UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE CIENCIAS E INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

PLAN DE MEJORA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO/IEC 27001: 2013 EN LA EMPRESA BROZZANDII PASTELERÍA S.A.C. PIURA, 2022.

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

AUTOR
SEMINARIO VASQUEZ, RAFAEL ASUNCION
ORCID: 0000-0002-4683-433X

ASESOR
MORE REAÑO, RICARDO EDWIN
ORCID: 0000-0002-6223-4246

CHIMBOTE – PERÚ
2022

EQUIPO DE TRABAJO

AUTOR

Seminario Vasquez, Rafael Asuncion

ORCID: 0000-0002-4683-433X

Universidad Católica Los Ángeles de Chimbote, Estudiante de Posgrado

Piura, Perú

ASESOR

More Reaño, Ricardo Edwin

ORCID: 0000-0002-623-4246

Universidad Católica Los Ángeles de Chimbote, Facultad de Ingeniería de Ingeniería, Escuela Profesional de Ingeniería de Sistemas, Chimbote, Perú

JURADO

Ocaña Velásquez, Jesús Daniel

ORCID: 0000-0002-1671-429X

Castro Curay, José Alberto

ORCID: 0000-0003-0794-2968

Sullón Chinga, Jennifer Denisse

ORCID: 0000-0003-4363-0590

JURADO EVALUADOR DE TESIS Y ASESOR

DR. JESÚS DANIEL OCAÑA VELÁSQUEZ
PRESIDENTE

MGTR. JOSÉ ALBERTO CASTRO CURAY
MIEMBRO

MGTR. JENNIFER DENISSE SULLÓN CHINGA
MIEMBRO

MGTR. RICARDO EDWIN MORE REAÑO
ASESOR

DEDICATORIA

A nuestro Señor todopoderoso que me ha permitido concluir la Tesis de la Maestria.

A mis padres Ricardo Seminario y Estela Vasquez que desde el cielo verán cumplido este nuevo pilar académico dentro de mi vida y por ser ellos siempre motivadores al estudio.

A mis hnos., la Psicóloga María Teresa, el Dr. Ricardo Gerónimo y también a mis hnos. Milton y Carmen que me verán desde el cielo.

A mi esposa Alejandra Guaylupo, y a mis hijos Rosaester, Daviserge y Ricardo Manuel por su apoyo moral, compañía y sus avances personales.

Seminario Vasquez Rafael Asunción

AGRADECIMIENTO

Mi mayor agradecimiento a quienes dirigen esta Digna casa de estudios Superiores la Universidad Católica Los Ángeles de Chimbote, así como también a los excelentes Maestros que impartieron sus clases con seriedad, calidad y gran docencia universitaria, que me permitió desarrollar una gran visión de esta maestría para mi vida profesional.

Al Mgtr. Ricardo Edwin More Reaño, mi asesor, por su capacidad, paciencia y guía, en la orientación de la Tesis

Y mi agradecimiento a los docentes, miembros del jurado de mi tesis de Maestria por su dedicación, correcciones y aprobación del proyecto e informe de la tesis de esta Maestria

Seminario Vasquez Rafael Asunción

RESUMEN

El presente informe de tesis está basado su desarrollo bajo la línea de investigación de las TIC., Tecnología de la información y comunicación de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Los Ángeles de Chimbote (ULADECH CATÓLICA). El objetivo principal fue Proponer un plan de mejora de seguridad de la información, para la empresa BROZZANDII PASTELERÍA S.A.C.; 2022 basado en la ISO/IEC 27001: 2013. Según sus características la investigación fue de tipo cuantitativa, de diseño no experimental, de nivel descriptiva y de corte transversal, la población está constituida por 8 trabajadores administrativos y ejecutivos, los cuales constituyeron la población muestral. En la investigación se obtuvo que el 87,5% de los trabajadores encuestados no conocen sobre seguridad de la información, y el 75% de los encuestados dan a conocer que la empresa no tiene protección de los procesos de información. Por lo que conlleva a la elaboración de la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013, para la solución de los problemas de la empresa BROZZANDII PASTELERIA S.A.C. en la ciudad de Piura.

Palabras clave: Plan de mejora, protección de la información, seguridad de la información, tecnología de información.

ABSTRACT

This thesis report is based on its development under the ICT research line, Information and Communication Technology of the Professional School of Systems Engineering of the Los Angeles University of Chimbote (ULADECH CATÓLICA). The main objective was to propose an information security improvement plan for the company BROZZANDII PASTELERÍA S.A.C.; 2022 based on ISO/IEC 27001: 2013. According to its characteristics, the research was quantitative, non-experimental, descriptive and cross-sectional in design, the population is made up of 8 administrative and executive workers, who constituted the population. sample. The investigation found that 87.5% of the workers surveyed do not know about information security, and 75% of the respondent's state that the company does not have protection of information processes. For what it entails to the elaboration of the proposal of an information security improvement plan based on ISO / IEC 27001: 2013, for the solution of the problems of the company BROZZANDII PASTELERIA S.A.C. in the city of Piura.

Keywords: Improvement plan, Information protection, information security, information technology.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

I. INTRODUCCION

UNILA (1), en su artículo sobre seguridad informática en las empresas indica que la evolucion de la tecnología es enorme de tal manera que se hace más fácil hackear a una empresa, exponiendo a riesgo a toda su información importante, en tanto que hay una seguridad informática para prevenir este tipo de obstáculos al desarrollo empresarial. Esta seguridad informática es importante por la prevención del hurto de la información de la empresa generando alertas en los sistemas de información internos por las amenazas y riesgos

Movistar (2), indica que, no es secreto la tendencia ascendente la IoT, o llamada Internet de las cosas sea un factor principal que propulse la capacidad y calidad de la interconexión de las empresas. La inmensidad de datos producidos con el auge de los celulares y otras tecnologías, ha impulsado la necesidad de afianzar su conectividad en sus empresas dado la enorme facilidad de sus procesos. Por todo esto varias empresas han priorizado en las 2018 nuevas soluciones que faciliten incrementar su productividad con un control automatizado en tiempo real para recolección de datos y monitoreo, reduciendo con ello los costos y facilitándose el acceso a coyunturas nuevas de negocio.

Asturias M. (3), da a conocer que las empresas y agencias de todos los gobiernos se encuentran agilizando su adaptación a negocios de modelos digitales que les facilita respuestas mas agiles ante los constantes cambios en los pedidos de sus consumidores, procesos transacciones e inmediates en tiempo real, consiguiendo con ello mayor agilidad, mejor productividad, óptimos resultados en la comercialización y un excelente servicio. Estos cambios saltan más allá de lo corporativo. La sociedad esta cambiando gracias a la transformación digital hacia niveles nunca vistos, Estos cambios se dan especialmente en la forma de aprender, de trabajar, de gestionar sus finanzas, de comprar y socializar, es diferente la interacción con el mundo que nos rodea. Por ello el reto es lograr la innovación en equilibrio con la productividad de la mano con la ciberseguridad y seguridad pragmática

La empresa BROZZANDII PASTELERIA S.A.C. en la ciudad de Piura, está dedicada a la pastelería y exclusivamente a elaborar tortas de matrimonio, cumpleaños, agasajos, etc. vía on line, tiene muchos riesgos en cuanto a la posibilidad de que se tome sus modelos por otras empresas del rubro como si fueran suyos, además también que algunos clientes puedan ser sorprendidos con algo que les pueda afectar, y así generar perdidas de clientes por alteración de la información

La confidencialidad en cuanto al uso de productos naturales para los clientes veganos, y de las proporciones de los ingredientes para el gusto del cliente, así como para la seguridad intima de la información de la empresa y también de los posibles problemas que pudieran tener los equipos de procesamiento de la información de la misma.

Para toda esta problemática se ha planteado la pregunta de investigación, ¿En qué medida la propuesta de un plan de mejora de seguridad de la información, basado en la ISO/IEC 27001:2013, en la empresa Brozzandii Pastelería S.A.C. - Piura; 2022, permite reducir los riesgos de pérdida de su información

Así también el objetivo de esta investigación dice: Elaborar un plan de mejora de seguridad de la información, en la empresa Brozzandii Pastelería S.A.C. - Piura; 2022 basado en la ISO/IEC 27001: 2013., y sus específicos: dicen: el primero, Determinar los activos de la empresa, con la finalidad de que se sepa cuales son los activos que la empresa tiene que valorar y proteger el segundo objetivo dice: Reconocer las amenazas a las que esta expuesta la empresa, generando con ello la necesidad de saber de que tenemos que proteger a los activos de la información de la empresa, y el tercero dice: Identificar las principales salvaguardas en la empresa BROZZANDII PASTELERIA S.A.C. generando con ello una cultura de seguridad de la información que será fortalecida con el plan de mejora de la seguridad de la información sus alcances, y su política de seguridad.

La metodología de esta investigación es de una investigación de tipo cuantitativa, de nivel descriptivo, así como de diseño no experimental y de corte transversal.

La investigación se justifica operativamente ya que la empresa realizara en menor tiempo la ejecución de sus procesos esta empresa para la que se genera este proyecto de investigación uno de sus principales valores es la información por lo que se hace

necesario desarrollar un plan de seguridad informática para que al ser procesada la información pueda alcanzar los fines que han sido previstos, dado que esta información podría ser dañada y por ende se altera todo el orden de la empresa tanto en el aspecto de tipo financiero, así como en el aspecto productivo, en el aspecto comercial con los clientes, etc.

Para salvaguardar el funcionamiento de la empresa es la informática la ciencia encargada de proporcionar todos los mecanismos apropiados para que automáticamente se controle cualquier indicio de alteración por parte de algún agente que pretenda afectarla. Por ello se hace indispensable de que protejamos nuestra información constantemente y con ello tener la seguridad de la solidez de la empresa.

La investigación se justifica tecnológicamente dado que la empresa utiliza en toda su infraestructura computacional un antivirus, lo cual es importante pero no suficiente para toda su información dado que se requiere un conjunto de acciones en un plan que se maneje con controles de seguridad informática, dado que existen muchas amenazas constantes en las redes por lo que se requiere de un eficiente plan de seguridad informática para la Empresa Brozzandii Pastelería S.A.C. Piura.

Se justifica la investigación económicamente porque la empresa invierte para obtener ganancias, paga sus impuestos y crece, gestiona compras y ventas, genera transacciones bancarias, etc., por tanto, su seguridad informática debe ser muy sólida para evitar los múltiples inconvenientes ante agentes perniciosos que podrían generar grandes pérdidas para la empresa. Además, por el lado de la información de los productos también se tiene necesidad de que esta información permanezca bien resguardada y evitarnos inconvenientes con la competencia y con nuestros clientes.

Los resultados muestran la importancia del planteamiento del plan de mejora de seguridad de la información en la cual el 87.5% de los encuestados no tiene conocimiento de la seguridad de la información y el 75% que no hay protección a los procesos de información en relación a la empresa BROZZANDII PASTELERIA S.A.C.

Las conclusiones indican que se logró realizar la propuesta de un plan de mejora de la seguridad de la información, para la empresa BROZZANDII PASTELERIA

S.A.C., 2022 basado en la ISO/IEC 27001: 2013, aportando conjuntamente con el conocimiento de los activos, amenazas y salvaguardas ya encontradas para la empresa, y el valor agregado está constituido por las políticas desarrolladas en la tabla 30 del plan de mejora de la seguridad de la información de la empresa.

II. Marco teórico

2.1. Antecedentes

Antecedentes a nivel internacional

Ulloa (6), en el año 2021 en la tesis de la Pontificia Universidad Católica del Ecuador en su tesis denominada “Análisis de problemas técnicos y legales de ciberseguridad y sus posibles soluciones en el contexto de la computación en la nube, indica que Desde hace varios años se vive en una era de revolución en donde, gracias a la tecnología, se experimenta grandes cambios en la estructura de nuestra sociedad, uno de estos cambios, y el cual generó un gran impacto en la forma de vida de la humanidad es el internet, una herramienta muy poderosa que significó una transformación global y que dio pasó a lo que hoy se conoce como la era digital, en la cual los datos y la información son las herramientas más poderosas. Tal es así, que en los últimos años el uso de servicios de internet en sus diferentes plataformas ha aumentado considerablemente, y como se evidencia en la actualidad, este entorno dio un giro, incluyendo al crecimiento exponencial de la economía digital, pues los servicios en línea significaron que muchas empresas podían ofrecer servicios sin la necesidad de que los clientes tengan que acudir físicamente, sin embargo, por maravilloso que suene todo esto lo cierto es que también dejó la puerta abierta para un nuevo problema, la seguridad en línea. Una de las medidas de seguridad es el uso de contraseñas, mismas que en varias ocasiones han sido usurpadas y han dado lugar al robo de dinero o suplantación de la identidad de usuarios, entre otras, tanto usuarios como empresas son cada vez más conscientes de esta problemática, en un ambiente donde gran parte de la sociedad considera que la manera tradicional que se tenía para cubrir la seguridad en línea podría ya no ser suficiente. Si bien los usuarios muestran cierta conciencia y preocupación a los ataques informáticos, pueden tener una idea equivocada de los mismos, por ejemplo, muchos usuarios suelen creer que no poseen ninguna información valiosa y por ende eso los permite de ser blanco de potenciales atacantes informáticos, sin embargo, lo cierto es

que, de alguna manera, todos somos vulnerables, pues los atacantes tiene interés en todo tipo de información como listas de contactos, robo de información, pedido de rescates por bloquear un ordenador y solicitar una suma de dinero a cambio de recuperar la información del mismo. Ante estas amenazas, surge la Ciberseguridad que, dentro del contexto de la tecnología, puede ser definida como un proceso que abarca la prevención, detección, respuesta y que, a su vez debe implicar el aprendizaje como una característica de mejora continua, estos términos se explican mejor de la siguiente manera. La ciberseguridad se resume en la práctica de defender servidores, sistemas, redes y datos de ataques maliciosos. Se trata de un término demasiado general y que puede aplicarse en diferentes contextos, siendo quizás algunos de los más destacados la seguridad de res, de aplicaciones, de la información entre muchos otros. Es por ello, que su definición se verá limitada únicamente a la temática principal del trabajo.

Amoguimba (5), en el año 2018 en la tesis de la Pontificia Universidad Católica del Ecuador, denominada "Propuesta de políticas de seguridad de la información aplicado al entorno empresarial del Soft Warehouse S.A.", indica que, COBIT 5 define a la información como: "... Un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel muy importante." (ISACA, 2012) Con esto se puede entender que la información es un activo importante para todo tipo de organización grande, mediana o pequeña, de tal manera que si este recurso está bien sustentado puede reducir los problemas de incertidumbre y puede determinar la calidad de las decisiones que se tomen. Los directivos de las empresas constantemente toman decisiones importantes encaminadas a llevar al éxito a la empresa, tomando en cuenta que dicha información que usan debe ser útil como materia prima para el desempeño y organización de la misma. Al ser la información un factor esencial que proporciona valor; las personas, organizaciones y estados han buscado formas de protegerlas, generando estándares, guías de buenas prácticas, procedimientos y sistemas de control; dando paso a la seguridad de la información que tiene como base el mantener tres principios (Confidencialidad, Disponibilidad e

Integridad), durante todo el ciclo de vida de la información

Arévalo (4), en el año 2017 en la tesis de gestión estratégica de tecnologías de la información denominada Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos", de la Universidad de cuenca Ecuador, indica que: En las empresas industriales de alimentos, existe información crítica para este tipo de organizaciones, como los datos de sus clientes, proveedores, transacciones diarias y las características principales que definen un producto como son sus recetas, proceso de fabricación, costos, etc. siendo necesario que toda esta información este resguardada confiablemente ante los posibles riesgos que se puedan materializar en cualquier momento. Para proteger los sistemas de información de los crecientes niveles de amenazas cibernéticas, las organizaciones actualmente tienen la necesidad de establecer programas o proyectos de seguridad informática y, debido a que las políticas de seguridad de la información son una base necesaria de los programas de seguridad organizacional, existe una necesidad de contribuciones académicas en esta área. Por ello se plantea en el presente trabajo una investigación en temas relativos a la seguridad de la información, gestión de riesgos y políticas de seguridad informática para posteriormente plantear un método adecuado consistente de 3 etapas y un total de 9 pasos para el desarrollo y difusión de políticas de seguridad a partir de la identificación de los posibles riesgos y vulnerabilidades que presenta una organización o un área de la misma, seleccionando los controles más adecuados de la norma ISO/IEC 27002, la cual es una guía aceptada internacionalmente de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de la información para una organización. La aplicación de la metodología propuesta se la realiza como un caso de estudio en el departamento de producción de una empresa industrial productora de alimentos en la ciudad de Cuenca - Ecuador. Éste trabajo puede servir como referencia a otras empresas industriales de alimentos que requieran elaborar de manera técnica y apropiada sus políticas de seguridad de la información; sin

embargo, también podría servir en empresas de diversos tipos, realizando las validaciones correspondientes y su aplicación.

Antecedentes a nivel nacional

Aliaga (7), en el año 2021 en la tesis denominada “Implementación de un Sistema de Ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza, 2021, el objetivo general de la presente investigación fue la realización de la implementación de un sistema de ciberseguridad que influye de manera positiva en la prevención ataques cibernéticos en la empresa radiadores fortaleza, 2021. El presente estudio fue de tipo aplicada, con un diseño pre experimental, la población elegida fue de 50 empleados de la empresa Radiadores Fortaleza, se concluye que el valor de la prueba de Student de -46.680, asociado a las medias de pres test y posttest donde hay una diferencia significativa , donde se asocia a un nivel de significancia p valor=0,000 menor al nivel de significancia establecido en la investigación ($p<0,05$) lo que con lleva al rechazo de la hipótesis nula (Ho) y la aceptación de la hipótesis general planteada en la investigación (Ha). El modelo de implementación de ciberseguridad que se adoptó en la empresa fue el idóneo porque hay una mejora notable en la defensa de los ataques informáticos y una disminución de las vulnerabilidades que con lleva a un mejor desempeño de negocio de la empresa Radiadores Fortaleza

Calderón (8), en el año 2019 en la tesis denominada Seguridad de la Información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018", en la cual el objetivo de la investigación es determinar la relación que existe entre la seguridad de la información y la gestión de riesgos en los trabajadores de la Dirección de Gestión de Recursos Educativos del Ministerio de Educación, 2018. Esta investigación tubo un diseño no experimental y un nivel experimental así como también es de tipo básico y transversal, la población de trabajo fue de 106 trabajadores de la DIGERE del Ministerio de Educación, los cuales fueron seleccionados con muestreo de tipo probabilístico y aleatorio simple; y por otra parte el método de investigación hipotético-deductivo

con enfoque cuantitativo; utilizándose el software SPSS para el tratamiento de los datos, sus resultados indican un promedio de más del 50 % de nivel regular la seguridad de la información y podemos ver una de sus conclusiones indica que hay una relación directa entre la seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación.

Calderón TLH (9), en el año 2019 en la tesis denominada " Gestión de riesgos y seguridad de la información del Programa Fortalece Perú del MTPE, 2019, la cual tuvo como objetivo general determinar la relación entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019, para lo cual uso la metodología MAGERIT, y sus resultados indican que el 56 % de la población del programa Fortalece Perú es bajo y se concluye que existe una relación directa y significativa de nivel medio entre la gestión de riesgos y la seguridad de la información del Programa Fortalece Perú 2019.

Olaya (10), en el año 2017 en la tesis denominada "Gestión del Sistema de Seguridad de Información bajo el enfoque de ISO 27001 en la Municipalidad Provincial de Tumbes, cuyo objetivo fue mostrar un modelo de Seguridad Informática basándose en la norma ISO 27001, su metodología consistió en un diseño no experimental con un nivel descriptivo y a su vez se aplica un muestreo no probabilístico, sus resultados corresponden a que el nivel de seguridad de la información es de 38 %, no hay revisiones de la política de seguridad de la información, la asignación de responsabilidades para la seguridad de la información es solo del 25 %, atención a los ciudadanos solo el 12,5 % , el procesamiento de la información un 50 %, confidencialidad solo el 25 %, y entre sus conclusiones se plantea la necesidad de un plan de mejora basado en el modelo ISO 27001, requiere una participación completa a nivel estratégico. Su papel tiene que ser protagónico en la implantación del modelo.

Antecedentes a nivel regional

Merino (13), en el año 2021 en la tesis denominada "Diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa comercial S.A- Piura; 2020. En la que su objetivo fue realizar el diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A – Piura; 2020. El tipo de investigación utilizado fue cuantitativo, de nivel descriptivo, el diseño fue de tipo no experimental y de corte transversal. Los resultados obtenidos en la dimensión 01: Nivel de satisfacción con el sistema actual; el 87% de los trabajadores encuestados NO están satisfechos con el sistema actual, en la dimensión 02: Nivel de aceptación de la propuesta de mejora; se observó que el 100% de los encuestados SI necesitan de una propuesta de mejora. Y en la dimensión 03: Nivel de conocimiento de Tecnologías de la Información y la Comunicación; el 67% de los trabajadores encuestados NO tiene conocimiento acerca de las TIC. Se concluyó que el diagnóstico para la seguridad informática basada en la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A – Piura; 2020, mejoró los procesos de seguridad, confiabilidad y disponibilidad de la información

Pangalima (11), en el año 2018 en la tesis denominada Auditoria Basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad Informática en la Empresa ARCOPA S.A. Paita; 2017. Cuyo objetivo fue objetivo general consistió en Implementar la auditoría basada en COBIT 4.1, para el uso óptimo de las TIC y la seguridad informática en la Empresa ARCOPA S.A; se utilizó un diseño de investigación no experimental y un nivel descriptivo y su resultados indican que el 61 % de los implicados revelan que se hace necesario la aplicación de la auditoria en la empresa, además el 69% de los trabajadores encuestados se encuentran satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en

cada uno de sus procesos de toda la organización y el 75% de los trabajadores encuestados están satisfactoriamente de acuerdo que al aplicar la Auditoría será de gran beneficio para mejorar la seguridad en cada uno de sus procesos de toda la organización

Lara (12), en el año 2018 en la tesis denominada "Propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la clínica Simedic diagnóstica S.A.C – Piura; 2018" cuyo objetivo fue realizar la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura; 2018, permitirá mejorar la gestión en los activos de información. La investigación tuvo un diseño de tipo no experimental porque los datos no se manipularán y de corte transversal porque se realiza en un determinado tiempo; la población de esta investigación fue de 28 empleados de los cuales se tomó en conciencia que esta investigación no se delimitará debido a que se verán beneficiados en su totalidad de empleados, a quien se les aplicó el instrumentos donde se lograron obtener los siguientes resultados: En la dimensión 01: Situación actual; que el 61% de los trabajadores encuestados opinaron que la situación actual NO cuenta con la adecuada gestión en los procesos de la clínica Simedic Diagnóstica S.A.C, mientras que el 39% SI está conforme con la situación actual de la clínica. Y en la dimensión 02: seguridad de información; se observó que el 68% de los trabajadores encuestados opinaron que, SI están de acuerdo con la que se debería realizar la propuesta para la seguridad informática para la clínica Simedic Diagnóstica S.A.C, mientras que el 32% NO cree necesario la propuesta para la seguridad informática. Se concluyó la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura; 2018, para la seguridad de información queda aceptada en su totalidad para brindar mayor seguridad en la clínica, trabajadores y clientes.

Ancajima (14), en el año 2016 en la tesis denominada " propuesta de implementación de seguridad informática en las tic de la i.e. san miguel

arcángel, Catacaos - Piura; 2016 El tipo de la investigación fue cuantitativa, nivel descriptivo, diseño no experimental y de corte transversal; teniendo como objetivo general realizar un estudio de los riesgos que se tiene en la institución, y así brindar una buena propuesta de implementación de Seguridad Informática de la I.E. San Miguel Arcángel, la cual mejorará el control de seguridad de la institución y se tendrá un mejor manejo en las herramientas tecnológicas por los docentes, personal administrativos y alumnos. Con una población muestral de 60 personas entre docentes, alumnos y personal administrativo que utilizan los equipos tecnológicos dentro de las áreas dentro de la institución. Se obtuvieron como resultados el 75.00% de los encuestado expresó que se encuentran satisfechos con las TIC en el proceso de enseñanza, así mismo el 73.00% expresó que se encuentran satisfechos con la formación y capacitación sobre el manejo de las TIC y el 73.00% de los encuestado expresó que se encuentran satisfechos con la seguridad Informática en las TIC en la institución. Por lo que se puede concluir que las políticas ayudarán en la Seguridad Informática de la institución permitiendo que los docentes, alumnos y personal administrativo queden satisfechos en el momento de utilizarlas, sintiéndose seguros a través de ellas y esta pueda ser más fácil manejar.

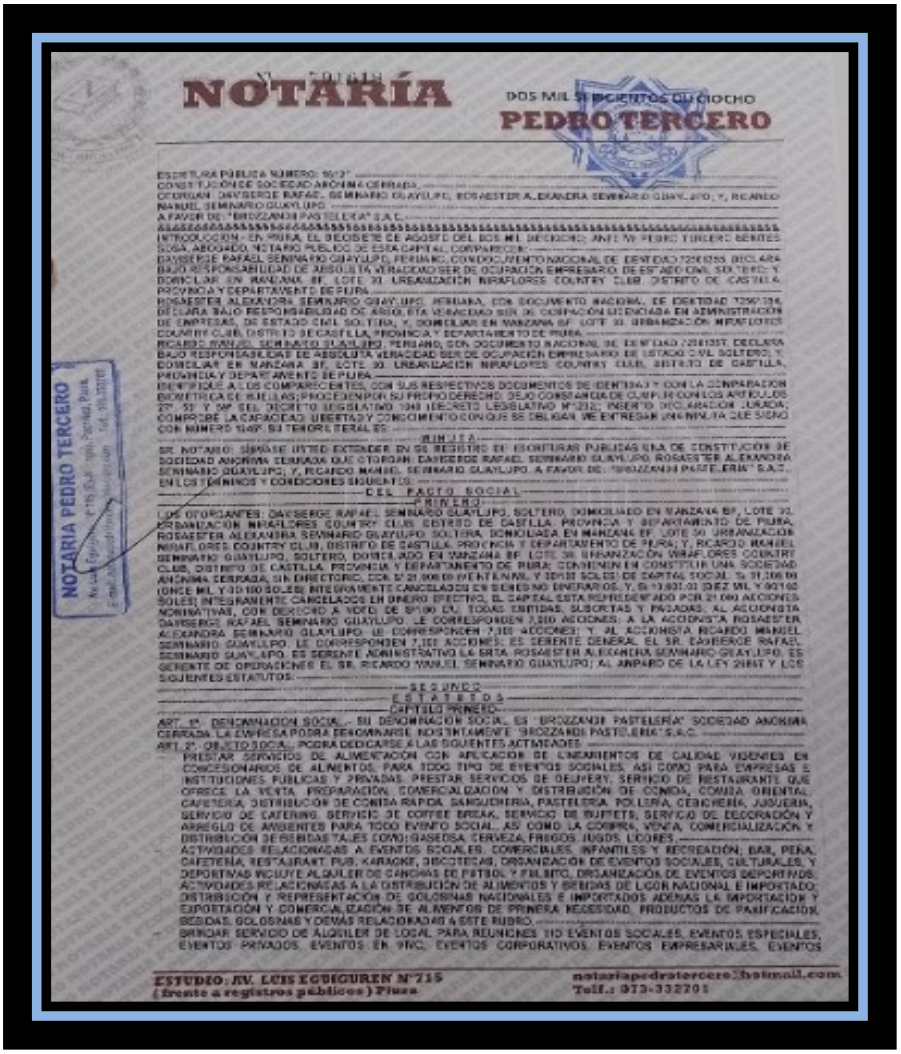
2.2. Bases teóricas relacionadas con el estudio

2.2.1. El Rubro de la Empresa

Información de Brozzandii Pastelería S.A.C.: Brozzandii Pastelería S.A.C. es una empresa que se encuentra inscrita en la partida N° 11199336 del registro de personas jurídicas de Piura, el 23 de agosto del 2018. Su dirección corresponde a Urbanización Miraflores Country Club Mz. BF-30 Castilla – Piura.

EMPRESA BROZZANDII PASTELERIA SAC

Escritura pública (1ra y ultima Pág.)



C O N C U E R D A

ESTE PRIMER TESTIMONIO, CON LA ESCRITURA ORIGINAL CORRIENTE A FOJAS 2,618. DE MI REGISTRO DE ESCRITURAS PÚBLICAS DEL AÑO 2,018. LO SELLO SIGNO, RUBRICO Y FIRMO DE ACUERDO A LEY.----------

PIURA, 23 DE AGOSTO DEL 2018.

NOTARIA PUBLICA ABOGADO PEDRO TERCERO BENITES SOSA

Pedro Tercero Benites Sosa
Notario Público
ABOGADO

NIHIL PRIUS FIDE P B S

I N S C R I P C I O N

INSCRITA EN LA PARTIDA N°11199336, DEL REGISTRO DE PERSONAS JURÍDICAS DE PIURA.--------

PIURA, 23 DE AGOSTO DEL 2018.

NOTARIA PUBLICA ABOGADO PEDRO TERCERO BENITES SOSA

Pedro Tercero Benites Sosa
Notario Público
ABOGADO

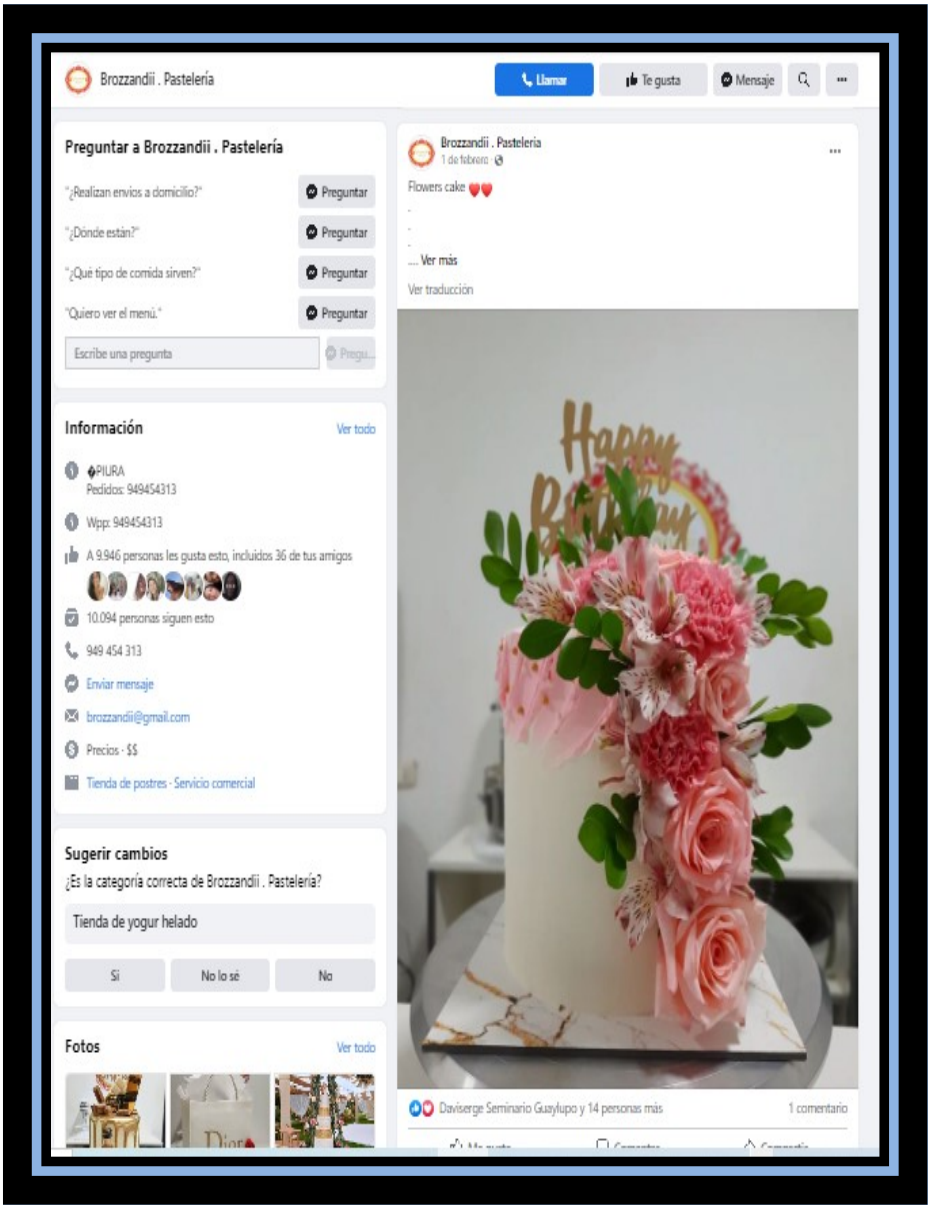
NIHIL PRIUS FIDE P B S

Sus actividades desarrolladas corresponden a servicios de alimentación con lineamientos de calidad vigentes en instituciones públicas y privadas, servicio de delivery a todos sus clientes de la pastelería, en todo lo correspondiente a tortas de todo tamaño y especializadas, bocaditos diversos, para todo tipo de eventos sociales como matrimonios, quinceañeros, cumpleaños, reuniones sociales, etc.

La empresa Brozzandii Pastelería S.A.C. (15), cuenta con una página

web para toda la ciudadanía, la cual es consultada diariamente y todos los pedidos se realizan por teléfono, para lo cual ponemos una captura de pantalla de la web.

BROZZANDII PASTELERIA SOCIEDAD ANONIMA CERRADA
PAGINA WEB



En este periodo de trabajo han logrado elaborar más de 300 tortas de este nivel con las interrupciones como la pandemia -Cobi 2019, además de bocaditos, en diversos agasajos.

- **Visión**

  Brozzandii Pastelería S.A.C. es una empresa muy sólida económica y bien cimentada en la sociedad regional de Piura con varios locales en funcionamiento y con muchas ventas, y gran prestigio.

- **Misión**

  Planificar, organizar, esfuerzo constante y disciplina en la conducción de toda la empresa, además el mantenimiento de la calidad, en el producto y en el servicio a nuestros clientes, capacitación constante del personal.

- **Valores**
  - Calidad en el servicio
  - Respeto
  - Puntualidad
  - Lealtad
  - Liderazgo
  - Responsabilidad
  - Transparencia
  - Honestidad
  - Equidad y Justicia
  - Amor al Trabajo

- **Organigrama de la Empresa BROZZANDII PASTELERIA S.A.C.**

BROZZANDII PASTELERIA S.A.C.

Fuente: elaboración propia

- **Infraestructura Tecnológica hardware y software**

La empresa BROZZANDII PASTELERIA S.A.C. cuenta con cinco computadoras tres para las gerencias y dos para la parte productiva. La información está bien ordenada en cada una de ellas y una hace de servidor, además se guarda la información en discos duros para evitar alguna perdida y por seguridad, se usan los softwares como es Windows 10, Excel, word, Powers point, pdf, y otros para diseñar el arte de los modelos de tortas o bocaditos a elaborar, también tienen equipos para fotografía de los productos, así como también proyector para los videos de propaganda de la empresa.

Inventario de hardware de la empresa

Tabla 01 Hardware (Laptops) de la Empresa BROZZANDII PASTELERIA S.A.C.					
Laptop	**N° - 1 - RI**	**N° - 2 - DA**	**N° - 3 - RO**	**N° - 4 -JA**	**N° - 5 - RA**
Marca	HP	HP	LENOBO	SAMSUNG	HP
Modelo	Laptop	Laptop	Laptop	Laptop	Laptop
Pantalla	15”	15”	15”	15”	15”
Condición	Servidor	Normal	Normal	Normal	Normal
Procesador	CORE I-7	RYZEN AMD - 7	CORE I-7	Intel Celeron	CORE I-7
Memoria RAM	8 GB	12 GB	8 GB	4 GB	12 GB
Tarjeta grafica	INTEL IRIS	NIVIDIA GEFORCE GTX	RADEON AMD	---------	RADEON GRAPHICS
Disco Duro	500 GB	500 GB	700 GB	250 GB	1000 GB
Baterías duración	10 horas	10 horas	10 horas	10 horas	10 horas
Entradas USB 3.0	2 entradas	2 entradas	2 entradas	3 entradas	3 entradas
Salidas HDMI	1 salida	1 salida	1 salida	1 salida	1 salida

Fuente: Elaboración propia

Inventario de Software de la Empresa BROZZANDII

Tabla 02 SOFTWARES INSTALADOS	
SISTEMA	WINDOWS 10
	Excel
	Word
	Poner Point
	Corel Draw
	PDF
PROGRAMAS	Antivirus
	Otros softwares especializados
	WhatsApp
	Correo electrónico
	Comunicación en línea con SUNAT y otras entidades.

Fuente: Elaboración propia

2.2.2. Marco teórico conceptual

- **Conceptos de seguridad informática**

UNAM (16), indica que la Seguridad Informática en los últimos años, ha logrado ser un tema de interés público. Tal es así que expertos en la materia y los usuarios generales usan los siguientes términos como es clave del usuario, contraseña password, fraude informático", "hacker", etc. Actualmente es requerido e indispensable, conocer bien este tema,

dado que sin tener este conocimiento apropiado pues sin ellos el usuario de las laptops podría estar en un estado inadecuado y se ponga en riesgo su equipo e información, o aun su integridad personal. Hay múltiples medidas preventivas que protegen este trio de factores de protección a la información con Backus, el hardware y el software con programas antivirus, antispyware y antispam, así como uso de firewalls, una continuidad de actualizaciones al sistema operativo, con un mantenimiento físico a los equipos de cómputo, así como a las areas de operaciones de red con detectores de humo y calor, extintores, controles de temperatura y humedad, reguladores de voltaje, sistemas de anclaje, ventilación, sistemas de suministro continuo de energía, etc.

ISO 27001 (17), responde a la pregunta ¿Cuáles son los requisitos de seguridad?. Para ello tenemos que recordar que no hay sistema de seguridad totalmente seguro por ello debemos tener claro que un sistema siempre es vulnerable. Es indispensable que tengamos en cuenta las causas de los riesgos y posibles fallas, una vez que lo sabemos podemos aplicar las medidas requeridas para obtener un sistema poco vulnerable. A continuación, explicamos cada uno de los puntos que forman la CIA.

Confidencialidad

La confidencialidad se conoce como una forma de prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados.

Integridad

Cuando hablamos de integridad en seguridad de la información nos referimos a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros, cuando una violación modifica algo en la base de datos, sea por accidente o intencionado se pierde la integridad y falla el proceso

Por este motivo se debe proteger la información para que sólo sea

modificada por la misma persona, evitando así que se pierda la integridad. Una manera de proteger los datos es cifrando la información mediante un método de autenticidad como una contraseña o mediante huella digital

Disponibilidad

Es un pilar fundamental de la seguridad de la información, nada hacemos teniendo segura e integra nuestra información, si no va a estar disponible cuando el usuario o sistema necesite realizar una consulta.

Para cumplir con la última condición tenemos que tener claro cuál será el flujo de datos que debemos manejar, para conocer donde se debe almacenar dicha información, que tipo de servicio debemos contratar, etc.

Gonzales Y. (18), dice que actualmente las empresas que trabajas en sistemas de información establecen lo indispensable que es el aseguramiento de la información, creando políticas y controles, que garanticen la estabilidad y confiabilidad de la información, … , se hace necesario presentar una línea de base sobre la cual se integren varios tipos de esfuerzos encaminados a ofrecer la diferentes esfuerzos encaminados a brindar la seguridad en la información, considerando las múltiples amenazas y vulnerabilidades que afectarían la integridad de los datos, redes, servicios y todas las demás herramientas tecnológicas. Se debe indicar que este proyecto de plan de seguridad informática parte de copias de seguridad, protección, integralidad, control de acceso y otros factores a tomarlos en cuenta.

ISO 27001, normas de seguridad de la información internacionales, amenazas, riesgos.

ISO/IEC 27001 (19), es una norma internacional muy reconocida por los sistemas de gestión y la seguridad de la información:

- Apoya a las instituciones a establecer la política y objetivos de dirección de la seguridad de la información y a entender

cómo se pueden gobernar los aspectos importantes, colocar los controles necesarios y establecer objetivos claros y fortalecer la seguridad de la información.

- Permite a una organización gestionar su obligación de cumplir con los requisitos legales aplicables, como el GDPR (junto con la norma ISO 27701) y comprobar periódicamente el estado de cumplimiento. Esto permite una mejora continua del sistema para garantizar la protección y abordar las vulnerabilidades.
- Adopta un enfoque integral de la seguridad de la información. Los activos que necesitan protección van desde la información digital, los documentos en papel y los activos físicos (ordenadores y redes) hasta los conocimientos de los empleados individuales. Las cuestiones que hay que abordar van desde el desarrollo de la competencia del personal a la protección técnica contra el fraude informático.
- La norma ISO 27001 está diseñada para ser compatible y armonizada con otras normas reconocidas de sistemas de gestión. Por lo tanto, es ideal para su integración en los sistemas y procesos de gestión existentes. (ISO 27001 - Sistema de Gestión de Seguridad de la Información).

Conformio ISO 27001 (21), este software es una herramienta de cumplimiento todo en uno que incluye todo lo que necesita para implementar y mantener los estándares de documentos con plantillas, formularios en línea, políticas, procedimientos, gestión de riesgos, listas de verificación con recordatorios automáticos y más. Minimice el tiempo y el dinero necesarios para obtener y mantener la certificación ISO 27001.

2.3. Hipótesis

2.3.1. Hipótesis general

El Plan de Mejora de Seguridad de la Información basado en la ISO/TEC 27001:2013 para la Empresa BROZZANDII PASTELERIA S.A.C. Indica los procedimientos que mitigaran los riesgos que pueden presentarse en el uso de la información

2.3.2. Hipótesis Especificas

- La determinación de la información necesaria para constituir el PMSI permitirá mejorar la seguridad de la información.
- Establecer las acciones respectivas para elaborar el PMSI con la gestión de riesgos, el propósito de seguridad de la información, demostración y ejecución del Plan de mejora.
- Indicar los componentes correspondientes para ejecutar el plan de mejora de la seguridad informática de la empresa.

2.4. Variables

2.4.1. Variable independiente: El Plan de Mejora de Seguridad de la Información basado en la ISO/IEC 27001:2013.

2.4.2. Variable dependiente: L os procedimientos que mitigaran los riesgos que pueden presentarse en el uso de la información.

III. Metodología

3.1. El tipo y el nivel de la investigaciónTipo de estudio:

La presente investigación fué de tipo cuantitativa. La Investigación cuantitativa corresponde dado que se va ha aplicar cuestionarios y se va a trabajar estadísticamente. Rasinger, indica que la característica principal de los datos cuantitativos es que se componen de información que puede ser ,de una forma u otra, cuantificable, en otra palabras podemos convertir los datos cuantitativos en números, cifras y gráficos y procesarlos empleando procedimientos estadísticos (que son un tipo de procedimientos matemáticos) (38).(22).

Nivel de la investigación:

El nivel de esta investigación será de nivel descriptivo debido a que detallamos como se están dando las actividades de la organización. Según Hernández y otros se emplea cuando lo que se pretende es describir las características que se estudian de los elementos que integran la muestra seleccionada (39) (23).

3.2. Diseño de la investigación

El diseño de esta investigación será no experimental y de corte transversal. Dado que en la investigación no experimental no se manipulan deliberadamente las variables, es decir, se estudian tal y como se desarrollan en su contexto natural. (23) Según Heinemann, en la investigación de corte trasversal se recopilan los datos en un momento determinado (llamado por esto también análisis puntual y sincrónico). (24).

Población y Muestra

Se denomina población o universo a la totalidad de conjunto de elementos susceptibles de presentar una o varias características en común que estén bien definidas ,aunque no necesariamente, presentan una característica (medible o no) (41) (25).

En esta investigación la población está constituida por personal de la empresa a cargo de las areas correspondientes en un total de ocho personas que tienen acceso a la información de BROZZANDII PASTELERIA S.A.C.

La muestra es el conjunto de individuos que realmente se estudiaran. Es un subconjunto de la población. Para que se puedan generalizar los resultados obtenidos, dicha muestra ha de ser representativa de la población (42) (26)

En este caso por tratarse de una población pequeña la muestra será igual a la población

3.3. Definición y Operacionalización de variables y los indicadores

Ver Tabla N° 03 Definición y operacionalización de variables y los indicadores.

Tabla 3:
Matriz de Operacionalización de Variables

Variable	Definición conceptual	Definición operacional	Dimensión	Indicadores	Escala de dimensión
Propuesta de un plan de mejora de seguridad de la información (PMSI)	.Aguirre M. (27). El plan de seguridad de la información desarrollado en el presente documento, está orientada al aseguramiento de la confidencialidad, integridad y disponibilidad de la información e incluye las normas, controles y procedimientos en los siguientes dominios: Organización de la seguridad, clasificación y control de activos de información, seguridad de Comunicaciones y operaciones, control de accesos, adquisición, desarrollo y Mantenimiento de sistemas de información, Gestión de incidentes, Gestión de Continuidad del Negocio.	El Plan de Mejora de Seguridad de la Información (PMSI) será implementado en la Empresa BROZZANDII PASTELERIA S.A.C., es un instrumento de gran importancia porque va a permitir que todo el personal de la empresa tenga el conocimiento y cambie de actitud en relación a la protección de los procesos de información para la seguridad de la empresa. Es decir, aplicar este instrumento, diariamente en el uso y desuso de los sistemas de información y la infraestructura informática, tal es así que deberán tener cuidado tanto al usar, así como al cerrar sus equipos.	1.- Nivel de conocimiento sobre seguridad de la información. 2.- Nivel de protección de los procesos de información	-Enviar y recibir información - Compartir recursos en la empresa. - Facilitar el control - Agilizar los procesos de gestión administrativa en la empresa.	Nominal

Fuente: Elaboración propia.

3.4. Técnicas e instrumentos

Técnica

En esta investigación se utilizará las técnicas de la encuesta y la entrevista para obtener la información de la empresa BROSANDII PASTELERIA S.A.C.

López P. y Roldan S. (28), la encuesta es una de las técnicas de investigación social de más extendido uso en el campo de la Sociología que ha trascendido el ámbito estricto de la investigación científica, para convertirse en una actividad cotidiana de la que todos participamos tarde o temprano. Se ha creado el estereotipo de que la encuesta es lo que hacen los sociólogos y que éstos son especialistas en todo.

- **Abiertas,** cuando el encuestado puede responder a las preguntas con sus propias palabras, lo cual le otorga una mayor libertad de respuesta y le permite alcanzar una mayor profundidad en las mismas, como respondiendo al porqué de lo dicho, o bien obtener respuestas novedosas y diferentes.
- **Cerradas,** cuando al encuestado se le ofrece un conjunto de respuestas posibles y se le pide que elija la que mejor se adecúa a su opinión. Estas respuestas tienen la virtud de ser sencillas y fáciles de totalizar y cuantificar para obtener datos estadísticos.

  La aplicación de encuestas es un método muy común en diferentes tipos de investigación, siempre que requieran del levantamiento de datos estadísticos, de la recopilación de opiniones o bien de algún tipo de consulta masiva que permita luego ser interpretada para obtener conclusiones. Sondeos políticos, de mercado o de evaluación de servicios, son algunos posibles ejemplos de ello.

Diaz L. (29), Observar científicamente. Significa observar un objetivo claro, definido y preciso: el investigador sabe que es lo que desea observar y para que

quiere hacerlo, lo cual implica que debe preparar cuidadosamente la observación.

Instrumentos

Cuestionario:

El instrumento utilizado en esta investigación fundamentalmente es el cuestionario el cual ha sido elaborado de forma muy especial para obtener la información necesaria y suficiente para la elaboración del plan de mejora de la seguridad de la información de la empresa BROZZANDII PASTELERIA S.A.C., tomando en consideración que es una empresa privada con información confidencial del procesamiento de sus productos y del nivel de marketing desarrollado por la empresa a su favor; con este cuestionario se podrá determinar las actitudes y aptitudes que influencian en el comportamiento del sistema ligado al control y resguardo de la información de la empresa.

Bravo T. y Valenzuela S. 2019, (30), El cuestionario es un instrumento utilizado para recoger de manera organizada la información que permitirá dar cuenta de las variables de interés en cierto estudio, investigación, sondeo o encuesta. En el contexto de la evaluación educacional, este instrumento es útil para recoger de manera estandarizada información sobre características de una población de interés, así como para medir opiniones, creencias o actitudes. Al igual que en el caso de pruebas de conocimiento, la construcción de un cuestionario implica un diseño cuidadoso que aumente la probabilidad de que la información que se recogerá a través de él sea la correcta. El siguiente cuadernillo define los principales pasos que se deben llevar a cabo para la construcción de un cuestionario: definición del constructo, diseño de la tabla de especificaciones, construcción de las preguntas y pilotaje. Para cada una de estas etapas se presentan sugerencias y recomendaciones que permitirán asegurar una mayor calidad de los instrumentos desarrollados.

Este cuestionario ha sido elaborado de acuerdo al tipo de empresa que es BROZZANDII PASTELERIA S.A.C., y en función a los integrantes de la

empresa, así también las preguntas son de orden cerradas y dicotómicas.

Procedimiento de recolección de datos

La recolección de datos realizada a la empresa BROZZANDII PASTELERÍA S.A.C., tuvo lugar en su local ubicado en la Urbanización Miraflores Country Club - Castilla - Piura, en el cual se dialogó con los directivos informándoseles sobre el motivo y beneficios que se obtendrían con la realización de esta investigación, recibiendo todo el apoyo por parte de ellos en cuanto a la información requerida para su ejecución.

Dentro del dialogo se pudo saber todos los por menores requeridos para la investigación, e indicándoles también que esta información es de completa reserva y solo se utilizara para fines de investigación y después de esta conversación se procedió a aplicar la encuesta ya elaborada, y así se pudo conocer mucho más la realidad problemática y conocer cuanto saben tanto individualmente, así como en equipo sobre seguridad de la información.

3.5. Plan de análisis

En función a las condiciones del diseño no experimental y de sus variables en esta investigación, durante el procesamiento de la información, se estructuro los datos obtenidos, se los codifico y a través de una hoja Excel, de office, para el cálculo respectivo a nivel de cálculos y gráficos de las variables de la investigación, determinando las frecuencias y la determinación y su distribución correspondiente; dicha información esta indicada en esta investigación a través de tablas individuales y de resumen así como de gráficos de los resúmenes totales.

En esta investigación los resultados se han expresado a nivel de porcentajes , y el análisis de toda la información y su interpretación se realizó haciendo uso de la estadística descriptiva a través de las frecuencias y porcentajes de las respuestas de los encuestados.

3.6. Matriz de consistencia

Tabla 04

Matriz de Consistencia

TÍTULO**: "**PLAN DE MEJORA DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA ISO/IEC 27001:2013, PARA LA EMPRESA BROZZANDII PASTELERIA S.A.C. - PIURA; 2022

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLE	METODOLOGÍA
¿n qué medida el plan de mejora de seguridad de la información, basado en la ISO/IEC 27001:2013, para la empresa Brozzandii Pastelería S.A.C. - Piura; 2022, permite reducir los riesgos de pérdida de su información?	**Objetivo General** Elaborar un plan de mejora de seguridad de la información, para la empresa Brozzandii Pastelería S.A.C. - Piura; 2022 basado en la ISO/IEC 27001: 2013.	Hipótesis general El Plan de mejora de Seguridad de la información basado en la ISO/TEC 27001: 2013 para la Empresa BROZZANDII PASTELERIA S.A.C. Indica los procedimientos que mitigaran los riesgos que pueden presentarse en el uso de la información.	Plan de mejora de seguridad de la información basado en la ISO/TEC 27001: 2013 para la Empresa BROZZANDII PASTELERIA S.A.C. que concede alternativas más convenientes para sus actividades empresariales.	Tipo: Cuantitativa Nivel: Descriptivo Diseño: No experimental y de corte transversal.
	Objetivos Específicos 1.- Determinar los activos de la empresa BROZZANDII PASTELERÍA S.A.C	**Hipótesis especificas** 1.- La Determinación de los activos de la empresa BROZZANDII PASTELERÍA S.A.C. permitirá conocer la		

		infraestructura física y lógica de TIC e la empresa		
	2.- Reconocer las amenazas a las que está expuesta la empresa BROZZANDII PASTELERÍA S.A.C.	2.- El reconocimiento de las amenazas a las que está expuesta la empresa BROZZANDII PASTELERÍA S.A.C. permite tomar medidas preventivas y correctivas		
	3.- Identificar las principales salvaguardas en la empresa BROZZANDII PASTELERÍA S.A.C	3.- La Identificación de las principales salvaguardas en la empresa BROZZANDII PASTELERÍA S.A.C. permitirá proponer un plan de mejora para la empresa		

Fuente: Elaboración propia.

3.7.Consideraciones éticas y de rigor científico

La investigación realizada a la Empresa BROZZANDII PASTELERIA S.A.C., se denomina “Propuesta de un plan de mejora de seguridad de la información basado en la ISO/TEC 27001 – 2013, para la Empresa BROZZANDII PASTELERIA S.A.C. Piura -2022.”, ha desarrollado todos sus ítems en las distintas etapas del proceso de investigación como son el marco teórico, la introducción hipótesis , etc., con mucha pulcritud tomando las citas correspondientes a los autores en forma fidedigna tanto de tesis así como de libros, cumpliendo con los principios éticos para así garantizar una investigación original tomando en cuenta que es una entidad privada que contiene mucha información de carácter confidencial, la cual tiene que ser resguardada.

También se tuvo en cuenta el resguardo de las identidades de los encuestados a solicitud de ellos mismos.

Además, también las citas electrónicas han sido correctamente consultadas y presentadas para mayor solidez de la información, las cuales se encuentran ordenadas en las referencias al final de esta investigación con los datos correspondientes y con su URL respectiva.

IV. Resultados

4.1. Resultados

Dimensión 01: Nivel de conocimiento sobre seguridad de la información

Tabla 5: Antivirus a dispositivos de almacenamiento

Distribución de frecuencias y respuestas relacionadas con el antivirus a dispositivos de almacenamiento respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	03	25.00
NO	05	75.00
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: Al iniciar sus labores del día ¿Conoce cómo realizar el análisis con antivirus a todos sus dispositivos de almacenamiento que ha de conectar al equipo informático?

Aplicado por Seminario R.; 2022.

.

En la tabla 5 se puede observar que el 75.00% de los trabajadores No conocen cómo realizar el análisis con antivirus a todos sus dispositivos de almacena miento que ha de conectar al equipo informático, y el 25.00% indico que Sí

Tabla 6 : Cambio de contraseñas

Distribución de frecuencias y respuestas relacionadas con el cambio de contraseñas respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	03	37.50
NO	05	62.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Conoce cómo cambiar la contraseña en los sistemas que usa en la empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

.

En la tabla 6 se puede observar que el 62.50% de los trabajadores No conoce cómo cambiar la contraseña en los sistemas que usa en la empresa BROZZANDII PASTELERIA S.A.C, y el 37,50% indico que Sí.

Tabla 7: Clave de acceso

Distribución de frecuencias y respuestas relacionadas con la clave de acceso respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	01	12.50
NO	07	87.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Le han cambiado clave de acceso al, correo de la empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

En la tabla 7 se puede observar que el 87.50% de los trabajadores No le han cambiado clave de acceso al, correo de la empresa BROZZANDII PASTELERIA S.A.C. y el 12,50% indico que Sí.

Tabla 8 : Compartir clave de correo

Distribución de frecuencias y respuestas relacionadas con el compartir clave de correo respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	05	62.50
NO	03	37.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Comparte la clave del correo empresarial con alguien más de la empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

.

En la tabla 8 se puede observar que el 62.50% de los trabajadores Si comparten la clave del correo empresarial con alguien más de la empresa BROZZANDII PASTELERIA S.A.C., y el 37,50% indico que No.

Tabla 9: Seguridad de la información

Distribución de frecuencias y respuestas relacionadas con la seguridad de la información respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	03	37.50
NO	05	62.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Sabe de qué se trata la seguridad de la información en la empresa?

Aplicado por Seminario R.; 2022.

.

En la tabla 9 se puede observar que el 62.50% de los trabajadores No sabe de qué se trata la seguridad de la información en la empresa, y el 37,50% indico que No.

Tabla 10 : Normas ISO 27000

Distribución de frecuencias y respuestas relacionadas con las normas ISO 27000 respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	01	12.50
NO	07	87.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Sabes que son las normas ISO 27000?

Aplicado por Seminario R.; 2022.

En la tabla 10 se puede observar que el 12.50% de los trabajadores No saben qué son las normas ISO 27000, y el 87,50% indico que No.

Tabla 11 : Normas ISO 27001

Distribución de frecuencias y respuestas relacionadas con las normas ISO 27001 respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	06	75.00
NO	02	25.00
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Te gustaría saber qué es y cómo utilizar la norma ISO 27001?

Aplicado por Seminario R.; 2022.

.

En la tabla 11 se puede observar que al 75.00% de los trabajadores Si les gustaría saber qué es y cómo utilizar la norma ISO 27001, y el 25,00% indico que No.

Tabla 12: Información importante de la empresa

Distribución de frecuencias y respuestas relacionadas con Información importante de la empresa respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	05	62.50
NO	03	37.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Sabe qué tipo de información importante se genera en la empresa BROZZANDII PASTELERIA S.A.C., que deba protegerse?

Aplicado por Seminario R.; 2022.

.

En la tabla 12 se puede observar que el 62.50% de los trabajadores Si sabe qué tipo de información importante se genera en la empresa BROZZANDII PASTELERIA S.A.C., que deba protegerse, y el 37,50% indico que No.

4.2 DIMENCION 02: Nivel de protección de los procesos de información

Tabla 13: Resguardo información digital

Distribución de frecuencias y respuestas relacionadas con el resguardo de la información digital, respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	06	75.00
NO	02	25.00
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Considera que debe ser resguardada la cantidad de información digital que genera la empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

.

En la tabla 13 se puede observar que el 75.00% de los trabajadores Si considera que debe ser resguardada la cantidad de información digital que genera la empresa BROZZANDII PASTELERIA S.A.C., y el 25,00% indico que No.

Tabla 14 : Inspecciones periódicas a los equipos Informáticos

Distribución de frecuencias y respuestas relacionadas con Inspecciones periódicas a los equipos Informáticos, respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	01	12.50
NO	07	87.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Realiza periódicamente inspecciones a los equipos informáticos la Empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

.

En la tabla 14 se puede observar que el 87.50% de los trabajadores No realiza periódicamente inspecciones a los equipos informáticos la Empresa BROZZANDII PASTELERIA S.A.C., y el 12,50% indico que Si.

Tabla 15: Actualización de Sistemas Informáticos

Distribución de frecuencias y respuestas relacionadas con Actualización de Sistemas Informáticos, respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	02	25.00
NO	06	75.00
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Se actualiza en relación a las nuevas condiciones de los sistemas informáticos la Empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

.

En la tabla 15 se puede observar que el 75.00% de los trabajadores No se actualiza en relación a las nuevas condiciones de los sistemas informáticos la Empresa BROZZANDII PASTELERIA S.A.C., y el 25,00% indico que Si.

Tabla 16 : Mantenimiento de los equipos informáticos

Distribución de frecuencias y respuestas relacionadas con el mantenimiento de los equipos informáticos, respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	01	12.50
NO	07	87.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Tiene un programa de mantenimiento de los equipos informáticos la empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

En la tabla 16 se puede observar que el 87.50% de los trabajadores No tiene un programa de mantenimiento de los equipos informáticos la empresa BROZZANDII PASTELERIA S.A.C., y el 12.50% indico que Si.

Tabla 17 : Historial de los mantenimientos y sus fallas

Distribución de frecuencias y respuestas relacionadas con historial de los mantenimientos y sus fallas, respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	01	12.50
NO	07	87.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Hay un historial de los mantenimientos y sus fallas de la empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

.

En la tabla 17 se puede observar que el 87.50% de los trabajadores No hay un historial de los mantenimientos y sus fallas de la empresa BROZZANDII PASTELERIA S.A.C. y el 12.50% indico que Si.

Tabla 18 : Continuidad de sistemas de información

Distribución de frecuencias y respuestas relacionadas con continuidad de sistemas de información, respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	02	25.00
NO	06	75.00
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Evalúa el nivel de continuidad de sus sistemas de información la Empresa BROZZABDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

En la tabla 18 se puede observar que el 75.00% de los trabajadores No evalúa el nivel de continuidad de sus sistemas de información la Empresa BROZZABDII PASTELERIA S.A.C., y el 25.00% indico que Si.

Tabla 19: Control de continuidad de la información

Distribución de frecuencias y respuestas relacionadas con controles de continuidad de la información, respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	01	12.50
NO	07	87.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Verifica periódicamente los controles de continuidad de la información establecidos la empresa BROZZANDII PASTELERIA SAC?

Aplicado por Seminario R.; 2022.

En la tabla 19 se puede observar que el 87.50% de los trabajadores No verifica periódicamente los controles de continuidad de la información establecidos la empresa BROZZANDII PASTELERIA SAC?, y el 12.50% indico que Si.

Tabla 20: Disponibilidad, integridad y confidencialidad

Distribución de frecuencias y respuestas relacionadas con disponibilidad, integridad y confidencialidad respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	03	37.50
NO	05	62.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿A identificado algún tipo de riesgo que pudiera afectar la disponibilidad, integridad y confidencialidad de los sistemas de información y de su infraestructura la empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

.

En la tabla 20 se puede observar que el 62.50% de los trabajadores No ha identificado algún tipo de riesgo que pudiera afectar la disponibilidad, integridad y confidencialidad de los sistemas de información y de su infraestructura la empresa BROZZANDII PASTELERIA S.A.C., y el 37.50% indico que Si.

Tabla 21: Proceso de valoración de riesgos

Distribución de frecuencias y respuestas relacionadas con proceso de valoración de riesgos respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	01	12.50
NO	07	87.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Existe algún proceso de valoración de riesgos de la información en la Empresa BROZZANDII PASTELERIA S.A.C.?

Aplicado por Seminario R.; 2022.

.

En la tabla 21 se puede observar que el 87.50% de los trabajadores No existe algún proceso de valoración de riesgos de la información en la Empresa BROZZANDII PASTELERIA S.A.C., y el 12.50% indico que Si.

Tabla 22: Proceso de tratamiento de los riesgos

Distribución de frecuencias y respuestas relacionadas con Proceso de tratamiento de los riesgos respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	01	12.50
NO	07	87.50
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para responder a la pregunta: ¿Ha desarrollado algún proceso de tratamiento de los riesgos de su información la EMPRESA BROZZANDII PASTELERÍA S.A.C.

Aplicado por Seminario R.; 2022.

.

En la tabla 22 se puede observar que el 87.50% de los trabajadores No existe algún proceso de valoración de riesgos de la información en la Empresa BROZZANDII PASTELERIA S.A.C., y el 12.50% indico que Si.

Tabla 23: Dimensión 01, Nivel de conocimiento sobre seguridad de la información

Distribución de frecuencias y respuestas relacionadas con el nivel de conocimiento sobre seguridad de la información respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura-2022.

Alternativas	n	%
SI	01	12.50
NO	07	87.50
TOTAL	08	100.00

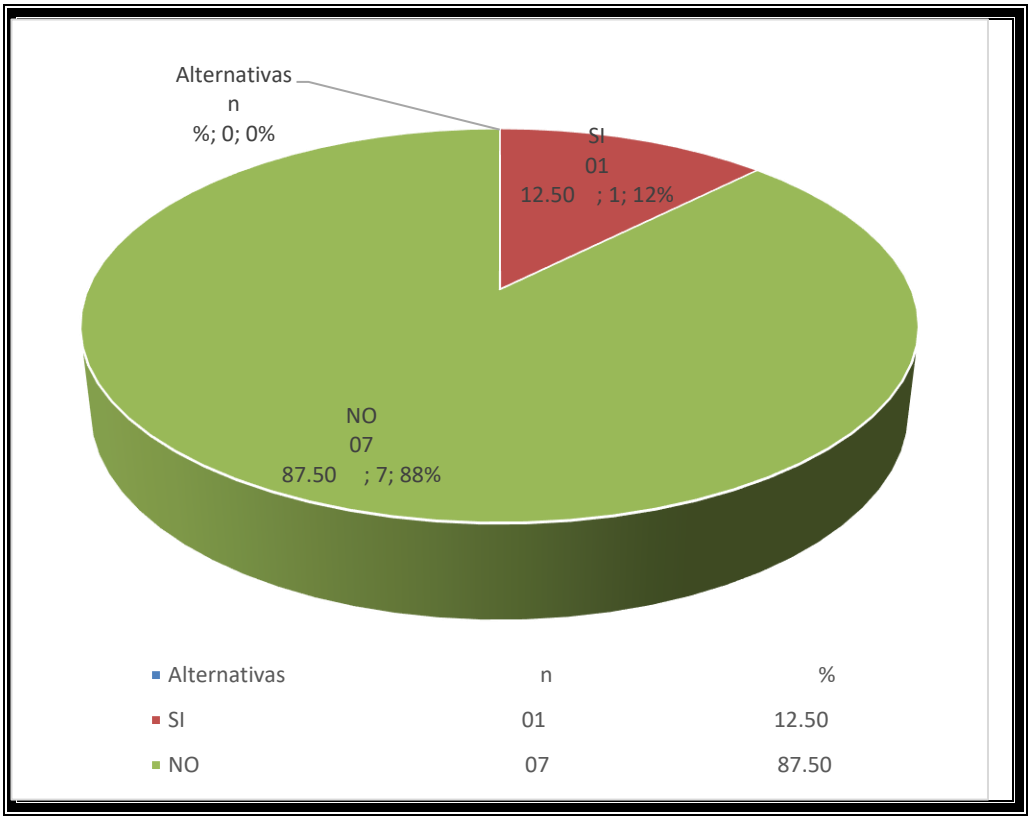
Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para medir la dimensión Nivel de conocimiento sobre seguridad de la información basados en ocho preguntas.

Aplicado por Seminario R.; 2022.

En la tabla 23 se puede observar que el 87.50% de los trabajadores No tiene el nivel de conocimiento sobre seguridad de la información en la Empresa BROZZANDII PASTELERIA S.A.C., y el 12.50% indico que Si.

Gráfico 2: Dimensión Nivel de conocimiento sobre seguridad de la información

Distribución de frecuencias y respuestas relacionadas con la dimensión 01: Nivel de conocimiento sobre seguridad de la información, respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.



Fuente: tabla 23

Tabla 24: Dimensión 02 Nivel de protección de los procesos de información

Distribución de frecuencias y respuestas relacionadas con el nivel de protección de los procesos de información respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

Alternativas	n	%
SI	02	25.00
NO	06	75.00
TOTAL	08	100.00

Fuente: Cuestionario aplicado a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022; para medir la dimensión Nivel de protección de los procesos de información basados en diez preguntas.

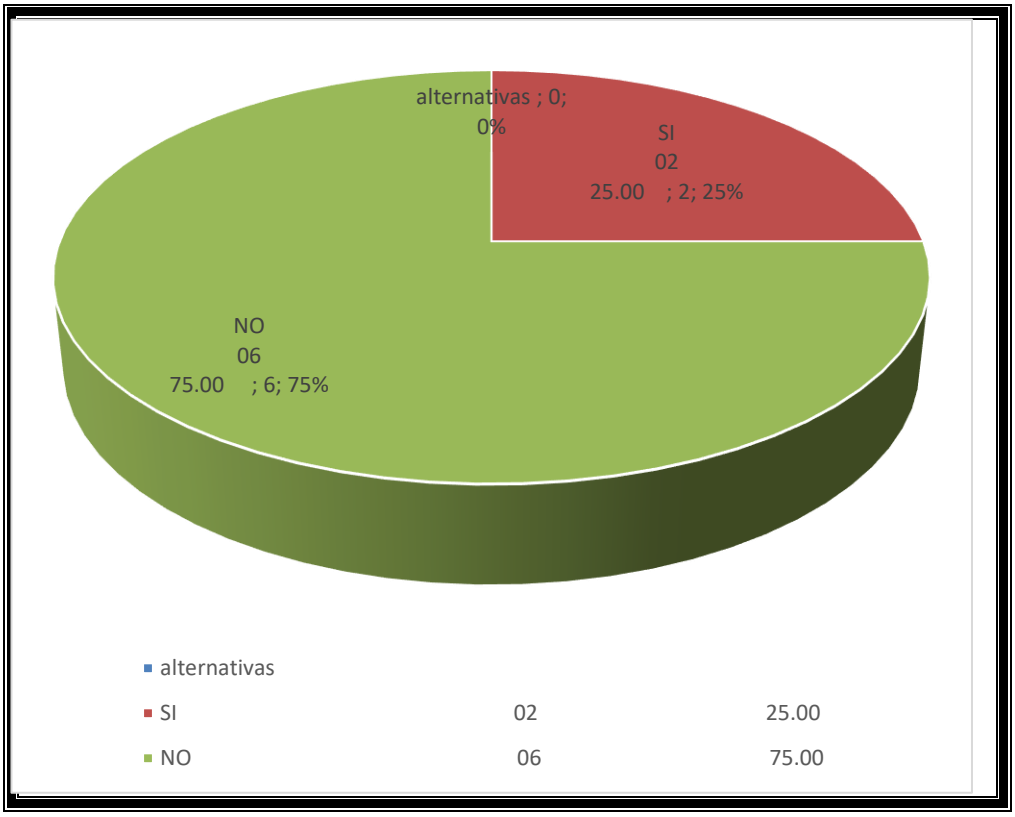
Aplicado por Seminario R.; 2022.

.

En la tabla 24 se puede observar que el 75.00% de los trabajadores indica que No tiene el nivel de protección de los procesos de información la Empresa BROZZANDII PASTELERIA S.A.C., y el 25.00% indico que Si.

Gráfico 3: Dimensión 2 Nivel de protección de los procesos de información

Distribución de frecuencias y respuestas relacionadas con la dimensión 02: Nivel de protección de los procesos de información; respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura-2022..



Fuente: Tabla 24

Tabla 25: Resumen general por dimensiones

Distribución de frecuencias y respuestas relacionadas con las dos dimensiones definidas para determinar los niveles de conocimiento sobre seguridad y de protección de los procesos respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

DIMENSIONES	ALTERNATIVAS DE RESPUESTAS			TOTAL, MUESTRA		
	SI	%	NO	%	N	%
Conocimiento sobre seguridad	1	12,50	7	87,50	8	100,00
Protección de los procesos	2	25,00	6	75,00	8	100,00

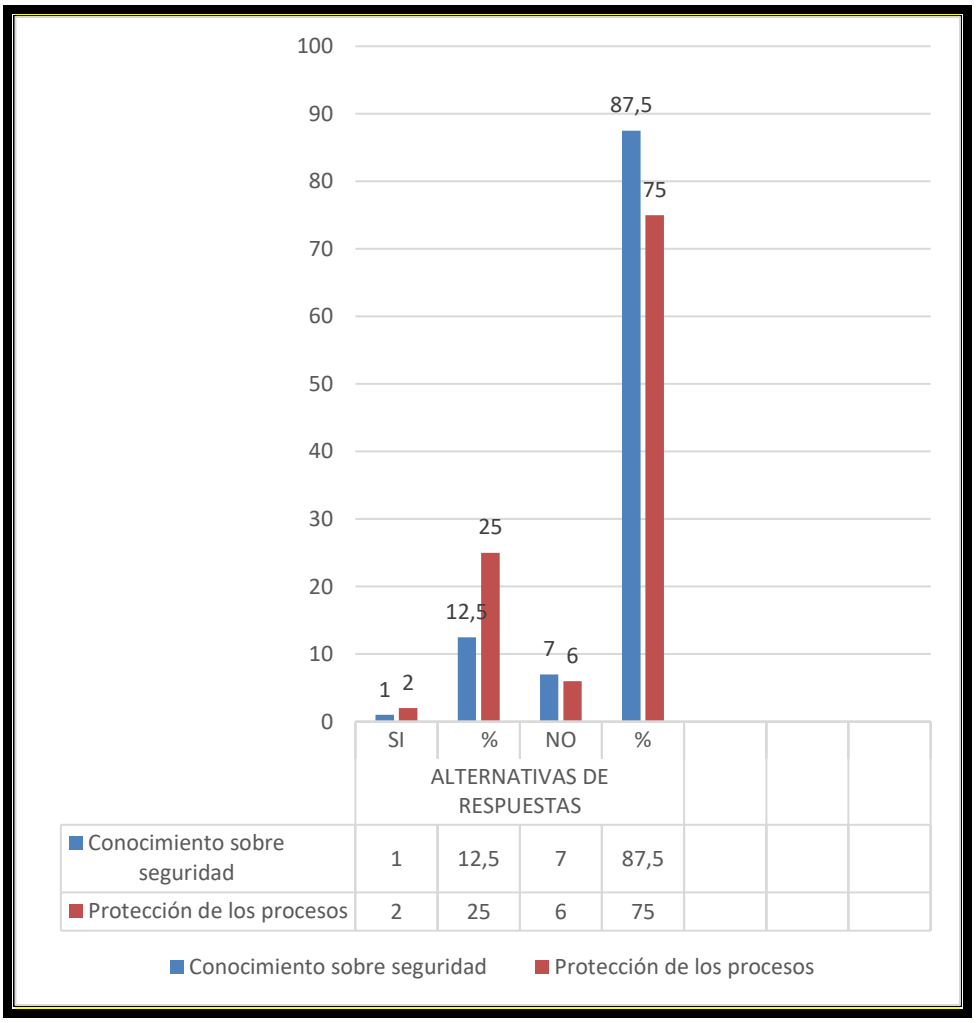
Fuente: Cuestionario aplicado sobre las dos dimensiones: Nivel de conocimiento sobre seguridad de la información y Nivel de protección de los procesos de información basado en 10 preguntas aplicados a los trabajadores involucrados en los procesos de las TIC de la Empresa BROZZANDII PASTELERIA S.A.C. 2022.

Aplicado por Seminario R.; 2022.

En la tabla 25 se puede observar que en la primera dimensión el 87.50% de los trabajadores No conoce sobre seguridad de la información, en la segunda dimensión el 75% de los trabajadores indica que No tiene protección de los procesos de información la Empresa BROZZANDII PASTELERIA S.A.C. 2022.

Gráfico 4: Resumen general por dimensiones

Distribución de frecuencias y respuestas relacionadas con las dos dimensiones definidas para determinar los niveles de conocimiento sobre seguridad y de protección de los procesos respecto a la propuesta de un plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.



Fuente: Tabla 25

4.2. Análisis de Resultados

Se aplico un cuestionario para obtener la opinión de los trabajadores involucrados encuestados referente a las dos dimensiones determinadas. La interpretación de los resultados presentados anteriormente la hacemos seguidamente:

4.2.1 En la dimensión 01: conocimiento sobre seguridad en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura en la tabla 25 podemos observar y comprender que el 87.50% de los trabajadores de la empresa BROZZANDII PASTELERÍA S.A.C. – Piura indicaron que NO tienen conocimiento sobre seguridad de la información, incluso no pasan antivirus al iniciar el día de trabajo, no saben cómo cambiar la contraseña en los sistemas que usa en la empresa, y además comparten la clave con otra persona de la empresa, por ello se opta por la opción de aprender sobre la seguridad de la información de la empresa, no obstante el 12.5% indico que SI. Estos resultados obtenidos tienen semejanza en la investigación de Merino R. (13), y en la investigación de Pangalima R. (11) así como también en la investigación de Olaya J. (10), quienes en sus exploraciones de su tesis con una dimensión parecida llegan a la conclusion de que se hace indispensable la aplicación de un plan de mejora ante la falta de conocimiento de la seguridad de la información.

4.2.2 Así mismo respecto a la dimensión 2: protección de los procesos de información en la tabla 25 se interpreta el resultado que el 75 % de los trabajadores de la empresa BROZZANDII PASTELERÍA S.A.C. – Piura, indicaron que NO tiene el nivel de protección la empresa BROZZANDII PASTELERÍA S.A.C. – Piura y por tanto se requiere de la aplicación de un plan de mejora para determinar los pasos a seguir en cuanto a la protección de los procesos de información y evitando riesgos para la empresa y por ende de sus trabajadores. Este resultado de esta investigación tiene relación o semejanza con las tesis desarrolladas por la investigación de

Merino R. (13), en la investigación de Pangalima R. (11) así como también en la investigación de Olaya J. (10), quienes en sus exploraciones dan a conocer la relación entre los riesgos en la información y la falta de conocimiento de la seguridad de la información en la empresa, así como también indican la necesidad de aplica un plan de mejora en la organización, por lo que considero que la empresa BROZZANDII PASTELERÍA S.A.C. – Piura, requiere de la implementación de un plan de mejora de la seguridad de la información basado en la ISO/IEC 27001:2013.

4.2.3. Plan de mejora .

La empresa BROZZANDII PASTELERÍA S.A.C. conociendo las posibles amenazas a sus activos, que posee ha considerado una serie de posibles salvaguardas para protegerlos, plantea la siguiente propuesta de un plan de mejora, con las políticas a cumplir en todo su accionar y por todos sus integrantes según corresponda.

El plan de mejora tiene como objetivo fundamental establecer una cultura se seguridad de la información a nivel de la empresa, y esta basado en la Norma ISO/IEC 27001- 2013., y en los activos inherentes a la empresa, así como el tipo de amenazas, y de las salvaguardas que inciden en la empresa BROZZANDII PASTELERÍA S.A.C. y mitigar los riesgos(31) inherentes a la información.

A continuación, el plan:

PLAN DE MEJORA DE LA SEGURIDAD DE LA INFORMACION DE LA EMPRESA BROZZANDII PASTELERIA S.A.C. PIURA 2022.

A.- Objetivo del Plan de mejora:

Establecer una cultura se seguridad de la información a nivel de la empresa BROZZANDII PASTELERIA S.A.C.

B.- Bases:

1.- Norma ISO/IEC 27001-2013.

2.- Activos de la empresa, amenazas existentes y salvaguardas de

protección.

Tabla 26: Activos de la Empresa (32) BROZZANDII PASTELERIA S.A.C.	
I	ACTIVOS ESENCIALES
1	[pub] de carácter público
2	(service) servicio
II	ARQUITECTURA DEL SISTEMA
3	[sap] punto de [acceso al] servicio
III	DATOS/INFORMACIÓN
4	[backup] copias de respaldo
5	[password] credenciales (ej. contraseñas)
6	[log] registro de actividad
IV	CLAVES CRIPTOGRÁFICAS
7	[info] protección de la información
V	SERVICIOS
8	[www] world wide web
9	[email] correo electrónico
VI	SOFTWARES
10	[office] ofimática
11	[av] anti virus
12	[os] sistema operativo
VII	EQUIPAMIENTO INFORMÁTICO (HARDWARE)
13	[pc] informática personal
14	[mobile] informática móvil
15	medios de impresión
16	[modem] módems
VIII	REDES DE COMUNICACIÓN
17	[PSTN] red telefónica
18	[mobile] telefonía móvil
19	[Internet] Internet
IX	SOPORTES DE INFORMACIÓN
20	[disk] discos duros externos
21	[cd] cederrón (CD-ROM)
22	[usb] memorias USB
X	EQUIPAMIENTO AUXILIAR
23	[furniture] mobiliario: armarios, etc
XI	INSTALACIONES
24	local] cuarto
XII	PERSONAL
25	[ue] usuarios externos
26	[prov] proveedores
XII	PERSONAL
25	[ue] usuarios externos
26	[prov] proveedores

Tabla 27: Amenazas a la información de la Empresa BROZZANDII PASTELERIA S.A.C.			
N°	Amenaza	Activos	Dimensiones
1	or fuego - Incendio	HW)Equipos informáticos (hardware)	isponibilidad
2	or agua - Perjuicios ocasionados por el agua	HW)Equipos informáticos (hardware)	isponibilidad
3	esastres naturales - Fenómeno sísmico	HW)Equipos informáticos (hardware)	isponibilidad
4	ontaminación mecánica - contaminación	HW)Equipos informáticos (hardware)	isponibilidad
5	vería física o lógica -Avería del hardware	HW)Equipos informáticos (hardware)	isponibilidad
6	orte de suministro eléctrico - perdida de suministro	HW)Equipos informáticos (hardware)	isponibilidad
7	allas en la climatización	HW)Equipos informáticos (hardware)	isponibilidad
8	alla de funcionamiento del hardware	HW)Equipos informáticos (hardware)	isponibilidad
9	rrores y fallos no intencionados- Errores de los suarios	[D] datos / información [S] servicios	ntegridad, Confidencialidad y isponibilidad
10	rrores del administrador – error de uso	[D] datos / información [S] servicios	ntegridad, Confidencialidad y isponibilidad
11	rrores de configuración	D.conf] datos de configuración	isponibilidad
12	eficiencias en la organización	P] personal	
13	ifusión de software dañino	SW] aplicaciones (software)	ntegridad, Confidencialidad y isponibilidad
14	lteración accidental de la información	[D] datos / información [S] servicios [SW] aplicaciones (SW)	ntegridad
15	ugas de información	[D] datos / información [SW] aplicaciones (SW) [P] personal (revelación)	onfidencialidad
16	rrores de mantenimiento	HW)Equipos informáticos (hardware)	isponibilidad
17	erdida de equipos	[HW] equipos informáticos (hardware) [Media] soportes de información	isponibilidad y confidencialidad
18	ndisponibilidad del personal	[P] personal interno	isponibilidad
19	taques intencionados – manipulación de registros e actividad	[D.log] registros de actividad	ntegridad
20	buso de privilegios de acceso	[D] datos / información [S] servicios	Integridad, confidencialidad y disponibilidad.

		[SW] aplicaciones (software) [HW] equipos informáticos (hardware)	
21	Manipulación de programas - alteración	[SW] aplicaciones (software)	Integridad, confidencialidad y disponibilidad.
22	Manipulación de los equipos	[HW] equipos	Confidencialidad y disponibilidad
23	Robo - robode hardware	[HW] equipos informáticos (hardware)	Confidencialidad y disponibilidad

Tabla 28: Correlación amenazas- errores a la Empresa BROZZANDII PASTELERIA S.A.C.		
N°	Error	Ataque
1	Errores de los usuarios	
2	Errores del Administrador	
3	Errores de monitorización	Manipulación de los registros de actividad
4	Errores de configuración	Manipulación de la configuración
		Suplantación de la identidad del usuario
		Abuso de privilegios de acceso
5	Difusión de software dañino	Difusión de software dañino
6	Errores de secuencia	Alteración de secuencia
		Acceso no autorizado
		Análisis de tráfico
7	Alteración accidental de la información	Modificación deliberada de la información
8	Destrucción de información	Destrucción de información
9	Fugas de información	Revelación de información
		Manipulación de programas
10	Errores de mantenimiento / actualización de equipos (hardware)	Manipulación de los equipos
11	Caída del sistema por agotamiento de recursos	Denegación de servicio
12	Pérdida de equipos	Robo
		Ataque destructivo
		Ocupación enemiga
13	Indisponibilidad del personal	Indisponibilidad del personal

Tabla 29: Salvaguardas de Empresa BROZZANDII PASTELERIA S.A.C.		
I		Generales
1	H	Protecciones Generales
2	H. IA	Identificación y autenticación
3	H.tools.SFV	Verificación de las funciones de seguridad
II		Protección de los datos / información
4	D	Protección de la Información
5	D.A	Copias de seguridad de los datos (backup)
6	D.I	Aseguramiento de la integridad
7	D.DS	Uso de firmas electrónicas
III		Protección de los servicios
8	S. email	Protección del correo electrónico
9	S.www	Protección de servicios y aplicaciones web
IV		Protección de las aplicaciones (software)
10	SW	Protección de las Aplicaciones Informáticas
V		Protección de los equipos (hardware)
11	HW	Protección de los Equipos Informáticos
12	HW.SC	Se aplican perfiles de seguridad
VI		Protección de las comunicaciones
13	COM	Protección de las Comunicaciones
14	COM.I	Protección de la integridad de los datos intercambiados
VII		Seguridad física-Protección de las instalaciones
15	L	Protección de las Instalaciones
16	L.AC	Control de los accesos físicos
VIII		Salvaguardas relativas al personal
17	PS	Gestión del Personal
18	PS.AT	Formación y concienciación
IX		Salvaguardas de tipo organizativo
19	G.RM	Gestión de riesgos
20	G. plan	Planificación de la seguridad
X		Continuidad de operaciones
21		Prevención y reacción frente a desastres
22	BC	Continuidad del negocio

C.- POLITICAS DE ACCIÓN DEL PLAN DE MEJORA EN SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA "BROZZANDII PASTELERÍA S.A.C

Estas políticas(33), presentadas a continuación se han desarrollado en relación a la administración, flujo y mantenimiento de la información y las bases de datos de la empresa "BROZZANDII PASTELERÍA S.A.C" rubro pastelería.

El desarrollo de las Políticas del presente plan de seguridad de la información se orienta hacia la confidencialidad, integridad y disponibilidad de la información en los siguientes dominios:

- Clasificación y control de activos de información
- Seguridad física y ambiental
- Control de accesos
- Adquisición, Desarrollo y Mantenimiento de sistemas de información
- Gestión de Continuidad del Negocio

Como el objetivo de la empresa BROZZANDII PASTELERÍA S.A.C. es brindar un servicio de calidad a sus clientes y asimismo más del 95% de estos clientes son contactados a través de internet con su pág. web, y contactos por intermedio de la computadora, además del correo de la empresa, se hace necesario y de mucha urgencia la aplicación a toda la organización de estas políticas del plan de mejora que se maneje con controles de seguridad informática, dado que existen muchas amenazas en las redes y si además agregamos la falta de conocimiento de seguridad de la información y por ende la falta de protección a los procesos de información podríamos estar muy pronto en serios problemas.

En relación a los dominios antes indicados tenemos la siguiente tabla 30 de las políticas del plan de mejora de la seguridad de la información para la empresa BROZZANDII PASTELERÍA S.A.C.

Tabla 30: PLAN DE MEJORA DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA BROZZANDII PASTELERIA S.A.C.		
N°	**Dominio**	**Política**
1	Clasificación y control de activos de información	La empresa BROZZANDII PASTELERIA S.A.C., es el propietario de todos los activos de información de la organización, y delega la responsabilidad de los mismos a cada gerente de area quienes a su vez controlaran con todo su personal.
2		Los usuarios deberán adecuarse a la normativa del uso adecuado de los activos de información.
3		Cada gerente coordinara y controlara el buen uso y protección de los activos de información dados a su personal.
4		Ningún usuario deberá realizar actividades no autorizadas que puedan vulnerar la seguridad de los activos, bajo sanción.
5	Seguridad física y ambiental	Las áreas de procesamiento de información deberán ser areas de acceso restringido y limitado.
6		Los visitantes o proveedores que ingresen a areas restringidas deberán ser visiblemente identificables.
7		Toda oficina que se encuentre sin personal deberá ser cerrada hasta que venga el encargado

8		Los directorios internos ligados a los recursos de información reservada no serán accesibles a personas ajenas a la empresa.
9		En el escritorio no debe quedar información en documentos, ni USB u otro material, ya sea momentánea o al finalizar jornada.
10		Todo material peligroso e inflamable debe almacenarse lejos de las areas de manejo de la información.
11		La información de respaldo deberá estar ubicada lejos de las areas de los equipos principales.
12		Se instalarán los equipos de procesamiento de información crítica en áreas de acceso limitado o restringido.
13		Los equipos instalados en ubicaciones restringidas contarán con protectores que impidan ser trasladados sin autorización.
14		Se dará a conocer las condiciones ambientales para los equipos como temperatura y humedad que puedan afectarlo.
15		Todo equipo para su conexión remota, se someterá a evaluación de riesgos.
16	Control de accesos	Se utilizará la normativa de accesos lógicos para los registros de usuarios y cuentas

17		Cada usuario tendrá su identidad y contraseña propias
18		Para el personal que haya concluido su labor en la empresa será retirada los usuarios y contraseñas
19		La contraseña del correo es personal
20		Las contraseñas se cambiarán periódicamente según acuerdo de la empresa
21		La contraseña será secreta y no se compartirá con nadie
22		A los usuarios con privilegios se les revisara con mayor frecuencia
23		Si se deja sin actividad los equipos el usuario debe inactivarlo hasta que vuelva a usarlo
24		Al termino de la jornada laboral o ausentarse de la oficina se deberá bloquear la pantalla
25	Adquisición, Desarrollo y Mantenimiento de sistemas de información	Se tendrá restricciones para mitigar el riesgo por fallas en los sistemas de información, permitiendo su recuperación y solución del problema.
26		Se utilizará escaneo de medios de comunicaciones y salida, así como monitoreo regular de las actividades del sistema y también del personal, además del monitoreo para el uso de los recursos informáticos
27	Gestión de Continuidad del Negocio	Se tendrá identificado todo evento que cause o pueda causar interrupciones a los procesos de negocios y para la seguridad de la información

28		Se evaluarán los riesgos y los eventos identificados para la continuidad del plan de negocio.
29		Se guardará como respaldo y restauración la información de la empresa en otra ubicación en caso de contingencia
30		Si fuera necesario se realizarán procedimientos temporales de reanudación de operaciones

BENEFICIOS A CORTO Y LARGO PLAZO DE LA APLICACIÓN DE LAS POLÍTICAS DEL PLAN DE MEJORA EN SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA BROZZANDII PASTELERIA S.A.C.

Entre los más destacados tenemos:

1. Reducción de riesgos de perdida de información para la empresa
2. Incorporación de una metodología clara para gestionar la seguridad
3. Implantación de medidas de seguridad para la empresa y sus clientes
4. Identificación y registro de incidencias para una mejora continua de la seguridad en la organización
5. Garantizar seguridad ante el cliente y los socios
6. Planes de contingencia para seguir operando con normalidad ante un incidente de seguridad
7. Ventaja competitiva frente a sus clientes, incrementando su imagen a través de un entorno seguro
8. Permitir la certificación en la norma internacional 27001 en cuanto a seguridad se refiere.
9. Se logrará un cambio cultural al respecto del comportamiento del personal en el desarrollo de las actividades de la empresa.

.

V. Conclusiones

1. Se logro determinar los activos de la empresa BROZZANDII PASTELERIA S.A.C., analizando las diversas características del accionar de la empresa, con esto se aporta el poder canalizar por medio de ellos, las políticas de acción, y el valor agregado se constituye porque ahora la empresa sabe cuáles son sus activos, los cuales tiene que cuidar y preservar, a través del plan de mejora de la seguridad de la información.

2. Se reconoció las amenazas a las que está expuesta la empresa BROZZANDII PASTELERÍA S.A.C. tomando en consideración los activos ya determinados aportando esto al desarrollo del plan de mejora de la seguridad informática de la empresa. El valor agregado de reconocer las amenazas, esta dado por que permite la oportunidad de proteger a la empresa

3. Se identifico las principales salvaguardas en la empresa BROZZANDII PASTELERÍA S.A.C. las cuales permiten proteger la seguridad de la información de la empresa aportando con ello la solución a las amenazas contra los activos de la empresa y el valor agregado de encontrar las salvaguardas, se constituye en el motivo y parámetro para desarrollar las políticas del plan de mejora de la seguridad informática de la empresa

   Se logro realizar la propuesta de un plan de mejora de la seguridad de la información, para la empresa BROZZANDII PASTELERIA S.A.C., 2022 basado en la ISO/IEC 27001: 2013, aportando conjuntamente con el conocimiento de los activos, amenazas y salvaguardas ya encontradas para la empresa, y el valor agregado está constituido por las políticas desarrolladas en la tabla 30 del plan de mejora de la seguridad de la información de la empresa.

Recomendaciones

1. Se sugiere a los directivos de la empresa BROZZANDII PASTELERIA S.A.C., que periódicamente capacite a su personal sobre seguridad de la información para su empresa.

2. Se hace la sugerencia a que este plan desarrollado para su representada sea aplicado varias veces a manera de practica para lograr eficiencia en la gestión de todas las actividades de la empresa.

3. Se recomienda realizar un análisis de la empresa en relación a sus activos para que todo el personal tome conciencia de sus activos y a su vez los pueda proteger.

Referencias Bibliográficas

1. Unila. “Porque es Importante la seguridad informática en las empresas”. Marzo – 2022. Universidad Latina.

   https://www.unila.edu.mx/por-que-es-importante-seguridad-informatica/#:~:text=La%20importantes%20de%20la%20seguridad,los%20sistemas%20de%20informaci%C3%B3n%20internos.

2. Movistar. La conectividad como facilitador de soluciones IoT- Negocio por internet 2018.
   https://negociosdigitalesmovistar.com/negocio-por-internet/conectividad-soluciones-iot/.

3. Asturias M, Retos a la seguridad en la transformación digital. 2022. IDEAS Revista UNO.

   https://www.revista-uno.com/31-revista-uno-hiperconectados-hipervulnerables/retos-a-la-seguridad-en-la-transformacion-digital/

4. Arévalo F. . Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos Universidad de Cuenca Ecuador.2017

5. Amoguimba, D. “Propuesta de políticas de seguridad de la información aplicado al entorno empresarial del Soft Warehouse, Pontificia Universidad Católica del Ecuador, 2018.

6. Ulloa, J. “Análisis de problemas técnicos y legales de ciberseguridad y sus posibles soluciones en el contexto de la computación en la nube” De la Pontificia Universidad Católica del Ecuador. 2021.

7. Aliaga, Ch. Implementación de un Sistema de Ciberseguridad para la prevención de los ataques cibernéticos en la Empresa Radiadores Fortaleza.2021.

8. Calderón J. Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del ministerio de Educación, Universidad Cesar Vallejo Lima Perú. 2018

9. Calderón, TLH., Gestión de riesgos y seguridad de la información del Programa Fortalece Perú del MTPE. 2019

10. Olaya, J. Gestión del Sistema de Seguridad de Información bajo el enfoque de ISO 27001 en la Municipalidad Provincial de Tumbes". 2017.

11. Pangalima, R. "Auditoria Basada en COBIT 4.1 para el uso óptimo de las TIC y la seguridad Informática en la Empresa ARCOPA S.A. Paita. 2018

12. Lara, K. en su tesis "Propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la clínica Simedic diagnóstica S.A.C – Piura. 2018.

13. Merino, C. "Diagnóstico de la seguridad informática utilizando la norma ISO/IEC 27001 de la empresa Ransa comercial S.A- Piura. 2021

.

14. Ancajima, M. "Propuesta de implementación de seguridad informática en las tic de la i.e. san miguel arcángel, Catacaos - Piura. 2016.

15. Brozzandii. Pastelería, Sociedad Anónima Cerrada (2018) https://www.universidadperu.com/empresas/brozzandii-pasteleria.php

16. Portal del Instituto de Ingeniería, UNAM. 2018. http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/seguridadinformatica.aspx

17. Seguridad de la Información, "Cuales son los requisitos de seguridad" Especializado en Seguridad de la Información y Ciberseguridad. Blog editado por ISOTools Excellence 2017. ISO 27001 ¿Cuáles son los requisitos de seguridad? (pmg-ssi.com)

18. Gonzales Y. Seguridad de la Información, Plan de seguridad informática. CRC corporación Autónoma DEL Cauca – Colombia.2018. https://web2018.crc.gov.co/index.php/corporativo/gestion-institucional/planea-ción -gestion-y-control/planes-estrategicos/plan-de-seguridad-informatica-2017 - 2019

19. ISO 27001 - Sistema de Gestión de Seguridad de la Información 2018 https://www.dnv.com/ar/services/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-3327#.

20. Academy 27001 Herramientas gratuitas creadas para facilitar la implementación de ISO 27001 e ISO 22301. 2018. https://advisera.com/27001academy/es/herramientas/.

21. Conformio ISO 27001, Software para implementación y manejo de ISO 27001, 2018. https://advisera.com/conformio/

22. Rasinger S. La investigación cuantitativa en lingüística: Una introducción - Sebastián Rasinger - Google Libros [Internet]. 2da ed. AKAL E, editor. Madrid; 2020 [cited 2021 Apr 24]. Available from: https://books.google.com.pe/books?id=0h4EEAAAQBAJ&printsec=frontcover&dq=investigacion+cuantitativa&hl=es-419&sa=X&ved=2ahUKEwjtkfHYh5jwAhWnqpUCHbt6DyEQ6AEwAHoECAAQAg#v=onepage&q&f=false

23. Hernández A, Ramos M, Indacochea I, Plascencia B y otros. Metodología De La Investigación Científica [Internet]. 1era ed. 3Ciencias, editor. Ecuador; 2018 [cited 2021 May 6]. Available from https://books.google.com.pe/books?id=y3NKDwAAQBAJ&printsec=frontcover&dq=investigacion+descriptiva&hl=es-419&sa=X&ved=2ahUKEwiOh9nP37XwAhWQpJUCHQo8Aq8Q6AEwBHoECAEQAg#v=onepage&q&f=false

24. Heinemann K. Introducción A La Metodología De La Investigación Empírica En Las Ciencias [Internet]. Pidotribo, editor. Barcelona; 2003 [cited 2021 Apr 26]. Available from https://books.google.com.pe/books?id=bjJYAButfB4C&pg=PA176&dq=investigacion+de+corte+transversal&hl=es-419&sa=X&ved=2ahUKEwjCzOCSrJ3wAhXcqZUCHcdoAyAQ6AEwAHoECAQQAg#v=onepage&q=investigacion de corte transversal&f=false

25. Díaz V. Metodología de la investigación científica y bioestadística [Internet]. RIL, editor. chile; 2006 [cited 2021 Apr 27]. Available from: https://books.google.com.pe/books?id=KfscYYsconYC&pg=PA276&dq=que+es+el+universo+en+la+investigacion+cientifica&hl=es-419&sa=X&ved=2ahUKEwi1y8j625_wAhW2ppUCHQDwAyoQ6AEwB3oECAgQAg#v=onepage&q=que es el universo en la investigacion cientifica&f=false

26. . Fuente salz C, Icart M, Pulpón A. Elaboración y presentación de un proyecto de investigación y una tesina [Internet]. 1era ed. Edicions Universitat Barcelona, editor. Barcelona; 2011 [cited 2021 Apr 26]. Available from: https://books.google.com.pe/books?id=5CWKWi3woi8C&pg=PA55&dq=la+poblacion+y+la+muestra&hl=es-419&sa=X&ved=2ahUKEwiYqr7Fup3wAhWcpZUCHSL5CmIQ6AEwAnoECAAQAg#v=onepage&q=la población y la muestra&f=false

27. Aguirre M. Plan de mejora de la seguridad de información, empresa B blanco Safi Lima Perú, piso 8 Torre el pilar del centro comercial camino real San Isidro.2019 https://www.smv.gob.pe/ConsultasP8/temp/Plan%20de%20Seguridad%20de%20la%20Informaci%c3%b3n.pdf

28. Katz M, Seid G y Abiuso F , Metodología de la investigación cuaderno de catdra Nro 7 carrera de sociología UBA 2019.. http://metodologiadelainvestigacion.sociales.uba.ar/wp-content/uploads/sites/117/2019/03/Cuaderno-N-7-La-t%C3%A9cnica-de-encuesta.pdf

29. Diaz L. Método de la observación., textos de apoyo, Facultad de Psicología Universidad Nacional de México UNAM. 2011 http://www.psicologia.unam.mx/documentos/pdf/publicaciones/La_observacion_Lidia_Diaz_Sanjuan_Texto_Apoyo_Didactico_Metodo_Clinico_3_Sem.pdf

30. Bravo T. y Valenzuela S. Desarrollo de instrumentos de evaluación: cuestionarios © Centro de Medición MIDE UC, Chile, y © Instituto Nacional para la Evaluación de la Educación INEE Ciudad de México. Editora María Rosa García González, MIDE UC, Chile, 2019. https://www.inee.edu.mx/wp-content/uploads/2019/08/P2A355.pdf

31 Magerit libro III versión 3.0, metodología de análisis y gestión de riesgos de los sistemas de información, Guía de técnicas. Gobierno de España, ministerio de hacienda secretaria de estado.2012,

32 Magerit libro II versión 3.0, metodología de análisis y gestión de riesgos de los sistemas de información, Catalogo de elementos. Gobierno de España, ministerio de hacienda secretaria de estado.2012.

33 Magerit libro I versión 3.0, metodología de análisis y gestión de riesgos de los sistemas de información, Método. Gobierno de España, ministerio de hacienda secretaria de estado.2012,

ANEXOS
Anexo I: Cronograma de actividades

Rafael Asuncion Seminario Vasquez

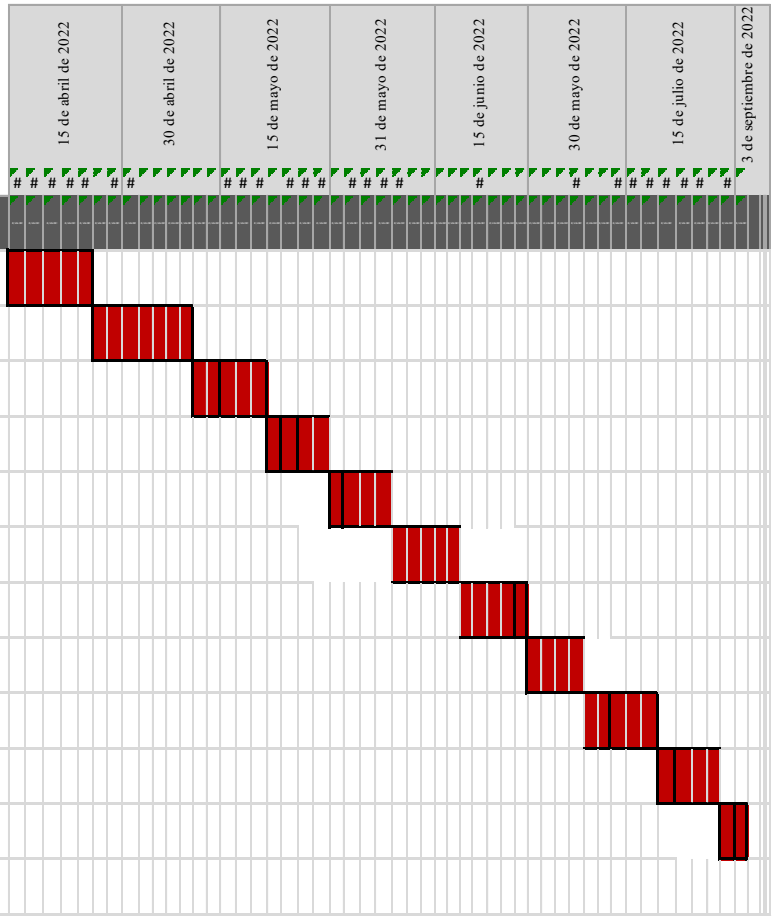
Inicio del proyecto: 4/15/2022

8

GRÁFICO GANTT SIMPLE de Vertex42.com

https://www.vertex42.com/ExcelTemplates/simple-gantt-chart.html

TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
PLANEAMIENTO DE LA INVESTI	Rafael Seminario Vasquez		15-4-22	30-4-22
REVISION DE LA LITERATURA			1-5-22	27-5-22
MEJORA DE LA METODOLOGIA			28-5-22	12-6-22
ANALISIS DE RESULTADOS			13-6-22	30-6-22
CONCLUSIONES Y RECOMENDACIONES			1-7-22	12-7-22
ANTECEDENTES DE LA INVESTIGACION			12-7-22	22-7-22
REDACCION DEL ARTICULO CIENTIFICO			23-7-22	1-8-22
INFORME FINAL			2-8-22	11-8-22
PREBANCA			12-8-22	21-8-22
LEVANTAMIENTO DE OBSERVACIONES			21-8-22	30-8-22
SUSTENTACION FINAL			30-8-22	3-9-22



Anexo II: Presupuesto desembolsable (Estudiante)			
Item	**Costo**	**Cant.**	**Total**
Bienes			
• Laptop	2000	0.1	200,00
• Mobiliario	350	0.1	35,00
• Impresora	700	0.1	700,00
Sub total			305,00
Suministros			
• Impresiones	0,20	30	6,00
• Fotocopias	0,10	30	3,00
• Papel bond A-4 (500Hojas)	25	0.5	12.50
Sub total			326,50
Servicios			
• Uso de Turnitin	50	2	100,00
Sub total			100,00
Gastos de transporte			
• Pasajes para búsqueda de información	10	3	30,00
Sub total			30,00
Total de presupuesto desembolsable por el estudiante			456,50
Presupuesto desembolsable (Universidad)			
Item	**Costo**	**Cant.**	**Total**
• Uso de Internet (Laboratorio de aprendizaje Digital - LAD)			0,00
•			
• Soporte informático (Módulo de Investigación del ERPUniversity - MOIC)			**0.00**
•			
Sub total (S/)			
Recurso humano			
•			
Sub total (S/)			**0,00**
Total de presupuesto no desembolsable (S/)			**0,00**
Total (S/)			**456,50**

Fuente: Elaboración propia.

Anexo III: CUESTIONARIO

TÍTULO: Plan de mejora de seguridad de la información basado en la ISO/IEC 27001:2013 en la empresa BROZZANDII PASTELERÍA S.A.C. – Piura- 2022.

MAESTRANTE: Seminario Vasquez, Rafael Asuncion

PRESENTACIÓN:

Este cuestionario es parte del trabajo actual de investigación; por lo que se solicita su participación, dando respuesta a cada pregunta de manera objetiva, clara y veraz. La información que Ud. Proporciona es de carácter confidencial y reservada y los resultados obtenidos de esta investigación serán utilizados para fines académicos y de investigación científica.

INSTRUCCIONES:

Presento ante usted a continuación, un listado de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa ("X") en el recuadro correspondiente (SI o NO) según así lo considere:

Favor de leer y marcar las preguntas propuestas **(Marque con un aspa SI o NO):**

Dimensión 1: NIVEL DE CONOCIMIENTO SOBRE SEGURIDAD DE LA INFORMACION			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Conoce cómo realizar el análisis con antivirus a todos sus dispositivos de almacenamiento que ha de conectar al equipo informático al iniciar sus labores del día?		
2	¿Conoce cómo cambiar la contraseña en los sistemas que usa en la empresa BROZZANDII PASTELERIA S.A.C.?		
3	¿Le han cambiado clave de acceso al, correo de la empresa BROZZANDII PASTELERIA S.A.C.?		
4	¿Comparte la clave del correo empresarial con alguien más de la empresa BROZZANDII PASTELERIA S.A.C.?		
5	¿Sabe de qué se trata la seguridad de la información en la empresa?		
6	Sabes que son las normas ISO 27000?		
7	¿Te gustaría saber qué es y cómo utilizar la norma ISO 27001?		

8	¿Sabe qué tipo de información importante se genera en la empresa BROZZANDII PASTELERIA S.A.C., que deba protegerse?		
Dimensión 2: DE PROTECCION DE LOS PROCESOS DE INFORMACION			
1	¿Considera que debe ser resguardada la cantidad de información digital que genera la empresa BROZZANDII PASTELERIA S.A.C.?		
2	¿Realiza periódicamente inspecciones a los equipos informáticos la Empresa BROZZANDII PASTELERIA S.A.C.?		
3	¿Se actualiza en relación a las nuevas condiciones de los sistemas informáticos la Empresa BROZZANDII PASTELERIA S.A.C.?		
4	¿Tiene un programa de mantenimiento de los equipos informáticos la empresa BROZZANDII PASTELERIA S.A.C.?		
5	¿Hay un historial de los mantenimientos y sus fallas de la empresa BROZZANDII PASTELERIA S.A.C.?		
6	¿Evalúa el nivel de continuidad de sus sistemas de información la Empresa BROZZABDII PASTELERIA S.A.C.?		
7	¿Verifica periódicamente los controles de continuidad de la información establecidos la empresa BROZZANDII PASTELERIA SAC?		
8	¿A identificado algún tipo de riesgo que pudiera afectar la disponibilidad, integridad y confidencialidad de los sistemas de información y de su infraestructura la empresa BROZZANDII PASTELERIA S.A.C.?		
9	¿Existe algún proceso de valoración de riesgos de la información en la Empresa BROZZANDII PASTELERIA S.A.C. ?		
10	¿Ha desarrollado algún proceso de tratamiento de los riesgos de su información la EMPRESA BROZZANDII PASTELERIA S.A.C?		
MUCHAS GRACIAS			

Fuente: Elaboración Propia

Anexo IV: PROTOCOLO DE CONSENTIMIENTO INFORMADO

UNIVERSIDAD CATÓLICA LOS ÁNGELES
CHIMBOTE

PROTOCOLO DE CONSENTIMIENTO INFORMADO PARA ENCUESTAS

(Ingeniería y Tecnología)

La finalidad de este protocolo en Ingeniería y tecnología es informarle sobre el proyecto de investigación y solicitarle su consentimiento. De aceptar, el investigador y usted se quedarán con una copia.

La presente investigación se titula _____

_____ y es dirigido por _____

_____ investigador de la Universidad Católica Los Ángeles de Chimbote.

El propósito de la investigación es _____

Para ello, se le invita a participar en una encuesta que le tomará _____ minutos de su tiempo. Su participación en la investigación es completamente voluntaria y anónima. Usted puede decidir interrumpirla en cualquier momento, sin que ello le genere ningún perjuicio. Si tuviera alguna inquietud y/o duda sobre la investigación, puede formularla cuando crea conveniente.

Al concluir la investigación, usted será informado de los resultados a través _____. Si desea, también podrá escribir al correo _____ para recibir mayor información. Asimismo, para consultas sobre aspectos éticos, puede comunicarse con el Comité de Ética de la Investigación de la universidad Católica los Ángeles de Chimbote.

Si está de acuerdo con los puntos anteriores, complete sus datos a continuación:

Nombre: _____

Fecha:_____

Correo electrónico: _____

Firma del participante: _____

Firma del investigador (o encargado de recoger información):

_____