bailón Sánchez, E. R. (2015). *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.* Guayaquil - Ecuador: Recuperado de http://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf.

Canal, A. (2006). *Seguridad de la Información: Expectativas, riesgos y técnicas.* D.F, México: Limusa S.A de C.V.

Cano. (2011). Obtenido de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

Definición de Política . (s.f.). Recuperado el 25 de Noviembre de 2016, de Definición de Política : http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/PoliticasSeguridad.php

Diario El Peruano. (s.f.). Recuperado el 12 de Diciembre de 2016, de Diario el Peruno: Recuperado de: http://busquedas.elperuano.com.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/

Galeano Villa, J. L., & Alzate Castañeda, C. C. (2013). *Protocolo de Políticas de Seguridad Informática para las Universidades de Risaralda.* Pereira - Colombia: Recuperado de http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1731/CDMIST65.pdf?sequence=1.

Henao Acosta, C., & Ortiz Villegas, J. P. (2010). *Política de Seguridad Informática para Apostar S.A.* Pereira - Colombia: Recuperado de http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1503/CDMIST26.

Herrera, H. E. (2009). *¿ De qué hablamos cuando hablamos de Estado?* Santiago (Chile).

ISO 27001 SGSI . (s.f.). Recuperado el 25 de Noviembre de 2016, de ISO 27001 SGSI : Recuperado de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001

La importancia de contar con una Política de Seguridad en la empresa. (s.f.). Recuperado el 25 de Noviembre de 2016, de La importancia de contar con una Política de Seguridad en la empresa: Recuperado de http://www.protegetuinformacion.com/perfil_tema.php?id_perfil=7&id_tema=63

Macen Rojas, C. D. (2014). *Políticas de Seguridad de la Información: Realidad de la UTIC para la Construcción de Políticas de Seguridad de la Información.* Asunción - Paraguay: Recuperado de http://www.utic.edu.py/investigacion/attachments/article/118/TESIS.pdf.

Marco teorico s,f. (s.f.). Recuperado el 25 de Noviembre de 2016, de Marco teorico s,f: Recuperado de http://problema.blogcindario.com/2008/10/00014-marco-teorico.html

Mediavilla Mauriz, M. (1998). *Seguridad en Unix.* México D.F: México AlfaOmega.

Monografías. (s.f.). Recuperado el 25 de Noviembre de 2016, de Monografías : Recuperado de www.monografias.com/seguridadinformatica

Monografías s,f. (s.f.). Recuperado el 18 de Noviembre de 2016, de Monografías.com: http://www.monografias.com/trabajos22/auditoria-informatica/auditoria-informatica.shtml

Politica s,f. (s.f.). Recuperado el 26 de Noviembre de 2016, de Politica s,f: http://definicion.de/politica/

Politicas y Seguridad. (s.f.). Recuperado el 25 de Noviembre de 2016, de Politicas y Seguridad: Recuperdo de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

Seguridad Informática. (s.f.). Recuperado el 25 de Noviembre de 2016, de Seguridad Informática: Recuperado de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/PoliticasSeguridad.php

Seguridad Informática . (s.f.). Recuperado el 25 de Noviembre de 2016, de Seguridad Informática : Recuperado de www.wikipedia.com/seguridadinformatica

Universidad Nacional de Colombia. (2003). *Guía para elaboración de Políticas de Seguridad.* UNAL, Vicerrectoría General, Bogotá.

Wikipedia s,f. (s.f.). Recuperado el 18 de Noviembre de 2016, de Wikipedia: https://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

Wikipedia s,f. (s.f.). Recuperado el 25 de Noviembre de 2016, de Wikipedia s,f: Recuperado de https://es.wikipedia.org/wiki/ISO/IEC_27001

Wikipedia, Politica. (s.f.). Recuperado el 25 de Noviembre de 2016, de Wikipedia: https://es.wikipedia.org/wiki/Pol%C3%ADtica

Wikipedia, Poltica de Seguridad. (s.f.). Recuperado el 25 de Noviembre de 2016, de Wikipedia, Poltica de Seguridad: https://es.wikipedia.org/wiki/Pol%C3%ADtica_de_seguridad

Wood, C. C. (2002). *Políticas de Seguridad Informática Mejores Prácticas Internacionales.* . Houston, TX, USA: NetlQ, Inc.

Yan Carranza, F., & Zavala Vasquez, C. (2013). *Plan de Mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad Aplicando Lineamientos ISO 27001 y Buenas Prácticas COBIT*. Trujillo - Perú: Recuperado de http://repositorio.upao.edu.pe/bitstream/upaorep/645/1/YAN_FREDDY_MEJORA_SEGURIDAD_COBIT.pdf.

ANEXOS

ANEXO 01: Encuesta a los Colaboradores

ENCUESTA

El propósito de esta encuesta es conocer su opinión, por ende a continuación se le presenta un conjunto de preguntas, el cual debe marcar con un (X) la respuesta que cree conveniente con responsabilidad y atendiendo a las indicaciones específicas. Por favor responda con sinceridad todas las preguntas. Se agradece.

1. ¿Tiene conocimiento si hay manuales o procedimientos en la empresa, aprobados por la gerencia?

   a) Si
   b) No
   c) No sabe /No Opina

2. ¿El área donde labora, cuenta con procedimientos, manuales o instructivos establecidos para el manejo de información del sistema?

   a) Si
   b) No
   c) No sabe /No Opina

3. ¿Existe algún manual de contingencia elaborado y aprobado por la empresa?

   a) Si
   b) No
   c) No sabe /No Opina

4. ¿Se ha implementado alguna política de seguridad para la protección y seguridad de la información?
   a) Si
   b) No
   c) No sabe /No Opina

5. ¿Sabe Usted si la empresa se rige por alguna norma o estándar de calidad para la protección de la información?
   a) Si
   b) No
   c) No sabe /No Opina

6. ¿Conoce si en la empresa hay algún encargado sobre la seguridad informática?
   a) Si
   b) No
   c) No sabe /No Opina

7. ¿Posee Ud. algún conocimiento acerca de la seguridad informática?
   a) Si
   b) No

8. ¿Con que frecuencia se presentan dificultades o inconvenientes en el sistema?
   a) Siempre
   b) Algunas Veces
   c) Nunca

9. ¿En cuánto tiempo se resuelve las dificultades presentadas en el sistema?
   a) Enseguida
   b) Se espera un poco
   c) Se demora

10. ¿La información que facilita el sistema de almacén es?
    a) Adecuada
    b) Correcta
    c) Sólida
    d) Confiable

11. ¿El manejo del sistema de almacén es?
    a) Fácil
    b) Más o Menos
    c) Difícil

12. ¿El acceso a la información en el sistema de almacén es?
    a) Limitado
    b) En algunos casos
    c) Libremente accedidos

13. ¿Se realizan copias de seguridad sobre la información de la empresa?
    a) Si
    b) No
    c) No sabe /No Opina

14. ¿Usted cierra sesión de su computadora, cuando no está trabajando en ella?
    a) Si
    b) No

15. En el tiempo que labora ¿Usted ha recibido alguna capacitación acerca de la seguridad informática y de los sistemas que se maneja en la empresa?
    a) Si
    b) No

16. ¿Se realizan mantenimiento a las computadoras y sistemas de información?
    a) Si
    b) No
    c) No Sabe/No opina

17. ¿Usted cree importante aplicar controles de seguridad para evitar alguna manipulación o robo de información?
    a) Muy importante
    b) Más o menos importante
    c) No es importante

18. Al inicio de sus labores ¿Usted firmó algún acuerdo de confidencialidad de la información referente a la empresa?
    a) Si
    b) No

19. Cuando termina de laborar ¿Usted guarda los documentos o archivos confidenciales en un lugar seguro?
    a) Siempre
    b) A veces
    c) Nunca

20. ¿La empresa tiene lugares de acceso restringido?
    a) Si
    b) No
    c) No Sabe/No opina

Agradecemos su colaboración y atención prestada a la presente encuesta.

ANEXO 02: Entrevista a la Administradora de sucursal

Empresa: Distribuciones Almapo S.R.L. Huacho

Persona Entrevistada: Administradora – Srta. Melissa Espinoza Cipra

1. ¿Poseen algún manual de políticas de seguridad informática?
2. ¿Cuentan con procedimientos o instructivos para cualquier incidente?
3. ¿A qué cree que se deba estos inconvenientes en el sistema?
4. ¿Si hay alguna dificultad que se presenta en el sistema, que acciones se toman en cuenta para resolverlo?
5. ¿Cada que tiempo se realiza el mantenimiento a los equipos de cómputo de la empresa?
6. ¿Qué nivel de seguridad posee el sistema y las aplicaciones que se utilizan en los equipos de cómputo de la empresa?
7. ¿Qué nivel de seguridad tiene la información almacenada en el sistema del área de almacén?
8. ¿Conoce Ud. algún riesgo acerca de la seguridad informatica que puedan afectar a la empresa?
9. ¿Se realizan periódicamente capacitaciones a los colaboradores en temas de seguridad de información?
10. ¿Cuentan con perfiles de usuario, establecidos de acuerdo a sus roles?
11. ¿Cada cuánto tiempo se realizan inventarios de los equipos de la empresa?
12. ¿Se tiene algún registro de control de los incidentes que ocurren diariamente en la empresa?
13. ¿Tiene algún plan de contingencia contra los desastres naturales?

ANEXO 03: Matriz De Consistencia

TÍTULO: ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL MANEJO DE INFORMACIÓN DE LA DISTRIBUIDORA ALMAPO S.R.L. HUACHO, 2016

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	INDICADORES	MÉTODOS
¿Cómo establecer políticas de seguridad informática para el manejo de información de la Distribuidora Almapo S.R.L Huacho, 2016?	**Objetivo General** Establecer políticas de seguridad informática para el manejo de información de la Distribuidora Almapo S.R.L. Huacho, a través de la norma ISO/IEC 27001:2013 **Objetivo Específicos** - Conocer la situación actual en la que se encuentra el manejo de información de la Distribuidora Almapo S.R.L. Huacho, 2016. - Aplicar la Norma ISO/IEC 27001:2013 para identificar las vulnerabilidades de seguridad informática en el manejo de información de la Distribuidora Almapo S.R.L. Huacho, 2016. - Determinar las políticas de seguridad informática que permitan el manejo adecuado de la información de la Distribuidora Almapo S.R.L. Huacho, 2016	En vista de que la investigación tiene un alcance de carácter descriptivo, no es posible plantear una hipótesis debido a que no se intenta correlacionar o explicar casualidad de variables. Por tanto la hipótesis es implícita	**Variable 1** Políticas de Seguridad **Variable 2** Seguridad Informática	- Normas - Procedimientos - Reglas - Integridad. - Disponibilidad - Confidencialidad	**Tipo de Investigación** - Es de tipo Aplicada **Nivel de Investigación** - Nivel Descriptivo **Diseño de la Investigación** - No Experimental **Población y Muestra:** Es igual a 32 colaboradores de la empresa **Técnicas de Recolección de Datos** - Encuesta - Entrevista - Observación

ANEXO N° 04: Resultados de Observación (Visitas a la empresa)

FIGURA N°22. **Login Del Sistema**
Fuente: Fotos tomadas del Sistema

FIGURA N°23. **Estantes llenos de archivadores**
Fuente: Fotos tomadas en la empresa

FIGURA N°24. **Facturas dejadas en cualquier mobiliario**
Fuente: Fotos tomadas en la empresa

FIGURA N°25**: Equipos Informáticos**
Fuente: Fotos tomadas en la empresa

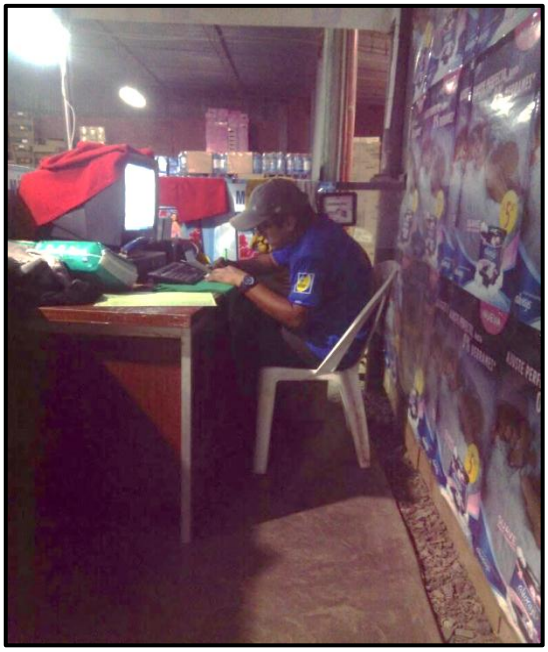

FIGURA N°26. **Área de almacén**
Fuente: Fuente tomadas en la empresa

FIGURA N°27. **Algunos colaboradores de la empresa**
Fuente: Fotos tomadas en la empresa