Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Escuela Profesional de Ingeniería de Sistemas

Diseño de un Sistema de Gestión de Seguridad de la Información en el proceso de emisión de certificados médicos de aptitud. Caso: Clínica IPC Salud

TESIS

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Daniel Ricardo FERNÁNDEZ CASO

ASESOR

Víctor Hugo BUSTAMANTE OLIVERA

Lima, Perú

2024

Referencia bibliográfica

Fernández, D. (2024). *Diseño de un Sistema de Gestión de Seguridad de la Información en el proceso de emisión de certificados médicos de aptitud. Caso: Clínica IPC Salud*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios autor/ asesor

Datos de autor	
Nombres y apellidos	Daniel Ricardo Fernández Caso
Tipo de documento de identidad	DNI
Número de documento de identidad	44272268
URL de ORCID	--------
Datos de asesor	
Nombres y apellidos	Víctor Hugo Bustamante Olivera
Tipo de documento de identidad	DNI
Número de documento de identidad	25655590
URL de ORCID	https://orcid.org/0000-0001-8805-9629
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Fany Yexenia Sobero Rodriguez
Tipo de documento	DNI
Número de documento de identidad	20120467
Miembro del jurado 1	
Nombres y apellidos	Nilo Eloy Carrasco Ore
Tipo de documento	DNI
Número de documento de identidad	09342780
Datos de investigación	
Línea de investigación	C.0.3.20 Gestión de los Sistemas informáticos y de información

Grupo de investigación	No aplica
Agencia de financiamiento	No aplica
Ubicación geográfica de la investigación	Universidad Nacional Mayor de San Marcos País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Calle: Amézaga Latitud: -12.05313 Longitud: -77.08417 Se requieren coordenadas, no colocar enlaces. Puedes obtener las **coordenadas GD** de sitios como https://www.google.com.pe/maps/ https://www.coordenadas-gps.com/ https://www.mapsdirections.info/
Año o rango de años en que se realizó la investigación	Octubre 2022 – Diciembre 2023
URL de disciplinas OCDE	Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04 Otras ingenierías y tecnologías https://purl.org/pe-repo/ocde/ford#2.11.02

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación de Tesis

Siendo las20:00 horas del día 04 de enero del año 2024, se reunieron virtualmente los docentes designados como miembros de Jurado de Tesis, presidido por el Mg. Fany Sobero Rodriguez, Mg. Nilo Carrasco Oré (Miembro) y el Lic. Victor Bustamante Olivera (Miembro Asesor), usando la plataforma Meet (https://meet.google.com/bsd-kmiz-zzx), para la sustentación Virtual de la tesis Intitulada: **"Diseño de un Sistema de Gestión de Seguridad de la Información en el proceso de emisión de certificados médicos de aptitud. Caso: Clínica IPC Salud",** del Bachiller: **Daniel Ricardo Fernández Caso;** para obtener el Título Profesional de Ingeniero de Sistemas.

Acto seguido de la exposición de la Tesis, la Presidenta invitó al Bachiller a responder las preguntas formuladas por los Miembros del Jurado.

El Bachiller, en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez las preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el bachiller obtuvo la nota de 17 **(Diecisiete)**

A continuación, la Presidenta del Jurado Mg. Fany Sobero Rodriguez, declara al Bachiller **Ingeniero de Sistemas.**

Siendo 20:44: horas, se levantó la sesión.

Mg. Fany Sobero Rodriguez
Presidente

Mg. Nilo Carrasco Ore
Miembro

Lic. Víctor Bustamante Olivera
Miembro Asesor

Yo **VICTOR HUGO BUSTAMANTE OLIVERA** en mi condición de **asesor** acreditado con la Resolución Directoral N° 000011-2022-EPISI-FISI/UNMSM de la **tesis**/monografía/informe de investigación/trabajo académico, cuyo título es **DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE EMISIÓN DE CERTIFICADOS MÉDICOS DE APTITUD. CASO: CLÍNICA IPC SALUD**, presentado por el **bachiller**/magíster/egresado/licenciado/estudiante **DANIEL RICARDO FERNANDEZ CASO** para optar el grado**/título**/especialidad de **INGENIERO DE SISTEMAS**, CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de **13 %** de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional.**

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado/ título/ especialidad correspondiente.

Firma del Asesor: 

Nombres y apellidos del asesor:
Víctor Hugo Bustamante Olivera

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Diseño de un Sistema de Gestión de Seguridad de la Información en el proceso de emisión de certificados médicos de aptitud. Caso: Clínica IPC Salud

RESUMEN

En el contexto de la recuperación económica del Perú postpandemia de COVID-19, algunos sectores económicos se han visto sustancialmente beneficiados por el incremento de sus actividades, los precios de sus productos y servicios, y la constante necesidad de cubrir la demanda de estos. Este es el caso de mineras, constructoras, consultoras y empresas de comercio entre otras, que a pesar del impacto negativo producido por la pandemia de COVID-19, han mantenido su necesidad de contar con personal que cubra las expectativas que sus funciones, por ello demandan realizar exámenes médicos de salud ocupacional a los aspirantes a una posición laboral dentro de su organización, siendo este un proceso que exige precisión y absoluta celeridad en la obtención de sus resultados.

La obtención de un certificado de aptitud médica confirma la adecuada condición física de una persona para realizar determinada labor en una organización. Este certificado debe ser emitido por instituciones acreditadas para tal fin, cumpliendo normas y exigencias de confidencialidad, integridad y disponibilidad de los resultados. La utilización de firmas digitales constituye una herramienta de fácil auditoría y por ende reduce la probabilidad de falsificación de firmas en exámenes médicos.
De esta necesidad se genera la oportunidad de diseñar un Sistema de Gestión de Seguridad la Información (SGSI) aplicable al proceso de emisión del certificado de aptitud médica, considerando políticas, procedimientos y lineamientos. Para cumplir con lo planteado, se propone desarrollar las categorías temáticas de controles del SGSI conforme al estándar ISO/IEC 27001:2022 según la aplicabilidad identificada respecto al proceso de emisión de certificados de aptitud médica. Dicho proceso al que se aplicará el SGSI se ejecuta combinando procedimientos manuales de toma de exámenes médicos y gestión de los resultados mediante un sistema de información a medida.
El presente trabajo permitirá a la clínica IPC Salud el reforzamiento de la seguridad en el proceso de emisión de certificados médicos y en la gestión de la información de sus pacientes proporcionando un incremento en la confianza proyectada ante sus clientes respecto al tratamiento de la información.

Palabras clave: Sistema de Gestión de Seguridad de la Información Salud Ocupacional, Medicina Ocupacional, ISO/IEC 27001:2022

Design of an Information Security Management System in the process of issuing medical fitness certificates. Case: IPC Salud Clinic

ABSTRACT

In the context of Peru's economic recovery after the COVID-19 pandemic, some economic sectors have benefited substantially from the increase in their activities, the prices of their products and services, and the constant need to cover the demand for these. This is the case of mining companies, construction companies, consultants and trading companies, among others, which despite the negative impact produced by the COVID-19 pandemic, have maintained their need to have personnel who meet the expectations of their functions, therefore They demand that occupational health medical examinations be carried out on applicants for a job position within their organization, this being a process that requires precision and absolute speed in obtaining its results. Obtaining a certificate of medical aptitude confirms the adequate physical condition of a person to carry out a certain job in an organization. This certificate must be issued by accredited institutions for this purpose, complying with standards and requirements of confidentiality, integrity, and availability of the results. The use of digital signatures constitutes an easy auditing tool and therefore reduces the probability of forgery of signatures in medical examinations. This need gives rise to the opportunity to design an Information Security Management System (SGSI) applicable to the process of issuing the medical aptitude certificate, considering policies, procedures, and guidelines. To comply with the above, it is proposed to develop the thematic categories of ISMS controls in accordance with the ISO/IEC 27001:2022 standard according to the applicability identified regarding the process of issuing medical aptitude certificates. Said process to which the ISMS will be applied is carried out by combining manual procedures for taking medical examinations and managing the results through a customized information system. The present work will allow the IPC Salud clinic to reinforce security in the process of issuing medical certificates and in the management of its patients' information, providing an increase in the confidence projected before its clients regarding the treatment of information.

Keywords: Occupational Health Information Security Management System, Occupational Medicine, ISO/IEC 27001:2022

Capítulo

1. Introducción

1.1 Antecedentes

Para que las organizaciones puedan conocer si un candidato a colaborador cuenta con el estado físico y médico apto para el puesto al que postula, se requiere una evaluación médica que se adecúe a su perfil ocupacional dentro de la empresa.

Con el desarrollo tecnológico actual, muchas empresas han empezado a adoptar estas tecnologías y adaptan sus procesos para beneficiarse de su uso. De este modo agilizan sus actividades a la vez que mejoran la seguridad de la información que manejan. La importancia del trabajo se ajusta a la necesidad de que los procesos deben ser controlados de la mejor manera generando seguridad a las personas, su información médica e historia ocupacional.

El proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud requiere una correcta gestión de la Seguridad de la información, en adelante SI, por tratar información sensible de los pacientes, actualmente presenta algunas demoras debido a la necesidad de firma manuscrita de los médicos ocupacionales, encargados de brindar la aptitud médica de los pacientes. La implementación de la firma electrónica a través del DNI electrónico (DNIe) reduce el tiempo de firma y la necesidad de presencialidad del médico en las instalaciones de la clínica para firmar los expedientes. El Sistema de Gestión de Seguridad de la Información, en adelante SGSI deberá ser diseñado contemplando los controles de seguridad necesarios para dotar de confidencialidad, disponibilidad e integridad al proceso completo y por ende a la firma digital.

La Clínica IPC Salud ha tenido que enfrentar las consecuencias del mal proceder de algunos trabajadores que han falsificado un certificado de aptitud médica alterando el nombre del paciente con el fin de obtener una plaza laboral a pesar de no estar en condiciones físicas aptas para desempeñar las funciones que ese trabajo demande. Esto es una constante en sectores como minería y construcción, sectores del cual forman parte los principales clientes de la Clínica. La falsificación de certificados médicos aunado a los antecedentes penales y/o policiales son una práctica recurrente en los procesos de captación de talento en las empresas de estos sectores.

Esta falsificación puede traer consigo incidentes que pueden ir desde lesiones leves hasta muy graves, incluso con la consecuente muerte del trabajador. Un accidente de este tipo implica consecuencias legales para la empresa contratante y también para el centro de salud que expidió el certificado de aptitud médica.

1.1 El problema

El problema que se pretende resolver es la falta del diseño de un Sistema de Gestión de Seguridad de la Información que asegure la confidencialidad, disponibilidad e integridad de los datos generados en el proceso de emisión de certificados de aptitud médica dentro de la Clínica IPC Salud.

1.2 Objetivos

1.2.1 Objetivo principal

Determinar la influencia del diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

1.2.2 Objetivos específicos

- Determinar la influencia del diseño de un SGSI bajo la ISO/IEC 27001:2022 en la protección de datos personales para el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

- Identificar la influencia diseño de un SGSI bajo la ISO/IEC 27001:2022 en el aseguramiento de los activos de información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

- Estimar la influencia del diseño de un SGSI bajo la ISO/IEC 27001:2022 en el nivel de percepción de los trabajadores sobre la seguridad de la información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

- Evaluar la influencia del diseño de un SGSI bajo la ISO/IEC 27001:2022 en el grado de adaptabilidad para el personal respecto a la seguridad de la información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

1.3 Justificación

El proceso de emisión de certificados de aptitud médica requiere intervención humana y uso de tecnologías de información, ambos tratan datos personales y sensibles de los pacientes, por lo que es necesario mitigar los riesgos de seguridad de dicha información, así como la autenticidad de los resultados que los exámenes médicos generan. La falta de un SGSI ha generado, entre otros, incidentes de seguridad que se muestran a continuación:

- Falsificación de certificados de aptitud médica.
- Incumplimiento de SLA de entrega de certificados en el tiempo ofrecido.
- Acceso a información sensible por usuarios no autorizados para tal fin.
- Demora en restablecimiento de operatividad luego de una interrupción causada por ciberdelincuencia, infección de virus, etc.
- Pérdida de expedientes con información médica de los pacientes.

Identificación de beneficios al contar con un Sistema de gestión de la seguridad de la información.

Un SGSI reditúa en los siguientes beneficios:

A nivel organizacional: El SGSI provee de controles en el proceso de gestionar información de los clientes, lo que brinda garantía y proyecta una imagen de responsabilidad en dicha gestión. Además, reduce los riesgos inherentes al tratamiento, almacenamiento y distribución de los registros médicos durante la emisión del certificado de aptitud.

A nivel económico: El impacto económico por la imposición de una multa, puede acarrear dificultades en la gestión financiera de la organización; asimismo, cualquier demanda por ejercicio indebido de la medicina o resultados inexactos de las pruebas de aptitud genera un perjuicio económico al dirigir esfuerzos para atender dichas demandas.

A nivel tecnológico: Además de constituir una mejora en la gestión de activos de información, la implementación del SGSI permite la incorporación de nuevas tecnologías en el proceso operativo de la emisión de certificados médicos, este es el caso de las firmas digitales para los documentos de aptitud médica que son entregados a los clientes.

A nivel legal: La normativa legal establece los lineamientos y exigencias en el servicio de seguridad y salud en el trabajo, esto puede encontrarse en la Ley N° 29783 - Ley de Seguridad y Salud en el trabajo, modificado por Ley N° 30222, de la cual se desprende la necesidad de contar con personal apto médicamente y con la vigilancia médica adecuada. Asimismo, se cuenta con la norma técnica NTP ISO/IEC 27001:2014 que procura la correcta gestión de la información en las organizaciones y que indica que el SGSI "consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información, así como de los sistemas implicados en su tratamiento dentro de una organización".

1.4 Alcances y limitaciones

1.4.1 Alcance

El presente trabajo de investigación pertenece al área de investigación Gobierno y Gestión de TIC (Área 5: Gestión de TIC) de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos.

Diseña el SGSI para dotar de cumplimiento y mejora a la gestión de información de los clientes de la clínica IPC Salud, ubicada en la ciudad de Lima, República del Perú. Dicha empresa se dedica a la evaluación médica de postulantes y trabajadores de organizaciones en distintas áreas productivas. Estas evaluaciones se desarrollan dentro de las instalaciones de la Clínica y en ocasiones se puede desarrollar en las oficinas del cliente y en lugares remotos al interior del país cuando el cliente así lo requiere.

El alcance del SGSI propuesto en este trabajo no incluye procesos externos, paralelos ni conexos al de la emisión de certificados de aptitud médica.

1.4.2 Limitación

Se logrará contar con un sistema que coadyuve a la conservación de la confidencialidad, la integridad y la disponibilidad de la información tratada en el proceso de emisión de certificados de aptitud médica, teniendo como límite dicho proceso, ya que este pertenece a un proceso macro que es la atención de pacientes en la clínica. La consecución de este objetivo estará apoyada por la inclusión de los dominios pertinentes de la ISO/IEC 27001:2022, norma que, a la redacción de este trabajo, está recientemente publicada e incluye un conjunto de cambios respecto a la ISO/IEC 27001:2013, versión anterior de la norma.

1.5 Organización de la tesis

El detalle de organización del presente trabajo de investigación es el siguiente:

En el capítulo 1 se aborda la problemática de la investigación, se trazan los objetivos generales y específicos, así como la justificación y alcance del proyecto.

El capítulo 2 está dedicado al estudio del marco teórico con la consecuente especificación del estado del arte, incluyendo estudios previos sobre implementación de firma digital, proceso de gestión de salud y seguridad de la información.

En el capítulo 3 se consignan las hipótesis y variables consideradas en la tesis, estas son resultado de la metodología de investigación aplicada al presente trabajo.

El capítulo 4 incluye el desarrollo del proyecto de diseño de SGSI que permite detallar los controles, normas y políticas aplicables al proceso de emisión de certificados de aptitud médica.

Finalmente, en el capítulo 5 se contemplan los resultados y conclusiones del proyecto.

Capítulo

2. Marco Teórico

2.1 Estado del arte

2.1.1 Introducción

Las organizaciones dedicadas al sector salud gestionan información sensible de sus clientes y hacerlo con apego a la normatividad y buenas prácticas es menester para proyectar confianza interna y externamente. Esto ha sido representado en distintos trabajos de investigación nacionales y extranjeros que han sido elegidos para mostrar la vigencia e importancia de su implementación en las organizaciones.

Como resultado de las investigaciones realizadas se han encontrado distintos trabajos de diseño de implementación, pero ninguno similar al que se plantea en esta tesis, la cual se dirige a un proceso principal de la operatividad de una clínica de salud ocupacional. El hallazgo de estos estudios refuerza la necesidad de dotar a las instituciones de sistemas de gestión de seguridad de la información y constituyen base de referencia para el desarrollo de este proyecto de investigación.

2.1.2 Investigaciones a nivel internacional

Barbosa Salinas, Jefferson Fabian y Gonzáles Vargas, David Alejandro (2021) en su tesis "Diseño del sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 para telemedicina en la IPS Colombiana de Trasplantes" (Colombia)

Esta investigación tuvo como propósito diseñar un Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27001:2013 para aplicarlo en el proceso de atención a través de telemedicina.

En el estudio, la metodología incluye el análisis de riesgo, dar opciones de tratamiento al riesgo en seguridad de la información y capacitar a las partes involucradas respecto a la seguridad informática.

El instrumento utilizado fue un plan de concienciación a los trabajadores de la empresa para la comprensión y cumplimiento de las políticas de protección de datos.

Los autores llegan a la conclusión de que su propuesta de implementación de SGSI presentada a la dirección de dicha institución permitió identificar el bajo porcentaje de cumplimiento e implementación de los controles especificados en la ISO//IEC 27001:2013, lo que expone a la información tratada por la empresa a distintos riesgos internos y externos. De la misma forma, el SGSI permite reducir los riesgos inaceptables hasta un nivel de aceptación impuesta por la empresa, esto gracias a la aplicación de los controles del anexo A de la norma ISO/IEC 27001:2013 proponiendo la reducción del impacto y la probabilidad de materialización de cada uno de sus riesgos. Para este fin, el trabajo propone políticas de seguridad de la información alineadas a los objetivos empresariales soportadas por controles recomendados en la norma.

Rodriguez Correa, Jorge Leonardo (2017) en su tesis "Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en ISO27001 para Laboratorios Servicios Farmacéuticos de Calidad SFC Ltda." (Colombia)

Esta tesis tuvo como finalidad el diseño de un SGSI basado en la ISO/IEC 27001 mediante el ciclo PHVA con el propósito de proveer de confidencialidad, disponibilidad e integridad a los datos generados en Laboratorios Servicios Farmacéuticos de Calidad SFC.

La metodología de trabajo consistió en clasificar los activos, analizar las vulnerabilidades y determinar los controles de seguridad de información necesarios. La población de análisis fue conformada por jefes responsables de las 4 áreas más críticas involucradas en la gestión y operatividad de la organización. El estudio hace énfasis en el análisis y determinación de riesgos, amenazas y vulnerabilidades que pueden afectar a la institución durante sus operaciones, lo que le permite seleccionar salvaguardas y contramedidas para su atención, tratamiento y mitigación.

Para la investigación, el instrumento de recolección de datos fue una encuesta; el resultado obtenido fue la implementación del SGSI, lo cual representa un gran avance en el desarrollo de sus actividades y en la reputación proyectada a sus clientes, gracias a la consigna de manejar la información de clientes, proveedores, información descriptiva y analítica de sus productos y materias primas de manera confidencial y segura.

Finalmente, la implementación del SGSI permitió generar en el personal de la empresa, un sentido

de asertividad y visión global en término de seguridad de la información, además del apoyo decidido de los directores de la empresa para encaminar los procesos internos hacia el cumplimiento de estándares de tratamiento de la información de sus clientes.

Pinela Requena, Edison Roberto (2013) en su tesis "Análisis de la necesidad de la firma digital en las exportadoras e importadoras guayaquileñas para la creación de una empresa de certificación". (Ecuador)

El estudio propone la creación de una guía de seguridad para el uso de firma electrónica, reconociendo su validez legal y los mismos efectos jurídicos que una firma manuscrita, por lo que podría ser admitida como prueba en algún proceso judicial.

En esta tesis, el diseño de investigación fue de tipo cuantitativo, la población identificada corresponde a 2280 importadores y exportadores de Guayaquil, quienes tienen habilitada la opción de compras por internet, el instrumento de recolección de información que se utilizó fue un cuestionario cuantitativo estructurado y para el procesamiento de datos se utilizó el software Microsoft Excel.

El resultado obtenido de la investigación fue la implementación de firma digital a la sociedad ecuatoriana relacionada con el comercio exterior; para lograr esto, identificó que un factor influyente para que las empresas no tengan certificación digital es el desconocimiento de las ventajas proporcionadas por esta y el autor llega a la conclusión que aquellas entidades de certificación son consideradas como terceros confiables, esto es muy importante porque cuando una persona, sea natural o jurídica requiera adquirir una Firma Electrónica lo puede realizar en una empresa que le brinde todas las garantías que provean de respaldo al cliente.

Valencia Duque, Francisco Javier y Orozco Alzate, Mauricio (2017) en su artículo "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000" (Colombia)

Este artículo tuvo como propósito la implementación de un SGSI basado en la familia ISO 27000 teniendo como pilares las ISO 27002, 27003 y 27005, definiendo la metodología y consideraciones para su implementación en organizaciones tanto públicas cuando privadas.

La metodología utilizada estuvo conformada por 5 fases consistentes en la aprobación de la dirección

para iniciar el proyecto (aceptación del proyecto); definición del alcance, límites y la política del SGSI; estudio de requerimientos, valoración y plan de tratamiento de los riesgos y finalmente el diseño del SGSI.

Se concluyen que se hace necesario el establecimiento de un proceso metodológico para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información, debido a la cantidad de normas incluidas en la familia ISO/IEC 27000. Por ello, a través de la interrelación de las normas ISO/IEC 27001:2013, ISO/IEC 27002: 2013, ISO/IEC 27003:2010 e ISO/IEC 27005: 2008 los autores proponen un enfoque con perspectiva sistémica que permite la implementación del SGSI con un nivel de éxito aceptable y, en consecuencia, la disminución de incertidumbre en sus resultados.

2.1.3 Investigaciones a nivel nacional

Escalante Coronel, Diego Milker (2019) en su tesis "Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas – Chincheros"

El trabajo de investigación plantea dividir la implementación de un Sistema de Gestión de Seguridad de la Información en 3 fases:

1) Diagnóstico inicial, donde se evalúa el estado de la Dirección de Salud Virgen de Cocharcas en relación de los requisitos de la NTP – ISO/IEC 27001:2014 y se establece la posibilidad de aceptación del SGSI.

2) Preparación del SGSI, fase que permite detallar el contexto de la organización, las políticas de seguridad de información a utilizar, el alcance, objetivos y establecimiento del Comité de seguridad de la información.

3) Finalmente, la planificación del SGSI consistente en evaluación de riesgos mediante la metodología OCTAVE, valoración de activos, identificación y valoración de amenazas, cálculo de impacto y cálculo de riesgos.

   Como resultado, se concluye que ha sido determinante el apoyo de la alta dirección y el compromiso de los trabajadores de la entidad para lograr la implementación del SGSI bajo la NTP – ISO/IEC 27001:2014 para la Dirección de Salud Virgen de Cocharcas, además la investigación concluye que los controles de seguridad NTP – ISO/IEC 27001:2014 permiten

establecer métricas confiables sobre la eficacia y eficiencia del SGSI.

Barrantes Porras, Carlos Eduardo y Hugo Herrera, Javier Roberto (2012) en su tesis "Diseño e Implementación de un sistema de gestión de seguridad de información en procesos tecnológicos"

La investigación tuvo como objetivo disminuir y moderar los riesgos de los activos de información de los procesos de la gerencia de tecnología de la empresa Card Perú, para esto se busca gestionar y monitorear de manera eficiente los incidentes y vulnerabilidades de seguridad de la información para reducirlos en un 80%. Asimismo, se busca formar y concientizar al 100% de los trabajadores involucrados en los procesos de TI sobre temas de seguridad de la información. Además, se plantea el objetivo de gestionar y controlar el 100% de los documentos del SGSI.

La metodología utilizada fue la gestión de proyecto del PMBOK y la gestión de riesgos basada en la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT. Para la elección de esta metodología, los autores realizan una comparación entre distintos marcos y normativas relacionadas a Seguridad de la Información.

Como parte del proyecto, se implementó una política de seguridad de información socializada a todo el personal de la empresa y también a terceros involucrados en los procesos de TI; los incidentes y vulnerabilidades de seguridad de la información fueron gestionados y monitoreados permitiendo controlar toda la documentación del SGSI.

La conclusión a la que se llegó es que la implementación de un SGSI permite a la empresa estar preparados ante el incremento de activos y por ende sus amenazas y vulnerabilidades. Establecer una adecuada gestión para reducir y mitigar los riesgos asociados a los activos de información involucrados en los procesos de la empresa Card Perú S.A representa una ventaja comparativa dentro de su sector. Finalmente, los autores concluyen que, la implementación de un SGSI tiene como componente crítico el factor humano, por lo que consideran relevante la formación y concienciación en temas de seguridad de la información.

Aguirre Mollehuanca, David (2014) en su tesis "Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A."

La tesis centra a la institución pública Servicios Postales del Perú (SERPOST S.A.) como caso de

estudio para el cumplimiento de la exigencia de implementación de la NTP–ISO/IEC 27001:2008, la cual presenta dificultades en el cumplimiento de los tiempos establecidos por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) del Perú, básicamente por desconocimiento de la alta dirección sobre su importancia. Esta investigación requirió de continuas reuniones con la alta dirección para definir el alcance y la aprobación de las políticas de seguridad de la información.

El proyecto sigue la metodología consistente en elaborar un Business Case del diseño de SGSI, definición de alcance y elaboración de políticas de seguridad de la información. Posteriormente elabora un mapa de procesos relacionados al sistema de gestión, identifica y valora los activos de la información. Se evalúa y trata los riesgos inherentes a la gestión de la información para terminar con la declaración de aplicabilidad.

El trabajo de investigación concluye que el diseño de un SGSI para la empresa SERPOST obtuvo el apoyo de la alta gerencia, componente muy importante al intentar concientizar a los jefes de área y dueños de los procesos para reforzar el entendimiento de que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga. Se hace un mayor énfasis en la integridad de la información tratada en su operatividad dedicada al envío y traslado de documentos, paquetes y cargas a nivel nacional e internacional. Lo que representa confianza en la operatividad proyectada por la organización.

Ccesa Quincho, Mercedes (2017) en su tesis "Diseño de un Sistema de Gestión de Seguridad de la Información bajo la NTP ISI/IEC 27001:2014 para la Municipalidad Provincial de Huamanga"

La autora propone el diseño de un SGSI para cumplir la exigencia del estado peruano a las entidades públicas integrantes del sistema nacional de informática, consistente en la implementación de la NTP ISO/IEC 27001:2014. Determina que el cronograma de implementación establecido por el estado no refleja cumplimiento debido al desconocimiento, presupuesto insuficiente y carencia de personal especializado entre otras causas.

En cuanto a la metodología, la investigación se inicia mediante un análisis de brechas (también llamado Gap) a la entidad con respeto a la NTP ISO/IEC 27001:2014, luego se estudió a la organización y su contexto, permitiendo la identificación del proceso crítico, definición de políticas de seguridad de la información y establecimiento de Comité de Seguridad de la Información en la organización, el Comité tiene el encargo de proponer, aprobar y hacer cumplir las políticas que

forman parte del SGSI; posteriormente, la autora analizó, identificó y valoró los activos de información mediante la metodología de análisis y gestión de riesgos, con esto se logró calcular la probabilidad y el impacto de materializarse los riesgos, generando así las medidas de control necesarias para su mitigación. Finalmente, se elaboró el documento de aplicabilidad que justifica los controles del Anexo A de la NTP ISO/IEC 27001:2014 pueden ser implementados en la Municipalidad Provincial de Huamanga.

Las conclusiones a las que llega el trabajo es que al apoyo de la alta gerencia es imprescindible cuando se desea diseñar e implementar un SGSI. También refiere la importancia de la difusión de las normas de seguridad de información existentes y otras resultantes del SGSI implementado. La autora considera importante contar con personal especializado que ayude al mantenimiento y soporte del SGSI posterior a su implementación.

2.2 Bases teóricas

2.2.1 Detalle de la organización

La clínica IPC Salud es un instituto de servicios médicos especializados en salud ocupacional, medicina física y rehabilitación con operaciones en la ciudad de Lima desde el año 2001 atendiendo a clientes dedicados a la mayoría de las actividades económicas, tan variadas como la construcción, minería, industria, educación y servicios en general. El proceso de atención a pacientes está soportado por un sistema de información llamada IPCNet, desarrollada y mantenida por un proveedor externo. Dicho sistema se encuentra implementado en el centro de datos propio de la empresa, fue desarrollada en lenguaje PHP, utiliza base de datos MySQL y permite la inserción, modificación y eliminación de módulos internos del sistema.

La emisión de certificados de aptitud médica es la actividad concluyente del proceso de atención a los pacientes, pues determina si el futuro trabajador cumple o no con las condiciones físicas y mentales que exige el puesto laboral al que postula. Estas exigencias vienen indicadas en un protocolo médico donde la empresa contratante del examen especifica el conjunto de evaluaciones médicas que se deben realizar, estos exámenes incluyen los servicios de laboratorio, radiología, odontología, dermatología, oftalmología, neumología, psicología, cardiología, entre otras.

Cada especialidad médica donde se atiende a un paciente genera resultados que son ingresados manualmente en algunos casos, y en otros son capturados de los equipos médicos que realizan las evaluaciones (por ejemplo, el espirómetro o el equipo de electrocardiograma). Estos resultados son revisados por los médicos especialistas que deberán firmar los resultados de cada paciente, labor que ha incorporado la firma digital en reemplazo de la firma manuscrita. Es gracias a la firma digital que los médicos pudieron dar continuidad a sus labores antes, durante y después del periodo de confinamiento decretado por el gobierno peruano a raíz de la pandemia por COVID-19 y se suprimió la necesidad de trasladarse físicamente a las instalaciones de la clínica para revisar expedientes y demorar la firma por tratarse de una labor que tenía que hacerse con cada documento de forma individual.

Los tiempos de entrega ya no incluyen el traslado del médico ni la necesidad de realizar esta actividad en horarios de atención de la clínica. Actualmente el compromiso de entrega de resultados estipula que estos deben ser publicados en el portal web de resultados (https://ipcnet.ipcsalud.com) como máximo a las 18:00h del mismo día del examen, esto es un gran aporte al proceso en

comparación con las 24 horas que ofrecía anteriormente la clínica debido a la demora en las firmas manuscritas. Se debe considerar en este contexto que los médicos especialistas no son colaboradores in situ de la clínica, sino que desarrollan la labor como médicos diagnosticadores, auditores y ocupacionales según sea el caso desde sus consultorios externos o domicilios. La ubicuidad de su labor se ha logrado en parte por el sistema de información de la clínica y también por la inclusión de la firma digital en el proceso de emisión de certificados.

Las áreas organizativas involucradas en el proceso son las siguientes:

Área Comercial: Compuesta por la Gerencia Comercial y los ejecutivos comerciales, Esta área es la encargada de ofertar, acordar y coordinar los protocolos de atención médica con las empresas clientes. Los protocolos de atención deben ser ingresados al sistema de información IPCNet para que el área encargada de realizar la atención de pacientes tenga conocimiento de los exámenes que debe realizar. También realizan el acuerdo de pago con los clientes y el seguimiento de cobranza por los servicios prestados.

Área de operaciones: Una vez definido el protocolo para cada paciente, el área de operaciones se encarga de la recepción, admisión y evaluación de cada prueba médica, teniendo para esto personal capacitado en todas las especialidades. Cada resultado obtenido es registrado en IPCNet para ser revisado por los médicos diagnosticadores.

Personal de atención: Son profesionales de la salud encargados de la toma de algunas muestras o toma de exámenes que no requieren de la intervención de un médico especialista, como laboratorio, rayos X o test oftalmológicos, por ejemplo.

Médico diagnosticador: Es el profesional de medicina con especialidad, encargado de registrar según su evaluación los resultados de una prueba médica realizada a los pacientes. Registran los resultados y posibles observaciones en el sistema de información adjuntando su firma digital.

Médico auditor: Un expediente médico recaba los resultados de todas las evaluaciones realizadas a un paciente, cuenta con las firmas de los distintos médicos diagnosticadores y deben ser aprobados por el médico auditor, quien vuelve a revisar cada resultado para consignar su acuerdo con lo estipulado en el expediente.

Médico ocupacional: El médico con especialidad en Salud Ocupacional es el único que

puede firmar un certificado de aptitud médica. El especialista firma este documento consignando el resultado final de la ejecución del protocolo médico, previa revisión del expediente y de las posibles observaciones de los médicos que antecedieron la revisión.

2.2.2 Norma ISO/IEC 27001:2022

Esta norma internacional de mucha aceptación y referente en la gestión de seguridad de la información es emitida por la Organización Internacional de Normalización (ISO por sus siglas en inglés). Ha recibido una actualización en octubre del 2022, consistente en una reorganización e inclusión de dominios, recibiendo la denominación ISO/IEC 27001. Es con esta última versión que se ha diseñado el sistema de gestión de información en esta tesis.

La norma establece claramente los lineamientos de gestión de la seguridad de la información en una organización más allá de su origen público o privado, con o sin fines de lucro, con independencia de su tamaño y complejidad. Su primera revisión fue publicada en 2005 y su desarrollo se basó en la norma británica BS7799-2. La redacción de esta norma recae en los mejores especialistas del mundo en el tema y constituye una guía metodológica que permite implementar la gestión de la seguridad de la información.

Las organizaciones pueden alcanzar la certificación internacional en esta norma, lo que significa que una entidad certificadora independiente valida y confirma que la seguridad de la información es tratada e implementada en la organización que aspira a obtener la certificación, en estricto cumplimiento con la norma, cumpliendo los principios básicos que garantizan la seguridad de la información, los cuales son:

Integridad. - Es la garantía de que la información no puede ser manipulada sin autorización expresa.

Confidencialidad. - Principio que especifica que la información solo puede ser accedida por personas que cuenten con la autorización debida.

Disponibilidad. - Indica que el acceso a la información tratada debe estar garantizada en todo momento.

Figura 1.- Componentes de la seguridad de información

La norma ISO/IEC 27001:2022 constituye una guía basada en la investigación de los problemas potenciales relacionados con la información, es decir, la evaluación de riesgos. Posteriormente se deberá establecer el conjunto de acciones para hacer frente a los riesgos, a esto se le denomina tratamiento del riesgo enfocado a su mitigación, eliminación o asunción.

El tratamiento de riesgo se realiza principalmente con la formulación de políticas, procedimientos, infraestructura tecnológica y lineamientos aplicables a la realidad de la organización. Para que el SGSI cumpla con sus objetivos debe contar con la aceptación e involucramiento del personal directivo y de los colaboradores en general, puesto que la correcta gestión de la seguridad de la información debe ser un objetivo organizacional y no de un área específica. En este sentido, la norma sugiere la conformación e intervención de distintos comités encargados de la elaboración, publicación, actualización y cumplimiento de los requerimientos del SGSI.

Es imperante también, definir la seguridad de la información como un concepto paraguas que incluye la seguridad física, concienciación de las personas, establecimiento de procedimientos y análisis de procesos. La ISO/IEC 27001 considera todos estos elementos dentro de un sistema de gestión de seguridad de la información.

Aunque contar con una certificación organizacional en ISO/IEC 27001 no es una exigencia

legal ni un requisito para poder brindar servicios médicos, no son pocas las organizaciones que se interesan en obtener esta certificación.

2.2.3 COBIT

COBIT 5 es un marco de referencia de Gobierno de TI y un conjunto de herramientas de soporte que permite a los gerentes reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. Además, permite el desarrollo de una política clara y una buena práctica para el control de TI en las organizaciones. El marco acentúa el cumplimiento regulatorio, ayuda a las organizaciones a incrementar el valor asociado al área de TI, habilita la alineación y simplifica la puesta en práctica del marco de referencia. Desde su nacimiento, ha ido evolucionando desde su propósito inicial de auditoría de TI, pasando por Control, Gestión de TI, Gobierno de TI, hasta el enfoque holístico de gobierno corporativo de TI.

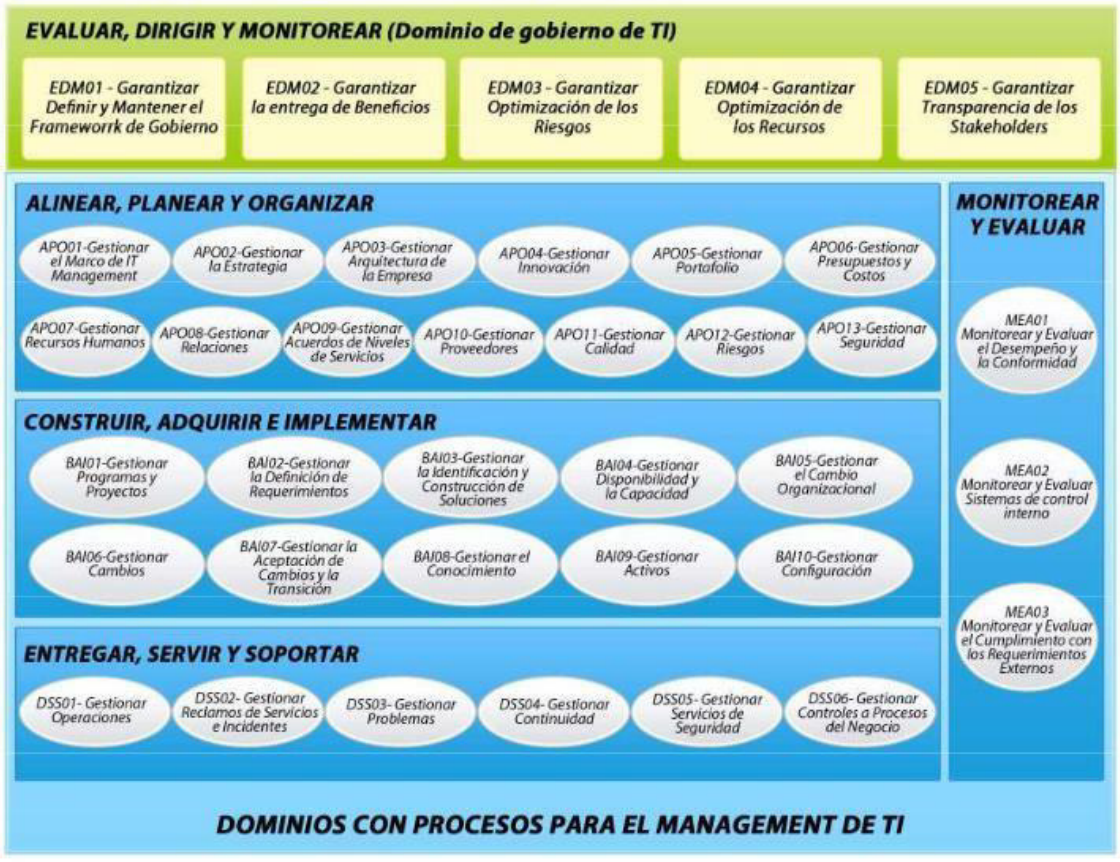


Figura 2.- Diagrama de procesos de COBIT 5

COBIT 5 usa prácticas de gobierno y gestión para describir las acciones que son ejemplo de las mejores prácticas de su aplicación. De igual manera, cambió su enfoque de objetivos de control a una visión por proceso. COBIT en su versión 5 incorpora importantes marcos de ISACA como BMIS, Val IT, Risk IT, ITAF entre otros. Además, separa claramente el gobierno de la gestión.

2.2.4 MAGERIT

Consejo Superior de Administración Electrónica de España elaboró MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) para gestionar los riesgos de las TIC debido al creciente uso y dependencia de estas para alcanzar los objetivos que cada individuo u organización desea. En esta metodología la gestión de riesgos se divide en 2 subprocesos, estos son:

- Análisis de Riesgos:

Permite determinar lo que posee la organización y que le podría suceder.

- Tratamiento de Riesgos:

Organiza una defensa prudente para sobrevivir a los incidentes y seguir operando en las mejores condiciones, al no poder controlar se maneja un riesgo residual que es asumido por la alta dirección.

De esta manera MAGERIT busca no solo concienciar a los responsables del gobierno de TI de la existencia de riesgos sino que ayuda a descubrir y planificar un tratamiento oportuno para mantener a estos riesgos bajo control.

El método de análisis de riesgos que proporciona MAGERIT consiste en cinco (5) pasos [MAGERIT, 2012]:

1. Determinar los activos relevantes para la organización, sus relaciones entre si y el valor que tienen (según el coste que supondría su degradación).
2. Determinar las amenazas a las que se exponen los activos.
3. Determinar las salvaguardas disponibles y que tan eficaces son frente al riesgo.
4. Estimar el impacto que tendría una amenaza al dañar un activo.
5. Estimar el riesgo.

Figura 3.- Elementos del análisis de riesgos potenciales

Fuente: Elaboración Consejo Superior de Administración Electrónica de España – MAGERIT – Libro I – Método

2.2.5 ITIL 4

Se entiende como un conjunto de procesos referidos a la colaboración entre proveedores y consumidores del servicio contribuyendo a la percepción de valor para el usuario (Morón, 2020). Asimismo, la biblioteca de infraestructura de tecnología de la información, por sus siglas en inglés ITIL 4 (Information Technology Infraestructure Library), es una guía de 30 mejores prácticas para la gestión de servicios de TI, que permite proporcionar a las organizaciones un marco de orientación para emplear el potencial del avance tecnológico y para adecuarse a los nuevos retos de la gestión de servicios. Este marco de mejores prácticas permite diseñar un sistema coordinado, flexible e integrado para el gobierno y la gestión efectiva de los servicios referidos a tecnologías de la información de la organización (Axelos, 2019).

Como la Biblioteca de Infraestructura de Tecnologías de Información es un conjunto de conceptos y buenas prácticas que se actualiza con los cambios y avances tecnológicos va cambiando de enfoque y estructura. En la versión anterior ITIL 3, el enfoque se orientaba a la gestión de procesos y se estructuraba en base al ciclo de vida para la Gestión de Servicios (limitado). Con la actual versión, ITIL 4 se enfoca en prácticas de creación de valor y su estructura se basa en la cadena de creación de valor (flexible).

El Sistema de Valor del Servicio ITIL (ITIL SVS) permite representar la interacción entre los diversas actividades y compontes de la organización que operan de manera conjunta para que se

facilite la creación de valor mediante los servicios que se encentren habilitados de tecnologías de la información. En la figura a continuación se presenta la estructura del sistema de valor del servicio en la cual se representa la integración y coordinación de cada componente, permite diseñar una dirección sólida, unificada y centrada en el valor para la organización. Los principales componentes del ITIL SVS son: La cadena de valor del servicio ITIL, las prácticas ITIL, los principios guía de ITIL, gobernabilidad y la mejora continua (Axelos, 2019).

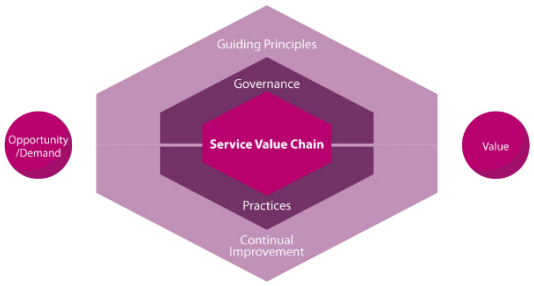


Figura 4.- El sistema de valor del servicio (ITIL SVS)

Fuente: Axelos (2019)

2.3 Cuadro comparativo de normas

A continuación, se muestra un benchmarking que utiliza una escala de 1 a 5 para calificar cada norma y/o estándar y un factor de ponderación aplicado a cada ítem (características, ventajas, desafíos y objetivos. De esta forma se podrá identificar la normativa con más alto puntaje siendo la elegida para la investigación.

	COBIT	ITIL	ISO 27001	ISO 31000
Características	Corrige los criterios de toma de decisión en la gerencia.	Corrige la comunicación entre usuarios finales y trabajadores.	Mejora los procesos de producción y distribución de productos.	Facilita la mejora continua de la organización, es sistemática, estructurada y adecuada.
0.3	3	4	5	4
Ventajas	Extiende los conocimientos a todos los sectores productivos de la empresa.	Aumenta la confiabilidad de la entrega de servicio de TI.	Se logra mejoras en un corto plazo siendo útil para PYMES.	Mejora la gestión organizacional, establece una base confiable para la toma de decisiones y la planificación estratégica.
0.3	4	3	4	3
Desafíos	Se necesita mucho tiempo para adoptarlo.	Se necesita mucho tiempo y esfuerzo para completar la	Se corre el riesgo de eliminar la perspectiva independiente entre	Orientado a todo tipo de riesgo y no a riesgos de seguridad de la

	COBIT	ITIL	ISO 27001	ISO 31000
		absorción a la cultura empresarial.	procesos.	información.
0.2	2	1	4	3
Objetivos	Delimita los planes estratégicos de TI basados en la arquitectura de red y equipos.	Se logra conectar las TI con el negocio con seguridad, precisión y disponibilidad de los servicios.	Mejora la adecuación de los procesos a los avances tecnológicos.	Ayuda a generar un enfoque para mejorar la gestión de riesgos más sistemática alcanzando los objetivos empresariales.
0.2	3	2	5	3
Total	3.1	2.7	4.5	3.3

Tabla 1.- Cuadro comparativo de normas

Leyenda:

Factor de ponderación
Calificación de cada ítem aplicado a la norma
Resultado total para cada norma

Fuente: Elaboración propia

El cálculo se realiza multiplicando el factor de ponderación por cada calificación de las normas y sumando todos los resultados parciales para obtener la calificación total de la norma.

De acuerdo con los resultados se eligió la ISO 27001 por tener el puntaje más alto (4.5). Con los resultados identificamos que esta normativa es la única que se enfoca en la seguridad de información ayudando en la disminución de riesgos, también permite la reducción de costes por la disminución de incidentes. De igual forma fortalece la organización interna y los procesos de mejora continua.

Capítulo

3. Hipótesis y variables

3.1 Hipótesis general

- El diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye de forma eficaz en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

3.2 Hipótesis específicas

- El diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye de forma eficaz en la protección de datos personales para el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

- El diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye de forma eficaz en el aseguramiento de los activos de información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

- El diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye de forma eficaz en el nivel de percepción de los trabajadores sobre la seguridad de la información en el proceso de emisión de certificados médicos de aptitud en la Clínica IPC Salud.

- El diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye de forma eficaz en el grado de adaptabilidad para el personal respecto a la seguridad de la información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

3.3 Identificación de variables

Variable independiente: Diseño de un Sistema de Gestión de Seguridad de la Información bajo la ISO/IEC 27001:2022.

Variable dependiente: Proceso de emisión de certificados de aptitud médica

3.4 Matriz de consistencia

<table>
<tr><th>Problema
General</th><th>Objetivo
General</th><th>Hipótesis
General</th><th>Variables e
Indicadores</th><th>Métodos y técnicas de
investigación</th></tr>
<tr><td>¿De qué manera el diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud?</td><td>Determinar la influencia del diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud</td><td>El diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye de forma eficaz en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud</td><td>Variable Independiente:
Diseño de un sistema de gestión de seguridad de la información

Dimensiones e Indicadores:

D1. Planificar
1. Actividades operativas de planificación

D2. Hacer
2. N° de actividades de seguridad ejecutadas

D3. Verificar
3. Revisión de las actividades planificadas y ejecutadas

D4. Actuar
4. Análisis de la mejora de la seguridad</td><td rowspan="3"><u>Metodología</u>

Enfoque:
Cuantitativo

Tipo:
Aplicado

Diseño: Cuasiexperimental

Técnicas e Instrumentos de recolección de datos:

• Encuesta por cuestionario de satisfacción</td></tr>
<tr><td>Problemas
Específicos</td><td>Objetivos
Específicos</td><td>Hipótesis
Específicas</td><td></td></tr>
<tr><td>1: ¿De qué manera el diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022</td><td>1: Determinar la influencia del diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 en la</td><td>1: El diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye de forma eficaz en</td><td>Variable Dependiente:
Proceso de emisión de certificados médicos de aptitud</td></tr>
</table>

influye en la protección de datos personales en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud? 2: ¿De qué forma el diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye en el aseguramiento de los activos de información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud? 3: ¿En qué medida el diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye en el nivel de percepción de los trabajadores sobre la seguridad de la información en el	protección de datos personales para el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud 2: Identificar la influencia diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 en el aseguramiento de los activos de información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud 3: Estimar la influencia del diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 en el nivel de percepción de los trabajadores sobre la seguridad de la información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud 4: Evaluar la influencia del diseño de un sistema de gestión de seguridad de la	la protección de datos personales para el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud 2: El diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye de forma eficaz en el aseguramiento de los activos de información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud 3: El diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye de forma eficaz en el nivel de percepción de los trabajadores sobre la seguridad de la información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud 4: El diseño de un sistema de gestión de seguridad de la información bajo la	**Dimensiones e Indicadores:** D1. Protección de datos personales 1. Controles de seguridad de la información D2. Aseguramiento de los activos de información 1. Confiabilidad 2.Integridad 3.Disponibilidad D3. Nivel de percepción 1. Nivel de percepción de los trabajadores sobre la seguridad de la información D4. Grado de adaptabilidad para el personal respecto a la seguridad informática 1. Adaptabilidad de procedimientos de seguridad	

proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud? 4: ¿Como el diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 influye en el grado de adaptabilidad para el personal respecto a la seguridad de la información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud?	información bajo la ISO/IEC 27001:2022 en el grado de adaptabilidad para el personal respecto a la seguridad de la información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud	ISO/IEC 27001:2022 influye de forma eficaz en el grado de adaptabilidad para el personal respecto a la seguridad de la información en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud		

Tabla 2.- Matriz de consistencia

Fuente: Elaboración Propia

3.5 Operacionalización de variables

Variable	Definición Conceptual	Definición operacional	Dimensiones	Indicadores	Ítem	Escala de medición
Diseño de un Sistema de Gestión de Seguridad de la Información bajo la ISO/IEC 27001:2022	La ISO/IEC 27001 tiene el propósito de sostener la integridad de la información proporcionando la gestión de forma oportuna los activos con el uso de técnicas con la finalidad de reducir el riesgo y usando los controles y medidas necesarios para los peligros.	El SGSI conlleva la evaluación de medidas de seguridad basándose en la confiabilidad, integridad y disponibilidad, medidas de protección y políticas de seguridad para el resguardo de información y protección de activos.	Planificar	• Actividades operativas de planificación	1,2	Ordinal
			Hacer	• N° de actividades de seguridad ejecutadas	3,4	
			Verificar	• Revisión de las actividades planificadas y ejecutadas	5,6	
			Actuar	• Análisis de la mejora de la seguridad	7	
Proceso de emisión de certificados aptitud médica	El certificado médico es una declaración escrita sobre la salud del paciente, luego de realizarse pruebas o exámenes de su estado físico donde se puede identificar si se encuentra apto para trabajar y poder realizar las actividades de su puesto de trabajo.	Para la emisión del certificado médico el paciente pasa por pruebas realizadas por la enfermera pasando por los médicos verificando el estado actual del paciente donde los datos son importantes las cuales deben ser protegidos para evitar el filtrado de datos, para posteriormente ser aprobado o no por el médico encargado del área.	Protección de datos personales	• Controles de seguridad de la información	8,9,10	Ordinal
			Aseguramiento de los activos de información	• Confiabilidad	11,12,13,14,15	
				• Integridad	16,17,18,19,20	
				• Disponibilidad	21,22,23,24	
			Nivel de percepción de los trabajadores sobre la SI	• Nivel de percepción	25,26,27,28,29,30,31,32	
			Grado de adaptabilidad para el personal respecto a la SI	• Adaptabilidad de procedimientos de seguridad	33,34,35,36	

Tabla 3.- Operacionalización de variables

Fuente: Elaboración Propia

Capítulo

4. Metodología

4.1 Tipo y diseño de investigación

La presente investigación se definió como tipo cuantitativo, para llevarla a cabo fue necesaria la recolección y análisis de información, la medición y observación de resultados, siendo favorable a dar respuesta a los problemas encontrados y aprobar o no la hipótesis planteada. Por otro lado, el diseño es de tipo aplicada la cual tiene la finalidad de solucionar un determinado problema orientándose a ampliar el conocimiento y enriqueciendo el desarrollo científico.

En cuanto al diseño experimental, según Campbell y Stanley (2005) existen tres grandes clases de experimentos: experimentos puros o verdaderos, cuasi experimentos y preexperimento. En el caso de los experimentos puros, estos cuentan con tres características clave: Variables dependientes e independientes, pretest y posttesting, y grupos experimentales y control. Un concepto importante para considerar es que los participantes del experimento puro necesitan ser asignados aleatoriamente a los grupos experimentales. Para definir si una investigación es o no experimental se debe considerar la condición del control directo (manipulación) de la variable independiente, en el caso de la presente tesis es el Diseño del Sistema de Gestión de Seguridad de la Información.

Para Hernández et al. también existe una clasificación de los tipos de investigación en la que se puede advertir que "En los diseños cuasiexperimentales, los sujetos no se asignan al azar a los grupos ni se emparejan, sino que dichos grupos ya están conformados antes del experimento: son grupos intactos (la razón por la que surgen y la manera como se integraron es independiente o aparte del experimento)." (2014, p. 151).

De esta revisión, podemos concluir que en el caso de la presente tesis, para el diseño de investigación se considera de tipo cuasiexperimental, el cual está siendo usado para identificar la relación causa y efecto de una situación donde el investigador manipula la variable independiente frente a la variable dependiente identificando su influencia y la determinación del grupo de estudio se encuentra definido previamente a la investigación.

4.2 Población de estudio

La población para esta investigación está conformada por el personal técnico y administrativo de las distintas áreas involucradas en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

4.3 Tamaño y selección de muestra

La muestra que se utilizará para la presente investigación estará conformada por un total de 23 personas entre personal técnico y administrativo; por tanto, el tamaño de la muestra será N = 23.

4.4 Técnica de recolección de datos

La técnica elegida para la recolección y análisis de datos es la siguiente:

-**Encuesta:** Usada para la recolección de información adquirida mediante preguntas con el propósito de identificar la opinión y satisfacción de los entrevistados sobre un tema específico.

4.5 Validez de los instrumentos por expertos

Para la validación de los instrumentos de recolección de datos fue necesario el juicio por expertos, proceso por el cual la encuesta obtuvo la validación por 3 expertos en seguridad de la información:

N°	EXPERTO	RESULTADO DE VALIDEZ
1	Cesar Molina Neyra	95%
2	Nilo E. Carrasco Ore	100%
3	Julio Molina Gárate	91%

Tabla 4.- Validez de los instrumentos por expertos

Fuente: Elaboración propia

De igual forma se utilizará el Alfa de Cronbach para determinar la confiabilidad de los instrumentos usados para la recolección de datos, a continuación, se muestra la escala que se utilizó:

Alfa de Cronbach	Consistencia Interna
[0; 0,3]	Deficiente
[0,3; 0,5]	Regular
[0,5; 0,7]	Bueno
[0,7; 0,9]	Muy Bueno
[0,9; 1]	Excelente

Tabla 5.- Escala de Alfa de Cronbach

Fuente: Alfa de Cronbach para validar un cuestionario de uso de TIC.

El resultado obtenido del Alfa de Cronbach se puede visualizar en el Anexo 1 de la presente tesis.

Capítulo

5. Desarrollo

5.1 Inicio del proyecto

El 01 de agosto de 2023 se dio inicio al proyecto con la elaboración del cuestionario que se sometió a escrutinio y juicio de experto. Posteriormente, la encuesta fue aplicada al personal de la Clínica IPC Salud. El cuestionario fue desarrollado en concordancia con la normativa ISO/IEC 27001 para el proceso de emisión de certificados de aptitud médica. Con este fin, se desarrolló un Project Charter.

NOMBRE DEL PROYECTO	**SIGLAS DEL PROYECTO**
DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2022	DSGSI
DESCRIPCIÓN DEL PROYECTO	
El proyecto: La implementación de un SGSI bajo la normativa ISO 27001:2022 para la protección de activos de información, consistiendo en las siguientes etapas: **Etapas:** **DIAGNÓSTICO** **PLANIFICAR** ● Contexto de la organización ● Liderazgo ● Planeación ● Soporte **HACER** ● Operación **MEDIR** ● Evaluación del desempeño **ACTUAR** ● Mejora	
DEFINICIÓN DEL PROYECTO	

Diseño de un sistema de gestión de seguridad de la información bajo el estándar ISO/IEC 27001:2022 para el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud

OBJETIVOS DEL PROYECTO		
CONCEPTO	**OBJETIVOS**	**CRITERIO DE ÉXITO**
1.- Alcance	Cumplir con la elaboración de los siguientes entregables: alcance del SGSI, Metodología de riesgos, Política y objetivos de Seguridad de información	Aprobación de todos los documentos
2. Tiempo	Ejecutar las etapas del proyecto según los tiempos establecidos en el cronograma	Seguimiento del cronograma del proyecto
3. Costo	Cumplir con el presupuesto estimado S/.5244.00	No exceder del presupuesto

CRONOGRAMA DE HITOS DEL PROYECTO	
ETAPAS	**FECHA PROGRAMADA**
Inicio del proyecto	01/08/2023
Diagnóstico	07/08/2023
Planificar	18/08/2023
Hacer	23/08/2023
Medir	03/09/2023
Actuar	10/09/2023

PRINCIPALES AMENAZAS DEL PROYECTO

- Tiempo insuficiente para consolidar los controles y almacenar evidencias asociadas al SGSI
- No aprobación por parte de la alta dirección de los documentos generados a raíz del proyecto
- No cumplimiento en el tiempo establecido de actividades o documentos del cronograma del proyecto

PRINCIPALES OPORTUNIDADES DEL PROYECTO

La implementación del SGSI ayudará a conocer la eficacia de los controles y tecnologías usadas en el presente proyecto.

COSTO DEL PROYECTO	
CONCEPTO	**MONTO**
Hardware	S/.3430.00
Software	S/.400.00
Documentos	S/.1298.00
Costos Extras	S/.116.00
Presupuesto total	S/.5244.00

Tabla 6.- Project Charter

Fuente: Elaboración propia

RECURSOS

TIPO	RECURSO	COSTO
Hardware	Laptop Lenovo Thinkpad X270	S/ 1900.00
	Impresora Epson EcoTank L3210	S/ 550.00
	Celular Samsung A12	S/ 980.00
Costo Total		S/ 3430.00
Software	Microsoft Office	S/120.00
	Microsoft Visio	S/ 80.00
	IBM SPSS Statistics	S/ 200.00
Costo Total		S/ 400.00
Documentos	ISO/IEC 27001: 2022	S/ 517.53
	ISO/IEC 27002: 2022	S/ 780.47
Costo Total		S/ 1298.00
Costos Extras	Lapiceros	S/ 3.00
	Hojas bond	S/ 10.00
	Folder Manila	S/ 3.00
	Pasajes	S/ 100.00
Costo Total		S/ 116.00
SUMATORIA TOTAL		S/ 5244.00

Tabla 7.- Recursos del proyecto

Fuente: Elaboración propia

5.2 Organigrama operativo

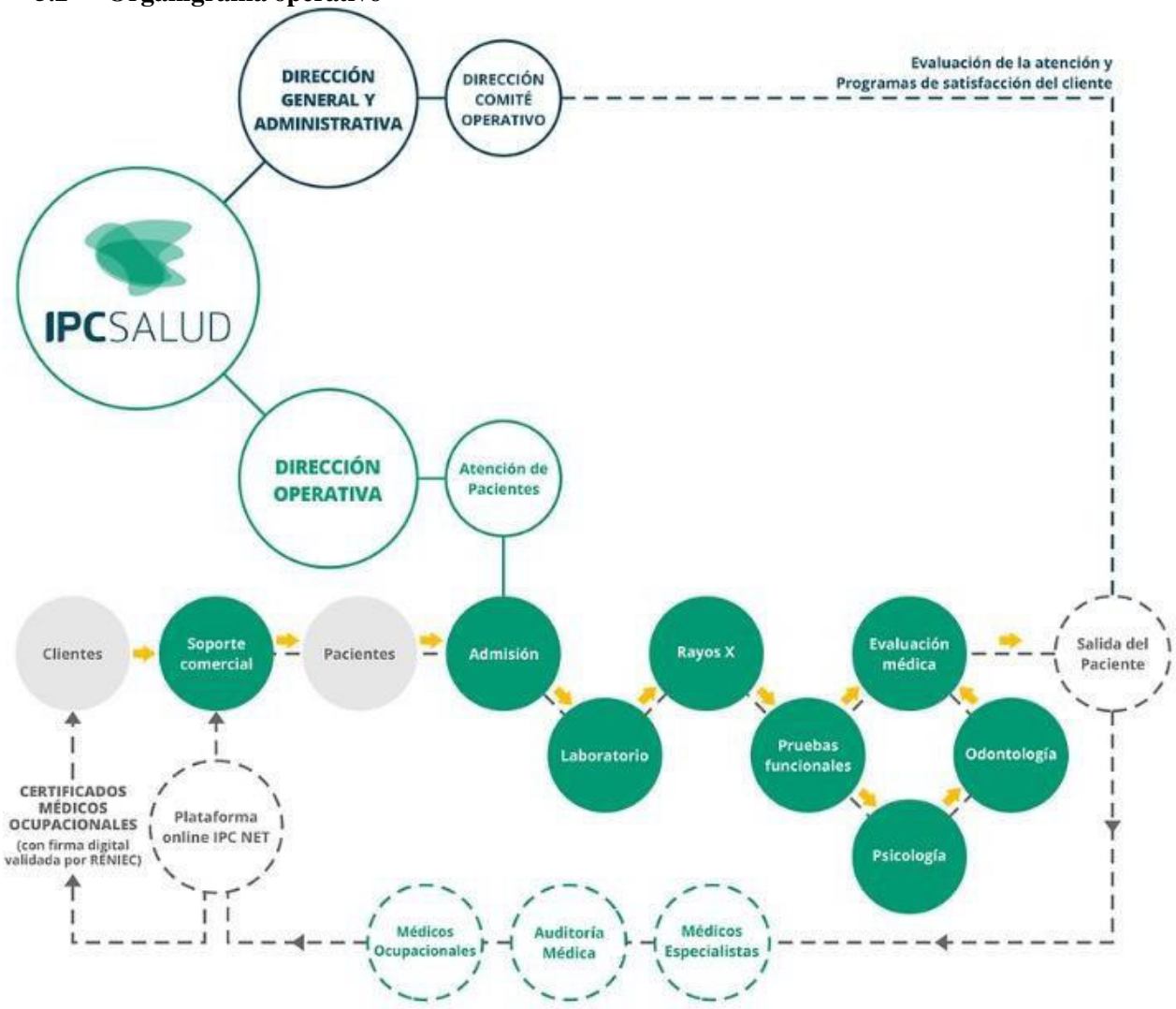


Figura 5.- Organigrama operativo

5.3 Riesgos de proyecto

Probabilidad	Valor	Impacto	Valor	Nivel de riesgo
Casi Seguro	5	Muy Alto	5	Muy Alto
Probable	4	Alto	4	Alto
Posible	3	Moderado	3	Moderado
Improbable	2	Bajo	2	Bajo
Raro	1	Muy Bajo	1	Muy Bajo

Código	Descripción del riesgo	Causa del riesgo	Consecuencia	Probabilidad	Impacto	Total	Tipo de riesgo	Plan de respuesta
R1	Modificación del cronograma de trabajo	Cambios en contexto de la empresa	Incumplimiento de las actividades según el cronograma	2	3	6	Moderado	Aprobación del cronograma
R2	Mala identificación de los activos de información	Error humano	Inconformidad del SGSI	4	4	16	Muy Alto	Realizar reuniones con el encargado del proceso
R3	Controles implementados no son los correctos	Error Humano	Inconformidad del SGSI	3	4	12	Alto	Realizar reuniones con el encargado del proceso
R4	Demora en la aprobación de los documentos generados por el proyecto	Indiferencia del personal	Inconformidad del SGSI	3	4	12	Alto	Actualización del cronograma
R5	Incumplimiento en los programas y planes de auditorías internas	Retraso con el cumplimento del plan de trabajo	Inconformidad del SGSI	3	4	12	Alto	Actualización del cronograma

Tabla 8.- Riesgos del proyecto

Fuente: Elaboración propia

5.4 Diseño del SGSI

5.4.1 Contexto de la organización

IPC SALUD es un Instituto Médico dedicado a la Salud Ocupacional y Servicios Médicos Especializados, desde hace más de 23 años, iniciando sus operaciones como un Centro de Salud especializada en Medicina Física y Rehabilitación, Traumatología y Ortopedia, y Reumatología. Posteriormente amplió sus Especialidades Médicas en las áreas de Medicina Interna, Cardiología, Otorrinolaringología, Gastroenterología, Neumología, Cirugía General y Psicología, y abrió su División de Salud Ocupacional con la que realizan evaluaciones médicas que proporcionan aptitud de las condiciones físicas de los trabajadores y así asegurar que los postulantes cumplan las exigencias propias de la función laboral que eventualmente desempeñarán en la organización que solicita y paga la evaluación médica.

5.4.1.1 Objetivos organizacionales

- Velar por la salud del trabajador con la finalidad de hacer diagnósticos precoces de enfermedades médicas y de las causadas por el trabajo físico y mental.

- Disminuir y controlar los factores de riesgo químicos, físicos, biológicos y ergonómicos; así como prevenir infecciones y contagios entre el personal de la empresa, logrando una población sana y productiva.

- Desarrollar el trabajo médico ocupacional que cubra los requerimientos médico-legales de la legislación vigente, con la finalidad de representar a su empresa ante las inspectorías y auditorías.

- Finalmente, somos absolutamente conscientes de las consecuencias de nuestro trabajo, que permitirán dar a conocer a nuestros clientes el estado de salud de sus trabajadores, antes, durante y después de su relación laboral.

5.4.2 Identificación de los procesos de negocio

Figura 6.- Mapa de Procesos

5.4.3 Necesidades y expectativas de las partes interesadas y requisitos de SI

A continuación, se identifican las partes interesadas y requisitos de seguridad de la información sobre el proceso de emisión de certificados de aptitud médica:

PARTES INTERESADAS		REQUISITOS DEL SGSI
INTERNAS	Accionistas	Aumento de rentabilidad de la empresa
	Gerente	Maximización de rentabilidad de la empresa Asegurar la disponibilidad de los servicios a los clientes
	Trabajadores	Asegurar la protección personal
EXTERNAS	Clientes	Protección de la confiabilidad, integridad y disponibilidad de su información
	Gobierno	Cumplir con las leyes de protección de datos y servicio de calidad

Tabla 9.- Partes interesadas

Fuente: Elaboración propia

5.4.4 Alcance del sistema de SGSI

Luego de realizar el análisis sobre el contexto interno y externo de la empresa y de haber identificado las necesidades de las partes interesadas, se ha determinado que el alcance del Sistema de Gestión de Seguridad de la Información comprende los activos de la información del proceso de emisión de certificados de aptitud médica, el cual es un proceso misional de la empresa que comprende la evaluación médica del personal de las empresas clientes de la Clínica IPC Salud.

Así también, se puede describir que el proceso señalado para el SGSI se realiza en las siguientes áreas:

- Dirección General y Administrativa
- Comité Operativo
- Dirección Operativa
- Área Comercial
- Especialidades Médicas
- Auditoría Médica

- Medicina Ocupacional

El detalle de los activos de información que forman parte del proceso se encuentra identificados en el ***ítem 5.5.1 Identificación de los Activos de Información***.

5.4.5 Políticas de Seguridad de la información

La Política del Sistema de Gestión de Seguridad de la Información deberá estar expresada por la Alta Dirección y archivada en los Documentos del Sistema de Seguridad de la Información de la Organización para asegurar que es adecuada a la organización, al contexto de la organización, e incluirá el compromiso de mejora continua de la misma.

Esta Política es la base para establecer los objetivos de Seguridad de la Información, y es entendida y comunicada a toda la organización, además debe ser revisada periódicamente.

La Política estará disponible para todas las partes involucradas en el proceso y al personal de toda la organización. Será comunicada para su entendimiento y aplicación en toda la organización.

Así también, los objetivos de Seguridad de la Información (que son parte de la Política) para controles individuales de seguridad o grupos de controles son propuestos por la autoridad competente y son aprobados por la Dirección.

Finalmente, se comunica que todos los objetivos de seguridad, establecidos en la Política deberán ser revisados al menos una vez al año.

5.5 Gestión de riesgos de Seguridad de la información

La Gestión de riesgos (GR) de Seguridad de información está basada en una metodología de la ISO 31000:2018 y contextualizada bajo los parámetros de la ISO 27005:2022 que comprende las siguientes fases:

5.5.1 Identificación de los activos

Para la identificación de los activos de realiza una lista donde se puede observar de acuerdo con su categoría mostrados a continuación:

Categoría	Descripción
Hardware	Laptops
	Pc
	Impresoras
	Discos de almacenamiento externo
	Lector de huellas digitales
	Pad de firma electrónica
	Equipo de electrocardiograma
	Lector de tarjetas para firma digitales
	Dispositivo de control biométrico
	Switch core de comunicaciones
Software	Base de datos MySQL
	Página Web
	Windows Server
	Sistema IPCNet
	Dropbox
	Cobian Backup
	Portal de validación de certificados
	Firewall Perimetral
	Servidor de aplicaciones
	Servidor de archivos
Personal	Coordinadora de operaciones
	Ejecutivo Comercial
	Médico Ocupacional
	Médico Diagnosticador
	Médico evaluador
	Enfermera
	Gerente de Administración y Finanzas
	Gerente General
	Soporte TI
	Jefe de TI
Documentación	Solicitud de evaluación médica
	Consentimiento informado
	Certificado de aptitud médica

Tabla 10.- Activos de Clínica IPC Salud

Fuente: Elaboración propia

5.5.2 Análisis de riesgos

Luego distinguir los activos más importantes de la clínica es importante determinar los posibles campos de acción frente a los riesgos que puedan afectar al proceso, cuál es el problema y los efectos si se llegase a materializar.

De esta forma se elaboró una tabla para conocer los peligros de los activos donde se puede observar las causas y efectos.

Activo	Amenaza	Vulnerabilidad	Riesgo	
			Código	Consecuencia
Laptops	Acceso no autorizado	Errores de configuración Errores en los sistemas de validación. Errores que permiten el acceso a directorios.	R1	Fuga de información importante y robo de contraseñas y cuentas de los clientes
	Infección de virus (cualquier tipo)	Ingresar a páginas inadecuadas, mal control sobre los correos electrónicos(spam) Errores de configuración	R2	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales
	Obsolescencia tecnológica de equipos de cómputo	Carencia de un plan de cambios de equipos de cómputo de acuerdo a su vida útil.	R3	Lentitud de las operaciones debido a fallas de equipos de cómputo
	Hurto o robo de activo	Falta de control en el listado de activos	R4	Pérdida de información importante
PC	Acceso no autorizado	Errores de configuración Errores en los sistemas de validación. Errores que permiten el acceso a directorios.	R5	Fuga de información importante y robo de contraseñas y cuentas de los clientes
	Infección de virus (cualquier tipo)	Ingresar a páginas inadecuadas, mal control sobre los correos electrónicos(spam) Errores de configuración	R6	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales
	Hurto de equipos	Deficiencia de procedimientos de control de salida e ingresos de equipos	R7	Pérdida del equipo por robo.
	Corte de Energía eléctrica	Mal estado de los enchufes o sobre carga.	R8	Interrupción de las operaciones por corte de energía eléctrica
	Fuego (Incendio)	Carencia de sistema de seguridad contra incendio, planes y procedimientos contra incendio	R9	Pérdida de equipos por eventos de fuego
	Agua (Inundaciones, fugas) Infraestructura inadecuada para instalación de equipos	Infraestructura inadecuada para instalación de equipos	R10	Pérdida de equipos por eventos de agua.
	Obsolescencia tecnológica de equipos de cómputo	Carencia de un plan de cambios de equipos de cómputo de acuerdo a su vida útil.	R11	Lentitud de las operaciones debido a fallas de equipos de cómputo
Impresoras	Pérdida de documentos	Modificación de configuraciones de red	R12	Los documentos pueden ser expuestos en la bandeja de salida y sustraída por personas no autorizadas
	Hurto de equipos	Deficiencia de procedimientos de control de salida e ingresos de equipos	R13	Pérdida del equipo por robo.
	Corte de Energía eléctrica	Mal estado de los enchufes o sobre carga.	R14	Interrupción de las operaciones por corte de

Activo	Amenaza	Vulnerabilidad	Riesgo	
			Código	Consecuencia
				energía eléctrica
	Obsolescencia tecnológica de equipos de cómputo	Carencia de un plan de cambios de equipos de cómputo de acuerdo a su vida útil.	R15	Lentitud de las operaciones debido a fallas de equipos de cómputo
	Malware o virus	Infección por códigos maliciosos	R16	Infección a todos los equipos conectados a la misma red
Lector de huellas digitales	Acceso no autorizado	Errores de configuración Errores en los sistemas de validación.	R17	Ingresos no autorizados
	Error de usuario	Carencia de validación de datos de entradas del usuario.	R18	Bloqueo de usuario
Pad de firma electrónica	Obsolescencia tecnológica de equipos externo	Carencia de un plan de cambios de equipos de acuerdo con su vida útil.	R19	Lentitud de las operaciones debido a fallas de equipos externo
Equipo de electrocardiograma	Corte de Energía eléctrica	Corte de Energía eléctrica	R20	Interrupción de las operaciones por corte de energía eléctrica
Lector de tarjetas para firma digitales	Error de usuario	Carencia de validación de datos de entradas del usuario.	R21	Bloqueo de usuario
Switch core de comunicaciones	Malware o virus	Puertos abiertos	R22	Ingreso a la red y ejecución de servicios no autorizados en los puestos de red.
	Avería de equipos de comunicación	Falla del Switch core	R23	Pérdida de la conexión la red LAN
		Falla de equipos de radio enlaces	R24	Pérdida de la conexión de la red MAN
		Falla de equipos de enrutamiento WAN	R25	Pérdida de la conexión de la red WAN
		Ausencia de políticas de mantenimiento preventivo de los equipos de comunicación	R26	Deterioro del equipo e infraestructura de comunicación
Discos de almacenamiento externo	Hurto de equipos	Deficiencia de procedimientos de control de salida e ingresos de equipos	R27	Pérdida del equipo por robo.
	Obsolescencia tecnológica de equipos externos	Carencia de un plan de cambios de equipos de cómputo de acuerdo con su vida útil.	R28	Lentitud de las operaciones debido a fallas de equipos externo
Base de datos SQL	Acceso no autorizado	Contraseñas débiles Base de datos sin actualización	R29	Hackeo o robo de la cuenta para venderlo a terceros
	Robo de información por infección de virus	Datos sensibles sin cifrar Inyección de SQL	R30	Control de la base de datos, secuestro de información de los usuarios

Activo	Amenaza	Vulnerabilidad	Riesgo	
			Código	Consecuencia
	Abuso de privilegios de acceso.	Falta de políticas de acceso al servidor de BD.	R31	Robo de información
	Errores de mantenimiento y actualización de software.	Inadecuado control de mantenimientos y actualización de software	R32	Retraso en las operaciones
	Error de configuración de software	Carencia de un plan de gestión de cambios	R33	Fallas de operación del equipo.
	Agotamiento de recursos de software	Inadecuado dimensionamiento de hardware (disco duro, memoria RAM, etc.,)	R34	Interrupción del sistema y lentitud de las operaciones
	Corte de Energía eléctrica	Falta de abastecimiento de energía eléctrica de respaldo (UPS, Generador eléctrico	R35	Interrupción de las operaciones por corte de energía eléctrica.
Página Web	Acceso no autorizado	Pérdida de control de accesos	R36	Ingreso de hacker al sistema con permiso de usuario y administrador teniendo accesos al registro, direcciones y archivos confidenciales para una posterior divulgación
		Carencia de auditoría detallada de acceso y acciones ejecutadas a la base de datos.	R37	Robo de información
		Modificación no autorizada de BD y configuraciones.	R38	Pérdida de integridad de datos
	Error de usuario	Carencia de validación de datos de entradas del usuario.	R39	Pérdida de integridad de datos
	Redirección a sitios maliciosos	Inyección de códigos malicioso	R40	Redirección a otra página pudiendo descargar malwares, software malicioso y ataques de phishing, etc.
Windows Server	Condiciones de licencias inapropiadas	Renovación de licencias extemporáneas	R41	Condiciones de licencias inapropiadas por renovación de licencias extemporáneas
	Sanciones a infracciones respecto a los derechos de autor		R42	Sanciones a infracciones respecto a los derechos de autor por renovación de licencias extemporáneas
	Hacking	Falla actualización del Sistema Operativo	R43	Hacking por falta de actualizaciones del sistema operativo
	Código Maliciosos (virus, troyanos, bomba lógica, etc.)		R44	Códigos maliciosos (virus, troyanos, bomba lógica, etc.) por falta de actualización del

Activo	Amenaza	Vulnerabilidad	Riesgo	
			Código	Consecuencia
				sistema operativo
	Mal funcionamiento del software	Pruebas al software inexistentes o insuficientes	R45	Mal funcionamiento del software por pruebas al software inexistentes o insuficientes
		Falta de control de cambios eficaz	R46	Mal funcionamiento del software por falta de control de cambios eficaz
		Falta de procedimientos de control de cambios	R47	Mal funcionamiento del software por falta de procedimientos de control de cambios
		Parches no instalados correctamente	R48	Mal funcionamiento del software por parche no instalado correctamente
Sistema IPCNet	Error de usuario	Carencia de validación de datos de entradas del usuario.	R49	Pérdida de integridad de datos
	Redirección a sitios maliciosos	Inyección de códigos malicioso	R50	Redirección a otra página pudiendo descargar malwares, software malicioso y ataques de phishing, etc.
Dropbox	Acceso no autorizado	Pérdida de control de accesos	R51	Robo de información, modificación de documentos
	Mala configuración	Ingreso no autorizado, modificación de permisos	R52	Problemas con el almacenamiento, error de uso, problemas de carga de datos
	Fuga de información	Falta de procedimientos para la gestión de incidentes de seguridad de la información	R53	Fuga de información por falta de procedimientos sobre la gestión de incidentes de seguridad de información
Cobian Backup	Abuso de privilegios de acceso.	Falta de políticas de acceso al servidor de BD.	R54	Robo de información
	Acceso no autorizado	Contraseñas débiles Base de datos sin actualización	R55	Hackeo o robo de la cuenta para venderlo a terceros
	Robo de información por infección de virus	Datos sensibles sin cifrar Inyección de SQL	R56	Control de la base de datos, secuestro de información de los usuarios
Portal de validación de certificados	Robo de información por infección de virus	Inyección de códigos maliciosos	R57	Error y robo de certificados médicos
	Acceso no autorizado	Pérdida de control de accesos	R58	Modificación no autorizada de certificados
Firewall Perimetral	Malware o virus	Puertos abiertos	R59	Ingreso a la red y ejecución de servicios no autorizados en los puestos de red.

Activo	Amenaza	Vulnerabilidad	Riesgo	
			Código	Consecuencia
	Mal funcionamiento	Incorrecta configuración	R60	Incorrecta configuración del equipo
Servidor de aplicaciones	Indisponibilidad del equipo	Falta de planes de continuidad	R61	Indisponibilidad del equipo por falta de red inestable de energía eléctrica
	Mal funcionamiento	Falta de actualización del Sistema Operativo	R62	Falla del equipo por falta de actualización del sistema operativa
		Incorrecta configuración	R63	Incorrecta configuración del equipo
	Fuga de información	Falta de procedimientos para la gestión de incidentes de seguridad de la información	R64	Fuga de información por falta de procedimientos sobre la gestión de incidentes de seguridad de información
	Pérdida de datos	Falta de copias de respaldo	R65	Pérdida de información por falta de copias de respaldo
Servidor de archivos	Indisponibilidad del equipo	Red inestable de energía eléctrica	R66	Indisponibilidad del equipo o medio por falta de planes de continuidad
		Falta de planes de continuidad	R67	Indisponibilidad del equipo por falta de red inestable de energía eléctrica
	Mal funcionamiento	Falta de procedimientos de control de cambios	R68	Problemas con el equipo por falta de controles de cambios
		Incorrecta configuración	R69	Incorrecta configuración del equipo
	Fuga de información	Mal monitoreo de actividades de cuestas administradoras	R70	Fuga de datos por falta de procedimientos de protección de datos
	Pérdida de datos	Falta de copias de respaldo	R71	Pérdida de información por falta de copias de respaldo
Coordinadora de operaciones	Ataque cibernético con o sin intención	Mala asignación de privilegios o permisos	R72	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios
Ejecutivo Comercial	Ataque cibernético con o sin intención	Mala asignación de privilegios o permisos	R73	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios
Médico Ocupacional	Poco compromiso con la seguridad de la información	Falta de conciencia de seguridad	R74	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente
Médico Diagnosticador	Poco compromiso con la seguridad de la información	Falta de conciencia de seguridad	R75	Poco compromiso con la seguridad de la información por capacitación de seguridad

Activo	Amenaza	Vulnerabilidad	Riesgo	
			Código	Consecuencia
				insuficiente
Médico evaluador	Poco compromiso con la seguridad de la información	Capacitación de seguridad insuficiente	R76	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente
Enfermera	Poco compromiso con la seguridad de la información	Capacitación de seguridad insuficiente	R77	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente
Gerente de Administración y Finanzas	Ataque cibernético con o sin intención	Mala asignación de privilegios o permisos	R78	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios
Gerente General	Ataque cibernético con o sin intención	Mala asignación de privilegios o permisos	R79	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios
Soporte TI	Poco compromiso con la seguridad de la información	Capacitación de seguridad insuficiente	R80	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente
Jefe de TI	Poco compromiso con la seguridad de la información	Capacitación de seguridad insuficiente	R81	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente
Solicitud de evaluación médica	Perdida de documentos	Falta de procedimientos para el control de incidente	R82	Perdida de documentos por falta de métodos para el control de incidentes
Consentimiento informado	Mal uso de información	Inadecuado ambiente físico	R83	Mal uso de los datos por un mal ambiente físico
Certificado de aptitud médica	Perdida de documentos	Inadecuado procedimiento de ingreso y salida del personal, documentos y equipos en la clínica	R84	Extravió de documentos por mal manejo de procedimientos de control de ingreso y salida de personal, documentos y personal en la clínica

Tabla 11.- Identificación de peligros de los activos

Fuente: Elaboración propia

5.5.3 Evaluación del riesgo

Luego de la identificación de los activos es importante darle un valor a cada uno de ellos donde se pueda observar el grado de riesgo ante la pérdida o daño del activo, de esta forma se dividirá en 3 dimensiones la valoración. Para la valoración se usará la escala de Likert siendo del 1 al 5 estableciendo la conformidad en las 3 dimensiones (Confidencialidad, Integridad, Disponibilidad).

Confidencialidad (C): Protege la privacidad de los datos por medio de limitaciones de accesos a terceros.

Integridad (I): Protege que los datos sean precisos y confiables.

Disponibilidad (D): Asegura que la información sea accesible cuando sea necesaria.

	Valor	Criterio
Confidencialidad (C)	5	El perjuicio es catastrófico, fraude, pérdida de reputación y credibilidad
	4	El perjuicio es relevante, el incidente afecta a otros procesos
	3	El incidente no afecta a otros procesos
	2	El incidente no es tan grave
	1	No relevante

Tabla 12.- Valores de criterios de confidencialidad

Fuente: Elaboración propia

	Valor	Criterio
Integridad (I)	5	Debe se precisa y confiable al menos en un 95.5%
	4	Debe se precisa y confiable al menos en un 75%
	3	Debe se precisa y confiable al menos en un 50%
	2	No es precisa y confiable
	1	No relevante

Tabla 13.- Valores de criterios de Integridad.

Fuente: Elaboración propia

	Valor	Criterio
Disponibilidad (D)	5	Debe ser accesible al menos en el 95.5% del tiempo
	4	Debe ser accesible al menos en el 75% del tiempo
	3	Debe ser accesible al menos en el 50% del tiempo
	2	Debe ser accesible al menos en el 10% del tiempo
	1	No relevante

Tabla 14.- Valores de criterios de Disponibilidad.

Fuente: Elaboración propia

El grado de criticidad de los activos se identificará de acuerdo con la sumatoria hecha por el criterio de seguridad obteniendo la siguiente clasificación:

Nivel de criticidad: Confidencialidad + Integridad + Disponibilidad

Rango	Nivel de Criticidad	Descripción		Criterio
1 – 3	1	Muy Bajo	MB	Insignificante en los procesos
4 – 6	2	Bajo	B	Afecta los procesos en un 10%, sin pérdida de información.
7 - 9	3	Medio	M	Afecta los procesos en un 50%, sin pérdida de información.
10 – 12	4	Alto	A	Afecta los procesos en un 75%, ocasiona casi poca pérdida de información
13 - 15	5	Muy alto	MA	Afecta los procesos en un 95%, significativa pérdida de información.

Tabla 15.- Niveles de criticidad de riesgo

Fuente: Elaboración propia

De esta forma se obtendrá el rango donde se encuentra cada activo según el nivel de criticidad

N° Activo	Nombre de activo	Criterio de Seguridad			Total	Nivel de Criticidad
		C	I	D		
1.	Laptops	4	4	4	12	Alto [A]
2.	Pc	4	5	4	13	Muy Alto [MA]
3.	Impresoras	3	4	3	10	Alto [A]

4.	Discos de almacenamiento externo	3	3	2	9	Medio[M]
5.	Lector de huellas digitales	2	2	2	6	Bajo [B]

N° Activo	Nombre de activo	Criterio de Seguridad			Total	Nivel de Criticidad
		C	I	D		
6.	Pad de firma electrónica	2	2	2	6	Bajo [B]
7.	Equipo de electrocardiograma	4	5	5	14	Muy Alto [MA]
8.	Lector de tarjetas para firma digitales	4	3	4	11	Alto [A]
9.	Switch core de comunicaciones	4	4	5	13	Muy Alto [MA]
10.	Base de datos SQL	5	5	5	15	Muy Alto [MA]
11.	Página Web	4	4	4	12	Alto [A]
12.	Windows Server	5	5	5	15	Muy Alto [MA]
13.	Sistema IPCNet	4	3	5	12	Alto [A]
14.	Dropbox	4	4	5	13	Muy Alto [MA]
15.	Cobian Backup	4	4	4	12	Alto [A]
16.	Portal de validación de certificados	3	3	3	9	Medio[M]
17.	Firewall Perimetral	4	4	4	12	Alto [A]
18.	Servidor de aplicaciones	4	4	4	12	Alto [A]
19.	Servidor de archivos	4	4	4	12	Alto [A]
20.	Coordinadora de operaciones	3	4	3	10	Alto [A]
21.	Ejecutivo Comercial	3	2	3	8	Medio[M]
22.	Médico Ocupacional	4	3	3	10	Alto [A]
23.	Médico Diagnosticador	4	2	3	9	Medio[M]
24.	Médico evaluador	4	2	3	9	Medio[M]
25.	Enfermera	3	2	2	7	Medio[M]
26.	Gerente de Administración y Finanzas	3	3	3	9	Medio[M]
27.	Gerente General	4	2	3	9	Medio[M]
28.	Soporte TI	4	3	2	9	Medio[M]
29.	Jefe de TI	4	2	3	9	Medio[M]
30.	Solicitud de evaluación médica	3	3	3	9	Medio[M]
31.	Consentimiento informado	3	3	3	9	Medio[M]
32.	Certificado de aptitud médica	5	4	4	13	Muy Alto [MA]

Tabla 16.- Cuadro de Criterios de criticidad de riesgos

Fuente: Elaboración propia

EVALUACIÓN DE LAS CONSECUENCIAS

Para la evaluación se obtiene los datos de las matrices de los activos para que estos sean evaluados

identificando el impacto y la probabilidad de que el riesgo ocurra.

MATRIZ DE RIESGO POR PROBABILIDAD

PROBABILIDAD		
Valor	**Clasificación**	**Descripción**
5	Casi Seguro	Se podría presentar mensualmente.
4	Probable	Se podría presentar mensualmente.
3	Posible	Se podría presentar hasta tres veces al año.
2	Improbable	Se podría presentar una vez al año.
1	Raro	No se presenta en varios años.

Tabla 17.- Escala de riesgo por probabilidad

Fuente: Elaboración propia

MATRIZ DE RIESGO POR IMPACTO

IMPACTO		
Valor	**Clasificación**	**Descripción**
5	Muy Alto	Tiene un efecto adverso grave o catastrófico que paraliza todas las operaciones o activos críticos de la organización
4	Alto	Tiene un efecto adverso grave o catastrófico que paraliza algunas operaciones o activos críticos de la organización
3	Moderado	Tiene un efecto adverso considerable que ralentiza operaciones o activos de la organización.
2	Bajo	Tiene un efecto adverso limitado en las operaciones o activos, de la organización
1	Muy Bajo	Tiene un efecto adverso insignificante en las operaciones o activos de la organización.

Tabla 18.- Escala de riesgo por impacto

Fuente: Elaboración propia

Posterior a la identificación de la escala para definir los niveles del activo, el nivel de probabilidad de la amenaza y el nivel de las consecuencias por cada activo en riesgo, se podrá calcular la medida del peligro (probabilidad x impacto) = Medida del riesgo

MATRIZ DE RIESGOS

Para la evaluación del riesgo se presenta la siguiente matriz:

		Valor					
PROBABILIDAD	Casi Seguro	5	5	10	15	20	25
	Probable	4	4	8	12	16	20
	Posible	3	3	6	9	12	15
	Improbable	2	2	4	6	8	10
	Raro	1	1	2	3	4	5
		Valor	1	2	3	4	5
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
			IMPACTO				

Tabla 19.- Criterios de criticidad

Fuente: Elaboración propia

ESCALA DE PRIORIZACIÓN DEL RIESGO

Nivel de Riesgo	Calificación
Muy Alto	15 a 25
Alto	9 a 14
Moderado	4 a 8
Bajo	1 a 3

Tabla 20.- Escala de criticidad

Fuente: Elaboración propia

A continuación, se mostrará la matriz con la valoración de los activos siendo evaluados por la probabilidad, el impacto determinación del nivel del riesgo y la clasificación de prioridad del riesgo.

MATRIZ DE VALORACIÓN DEL RIESGO

Código	Riesgo	Probabilidad		Impacto		Evaluación del Riesgo	Categoría
		Nivel	Descripción	Nivel	Descripción		
R1	Fuga de información importante y robo de contraseñas y cuentas de los clientes	3	Posible	5	Muy Alto	15	Muy Alto
R2	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales	2	Imposible	5	Muy Alto	10	Alto
R3	Lentitud de las operaciones debido a fallas de equipos de cómputo	4	Raro	4	Alto	16	Muy Alto
R4	Pérdida de información importante	4	Probable	4	Alto	16	Muy Alto
R5	Fuga de información importante y robo de contraseñas y cuentas de los clientes	3	Posible	4	Alto	12	Alto
R6	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales	2	Imposible	4	Alto	8	Moderado
R7	Pérdida del equipo por robo.	3	Raro	2	Bajo	6	Moderado
R8	Interrupción de las operaciones por corte de energía eléctrica	2	Posible	5	Muy Alto	10	Alto
R9	Pérdida de equipos por eventos de fuego	1	Raro	4	Alto	4	Moderado
R10	Pérdida de equipos por eventos de agua.	3	Posible	2	Bajo	6	Moderado
R11	Lentitud de las operaciones debido a fallas de equipos de cómputo	1	Raro	4	Alto	4	Moderado
R12	Los documentos pueden ser expuestos en la bandeja de salida y sustraída por personas no autorizadas	2	Improbable	2	Bajo	4	Moderado
R13	Pérdida del equipo por robo.	3	Posible	2	Bajo	6	Moderado
R14	Interrupción de las operaciones por corte de energía eléctrica	2	Improbable	5	Muy Alto	10	Alto
R15	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo	1	Raro	4	Alto	4	Moderado
R16	Infección a todos los equipos conectados a la misma red	3	Posible	3	Moderado	9	Alto
R17	Ingresos no autorizados	2	Improbable	3	Moderado	6	Moderado
R18	Bloqueo de usuario	3	Posible	2	Bajo	6	Moderado

R19	Lentitud de las operaciones debido a fallas de equipos externo	1	Raro	2	Bajo	3	Bajo
R20	Interrupción de las operaciones por corte de energía eléctrica	3	Posible	3	Moderado	9	Alto
R21	Bloqueo de usuario	3	Posible	2	Bajo	6	Moderado
R22	Ingreso a la red y ejecución de servicios no autorizados en los puestos de red.	2	Improbable	4	Alto	8	Moderado
R23	Pérdida de la conexión la red LAN	2	Improbable	4	Alto	8	Moderado
R24	Pérdida de la conexión de la red MAN	3	Posible	4	Alto	12	Alto
R25	Pérdida de la conexión de la red WAN	2	Improbable	4	Alto	8	Moderado
R26	Deterioro del equipo e infraestructura de comunicación	2	Improbable	3	Moderado	6	Moderado
R27	Pérdida del equipo por robo.	3	Raro	2	Bajo	6	Moderado
R28	Lentitud de las operaciones debido a fallas de equipos externo	2	Improbable	1	Muy Bajo	2	Bajo
R29	Hackeo o robo de la cuenta para venderlo a terceros	3	Posible	3	Moderado	9	Alto
R30	Control de la base de datos, secuestro de información de los usuarios	3	Posible	5	Muy Alto	15	Muy Alto
R31	Robo de información	4	Probable	4	Alto	16	Muy Alto
R32	Retraso en las operaciones	2	Improbable	5	Muy Alto	10	Alto
R33	Fallas de operación del equipo.	1	Raro	5	Muy Alto	5	Moderado
R34	Interrupción del sistema y lentitud de las operaciones	1	Raro	4	Alto	4	Moderado
R35	Interrupción de las operaciones por corte de energía eléctrica.	2	Improbable	5	Muy Alto	10	Alto
R36	Ingreso de hacker al sistema con permiso de usuario y administrador teniendo accesos al registro, direcciones y archivos confidenciales para una posterior divulgación	2	Improbable	4	Alto	12	Alto
R37	Robo de información	1	Raro	3	Posible	3	Bajo
R38	Pérdida de integridad de datos	1	Raro	3	Posible	3	Bajo
R39	Pérdida de integridad de datos	3	Posible	2	Bajo	6	Moderado
R40	Redirección a otra página pudiendo descargar malwares, software malicioso y ataques de phishing, etc	2	Improbable	4	Alto	12	Alto
R41	Condiciones de licencias inapropiadas por renovación de licencias extemporáneas	1	Raro	4	Alto	4	Bajo

R42	Sanciones a infracciones respecto a los derechos de autor por renovación de licencias extemporáneas	1	Raro	1	Muy Bajo	1	Bajo
R43	Hacking por falta de actualizaciones del sistema operativo	3	Posible	3	Moderado	9	Alto
R44	Códigos maliciosos (virus, troyanos, bomba lógica, etc) por falta de actualización del sistema operativo	3	Posible	3	Moderado	9	Alto
R45	Mal funcionamiento del software por pruebas al software inexistentes o insuficientes	2	Improbable	4	Alto	8	Moderado
R46	Mal funcionamiento del software por falta de control de cambios eficaz	3	Posible	4	Alto	12	Alto
R47	Mal funcionamiento del software por falta de procedimientos de control de cambios	3	Posible	4	Alto	12	Alto
R48	Mal funcionamiento del software por parche no instalado correctamente	2	Improbable	4	Alto	8	Moderado
R49	Pérdida de integridad de datos	3	Posible	3	Moderado	9	Alto
R50	Redirección a otra página pudiendo descargar malwares, software malicioso y ataques de phishing, etc	1	Raro	3	Moderado	3	Bajo
R51	Robo de información, modificación de documentos	2	Improbable	4	Alto	8	Moderado
R52	Problemas con el almacenamiento, error de uso, problemas de carga de datos	1	Raro	3	Moderado	3	Bajo
R53	Fuga de información por falta de procedimientos sobre la gestión de incidentes de seguridad de información	2	Improbable	4	Alto	8	Moderado
R54	Robo de información	3	Posible	3	Moderado	9	Alto
R55	Hackeo o robo de la cuenta para venderlo a terceros	2	Improbable	3	Moderado	6	Moderado
R56	Control de la base de datos, secuestro de información de los usuarios	3	Posible	5	Muy Alto	15	Muy Alto
R57	Error y robo de certificados médicos	3	Posible	4	Alto	12	Alto
R58	Modificación no autorizada de certificados	3	Posible	3	Moderado	9	Alto
R59	Ingreso a la red y ejecución de servicios no autorizados en los puestos de red.	2	Improbable	3	Moderado	6	Moderado
R60	Incorrecta configuración del equipo	2	Improbable	1	Muy Bajo	2	Bajo
R61	Indisponibilidad del equipo por falta de red inestable de energía eléctrica	3	Posible	3	Moderado	9	Alto

R62	Falla del equipo por falta de actualización del sistema operativa	1	Raro	1	Muy Bajo	1	Bajo
R63	Incorrecta configuración del equipo	2	Improbable	1	Muy Bajo	2	Bajo
R64	Fuga de información por falta de procedimientos sobre la gestión de incidentes de seguridad de información	4	Probable	4	Alto	16	Muy Alto
R65	Pérdida de información por falta de copias de respaldo	4	Probable	4	Alto	16	Muy Alto
R66	Indisponibilidad del equipo o medio por falta de planes de continuidad	3	Posible	3	Moderado	9	Alto
R67	Indisponibilidad del equipo por falta de red inestable de energía eléctrica	3	Posible	3	Moderado	9	Alto
R68	Problemas con el equipo por falta de controles de cambios	3	Posible	4	Alto	12	Alto
R69	Incorrecta configuración del equipo	2	Improbable	1	Muy Bajo	2	Bajo
R70	Fuga de datos por falta de procedimientos de protección de datos	3	Posible	3	Moderado	9	Alto
R71	Pérdida de información por falta de copias de respaldo	2	Improbable	3	Moderado	6	Moderado
R72	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios	3	Posible	4	Alto	12	Alto
R73	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios	3	Posible	4	Alto	12	Alto
R74	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	3	Posible	2	Bajo	6	Moderado
R75	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	3	Posible	2	Bajo	6	Moderado
R76	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	3	Posible	2	Bajo	6	Moderado
R77	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	3	Posible	2	Bajo	6	Moderado
R78	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios	3	Posible	4	Alto	12	Alto
R79	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios	3	Posible	4	Alto	12	Alto
R80	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	3	Posible	2	Bajo	6	Moderado

R81	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	3	Posible	2	Bajo	6	Moderado
R82	Perdida de documentos por falta de métodos para el control de incidentes	1	Raro	2	Bajo	4	Bajo
R83	Mal uso de los datos por un mal ambiente físico	1	Raro	2	Bajo	4	Bajo
R84	Extravió de documentos por mal manejo de procedimientos de control de ingreso y salida de personal, documentos y personal en la clínica	1	Raro	2	Bajo	4	Bajo

Tabla 21.- Matriz de valoración del riesgo

Fuente: Elaboración Propia

MATRIZ DE CALOR

PROBABILIDAD					
5					
4				R3,R4,R31,R64, R65	
3		R7,R10,R13, R18, R21,R27,R39,R74,R75,R76,R77,R80, R81	R16,R20,R29, R43,R44,R49, R54,R58,R61, R66,R67,R70	R5,R24,R46,R47, R57,R68,R72,R73, R78,R79	R1,R30,R56
2	R28,R60, R63,R69	R12	R17,R26,R55, R59,R71	R6,R22,R23,R25, R36,R40,R45,R48, R51	R2,R8,R14,R32,R35
1	R42, R62	R19,R82,R83,R84	R37,R38,R50, R53	R9,R11, R15,R34,R41	R33
	1	2	3	4	5

IMPACTO

Tabla 22.- Matriz de calor

Fuente: Elaboración Propia.

5.5.4 Tratamiento del riesgo

Luego de identificar los riesgos, es necesario darle un correcto tratamiento para los riesgos que se encuentren en los niveles: muy alto, alto y moderado con el fin de que puedan ser mitigados. Con este fin, se aplicarán las siguientes estrategias de tratamiento:

- Evitar el riesgo: Se implementan acciones para hacer que las condiciones o los factores que pueden generar el riesgo desaparezcan, y con ellos, el riesgo.
- Reducir el riesgo: El riesgo se reduce a través de la prevención por medio de la implementación de controles.
- Aceptar el riesgo: Decisión generada por la entidad de aceptar las consecuencias y probabilidad de un riesgo.
- Transferir el riesgo: El riesgo puede ser transferido a otra empresa que tenga más capacidad de tratarlo.

Donde, E= Evitar el riesgo, R= Reducir el riesgo, A= Aceptar el riesgo, T = Transferir el riesgo

A continuación, se muestra un plan de tratamiento de los riesgos sobre los activos de valoración moderado, alta y muy alta:

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
R1	Fuga de información importante y robo de contraseñas y cuentas de los clientes	15	Muy Alto	R	**9.4.1 Restricción de acceso a la información** El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso.	Controlar los datos que pueden ser accedidos por un usuario en particular; controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicación o sistemas.
R3	Lentitud de las operaciones debido a fallas de equipos de cómputo	16	Muy Alto	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	Solo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo
R4	Pérdida de información importante	16	Muy Alto	R	**8.2.1 Clasificación de la información** Los propietarios de los activos deberían revisar los derechos de acceso de usuario a intervalos regulares.	los derechos de acceso de los usuarios deberían ser revisados en intervalos regulares y después de cualquier cambio, tal como la promoción, la degradación o la terminación del empleo, los derechos de acceso de usuario deberían ser revisados y reasignados al pasar de un rol a otro dentro de la misma organización; las autorizaciones de los derechos de acceso privilegiados deberían revisarse a intervalos más frecuentes.
R20	Control de la base de datos, secuestro de	15	Muy Alto	R	**9.1.1 Política de control de acceso**	Los propietarios de activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
	información de los usuarios				Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	restricciones para las funciones específicas de los usuarios con respecto a sus activos, con el nivel de detalle y el rigor de los controles que reflejan los riesgos de seguridad de información asociados.
R21	Robo de información	16	Muy Alto	R	**9.1.1 Política de control de acceso** Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Los propietarios de activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y restricciones para las funciones específicas de los usuarios con respecto a sus activos, con el nivel de detalle y el rigor de los controles que reflejan los riesgos de seguridad de información asociados.
R56	Control de la base de datos, secuestro de información de los usuarios	15	Muy Alto		**9.1.1 Política de control de acceso** Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Los propietarios de activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y restricciones para las funciones específicas de los usuarios con respecto a sus activos, con el nivel de detalle y el rigor de los controles que reflejan los riesgos de seguridad de información asociados.
R64	Fuga de información por	16	Muy Alto		**9.4.1 Restricción de acceso a la información**	Controlar los datos que pueden ser accedidos por un usuario en particular; controlar los

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
	falta de procedimientos sobre la gestión de incidentes de seguridad de información				El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso.	derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicación o sistemas.
R65	Pérdida de información por falta de copias de respaldo	16	Muy Alto		**12.3.1 Respaldo de la información** Copias de respaldo de la información, del software y de las imágenes del sistema deberían ser realizadas y verificadas regularmente en concordancia con una política de respaldo acordada.	Debería establecerse una política de respaldo para definir los requisitos de la organización para los respaldos de la información, software y sistemas. La política de respaldo debería definir los requisitos de retención y protección. Deberían proporcionarse instalaciones adecuadas de respaldo para garantizar que toda la información y software esenciales se pueden recuperar después de un desastre o falla de medios.
R2	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales	10	Alto	R	**9.4.1 Restricción de acceso a la información** El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso.	Controlar los datos que pueden ser accedidos por un usuario en particular; controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicación o sistemas.

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
R5	Fuga de información importante y robo de contraseñas y cuentas de los clientes	12	Alto	R	**9.4.1 Restricción de acceso a la información** El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso.	Controlar los datos que pueden ser accedidos por un usuario en particular; controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicación o sistemas.
R8	Interrupción de las operaciones por corte de energía eléctrica	10	Alto	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	controles para reducir al mínimo el riesgo de amenazas físicas potenciales, como: hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética y vandalismo
R14	Interrupción de las operaciones por corte de energía eléctrica	10	Alto		**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	controles para reducir al mínimo el riesgo de amenazas físicas potenciales, como: hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética y vandalismo

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
R16	Infección a todos los equipos conectados a la misma red	9	Alto	R	**13.1.2 Seguridad de servicios de red** Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deberían ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados	Las medidas de seguridad necesarias para los servicios particulares, tales como características de seguridad, niveles de servicio y los requisitos de gestión, deberían estar identificadas. La organización debería asegurarse que los proveedores de los servicios de red implementen estas medidas
R19	Hackeo o robo de la cuenta para venderlo a terceros	9	Alto	R	**12.2.1 Controles contra software malicioso (malware)** Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concienciación apropiada de los usuarios.	La protección contra software malicioso debería basarse en el empleo de software de detección de código malicioso y reparación, en la creación de conciencia de la seguridad de información y en apropiados controles de acceso al sistema y gestión de cambios
R20	Interrupción de las operaciones por corte de energía eléctrica	9	Alto		**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de	controles para reducir al mínimo el riesgo de amenazas físicas potenciales, como: hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
					amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética y vandalismo
R22	Retraso en las operaciones	10	Alto	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad	Se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo
R24	Pérdida de la conexión de la red MAN	12	Alto		**13.1.3 Segregación en redes** Grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes	El perímetro de cada dominio debería estar bien definido. Se permite el acceso entre dominios de la red, pero debería ser controlado en el perímetro utilizando una puerta de enlace (por ejemplo, cortafuegos, router con capacidad de filtrado)
R25	Interrupción de las operaciones por corte de energía eléctrica.	10	Alto	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado	Controles para reducir al mínimo el riesgo de amenazas físicas potenciales, como: hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética y vandalismo
R26	Ingreso de hacker al sistema con	12	Alto	R	**9.2.1 Registro y baja de usuarios**	Utilizar la identificación única de usuario (ID´s) para que los usuarios puedan estar vinculados y sean responsable de sus

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
	permiso de usuario y administrador teniendo accesos al registro, direcciones y archivos confidenciales para una posterior divulgación				Un proceso formal de registro y baja de usuarios debería estar implementado para permitir la asignación de derechos de acceso.	acciones; el uso de identificaciones compartidas debería sólo ser permitido cuando sean necesarios por razones de negocios o de funcionamiento y debería estar aprobados y documentados; deshabilitar o quitar inmediatamente los ID de usuario a los usuarios que han dejado la organización
R30	Redirección a otra página pudiendo descargar malwares, software malicioso y ataques de phishing, etc	12	Alto	R	**9.4.5 Control de acceso al código fuente de los programas** El acceso al código fuente de los programas debería estar restringido.	El acceso al código de los programas fuente y elementos asociados (tales como diseños, especificaciones, planos de verificación y planos de validación) deberían estar estrictamente controlados, con el fin de prevenir la introducción de funcionalidades no autorizadas y evitar cambios no intencionales, así como para mantener la confidencialidad de la propiedad intelectual de valor
R33	Hacking por falta de actualizaciones del sistema operativo	9	Alto	R	**12.2.1 Controles contra software malicioso** Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concienciación apropiada de los usuarios.	La protección contra software malicioso debería basarse en el empleo de software de detección de código malicioso y reparación, en la creación de conciencia de la seguridad de información y en apropiados controles de acceso al sistema y gestión de cambios

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
R34	Códigos maliciosos (virus, troyanos, bomba lógica, etc) por falta de actualización del sistema operativo	9	Alto	R	**12.2.1 Controles contra software malicioso** Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concienciación apropiada de los usuarios.	La protección contra software malicioso debería basarse en el empleo de software de detección de código malicioso y reparación, en la creación de conciencia de la seguridad de información y en apropiados controles de acceso al sistema y gestión de cambios
R36	Mal funcionamiento del software por falta de control de cambios eficaz	12	Alto	R	**12.1.2 Gestión del cambio** **12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones** **14.2.2 Procedimientos de control de cambio del sistema** **14.2.3 Revisión técnica de aplicaciones después de cambios a la plataforma operativa**	Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información deberían ser controlados. Los entornos de desarrollo, pruebas y operaciones deberían estar separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo. Cambios a los sistemas dentro del ciclo de vida del desarrollo deberían estar controlados por medio del uso de procedimientos formales de control de cambios. Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deberían ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización
R37	Mal funcionamiento	12	Alto	R	**12.1.2 Gestión del cambio** **14.2.2 Procedimientos de**	Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
	del software por falta de procedimientos de control de cambios				**control de cambio del sistema**	información y sistemas que afecten la seguridad de la información deberían ser controlados. Cambios a los sistemas dentro del ciclo de vida del desarrollo deberían estar controlados por medio del uso de procedimientos formales de control de cambios.
R49	Pérdida de integridad de datos	9	Alto	R	**12.3.1 Respaldo de la información** Copias de respaldo de la información, del software y de las imágenes del sistema deberían ser realizadas y verificadas regularmente en concordancia con una política de respaldo acordada.	Debería establecerse una política de respaldo para definir los requisitos de la organización para los respaldos de la información, software y sistemas. La política de respaldo debería definir los requisitos de retención y protección. Deberían proporcionarse instalaciones adecuadas de respaldo para garantizar que toda la información y software esenciales se pueden recuperar después de un desastre o falla de medios.
R54	Robo de información	9	Alto		**9.1.1 Política de control de acceso** Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Los propietarios de activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y restricciones para las funciones específicas de los usuarios con respecto a sus activos, con el nivel de detalle y el rigor de los controles que reflejan los riesgos de seguridad de información asociados.
R57	Error y robo de certificados	12	Alto		**8.2.2 Etiquetado de la información**	Los procedimientos para el etiquetado de la información necesitan cubrir la información y

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
	médicos				Un conjunto apropiado de procedimientos para el etiquetado de la información debería estar desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.	sus activos relacionados en formato físico y electrónico. La salida de los sistemas que contienen información clasificada como sensible o crítica debería llevar una etiqueta adecuada de clasificación.
R58	Modificación no autorizada de certificados	9	Alto		**8.2.3 Manejo de activos** Los procedimientos para el manejo de activos deberían ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.	Deberían elaborarse procedimientos para el manejo, procesamiento, almacenamiento y comunicación de la información, de acuerdo con su clasificación
R61	Indisponibilidad del equipo por falta de red inestable de energía eléctrica	9	Alto		**11.2.2 Servicios de suministro** Los equipos deberían estar protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	Los elementos de soporte (por ejemplo, la electricidad, las telecomunicaciones, el agua potable, el gas, el alcantarillado, la ventilación y el aire acondicionado)

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
R66	Indisponibilidad del equipo o medio por falta de planes de continuidad	9	Alto		**17.1.2 Implementación de continuidad de seguridad de la información** La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa	Se establece una estructura de gestión adecuada para estar preparados para, mitigar y responder a un evento disruptivo utilizando personal con la autoridad, experiencia y competencia necesarias
R67	Indisponibilidad del equipo por falta de red inestable de energía eléctrica	9	Alto		**11.2.2 Servicios de suministro** Los equipos deberían estar protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	Los elementos de soporte (por ejemplo, la electricidad, las telecomunicaciones, el agua potable, el gas, el alcantarillado, la ventilación y el aire acondicionado)
R68	Problemas con el equipo por falta de controles de cambios	12	Alto		**12.1.2 Gestión del cambio** Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afecten la seguridad de	Identificación y registro de cambios significativos; planificación y pruebas de los cambios; evaluación de los impactos potenciales, incluyendo los impactos en la seguridad de la información de tales cambios

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
					la información deberían ser controlados**.**	
R70	Fuga de datos por falta de procedimientos de protección de datos	9	Alto	R	**12.4.2 Protección de información de registros.** Las instalaciones para registros y la información de los registros deberían estar protegidas contra la adulteración y el acceso no autorizado.	Los controles deberían proteger contra cambios no autorizados y problemas operativos en los medios de registro
R72	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios	12	Alto	R	**9.4.3 Sistema de gestión de contraseñas** Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar que las contraseñas sean de calidad	La política debería incluir los requisitos para la gestión de claves. La contraseña deberá tener mínimo 9 caracteres y contemplar mayúsculas, minúsculas, números y caracteres especiales.
R73	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios	12	Alto	R	**9.4.3 Sistema de gestión de contraseñas** Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar que las contraseñas sean de calidad	La política debería incluir los requisitos para la gestión de claves. La contraseña deberá tener mínimo 9 caracteres y contemplar mayúsculas, minúsculas, números y caracteres especiales.
R78	Eliminación de carpetas importantes, cambio de contraseñas,	12	Alto	R	**9.4.3 Sistema de gestión de contraseñas** Los sistemas de gestión de contraseñas deberían ser	La política debería incluir los requisitos para la gestión de claves. La contraseña deberá tener mínimo 9 caracteres y contemplar mayúsculas, minúsculas, números y caracteres especiales.

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
	quitar privilegios a los usuarios				interactivos y asegurar que las contraseñas sean de calidad	
R79	Eliminación de carpetas importantes, cambio de contraseñas, quitar privilegios a los usuarios	12	Alto	R	**9.4.3 Sistema de gestión de contraseñas** Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar que las contraseñas sean de calidad	La política debería incluir los requisitos para la gestión de claves. La contraseña deberá tener mínimo 9 caracteres y contemplar mayúsculas, minúsculas, números y caracteres especiales.
R6	Destrucción de información, secuestro de datos, suplantación de identidad y filtrado de datos personales	8	Moderado	R	**9.4.1 Restricción de acceso a la información** El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso	controlar los datos que pueden ser accedidos por un usuario en particular; controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicación o sistemas.
R7	Pérdida del equipo por robo.	6	Moderado	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado	Las instalaciones de almacenamiento deberían asegurarse para evitar el acceso no autorizado; las instalaciones de procesamiento de la información que manejan datos sensibles deberían colocarse cuidadosamente para reducir el riesgo de que la información sea vista por personas no autorizadas durante su uso

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
R9	Pérdida de equipos por eventos de fuego	4	Moderado	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	El equipamiento debería situarse de manera que minimice el acceso innecesario a las áreas de trabajo; Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado
R10	Pérdida de equipos por eventos de agua.	6	Moderado	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	El equipamiento debería situarse de manera que minimice el acceso innecesario a las áreas de trabajo; Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado
R11	Lentitud de las operaciones debido a fallas de equipos de cómputo	4	Moderado	T	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	Solo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo
R12	Los documentos pueden ser expuestos en la bandeja de	4	Moderado	R	**13.2.2 Acuerdo sobre transferencia de información** Los acuerdos deberían	Las responsabilidades de gestión para el control y la notificación de transmisión, despacho y recepción; b) los procedimientos para garantizar la trazabilidad y el no repudio;

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
	salida y sustraída por personas no autorizadas				dirigir la transferencia segura de información del negocio entre la organización y partes externas**.**	c) las normas técnicas mínimas para el empaquetado y transporte
R13	Pérdida del equipo por robo.	6	Moderado	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	Las instalaciones de almacenamiento deberían asegurarse para evitar el acceso no autorizado; las instalaciones de procesamiento de la información que manejan datos sensibles deberían colocarse cuidadosamente para reducir el riesgo de que la información sea vista por personas no autorizadas durante su uso
R15	Lentitud de las operaciones de venta debido a fallas de equipos de cómputo	4	Moderado	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo
R17	Ingresos no autorizados	6	Moderado	R	**9.1.1 Política de control de acceso** Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Los propietarios de activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y restricciones para las funciones específicas de los usuarios con respecto a sus activos, con el nivel de detalle y el rigor de los controles que reflejan los riesgos de seguridad de información asociados.

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
R18	Bloqueo de usuario	6	Moderado	R	**9.4.2 Procedimientos de ingreso seguro** Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debería ser controlado por un procedimiento de ingreso seguro.	Se requiera una fuerte autentificación y verificación de identidad, deberían utilizar métodos de autentificación alternativa a las contraseñas, tales como medios de cifrado, tarjetas inteligentes, tokens o medios biométricos.
R21	Bloqueo de usuario	6	Moderado	R	**9.4.2 Procedimientos de ingreso seguro** Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debería ser controlado por un procedimiento de ingreso seguro.	Se requiera una fuerte autentificación y verificación de identidad, deberían utilizar métodos de autentificación alternativa a las contraseñas, tales como medios de cifrado, tarjetas inteligentes, tokens o medios biométricos.
R22	Ingreso a la red y ejecución de servicios no autorizados en los puestos de red.	8	Moderado	R	**13.1.2 Seguridad de servicios de red** Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deberían ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se	Las medidas de seguridad necesarias para los servicios particulares, tales como características de seguridad, niveles de servicio y los requisitos de gestión, deberían estar identificadas. La organización debería asegurarse que los proveedores de los servicios de red implementen estas medidas.

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
					provean internamente o sean tercerizados	
R23	Pérdida de la conexión la red LAN	8	Moderado	T	**13.1.3 Segregación en redes** Grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes.	El perímetro de cada dominio debería estar bien definido. Se permite el acceso entre dominios de la red, pero debería ser controlado en el perímetro utilizando una puerta de enlace (por ejemplo, cortafuegos, router con capacidad de filtrado).
R25	Pérdida de la conexión de la red WAN	8	Moderado	T	**13.1.3 Segregación en redes** Grupos de servicios de información, usuarios y sistemas de información deberían estar segregados en redes.	El perímetro de cada dominio debería estar bien definido. Se permite el acceso entre dominios de la red, pero debería ser controlado en el perímetro utilizando una puerta de enlace (por ejemplo, cortafuegos, router con capacidad de filtrado).
R26	Deterioro del equipo e infraestructura de comunicación	6	Moderado	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo
R27	Pérdida del equipo por robo.	6	Moderado	R	**11.2.1 Ubicación y protección de los equipos** Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	Las instalaciones de almacenamiento deberían asegurarse para evitar el acceso no autorizado; las instalaciones de procesamiento de la información que manejan datos sensibles deberían colocarse cuidadosamente para reducir el riesgo de que la información sea vista por personas no autorizadas durante su uso

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
R33	Fallas de operación del equipo.	5	Moderado	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo
R34	Interrupción del sistema y lentitud de las operaciones	4	Moderado	R	**11.2.4 Mantenimiento de equipos** Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos; se debería mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo
R39	Pérdida de integridad de datos	6	Moderado	R	**12.3.1 Respaldo de la información** Copias de respaldo de la información, del software y de las imágenes del sistema deberían ser realizadas y verificadas regularmente en concordancia con una política de respaldo acordada.	Debería establecerse una política de respaldo para definir los requisitos de la organización para los respaldos de la información, software y sistemas. La política de respaldo debería definir los requisitos de retención y protección. Deberían proporcionarse instalaciones adecuadas de respaldo para garantizar que toda la información y software esenciales se pueden recuperar después de un desastre o falla de medios
R45	Mal funcionamiento del software por pruebas al software inexistentes o	8	Moderado	A	**14.2.2 Procedimientos de control de cambio del sistema** Cambios a los sistemas dentro del ciclo de vida del	Para garantizar la integridad del sistema, las aplicaciones y los productos, desde las primeras etapas de diseño y a través de todos los esfuerzos de mantenimiento posteriores, deberían documentarse y hacerse cumplir los procedimientos formales de control de

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
	insuficientes				desarrollo deberían estar controlados por medio del uso de procedimientos formales de control de cambios.	cambio.
R48	Mal funcionamiento del software por parche no instalado correctamente	8	Moderado	R	**12.6.2 Restricciones sobre la instalación de software** Reglas que gobiernen la instalación de software por parte de los usuarios deberían ser establecidas e implementadas.	La organización debería definir y hacer cumplir una política estricta sobre qué tipos de software pueden instalar los usuarios.
R51	Robo de información, modificación de documentos	8	Moderado	R	**9.4.1 Restricción de acceso a la información** El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso.	Controlar los datos que pueden ser accedidos por un usuario en particular; controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos de aplicación o sistemas.
R53	Fuga de información por falta de procedimientos sobre la gestión de incidentes de seguridad de información	8	Moderado	R	**9.4.1 Restricción de acceso a la información** El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la	Controlar los datos que pueden ser accedidos por un usuario en particular; controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, borrar y ejecutar; controlar los derechos de acceso de otras aplicaciones; limitar la información contenida en las salidas; proporcionar controles de acceso físicos o lógicos para el aislamiento de

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
					política de control de acceso.	aplicaciones sensibles, datos de aplicación o sistemas.
R55	Hackeo o robo de la cuenta para venderlo a terceros	6	Moderado	R	**12.2.1 Controles contra software malicioso (malware)** Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concienciación apropiada de los usuarios.	La protección contra software malicioso debería basarse en el empleo de software de detección de código malicioso y reparación, en la creación de conciencia de la seguridad de información y en apropiados controles de acceso al sistema y gestión de cambios
R59	Ingreso a la red y ejecución de servicios no autorizados en los puestos de red.	6	Moderado	R	**13.1.1 Controles de la red** Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	las responsabilidades y procedimientos para la gestión de equipos de red debería estar establecida; la responsabilidad operacional de las redes debería separarse de las operaciones de cómputo donde sea apropiado; deberían establecerse controles especiales para resguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas o sobre las redes inalámbricas y para proteger los sistemas conectados y aplicaciones; controles especiales también pueden ser necesarios para mantener la disponibilidad de los servicios de red y computadoras conectadas; los sistemas en la

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
						red deberían estar autenticados; la conexión de sistemas a la red debería ser restringida
R71	Pérdida de información por falta de copias de respaldo	6	Moderado	R	**12.3.1 Respaldo de la información** Copias de respaldo de la información, del software y de las imágenes del sistema deberían ser realizadas y verificadas regularmente en concordancia con una política de respaldo acordada.	Debería establecerse una política de respaldo para definir los requisitos de la organización para los respaldos de la información, software y sistemas. La política de respaldo debería definir los requisitos de retención y protección. Deberían proporcionarse instalaciones adecuadas de respaldo para garantizar que toda la información y software esenciales se pueden recuperar después de un desastre o falla de medios.
R74	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	6	Moderado	R	**6.1.1 Roles y responsabilidades para la seguridad de la información** Todas las responsabilidades de seguridad de la información deberían definirse y asignarse.	La asignación de las responsabilidades de seguridad de la información debería hacerse de acuerdo con las políticas de seguridad de la información, Deberían definirse las responsabilidades de las actividades de gestión de riesgos de seguridad de la información y en particular, para la aceptación de riesgos residuales.
R75	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	6	Moderado	R	**6.1.1 Roles y responsabilidades para la seguridad de la información** Todas las responsabilidades de	La asignación de las responsabilidades de seguridad de la información debería hacerse de acuerdo con las políticas de seguridad de la información, Deberían definirse las responsabilidades de las actividades de gestión de riesgos de seguridad de la

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
					seguridad de la información deberían definirse y asignarse.	información y en particular, para la aceptación de riesgos residuales.
R76	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	6	Moderado	R	**6.1.1 Roles y responsabilidades para la seguridad de la información** Todas las responsabilidades de seguridad de la información deberían definirse y asignarse.	La asignación de las responsabilidades de seguridad de la información debería hacerse de acuerdo con las políticas de seguridad de la información, Deberían definirse las responsabilidades de las actividades de gestión de riesgos de seguridad de la información y en particular, para la aceptación de riesgos residuales.
R77	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	6	Moderado	R	**6.1.1 Roles y responsabilidades para la seguridad de la información** Todas las responsabilidades de seguridad de la información deberían definirse y asignarse.	La asignación de las responsabilidades de seguridad de la información debería hacerse de acuerdo con las políticas de seguridad de la información, Deberían definirse las responsabilidades de las actividades de gestión de riesgos de seguridad de la información y en particular, para la aceptación de riesgos residuales.
R80	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	6	Moderado	R	**6.1.1 Roles y responsabilidades para la seguridad de la información** Todas las responsabilidades de seguridad de la información deberían	La asignación de las responsabilidades de seguridad de la información debería hacerse de acuerdo con las políticas de seguridad de la información, Deberían definirse las responsabilidades de las actividades de gestión de riesgos de seguridad de la información y en particular, para la aceptación de riesgos

Código	Riesgo	Evaluación del riesgo	Categoría	Opción de tratamiento	Control	Procedimiento de implementación ISO 27002
					definirse y asignarse.	residuales.
R81	Poco compromiso con la seguridad de la información por capacitación de seguridad insuficiente	6	Moderado	R	**6.1.1 Roles y responsabilidades para la seguridad de la información** Todas las responsabilidades de seguridad de la información deberían definirse y asignarse.	La asignación de las responsabilidades de seguridad de la información debería hacerse de acuerdo con las políticas de seguridad de la información, Deberían definirse las responsabilidades de las actividades de gestión de riesgos de seguridad de la información y en particular, para la aceptación de riesgos residuales.

Tabla 23.- Tratamiento del riesgo

Fuente: Elaboración Propia

5.6 Verificar

En este punto se realiza una auditoría o revisión por las partes involucradas posterior a la implementación del SGSI, fase no abarcada en la tesis por ser una fase posterior al diseño del SGSI. También se integran en esta fase el monitoreo y seguimiento de los objetivos planteados en la fase de alcance.

5.7 Actuar

En esta última etapa de toma de acciones, la clínica decide las acciones de corrección y prevención que se deben optar, o bien la adopción de acuerdos basados en los análisis hechos. Asimismo, la realización la mejora continua sobre la seguridad de la información en la Clínica IPC Salud.

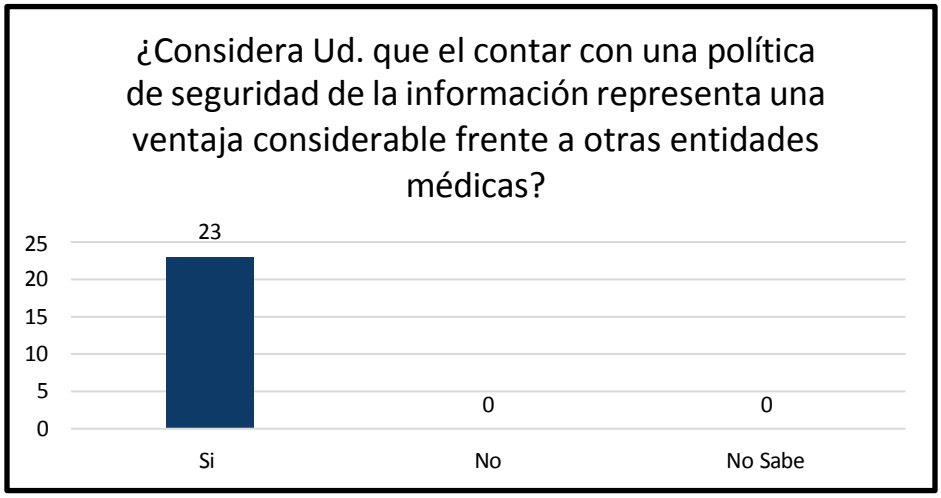
Capítulo

6. Resultados

Luego de aplicar los instrumentos de recolección de datos a los trabajadores de la clínica los resultados obtenidos por cada ítem encuestado fue el siguiente:

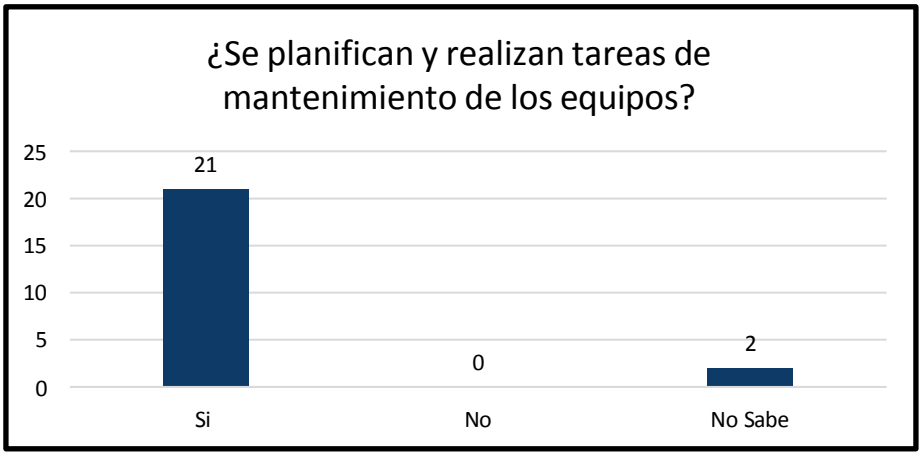
DIMENSIÓN: <u>Planificar</u>
INDICADOR: Actividades operativas de planificación

1.- ¿Considera Ud. que el contar con una política de seguridad de la información representa una ventaja considerable frente a otras entidades médicas?



Según el gráfico mostrado, 23 encuestados indicaron que las políticas de seguridad de información sí son una ventaja, con lo cual la empresa proyecta más seguridad en el tratamiento de los datos en comparación a otras entidades del mismo rubro.

2.- ¿Se planifican y realizan tareas de mantenimiento de los equipos?

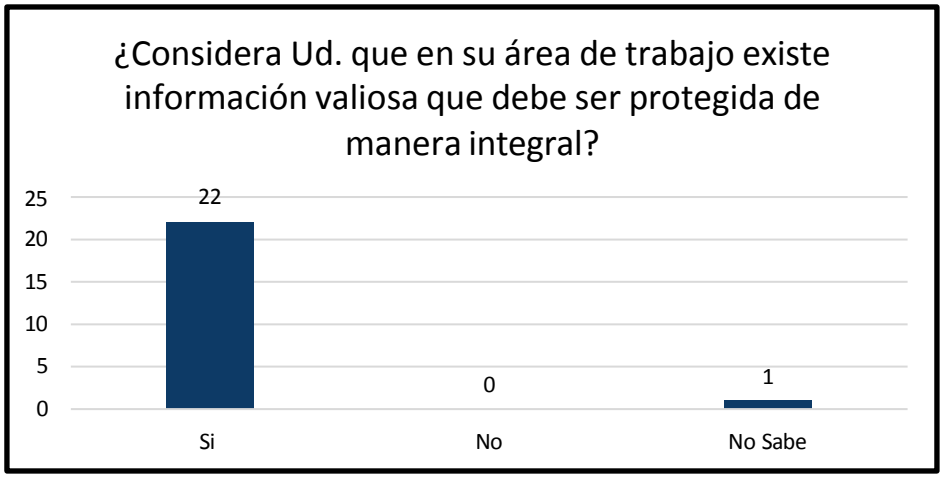


Para esta pregunta 21 trabajadores indicaron que sí se realizan tareas de mantenimiento en los

equipos, mientras que 2 trabajadores desconocen sobre estos mantenimientos.

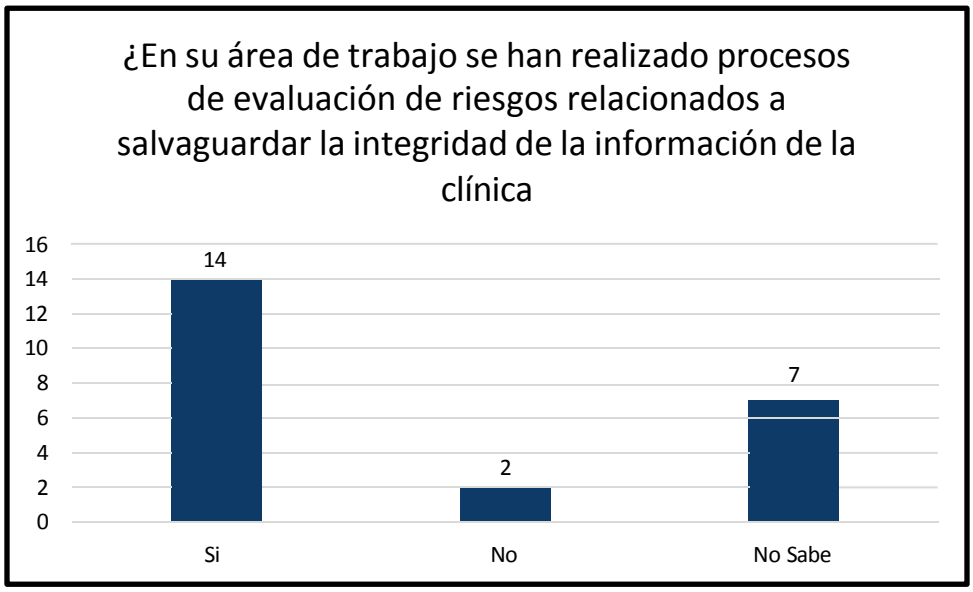
DIMENSIÓN: <u>Hacer</u>
INDICADOR: N° de actividades de seguridad ejecutadas

3.- ¿Considera Ud. que en su área de trabajo existe información valiosa que debe ser protegida de manera integral?



22 trabajadores indicaron que sí existía información importante que debía ser protegida en la Clínica, mientras que uno manifestó que desconocía la existencia de esta información.

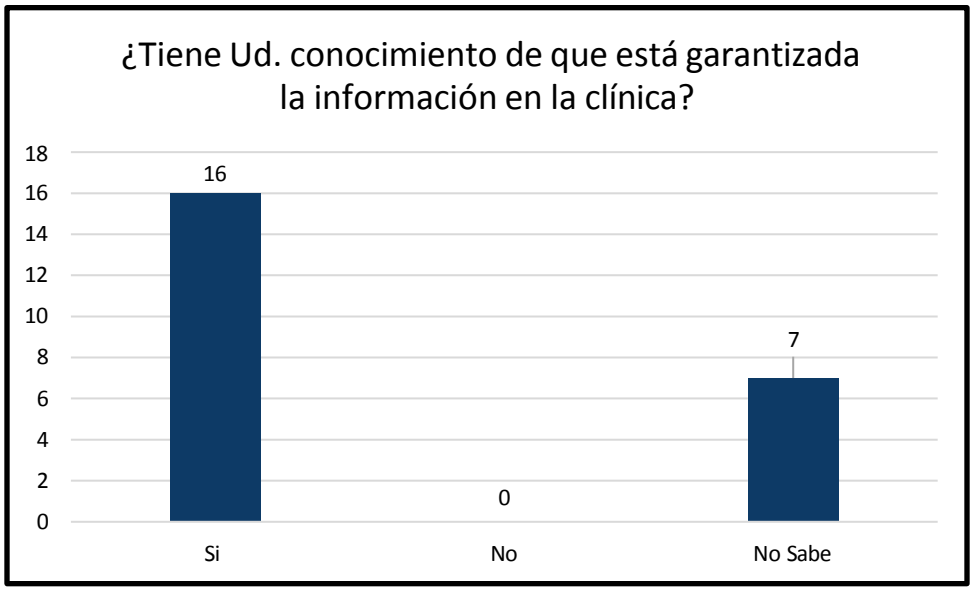
4.- ¿En su área de trabajo se han realizado procesos de evaluación de riesgos relacionados a salvaguardar la integridad de la información de la clínica?



Según el gráfico 14 encuestados indicaron que, si se han realizado evaluaciones de riesgos respecto a la integridad de información, 2 encuestados manifestaron que no se han realizado estas evaluaciones, mientras que 7 encuestados indicaron que desconocían sobre estas evaluaciones.

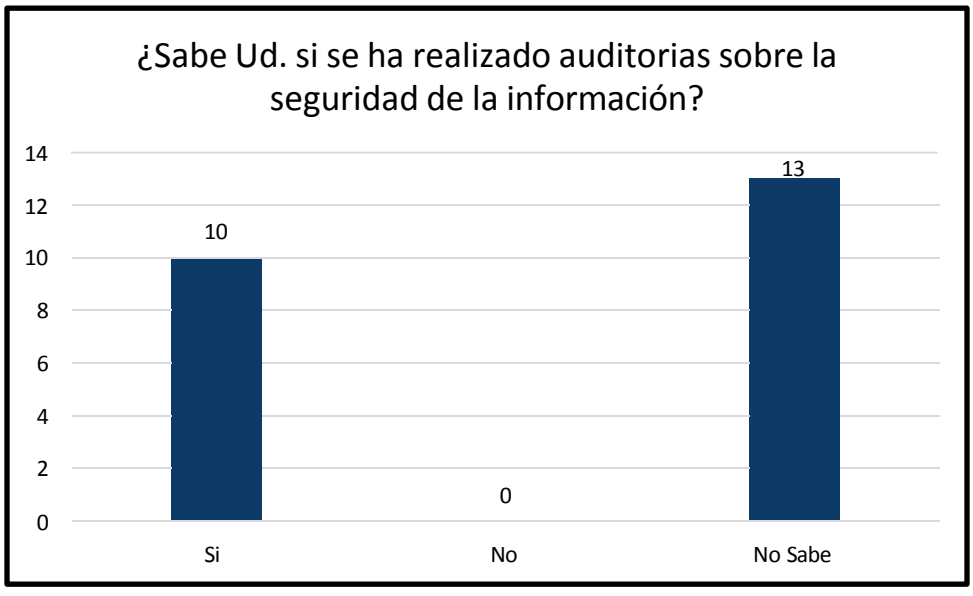
DIMENSIÓN: <u>Verificar</u>
INDICADOR: Revisión de las actividades planificadas y ejecutadas

5.-¿Tiene Ud. conocimiento de que está garantizada la información en la clínica?



Para este ítem 16 trabajadores indicaron que sí está garantizada la información en la clínica, mientras que 7 trabajadores no saben sobre este tema.

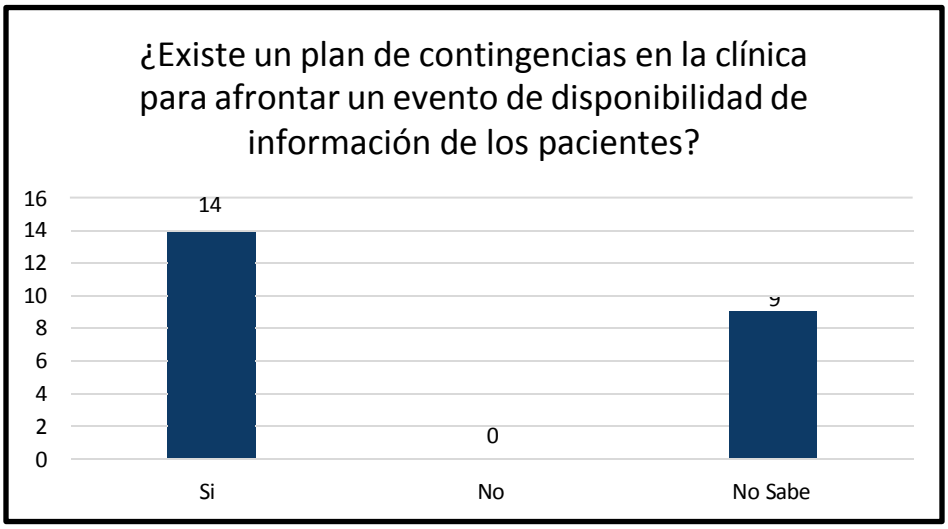
6.- ¿Sabe Ud. si se ha realizado auditorías sobre la seguridad de la información?



Para esta pregunta 10 encuestados manifestaron que sí se ha realizado auditorías de seguridad de información en la clínica, mientras que 13 desconocían que se haya realizado esta auditoría

DIMENSIÓN: <u>Actuar</u>
INDICADOR: Análisis de la mejora de la seguridad

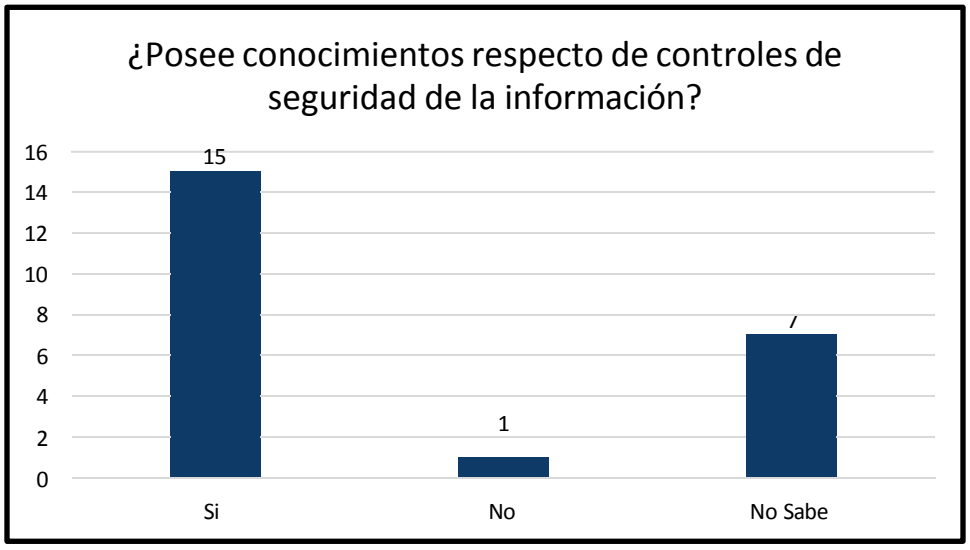
7.- ¿Existe un plan de contingencias en la clínica para afrontar un evento de disponibilidad de información de los pacientes?



Para esta pregunta 14 trabajadores indicaron que sí existe un plan de contingencia en la clínica, mientras que 9 trabajadores desconocían sobre estas medidas llevadas a cabo por la empresa.

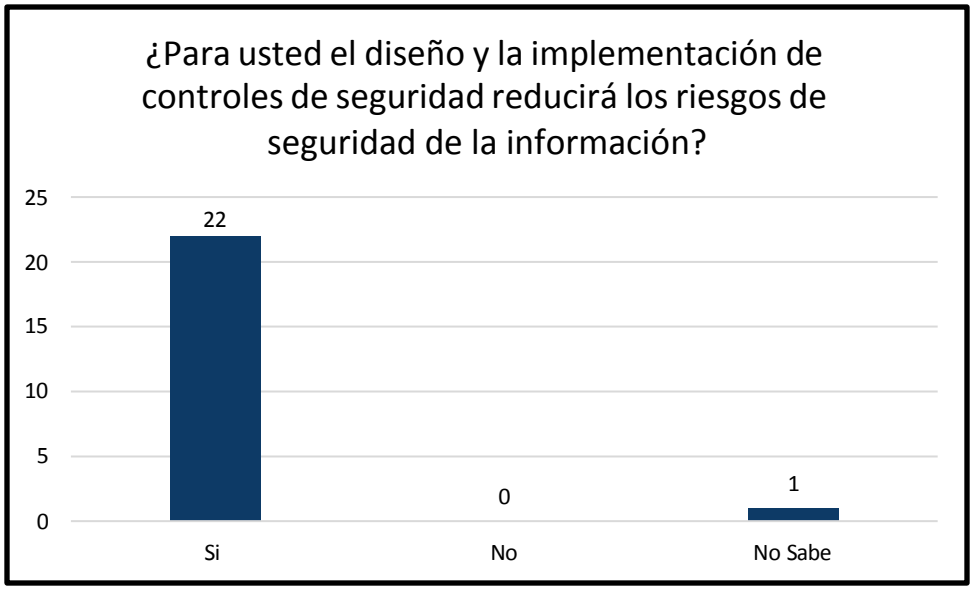
DIMENSIÓN: <u>Protección de los Datos Personales</u>
INDICADOR: Controles de seguridad de la información

8.- ¿Posee conocimientos respecto de controles de seguridad de la información?



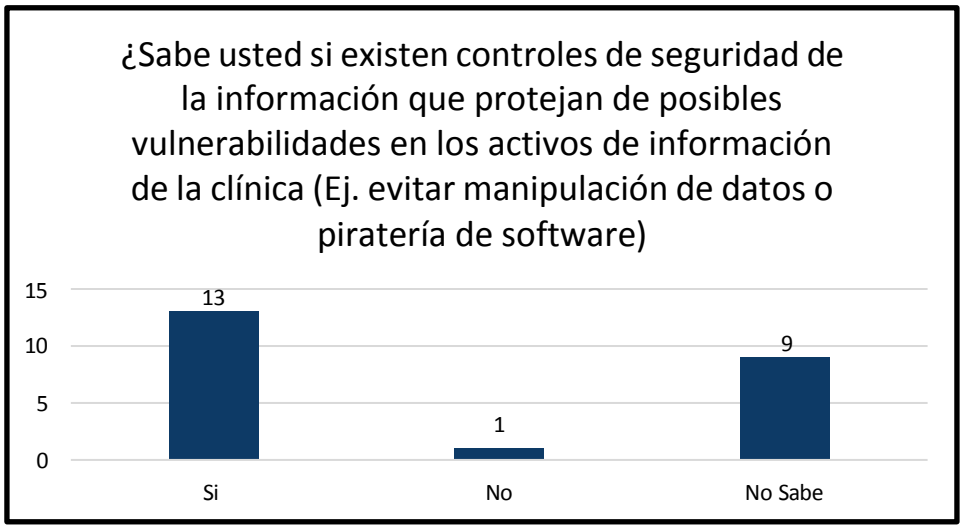
Para este ítem 15 encuestados indicaron que sí tenían conocimientos sobre controles de seguridad de información, uno indicó que no tiene conocimientos sobre los controles y 7 manifestaron que no sabían sobre este tema.

9.- ¿Para usted el diseño y la implementación de controles de seguridad reducirá los riesgos de seguridad de la información?



22 encuestados indicaron que la implementación de controles de seguridad de información ayudaría con la reducción de los riesgos de seguridad de información, mientras que uno indicó que desconocía sobre este tema.

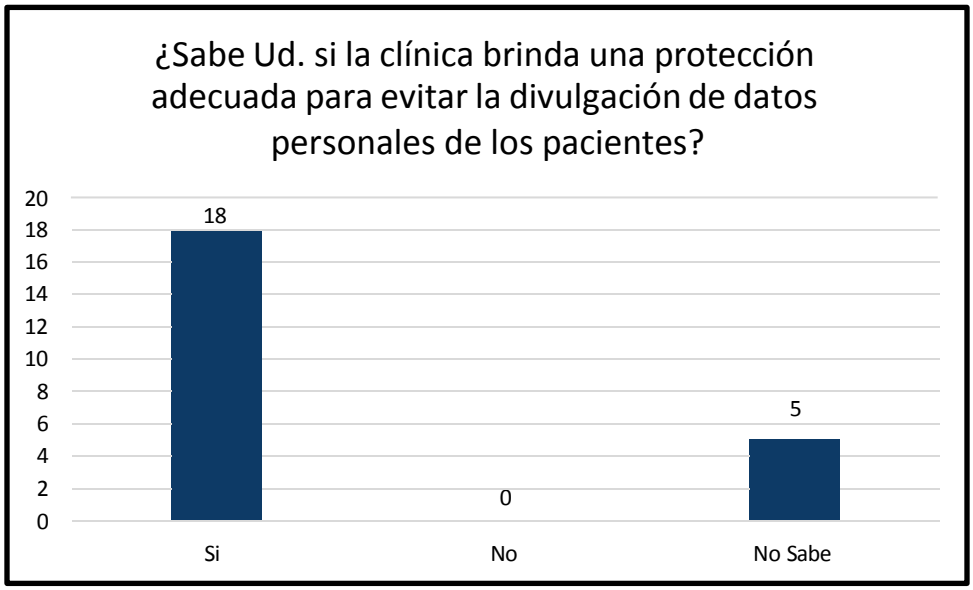
10.- ¿Sabe usted si existen controles de seguridad de la información que protejan de posibles vulnerabilidades en los activos de información de la clínica (Ej. evitar manipulación de datos o piratería de software)



Para esta pregunta, 13 trabajadores indicaron que sí existen controles de seguridad de información que protegen los activos de la clínica, 1 indicó que no existía estos controles y 9 desconocían que en la empresa existiera estos tipos de controles.

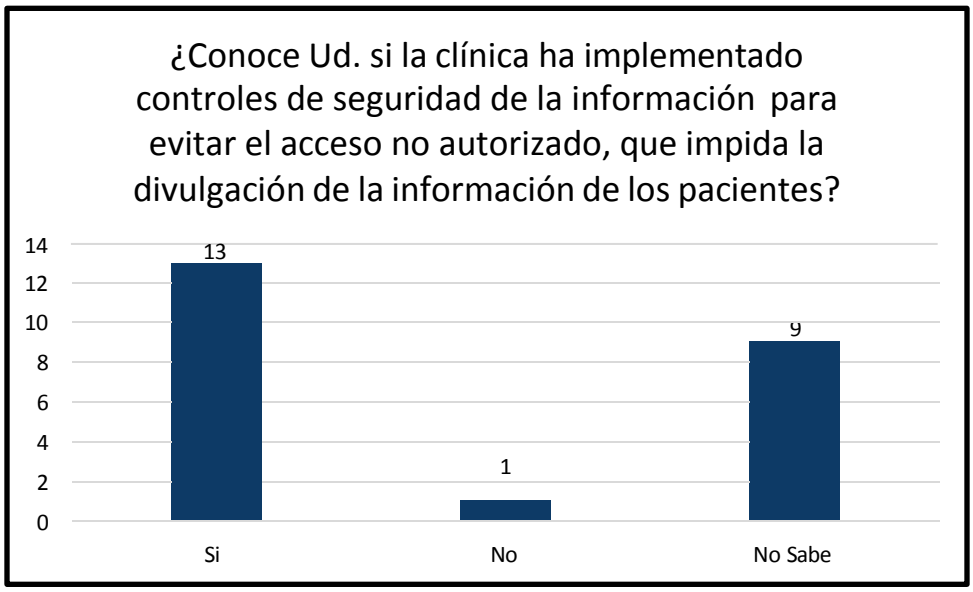
DIMENSIÓN: **Aseguramiento de los Activos de Información**
INDICADOR: Confidencialidad

11.- ¿Sabe Ud. si la clínica brinda una protección adecuada para evitar la divulgación de datos personales de los pacientes?



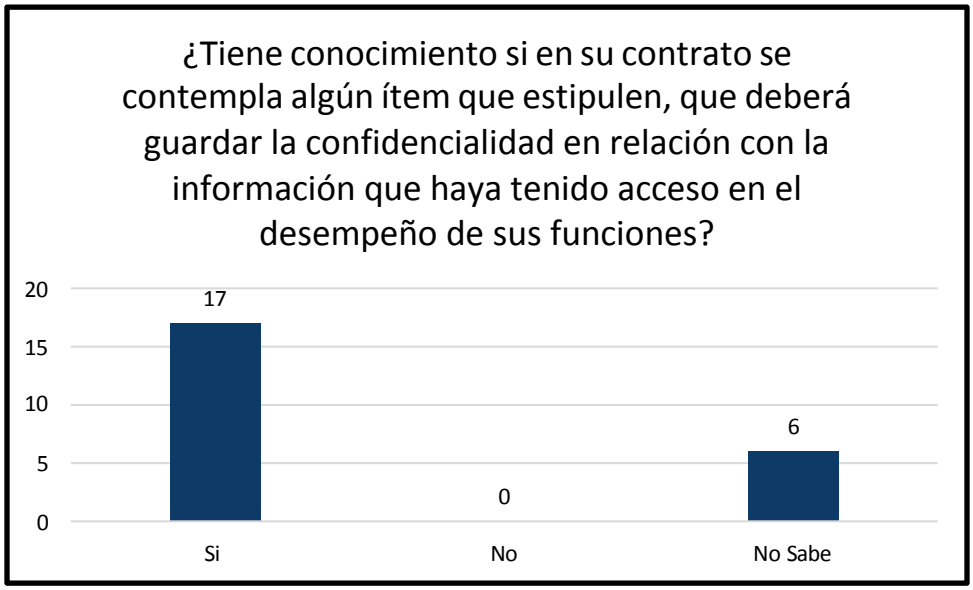
18 encuestados indicaron que la clínica sí brinda una protección oportuna contra la divulgación de datos personales, 5 manifestaron que no sabían sobre esta protección.

12.- ¿Conoce Ud. si la clínica ha implementado controles de seguridad de la información para evitar el acceso no autorizado, que impida la divulgación de la información de los pacientes?



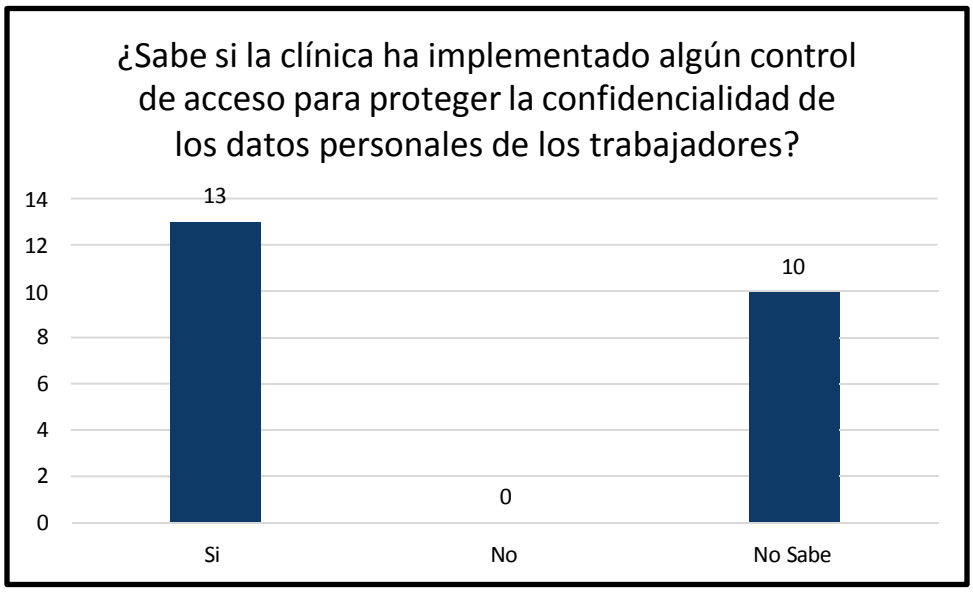
Para esta pregunta el resultado obtenido fue que 13 trabajadores indicaron que sí se han implementado controles contra el acceso no autorizado, 1 indicó que no habían implementado estos controles, mientras que 9 no sabían sobre la implementación de estos controles.

13.- ¿Tiene conocimiento si en su contrato se contempla algún ítem que estipula, que deberá guardar la confidencialidad, en relación con la información que haya tenido acceso en el desempeño de sus funciones?



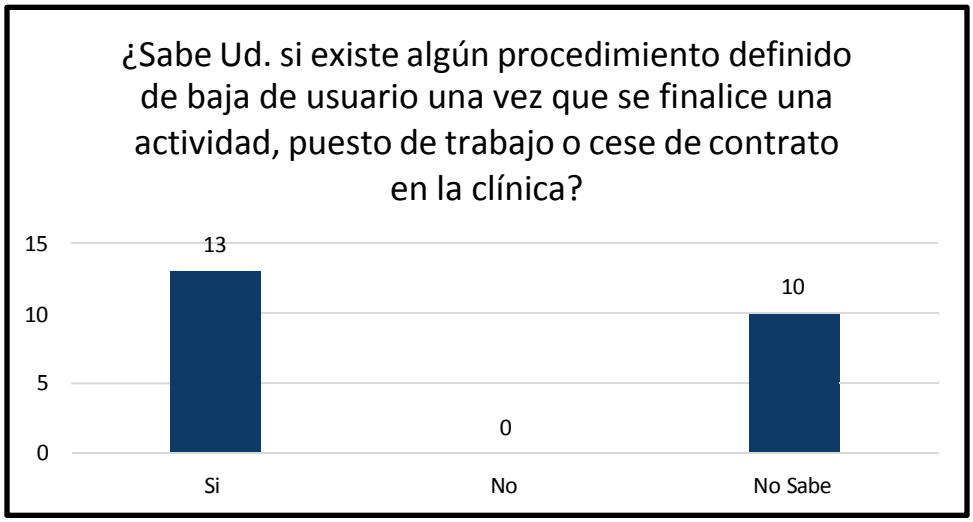
El resultado para esta pregunta fue que 17 trabajadores indicaron que en su contrato sí existe un ítem sobre la protección de los datos personales sobre los clientes, mientras que 6 trabajadores indicaron que no sabían o no se dieron cuenta si existía este ítem sobre la protección de datos.

14.- ¿Sabe si la clínica ha implementado algún control de acceso para proteger la confidencialidad de los datos personales de los trabajadores?



13 encuestados manifestaron que sí se ha implementado controles sobre la confidencialidad de datos personales sobre los trabajadores, 10 indicó que no sabían sobre la implementación de estos controles en la clínica.

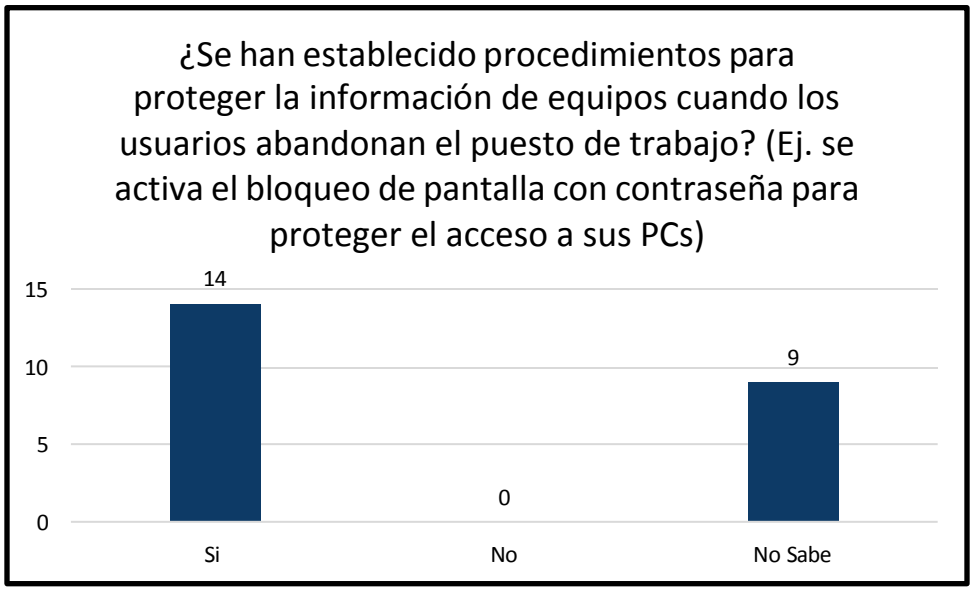
15.- ¿Sabe Ud. si existe algún procedimiento definido de baja de usuario una vez que se finalice una actividad, puesto de trabajo o cese de contrato en la clínica?



Para esta pregunta 13 encuestados indicaron que sí existe un procedimiento para baja de usuarios, mientras que 10 indicaron que no sabían sobre este procedimiento.

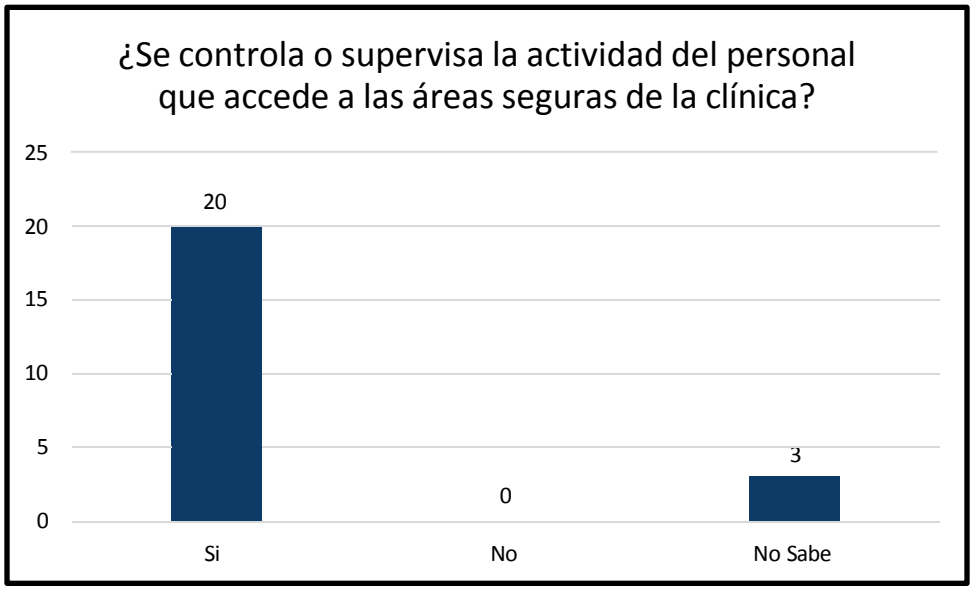
DIMENSIÓN: **<u>Aseguramiento de los Activos de Información</u>**
INDICADOR: Integridad

16.- ¿Se han establecido procedimientos para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo? (Ej. se activa el bloqueo de pantalla con contraseña para proteger el acceso a sus PCs)



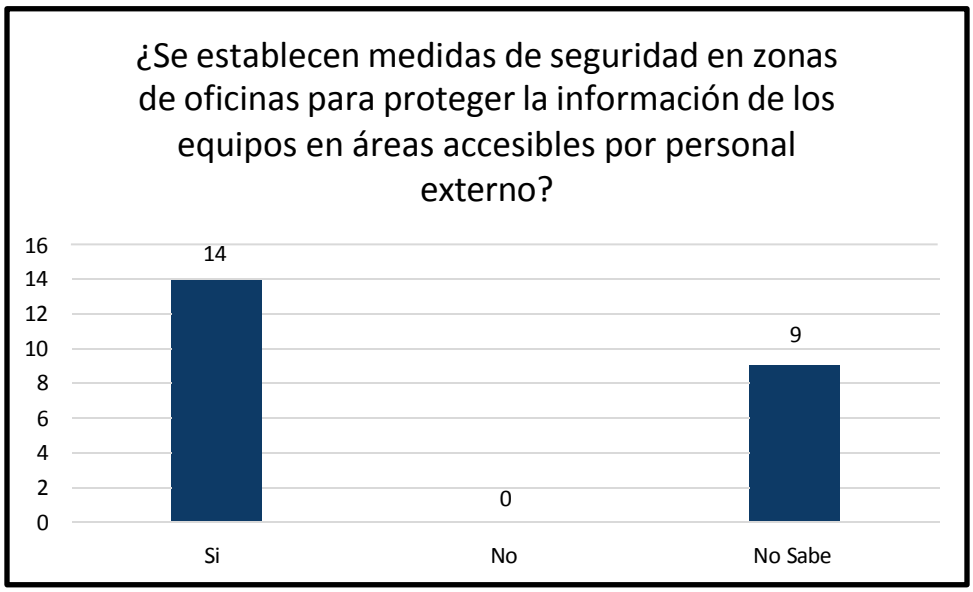
Para este ítem, 14 encuestados indicaron que sí se usan procedimientos para la protección de datos cuando los usuarios se encuentran fuera de su puesto de trabajo, mientras que 9 indicaron que no tenían conocimientos de estos procedimientos.

17.- ¿Se controla o supervisa la actividad del personal que accede a las áreas seguras de la clínica?



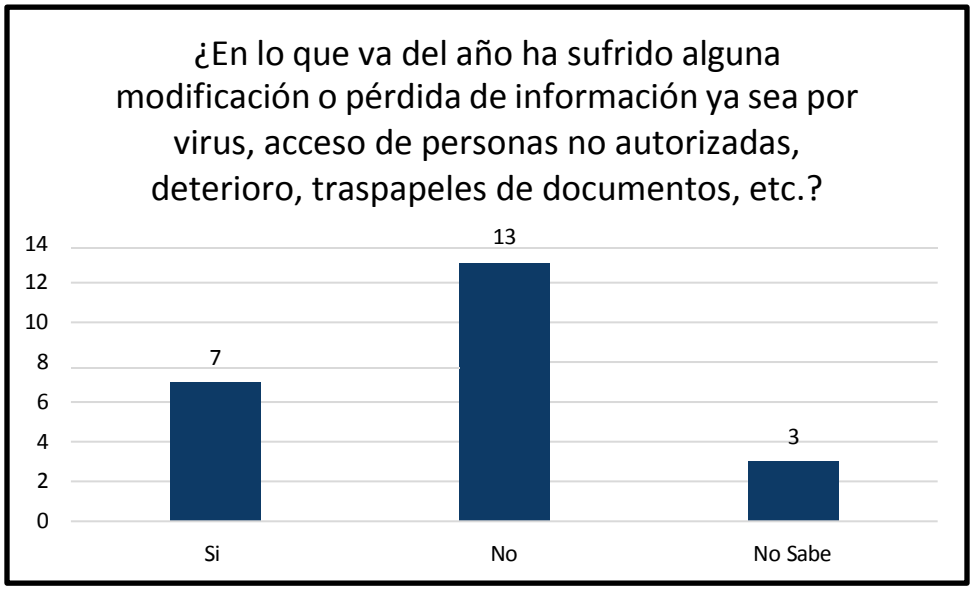
En esta pregunta, 20 entrevistados manifestaron que sí se supervisa las actividades de los trabajadores dentro de las áreas, 3 indicaron que no saben sobre estas supervisiones.

18.- ¿Se establecen medidas de seguridad en zonas de oficinas para proteger la información de los equipos en áreas accesibles por personal externo?



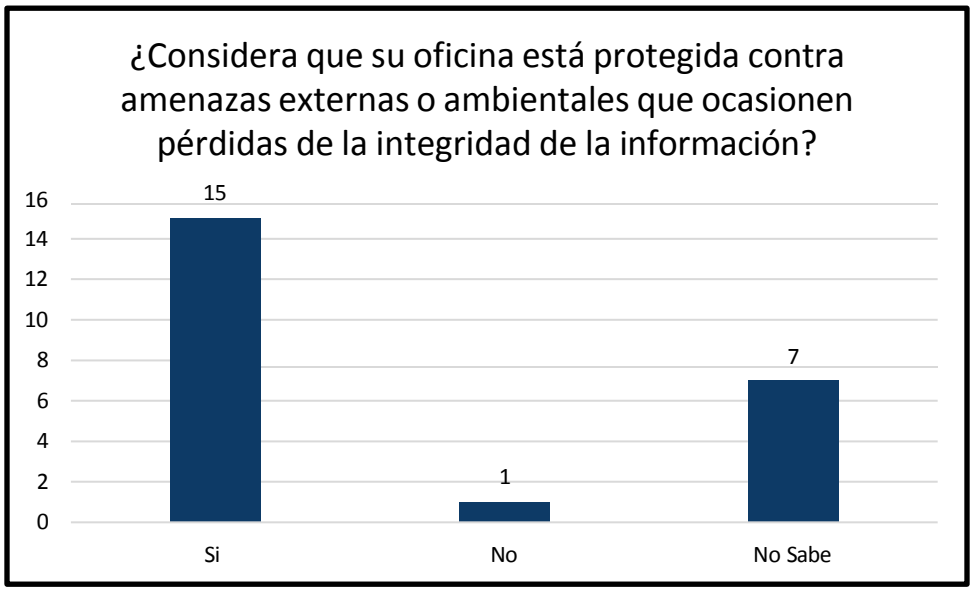
Para esta pregunta, 14 entrevistados indicaron que sí han usado medidas de protección de equipos para el personal externo, mientras que 9 indicaron que no sabían sobre estas medidas realizadas por la clínica.

19.- ¿En lo que va del año ha sufrido alguna modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, traspapeles de documentos, etc.?



Para este ítem 7 encuestados indicaron que sí han sufrido algún percance con pérdida de información o un ataque informático, 13 indicaron que no han tenido ningún problema respecto a la pérdida de datos, mientras que 3 manifestaron que no sabían sobre estos hechos.

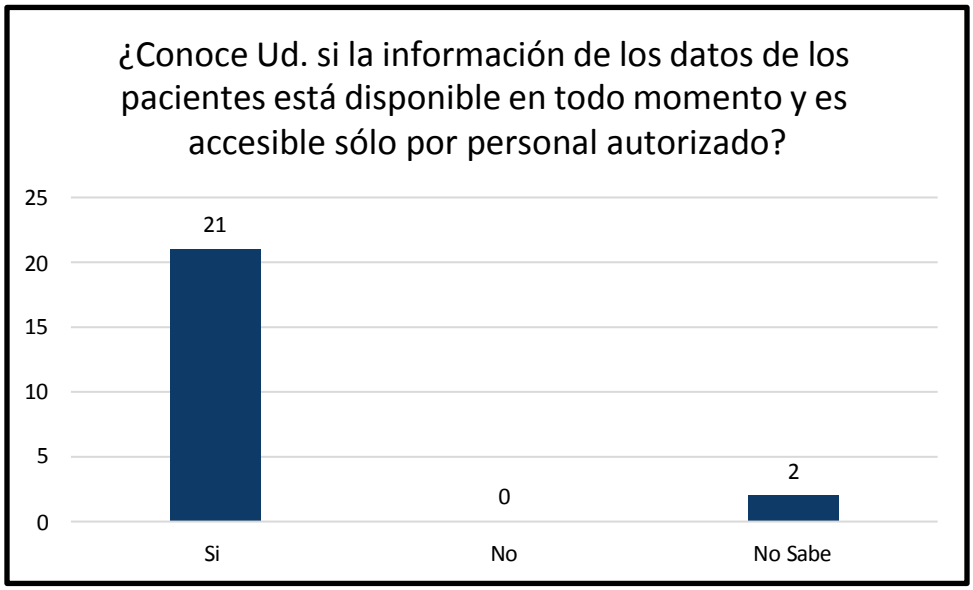
20.- ¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionen pérdidas de la integridad de la información?



En esta pregunta, 15 encuestados consideraron que su oficina sí está protegida contra amenazas externas contra la pérdida de información, 1 consideró que no está protegida y 7 indicaron que no sabían.

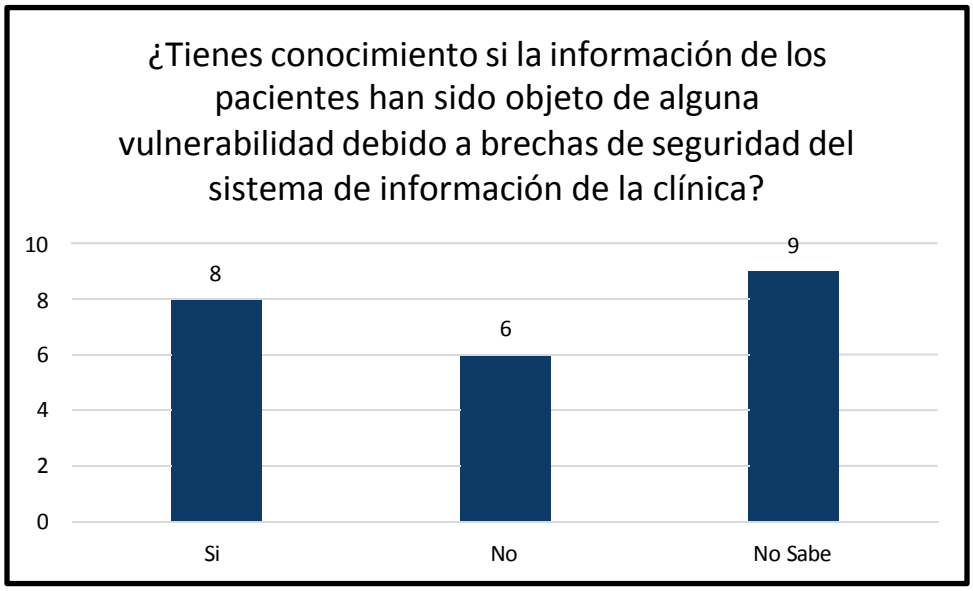
DIMENSIÓN: **Aseguramiento de los Activos de Información**
INDICADOR: Disponibilidad

21.- ¿Conoce Ud. si la información de los datos de los pacientes está disponible en todo momento y es accesible sólo por personal autorizado?



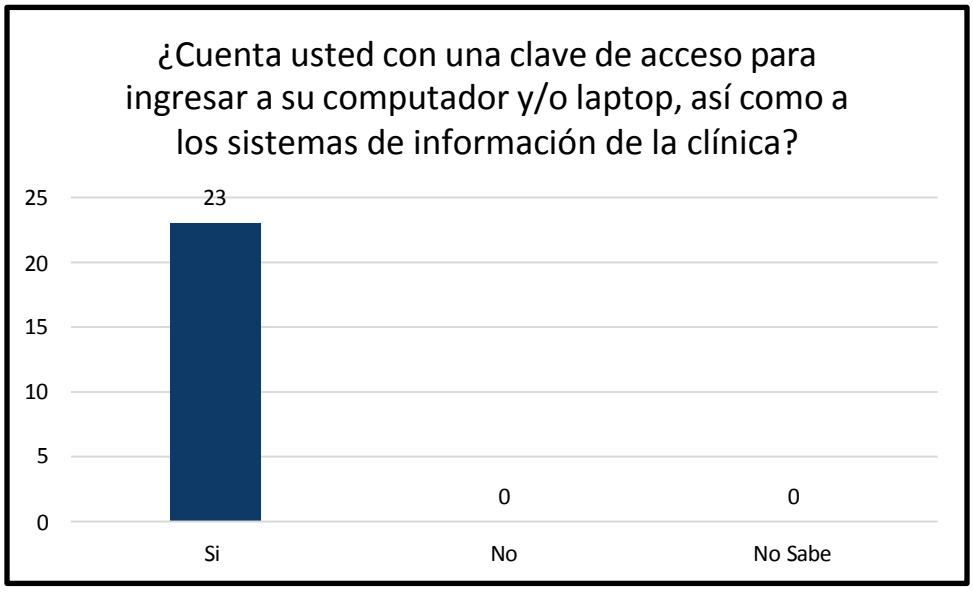
Para este ítem, 21 encuestados indicaron que la información de los pacientes sí está disponible en todo momento para el personal y 2 manifestaron que no sabían sobre la disponibilidad de los datos

22.- ¿Tienes conocimiento si la información de los pacientes han sido objeto de alguna vulnerabilidad debido a brechas de seguridad del sistema de información de la clínica?



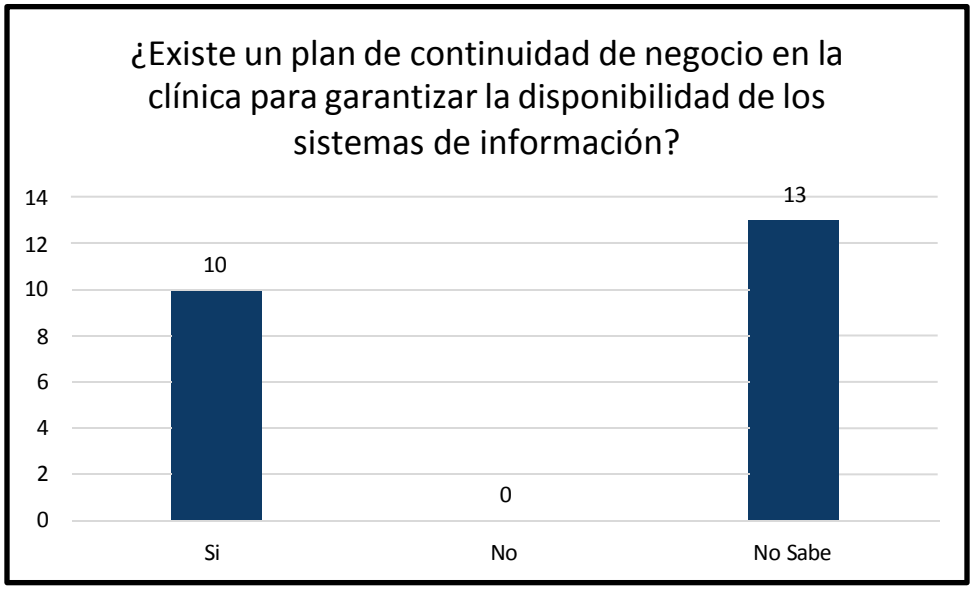
Según el gráfico, 8 encuestados opinaron que los datos de los pacientes sí han sufrido alguna vulnerabilidad, 6 indicaron que los datos no han sido afectados por algún riesgo informático y 9 manifestaron que no sabían si ha ocurrido algún problema con los datos de los pacientes.

23.- ¿Cuenta usted con una clave de acceso para ingresar a su computador y/o laptop, así como a los sistemas de información de la clínica?



Según el gráfico, se puede apreciar que 23 encuestados sí tienen una clave de acceso para el ingreso a su computador y/o laptop.

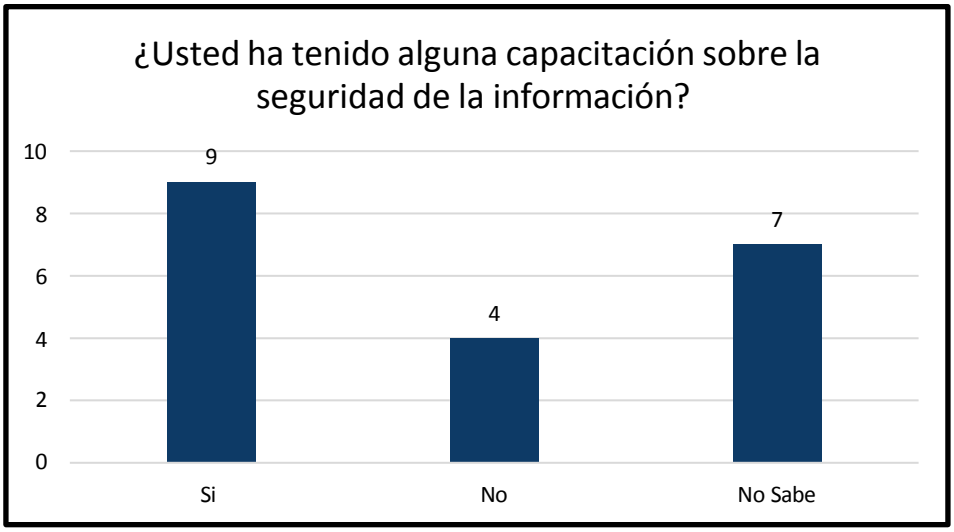
24.- ¿Existe un plan de continuidad de negocio en la clínica para garantizar la disponibilidad de los sistemas de información?



Según el gráfico mostrado, 10 encuestados indicaron que hay un plan de continuidad que garantice la disponibilidad de los sistemas de información, 13 no saben si existe algún plan de continuidad por parte de la clínica.

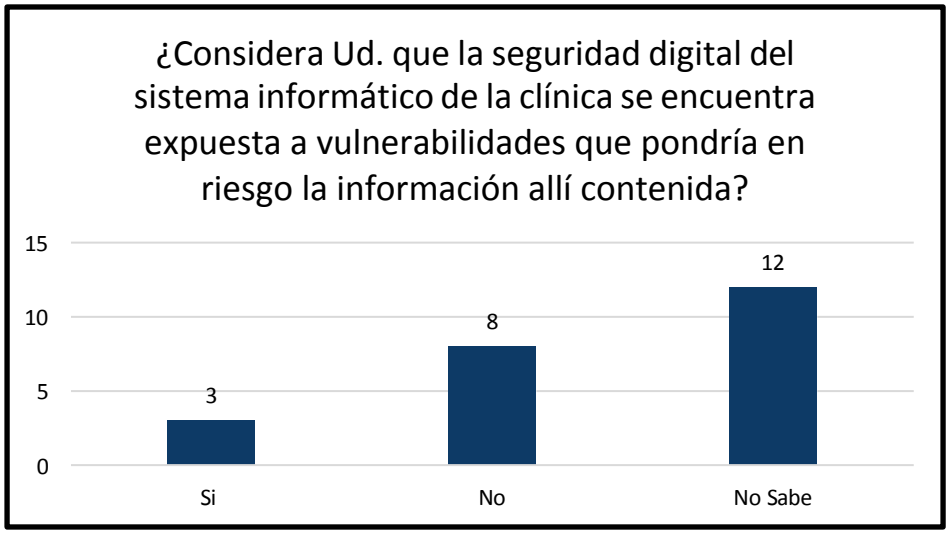
DIMENSIÓN: **Nivel de percepción**
INDICADOR: Nivel de percepción de los trabajadores sobre la seguridad de la información

25.- ¿Usted ha tenido alguna capacitación sobre la seguridad de la información?



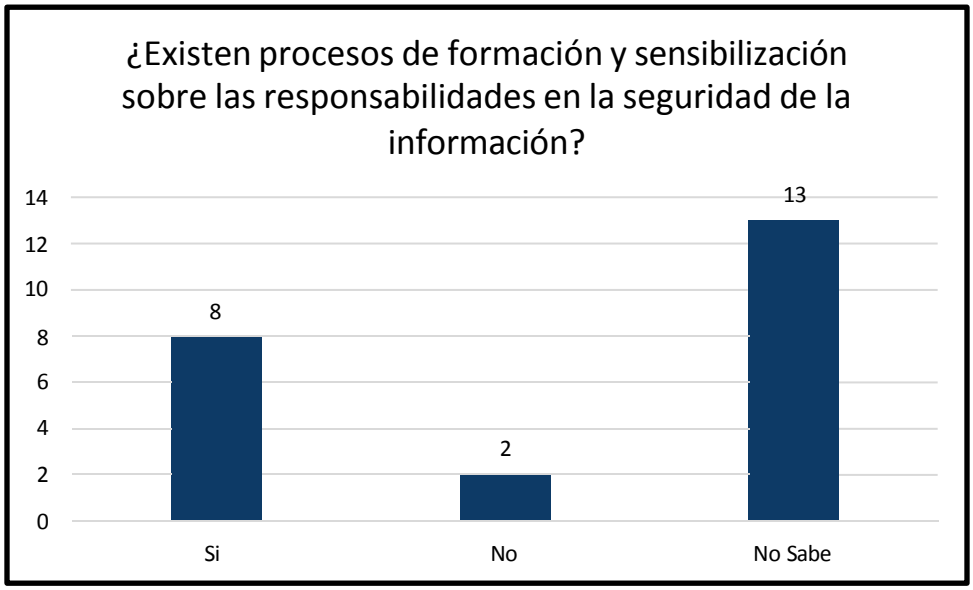
Para este ítem, 9 encuestados sí han tenido una capacitación sobre la seguridad de la información, 4 no han tenido estas capacitaciones y 7 no sabían si ha tenido alguna capacitación respecto a la seguridad de la información.

26.- ¿Considera Ud. que la seguridad digital del sistema informático de la clínica se encuentra expuesta a vulnerabilidades que pondría en riesgo la información allí contenida?



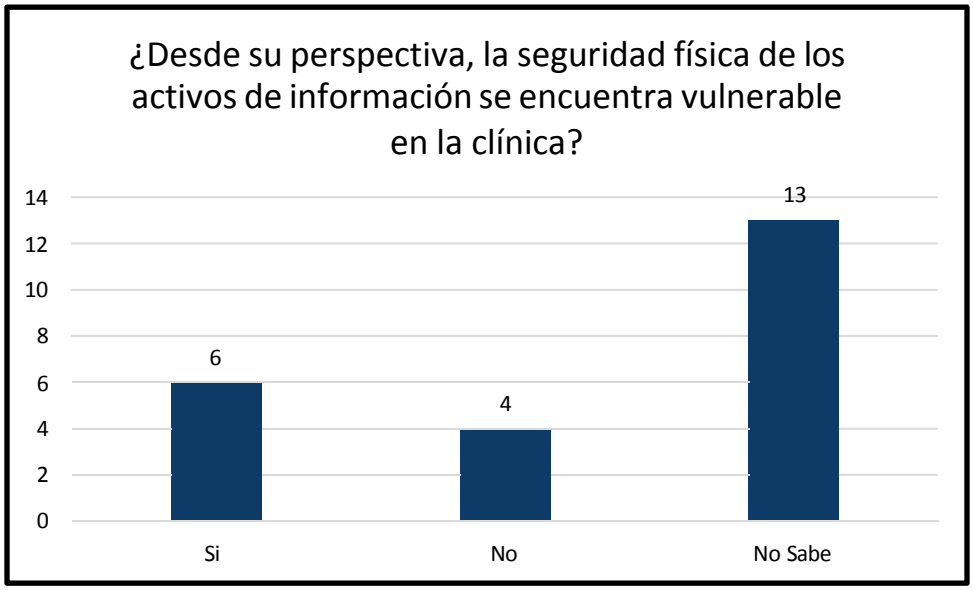
Según el gráfico, 3 encuestados manifestaron que la seguridad digital sí se encuentra expuesta a vulnerabilidades, 8 opinaron que no se encuentra expuesta y 12 no saben si la seguridad digital de la clínica se encuentra vulnerable.

27.- ¿Existen procesos de formación y sensibilización sobre las responsabilidades en la seguridad de la información?



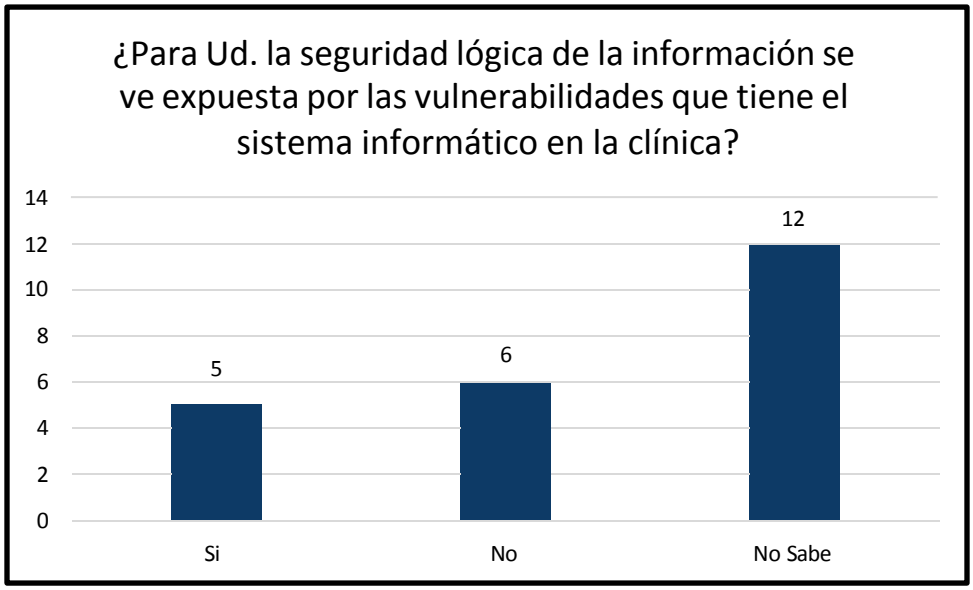
Según el gráfico, se puede observar que 8 encuestados indicaron que sí hay una sensibilización sobre la responsabilidad en la seguridad de la información, 2 manifestaron que no existe una sensibilización y 13 desconocían sobre este proceso.

28.- ¿Desde su perspectiva, la seguridad física de los activos de información se encuentra vulnerable en la clínica?



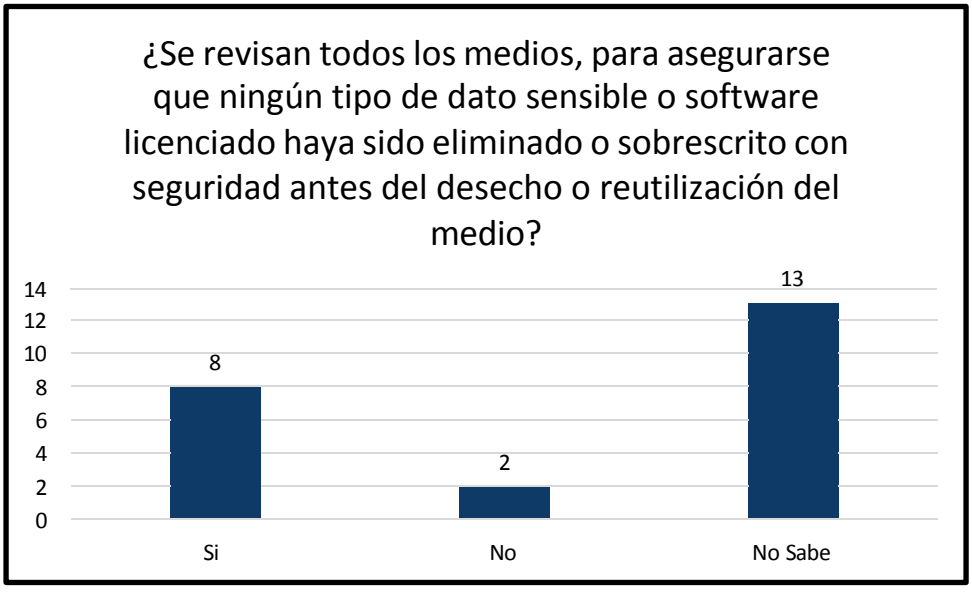
Para este ítem, 6 de los encuestados afirman que la seguridad física de los activos sí se encuentra vulnerable frente a un riesgo, 4 indicaron que no se encontraba vulnerable y 13 no sabían estos riesgos sobre los activos.

29.- ¿Para Ud. la seguridad lógica de la información se ve expuesta por las vulnerabilidades que tiene el sistema informático en la clínica?



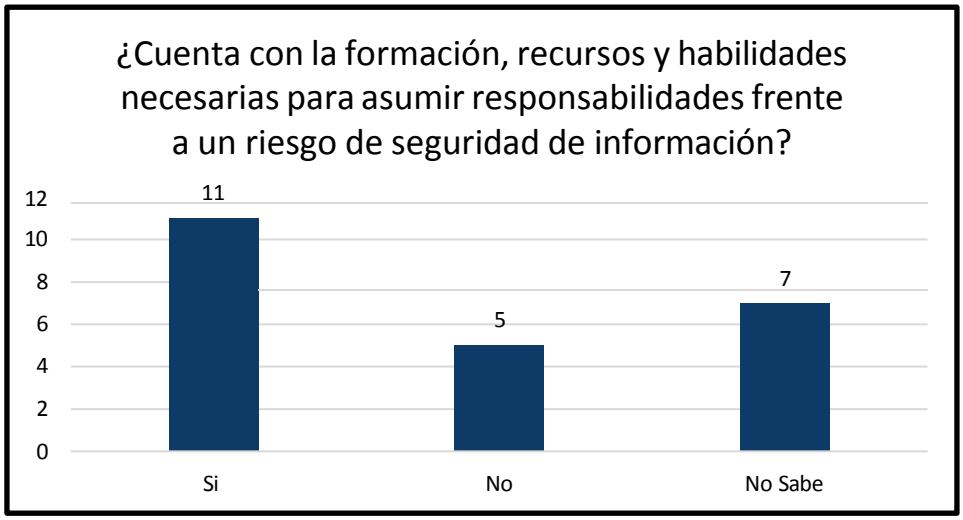
Según el gráfico, 5 encuestados afirmaron que la seguridad lógica sí se encuentra expuesta a la vulnerabilidad, 6 manifestaron que no existe alguna vulnerabilidad, 12 indicaron que no sabían si existe alguna vulnerabilidad en la seguridad lógica.

30.- ¿Se revisan todos los medios, para asegurarse que ningún tipo de dato sensible o software licenciado haya sido eliminado o sobrescrito con seguridad antes del desecho o reutilización del medio?



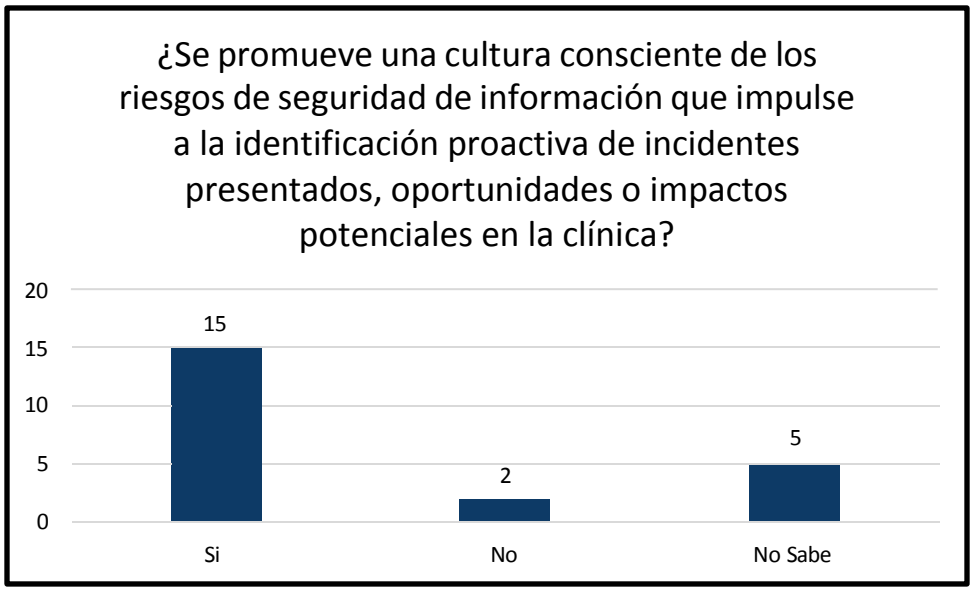
Para este ítem, 8 encuestados indicaron que sí se revisa los softwares o documentos antes de ser eliminados o modificados, 2 indicaron que no se revisa estos medios antes de la eliminación y 13 opinaron que no sabían si revisaba los documentos antes de su eliminación.

31.- ¿Cuenta con la formación, recursos y habilidades necesarias para asumir responsabilidades frente a un riesgo de seguridad de información?



Según el gráfico, 11 encuestados indicaron que sí tienen las habilidades necesarias para enfrentarse a un riesgo de seguridad de la información, 5 no saben qué hacer frente a estos riesgos y 7 no saben si son capaces de afrontar estos riesgos de seguridad de la información.

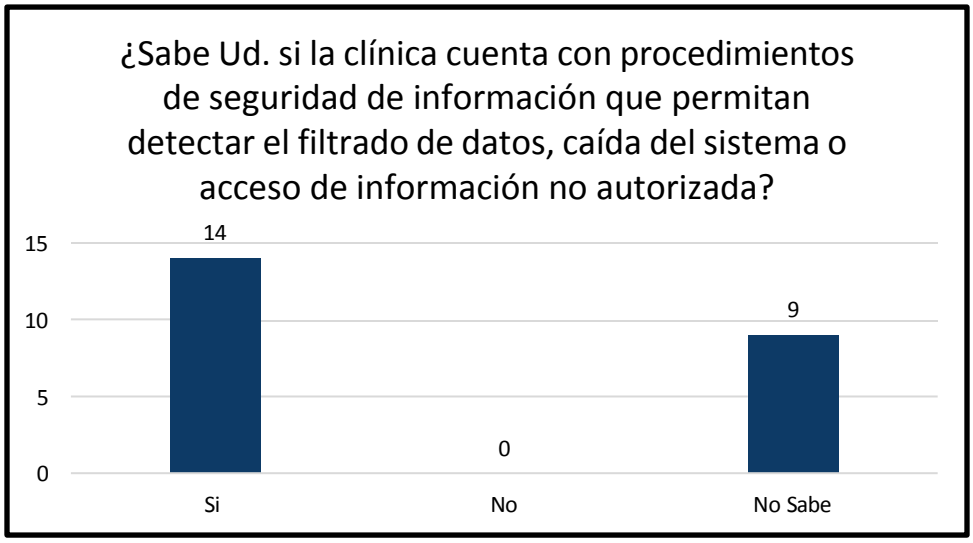
32.- ¿Se promueve una cultura consciente de los riesgos de seguridad de información que impulse a la identificación proactiva de incidentes presentados, oportunidades o impactos potenciales en la clínica?



Según el gráfico, 15 encuestados afirmaron que se promueve una cultura consciente para la identificación de incidentes o posibles riesgos, 2 indicaron que no se promueve esta cultura y 5 no sabían sobre este impulso sobre la identificación de incidentes.

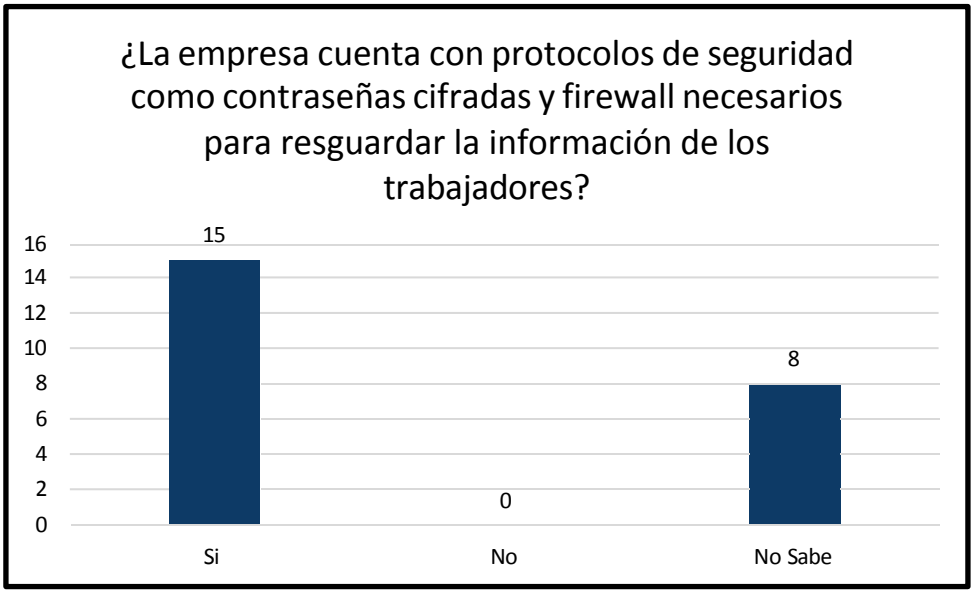
DIMENSIÓN: <u>Grado de adaptabilidad</u>
INDICADOR: Adaptabilidad de los procedimientos de seguridad

33.- ¿Sabe Ud. si la clínica cuenta con procedimientos de seguridad de información que permitan detectar el filtrado de datos, caída del sistema o acceso de información no autorizada?



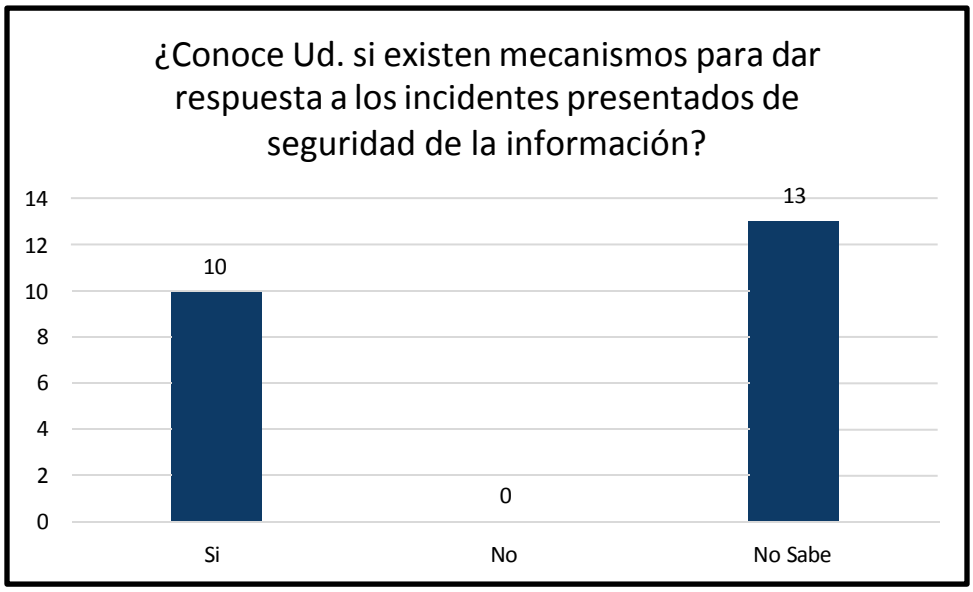
Según el gráfico, 14 encuestados indicaron que sí existen procedimientos para identificar el filtrado de datos y caída del sistema, mientras que 9 afirmaron que no saben si existe uno de estos procedimientos en la clínica.

34.- ¿La empresa cuenta con protocolos de seguridad como contraseñas cifradas y firewall necesarios para resguardar la información de los trabajadores?



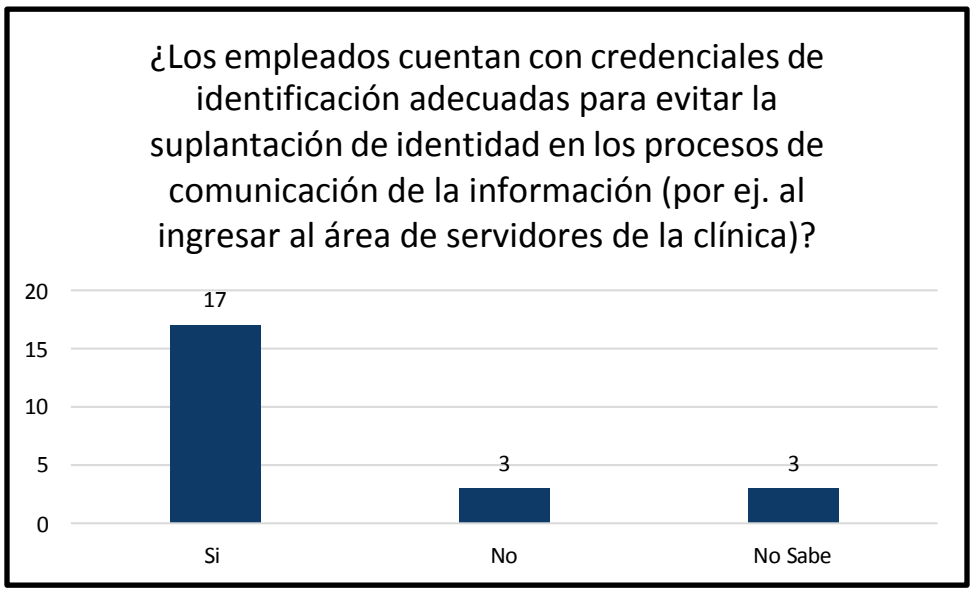
Según el gráfico, 15 personas afirman que sí existen protocolos de seguridad para el resguardo de contraseñas, 8 indicaron que no saben si existen estos protocolos de seguridad.

35.- ¿Conoce Ud. si existen mecanismos para dar respuesta a los incidentes presentados de seguridad de la información?



Según el gráfico, 10 encuestados afirmaron que sí existen mecanismos para dar respuestas contra incidentes, 13 afirmaron que no sabían si existen estos mecanismos frente a los incidentes.

36.- ¿Los empleados cuentan con credenciales de identificación adecuadas para evitar la suplantación de identidad en los procesos de comunicación de la información (por ej. al ingresar al área de servidores de la clínica)?



Según el gráfico, 17 encuestado afirman que sí cuentan con credenciales para evitar la suplantación, 3 indicaron que no cuentan con estas credenciales y 3 afirmaron que no sabían sobre estas credenciales.

Capítulo
7. Conclusiones

- El diseño del Sistema de Gestión de Seguridad de la Información bajo la ISO/IEC 27001:2022 influyó satisfactoriamente en el proceso emisión de certificados de aptitud médica donde se pudo dar una buena identificación sobre los activos que se encontraban en niveles altos de riesgos con esto se planificó los controles respectivos reduciendo los riesgos en estos activos.
- El diseño de un SGSI bajo la ISO/IEC 27001:2022 influye positivamente en la protección de datos personales a través de los controles y políticas que se contemplan acorde a lo establecido en la ISO /IEC 27001: 2022 y que posteriormente se deben implementar. Esto permite a la organización un tratamiento más seguro y consciente sobre los datos de los pacientes que se gestionan durante el proceso de emisión de los certificados de aptitud médica en la Clínica IPC Salud

- El aseguramiento de un correcto tratamiento de los activos de información en el proceso de emisión de certificados de aptitud médica se ve positivamente influenciado por un SGSI, debido a que se ha logrado identificar, tratar y mitigar los riesgos inherentes a su gestión.

- Aquellos trabajadores que interactúan con los pacientes en el proceso de emisión de certificados de aptitud médica perciben como positiva la implementación de un SGSI en la organización. Debido a esto se considera que el diseño influye positivamente en este objetivo ya que permite establecer el marco que regirá la implementación.

- Las personas involucradas en el proceso de emisión de certificados de aptitud médica de la Clínica IPC Salud lograrán adaptarse a los lineamientos establecidos por el SGSI debido a que han manifestado su acuerdo con la necesidad de que la información gestionada en la organización debe ser tratada respetando la confidencialidad, integridad y disponibilidad. Los resultados de la encuesta reflejan claramente esta visión.

Capítulo

8. Recomendaciones

- Se recomienda capacitar periódicamente al personal sobre temas de seguridad de información con la finalidad que puedan identificar los posibles riesgos y puedan estar al tanto de las nuevas tendencias y no sean vulnerables.

- Dar seguimiento a las políticas de seguridad propuestas, para reducir los riesgos en los activos de información y cumplir con los controles que tiene la ISO 27001:2022.

- Adquirir un software SIEM con lo cual sea más fácil la recopilación, análisis y poder observar los riesgos potenciales en tiempo real sin tener la necesidad de demorar y actuar más rápido disminuyendo los riesgos.

- Conformar un Comité de Seguridad que se encargue de gestionar la Seguridad de la Información, dando seguimiento del cumplimiento de las políticas y controles para una mayor protección de los activos.

Capítulo

9. Referencias Bibliográficas

Aguirre, D. (2014). *Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A.* [Tesis de pregrado, Pontificia Universidad Católica del Perú]. Repositorio de Tesis PUCP. http://hdl.handle.net/20.500.12404/5677

Barbosa, J. y Gonzáles, D. (2021). *Diseño del sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 para telemedicina en la IPS Colombiana de Trasplantes.* [Tesis de pregrado, Universidad Piloto de Colombia]

Barrantes, C. y Hugo, J. (2012). *Diseño e Implementación de un sistema de gestión de seguridad de información en procesos tecnológicos.* [Tesis de pregrado, Universidad de San Martin de Porres]. Repositorio USMP. https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/609/barrantes_ce.pdf?sequence=3&isAllowed=y

Campbell, D. y Stanley, J. (2005). *Diseños experimentales y cuasiexperimentales en la investigación social*. Amarrortu Editores [1ª edición en castellano 1973; novena reimpresión]

Ccesa, M. (2017). D*iseño de un Sistema de Gestión de Seguridad de la Información bajo la NTP ISI/IEC 27001:2014 para la Municipalidad Provincial de Huamanga.* [Tesis de pregrado, Universidad Nacional José Maria Arguedas]. Repositorio Institucional. https://hdl.handle.net/20.500.14168/504

Escalante, D. (2019). *Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la NTP ISO/IEC 27001 para la Dirección de Salud Virgen de Cocharcas – Chincheros.* [Tesis de pregrado, Universidad Nacional José Maria Arguedas]. Repositorio Institucional. https://repositorio.unajma.edu.pe/handle/20.500.14168/504

Hernández, R., Fernández C. y Baptista M. (2014). Concepción o elección del diseño de investigación. En M. Rocha (Ed.), *Metodología de la investigación* (pp. 126–168). McGraw-Hill / Interamericana editores, S.A. de C.V

ISO – International Organization for Standardization (2018). *Administración/Gestión de riesgos – Lineamientos guía.*

ISO – International Organization for Standardization (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements.*

Pinela, E. (2013). *Análisis de la necesidad de la firma digital en las exportadoras e importadoras guayaquileñas para la creación de una empresa de certificación*. [Tesis de pregrado, Universidad de Guayaquil]

Rodriguez, J. (2017). *Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en ISO27001 para Laboratorios Servicios Farmacéuticos de Calidad SFC Ltda.* [Tesis de pregrado, Universidad Nacional Abierta y a Distancia]

Tuapanta, J., Duque, M. y Mena, A. (2017) Alfa de Cronbach para validar un cuestionario de uso de TIC en docentes universitarios. *Revista mktDescubre 10*. 37-48. https://core.ac.uk/download/pdf/234578641.pdf

Valencia-Duque, F. y Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas y Tecnologías de Información, 22(6).* https://scielo.pt/pdf/rist/n22/n22a06.pdf

10. Anexos

Anexo 1. Resultados de Alfa de Cronbach

Sujeto	Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	Item 7	Item 8	Item 9	Item 10	Item 11	Item 12	Item 13	Item 14	Item 15	Item 16	Item 17	Item 18	Item 19	Item 20	Item 21	Item 22	Item 23	Item 24	Item 25	Item 26	Item 27	Item 28
1	3	3	3	2	2	2	2	1	3	3	2	2	3	2	2	2	3	2	1	2	3	1	3	3	3	2	1	2
2	3	3	3	3	3	3	3	3	3	2	3	2	3	2	2	2	3	3	1	3	3	2	3	2	3	1	2	3
3	3	3	3	3	3	2	3	3	3	3	3	2	3	3	3	2	3	2	3	3	3	2	3	3	3	3	2	2
4	3	3	3	3	2	3	3	3	3	2	3	3	2	3	3	3	3	3	1	3	2	1	3	2	3	1	3	1
5	3	3	3	2	3	2	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
6	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	2	2	2
7	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
8	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	2	2	2	2
9	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	2	2	2
10	3	3	3	3	2	2	2	2	2	3	3	3	2	3	3	2	3	3	2	3	3	3	3	2	2	1	3	3
11	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	2	2	2
12	3	3	3	3	2	3	2	3	3	3	3	3	3	3	3	2	3	3	1	3	3	2	3	3	3	1	3	1
13	3	3	3	1	3	2	3	3	3	2	3	3	3	3	3	3	2	2	1	1	3	1	3	2	3	1	2	3
14	3	3	3	1	3	3	3	3	3	2	3	3	3	2	2	3	3	2	1	2	3	3	3	2	3	1	2	3
15	3	3	3	2	3	2	2	2	3	1	3	1	3	3	2	3	3	3	1	3	3	1	3	2	1	2	3	1
16	3	3	3	3	2	2	2	2	3	3	2	2	2	2	2	2	3	2	1	3	3	2	3	2	2	2	2	2
17	3	2	3	2	3	2	2	2	3	2	3	2	2	2	2	2	2	2	1	2	2	2	3	2	1	2	2	2
18	3	3	3	3	3	3	2	2	3	2	2	2	3	2	2	2	3	3	1	3	3	2	3	3	3	2	3	2
19	3	3	3	3	2	2	2	2	3	2	2	2	2	2	2	3	3	3	2	2	3	2	3	2	2	2	2	2
20	3	2	3	2	3	2	2	3	3	3	3	2	3	2	2	2	2	2	1	2	3	2	3	2	1	1	2	1
21	3	3	3	3	3	2	3	3	3	2	3	3	3	2	3	3	3	2	1	2	3	1	3	3	3	1	3	2
22	3	3	2	2	2	2	3	2	3	2	2	2	3	2	2	3	3	3	2	2	3	1	3	2	1	2	1	2
23	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	1	3	3	2	3	3	3	2	2	2
Varianzas	0,000	0,083	0,043	0,443	0,221	0,257	0,249	0,340	0,043	0,352	0,178	0,352	0,202	0,257	0,257	0,249	0,119	0,249	0,838	0,340	0,083	0,628	0,000	0,257	0,601	0,451	0,383	0,447

Item 29	Item 30	Item 31	Item 32	Item 33	Item 34	Item 35	Item 36	Total
2	2	1	1	2	2	2	2	77
3	3	3	3	2	3	2	3	94
3	2	3	2	3	3	3	3	99
1	2	3	3	3	3	2	3	91
3	3	3	3	3	3	3	3	105
3	3	3	3	3	3	3	3	102
3	3	3	3	3	3	3	3	107
2	3	3	3	3	3	3	3	102
2	3	3	3	3	3	3	3	103
2	2	2	2	3	3	2	3	91
2	2	3	2	3	3	3	3	101
1	2	2	3	3	3	2	2	92
1	1	1	3	3	3	3	3	86
1	1	1	3	3	3	3	3	89
1	3	1	3	2	2	2	1	80
2	2	2	3	2	3	2	3	84
2	2	2	2	2	2	2	1	75
2	3	2	3	2	2	2	3	90
2	2	2	2	2	2	2	2	82
1	2	3	1	2	2	2	3	78
2	2	3	3	3	2	3	1	91
2	2	1	1	2	2	2	3	78
2	2	2	3	3	3	2	3	97
0,498	0,383	0,656	0,534	0,249	0,237	0,257	0,522	92,129

$$\alpha = \frac{k}{k-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

α : Alfa de Cronbach

k : Número de ítems

V_i: Varianza de cada ítem

V_t: Varianza del total

k=	36
V_i=	11,257
V_t=	92,129
α=	0,903

Anexo 2. Cuestionario sobre la seguridad de la información

Diseño de un Sistema de Gestión de Seguridad de la Información bajo la ISO/IEC 27001:2022 en el proceso de emisión de certificados de aptitud médica. Caso: Clínica IPC Salud

Nombre: _____

Cargo: _____ **Área:** _____

La presente encuesta tiene como objetivo:

Determinar la influencia del diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

Este cuestionario está dirigido al personal que forma parte del proceso de emisión de certificados de aptitud médica y no existe respuesta buena ni mala, todas son importantes y no debe dejar de marcar ningún casillero.

N°	CUESTIONARIO	Intervalo		
		Si	No sabe	No
Planificar				
	Actividades operativas de planificación			
1	¿Considera Ud. que el contar con una política de *seguridad de la información* [1] representa una ventaja considerable frente a otras entidades medicas?			
2	¿Se planifican y realizan tareas de mantenimiento de los equipos?			
Hacer				
N° de actividades de seguridad ejecutadas				
3	¿Considera Ud. que en su área de trabajo existe información valiosa que debe ser protegida de manera integral?			
4	¿En su área de trabajo se han realizado procesos de evaluación de riesgos relacionados a salvaguardar la integridad de la información de la clínica?			
Verificar				
Revisión de las actividades planificadas y ejecutadas				
5	¿Tiene Ud. conocimiento de que está garantizada la información en la clínica?			
6	¿Sabe Ud. si se ha realizado auditorías sobre la seguridad de la información?			
Actuar				
Análisis de la mejora de la seguridad				
7	¿Existe un plan de contingencias en la clínica para afrontar un evento de disponibilidad de información de los pacientes?			
De las Protección de los Datos Personales				

Controles de seguridad de la información				
8	¿Posee conocimientos respecto de controles de seguridad de la información?			
9	¿Para usted el diseño y la implementación de controles de seguridad reducirá los riesgos de seguridad de la información?			
10	¿Sabe usted si existen controles de *seguridad de la información* [1] que protejan de posibles vulnerabilidades en los activos de información de la clínica (Ej. evitar manipulación de datos o piratería de software)			
Del aseguramiento de los Activos de Información				
Confidencialidad				
11	¿Sabe Ud. si la clínica brinda una protección adecuada para evitar la divulgación de datos personales de los pacientes?			
12	¿Conoce Ud. si la clínica ha implementado controles de *seguridad de la información* [1] para evitar el acceso no autorizado, que impida la divulgación de la información de los pacientes?			
13	¿Tiene conocimiento si en su contrato se contempla algún ítem que estipulen, que deberá guardar la confidencialidad en relación con la información que haya tenido acceso en el desempeño de sus funciones?			
14	¿Sabe si la clínica ha implementado algún control de acceso para proteger la confidencialidad de los datos personales de los trabajadores?			
15	¿Sabe Ud. si existe algún procedimiento definido de baja de usuario una vez que se finalice una actividad, puesto de trabajo o cese de contrato en la clínica?			
Integridad				
16	¿Se han establecido procedimientos para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo? (Ej. se activa el bloqueo de pantalla con contraseña para proteger el acceso a sus PCs)			
17	¿Se controla o supervisa la actividad del personal que accede a las áreas seguras de la clínica?			
18	¿Se establecen medidas de seguridad en zonas de oficinas para proteger la información de los equipos en áreas accesibles por personal externo?			
19	¿En lo que va del año ha sufrido alguna modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, traspapeles de documentos, etc.?			
20	¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionen pérdidas de la integridad de la información?			
Disponibilidad				
21	¿Conoce Ud. si la información de los datos de los pacientes está disponible en todo momento y es accesible sólo por personal autorizado?			

22	¿Tienes conocimiento si la información de los pacientes, han sido objeto de alguna vulnerabilidad, debido a brechas de seguridad del sistema de información de la clínica?			
23	¿Cuenta usted con una clave de acceso para ingresar a su computador y/o laptop, así como a los sistemas de información de la clínica?			
24	¿Existe un plan de continuidad de negocio en la clínica para garantizar la disponibilidad de los sistemas de información?			
Del Nivel de percepción				
Nivel de percepción de los trabajadores sobre la seguridad de la información				
25	¿Usted ha tenido alguna capacitación sobre la seguridad de la información?			
26	¿Considera Ud. que la *seguridad digital*[2] del sistema informático de la clínica se encuentra expuesta a vulnerabilidades que pondría en riesgo la información allí contenida?			
27	¿Existen procesos de formación y sensibilización sobre las responsabilidades en la seguridad de la información?			
28	¿Desde su perspectiva, la *seguridad física*[3] de los activos de información se encuentran vulnerables en la clínica?			
29	¿Para Ud. la *seguridad lógica*[4] de la información se ve expuesta por las vulnerabilidades que tiene el sistema informático en la clínica?			
30	¿Se revisan todos los medios, para asegurarse que ningún tipo de dato sensible o software licenciado haya sido eliminado o sobrescrito con seguridad antes del desecho o reutilización del medio?			
31	¿Cuenta con la formación, recursos y habilidades necesarias para asumir responsabilidades frente a un riesgo de seguridad de información?			
32	¿Se promueve una cultura consciente de los riesgos de seguridad de información que impulse a la identificación proactiva de incidentes presentados, oportunidades o impactos potenciales en la clínica?			
Del grado de adaptabilidad				
Adaptabilidad de los procedimientos de seguridad				
33	¿Sabe Ud. si la clínica cuenta con procedimientos de seguridad de información que permitan detectar el filtrado de datos, caída del sistema o acceso de información no autorizada?			
34	¿La empresa cuenta con protocolos de seguridad como contraseñas cifradas y firewall necesarios para resguardar la información de los trabajadores?			
35	¿Conoce Ud. sí existen mecanismos para dar respuesta a los incidentes presentados de seguridad de la información?			
36	¿Los empleados cuentan con credenciales de identificación adecuadas para evitar la suplantación de identidad en los procesos de comunicación de la información (por ej. al ingresar al área de servidores de la clínica)?			

Leyenda:

1. Controles y políticas de seguridad: Cualquier tipo de protección utilizada para minimizar los riesgos de seguridad de la propiedad física, la información, los sistemas informáticos u otros activos.

2. Seguridad digital: Conjunto de políticas, procedimientos, estrategias y herramientas encargadas de proteger la infraestructura informática de una organización como la información frente a ciberataques y otros riesgos

3. Seguridad Física: Protección del sistema ante las amenazas físicas, planes de contingencia, control de acceso físico, políticas de backups.

4. Seguridad Lógica: Protección de la información en su propio medio mediante el uso de herramientas de seguridad.

- **Anexo 3.** Validación del instrumento de investigación por juicio de experto
-

ENTREVISTA

Objetivo: Determinar la influencia del diseño de un sistema de gestión de seguridad de la información bajo la ISO/IEC 27001:2022 en el proceso de emisión de certificados de aptitud médica en la Clínica IPC Salud.

N° Ítem	Preguntas relacionadas a la investigación	Observaciones del Experto
I. Planificar		
I.1.Actividades operativas de planificación		
1.	¿Considera Ud. que el contar con una política de seguridad de la información representa una ventaja considerable frente a otras entidades medicas?	
.	¿Se planifican y realizan tareas de mantenimiento de los equipos?	
II. Hacer		

II.1. N° de actividades de seguridad ejecutadas		
	¿Considera Ud. que en su área de trabajo existe información valiosa que debe ser protegida de manera integral?	
	¿En su área de trabajo se han realizado procesos de evaluación de riesgos relacionados a salvaguardar la integridad de la información de la clínica?	
III. Verificar		
III.1 Revisión de las actividades planificadas y ejecutadas **Revisión de las actividades planificadas y ejecutadas**		
	¿Tiene Ud. conocimiento de que está garantizada la información en la clínica?	¿Ha sido aprobado por la dirección un documento que contenga la política de seguridad de la información, y ha sido publicado y comunicado a todos los empleados y terceras partes relevantes?
	¿Sabe Ud. si se ha realizado auditorías sobre la seguridad de la información?	

IV. Actuar		
	¿Existe un plan de contingencias en la clínica para afrontar un evento de disponibilidad de información de los pacientes?	
V. De las Protección de los Datos Personales		
V.1. Controles de seguridad de la información		
	¿Posee conocimientos respecto de controles de seguridad de la información?	Existe una política de cambios de Contraseñas de los usuarios, Bases de Datos y Red. Cada cuanto tiempo caducan las contraseñas. Complejidad. Existe algún procedimiento de altas y bajas de usuarios, en coordinación con RRHH en casos de ingresos, ceses de trabajadores
	¿Para usted el diseño y la implementación de controles de seguridad reducirá los riesgos de seguridad de la información?	
	¿Sabe usted si existen controles de seguridad de información que protejan de posibles vulnerabilidades en los activos de información de la clínica (Ej. evitar manipulación de datos o piratería de software)	
VI. Del aseguramiento de los Activos de Información		

VI.1 Confidencialidad		
	¿Sabe Ud. si la clínica brinda una protección adecuada para evitar la divulgación de datos personales de los pacientes?	
	¿Conoce Ud. si la clínica ha implementado controles de seguridad de información para evitar el acceso no autorizado, que impida la divulgación de la información de los pacientes?	
	¿Tiene conocimiento si en su contrato se contempla algún ítem que estipule, que deberá guardar la confidencialidad en relación con la información que haya tenido acceso en el desempeño de sus funciones?	
	¿Sabe si la clínica ha implementado algún control de acceso para proteger la confidencialidad de los datos personales de los trabajadores?	
	¿Sabe Ud. si existe algún procedimiento definido de baja de usuario una vez que se finalice una actividad, puesto de trabajo o cese de contrato en la clínica?	

VI.2. Integridad		
	¿Se han establecido procedimientos para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo? (Ej. se activa el bloqueo de pantalla con contraseña para proteger el acceso a sus PCs)	¿Se utilizan perímetros de seguridad (barreras como: paredes, puertas de acceso controladas por tarjetas de identidad, puestos de recepción, ¿etc.) para proteger áreas que contengan información e infraestructura para el procesamiento de la información? ¿Están protegidas las áreas seguras por los controles de entrada apropiados para asegurarse de que solamente permiten el acceso de personal autorizado?
	¿Se controla o supervisa la actividad del personal que accede a las áreas seguras de la clínica?	
	¿Se establecen medidas de seguridad en zonas de oficinas para proteger la información de los equipos en áreas accesibles por personal externo?	
	¿En lo que va del año ha sufrido alguna modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, traspapeles de documentos, etc.?	
	¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionen pérdidas de la integridad de la información?	
VI.3. Disponibilidad		

	¿Conoce Ud. si la información de los datos de los pacientes está disponible en todo momento y es accesible sólo por personal autorizado?	
	¿Tienes conocimiento si la información de los pacientes, han sido objeto de alguna vulnerabilidad, debido a brechas de seguridad del sistema de información de la clínica?	
	¿Cuenta usted con una clave de acceso para ingresar a su computador y/o laptop, así como a los sistemas de información de la clínica?	
	¿Existe un plan de continuidad de negocio en la clínica para garantizar la disponibilidad de los sistemas de información?	
VII. Del Nivel de percepción		
VII.1 Nivel de percepción de los trabajadores sobre la seguridad de la información		
	¿Usted ha tenido alguna capacitación sobre la seguridad de la información?	

	¿Considera Ud. que la seguridad digital del sistema informático de la clínica se encuentra expuesta a vulnerabilidades que pondría en riesgo la información allí contenida?
	¿Existen procesos de formación y sensibilización sobre las responsabilidades en la seguridad de la información?
	¿Desde su perspectiva, la seguridad física de los activos de información se encuentra vulnerables en la clínica?
	¿Para Ud. la seguridad lógica de la información se ve expuesta por las vulnerabilidades que tiene el sistema informático en la clínica?
	¿Se revisan todos los medios, para asegurarse que ningún tipo de dato sensible o software licenciado haya sido eliminado o sobrescrito con seguridad antes del desecho o reutilización del medio?
	¿Cuenta con la formación, recursos y habilidades necesarias para asumir responsabilidades frente a un riesgo de seguridad de información?

	¿Se promueve una cultura consciente de los riesgos de seguridad de información que impulse a la identificación proactiva de incidentes presentados, oportunidades o impactos potenciales en la clínica?	
VIII. Del grado de adaptabilidad		
VIII.1 Adaptabilidad de los procedimientos de seguridad		
	¿Sabe Ud. si la clínica cuenta con procedimientos de seguridad de información que permitan detectar el filtrado de datos, caída del sistema o acceso de información no autorizada?	¿Existe un procedimiento formal de registro y de salida del registro para los usuarios de la organización con el fin de garantizar o revocar el acceso a todos los sistemas de información y servicios? ¿Se restringe y controla la asignación y retiro de accesos? ¿Los derechos de acceso de los usuarios, se revisan en intervalos regulares de tiempo siguiendo un proceso formal?
	¿La empresa cuenta con protocolos de seguridad como contraseñas cifradas y firewall necesarios para resguardar la información de los trabajadores?	
	¿Conoce Ud. sí existen mecanismos para dar respuesta a los incidentes presentados de seguridad de la información?	
	¿Los empleados cuentan con credenciales de identificación adecuadas para evitar la suplantación de identidad en los procesos de comunicación de la información (por ej. al	

	ingresar al área de servidores de la clínica)?	
	¿Los empleados cuentan con credenciales de identificación adecuadas para evitar la suplantación de identidad en los procesos de comunicación de la información (por ej. al ingresar al área de servidores de la clínica)?	

OPINIÓN DEL EXPERTO DEL INSTRUMENTO DE INVESTIGACIÓN – CÉSAR MOLINA

I. ASPECTOS DE VALIDACIÓN

Criterios	Indicadores	Deficiente 00-20%				Regular 21-40%				Buena 41-60%				Muy buena 61-80%				Excelente 81-100%			
		0 5	6 10	11 15	16 20	21 25	26 30	31 35	36 40	41 45	46 50	51 55	56 60	61 65	66 70	71 75	76 80	81 85	86 90	91 95	96 100
ridad	Esta formulado c enguaje apropia																			92	
Objetividad	Esta expresado e capacidades observables.																				98
Actualidad	Esta adecuado a conceptos.																			95	
Organización	Existe una organización lóg																			95	
Suficiencia	Comprende los aspectos de calid y cantidad.																			94	
Intencionali dad	Adecuado para valorar aspectos cognoscitivos.																				96
Consistencia	Basado en aspect eóricos del derecho.																			92	
Coherencia	Existe coherenci entre los ndicadores y las dimensiones.																			92	

Criterios	Indicadores	Deficiente 00-20%				Regular 21-40%				Buena 41-60%				Muy buena 61-80%				Excelente 81-100%			
		0 5	6 10	11 15	16 20	21 25	26 30	31 35	36 40	41 45	46 50	51 55	56 60	61 65	66 70	71 75	76 80	81 85	86 90	91 95	96 100
Metodología	**La estrategia responde al propósito de la investigación.**																				**97**

II. PROMEDIO DE VALORACIÓN: 95 %

III. OPCIÓN DE APLICABILIDAD:

(x) El instrumento puede ser aplicado, tal como está elaborado

(x) El instrumento debe ser mejorado -con las observaciones del experto- antes de ser aplicado

IV. VALIDADO POR:

Nombre y Apellido: CESAR MOLINA NEYRA	DNI/CE N.º: 40553679
Profesión: INGENIERO DE SISTEMAS	
Lugar de Trabajo: UNMSM	
Cargo que desempeña: DOCENTE	
Lugar y fecha de validación: LIMA, 10 DE AGOSTO 2023	
Firma de experto informante: 	

OPINIÓN DEL EXPERTO DEL INSTRUMENTO DE INVESTIGACIÓN

I. ASPECTOS DE VALIDACIÓN

Criterios	Indicadores	Deficiente 00-20%				Regular 21-40%				Buena 41-60%				Muy buena 61-80%				Excelente 81-100%			
		0 5	6 10	11 15	16 20	21 25	26 30	31 35	36 40	41 45	46 50	51 55	56 60	61 65	66 70	71 75	76 80	81 85	86 90	91 95	96 100
1. Claridad	Esta formulado con lenguaje apropiado.																				
2. Objetividad	Esta expresado en capacidades observables.																				
3. Actualidad	Esta adecuado a conceptos.																				
4. Organización	Existe una organización lógica.																				
5. Suficiencia	Comprende los aspectos de calidad y cantidad.																				
6. Intencionalidad	Adecuado para valorar aspectos cognoscitivos.																				
7. Consistencia	Basado en aspectos teóricos del derecho.																				
8. Coherencia	Existe coherencia entre los indicadores y las dimensiones.																				
9. Metodología	La estrategia responde al propósito de la investigación.																				

II. PROMEDIO DE VALORACION: 100 %

III. OPCIÓN DE APLICABILIDAD:

(x) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado -con las observaciones del experto- antes de ser aplicado

IV. VALIDADO POR:

Nombre y Apellido: Nilo E. Carrasco Ore	DNI/CE Nº: 09342780
Profesión: Ingeniero de Sistemas	
Lugar de Trabajo: Universidad Nacional Mayor de San Marcos	
Cargo que desempeña: Docente	
Lugar y fecha de validación: 16 agosto 2023	
Firma de experto informante: 	

OPINIÓN DEL EXPERTO DEL INSTRUMENTO DE INVESTIGACIÓN

I. ASPECTOS DE VALIDACIÓN

Criterios	Indicadores	Deficiente 00-20%				Regular 21-40%				Buena 41-60%				Muy buena 61-80%				Excelente 81-100%			
		0 5	6 10	11 15	16 20	21 25	26 30	31 35	36 40	41 45	46 50	51 55	56 60	61 65	66 70	71 75	76 80	81 85	86 90	91 95	96 100
1. Claridad	Esta formulado con lenguaje apropiado.																	X			
2. Objetividad	Esta expresado en capacidades observables.																		X		
3. Actualidad	Esta adecuado a conceptos.																		X		
4. Organización	Existe una organización lógica.																		X		
5. Suficiencia	Comprende los aspectos de calidad y cantidad.																		X		
6. Intencionalidad	Adecuado para valorar aspectos cognoscitivos.																			X	
7. Consistencia	Basado en aspectos teóricos del derecho.																		X		
8. Coherencia	Existe coherencia entre los indicadores y las dimensiones.																		X		
9. Metodología	La estrategia responde al propósito de la investigación.																			X	

II. PROMEDIO DE VALORACION: 91 %

III. OPCIÓN DE APLICABILIDAD:

(X) El instrumento puede ser aplicado, tal como está elaborado

( ) El instrumento debe ser mejorado -con las observaciones del experto- antes de ser aplicado

IV. VALIDADO POR:

Nombre y Apellido: Julio Arturo Molina Gárate	DNI/CE Nº: 08459708
Profesión: Economista	
Lugar de Trabajo: Ministerio de Economía y Finanzas	
Cargo que desempeña: Jefe de la Oficina e Gobierno de Tecnología de la Información	
Lugar y fecha de validación: 27/09/2023	
Firma de experto informante: