.

UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

PROPUESTA PARA LA SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001 EN LA CLÍNICA SIMEDIC DIAGNÓSTICA S.A.C – PIURA; 2018.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTORA:

BACH. KARLA STEFANY LARA MORALES

ASESOR:

ING. RICARDO EDWIN MORE REAÑO

PIURA – PERÚ

2018

JURADO EVALUADOR DE TESIS Y ASESOR

DR. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN
PRESIDENTE

MGTR. JENNIFER DENISSE SULLÓN CHINGA
MIEMBRO

MGTR. MARLENY SERNAQUÉ BARRANTES
MIEMBRO

ING. RICARDO EDWIN MORE REAÑO
ASESOR

DEDICATORIA

A mi Dios todo poderoso por brindarme sabiduría y poder permitirme llegar a este momento tan especial en mi vida ya que gracias a él he logrado concluir mi carrera.

A mi madre por ser la persona que me acompañó en mi trayectoria estudiantil, y por su apoyo incondicional.

A mi padre a quien con sus consejos ha sabido guiarme para culminar mi carrera profesional.

AGRADECIMIENTO

Como más importante, me gustaría agradecer sinceramente a mi asesor de tesis, Ing. Ricardo Edwin More Reaño y al Dr. Víctor Ángel Ancajima Miñan, por su dedicación, paciencia y constante apoyo en la elaboración de esta tesis.

Al personal docente y administrativo de la Universidad Católica los Ángeles de Chimbote por brindar las facilidades que han permitido culminar con éxito mi formación académica.

Extiendo también mi agradecimiento a todas las personas que me brindaron su confianza y me alentaron a que cada día siga superándome, y a la clínica Simedic Diagnóstica S.A.C. por el apoyo e información brindada.

RESUMEN

Esta tesis fue desarrollada bajo la línea de investigación en tecnología de la información y comunicación para la mejora continua de las organizaciones del Perú, de la escuela profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote Sede en Piura. La investigación tuvo como objetivo 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.

Palabras Claves: confidencialidad, gestión, información, seguridad.

ABSTRACT

This thesis was developed under the line of research in information technology and communication for the continuous improvement of the organizations of Peru, of the School the professional of Systems Engineering of the Universidad Católica los Ángeles de Chimbote Sede en Piura. The objective of the research was to carry out the proposal for computer security based on ISO/IEC 27001 in the Clinic Simedic Diagnostic S.A. C-Piura; 2018, will improve the management of information assets. The research had a non-experimental design because the data will not be manipulated and cross-cut because it is done at a certain time; The population of this investigation was of 28 employees of which it was taken in conscience that this investigation will not be delimited because they will be benefited in its totality of employees, to whom the instruments were applied where the following results were obtained: in dimension 01: current situation; That 61% of the workers surveyed felt that the current situation does not have adequate management in the processes of Clinic Simedic Diagnostic S.A. C, while 39% if it complies with the current situation of the clinic. . and in Dimension 02: Information security; It was noted that 68% of the workers surveyed felt that, if they agree with which the proposal for computer security should be made for the Clinic Simedic Diagnostic S.A. C, while 32% do not think necessary the proposal for computer security. The proposal for computer security based on ISO/IEC 27001 in the Clinic Simedic Diagnostic S.A. C-Piura was concluded; 2018, for the safety of information is fully accepted to provide greater safety in the clinic, workers and clients.

Key words: confidentiality, management, information, security.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

I. INTRODUCCIÓN

El avance de la tecnología en los sistemas de Información ofrece una mayor facilidad para incorporarla y difundirla en las organizaciones. Sin embargo, estos cambios no fueron asimilados en las empresas que no cuentan con una disposición financiera y/o organizativa para tener una aplicación completa o avanzada tecnológicamente, las cuales no han evolucionado a la misma velocidad.

La información se está volviendo un activo fundamental hoy en día ya que está sujeto a constantes amenazas que pueden ocasionar pérdidas dentro de las empresas o aquellos provocados por catástrofes naturales o fallos técnicos.

La presente investigación corresponde con la línea de investigación en Tecnología de la Información y Comunicación, para la mejora continua de las organizaciones del Perú, de la escuela profesional de Ingeniería de Sistemas ULADECH. La investigación se realizó en la clínica Simedic Diagnóstica S.A.C, que en la actualidad realiza todos sus procesos en Excel, lo que hace que no tengan un control de sus clientes y de los documentos de gestión que entra y sale de la clínica. Una parte importante del trabajo y del tiempo del personal se gasta en la búsqueda y asimilación de la información por lo tanto no se puede llevar un balance del estado de las diferentes áreas. Por otro lado, la clínica maneja información personal sobre sus pacientes, como también los diagnósticos de los exámenes que les fueron realizados, es por lo que debe ser protegida para que garantice una atención confiable y sin riesgos.

Actualmente no cuenta con los controles adecuados para la seguridad de información tales como:

- La falta de un control de acceso a las instalaciones de la clínica.
- Existencia de usuarios que acceden a información que no deberían tener acceso.

- Abandono de la administración de los sistemas de antivirus pertenecientes a la red.
- Falta de un sistema de gestión.
- Falta de control de uso malintencionado de claves de accesos y dispositivos.

De lo mencionado anteriormente se plantea el siguiente problema de investigación: ¿De qué manera la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C - Piura, 2018; permite una adecuada gestión en la seguridad de los activos de información?

Para el desarrollo de esta investigación se planteó el siguiente objetivo general: 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.

Para dar cumplimiento a nuestro objetivo general, también se plantearon los siguientes objetivos específicos.

1. Identificar la existencia de los riegos considerando la seguridad de la información en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.
2. Evaluar los mecanismos de seguridad, después de localizar los riesgos en los activos de información que enfrenta la clínica.
3. Analizar las diferentes normas internacionales basadas en la seguridad de información para la clínica Simedic Diagnóstica S.A.C – Piura; 2018.
4. Analizar las metodologías de evaluación y riesgos informáticos.

Este trabajo de investigación se justifica presupuestalmente por que la inversión para la propuesta para la seguridad informática será asumida por la persona que está realizando la investigación, no generando costos a la clínica investigada.

La clínica Simedic Diagnóstica tiene equipos de cómputo en cada área y cuenta con internet eficiente y rápido para las funciones que se realizan en la clínica, por otro lado, se justifica por la necesidad de tener claro los procesos de está, esto permitirá evaluar un sistema de gestión de seguridad aplicando la norma ISO/IEC 27001 en la clínica.

Esta investigación tiene un alcance y limitaciones que busca realizar una propuesta para la seguridad informática para la clínica Simedic Diagnóstica S.A.C- Piura. El alcance y las limitaciones del proyecto se describen a continuación.

El alcance del presente proyecto abarca realizar una propuesta para la seguridad informática basado en la norma ISO/IEC 27001, para proteger la confidencialidad, disponibilidad e integridad de todos los activos de información en la clínica Simedic Diagnóstica S.A.C Piura, para garantizar que los riesgos sean conocidos y minimizados por la clínica de una forma documentada, estructurada y adaptada en los cambios que se produzcan.

Las limitaciones del proyecto de tesis consistirán solo en un realizar una propuesta para la seguridad informática basada en la norma ISO/IEC 27001, pero no abarca la parte de la implementación del SGSI en la organización.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

Mesquida, Mas, Amengual, Cabestrero (1), realizó el artículo titulado "Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001", en el año 2010, da a conocer la gran aceptación que tuvo la implantación de un Sistema de Gestión de Calidad (SGC) de acuerdo con la norma ISO 9001, actualmente la mayoría de organizaciones que deciden implantar una nueva norma para gestionar sus servicios, como ISO/IEC 20000, o la seguridad de su información, como ISO/IEC 27001, normalmente ya cuentan con un SGC basado en ISO 9001. Con el objetivo de facilitar a las empresas la implantación de estas normas se ha realizado un estudio, tanto para analizar las posibles relaciones existentes entre los requisitos de los sistemas de gestión propuestos por estas normas, como para identificar los requisitos no compartidos entre ellos. En este artículo se presenta un nuevo Sistema de Gestión Integrado que amplía los requisitos de un SGC según ISO 9001 con los requisitos específicos de los otros dos estándares antes mencionados.

Por otro parte Pallas (2), en su informe de investigación titulado "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico"; en el año 2009, analizó diferentes enfoques de estos estándares, con el fin de proponer una metodología de implementación, gestión y mejora de un SGSI en un grupo empresarial jerárquico. Se presentan además diferentes alternativas estratégicas y se discute sobre su conveniencia o no. Se analizan

diferentes métodos conocidos de análisis y gestión de riesgos. Algunos de ellos promovidos por los gobiernos y/o industria de países de vanguardia y trayectoria reconocida en la seguridad de la información que han tenido gran aceptación. Se promueve un enfoque sistémico y pragmático, no dogmático, en pro de una metodología eficaz y sostenible, primando un criterio de conveniencia costo-beneficio. Se enfatiza la necesidad de su orientación y adecuación a los reales requerimientos de seguridad del negocio. Se presenta una metodología adecuada a un grupo empresarial, que busca integrar lo mejor de cada uno de los enfoques analizados; se incluye una propuesta de organigrama de Seguridad que compatibiliza la jerarquía estructural del grupo y las necesidades de un SGSI. Adicionalmente se incursiona en la aplicación de técnicas de grafos para la valoración de activos; se formaliza el concepto en términos de propiedades y algoritmia de grafos, y se define con una visión propia del tema, un algoritmo para el ajuste contemplando valoraciones cualitativas y cuantitativas y dependencias parciales y/o totales entre activos. También se describen características y funcionalidades deseables de una herramienta de software de apoyo a la metodología. Finalmente se analiza la aplicación de la metodología a un Caso de Estudio, en particular, un 'Internet Servicie Provider' (ISP) integrado verticalmente con una 'TelCo' (empresa de Telecomunicaciones). En el mismo se analizan las particularidades del caso de estudio: los estándares y recomendaciones internacionales específicos, el modelo organizacional aplicable al negocio, datos estadísticos, y la seguridad requerida para este sector de la industria.

Asimismo, Saizarbitoria, Bernardo, Casadesús (3), desarrolló un estudio sobre "La integración de sistemas de gestión basados en estándares internacionales: resultados de un estudio empírico

realizado en la CAPV"; en el año 2007, dio a conocer la evidencia empírica sobre cuál es el grado de integración de los diferentes estándares de sistemas de gestión en las empresas vascas, así como de recoger la opinión de las empresas que ya han implantado algún estándar internacional de sistemas de gestión sobre la dirección que ha de tomar el proceso de creación de estos estándares. Se trata de los primeros resultados de una investigación aún en curso, en la que el estudio cuantitativo mencionado pretende ser complementado con la realización de una serie de entrevistas y estudios de casos. La investigación se llevó a cabo entre enero y septiembre de 2007 en la Comunidad Autónoma del País Vasco (CAPV). Interesa señalar que esta misma investigación también se llevó a cabo en las comunidades autónomas de Cataluña y Madrid, que son, junto con la CAPV, las comunidades autónomas que cuentan con un mayor índice de intensidad certificadora (Heras, 2007). El cuestionario, que se diseñó con base en la literatura académica y empresarial existente, fue enviado a aquellas empresas de la CAPV que contaban con más de un sistema de gestión certificado conforme a un estándar internacional (ISO 9001 e ISO 14001). La base de datos utilizada para la realización del mailing se generó a partir del Catálogo Industrial y de Exportadores del País Vasco (Civex) de 2006 y del registro de empresas certificadas del Departamento de Industria, Comercio y Turismo del Gobierno Vasco. En total se enviaron 525 cuestionarios a otras tantas empresas de la CAPV que contaban con los certificados ISO 9001 e ISO 14001 en vigor. Los cuestionarios se enviaron por correo ordinario, junto con un sobre franqueado. Después de un seguimiento telefónico de la recepción de dichas encuestas, se obtuvieron 122 respuestas válidas, lo que representa una tasa de respuesta del 23%.

2.1.2. Antecedentes a nivel nacional

Talavera (4), en su tesis titulada "Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo con la ISO/IEC 27001; en el año 2013", dio a conocer que en la actualidad los sistemas que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de instituciones de diferentes rubros y funciones. Los sistemas de información se han vuelto más complejos debido a la globalización que tiene por consecuencia que las distancias geográficas ya no supongan un obstáculo. De esta forma se tiene que existe una cantidad cada vez mayor de personas que tienen acceso a información que podría ser crítica para las diferentes empresas e instituciones en las que trabajan. Adicionalmente a este riesgo interno, siempre se tiene presente el riesgo que supone la fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información, como por terceros que han accedido a ella mediante algún mecanismo de ataque. En respuesta a este nuevo escenario, las instituciones públicas han sido llamadas a realizar la implementación de diversos controles a través de un Sistema de Gestión de Seguridad de la Información – a través de diferentes normas, entre ellas la Norma Técnica NTP ISO/IEC 27001 – con la finalidad de asegurar el buen uso y protección de la información crítica que manejen, ya sea de clientes o información estratégica interna. El presente trabajo de fin de carrera desarrolla el Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad pública del sector Salud – el Instituto Nacional Materno Perinatal – sujeta al cumplimiento de la normativa vigente relativa a Seguridad de la Información.

Según Vivanco, Cortez, Bustamante (5), en su artículo titulado "La seguridad de información"; en el año 2011, se expone que la seguridad de los sistemas de información es un tema muy complejo que requiere la preparación de estrategias que permitan que la información circule libremente, garantizando al mismo tiempo la seguridad del uso de los sistemas de información en toda la comunidad. El proceso de garantía de seguridad está relacionado con establecer un nivel de confianza en el sistema que podría ser muy variable. Está es una cuestión de juicio profesional basado en evidencias sobre el sistema, su entorno y su proceso de desarrollo. Se puntualizará en el presente artículo todo lo relacionado a la seguridad de la información, custodia de datos, la auditoría de sistemas; así como el enfoque para medir el desempeño de las medidas de seguridad, el avance y progreso de las estrategias y la consecución de sus objetivos. Se considerará el impacto que tiene la falta de seguridad en la productividad enfocándose en el Modelo del Análisis para el Retorno de la Inversión de Seguridad (ROSI) derivado del conocido indicador financiero ROI (Retorno sobre la Inversión). Este modelo busca justificar la inversión en seguridad de la información en términos monetarios.

Por otro lado, Villena (6), en su informe de tesis titulada "Sistema de gestión de seguridad de información para una institución financiera"; en el año 2006, determinó que para gestionar la seguridad de la información de una entidad se debe partir de una premisa fundamental y es que la seguridad absoluta no existe. Tomando lo anterior como punto de partida, una entidad puede adoptar algunas de las normas existentes en el mercado que establecen determinadas reglas o estándares que sirven de guía para gestionar la seguridad de la información. La presente tesis ha realizado una investigación de las normas y estándares que van difundiéndose con mayor énfasis en el mercado peruano, en

especial en el sector financiero. Se rescataron los aspectos más saltantes de cada norma y estándar, a partir de los cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú, lo cual permitirá que ésta cumpla con las normas de regulación vigentes en lo relacionado a la Seguridad de Información.

2.1.3. Antecedentes a nivel regional

Nizama (7), en su artículo científico titulado "Evaluación del a seguridad para el personal informático y usuarios de sistemas en la Municipalidad Provincial de Piura"; año 2018, determina el nivel de evaluación de la seguridad para el personal informático y usuarios de sistemas, mediante el uso de listas de verificación estandarizadas para una auditoría a la seguridad informática, aplicadas a diversos trabajadores de las diferentes áreas y oficinas de la Municipalidad Provincial de Piura, durante el período octubre-diciembre 2014. La investigación fue descriptiva-cuantitativa; la muestra estuvo constituida por 50 trabajadores administrativos, seleccionados mediante un muestreo no probabilístico; por conveniencia de la investigación, a la totalidad de trabajadores (480) que laboraban en la citada municipalidad durante el periodo octubre-diciembre de 2014, se les aplicó, mediante la técnica de la encuesta, los tres formatos correspondientes a las Listas de Verificación para una Auditoría a la Seguridad Informática-Seguridad para el personal informático y los usuarios del sistema. Por ser instrumentos estandarizados y propios de una metodología aceptada, no se ha requerido su validación. Los resultados que se obtuvieron fueron: respecto a la dimensión de protección contra riesgos y contingencias relacionadas con el ambiente de trabajo más de la mitad de los usuarios (60%) no está de acuerdo ni en desacuerdo, en cuanto a la

dimensión de protección contra riesgos y contingencias por factores meteorológicos y desastres naturales hay un 3% de usuarios en desacuerdo, y solo un 11% está totalmente de acuerdo, y en la dimensión de protección contra riesgos y contingencias derivados del suministro de energía eléctrica más de la mitad de los usuarios 58% están en desacuerdo. En cuanto a las conclusiones, se puede indicar, en primer lugar, que se registra una relativa seguridad a nivel de protección de su ambiente de trabajo, asimismo, también se registra una relativa seguridad respecto al nivel de protección contra factores meteorológicos, aunque con valores polarizados. También se registra que en general no se confía en que se garantice una continuidad de los servicios de energía eléctrica.

Por otro lado, De la Cruz (8), en su trabajo de investigación titulado "Mejora del programa de seguridad basada en el comportamiento del sistema integrado de gestión de prevención de riesgos y medio ambiente de GYM S.A"; en el año 2014, tiene como fin dar a conocer las bases teóricas, conceptuales y técnicas de la Seguridad Basada en el Comportamiento (SBC) orientada a cambiar los comportamientos inseguros de los trabajadores por comportamientos seguros logrando mantenerlos en el tiempo. Además, busca contribuir al Sistema Integrado de Gestión (SIG) de la empresa Graña y Montero (GyM) en la reducción de incidentes, accidentes, lesiones producidas por actos o comportamientos inseguros. Esto implica comprender la estructura y metodología de implementación de un programa de seguridad basada en el comportamiento, y con todo ello proponer mejoras en el programa de SBC de GyM. De ambos sistemas, sistema cliente y sistema GyM, se rescatarán los puntos importantes y ventajosos realizando un análisis FODA; una vez obtenido dichos puntos, se identifican las falencias y faltas del programa de la SBC, logrando

así un mejoramiento al programa de seguridad basada en el comportamiento, y finalmente se propondrá el procedimiento de implementación y ejecución de la SBC. Como resultado de todo ello, se llegará a obtener un formulario GyM, en el que se presenten las conductas y comportamientos de las personas, y se pueda observar si es seguro o si no lo es, identificando las causas inmediatas y causas raíz de sus comportamientos.

Finalmente, Miranda (9), en su tesis de maestría titulada "Guía metodológica para implementar un sistema de gestión de seguridad en instituciones"; en el año 2013, da a conocer que existen estándares internacionales de seguridad dispuesto para su ejecución, pero muchas organizaciones fracasan en el intento de aplicarlo con rigurosidad, debido a que su personal de seguridad no interpreta adecuadamente las normas o tiene insuficiente conocimiento o falta de experiencia. El uso de estándares no únicamente es tratar de cumplir con todo lo que se indica, sino necesariamente aplicar aquello que sea gestionado por la organización. Se presenta una guía metodológica para la implementación de un sistema de gestión de seguridad basado en estándares internacionales referente a la gestión de seguridad y tecnologías de la información. En la cual se dan las pautas claves para la planificación, diseño, operación y retroalimentación de un sistema de gestión de seguridad. Finalmente se presentan los factores críticos de éxito y conclusiones de esta guía metodológica que está orientada a instituciones sea privada o estatal y sirva en gran medida en la aplicación de controles de seguridad.

2.2. Bases teóricas

2.2.1. Rubro de la empresa investigada

La clínica Simedic Diagnóstica S.A.C brinda servicios de salud ocupacional a diferentes empresas de la región Piura con la finalidad de minimizar los riesgos ocupacionales, prevención de las lesiones relacionadas a la actividad laboral y mantener estados de salud óptimos en sus colaboradores.

Salud ocupacional

La Organización Mundial de la Salud, define la salud ocupacional como una actividad multidisciplinaria que promueve y protege la salud de los trabajadores. Esta disciplina busca controlar los accidentes y las enfermedades mediante la reducción de las condiciones de riesgo. La salud ocupacional no se limita a cuidar las condiciones físicas del trabajador, sino que también se ocupa de la cuestión psicológica. Para los empleadores, la salud ocupacional supone un apoyo al perfeccionamiento del trabajador y al mantenimiento de su capacidad de trabajo (10).

La Organización Panamericana de la Salud, utilizaron la siguiente definición: "Es el conjunto de conocimientos científicos y de técnicas destinadas a promover, proteger y mantener la salud y el bienestar de la población laboral, a través de medidas dirigidas al trabajador, a las condiciones y ambiente de trabajo y a la comunidad, mediante la identificación, evaluación y control de las condiciones y factores que afectan la salud y el fomento de acciones que la favorezcan". Agregando a continuación "El desarrollo de la salud ocupacional, debe lograrse con la

participación y cooperación de los trabajadores, empresarios, sectores gubernamentales, instituciones y asociaciones involucradas. Para proyectar y ponerla en práctica es necesaria la cooperación interdisciplinaria y la constitución de un equipo, del cual tiene que formar parte el médico de los trabajadores" (11).

Según la organización mundial de la salud y la organización panamericana de la salud definen que la salud ocupacional mantiene la salud y el bienestar de los trabajadores por medio de varios exámenes que se realizan tanto físico y psicológico para saber si están aptos para el puesto de trabajo, por otro lado, esta disciplina estable medidas y condiciones para que el ambiente laboral sea adaptado a la capacidad que tienen sus trabajadores. Finalmente, la salud ocupacional brinda a las empresas gran apoyo para el perfeccionamiento del trabajador y al mantenimiento de su capacidad de trabajo.

La salud ocupacional tiene como objetivos prevenir las enfermedades laborales, proteger a los trabajadores de los riesgos a su salud presentes en el ambiente laboral donde se desempeñan, y establecer condiciones del medio ambiente adaptadas a las condiciones y capacidades físicas y psicológicas de los trabajadores. En este contexto se definen 3 objetivos específicos (12):

- Mantener y promover la salud y la capacidad de trabajo de los empleados.
- Mejorar las condiciones del trabajo para favorecer la salud y la seguridad de los trabajadores.

Salud ocupacional en el Perú

En Perú, la primera mención a las enfermedades ocupacionales es del periodo colonial cuando se hace referencia a los indígenas obligados a laborar en las minas de donde, por intoxicación, pocos sobrevivían. Sin embargo, la era científica de la salud ocupacional tendría que esperar hasta el periodo republicano cuando se encarga, en 1926, a la entonces Dirección de Salubridad del Ministerio de Fomento (aún no existía el Ministerio de Salud) el control e inspección de higiene de todos los centros de trabajo. En 1957 se realizó el Primer Seminario Nacional de Salud Ocupacional, y el director de aquel entonces Dr. Frederick J. Vintinner, quien durante la inauguración del evento dijo: La Salud Ocupacional ha sido definida como la ciencia y arte de preservar la salud mediante el reconocimiento, evaluación y control de las causas de medio ambiente, que originan las enfermedades en la industria… Es un axioma bien conocido que el trabajador enfermo es una carga para sí mismo, para la familia, para la comunidad y el país. El programa de Salud Ocupacional en el Perú ha sido desarrollado como un programa integral dirigido hacia la conservación y promoción de la salud del trabajador. Hablar de Salud Ocupacional en Perú, es hablar del Instituto de Salud Ocupacional, que inicia su historia con la creación del Departamento Nacional de Higiene Industrial por Decreto Supremo el 5 de agosto de 1940, el cual, posteriormente, se transformará en el Instituto de Salud Ocupacional. El 12 de marzo de 1947, fue promulgada la Ley 10833 que creaba fondos para el referido Departamento, además de especificar sus funciones (13).

En enero de 1969, el ISO es incorporado al INS; luego de varios cambios situacionales (reconocimiento como Instituto Nacional de Salud Ocupacional en 1985; y final reincorporación al INS en 2002) adopta finalmente la denominación de Centro Nacional de Salud Ocupacional y Protección del Ambiente para la Salud (CENSOPAS) (14).

Ley N°29783 Seguridad y salud en el trabajo en el Perú

En esta ley sobre la seguridad y salud en el trabajo se mencionan las condiciones en las que los trabajadores deben realizar sus funciones como se menciona posteriormente (15).

El empleador garantiza, en el centro de trabajo, el establecimiento de los medios y condiciones que protegen la vida, la salud y el bienestar de los trabajadores, y de aquellos que, no teniendo vínculo laboral, prestan servicios o se encuentran dentro del ámbito del centro de labores. Debe considerar factores sociales, laborales y biológicos, diferenciados en función del sexo, incorporando la dimensión de género en la evaluación y prevención de los riesgos en la salud laboral.

El empleador asume las implicaciones económicas, legales y de cualquier otra índole a consecuencia de un accidente o enfermedad que sufre el trabajador en el desempeño de sus funciones o a consecuencia de él, conforme a las normas vigentes.

2.2.2. Empresa Investigada

SIMEDIC DIAGNÓSTICA S.A.C

HISTORIA

Se inicia el día 7 de junio de 1997 como un Laboratorio Clínico Hematológico en la provincia de Sullana, con el objetivo de cubrir la necesidad de un servicio de laboratorio con servicios de calidad, entrega de resultados rápidos y oportunos, atención personalizada y cálida; recibiendo buena acogida del público lo que motivo a iniciar sus actividades en la ciudad de Piura ubicándose en el centro Médico "San Sebastián" y luego en el centro Médico Pediátrico "Carita feliz" bajo el nombre de "Laboratorio Clínico Hematológico San Sebastián MS", orientado a los servicios del público infantil. La demanda creciente llevó a la necesidad de atender a pacientes adultos que buscaban un laboratorio de confianza, rapidez y calidad en los resultados; a ello se sumó la necesidad de contar con un centro médico de primer nivel que complemente las actividades de ayuda al diagnóstico y servicios de salud integrados, por ello nace SIMEDIC DIAGNÓSTICA SAC – CENTRO MEDICO PIURA bajo la dirección del Dr. Jesús Alberto Juárez Eyzaguirre; como una unidad de atención preferente e integrada que persigue como único fin la atención integral de la familia abarcando todas las especialidades médicas y de apoyo al diagnóstico, siempre comprometidos en brindar a nuestros clientes servicios médicos especializados con atributos de accesibilidad, integralidad y de excelente calidad, lo cual no sería posible sino contáramos con profesionales médicos de excelente trayectoria con altos valores humanos y con equipos acordes con la tecnología actual. **SIMEDIC DIAGNÓSTICA S.A.C**, es un equipo de profesionales que ha cimentado buenas bases para tener una

empresa consistente y brindar a los usuarios los mejores servicios. Datos principales de la clínica Simedic Diagnóstica S.A.C (16).

RAZÓN SOCIAL: Simedic Diagnóstica SAC.
GERENTE : Dr. Jesús Alberto Juárez Eyzaguirre
INICIO : Junio de 1997
RUBRO : Servicios de Salud o salud ocupacional
DIRECCIÓN : Av. Grau 750 Urb. Club Grau – Piura.

¿QUIÉNES SOMOS?

Somos una empresa competitiva que ofrecemos los Servicios de Salud en Consulta Médica Especializada, Salud Ocupacional y de apoyo al Diagnóstico, a empresas, aseguradoras, EPS y a la sociedad, con el fin de satisfacer sus necesidades brindando la mejor atención a nuestros clientes. Somos una institución que se encuentra en renovación constante, apegándose a la demanda del mercado regional y global (16).

VISIÓN

Ser una empresa líder en atención de Salud Ocupacional, atención Médica Especializada y de apoyo al Diagnóstico dentro y fuera de la región, con un equipo médico, técnico y humano de primer nivel, con adecuada infraestructura, la tecnología más avanzada, estándares de calidad certificados, con el reconocimiento y respeto de las empresas y usuarios (16).

MISIÓN

Somos una Empresa que provee Servicios de Salud Ocupacional, Servicios Médicos Especializados y de Apoyo al Diagnóstico con atributos de accesibilidad, integralidad y de excelente calidad; con profesionales médicos y técnicos expertos con altos valores humanos y tecnología adecuada, con la finalidad de satisfacer las necesidades de salud de empresas y población en la Región Piura (16).

SERVICIO QUE BRINDA LA EMPRESA

Nosotros somos una empresa que se encarga de atender todas las esferas de la salud ocupacional, contamos con servicios de apoyo diagnóstico bien equipados y con especialistas certificados, lo cual permite tener confianza en los resultados, abarcando las áreas de (16):

EXÁMENES MÉDICOS OCUPACIONALES

Cubrimos las crecientes necesidades de las diferentes empresas de la Región Piura en el marco de sus propias políticas y de la legislación laboral nacional, con la finalidad de minimizar los riesgos ocupacionales, prevención de las lesiones relacionadas a la actividad laboral y mantener estados de salud óptimos en sus colaboradores (16).

- **Exámenes Pre – Ocupacionales**: Se realiza antes de que el colaborador ingrese al puesto de trabajo, permitiendo conocer su estado de salud y Aptitud al puesto de trabajo.

- **Exámenes Ocupacionales**: Tiene por finalidad monitorear la exposición a Factores de Riesgo y la detección precoz de Enfermedades Ocupacionales. Este es un examen periódico y debe realizarse una vez al año.
- **Exámenes Retiro**: Permite asegurar el bienestar de los colaboradores al término de la relación laboral y determinara las posibles secuelas relacionadas a la exposición en el trabajo. Debe realizarse previo al cese laboral.
- **Otros Exámenes Ocupacionales**:
    - Por cambios de ocupación o puesto de trabajo.
    - Por reincorporación laboral.
    - Por contratos temporales de corta duración

Los **Exámenes Médicos Ocupacionales** (EMO) se realizan bajo estrictos estándares de calidad, porque, entre otros:

- Contamos con equipamiento moderno, certificado con estándares de calidad.
- Contamos con profesionales y personal especializados en Salud Ocupacional.
- Nuestros Procedimientos de EMO tienen Homologación de calidad SGS.
- Existe permanente monitoreo de nuestro Flujo de Atención, que permite asegurar un servicio de calidad con comodidad para Ud. y sus colaboradores.
- Nuestra lectura de placas Radiográficas se ajusta a los protocolos de la Organización Internacional del Trabajo (OIT), con certificación.

- Nuestras audiometrías se realizan con los estándares y certificación del Council of Accreditation in Occupational Hearing Conservation (CAOHC).

SERVICIO DE ATENCIÓN REMOTA Y OFF SHORE EN SALUD (SARES)

Nuestro servicio médico en Zonas Remotas y Off Shore está conformado por médicos capacitados y con experiencia de trabajo en el rubro, para atenderlo en el lugar donde se desarrolla su actividad productiva. Contamos con equipamiento adecuado para poder responder ante posibles Emergencias y Urgencias Médicas, así como el servicio de evacuación y rescate para lo cual tenemos como aliado estratégico a OMNISALUD. El servicio Médico en Zonas Remotas y Off Shore tiene como finalidad (16):

- Atención medica en la producción de urgencias y emergencias médicas que se puedan suscitar dentro de la locación (incendios, trauma múltiple, etc.)
- Programa médico promocional y preventivo para disminuir el riesgo de accidentes laborales y de la producción de enfermedades ocupacionales.
- Aliados en la vigilancia médica del programa anual medico ocupacional de las empresas contratistas.
- Seguimiento de los pacientes con enfermedades crónicas como HTA, DBM o pacientes especiales, determinados por las empresas, que necesiten seguimiento.
- Desarrollo y capacitación de las brigadas de emergencias.
- Aplicación de gimnasia laboral para disminuir rangos de stress y ansiedad por el tipo de trabajo en aislamiento.

SERVICIO MÉDICO OCUPACIONAL PARA EMPRESAS (SEMOPE)

Nuestro compromiso nos lleva a ser aliados estratégicos para la regularización y cumplimiento de las normas vigentes en el tema de salud ocupacional por tal motivo brindamos el servicio de médicos ocupacionales para empresas, que tienen como objetivo implementar el programa de salud ocupacional dentro de la institución (empresa), con el fin de minimizar los factores de riesgo que puedan contribuir con un accidente de trabajo y/o enfermedades profesionales. Este servicio tiene como función (16):

- Vigilancia a través de la identificación y evaluación de los factores de riesgos laborales potenciales y reales de cada puesto de trabajo, de acuerdo con los estándares mínimos que establezcan la legislación local, relacionado con cada riesgo identificado.
- Promoción de salud en el trabajo en relación con los factores de riesgos identificado para cada puesto de trabajo.
- Atención médica integral orientada a asegurar la compatibilidad del estado de salud del trabajador en el puesto de trabajo asignado y los riesgos asociados. Vigilar el estado de salud de los trabajadores durante su desempeño laboral, procurando un diagnóstico oportuno, tratamiento adecuado y rehabilitación con reinserción o reubicación laboral.
- Evaluación médico-laboral con implicación legal.

OBJETIVOS DE LAS UNIDADES ORGÁNICAS:

Se describen todas las unidades orgánicas y la función que cumplen en la clínica Simedic Diagnóstica S.A.C (16):

- **Gerencia**: Representar como ente máximo a la empresa ante clientes e instituciones y dirigir a la empresa hacia los objetivos y metas acordados en la Junta General de Accionistas.
- **Convenios**: Promocionar el servicio de salud ocupacional al mercado y lograr captar nuevos clientes y estar en contacto con gerencia para la consolidación de convenios al respecto.
- **Administración**: Realizar el trabajo de apoyo administrativo para la organización ya sea en el servicio de Salud Ocupacional asimismo en los policlínicos de la empresa.
- **Policlínico**: Brindar el mejor servicio de atención hacia los pacientes, ya sea desde su recepción hasta su salida del Centro Médico, velando por su satisfacción. Para su ejecución estará en coordinación con las otras unidades orgánicas como tópico, recepción, mantenimiento y vigilancia; asimismo mantener coordinaciones correspondientes con los médicos especializados para velar y otorgar una mejor atención del policlínico.
- **Laboratorio**: Ofrecer análisis de calidad en las áreas de Bioquímica, Hematología, Inmunología y Microbiología, además la realización de pruebas de ADN.
- **Imágenes**: Es la Unidad Orgánica encargada de brindar el servicio de imágenes y radiografías para análisis correspondientes.

SISTEMA DE GESTIÓN DE LA CALIDAD

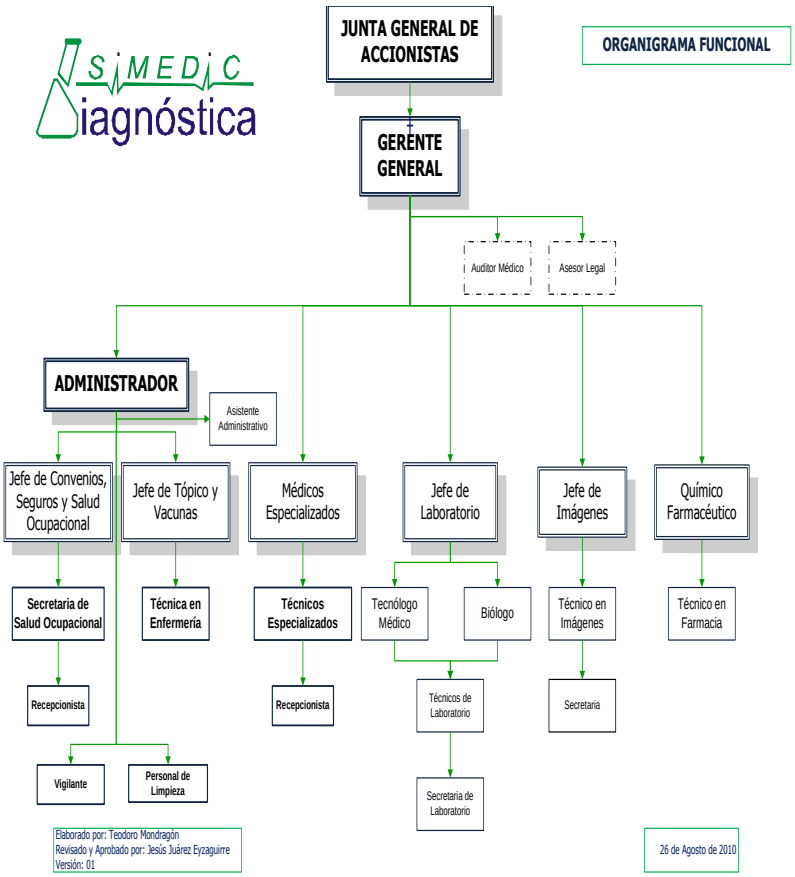
El Sistema de Gestión de la Calidad de SIMEDIC DIAGNÓSTICA SAC involucra un conjunto de procesos dirigidos a proporcionar una base documental, asegurando que los procesos se desarrollen bajo condiciones controladas, brindando las herramientas necesarias para la mejora continua de los procesos involucrados, tales como indicadores de medición y criterios de aceptación para los procesos y servicios, auditorías internas, servicios no conformes, acciones correctivas y acciones preventivas de acuerdo con los requisitos de la Norma ISO 9001:2008.

REFERENCIAS NORMATIVAS

Los siguientes documentos normativos contienen disposiciones o conceptos que son utilizados en el sistema de gestión de la calidad de Simedic Diagnóstica SAC (16):

- ISO 9000:2005, Sistemas de Gestión de la Calidad, Principios y Vocabulario.
- ISO 9001:2008, Sistemas de Gestión de la Calidad, Requisitos.
- ISO 9004:2009, Sistemas de Gestión de la Calidad, Direct rices para la Mejora del Desempeño.

Gráfico N° 1: Organigrama



Fuente: MOF de la clínica Simedic Diagnóstica Piura.

2.2.3. Seguridad

Según Gabriel Orozco en su investigación da a conocer la opinión de Thomas Hobbes que dice que el concepto de seguridad no se restringe únicamente a la garantía de la existencia física, sino que va más allá y se extiende, también, a la estabilidad social que permite disfrutar de una vida libre de amenazas. El trabajo conceptual que realiza Hobbes es un punto de inflexión en la filosofía política, ya que pone a la seguridad como una de las causas del establecimiento del Estado moderno, buscando la protección

del individuo y la satisfacción del bienestar general como justificación para su supervivencia (17).

Para George beekman la seguridad es un tema muy importante para cualquier empresa, este o no conectada a una red pública. No solamente es importante, sino que también puede llegar a ser compleja. Los niveles de seguridad que se pueden implementar son muchos y dependerá del usuario hasta donde quiera llegar (18).

Según thomas la seguridad no solo es una garantía física, sino es algo más grande que nos permitirá tener una vida libre de amenazas, buscando la protección del individuo y la satisfacción del bienestar. Por otro lado, Goerge se enfoca en que la seguridad no es solo un tema importante, sino que es fundamental para el usuario existen diferentes niveles de seguridad que se deben implementar y eso solo depende del usuario para proteger su información.

2.2.4. Informática

Según Elizondo (19), en su libro titulado "Informática 1" menciona a la organización de las naciones unidas para la educación, la ciencia y la cultura (Unesco) que propone la definición de informática como la ciencia que tiene que ver con los sistemas de procesamientos de información y sus implicaciones económicas, políticas y socioculturales. El termino informático es el acrónimo de información automática, y proviene del vocablo francés informatique.

Por otro lado, De pablos (20) , define la informática como "El conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".

2.2.5. Seguridad Informática

La seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo. También se encarga de controlar el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático o desde fuera, es decir, desde una red externa, usando una VPN, la WEB, transmisión de archivos, conexión remota (21).

Galdaméz (22), da a conocer el objetivo de la seguridad informática que es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales. Desafortunadamente, en ocasiones se ve a la seguridad informática como algo que dificulta la consecución de los propios objetivos de la organización, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores. Sin embargo, debe verse a la seguridad informática, no

como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos de la organización.

2.2.6. Activos de información

Los activos de información son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, los cuales son necesarios para que la organización funcione y alcance los objetivos que propone su dirección. Los activos de información se pueden clasificar en las siguientes categorías (11):

- Activos de información (Datos, manuales del usuario).
- Documentos de papel (contratos, resoluciones).
- Activos de software (aplicación, software de sistemas).
- Personal (trabajadores, población).
- Imagen de la empresa y reputación.
- Servicios (comunicaciones).

2.2.7. Seguridad de información

Según Talavera (23). Menciona en su investigación que la seguridad de información se denomina así al conjunto de políticas, estándares y controles que se implementan en la organización con la finalidad de asegurar la preservación de las siguientes propiedades de la información:

- **Confidencialidad:** Protección de la información confidencial del acceso o divulgación por parte de entidades – personas jurídicas o naturales – no autorizadas

al mismo, tanto por parte del originario de la información como por parte de la entidad que maneja la misma.

- **Integridad:** Protección de la información frente a la modificación o eliminación sin la autorización o accesos necesarios. De esta forma se garantiza que la información sea la correcta en todo momento.
- **Disponibilidad:** La información se encuentra accesible en todo momento, bajo demanda de todo usuario que se encuentre autorizado a poder acceder a la misma.
- **Autenticación**: Mediante esta propiedad, se permite identificar a la persona o personas que han generado la información que se está verificando, permite una validación en la autoría de la información por parte de un usuario específico.
- **No repudio:** Permite que la información sea validada a través de algún mecanismo que compruebe su integridad y contenido, declarándola como genuina.

Talavera en su investigación menciona que según Indecopi estas propiedades son las mínimas que un SGSI necesita para proteger la información.

2.2.8. Estándar de gestión de la seguridad de la información

Norma ISO

Según el International Organization for Standardization nos proporciona las siguientes definiciones (24):

¿Qué es ISO?

ISO (Organización Internacional de Normalización) es una organización no gubernamental, independiente, cuyos 163 miembros son los organismos nacionales de normalización. A través de sus miembros, la organización reúne a expertos que ponen sus conocimientos conjuntamente para desarrollar estándares internacionales, apoyo a la innovación relevante para el mercado, basado en el consenso voluntario y que ofrecen soluciones a los problemas mundiales.

¿Qué es un estándar?

Una norma es un documento que proporciona requisitos, especificaciones, directrices o características que pueden ser utilizadas consistentemente para asegurar que los materiales, productos, procesos y servicios son adecuados para su propósito. Hemos publicado más de 19 500 Normas Internacionales que se pueden comprar en la tienda de la ISO o de nuestros miembros.

¿Cuál es la norma?

Standard - un documento que recoja los requisitos, especificaciones, directrices o características por las que se pueden utilizar materiales, productos, procesos y servicios que son adecuados para estos fines. ISO ha publicado bolee21000 normas internacionales, que se pueden obtener de la ISO y sus miembros.

Beneficios de las normas internacionales

Normas Internacionales de traer beneficios tecnológicos, económicos y sociales. Ayudan a armonizar las especificaciones técnicas de los productos y servicios que hacen la industria más eficiente y rompiendo las barreras al comercio internacional. Conformidad con las Normas Internacionales de ayuda a tranquilizar a los consumidores que los productos sean seguros, eficientes y bueno para el medio ambiente.

Hechos y cifras sobre los beneficios de las normas

El repositorio de estudios sobre los beneficios económicos y sociales de las normas proporciona una visión de los enfoques y resultados de los estudios realizados por diferentes autores, como los organismos de normalizaciones nacionales e internacionales, institutos de investigación, universidades y otros organismos internacionales.

Para el negocio

Las normas internacionales son herramientas estratégicas y directrices para ayudar a las empresas hacer frente a algunos de los retos más exigentes de los negocios modernos. Se aseguran de que las operaciones comerciales son tan eficientes como sea posible, aumentar la productividad y ayudar a las empresas acceder a nuevos mercados.

Los beneficios incluyen:

- **Ahorro de costes:** Normas Internacionales de ayudar a optimizar las operaciones y por lo tanto mejorar la línea de fondo.
- **Satisfacción de la cliente mejorada**: Normas Internacionales de ayudar a mejorar la calidad, aumentar las ventas y aumentar la satisfacción del cliente.
- **El acceso a nuevos mercados:** Normas Internacionales de ayudar a prevenir las barreras comerciales y la apertura de los mercados mundiales.
- **El aumento de la cuota de mercado:** Normas Internacionales ayudan a aumentar la productividad y ventaja competitiva.
- **Beneficios ambientales:** Normas Internacionales ayudan a reducir los impactos negativos sobre el medio ambiente

ISO / IEC 27000

La serie ISO/IEC 27000, es un conjunto de normas de gestión de la seguridad de la información con la IEC (International Electrotechnical Commission), comisión internacional de electrotecnia. Cada una de las normas de la familia 27000, define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la información en cualquier empresa pequeña, mediana o grande, así como públicas y privadas. A continuación, se muestra un resumen de la familia de la de la ISO 27000 (25):

- **ISO 27000:** Gestión de la seguridad de la información (Fundamentos y vocabulario). Esta norma fue publicada el 1 de mayo de 2009 y contemplan en forma introductoria todos los aspectos fundamentales que enfoca un sistema de gestión de seguridad de la información (SGSI), una descripción del ciclo PDCA, al igual que las definiciones de los términos que se emplean en toda la serie 27000.

- **ISO 27001 Especificaciones para un SGSI:** Esta norma fue publicada el 15 de octubre de 2005, la cual enmarca los requisitos y/o especificaciones del sistema de Gestión de la seguridad de la información. Fue originaria de la BS 7799-2:2002, siendo identificada actualmente como norma ISO 27001:2013. Esta es la norma certificable en la actualidad por los auditores externos de los SGSI de las diferentes empresas. En esta norma se enumera en forma resumida, los objetivos de control y controles, para que sean seleccionadas por las empresas que desean implantar el SGS. Si bien es cierto que no es de carácter obligatorio que se implementen todos los controles de esta norma, la

empresa debe justificar ante los auditores la no aplicabilidad de los controles cuando estén en el proceso de evaluación para una certificación.

- **ISO 27002: código de buenas prácticas**: Publicado el 1 de julio de 2007. Esta norma no certificable, es una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información.

- **ISO 27003: Guía de implantación de un SGSI:** Publicado el 1 de febrero de 2010. Esta norma no es certificable y proporciona una guía que contempla todos los aspectos necesarios para el diseño e implementación de un SGSI de acuerdo con la norma certificable ISO/IEC 27001:2013. El objetivo de esta norma es describir las especificaciones y diseño en el proceso de la implementación del SGSI.

- **ISO 27004: Sistema de métricas e indicadores:** Publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

- **ISO/IEC 27005:** Publicada en segunda edición el 1 de junio de 2011 (primera edición del 15 de junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC

27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

- **ISO/IEC 27006: Especificaciones para Organismos Certificadores de SGSI:** Está norma fue publicada en su primera edición el 1 de marzo de 2007 y su segunda edición el 1 de diciembre de 2011. Esta norma específica los requisitos para la acreditación de entidades de auditoría y certificación de SGSI.

- **ISO 27007: Guía para auditar un SGSI:** Está norma fue publicada el 14 de noviembre de 2011. Es una guía para la aplicación de auditorías a un SGSI como complemento especificado en ISO 19011, no es una norma certificable.

2.2.9. La Normativa ISO/IEC 27001:2013

Estructura ISO/IEC 27001:2013

El estándar El ISO/IEC 27001: 2013, para los Sistemas Gestión de la Seguridad de la Información es un modelo de gestión de seguridad de la información, que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. Se define como un conjunto de lineamientos el cual especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Estos requisitos describen cual es el comportamiento esperado del sistema de Gestión una vez que esté en funcionamiento (25) .

Tabla N° 1 Lista de documentos requerida por la ISO/IEC 27001

Documentos	**Capítulo de la ISO/IEC 27001:2013**
Alcance del SGSI.	4.3
Políticas y objetivos de seguridad de la información.	5.2, 6.2
Metodología de evaluación y tratamiento de riesgos.	6.1.2
Declaración de aplicabilidad.	6.1.3 d)
Plan de tratamiento del riesgo.	6.1.3 e), 6.2
Informe de evaluación de riesgos.	8.2
Definición de funciones y responsabilidades de seguridad.	A.7.1.2, A.13.2.4
Inventario de activos.	A.8.1.1
Uso aceptable de los activos.	A.8.1.3
Política de control de acceso.	A.9.1.1
Procedimientos operativos para gestión de TI.	A.12.1.1
Principios de ingeniería para sistema seguro	A.14.2.5
Política de seguridad para proveedores	A.15.1.1

Procedimiento para gestión de incidentes.	A.16.1.5
Procedimientos de la continuidad del negocio.	A.17.1.2
Requisitos legales, normativos y contractuales.	A.18.1.1

Fuente: ISO (25).

2.2.10. Norma técnica Peruana ISO / IEC 27001:

La presente Norma Técnica Peruana ha sido elaborada por el comité técnico permanente de codificación e intercambio Electrónico de datos (EDI), mediante el sistema 1 o adopción, durante los meses de mayo a octubre del 2008, utilizando como antecedente la ISO/IEC 27001: 2005 Information technologu – Security techniques – Information security management systems – Requirements (26).

El comité técnico de Normalización de Codificación e Intercambio Electrónico de Datos –EDI presentó a la comisión de Normalización y de Fiscalización de barreras Comerciales No arancelarias –CNB-, con fecha 2008-10-22, el PNTP- ISO/IEC 27001:2008, PARA SU REVISIÓN Y APROBACIÓN, SIENDO SOMETIDO A LA ETAPA DE Discusión Pública el 2008-11-13. No habiéndose presentado observaciones fue oficializado como Norma Técnica Peruana PNTP-ISO/IEC 27001:2008 EDI. Tecnología de la información. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Requisitos, 1° Edición, el 11 de enero de 2009. Esta Norma Técnica Peruana reemplaza a la

NTP 921.101:2005 EDI. Sistemas de gestión de seguridad de la información. Especificaciones con guía de uso y es una adopción de la ISO/IEC 27001:2005. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo con las Guías Peruanas GP 001:1995 Y GP 002:1995. (26)

Esta Norma Técnica Peruana de Seguridad de la Información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo sistema de gestión de seguridad de la información ISMS, por sus siglas en inglés (Information Security Management System). La adopción de un ISMS debe ser una decisión estratégica para una organización. El diseño e implementación del ISMS de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño, y estructura de la organización. Se espera que éstos y sus sistemas de soporte cambien a lo largo del tiempo, así como que las situaciones simples requieran soluciones ISMS simples (26).

2.2.11. Metodologías de gestión de riesgos

Hoy en día las empresas sufren de riesgos informáticos que afecta su funcionamiento, una forma de prevenir estos riesgos es realizando una evaluación de riesgos informáticos. Esta evaluación se puede llevar acabo aplicando algunas de las siguientes metodologías:

MAGERIT

El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos). Si hablamos de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico. El Consejo Superior de Informática ha sido el encargado de elaborar la primera versión de MAGERIT, con lo que promueve su utilización como respuesta a la dependencia creciente de toda la sociedad respecto a las Tecnologías de la Información. MAGERIT se encuentra muy relacionada con la generación en la que se utilizan los medios electrónicos, informáticos y telemáticos, lo que genera grandes beneficios para los empleados y los ciudadanos, aunque también puede dar lugar a diferentes riesgos que se tienen que minimizar con medidas de seguridad que generan confianza (27).

Valoración de las amenazas

Para realizar la evaluación de los activos esta metodología nos brindas como valorizar las amenazas de un activo de la siguiente manera (28):

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos: degradación: cuán perjudicado resultaría el [valor del] activo probabilidad: cuán probable o improbable es que se materialice la amenaza La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva. La probabilidad de ocurrencia es más compleja de determinar y de expresar.

A veces se modela cualitativamente por medio de alguna escala nominal:

Tabla N° 2 Degradación del valor

MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

Fuente: Libro1 de Margerit (28).

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia, como medida de la probabilidad de que algo ocurra. Son valores típicos:

Tabla N° 3 Probabilidad de ocurrencia

MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: Libro1 de Margerit (28).

OCTAVE

Giménez (29), nos da a conocer sobre Octave que significa Operationally Critical Threat, Asset and Vulnerability Evaluation. El método está desarrollado por la universidad de Canegie Mellon, y define un conjunto de criterios, para poder emplear métodos más flexibles según la empresa. Existen tres métodos muy comunes que cumplen esos criterios de compatibilidad: El método de Octave original, el Octaves-s para pequeñas empresas, y el Octave-Allegro, especialmente centrado en los activos de información.

Los criterios son bastantes generales, e incluyen; que las medidas sean adaptables a las necesidades, que el proceso de análisis esté definido, sea continuo y tenga visión de futuro, y que el proceso se centre en un conjunto reducido de riesgos críticos.

Los resultados se dividen en diferentes fases: fase organizativa (activos críticos y sus requerimientos, amenazas, y prácticas de seguridad habituales), una fase tecnológica (componentes clave y vulnerabilidades), es una tercera y última fase estratégico, o de desarrollo del plan de riesgo.

CRAMM

Es el método de análisis y control de riesgos del Gobierno Británico (CCTA Risk Analysis and Management Method). CRAMM es un método estructurado y coherente para la identificación y la evaluación de riesgos en redes y sistemas de información. Abarca escenarios técnicos y no técnicos (por ejemplos, aspectos físicos de la seguridad de la tecnología de la información) y proporciona un método riguroso por etapas que permite programar adecuadamente las revisiones. Hay herramientas de software disponibles para CRAMM. La última versión es CRAMM Versión 5 de enero de 2013 (30).

Es una metodología de la Agencia Centrla de Cómpito y Telecomunicaciones del Reino Unido, que data de los años 80. El modelo es muy similar al visto (29):

- Una fase de análisis en la se estudian los activos, las vulnerabilidades, y las amenazas para generar unos riesgos.
- Una fase de gestión, que incluye unas contramedidas, una implantación, y por último una fase de auditoría.

III. HIPÓTESIS

La propuesta para la seguridad informática basado en la norma ISO/IEC 27001, en la clínica Simedic Diagnóstica S.A.C – Piura, permitirá mejorar la gestión en los activos de información.

IV. METODOLOGÍA

4.1. Diseño de la investigación

La investigación fue de tipo cuantitativo porque usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías (31).

Según la investigación su nivel fue descriptivo porque permite como su nombre lo indica describir las situaciones, los fenómenos o los eventos que nos interesan, midiéndolos, y evidenciando sus características. Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis (31).

El diseño de la investigación es no experimental porque según Sampieri, Fernández, Baptista dan a conocer que las variables independientes ocurren y no es posible manipularlas, no se tiene control directo sobre dichas variables ni se puede influir sobre ellas, porque ya sucedieron, al igual que sus efectos (31). Y de corte transversal según su característica de tiempo ya que el estudio se circunscribe a un momento puntual, recolectándose datos en un tiempo único, describiendo variables y analizando su incidencia, en el año 2018 (32).

La investigación fue de tipo cuantitativo porque que permite recolectar datos para tener resultado y brindar soluciones. Por otro lado fue descriptivo porque se caracterizan los hechos tal y como son observados. Asimismo, fue no experimental porque se observarán las características de los hechos, en los cuales no se interviene o manipula deliberadamente las variables de estudio, se observará el fenómeno tal como se encuentra dentro de su

contexto; y de corte Transversal ya que solo se recolectó datos en un momento único.

4.2. Población y Muestra

4.2.1. Población

La clínica SIMEDIC Diagnóstica S.A.C – Piura, cuenta con 30 trabajadores dispersos en las diferentes áreas de la clínica.

4.2.2. Muestra

Excluyendo trabajadores de limpieza, de los cuales podremos tomar como muestra la cantidad de 28 trabajadores. La técnica utilizada para la selección de la muestra fue la técnica no probabilística.

4.3. Definición operacional de las variables en estudio

Tabla N° 4: Matriz de Operacionalización

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIÓN	INDICADORES	ESCALA DE MEDICIÓN	DEFINICIÓN OPERACIONAL
Propuesta para la seguridad informática basado en la norma ISO/IEC 27001 .	La seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un	Situación actual	• Organización de la información. • Gestión de activos • Control de accesos • Criptografía • Transferencia de información. • Adquisición de sistemas, desarrollo y mantenimiento	ORDINAL	La clínica Simedic Diagnóstica S.A.C, brinda servicios a los trabajadores de algunas empresas privadas y públicas en Piura. Al brindar un servicio gurda información

	sistema informático e intentar reducir las amenazas que pueden afectar al mismo. También se encarga de controlar el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuarios autorizados (21).	Seguridad de información	• Políticas de seguridad. • Seguridad en recursos humanos. • Cumplimiento con requerimientos legales y contractuales. • Gestión de los incidentes de seguridad.		privadas de los usuarios. La propuesta de la seguridad informática basada en la norma ISO 27001 permitirá mayor confidencialidad en información de los usuarios y la clínica. Por otro lado, sus procesos serán realizados con mayor rapidez, precisión y con seguridad.

Fuente: Elaboración propia.

4.4. Técnicas e instrumentos de recolección de datos.

La técnica que se utilizó en esta investigación será la encuesta que según Mayntz citado por Díaz de Rada, describen que es la búsqueda sistemática de información en la que el investigador pregunta a los investigados sobre los datos que desea obtener, y posteriormente reúne estos datos individuales para obtener durante la evaluación datos agregados (33), y el instrumento que se utilizó es el cuestionario que según Casas es un documento que recoge en forma organizada los indicadores de las variables implicadas en el objetivo de la encuesta (34).

Encuesta: con esta técnica se busca recolectar información valiosa de parte de los usuarios aplicando la técnica del cuestionario el cual cuenta con dos dimensiones "Situación actual" y "seguridad de información" para la clínica Simedic Diagnóstica S.A.C.

4.5. Plan de análisis

Se seleccionó a las personas adecuadas y para poder aplicar los cuestionarios, se realizó visita a las diversas instalaciones de la Clínica Simedic Diagnóstica S.A.C, durante el desarrollo de los cuestionarios se pudo resolver cualquier duda en relación con las interrogantes planteadas. La recolección de datos se realizó mediante la aplicación de 02 cuestionarios cada uno contiene preguntas cerradas para medir conocimientos, actitudes y opiniones y finalmente para la tabulación de los datos se utilizará como soporte el programa Excel.

4.6. Matriz de consistencia

Tabla N° 5: Matriz de consistencia.

TÍTULO: PROPUESTA PARA LA SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001 EN LA CLÍNICA SIMEDIC DIAGNÓSTICA S.A.C – PIURA; 2018.

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	METODOLOGÍA
¿Cómo el desarrollo de la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C - Piura, 2018; permitirá una adecuada	**OBJETIVO GENERAL** Realizar la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura; 2018, que permitirá mejorar la gestión en los activos de información.	La propuesta para la seguridad informática basado en la norma ISO/IEC 27001, en la clínica Simedic Diagnóstica S.A.C – Piura, permitirá mejorar la gestión en los activos de información.	Propuesta para la seguridad informática basado en la norma ISO/IEC 27001	TIPO: - Cuantitativo. NIVEL: - Descriptivo. DISEÑO: - No experimental y de corte transversal. MUESTRA: - 28 trabajadores

gestión en la seguridad de los activos de información?	**OBJETIVOS ESPECÍFICOS** 1. Identificar la existencia de los riegos considerando la seguridad de la información en la clínica Simedic Diagnóstica S.A.C – Piura; 2018. 2. Evaluar los mecanismos de seguridad, después de localizar los riesgos en los activos de información que enfrenta la clínica.			TÉCNICA: - Encuesta INSTRUMENTO: - Cuestionario

	3. Analizar las diferentes normas internacionales basadas en la seguridad de información para la clínica Simedic Diagnóstica S.A.C – Piura; 2018. 4. Analizar las metodologías de evaluación y riesgos informáticos.			

Fuente: Elaboración propia.

4.7. Principios éticos

Durante el desarrollo de la presente investigación denominada "Propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura" se ha considerado en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación. Asimismo, se han respetado los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas, necesarias para estructurar el marco teórico.

Por otro lado, considerando que gran parte de los datos utilizados son de carácter público, y pueden ser conocidos y empleados por diversos analistas sin mayores restricciones, se ha incluido su contenido sin modificaciones, salvo aquellas necesarias por la aplicación de la metodología para el análisis requerido en esta investigación.

Igualmente, se conserva intacto el contenido de las respuestas, manifestaciones y opiniones recibidas de los trabajadores y funcionarios que han colaborado contestando las encuestas a efectos de establecer la relación causa-efecto de la o de las variables de investigación. Finalmente, se ha creído conveniente mantener en reserva la identidad de estos con la finalidad de lograr objetividad en los resultados.

V. RESULTADOS

5.1. Resultados

Tabla N° 6: Actividades y funciones el Trabajo

Distribución de frecuencia y respuestas relacionada con las actividades y funciones de los trabajadores; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	7	25
NO	21	75
TOTAL	28	100

Fuente: Aplicado para medir el conocimiento de los trabajadores encuestados relacionada a la pregunta: ¿Usted tiene claras las actividades y funciones que se realizan en su área de trabajo?, en las actividades y funciones que realizan los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 6 podemos apreciar que el 75% de los trabajadores encuestados indicaron que, SI conocen sus actividades y funciones en su área de trabajo, mientras que el 25% NO las conoce.

Tabla N° 7: Los datos registrados están seguros

Distribución de frecuencia y respuestas relacionada con la seguridad de los datos registrados en forma manual; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	9	32
NO	19	68
TOTAL	28	100

Fuente: Aplicado para medir el conocimiento de los trabajadores relacionado a la pregunta: ¿Cree Usted que, en el sistema manual los datos registrados son seguros?, a opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 7 se observa que el 68% de los trabajadores encuestados indicaron que, NO están seguro los datos que son registrados de forma manual, mientras que el 32% SI que los datos si están seguros.

Tabla N° 8: Política y procedimientos en la clínica

Distribución de frecuencia y respuestas relacionada con las políticas y procedimientos de seguridad en la clínica; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	0	0
NO	28	100
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen políticas y procedimientos para asegurar que se proporciona seguridad en la información de sus usuarios?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 8 podemos apreciar que el 100% de los trabajadores encuestados expresaron que NO existen políticas y procedimientos para asegurar que se proporciona seguridad en la información de sus usuarios.

Tabla N° 9: La información ya no utilizada

Distribución de frecuencia y respuestas relacionada sobre que hace con la información que ya no es utilizada; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	12	43
NO	16	57
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Usted desecha la información que ya no necesita?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 9 se observa que el 57% de los trabajadores encuestados expresaron que NO desechan la información que no es utilizada, mientras que el 43% se desase está información.

Tabla N° 10: Los documentos son catalogados como confidencial

Distribución de frecuencia y respuestas relacionada con la clasificación de los documentos que son confidencial o de acceso restringido; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	10	36
NO	18	64
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Usted cree que los documentos que maneja son catalogados como confidencial o acceso restringido?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 10 se observa que el 64% de los trabajadores encuestados expresaron que la información NO está catalogada como confidencial o acceso restringido, mientras que el 36% si cree que los documentos son confidenciales.

Tabla N° 11: Copias de seguridad

Distribución de frecuencia y respuestas relacionada con las copias de seguridad que se deben realizar en la clínica; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	8	29
NO	20	71
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Se realizan copias de seguridad (diariamente, semanalmente, mensualmente, etc.) ?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 11 se observó que el 71% de los trabajadores encuestados expresaron que NO realizan copias de seguridad, mientras que el 29% SI realiza.

Tabla N° 12: Responsabilidad de los equipos informáticos

Distribución de frecuencia y respuestas relacionada con la responsabilidad que cada trabajador debe tener con los equipos informáticos; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	19	68
NO	9	32
TOTAL	28	100

Fuente: Aplicado para medir el conocimiento de los trabajadores encuestados relacionado a la siguiente pregunta ¿Usted cree que es responsable del equipo informático que utiliza para realizar sus funciones en la clínica Simedic Diagnóstica S.A.C?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 12 se estimó que el 68% de los trabajadores encuestados expresaron que SI son responsables del equipo informático que utiliza para realizar sus funcionas, mientras que el 32% NO se hacen responsables.

Tabla N° 13: Documentación visible

Distribución de frecuencia y respuestas relacionada con respecto que personas tiene acceso a la documentación de la clínica; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	20	71
NO	8	29
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Cuándo no se encuentra en su oficina deja documentación visible en su escritorio?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 13 se estimó que el 71% de los trabajadores encuestados expresaron que SI dejan visible la documentación que se encuentra en su oficina cuando no están en ella, mientras que el 29% NO la deja visible.

Tabla N° 14: Claves de acceso para los equipos de cómputo

Distribución de frecuencia y respuestas relacionada con respecto a la clave de acceso para los equipos de cómputo; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	25	89
NO	3	11
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿La clave de acceso es la misma para ingresar a todos los equipos de cómputo?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 14 podemos apreciar que el 89% de los trabajadores encuestados expresaron que, SI se accede a los equipos de cómputo con la misma clave, mientras que el 11% NO tiene la misma clave.

Tabla N° 15: Ingerir alimentos enfrente de los equipos de cómputo

Distribución de frecuencia y respuestas relacionada con respecto a ingerir alimentos cuando realiza sus labores utilizando los equipos de cómputo; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	18	64
NO	10	36
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Usted ha observado que alguno de sus compañeros a ingerido alguna bebida o alimentos cuando realiza su trabajo en cualquiera de las computadoras de la clínica Simedic Diagnóstica?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 15 podemos apreciar que el 64% de los trabajadores encuestados expresaron que, SI ha observado a sus compañeros ingiriendo alimentos frente al equipo de cómputo, mientras que el 36% NO ha observado dicha situación.

Tabla N° 16: Funcionamiento y actualización del antivirus

Distribución de frecuencia y respuestas relacionada con respecto al funcionamiento y actualización del antivirus que se utiliza en los equipos de cómputo de la clínica; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	6	21
NO	22	79
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Usted ha detectado que el antivirus de la clínica Simedic Diagnóstica S.A.C funciona y se encuentra actualizado?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 16 podemos apreciar que el 79% de los trabajadores encuestados expresaron que NO existe un buen funcionamiento del antivirus que tiene los equipos de cómputo en la clínica, mientras que el 21% NO si existe un buen funcionamiento del antivirus.

Tabla N° 17: Alarmas contra incendios o robos

Distribución de frecuencia y respuestas relacionada con respecto a la existencia de alarmas en la clínica; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	28	100
NO	0	0
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Existe alguna alarma contra incendios, robos u otros?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N°117 se observa que el 100% de los trabajadores encuestados expresaron que, SI existe alarmas contraincendios, robos u otros.

.

Tabla N° 18: Plan de contingencia

Distribución de frecuencia y respuestas relacionada con el plan de contingencia que debe tener la clínica; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	0	0
NO	28	100
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿La clínica Simedic Diagnóstica S.A.C cuenta con algún plan de contingencia para dar solución a algún incidente tanto interno o ajeno de la organización?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 18 se observa que el 100% de los trabajadores encuestados expresaron que NO existe ningún plan de contingencia en la clínica para dar solución algún incidente.

Tabla N° 19: Conocimiento sobre la seguridad informática

Distribución de frecuencia y respuestas relacionada con el conocimiento que tiene los trabajadores sobre la seguridad informática; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	12	43
NO	16	57
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Conoce de que trata el tema de seguridad informática?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 19 se observa que el 57% de los trabajadores encuestados expresaron que NO tiene conocimientos sobre la seguridad informática, mientras que el 43% SI cuenta con conocimientos sobre la seguridad informática.

Tabla N° 20: Controles de seguridad

Distribución de frecuencia y respuestas relacionada con aplicar controles de seguridad para evitar algún daño en la información; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	28	100
NO	0	0
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Cree que es necesario aplicar controles de seguridad para evitar robo o daño de información importante para la clínica Simedic Diagnóstica S.A.C.?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 20 se estimó que el 100% de los trabajadores encuestados expresaron que SI es necesario aplicar controles de seguridad para evitar algún tipo de incidente.

Tabla N° 21: Responsable del área

Distribución de frecuencia y respuestas relacionada sobre si existe algún trabajador responsable del área de seguridad informática; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	0	0
NO	28	100
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Existe en la empresa un responsable para el área de informática?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 21 se estimó que el 100% de los trabajadores encuestados expresaron que NO existe ningún responsable en el área de informática para dar soluciones al tema de la seguridad.

Tabla N° 22: Importancia de la seguridad en la clínica

Distribución de frecuencia y respuestas relacionada con la importancia que le otorga la clínica a la seguridad; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	6	21
NO	22	79
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Considera que la clínica le da importancia suficiente a la seguridad?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 22 se estimó que el 79% de los trabajadores encuestados expresaron que la empresa NO le otorga la suficiente importancia a la seguridad, mientras que el 21% SI le otorga.

Tabla N° 23: Seguridad de información

Distribución de frecuencia y respuestas relacionada con la seguridad de información si es vital en la clínica; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	21	75
NO	7	25
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Considera que la seguridad de información debe ser vital en la clínica?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 23 se analizó que el 75% de los trabajadores encuestados expresaron que, SI consideran que la seguridad de información debe ser vital en la clínica, mientras que el 25% NO debe ser vital.

Tabla N° 24: Protocolos de seguridad

Distribución de frecuencia y respuestas relacionada con los protocolos de seguridad para los trabajadores; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	28	100
NO	0	0
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Usted como trabajador tiene la cultura de seguir con protocolos de seguridad?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 24 se observó que el 100% de los trabajadores encuestados expresaron que SI tiene la cultura de seguir con protocolos de seguridad.

Tabla N° 25: Norma ISO 27001

Distribución de frecuencia y respuestas relacionada a la norma ISO 27001; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	7	25
NO	21	75
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Conoce Usted sobre la norma ISO 27001 en la seguridad de información?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 25 se observa que el 75% de los trabajadores encuestados opinaron que NO conoce sobre la norma 27001 en la seguridad de información, mientras que el 25% SI la conoce.

.

Tabla N° 26: Propuesta para la seguridad informática

Distribución de frecuencia y respuestas relacionada con la propuesta de seguridad y los beneficios que brindará; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	28	100
NO	0	0
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Cree que la propuesta para la seguridad informática basado en la ISO 27001 ayudará en la seguridad de información en la clínica?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 26 se observó que el 100% de los trabajadores encuestados expresaron que la propuesta SI beneficiará a la clínica en la seguridad informática.

Tabla N° 27: Capacitaciones de seguridad

Distribución de frecuencia y respuestas relacionada con las capacitaciones que la clínica imparte sobre la seguridad de información; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	11	39
NO	17	61
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿Desea recibir capacitaciones sobre la seguridad de información y la norma ISO 27001?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 27 podemos apreciar que el 61% de los trabajadores encuestados expresaron que la clínica NO imparte contantemente capacitaciones de seguridad, mientras que el 39% SI ha recibido capacitaciones.

Tabla N° 28: Recibir capacitaciones sobre norma ISO 27001

Distribución de frecuencia y respuestas relacionada con brindar capacitaciones sobre norma ISO 2700 dirigidas a los trabajadores; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	19	68
NO	9	32
TOTAL	28	100

Fuente: Aplicado del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta ¿La clínica imparte constantemente capacitaciones de seguridad?, ha opinión de los trabajadores en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 28 se observó que el 68% de los trabajadores encuestados opinaron que, SI desean recibir capacitaciones sobre la seguridad de información y la norma ISO 27001, mientras que el 32% NO desea recibir capacitaciones.

DIMENSIÓN 01: SITUACIÓN ACTUAL

Tabla N° 29: Dimensión situación actual

Distribución de frecuencia y respuestas relacionada con la dimensión 01: situación actual; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	11	39
NO	17	61
TOTAL	28	100

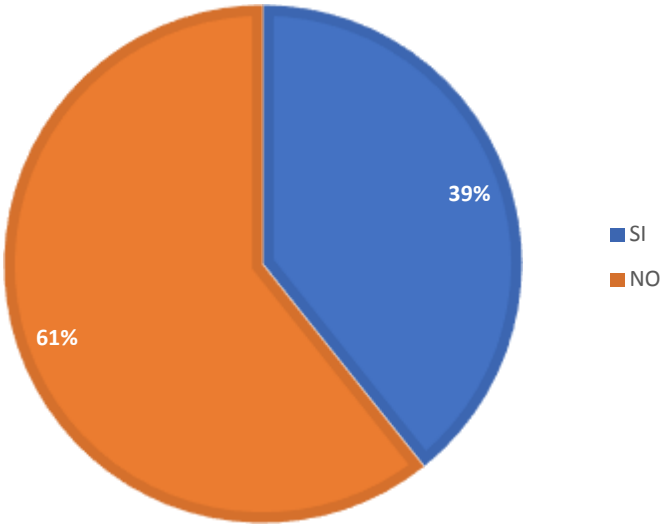
Fuente: Aplicado del instrumento para medir sobre la situación actual, basado en 13 preguntas aplicadas a los trabajadores de la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 29 se observó 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.

Gráfico N° 2: Resultado de la dimensión 01

Distribución porcentual de frecuencia y respuestas relacionada con la dimensión 01: situación actual; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.



Fuente: Tabla N°29

DIMENSIÓN 02: SEGURIDAD DE INFORMACIÓN

Tabla N° 30: Dimensión seguridad de información

Distribución de frecuencia y respuestas relacionada con la dimensión 02: seguridad de información; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Alternativa	**n**	**%**
SI	19	68
NO	9	32
TOTAL	28	100

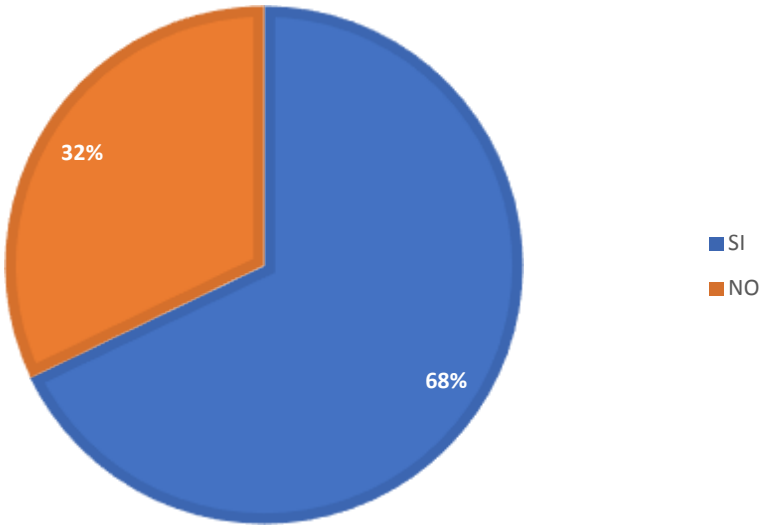
Fuente: Aplicado del instrumento para medir sobre la seguridad de información, basado en 11 preguntas aplicadas a los trabajadores de la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 30 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.

Gráfico N° 3: Resultado de la dimensión 01

Distribución porcentual de frecuencia y respuestas relacionada con la dimensión 02: Seguridad de información; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.



Fuente: Tabla N°30

RESUMEN GENERAL

Tabla N° 31: Resumen general por dimensiones

Distribución de frecuencia y respuestas relacionada con las dos dimensiones para determinar el conocimiento de los trabajadores; para la propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Dimensiones	**SI**		**NO**		**TOTAL**	
	n	**%**	**n**	**%**	**n**	**%**
Situación actual	11	39	17	61	28	100
Seguridad de información	19	68	9	32	28	100

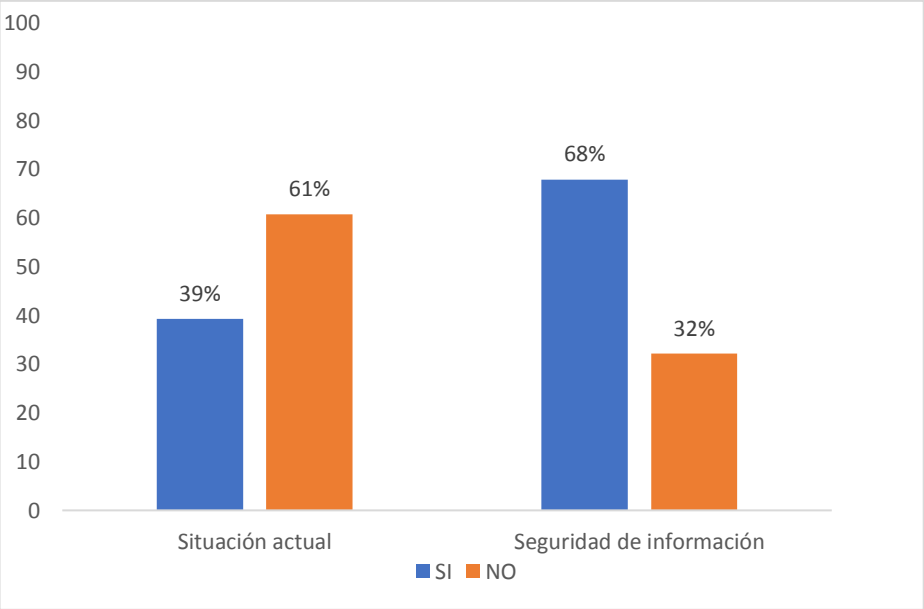
Fuente: Aplicado del instrumento para el conocimiento de los trabajadores encuestados acerca de las dos dimensiones definidas para la investigación, en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Aplicado por: Lara, K.; 2018.

En la Tabla N° 31 se puede observar que en las dos dimensiones el mayor porcentaje de los trabajadores encuestados expresan que la situación actual NO tiene una adecuada gestión para sus procesos, mientras que el menor porcentaje indica SI se están de acuerdo con la propuesta para la seguridad informática que les permitirá brindar confidencialidad a sus clientes.

Gráfico N° 3: Resultado del resumen general

Distribución porcentual de frecuencia y respuestas relacionada con los resultados del resumen general de las dos dimensiones escogidas para la investigación; para el Análisis y diseño del sistema de gestión basado en la norma ISO/IEC 27001 para la seguridad de información, en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.



Fuente: Tabla N° 31

5.2. Análisis de resultados

Esta investigación se enfocó para desarrollar de la Propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018. , tomando en cuenta las dimensiones de estudio: sistema de gestión y seguridad de información; con la finalidad de mejorar los procesos de negocio y la seguridad en la información para mejor la atención al cliente y brindarle mayor confidencialidad, así mismo nos permitirá poder establecer las recomendaciones de mejora.

1. Los resultados obtenidos de dimensión 01: Situación actual; en la presenta investigación mostraron 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. En cuanto Saizarbitoria, Bernardo & Casadesús, (3). En su artículo sobre "La integración de sistemas de gestión basados en estándares internacionales: resultados de un estudio empírico realizado en la CAPV; en el año 2007", realizó un estudio sobre los distintos procesos relacionados con la implantación de los sistemas de gestión basados en estándares internacionales de gestión cabe destacar también el elevado grado de integración que se ha detectado. Tal y como se puede observar en el cuadro 3, la mayoría de las empresas en concreto un 80 %, ha optado por integrar plenamente los principales procesos relacionados con la implantación de sistemas de gestión. Destaca el elevado grado de integración plena de los procesos de control de documentación y de comunicación interna. Por el contrario, los procesos de realización del producto e implementación y planificación son los que cuentan con un menor nivel de integración plena. Se justifica esta coincidencia porque en la clínica Simedic Diagnóstica los trabajadores están de acuerdo que

se elabore un sistema de gestión para poder minimizar los tiempos en realizar las cotizaciones optimizando este proceso realizando consulta, y así brindar un mejor servicio al cliente; además mejorará los procesos del área administrativa al realizar más rápido los pagos de los trabajadores, teniendo un mejor control de asistencia y finalmente se podrá tener un mejor control de la información, por otro lado en el estudio empírico realizado en la CAPV permite saber que la integración de los sistemas de gestión permite un mejor control de documentación y comunicación interna. En conclusión, la integración del sistema de gestión permitirá que los procesos en el área de trabajo se realicen más rápidos y de forma óptima para poder brindar un mejor servicio a los clientes.

2. Los resultados que fueron analizados de la dimensión 02: seguridad de información; en la presente investigación 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. En cuanto Saizarbitoria, Bernardo & Casadesús (3). En su artículo sobre "La integración de sistemas de gestión basados en estándares internacionales: resultados de un estudio empírico realizado en la CAPV; en el año 2007", concluyó que las empresas en relación con su grado de conocimiento sobre los distintos estándares de gestión y en relación también a su opinión sobre la pertinencia o no de que la empresa los implante en el futuro. Pues bien, tal y como se recoge en el cuadro 4, el 78,15% de las personas encuestadas afirman no conocer la norma ISO 27001 (seguridad de información), mientras que el 21,85% si conoce sobre la norma ISO 27001. Se justifica esta concurrencia porque los trabajadores de ambas empresas no conocen sobre la norma ISO 27001 para poder implementarla, por lo tanto la clínica Simedic Diagnóstica S.A.C no brinda protección necesaria

para la documentación interna y esto hace que los trabajadores, como los clientes estar descontentos con el servicio que les brinda la clínica porque su información está expuesta a los peligros que hay al tener toda su documentación en forma manual, en consecuencia el riesgo que existe en la información de ambas empresas conlleva la falta de confidencialidad que se brinda a los usuarios.

5.3. Propuesta de mejora

Después de haber analizados los resultados obtenidos en la presente investigación, se plantea la siguiente propuesta de mejora:

Se desarrollará la documentación exigida por la norma ISO/IEC 27001 para la clínica Simedic Diagnóstica Piura.

La norma ISO 27001 fue elijada para realizar el sistema de gestión de seguridad de información, porque se permitirá ver a la información tanto interna y externa de la clínica como un activo valioso, que debe tener una gestión adecuada, para que los trabajadores puedan trabajar con confianza. Así mismo al implementar esta norma permitirá minimizar los riesgos, al asegurar que se identifican, valoran los activos y sus riesgos, por otro lado, se podrá evaluar los diferentes riesgos y establecer una serie de estrategias, controles oportunos para asegurar la protección y defender la información.

5.3.1. ANÁLISIS DIFERENCIAL DEL ESTADO ACTUAL VERSUS ISO/IEC 27001 Y 27002 I/I

Teniendo como base está definición de la norma ISO27001:2013, este trabajo estará enfocado en analizar todos los controles y requerimientos de seguridad detallados en el Anexo A: ISO/IEC 27002:2013 con los procesos de la clínica Simedic diagnóstica S.A.C, para lo cual se mirará en detalle cada uno de los capítulos la misma, empezando por el numeral 5– Políticas de Seguridad de la información y terminando con el 18- Cumplimiento. Dentro de cada capítulo, existen controles que deben también implementarse.

Los hallazgos a continuación son resultados del análisis de las medidas de seguridad y la normativa que tiene la organización en

relación con la seguridad de la información. Este análisis nos permitirá conocer de manera global el estado actual de la clínica Simedic diagnóstica S.A.C en relación de la seguridad de la información.

Se agrega un valor a cada control en base al estado en el que se encuentra:

0- No esta implementado.

1- Esta parcialmente implementado.

2- Completamente implementado.

Tabla N° 32 ANÁLISIS DIFERENCIAL DEL ESTADO ACTUAL VERSUS ISO/IEC 27001 Y 27002 I/I

Norma	Sección	N°	Descripción	Hallazgos positivos	Hallazgos negativos	Valor
27001 - A.5	5. Políticas de la Seguridad de la Información	5.1	Orientación de la dirección para la gestión de la seguridad de la información			
		5.1.1	Políticas para la seguridad de la información	Existe un documento de políticas	No se tiene evidencia de los entrenamientos realizados a todos los empleados específicamente en las políticas de seguridad. No se incluye en todos los planes de entrenamiento las políticas de seguridad.	1
		5.1.2	Revisión de las políticas de seguridad de la información		las políticas se encuentran desactualizada.	0

	Organización de la Información	6.1	Organización Interna			
		6.1.1	Funciones de seguridad de la Información y las responsabilidades	Se tiene documentado los roles de la compañía y las responsabilidades de cada rol.	No se tiene un rol específico para el responsable del SGSI	1
		6.1.2	La segregación de funciones	existen roles y cargos definidos		2
		6.1.3	Póngase en contacto con las autoridades		No se tiene un documento donde se plasma el procedimiento disciplinario y su aplicación. Tampoco existe un proceso para la recolección de evidencia informática.	0

		6.1.4	Póngase en contacto con los grupos de interés especial		No se encontró un documento donde se centralice la información de grupos de interés.	0
	Organización de la Información	6.2	Dispositivos móviles y teletrabajo			
		6.2.1	Política de dispositivo móvil		No se tienen políticas de sobre el uso de dispositivos móviles, no hay controles para el uso de dispositivos móviles no se tiene analizados los riesgos para el uso de dispositivos móviles.	0

		6.2.2	Teletrabajo		No se tiene política sobre el trabajo remoto, no hay evidencia de una política de trabajo remoto el procedimiento para el acceso de terceros	0
	Seguridad de los Recursos Humanos	7.1	Antes de la contratación laboral			
		7.1.1	Proyección		No se tiene un documento donde se evalúen o se haga seguimiento a los proveedores, no se tiene definido qué tipo de evaluación y proceso se debe hacer para la evaluación de proveedores	0

		7.1.2	Términos y condiciones de empleo	Existen contratos en donde se incluye una cláusula de confidencialidad de la información	En la cláusula de confidencialidad no se tiene estipulado el tiempo por el cual será confidencial la información una vez terminando el contrato	1
	Seguridad de los Recursos Humanos	7.2	Durante la contratación laboral			
		7.2.1	Responsabilidades de gestión	Existen contratos en donde se incluye una cláusula de confidencialidad de la información.	No se tienen acuerdos de confidencialidad donde se definan las recomendaciones de seguridad sobre el tratamiento de la información	1

		7.2.2	Concienciación sobre la seguridad de la información, la educación y la formación		Los trabajadores no reciben entrenamiento en políticas de seguridad de la información, no existen evidencia de que a las personas sean entrenadas en políticas de seguridad en el plan de entrenamientos	0
		7.2.3	Proceso disciplinario		En la evaluación de los empleados no se tiene en cuenta los incidentes de seguridad de la información. No existe un proceso de recolección de evidencia	0
		7.3	Durante la terminación o cambio del contrato			

		7.3.1	La terminación o el cambio de las responsabilidades laborales		No se tiene un proceso documentado para el retiro de personal de la compañía	0
	Gestión de activos	8.1	Responsabilidad por los Activos	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		8.1.1	Inventario de activos	El área de plataforma maneja varios inventarios de activos de información en Excel (hardware y software)	No se tiene un proceso documentado para el inventario de activos.	1
		8.1.2	Propiedad de los bienes	Se tiene un inventario físico y digital de activos de información asignado a cada persona. Se tiene una carpeta de control de facturas de equipos comprados esto con el fin de control.	No se tiene un proceso documentado para la asignación de activos	1

		8.1.3	Uso aceptable de los activos	En el proceso de inducción de nuevos empleados se hace mención del trato y manejo de equipos que se les asigna, dentro del departamento de infraestructura cada técnico tiene asignadas unas áreas una de las premisas es velar por los equipos asignados y enviar correos a los analistas de cada área cuando se identifica maltrato o falta de cuidado de los activos de computo.	no hay un documento de responsabilidad frente a los recursos que se le entregan a los empleados	1

		8.1.4	Retorno de los activos	Se tiene un procedimiento que especifica las actividades de retiro de usuario, formato de retiro que se deposita de manera física en una carpeta del centro de cómputo como evidencia para Auditorías internas y externas.	Se debe complementar el procedimiento con todo el proceso ya que no menciona el proceso de paz y salvo y no hay una actividad dentro del formato que actualice los inventarios y carpetas físicas	1
		8.2	Clasificación de la Información	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		8.2.1	Clasificación de la información	Se tiene un modelo de seguridad para información sensible en servidores. Tip de seguridad que hablan del manejo de directorios compartidos de manera local	No se tiene un proceso formal de clasificación de información, existe información sensible en los equipos de usuarios administrativos	1

		8.2.2	Etiquetado de la información	Se tiene una estándar para el manejo de procesos e instructivos	No se tiene clasificación de la información con marcas de información pública, privada	1
		8.2.3	Manejo de activos	Dentro del archivo de inventario hay un campo de serial y de la maquina único de la misma, modelo, área, responsable, fecha de asignación de la máquina, así mismo en los archivos impresoras, Acces Point y switches	No hay el mismo tratamiento para monitores y equipos de terceros, no hay etiquetas físicas, no están clasificados por información	1
		8.3	Manipulación de Medios	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		8.3.1	Gestión de soportes extraíbles	Existe una estrategia que involucra el manejo y manipulación de medios extraíbles para este caso manejo de discos externos.	No se tiene una política sobre el uso de medios extraíbles no se tiene controles sobre el uso de medios extraíbles para personal administrativo No se monitoreo periódicamente la conexión de medios extraíbles	0
		8.3.2	La eliminación de los medios de comunicación	Se hace una disposición adecuada de los activos a dar de baja y se elimina todo tipo de información corporativa antes de esto la entrega de chatarra tecnológica se realiza.	No se tiene un proceso donde se definan los pasos a seguir en caso de la eliminación segura de equipos, eliminación de información y datos	1

		8.3.3	Transferencia de medios físicos	Los discos son trasladados siempre por una misma persona correo interno de la clínica y con un control en cajas.	La información de los discos no está encriptado, contiene información de la clínica. No existe un sistema para la restricción de los usuarios.	0
	Control de accesos	9.1	Control de Acceso de requerimientos del Negocio	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		9.1.1	Política de control de acceso	Se tiene una política sobre el control de acceso a la información y se sigue un proceso para solicitarlo. Hay una aplicativa que soporta este proceso, el área administrativa donde se encuentra la información más sensible.	No Se tiene clasificación de la información ni clasificaciones de perfiles de acceso	1

		9.1.2	El acceso a las redes y los servicios de red	Se tiene un proceso de solicitud de ingreso de usuario donde se especifica los servicios a asignarle, se tiene un archivo de permisos de carpetas para revisiones de seguridad en usuarios	Se debe tener un proceso de seguridad en red y actividades de revisiones permisos de acceso, Se debe centralizar las revisiones documentadas en un solo proceso y que existe mucha información dispersa se debe actualizar la información de los procesos.	1
		9.2	Gestión de Acceso de Usuarios	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		9.2.1	Registro de usuarios y de la matrícula	Se tienen registros para solicitud de acceso VPN, Solicitud de servicios informáticos para empleado; solicitud de terceros; correo de aprobaciones	se debe actualizar el procedimiento "Actualización de usuarios - Ingreso o Retiro" agregando ítems que apoye el SGSI	1
		9.2.2	Provisión de acceso al usuario	Existe un proceso de ingreso, actualización y retiros a los usuarios de los servicios informáticos, para empleados	No se tiene un sistema de control de acceso para los espacios físicos, se debe crear un el procedimiento "Actualización de usuarios - Ingreso o Retiro". Se debe realizar un estudio de control de acceso para áreas críticas.	1

		9.2.3	Gestión de derechos de acceso privilegiado	Se tiene dentro del proceso de ingreso a la clínica establecer unos servicios y asignarlo a determinados grupos de directorio activo y se les da permisos a bases de datos puntuales, todo a través del formato de ingreso y correos que adicionalmente entregan más información para la creación de usuario.	Se debe crear un sistema para que se pueda actualizar el procedimiento "Actualización de usuarios - Ingreso o Retiro" agregando ítems que apoye el SGSI.	1
		9.2.4	Gestión de la información de autenticación de secreto de los usuarios	En las políticas de seguridad se describe el manejo de contraseñas igualmente se tienen tips de seguridad enviados a todo el personal educando la importancia, uso, creación de contraseñas seguras; se tienen políticas	Se debe establecer una política de contraseña segura donde se defina el uso de caracteres especiales se deben generar controles que garanticen el uso de caracteres especiales en	1

				de grupo de dominio en cuanto a seguridad de contraseñas longitud mínima de 8 caracteres, bloqueo de contraseña 3 intentos fallidos.	las contraseñas se debe crear una política de control de acceso.	
		9.2.5	Revisión de los derechos de acceso de usuario	Se tiene incorporado por el jefe de infraestructura realizar unas revisiones semanales en cuanto a Directorio Activo, Diariamente como parte de la operación infraestructura envía informes en los cuales salen las conexiones establecidas, usuarios, tiempos.	Todas las actividades SGSI no están documentados en el proceso de "Procedimiento de Revisión Seguridad" que defina responsables, periodicidad de revisión y reportes asociados a todo este proceso.	1

		9.3	Responsabilidad de los usuarios	Hallazgo positivo		valor
		9.3.1	El uso de la información secreta de autenticación	se hacen entrenamientos políticos de seguridad donde se establecen las buenas prácticas para el manejo de la contraseña se tiene controles de directorio activo para la creación de contraseñas	Se debe definir una política de manejo de contraseñas y buenas prácticas para el uso de estas que incluyan un límite de historia de contraseñas se deben generar controles que garanticen la no reutilización de un límite de contraseña.	1
		9.4	Control de Acceso a Sistemas y aplicaciones	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		9.4.1	Restricción de acceso Información		No hay un proceso integral que maneje toda la trazabilidad de un usuario.	0

		9.4.2	Procedimientos seguros de inicio de sesión		no se tiene clasificada y documentada la información, las estrategias de autenticación y los procesos de solicitud de permisos a los diferentes sistemas de información	0

		9.4.3	Sistema de gestión de contraseñas	En las políticas de seguridad se describe el manejo de contraseñas creación de contraseñas seguras; se tienen políticas de grupo de dominio en cuanto a seguridad de contraseñas longitud mínima de 8 caracteres, bloqueo de contraseña 3 intentos fallidos, cambio de contraseña cada 3 meses.		2
		9.4.4	El uso de programas de utilidad privilegiados	Existen políticas de grupo a nivel de dominio que restringe el acceso a utilidades del sistema operativo, existen grupos de dominio para acceso a internet restringido; Se tienen reportes de	Se debe actualizar el procedimiento de "revisión de seguridad" ya que no contiene todas las actividades de monitoreo semanal de redes, firewall no están documentadas, no hay	1

				seguimiento y control de servicios de internet, uso de red local.	un documento que especifique los grupos creados en directorio activo sus privilegios y roles.	
		9.4.5	Control de acceso al código fuente del programa		No existen los documentos "Doc Guía - Etapa Implementación" y "Doc Guía - Etapa Desarrollo; " No tiene un sistema para especificar donde se guarda el código, no se menciona control de versiones, no se menciona manejo de cambios de estas fuentes.	0

	Criptografía	10.1	Controles criptográficos	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		10.1.1	Política sobre el uso de controles criptográficos		No se tiene una política de controles criptográficos y en qué caso son necesarios, , para discos externos que salen con información sensible de la empresa	0
		10.1.2	Gestión de claves		No se tiene una política de controles criptográficos y en qué caso son necesarios, para discos externos que salen con información sensible de la empresa	0
	Seguridad física y ambiental	11.1	Áreas Seguras	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		11.1.1	Perímetro de seguridad física	Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados y existen registros que lo evidencian		2
		11.1.2	Controles de entrada físicas	Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados y existen registros que lo evidencian.	Los archivos físicos que tienen información sensible e historia de la compañía no tienen control de acceso por carnet ni cámara cercana, el centro de cómputo no tiene control de acceso ni cámara de seguridad	1

		11.1.3	Asegurar oficinas, salas e instalaciones		No se menciona en el proceso seguridad física el manejo del control de llaves (cómo se maneja), quien es el responsable, por cuanto tiempo se almacena este formato, que personas pueden reclamar las llaves.	0
		11.1.4	La protección contra amenazas externas y ambientales		No se menciona ningún proceso para la seguridad contra las amenazas externas y ambientales.	0
		11.1.5	Trabajar en zonas seguras		No se menciona en el proceso de seguridad física el uso de sistemas seguridad cámaras	0

		11.1.6	Zonas de entrega y carga	Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados y existen registros que lo evidencian	No se tiene un proceso para el manejo de planilla de control ingreso.	1
		11.2	Equipos	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		11.2.1	Emplazamiento y Protección del equipo		No existen procesos, ni alineados que existen análisis de riesgos ambientales documentados.	0

		11.2.2	Apoyo a los servicios públicos	Se tiene incorporado una documentación con las UPS y una vez por año el proceso de mantenimiento con proveedor externo.	No se tiene registro de los mantenimientos de UPS en el proceso, No se menciona en el proceso de instrumentación y electricidad el sistema del centro de cómputo, sus revisiones y mantenimiento	1
		11.2.3	Seguridad del cableado		No hay cableado certificado en la empresa. Se detectó falta de canaletas y separación de cables eléctricos y de datos. No hay un documento o plano de la compañía que apoye las rutas de cableado estructurado.	0

		11.2.4	El mantenimiento del equipo	Se tiene un programa de mantenimientos de equipos tanto lógico como físico. Se tiene un indicador de mantenimiento que se evidencia cada mes.	El proceso de mantenimientos preventivos esta desactualizado hace falta incorporar el indicador de mantenimiento. No se menciona del programa de mantenimientos	1
		11.2.5	La eliminación de los activos	Se tiene incorporado un proceso de registro de dar de baja un equipo. Se tiene incorporado un proceso de desecho tecnológico	El proceso de dar de baja un equipo y que registros se deben realizar no está documentado	1
		11.2.6	Seguridad de los equipos y de los activos fuera del establecimiento	se tiene un proceso de control de salida de equipos de la empresa	No se tiene un sistema en los equipos portátiles. Las personas de seguridad no tienen claridad cuales portátiles son de la	1

					clínica y cuales son personales.	
		11.2.7	La eliminación segura o la reutilización de los equipos	se hace una disposición adecuada de los activos de información y se elimina todo tipo de información corporativa antes de esto los equipos dados de bajo y considerados desechos tecnológicos se les realiza un proceso adecuado	En el proceso "Actualización de usuarios - Ingreso o Retiro" se debe especificar el borrado de la información segura	1
		11.2.8	Equipos de usuario desatendida	Se tienen tips de seguridad educando al usuario con tema equipo desatendidos	Se debe crear una política de equipo desatendido. Se debe implementar un control para el tiempo de inactividad del equipo de cómputo.	1

		11.2.9	Política de escritorio y pantalla clear despejado	Se tienen tips de seguridad educando al usuario con escritorio despejado	Se debe crear una política de escritorio y pantalla despejadas, se debe monitorizar periódicamente la aplicación de la política de escritorio y pantalla despejada	1
	Seguridad en las operaciones	12.1	12. Procedimientos Operacionales y Responsabilidades	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.1.1	Procedimientos operacionales, adecuadamente documentados	Se tienen procesos diarios, semanales, mensuales, de todo el SI que soportan la operación	Se debe actualizar el documento "Manual de seguridad" colocando las tareas operativas y periodicidad	1

		12.1.2	Gestión del cambio	Existe un proceso de gestión de cambios para desarrollo de software. Existe proceso de gestión de cambios para infraestructura. Existe un proceso incorporado en manejo de versiones de aplicaciones de software	No se tiene estandarizado el proceso de Actualización de usuario. Se encuentra información desactualizada.	1
		12.1.3	Gestión de la capacidad	A nivel de desarrollo de software tienen procesos establecidos que les permiten manejar indicadores de calidad y reporte de defectos.	Se debe en el proceso de desarrollo de software detallar el cómo se realiza. No se tiene un proceso estandarizado que especifique la gestión de capacidades.	1
		12.1.4	Separación de desarrollo, prueba y entornos operativos	Se hacen entrenamiento sobre las buenas prácticas de desarrollo	No se evidencia el seguimiento del proceso en cuento los controles de calidad.	1

		12.2	Protección contra código malicioso	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.2.1	Controles contra malware		Se debe ampliar la política de antivirus de las políticas de seguridad de la compañía se debe actualizar procesos relacionados con los monitoreos de la seguridad para que cubran todo lo relacionado con el malware.	0
		12.3	Copias de Respaldo	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.3.1	Copia de seguridad de la información		Los procesos de copias de seguridad no están unificados	0

		12.4	Registro y Seguimiento	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.4.1	El registro de eventos	Se tiene un proceso de revisiones diarias, semanales y mensuales de seguridad y estado de salud de la plataforma.	El procedimiento de revisión de la seguridad se encuentra desactualizado. No se tiene protegida la información en cuanto a la manipulación de registros	1
		12.4.2	Protección de la información de registro	Dentro de los controles establecidos las personas no tienen acceso a la información de diferentes áreas.	No se tiene especificado en el procedimiento revisiones de seguridad quienes son los responsables del acceso, ni la protección a los mismos.	1

		12.4.3	Registros de administrador y operador	Se tiene un proceso incorporado de monitoreo diario, semanal por parte del administrador y el operador de los servicios críticos de la compañía.		2
		12.4.4	Sincronización de reloj	Se tiene un proceso incorporado para la sincronización de la hora de todos los equipos.		2
		12.5	Control de Software Operacional	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		12.5.1	La instalación del software en los sistemas operativos	Se tiene incorporado controles de instalación de aplicaciones en equipos de usuarios. Se tiene incorporado un sistema de actualización de aplicaciones Microsoft.	No se tiene control de instalación de aplicaciones para el área administrativa desde medios extraíbles. No se tiene implementado un sistema de actualización de parches para programas distintos de Microsoft	1
		12.6	Gestión de Vulnerabilidades técnicas	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.6.1	Gestión de vulnerabilidades técnicas	Se tiene incorporado en el mantenimiento del servidor chequeo de vulnerabilidades con el software de Microsoft.		2

		12.7	Consideraciones sobre auditorias de Sistemas de Información	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		12.7.1	Controles de auditoría de sistemas de información	Se tiene incorporada la periodicidad de auditoria.	No se tiene documentado el manual del administrador de seguridad la periodicidad de las auditorias.	1
		13.1	Gestión de la Seguridad de las redes	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		13.1.1	Controles de red	Se tiene un proceso incorporado para las revisiones de todos los servicios de plataforma. Se realizan monitoreos mensuales	El documento Manual del administrador de seguridad informática esta desactualizado las revisiones de los dispositivos.	1

		13.1.2	Seguridad de los servicios de red	Se tiene para los dispositivos de red configurados los roles de acceso a los dispositivos administrador, operador a nivel de dominio se tiene unos grupos creados y determinados accesos para los servicios de plataforma como internet.	No se tiene documentado como se configuran las seguridades de switch. No se tiene dentro del grupo de soporte técnico limitación de acceso al directorio.	1
		13.1.3	La segregación en las redes	Se tiene una documentación completa de la red de la empresa por cada switch e instalado y que dispositivos están conectados a él.		2
		13.2	Transferencia de Información	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		13.2.1	Las políticas y los procedimientos de transferencia de información	Se tiene incorporado en los procesos de inducción y entrenamiento del personal nuevo explicar las buenas prácticas para el uso del correo electrónico, la transferencia de archivos, el uso de la red inalámbrica de visitantes y producción.	Se debe crear una política para el manejo y transferencia de la información a clientes, proveedores, y empleados se debe divulgar la política de transferencia de información a clientes.	1
		13.2.2	Los acuerdos sobre la transferencia de información	Dentro de los contratos proveedores se tienen cláusulas de confidencialidad	Se debe establecer acuerdos de confidencialidad y manejo de la información de acuerdo con la ley con los empleados.	1
		13.2.3	La mensajería electrónica		Se deben establecer para el servicio de correo electrónico metodologías de	0

					encriptados. Se debe para el servicio de mensajería instantánea una política adecuada para el manejo de la información	
		13.2.4	Los acuerdos de confidencialidad o de no divulgación	Se tiene una cláusula de confidencialidad de la información en el contrato laboral (sección 7.3).	No se tiene acuerdos de confidencialidad donde se especifique el manejo adecuado, tiempo de retención y normalización de la información	1
		14.1	Requerimientos de seguridad de los SI	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		14.1.1	Análisis de los requisitos de seguridad de la información y especificación	Dentro de la metodología de desarrollo del proyecto de software se estables los requerimientos no funcionales de la seguridad, se elaboran estrategias de tratamiento a los riesgos según la criticidad del proyecto.		2
		14.1.2	Asegurar los servicios de aplicaciones en las redes públicas	Se tiene a nivel de Firewall protección IDS Las carpetas web server tienen seguridades	se deben fortalecer las políticas de firewall contra ataques Se debe implementar estrategias y protecciones hacia web server a nivel interno.	1
		14.1.3	La protección de las transacciones de servicios de aplicación		se debe establecer para las aplicaciones que manejan y trasmiten información sensible el	0

					uso de códigos criptográficos, certificados, firmas digitales	
		14.2	Seguridad en desarrollo y procesos de soporte	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		14.2.1	Políticas de desarrollo seguro.	Se tienen procesos establecidos para el desarrollo de software las personas del área de desarrollo son entrenadas en buenas prácticas de desarrollo seguro.		2
		14.2.2	Procedimientos de control de cambios del sistema	Se tiene procedimientos de cambios en las aplicaciones y son documentados en actas de entrega de proyectos	Se deben realizar análisis de riesgos de aplicaciones de cada proyecto, donde se identifiquen las amenazas.	1

		14.2.3	Revisión técnica de las aplicaciones después de operar cambios de plataforma	Se tiene incorporado dentro de un proceso de actualización de plataforma realizar reuniones de planeación donde se establecen las actividades, responsables y pruebas.	Se debe crear un procedimiento para la actualización de plataforma donde describa unos lineamientos a seguir se debe actualizar el proceso de pruebas.	1
		14.2.4	Restricciones en los cambios a los paquetes de software	En las aplicaciones que son necesaria se establecen bloqueos para aplicaciones como antivirus en los equipos de los usuarios, sistema operativo	de debe establecer un proceso estándar donde se establezca los lineamientos para elegir las aplicaciones que deben tener bloqueos, activación de logs, seguimientos.	1
		14.2.5	Uso de principios de ingeniería en protección de sistemas	Se tiene para la etapa de implementación unos entregables en la etapa de		2

				desarrollo que confirman requerimientos.		
		14.2.6	Seguridad en entornos de desarrollo	Se tienen incorporado prácticas de revisión de seguridad de micros para el área de informática y desarrollo.	Se debe tener una estrategia de seguridad para los entornos de desarrollo y estaciones de trabajo para proteger la información de estos equipos	2
		14.2.7	Desarrollo Outsourced	no aplica		
		14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	se tiene dentro de la metodología de desarrollo de software una etapa de pruebas funcionales	Se debe incorporar dentro del proceso de pruebas, pruebas de seguridad.	1
		14.2.9	Pruebas de aceptación del sistema		Se debe dentro de la documentación clasificar los tipos de prueba los documentos	0

		14.3	Datos de prueba	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		14.3.1	Protección de los datos de prueba	Los datos de pruebas no contienen información sensible para la compañía, sin embargo de requerirse, estos datos son alterados y no reflejan los reales	Se debe revisar el ambiente de desarrollo y pruebas en cuanto accesos, registros de seguridad	1
		15.1	Seguridad de la Información en la relación con los proveedores	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		15.1.1	Política de seguridad de la información para las relaciones con proveedores	En el contrato se estipulan las condiciones para confidencialidad y política de la información	Se debe incluir en los contratos las formas de tratamiento, retención y transmisión de información, y estas deben acordarse con los proveedores.	1

		15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	Existen un proceso de para la compra de servicios con proveedores, y se establecen los requerimientos del servicio brindado.	Se deben establecer acuerdos de confidencialidad donde se estipulen la forma para el tratamiento de la información, para los proveedores.	1
		15.2	Gestión de la prestación de servicios del proveedor	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		15.2.1	El seguimiento y la revisión de los servicios de proveedores	Se hacen un proceso de selección de proveedor y se evidencia en estudio de las cotizaciones y el análisis costo beneficio al final de cada contrato se hace evaluación de servicio a los proveedores.		2

		15.2.2	Gestión de cambios en los servicios de proveedores	Se siguen las buenas prácticas para el cambio de servicios por terceros.	No se tiene documentado los procesos y buenas prácticas para el control de cambios.	1
		16.1	Gestión de Incidentes y Mejoras en la SI	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		16.1.1	Responsabilidades y procedimientos	Se tiene un informe físico donde se ingresan todos los incidentes que afectan la disponibilidad, integridad y confidencialidad. Dentro de los roles se tiene especificado la función de quienes ingresan y clasifican los incidentes de seguridad.		2
		16.1.2	Informar sobre los eventos de seguridad de información	En el entrenamiento inicial de los empleados se les informa el procedimiento a		2

				seguir para el reporte de incidente		
		16.1.3	Presentación de informes de información debilidades de seguridad	Se tiene un proceso de reporte de incidentes tanto para empleados como proveedores.	Los proveedores externos no conocen el proceso y pueden reportar incidentes	1
		16.1.4.	Valoración de eventos de seguridad de la información y toma de decisiones	Se tiene incorporado en los grupos primarios de informática mensuales el análisis de resultados de las solicitudes atendidas y los reproceso a través de indicadores.	No se tiene clasificación en el sistema de ingreso de incidentes para seguridad, ni la criticidad.	1
		16.1.5	Respuesta a incidentes de seguridad de la información	Se tienen informes de gestión sobre el incidente los cuales son reportados a la dirección mensualmente con un acta de resultados.	No se tiene documentado el proceso donde se definen los tiempos de revisión y línea de mando.	1

		16.1.6	Aprendiendo de los incidentes de seguridad de la información	En cada uno de los incidentes se registra la solución y tratamiento, en caso de requerirse se hacen acciones correctivas, preventivas y de mejoramiento	En cada uno de los incidentes se registra la solución y tratamiento, en caso de requerirse se hacen acciones correctivas, preventivas y de mejoramiento	1
		16.1.7	El acopio de pruebas		No se tiene establecido un proceso para la recolección de evidencia formal	0
		17.1	Continuidad SI	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor

		17.1.1	Información de planificación de continuidad de seguridad		Los documentos del plan de continuidad de negocios se encuentran desactualizado, no se tiene un documento donde se estipulen los tiempos aceptables de recuperación de cada proceso crítico.	0
		17.1.2	Implantación de la continuidad de la seguridad de la información	S	No se tiene establecido un procedimiento que reúna toda la esfera de seguridad en cuanto a información de la clínica, no hay un comité de seguridad para velar las revisiones.	1

		17.1.3	Verificar, revisar y evaluar la información de seguridad de continuidad	El departamento realiza una vez al año como mínimo un simulacro para verificar que los procesos si sean efectivos la información.	No se tiene documentado el plan de simulacros y su periodicidad	1
		17.2	Redundancias	Hallazgo positivo	Hallazgos negativos (Que Falta)	valor
		17.2.1	Disponibilidad de instalaciones para el procesamiento de la información		No se tiene documentado en el plan de continuidad de negocios los servidores redundantes y su tiempo de activación en caso de incidentes.	1

		18.1	Información			
		18.1.1	Identificación de la legislación aplicable y los requisitos contractuales	Existe clausula confidencial; términos legales entre las partes tanto para empleados como para proveedores se tiene clausulas en los contratos para el cuidado de la propiedad intelectual	No se tiene un documento donde se definan y estipulen las leyes aplicables en tema de seguridad informática en la clínica.	1
		18.1.2	Derechos de propiedad intelectual	Se tiene en los contratos una cláusula hacia la propiedad intelectual, cláusula de confidencialidad y manejo de la información. Dentro de las políticas existen secciones para la instalación de software.	No se tiene un documento donde se defina la periodicidad del monitoreo de software.	1
		18.1.3	Protección de los registros	Se tiene controles de acceso a la información que garantizan la confidencialidad, integridad	La información no tiene ninguna clasificación. no se tiene documentación de	1

				y disponibilidad. Se tiene dos archivos físicos de manejo de documentos los cuales son controlados por uso de llave y autorización de personas solo autorizadas.	los procesos de clasificación de y tipos de protección y cuidados que se tiene para cada tipo de información.	
		18.1.4	Privacidad y protección de datos personales	Se tiene controles de acceso a la información que garantizan la confidencialidad, integridad y disponibilidad. los documentos físicos están bajo llave en zonas seguras y solo pueden ser accedidos por personal autorizado.	No se tiene documentación de los procesos de clasificación de y tipos de protección y cuidados que se tiene para cada tipo de información las personas.	1
		18.1.5	Regulación de los controles criptográficos	Se tiene controles criptográficos establecidos para los servicios de comunicación y	No se tiene documentados los procesos criptográficos	1

				transferencia de información.	de la clínica y en qué casos estos aplican.	
		18.2	Revisiones de SI			
		18.2.1	Revisión independiente de la seguridad de la información	Se tienen procesos de revisiones diarias, semanales y mensuales en cuanto a seguridad y salud de la plataforma; se tiene dentro del proceso de plataforma auditorías internas a los procesos de seguridad, 2 veces al año. Se hacen auditorías externas las áreas de informática a los diferentes procesos de plataforma se tiene planes de auditorías a los procesos.	Se debe incorporar en la programación de auditorías internas el sistema de gestión de seguridad de la información se debe actualizar el procedimiento de revisiones de seguridad agregando los reportes de servicios y vulnerabilidades técnicas y demás generalidades de SGSI	1

		18.2.2	El cumplimiento de las políticas y normas de seguridad		Se debe establecer una política donde se defina el tratamiento de la información segura y buenas prácticas se deben establecer controles para monitorizar y reportar todo uso indebido de los sistemas de información.	0
		18.2.3	Revisión de cumplimiento técnico		No se tiene definido el proceso formal para la revisión de actividades diarias de los servicios de infraestructura.	0

Fuente: Elaboración propia.

Tras el análisis completo de los diferentes dominios se encontró que, de un total de 114 ítems, 40 de estos no se cumplen, 61 se cumplen parcialmente y 13 se cumplen satisfactoriamente.

En lo que respecta a las políticas de seguridad no se cuenta con la documentación necesaria a los procedimientos y controles que ayuden a garantizar la seguridad de información, por otro lado, se realizó el análisis de la seguridad de la información en la organización se cuenta con acuerdos de confidencialidad, sin embargo, no tiene la documentación adecuada y clara en los roles para el control adecuado de la operación de la seguridad.

Asimismo, se observa que la seguridad de los recursos humanos no se cuenta con un control adecuado para los procesos referentes a la terminación de contratos, tampoco tiene un control de los equipos que serán devueltos a la culminación del contrato de los empleados. Por otro lado, en la gestión de activos se puede observar, que, aunque se ha trabajado en el inventario de activos, este no se encuentra actualizado en su totalidad, así mismo no se tiene procedimientos para las clasificaciones de la información.

En el control de accesos se cuenta con el uso de contraseñas, sin embargo, no se cuenta con documentación formal, mientras que en lo que respecta a la criptografía se observa que no existe procedimientos en todo lo relacionado al uso de las llaves criptográficas.

En la seguridad física y ambiental no se cuenta con una protección completa en la alimentación eléctrica, lo que evidencia falta de seguridad en el cableado y la restricción en el uso de los equipos móviles: así mismo se detectan errores en la seguridad en las

operaciones, puesto que no se cuenta con logs y/o contarles en la gestión de medios informativos.

En relación con los proveedores no se cuentan con un control adecuado referente a los requisitos de seguridad, tiendo en cuenta toda la comunicación, para el aseguramiento de la protección de los activos; así como en la gestión de incidentes de seguridad no se cuenta con una correcta gestión, para la recolección de evidencia.

Según el análisis realizado, se observa a nivel general, que se requiere una intervención inmediata a nivel de los dominios relacionados con políticas de seguridad, continuidad del negocio, control de accesos, criptografía y relación con los proveedores, puesto que son los que tiene mayor índice de incumplimiento con la norma y afectan la seguridad de la información que se requiere.

Gestión de riesgos

La realización del análisis de riesgos tiene como fin identificar de manera clara los riesgos a los cuales está expuesta la organización, y basados en esta identificación de los riesgos determinar cuáles son las medidas de seguridad adecuadas para los diferentes activos de seguridad de la información, de igual manera permite establecer los planes de contingencia, para este caso realizaremos un análisis de riesgo, que es un tipo de análisis que se realiza teniendo en cuentas las medidas de seguridad que la clínica ya tienen planteadas.

Por otro lado, describe la metodología a utilizar para la gestión de riesgos, derivados de las tecnologías de la información, así como el inventario de los activos de la clínica Simedic diagnóstica Piura y la valorización de estos. Se tendrá en cuenta la confidencialidad,

integridad y disponibilidad de la información, realizando de esta forma el análisis de amenazas y la valorización de los riesgos.

La metodología para realizar para la gestión de riesgos es MARGERIT que permitirá la implementación en el proceso de gestión de riesgos dentro de un marco de trabajo, que ayudará a la toma de decisiones teniendo en cuenta los riesgos derivados del uso de las tecnologías de la información.

Por otro lado ayudara a concientizar a los responsables de la organización de información de la existencia de riesgos y de la necesidad de gestionarlos, así mismo permitirá a analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones, por otro lados ayudara a descubrir y planificar el tratamiento oportuno para los riegos bajo control y finalmente ayudará a preparar a la clínica Simedic Diagnóstica con los procesos de evaluación, auditorio y certificación o acreditación según corresponde en cada caso.

Inventario de activos

Un análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado todos los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

Tabla N° 33 Inventario de los activos

Ámbito	Activo
Instalaciones	Ubicación local de infraestructura y comunicaciones
	sala eléctrica, ups, telecomunicaciones
Hardware	Servidores

	Equipos escritorio, portátiles
	Equipos de comunicaciones
	router inalámbrico
	telefonía
Software	Windows 2008 PRO
Aplicaciones	Paquete de office
	Correo empresarial
	Antivirus: ESET NOD32
	Sistema de backups: ESET NOD32
Datos	Información contable y administrativa
	Formatos documentales (manuales y acceso)
	Registros de operación: logs, informes y monitoreo
	Datos de proveedores y usuarios
Red	Red de datos
	Red de telefonía
	acceso a Internet
Servicios	Internet (navegador Chrome)
	Telefonía
	Servicio de internet, telefonía y cable de Movistar.
	Correo
Equipos adicionales	Generadores de energía
	Sistema de alimentación UPS
	Sistema de aire acondicionado
	Equipos de control de temperatura
Personal	Gerente
	Personal administrativo
	Personal para atención al cliente
	Personal para las atenciones medicas
	Jefe de informática

Soportes de información	Discos duros de servidores.
	Discos externos información de backups
	Unidades de CD, DVD y Memorias extraíbles

Fuente: Elaboración propia.

Valoración de activos

Siguiendo la metodología se define una tabla de valoración de activos con el fin de utilizarla para la evaluación de los activos de información.

Las escalas de valoración de los activos son las siguientes categorías muy bajo, bajo, medio, alto y Muy alto.

Tabla N° 34 Valor de los activos.

MA	Muy alta
A	Alta
M	Media
B	Baja
MB	Muy baja

Fuente: Libro de Magerit (28).

En esta tabla quedan establecidas las abreviaturas que se utilizaran para la valoración de los activos de información.

Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe indicarse cuál es el aspecto de la seguridad más crítico.

Identificados los activos se realiza entonces la valoración ACIDA de los mismos. Dicha valoración viene a medir la criticidad en las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio. Esta valoración valorar el impacto que tendrá la materialización de una amenaza sobre la parte de activo expuestos.

Cada activo de información puede poseer un valor diferente en cada una de las diferentes dimensiones para la organización que deseemos analizar.

En este caso utilizaremos una escala de valoración de diez valores siguiendo los siguientes criterios:

Tabla N° 35 Escala de valoración

Valor	Criterio
10	Daño muy grave de la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Fuente: Libro de Magerit (28).

A continuación, la valoración de las dimensiones de seguridad de los activos que incluyen aspectos como Autenticidad, Criticidad, Integridad, Disponibilidad y trazabilidad.

Tabla N° 36 Valoración de seguridad de los activos

Valoración Dimensiones de Seguridad de los Activos							
Ámbito	Activo	Valor	Aspectos Críticos				
			A	C	I	D	T
Instalaciones	Ubicación local de infraestructura y comunicaciones	Muy Alto				10	
	sala eléctrica, ups, telecomunicaciones	Alto				7	
Hardware	Servidores	Muy Alto	10	10	10	8	10
	Equipos escritorio, portátiles	Alto	8	6	7	7	7
	Equipos de comunicaciones	Muy Alto	10	9	9	10	9
	router inalámbrico	Alto	9	9	9	8	9
Aplicaciones	Sistemas Operativos: Windows 2010	Muy Alto	10	9	8	10	10
	Paquete de office	Medio	5	6	6	7	7
	Correo empresarial	Alto	9	8	8	7	8
	Antivirus: ESET NOD32	Alto	9	6	8	6	8
	Sistema de backups: ESET NOD32	Alto	9	9	8	6	8
Datos	Información contable y administrativa	Muy Alto	10	10	10	10	10
	Formatos documentales (manuales y acceso)	Muy Alto	9	9	9	10	9

	Registros de operación: logs, informes y monitoreo	Alto	9	8	8	9	8
	Datos de proveedores y usuarios	Alto	9	9	9	10	9
Red	Red de datos	Muy Alto				10	
	Red de telefonía	Medio				7	
	acceso a Internet	Alto				9	
Servicios	Internet (navegador Chrome)	Alto				9	
	Telefonía	Medio				7	
	Cable de Movistar.	Medio				7	
	Correo	Muy Alto				10	
Equipos adicionales	Generadores de energía	Muy Alto				10	
	Sistema de alimentación UPS	Muy Alto				10	
	Sistema de aire acondicionado	Alto				9	
	Equipos de control de temperatura	Medio				8	
Personal	Gerente	Muy alto		10		10	
	Personal administrativo	Muy alto		10		10	
	Personal para atención al cliente	Alto		8		8	
	Personal para las atenciones medicas	Muy Alto		10		10	
	Jefe de informática	Alto		9		9	

Soportes de Información	Discos duros de servidores.	Muy Alto	10	10	10	10	10
	Discos externos información de backups	Muy Alto	9	7	10	8	10
	Unidades de CD, DVD y Memorias extraíbles	Alto		6	8	7	

Fuente: Elaboración propia.

Análisis de amenazas

Una vez definidos los activos y su valor para la organización, se debe realizar un análisis que muestre cuales son los activos que siempre están expuestos a amenazas y estas pueden afectar a los distintos aspectos de la seguridad, para posteriormente estimar cuan vulnerable es el activo para dicha amenaza.

De acuerdo con lo anterior, se procedió a realizar la clasificación de las amenazas utilizando las tablas existentes en el libro 2: catálogo de elementos de Margerit, el cual seguiré la agrupación de las amenazas en cuatro grupos:

Desastres naturales, de origen industrial, errores y fallos no interconectados, y amenazas intencionales presenciales. Realizándose la siguiente tabla de amenazas:

Tabla N° 37 Análisis de amenazas

	Amenazas	Dimensión afectada					Activos Afectados							
		D	I	C	T	A	Hardware	Red	Instalaciones	Aplicaciones	Información	Datos	Servicios	Personal
Desastres Naturales	Fuego	X					X	X	X		X			
	Daños por agua	X					X	X	X		X			
	Inundación	X					X	X	X		X			
	Siniestro mayor	X					X	X	X		X			
	Fenómeno sísmico	X					X	X	X		X			
	Fenómeno meteorológico	X					X	X	X		X			
Accidentes de origen industrial	Fuego	X					X	X	X		X			
	Daños por agua	X					X	X	X		X			
	Sobrecarga eléctrica	X					X	X	X		X			
	Fluctuación eléctrica	X	X				X	X		X	X			
	Contaminación mecánica	X					X							
	Contaminación electromagnética	X					X		X					

	Avería de origen físico o lógico	X	X				X			X				
	Corte del suministro eléctrico	X					X	X	X					
	Condiciones inadecuadas de temperatura o humedad	X	X				X		X		X			
	Fallos de servicios de comunicaciones	X						X						
	Interrupción de otros servicios y suministros esenciales	X					X							
	Degradación de los soportes de almacenamiento de la información	X									X			
	Emanaciones electromagnéticas			X			X		X	X				
Errores y fallas no intencionados	Errores de los usuarios	X	X	X						X	X	X	X	
	Errores del administrador	X	X	X			X	X		X	X	X	X	
	Errores de monitorización		X		X						X			
	Errores de configuración		X								X			
	Deficiencias en la organización	X												X
	Difusión de software dañino	X	X	X						X				
	Errores de re-encaminamiento			X				X		X			X	
	Errores de secuencia		X					X		X			X	
	Escapes de información			X							X			

	Destrucción de información	X	X					X	X	X		X	X	
	Fugas de información			X						X	X	X	X	X
	Vulnerabilidades de los programas	X	X	X						X				
	Errores de mantenimiento/ actualizaciones de programas (software)	X	X							X				
	Errores de mantenimiento/ actualizaciones de equipos (hardware)	X					X	X						
	Caída del sistema por agotamiento de recursos	X					X	X					X	
	Pérdidas de equipos	X		X			X							
	Indisponibilidad del personal	X												X
Amenazas intencionales presenciales	Manipulación de los registros en actividad		X		X									
	Suplantación de la identidad del usuario		X	X		X		X		X		X	X	
	Abusos de privilegios de acceso	X	X	X						X				
	Re-encaminamiento de mensajes			X				X		X			X	
	Alteración de secuencias		X					X		X			X	
	Acceso no autorizado		X	X			X	X	X	X	X	X	X	
	Análisis de tráfico			X				X						X
	Repudio		X				X							
	Interceptación de información (Escucha)			X				X						
	Modificación deliberada de la información		X					X	X	X	X	X	X	
	Destrucción de información	X							X	X		X	X	

	Divulgación de información		X						X	X	X	X	X	
	Manipulación de programas	X	X	X						X				
	Manipulación de los equipos	X		X			X							
	Denegación de servicio	X					X	X					X	
	Robo	X		X			X							
	Ataque destructivo	X					X		X		X			
	Indisponibilidad del personal	X												X
	Extorsión	X	X	X										X
	Ingeniería social	X	X	X										X

Fuente: Elaboración propia.

Después de analizar los activos se encontraron más relevantes para la unidad son: la información y la infraestructura. Así mismo los datos, recursos humanos y respaldos (copias de seguridad), se constituyen en los activos que dan el valor agregado a la clínica.

Después de hacer el análisis de las posibles amenazas se ubicaron las siguientes como las posibles sobre los sistemas información:

Todas las relacionados con desastres naturales sobre las instalaciones, encontrándose que el impacto en caso de materializarse dejaría inoperativa la unidad.

Las amenazas de difusión de software dañino y destrucción de información se contribuyen en las que más activos impactan, teniendo un valor muy alto. Estoy es debido a que los procesos dentro de la clínica no tienen una adecuada protección para el canal de datos, los equipos y las aplicaciones de manera apropiada, se puede tener una caída a la clínica, dejando así inoperativo durante cierto tiempo, y creando destrucción en todos los procesos de la clínica. En otras áreas como la atención a los clientes puede verse afectada e interrumpida para sus procesos de evaluación y diagnostico que brinda la clínica.

Propuesta de proyectos

Introducción

En este momento ya se conoce el estado actual de la clínica Simedic Diagnóstica y los riesgos que afronta, por lo cual debe plantearse proyectos que ayuden a alcanzar los niveles de seguridad que se requieren.

Los proyectos que se proponen a continuación son resultados del análisis de riesgo, y a solicitud de la clínica para mejorar todos sus procesos. Para este caso se presentarán dos proyectos los cuales consisten en el plan de capacitación y de continuidad del negocio, además se formulará un plan de concientización en seguridad de la información para el personal.

Objetivos

Plan de capacitación

- Construir y mejorar el manejo de la seguridad de información de la clínica.

Plan de continuidad

- Asegurar la continuidad de la clínica ante diversas situaciones.
- Llevar los riegos a un nivel aceptable.

Plan de mitigación de riesgos

- Establecer acciones para mitigar los riesgos por difusión de software dañino, interceptación de información, y destrucción de información.

La siguiente tabla muestra la relación de los proyectos con los riesgos identificados para mitigar, y las dimensiones que se ve impactado.

Tabla N° 38 Relación de proyectos

Proyectos	Amenazas identificadas	Dimensiones	Acciones	Impacto	Prioridad del desarrollo
Plan de capacitación	Errores de los usuarios	Integridad	Cursos de capacitación	Alto	Medio
	Errores del administrador	Integridad	Cursos de capacitación	Alto	Medio
	Deficiencias en la organización	Disponibilidad	Campaña publicitaria	Medio	Medio
	Destrucción de la información	Integridad	Concienciación	Alto	Alto
	Fugas de información	Confidencialidad	Concienciación	Alto	Alto
Plan de continuidad	Fuego (Problemas industriales)	Disponibilidad	Generar un plan de acción	Alto	Alto
	Avería de origen físico o lógico	Disponibilidad	Generar un plan de acción	Alto	Alto
	Corte del suministro eléctrico	Disponibilidad	Establecer grupos de respuesta	Medio	Medio
	Sobrecarga eléctrica	Disponibilidad	Establecer grupos de respuesta	Medio	Medio
	Fluctuación eléctrica	Disponibilidad	Establecer grupos de respuesta	Medio	Medio
	Fuego	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
	Daños por agua	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
	Inundación	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto

	Siniestro mayor	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
	Fenómeno sísmico	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
	Ataque destructivo	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
Plan de mitigación de riesgos	Interceptación de información	Integridad y disponibilidad	Bloqueo de puertos de comunicación para empleados	Alto	Alto
	Destrucción de información	Disponibilidad	Bloqueo de puertos de comunicación para empleados	Alto	Alto
	Difusión de software dañino	Disponibilidad e integridad	Establecer políticas de uso de software, políticas de intercambio de información y actualización de políticas de uso de TIC.	Medio	Medio

Fuente: Elaboración propia.

A continuación, se describen los proyectos planteados anteriormente.

Plan de continuidad del negocio

Alcance:

El plan de continuidad busca generar las pautas que permitan restablecer en el menor tiempo posible la operatividad del negocio a causa de eventos que impidan su funcionamiento de manera parcial o total.

Los procedimientos planteados en este documento son las acciones por realizar en relación con el hardware, software y equipos activos involucrados en los procesos críticos definidos en este plan.

Adicionalmente se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos del área de informática para ser implementado un centro de datos para toda la información que se interconecta con las diferentes áreas de la clínica.

El plan de continuidad de la clínica busca reducir el riesgo de las amenazas de fluctuación eléctrica, avería de origen físico o lógico, fuego, daños por agua, inundación, siniestro mayor, fenómeno sísmico, fue, sobrecarga eléctrica, corte del suministro eléctrico, destrucción de información, ataque destructivo, con respecto a la disponibilidad en el área de informática.

Fases:

Evaluación del estado actual: Se realizo un análisis de riesgo para identificar los activos con que cuenta, activos críticos a ser protegidos y el estado de los a controles actuales y la definición de los equipos que deben ser adquiridos, los procesos y procedimientos que deben ser desarrollados. Esto se ha desarrollado a lo largo del documento.

Estrategia de respaldo: la clínica deberá implementar un centro de datos que permita la seguridad de todos los activos de información. Así mismo evaluar los recursos técnicos y humanos para dicha operación.

Desarrollo del plan: En esta etapa se definirán los equipos necesarios para un desarrollo adecuado del plan, además de sus responsabilidades y funciones, También se hará una descripción de los procedimientos de aleta y actuación ante los eventos que pueden llegar a activar el plan.

Pruebas: Se realizarán las pruebas pertinentes para verificar que el plan funciona correctamente.

Capacitación: se realizará la capacitación y el entrenamiento respectivo al personal a cargo del plan de contingencias y se realiza un plan de concientización entre todo el personal.

Puesta en marcha del plan, adicionalmente se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos del área de informática principal para implementar el centro de datos.

Plan de capacitación

Alcance

El plan de capacitación involucra al personal administrativos, atención al cliente y médicos. Así mismo para el personal administrativo deberá recibir capacitaciones de nivel medio y jurídico de modo que se mejore el manejo de la seguridad de la información.

El plan de concienciación está orientado a disminuir el nivel de riesgo presente con resto a deficiencias en la organización y fugas de información que fueron identificados en todo el personal de la clínica.

Fases:

Diseño del plan de sensibilización: En esta etapa se diseñarán estrategias para sensibilizar a todo el personal de la clínica. Para ello se utilizarán diferentes estrategias.

Diseño del plan de capacitación: En esta fase se revisará y diseñará los cursos relacionados con seguridad de la información para personal clave, así como talleres prácticos para todo el personal.

Consecución de recursos: En esta etapa se realizará la gestión de recurso financiero y de personal que se necesitan para poner en funcionamiento el plan de sensibilización y capacitación.

Plan de mitigación de riesgos

Alcance:

El plan de mitigación de riesgos busca establecer acciones y recursos que restrinjan de la mejor forma posible la propagación de software autoejecutable o que intercambiar información tanto en los equipos de cómputo, como en las aplicaciones y las redes utilizadas por la clínica. Así mismo se busca con este plan restringir el acceso a la información contenida en los discos duros de los equipos de cómputo, de acuerdo con los niveles de acceso del personal.

Objetivos:

Establecer las acciones encaminadas a mitigar los riesgos más relevantes detectados en el análisis de riesgos ante alguna eventualidad de toda acción que lo pueda paralizar, ya sea de forma parcial o total.

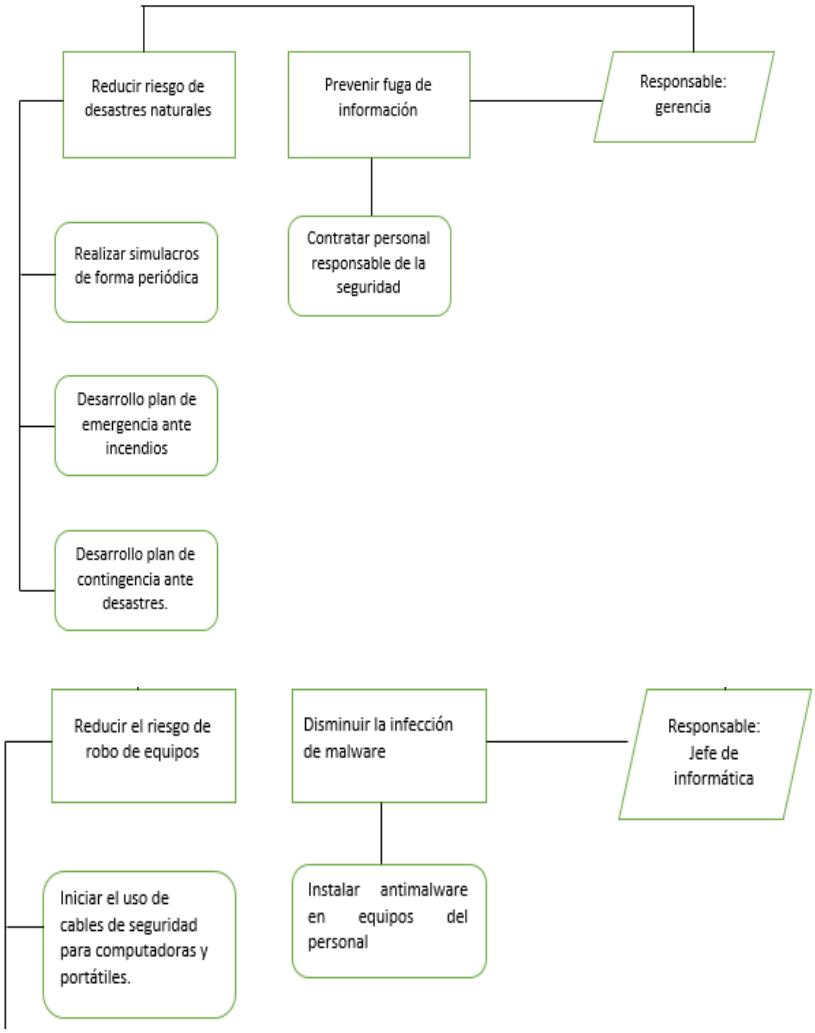
Plan de ejecución

A continuo se aplicarán salvaguardas para implementar el plan de gestión de los riesgos existentes. En primera instancia se deberá aplicar las salvaguardas en niveles con prioridad mayor es decir medidas preventivas y luego las salvaguardas con niveles superiores que conforman las medidas correctoras.

Entre las salvaguardas de mayor prioridad se encuentran la prevención contra incendios y terremotos, prevención de la fuga de información, prevención de perdida de almacenamiento y la prevención de acceso no autorizado.

A continuación, se muestra cómo aplicar las salvaguardas para prevenir y reducir los riesgos en este nivel.

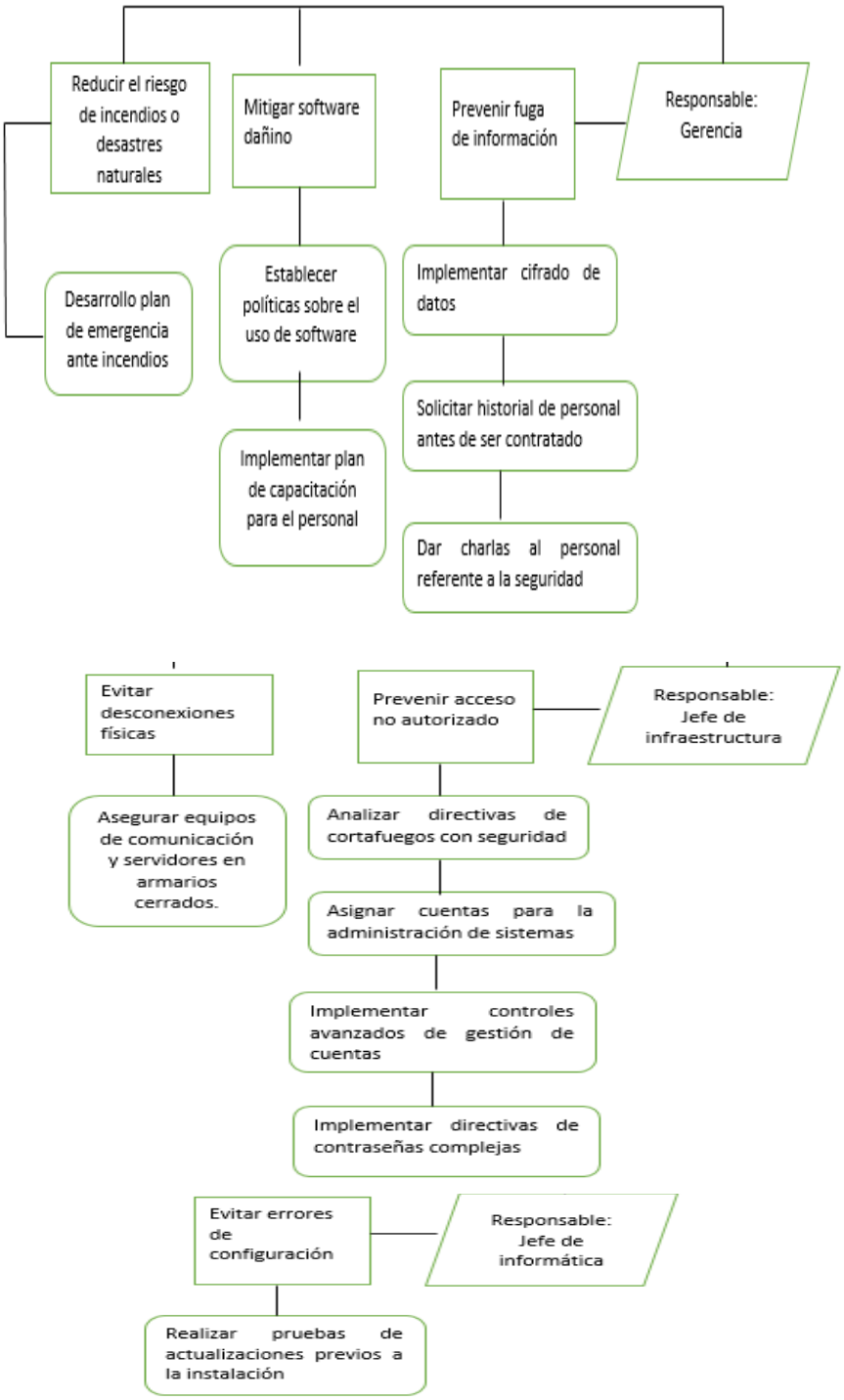
Gráfico N° 4 Salvaguardas en primer nivel



Fuente: Elaboración propia.

Se muestra cómo aplicar las salvaguardas para los procesos que requieren de mejoras en la gestión.

Gráfico N° 5 Salvaguardas de mejoras en la gestión



Fuente: Elaboración propia.

Luego de haber definido e implementado los diversos procesos a realizar dentro del plan de seguridad es necesario volver a realizar un nuevo análisis de riesgo para conocer el nivel de riesgo obtenido y así tratar de analizar las medidas de seguridad necesarias para mantener la seguridad de información.

Por otro lado, estas normas generales permitirán disminuir los riesgos en la clínica:

1. Ofrecer un mejor servicio a los pacientes, garantizando que se aplique los controles necesarios para asegurar su información.

2. Brindar confidencialidad a los trabajadores y proveedores por la información que tiene la clínica, así mismo los trabajadores deberán asumir una responsabilidad individual respecto a los criterios de confidencialidad, integridad y disponibilidad de los sistemas y tecnologías, así como del uso de información privilegiada.

3. Cumplir con los requerimientos legales en cuento a la protección de la información de los clientes.

4. Dar a conocer a los trabajadores sobre la importación del SGSI, así como su responsabilidad sobre el cumplimiento de los dispuestos por el SGSI.

5. La información y los recursos de vital importancia como activos en la Clínica Simedic Diagnóstica, debe ser utilizados con responsabilidad, bajo los principios de ética y moral, para protegerlos.

El tiempo de implantar del plan de seguridad no ha sido considero para este porque depende de una serie de factores como financieros y administrativos.

Finalmente se ha desarrollado un plan de ejecución que conlleva la participación del personal de varias área e implementación y mejorar de procesos aplicando medidas preventivas correctoras para reducir los niveles de riesgo existentes.

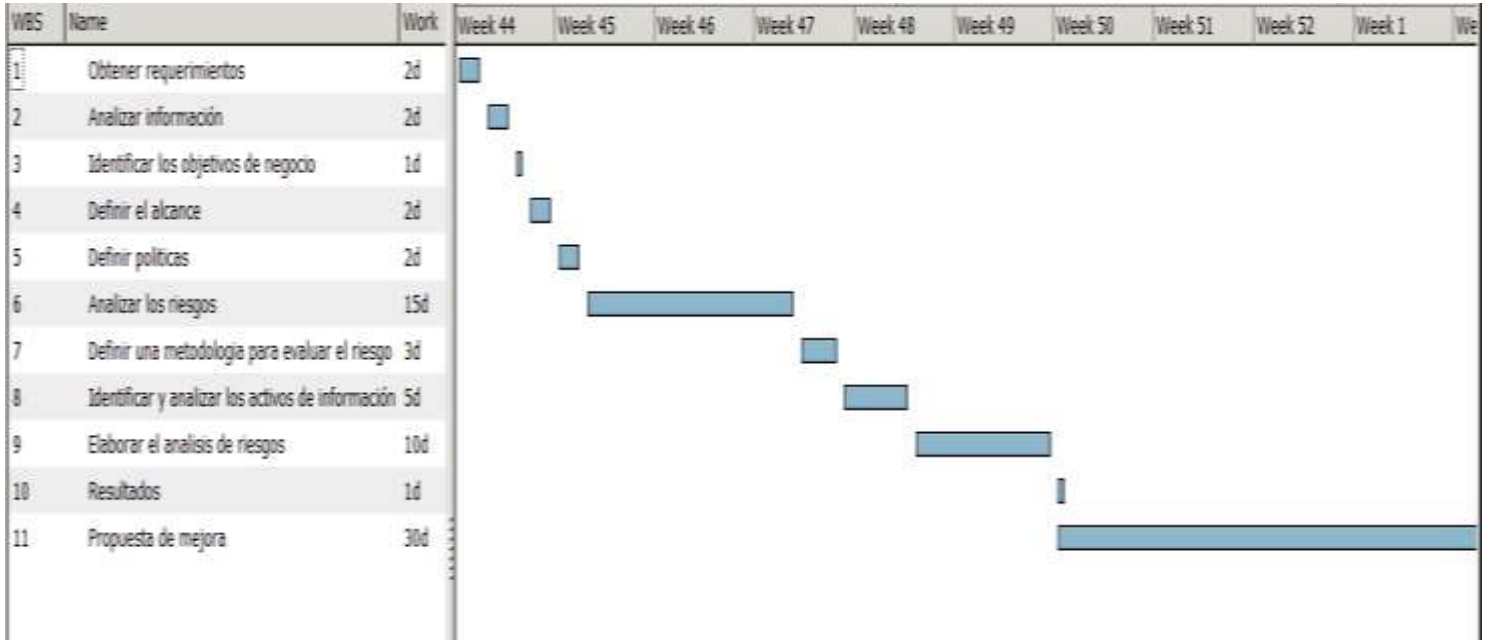
Es importante mencionar que las salvaguardas sugieren permitir minimizar los riesgos, pero cada una tiene un costo por lo que en cada caso en particular se debe evaluar el valor de la información a proteger y los costos que implicaría la pérdida o el sufrimiento de un ataque y en este sentido planificar las acciones pertinentes para la protección de tal información.

Los resultados ayudaran a la organización a reconocer la necesidad de iniciar la implementación de un plan de gestión de riesgos que permiten mitigar los riesgos más críticos, hasta que decidan desarrollar un plan de tratamiento de riesgo en el que se considera la contratación del personal especializado en seguridad, análisis de documentos y registros de incidente

5.3.2. Plazo de ejecución

La implementación del sistema se llevará acabó en un plazo no mayor de 80 días

Gráfico N° 6 Tiempo de realización



Fuente: Elaboración propia

5.3.3. Propuesta económica

Tabla N° 39 Propuesta económica

Equipos y materiales	**Costo S/**	**Cantidad**	**Total S/**
Laptop	1500.00	2	3000.00
impresora	200.00	1	200.00
Memoria USB Gb	20.00	2	40.00
Caja de lapiceros	22.00	1	22.00
1/2 millar de hojas A4	16.00	1	16.00
Total			S/ 3278.00
Recursos Humanos	**Costo S/**	**Cantidad**	**Total**
Experto	2000.00	1	2000.00
Supervisor	1500.00	1	1500.00
Total			S/ 3500.00
Otros Gastos	**Costo /S.**	**Cantidad**	**Total**
Movilidad	5.00		300.00
Total			300.00
Total de inversión			S/ 7078.00

Fuente: Elaboración propia.

VI. CONCLUSIONES

De acuerdo con los resultados obtenidos en la investigación titulada el análisis y diseño del sistema de gestión basado en la norma ISO/IEC 27001 para la seguridad de información, en la clínica Simedic Diagnóstica S.A.C – Piura; queda demostrada que para se necesita mejorar la atención al cliente y la seguridad de información en la clínica Simedic Diagnóstica; este resultado es semejante al indicado en la hipótesis general por lo que se concluye que queda aceptada.

En cuento a las dimensiones, se concluye con lo siguiente:

1. En la Tabla N°31 se observó 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, por lo tanto, no cuenta con la seguridad adecuada para los activos de la clínica, este resultado es similar al indicado en la hipótesis especifica por lo que se concluye que queda aceptada.

2. En la Tabla Nro.31 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, por lo tanto, se requiere la implementación de la norma ISO 27001, este resultado es similar al indicado en la hipótesis específica por lo que se concluye que queda aceptada.

RECOMENDACIONES

Dentro de una Tesis como está siempre se desea la mejora continua y la seguridad de su personal y sus clientes para ello se presentarán a continuación algunas recomendaciones para su buen desarrollo y excelente final de este proyecto:

1. Se sugiere que en la clínica Simedic Diagnóstica Piura implementar la norma ISO/IEC 27001:2014 que le permitirá brindar seguridad en los activos de información y protegerlos en caso de alguna vulnerabilidad de información.

2. Se propone que los trabajadores reciban capacitaciones sobre la seguridad de información para que se puedan adaptar al nuevo cambio con la implementación de la ISO/IEC 27001:2014.

3. Se pide que las políticas que se establecieron para mejorar la seguridad en la clínica sean cumplidas por todos los trabajadores, esto permitirá evaluar los riesgos y poder prevenirlos.

4. Se plantea utilizar software ISOTools para la implementación de la norma porque que ayuda a las organizaciones comprometidas con la calidad y la excelencia a Optimizar sus modelos y sistemas de gestión y facilita la aplicación de estos, haciéndolos accesibles, ágiles y medibles, y aportando resultados en el corto plazo.

REFERENCIAS BIBLIOGRÁFICAS

1. Lluís M, Mas A, Amengual E, Cabestrero. Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. Revista Española de Innovación, Calidad e Ingeniería del Software. 2010 ; VI(3).
2. Pallas M. Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Maestría. Montevideo: Instituto de Computación – Facultad de Ingeniería Universidad de la República, Ingeniería en Computación; 2009. Report No.: 1510 7264.
3. Heras I, Bernardo M, Casadesús F. La integración de sistemas de gestión basados en estándares internacionales: resultados de un estudio empírico realizado en la CAPV. Revista de Dirección y Administración de Empresas. 2007 diciembre;(14).
4. Talavera V. Diseno de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001. pregrado. Lima: pontificia universidad católica del perú, ciencias e ingeniería; 2013.
5. Vivanco M, Cortez V, Bustamante V. La seguridad de la información. Revista de Investigación de Sistemas e Informática. 2011;(8).
6. Villena M. Sistema de gestión de seguridad de información para una institución financiera. Pregrado. Lima: Pontificia universidad católica del Perú, ciencias e ingenieria; 2006.
7. Nizama M. Evaluación de la seguridad para el personal informático y usuarios de sistemas en la Municipalidad Provincial de Piura. In Crescendo. 2018; II(11).
8. De la Cruz A. Mejora del programa de seguridad basada en el comportamiento del sistema integrado de gestión de prevención de riesgos y medio ambiente de GYM S.A. Pregrado. Piura: Universidad de Piura, Ingeniería; 2014.
9. Miranda K. Guia metodologíca para implementar un sistema de gestión de seguridad en instituciones. Tesis de máster. Piura: Universidad de Piura, departamento de ingenieria ; 2013.

10. Organización mundial de la salud. Organización mundial de la salud. [Online].; 2014 [cited 2018 10 2. Available from: http://www.who.int/mediacentre/factsheets/fs389/es/.
11. Tudón J. La medicina del trabajo y la salud ocupacional. Latinoamericana se la Salus y el Trabajo. 2014; 4(2): p. 45.
12. Coppee G. Los servicios de la Salud en el trabajo y la práctica Madrid: Enciclopedia de salud y deguridad en el trabajo; 2013.
13. Gastañaga M. Historia y retos del futuro occupational. revista Peru Med Exp Salud Publica. 2012; II(29): p. 177-78.
14. Academia Peruana de Salud. Salud y Desarrollo. Historia de la salud en el Peru. 2007; I(14): p. 66-80.
15. Congreso de la republica. Ley de seguridad y salud en el trabajo. 2011. Ley N°29783.
16. Mogollón A. Manual de organización y funciones. 2012..
17. Orozco G. El concepto de la seguridad en la Teoría de las Relaciones Internacionales. CIDOB d'Afers Internacionals. ;(72).
18. Bekman G. introducción a la informática. sexta ed.
19. Elizondo Callejas A. Informática 1 Patria GE, editor.; 2014.
20. De Pablos Heredero C. Informática y comunicacioones en la empresa Madrid: ESIC EDITORIA; 2004.
21. Alegre R, Garcia. Seguridad Informática Madrid: S.A Ediciones Paraninfo; 2011.
22. Galdámez P. ITI. [Online].; 2003 [cited 2017 Junio 15. Available from: http://web.iti.upv.es/.
23. Talavera Álvarez V. Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001. Pregrado. Lima: pontificia universidad católica del perú, ciencias e ingeniería; 2013.
24. ISO. ISO. [Online]. [cited 2018 10 10. Available from: http://www.iso.org/.
25. López A, Ruiz J. El Portal de ISO 27000 en español. [Online].; 2005 [cited 2017 Junio 15. Available from: http://www.iso27000.es/.

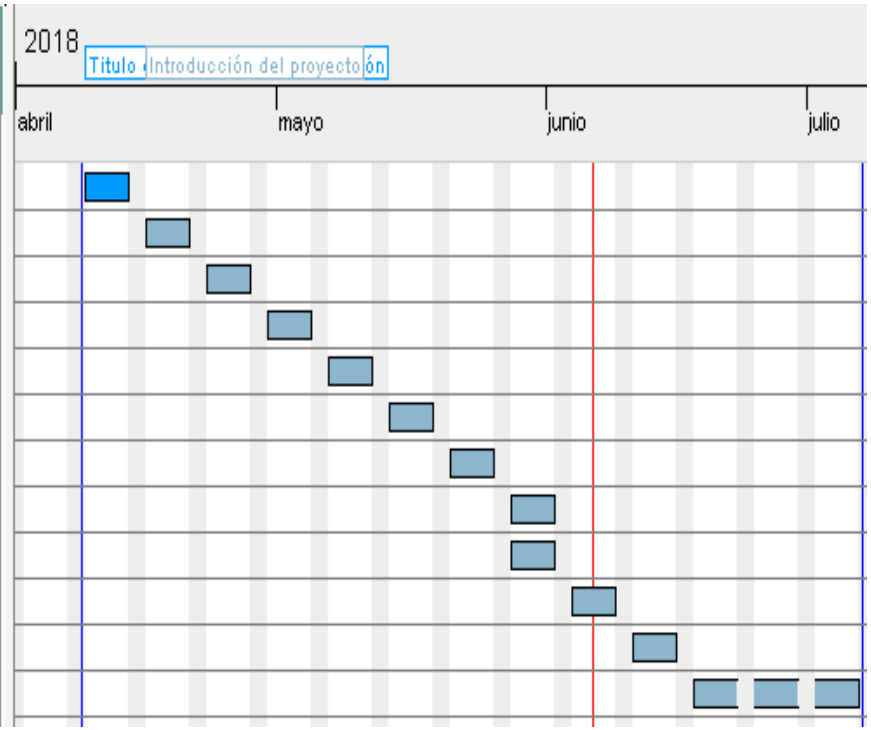
26. Comisión de Normalización y de Fiscalización de barreras comerciales no arancelarias -INDECOPI. Norma Técnica Peruana NTP-ISO 27001. 2008 Dec 12..
27. ISOTools Excellence. Blog especializado en Sistemas de Gestión. [Online].; 2018 [cited 2017 junio 25. Available from: http://www.pmg-ssi.com/2018/03/iso-27001-el-metodo-magerit/.
28. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. TÍTULO: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madird; 2012.
29. Giménez Albacete F. Seguridad en equipos informáticos. IFCT0109. primera ed. IC Editorial 2, editor. Malaga: IC Editorial; 2018.
30. Fernández Barcell M. Estudio de una estrategia para la implementación de los sistemas de gestión de la seguridad de información. Doctoral. Cadíz: Universidad de Cadíz, Ingeniería en Automática; 2003.
31. Hernandez Sampieri R, Fernandez Collado C, Baptista Lucio P. Metodología de la Investigación. cuarta ed. Mexico: McGraw Hill; 2004.
32. Velásquez. Metodologia de la Investigación Cientifíca limA; 2009.
33. Díaz D. Diseño y elaboración de cuestionarios para la investigación comercial. España:; 2001.
34. Casas J, Repullo L, Donado C. la encuesta como técnica de investigación. [Online].; 2003. Available from: http://external.doyma.es/pdf/27/27v31n08a13047738pdf001.pdf.

ANEXOS

Anexo Nº 01

CRONOGRAMA DE ACTIVIDADES

Nombre	Fecha de inicio	Fecha de fin
Titulo del proyecto de investigación	09/04/18	13/04/18
Introducción del proyecto	16/04/18	20/04/18
Planteamiento del problema	23/04/18	27/04/18
Objetivos de la investigación	30/04/18	04/05/18
Justificacion de la investigación	07/05/18	11/05/18
Antecedentes de la investigacion	14/05/18	18/05/18
Bases teoricas de la investigacion	21/05/18	25/05/18
Hipotesis de la investigacion	28/05/18	01/06/18
Metodologia de la investigacion	28/05/18	01/06/18
Referencias bibliograficas	04/06/18	08/06/18
Anexos de la investigacion	11/06/18	15/06/18
Proyecto	18/06/18	06/07/18



Fuente: Elaboración propia.

Anexo N.º 02

PRESUPUESTO

Proyecto: Propuesta para la seguridad informática basado en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura; 2018.

Ejecutora: Lara Morales Karla Stefany

Presupuesto: S/. 7078.00

Fuente: Recursos Propios.

Equipos y materiales	**Costo S/**	**Cantidad**	**Total S/**
Laptop	1500.00	2	3000.00
impresora	200.00	1	200.00
Memoria USB Gb	20.00	2	40.00
Caja de lapiceros	22.00	1	22.00
1/2 millar de hojas A4	16.00	1	16.00
Total			3278
Recursos Humanos	**Costo S/**	**Cantidad**	**Total**
Experto	2000.00	1	2000.00
Supervisor	1500.00	1	1500.00
Total			3500.00
Otros Gastos	**Costo S/**	**Cantidad**	**Total**
Movilidad	5.00		300.00
Total			300.00
Total de inversión			S/. 7078.00

Fuente: Elaboración propia.

Anexo Nº 03

CUESTIONARIO

INSTRUCCIONES:

Señor solicitamos su colaboración, respondiendo con sinceridad el presente cuestionario. El cuestionario tiene por objetivo conocer sobre los sistemas de gestión basados en la norma ISO/IEC 27001 para la seguridad de información. En este instrumento se presentarán 24 preguntas, que deben ser desarrolladas marcando con un aspa (“X”) en el recuadro correspondiente (SI o NO) según considere la alternativa correcta.

Situación actual

1. ¿Usted tiene clara las actividades y funciones que debe realizar en su área de trabajo?

   SI ☐ NO ☐

2. ¿Cree Usted que, en el sistema manual los datos registrados son seguros?

   SI ☐ NO ☐

3. ¿Existen políticas y procedimientos para asegurar que se proporciona seguridad en la información de sus usuarios?

   SI ☐ NO ☐

4. ¿Usted desecha la información que ya no necesita?

   SI ☐ NO ☐

5. ¿Usted cree que los documentos que maneja son catalogados como confidencial o acceso restringido?

   SI ☐ NO ☐

6. ¿Se realizan copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?

   SI ☐ NO ☐

7. ¿Usted cree que es responsable del equipo informático que utiliza para realizar sus funciones en la clínica Simedic Diagnóstica S.A.C?

   SI ☐ NO ☐

8. ¿Cuándo no se encuentra en su oficina deja documentación visible en su escritorio?

   SI ☐ NO ☐

9. ¿La clave de acceso es la misma para ingresar a todos los equipos de cómputo?

   SI ☐ NO ☐

10. ¿Usted ha observado que alguno de sus compañeros a ingerido alguna bebida o alimentos cuando realiza su trabajo en cualquiera de las computadoras de la clínica Simedic Diagnóstica?

    SI ☐ NO ☐

11. ¿Usted ha detectado que el antivirus de la clínica Simedic Diagnóstica SA.C funciona y se encuentra actualizado?

    SI ☐ NO ☐

12. ¿Existe alguna alarma contra incendios, robos u otros?

SI ☐ NO ☐

13. ¿La clínica Simedic Diagnóstica S.A.C cuenta con algún plan de contingencia para dar solución a algún incidente tanto interno o ajeno de la organización?

SI ☐ NO ☐

SEGURIDAD DE INFORMACIÓN

1. ¿Conoce de que trata el tema de seguridad informática?

SI ☐ NO ☐

2. ¿Cree que es necesario aplicar controles de seguridad para evitar robo o daño de información importante para la clínica Simedic Diagnóstica S.A.C.?

SI ☐ NO ☐

3. ¿Existe en la empresa un responsable del área de la seguridad informática?

SI ☐ NO ☐

4. ¿Ha ocurrido algún incidente de seguridad en su puesto de trabajo en el último año?

SI ☐ NO ☐

5. ¿Considera que la clínica le da importancia suficiente a la seguridad?

SI ☐ NO ☐

6. ¿Considera que la seguridad de información debe ser vital en la clínica?

SI ☐ NO ☐

7. ¿Usted como trabajador tiene la cultura de seguir con protocolos de seguridad?

SI ☐ NO ☐

8. ¿Conoce Usted sobre la norma ISO 27001 en la seguridad de información?

SI ☐ NO ☐

9. ¿Cree que el sistema de gestión basado en la ISO 27001 ayudara en la seguridad de información en la clínica?

SI ☐ NO ☐

10. ¿La clínica imparte constantemente capacitaciones de seguridad?

SI ☐ NO ☐

11. ¿La clínica imparte constantemente capacitaciones de seguridad?

SI ☐ NO ☐

12. ¿Desea recibir capacitaciones sobre la seguridad de información y la norma ISO 27001?

SI ☐ NO ☐