



FACULTAD DE INGENIERÍA Y ARQUITECTURA  
ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

**DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN  
DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS  
ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM PERÚ  
SAC**

**PRESENTADA POR**

**MIGUEL ANGEL CRUZ DIAZ  
SENYI FUKUSAKI INFANTAS**

**ASESORA**

**LUZ SUSSY BAYONA ORE**

**LUIS ESTEBAN PALACIOS QUICHIZ**

**TESIS**

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE  
COMPUTACIÓN Y SISTEMAS**

**LIMA – PERÚ**

**2017**



**CC BY-NC**

**Reconocimiento – No comercial**

Los autores permiten transformar (traducir, adaptar o compilar) a partir de esta obra con fines no comerciales, y aunque en las nuevas creaciones deban reconocerse la autoría y no puedan ser utilizadas de manera comercial, no tienen que estar bajo una licencia con los mismos términos.

<http://creativecommons.org/licenses/by-nc/4.0/>



**USMP**  
UNIVERSIDAD DE  
SAN MARTÍN DE PORRES

**FACULTAD DE  
INGENIERÍA Y ARQUITECTURA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y  
SISTEMAS**

**DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN  
DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER  
LOS ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM  
PERÚ SAC**

**TESIS**

**PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE  
COMPUTACIÓN Y SISTEMAS**

**PRESENTADA POR**

**CRUZ DIAZ, MIGUEL ANGEL  
FUKUSAKI INFANTAS, SENYI**

**LIMA – PERÚ**

**2017**

Dedico este trabajo a mi familia que con amor me apoyó desde el comienzo de la misma, en especial a mis padres, Edilberto y Rocío, que me inspiraron a superarme con sacrificio y esfuerzo. A mi abuela Julia que con sus consejos supieron motivarme a ser siempre mejor y a Alex y Sheila por su apoyo. Gracias a todos.

**Miguel Angel Cruz Diaz**

Dedico esta tesis a mi familia por sus consejos constantes y ser mi motivación diaria. A Emily, por su soporte, amor y comprensión, y a Dios por ser nuestro guía principal e incondicional.

**Senyi Fukusaki Infantas**

## ÍNDICE

	<b>Página</b>
<b>RESUMEN</b>	<b>i</b>
<b>ABSTRACT</b>	<b>ii</b>
<b>INTRODUCCIÓN</b>	<b>iii</b>
<b>CAPÍTULO I. MARCO TEÓRICO</b>	<b>1</b>
<b>1.1 Antecedentes</b>	<b>1</b>
<b>1.2 Bases teóricas</b>	<b>14</b>
<b>1.3 Términos básicos</b>	<b>28</b>
<b>CAPÍTULO II. METODOLOGÍA</b>	<b>30</b>
<b>2.1 Materiales</b>	<b>30</b>
<b>2.2 Métodos</b>	<b>31</b>
<b>CAPÍTULO III. DESARROLLO DEL PROYECTO</b>	<b>40</b>
<b>3.1 Cronograma de implementación</b>	<b>40</b>
<b>3.2 Implementación del SGSI</b>	<b>41</b>
<b>3.3 Prueba de Efectividad de Controles</b>	<b>116</b>
<b>CAPÍTULO IV. PRUEBAS Y RESULTADOS</b>	<b>118</b>
<b>CAPÍTULO V. DISCUSIONES Y APLICACIONES</b>	<b>127</b>
<b>5.1 Discusiones</b>	<b>127</b>

<b>5.2 Aplicaciones</b>	<b>130</b>
<b>CONCLUSIONES</b>	<b>131</b>
<b>RECOMENDACIONES</b>	<b>133</b>
<b>FUENTES DE INFORMACIÓN</b>	<b>139</b>
<b>ANEXOS</b>	<b>189</b>

## LISTA DE FIGURAS

	<b>Página</b>
<b>Figura 1. Beneficios de la Seguridad de Información</b>	<b>2</b>
<b>Figura 2. Certificaciones de ISO/IEC 27001 a nivel global</b>	<b>4</b>
<b>Figura 3. Preocupaciones de encargados de la seguridad de información en Latinoamérica</b>	<b>5</b>
<b>Figura 4. Incidentes de seguridad de la información en las empresas de Latinoamérica</b>	<b>7</b>
<b>Figura 5. Contexto regional de la legislación de protección de datos personales</b>	<b>12</b>
<b>Figura 6. Cronograma de la legislación peruana</b>	<b>13</b>
<b>Figura 7. Modelo PDCA aplicado a los Procesos SGSI</b>	<b>15</b>
<b>Figura 8. Cláusulas de la ISO/IEC 27001</b>	<b>16</b>
<b>Figura 9. Cláusulas de control de la ISO/IEC 27002</b>	<b>19</b>
<b>Figura 10. Proceso de Gestión de Riesgos</b>	<b>21</b>
<b>Figura 11. Área de aplicación de la ISO/IEC 31010 en el proceso de gestión de Riesgos</b>	<b>22</b>
<b>Figura 12. ISO/IEC 27005 dentro de la implementación de SGSI</b>	<b>22</b>
<b>Figura 13. Proceso de Gestión de Riesgo orientado a seguridad de información</b>	<b>24</b>



<b>Figura 14. Tratamiento de los Riesgos</b>	<b>26</b>
<b>Figura 15. Ciclo de Deming con las fases de Implementación</b>	<b>31</b>
<b>Figura 16. Ejemplo de Matriz de Riesgo</b>	<b>34</b>
<b>Figura 17. Diagrama del Proceso de Captación de Clientes</b>	<b>44</b>
<b>Figura 18. Diagrama del Proceso de Atención al Cliente</b>	<b>45</b>
<b>Figura 19. Diagrama del Proceso de Procesamiento de Datos</b>	<b>46</b>
<b>Figura 20. Diagrama del Proceso de Facturación</b>	<b>47</b>
<b>Figura 21. Diagrama del Proceso de Cobranza</b>	<b>47</b>
<b>Figura 22. Diagrama del Proceso de Logística</b>	<b>48</b>
<b>Figura 23. Comparación de la criticidad de los Riesgos previo al proyecto y posterior</b>	<b>119</b>
<b>Figura 24. Resultado de conocimiento de políticas de seguridad</b>	<b>121</b>
<b>Figura 25. Resultados de Encuesta: Pregunta 1</b>	<b>123</b>
<b>Figura 26. Resultados de Encuesta: Pregunta 2</b>	<b>124</b>
<b>Figura 27. Resultados de Encuesta: Pregunta 3</b>	<b>124</b>
<b>Figura 28. Resultados de Encuesta: Pregunta 4</b>	<b>125</b>
<b>Figura 29. Resultados de Encuesta: Pregunta 5</b>	<b>126</b>

## LISTA DE TABLAS

	Página
Tabla 1. Certificaciones de ISO/IEC 27001 a niveles regionales	5
Tabla 2. Certificaciones de ISO/IEC 27001 a nivel de servicios	5
Tabla 3. Certificaciones de ISO/IEC 27001 a nivel de países	7
Tabla 4. Infracciones por incumplimiento de la ley de protección de datos	13
Tabla 5. Sanciones por incumplimiento de la ley de protección de datos	14
Tabla 6. Materiales usados en el proyecto	30
Tabla 7. Pasos para la implementación de ISO/IEC 27001	31
Tabla 8. Cronograma de Implementación del Proyecto	40
Tabla 9. Misión, Visión y Objetivos de MEDCAM Perú SAC	41
Tabla 10. Campos del Análisis de Vulnerabilidades y Amenazas	49
Tabla 11. Criterios para la Tasa de Ocurrencia del Riesgo	49
Tabla 12. Criterios para la determinación del impacto	50
Tabla 13. Matriz de Calor	51
Tabla 14. Tratamiento del Riesgo	51
Tabla 15. Campos de la Matriz de Riesgos	52

<b>Tabla 16. Campos de la Identificación de Activos</b>	<b>53</b>
<b>Tabla 17. Inventario de Activos</b>	<b>54</b>
<b>Tabla 18. Valores asignados a las dimensiones del activo</b>	<b>63</b>
<b>Tabla 19. Valorización de Activos</b>	<b>65</b>
<b>Tabla 20. Amenazas y Vulnerabilidades de los Activos</b>	<b>66</b>
<b>Tabla 21. Matriz de Riesgos</b>	<b>71</b>
<b>Tabla 22. Controles Identificados</b>	<b>83</b>
<b>Tabla 23. Campos en la Declaración de Aplicabilidad</b>	<b>91</b>
<b>Tabla 24. Declaración de Aplicabilidad</b>	<b>92</b>
<b>Tabla 25. Comparación de Criticidad</b>	<b>119</b>
<b>Tabla 26. Comparación de Documentación Entregada</b>	<b>120</b>
<b>Tabla 27. Comparación de Controles por Dominio</b>	<b>122</b>
<b>Tabla 28. Objetivos asociados a sus pruebas y resultados</b>	<b>129</b>

## RESUMEN

La presente tesis tuvo como objetivo diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) con el fin de proteger los activos de información que influyan directamente en el cumplimiento de los objetivos de la empresa. Como metodología para el diseño del SGSI, se utilizó el método Deming o PDCA (Plan-Do-Check-Act), sugerida por la norma ISO/IEC 27001, la cual parte de la identificación de los activos de información y, es a base de la clasificación de los mismos, que se determina el posible impacto ante un evento de pérdida, y se establecen acciones de respuesta para la mitigación de los riesgos a los que están expuestos los activos. Los controles en respuesta se obtuvieron de la norma ISO/IEC 27002. Como resultado, se consiguió implementar un SGSI con lo que se logró minimizar los riesgos de amenazas y vulnerabilidades sobre los activos de información de MEDCAM Perú S.A.C. y así, lograr la confidencialidad, disponibilidad e integridad de la información. Concluimos que el beneficio más importante es asegurar los activos de información y así el cumplimiento de los objetivos de la empresa; así como, que cada SGSI debe estar acorde con el tamaño y madurez de los procesos de la empresa.

**Palabras Claves:** Sistema de Gestión de Seguridad de la Información, ISO/IEC 27001, ISO/IEC 27002, Activos de Información, Gestión de Riesgos

## **ABSTRACT**

The objective of this thesis is to design and implement an Information Security Management System (ISMS) in order to protect information assets that directly influence the fulfillment of the company's objectives. As a methodology for the design of the ISMS, the Deming or PDCA (Plan-Do-Check-Act) method was used, suggested by the ISO / IEC 27001 standard, which is based on the identification of information assets and is based on the classification of the same, which determines the possible impact before a loss event, and response actions are established to mitigate the risks to which the assets are exposed. The controls in response will be obtained from the ISO / IEC 27002 standard. As a result, an ISMS was implemented, which minimized the risks of threats and vulnerabilities on the information assets of MEDCAM Peru S.A.C. and ensure the confidentiality, availability and integrity of the information. We conclude that the most important benefit is to secure the information assets and thus the fulfillment of the company's objectives; as well as, that each ISMS must be commensurate with the size and maturity of the company's processes

**Keywords:** Information Security Management System, ISO/IEC 27001, ISO/IEC 27002, Information assets, Risk Management

## INTRODUCCIÓN

La seguridad de la formación ha sido una cuestión estratégica crucial en la gestión de la organización. La gestión de la seguridad de la información es un proceso sistemático para afrontar eficazmente las amenazas y los riesgos de la seguridad de la información en una organización. (Tu, Z., Yuan, Y., 2014)

Actualmente, los sistemas de información, los datos contenidos en ellas y la información son los activos más valiosos para las organizaciones empresariales y se hace necesario brindarles una protección adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad. Una manera efectiva de descubrir estas vulnerabilidades y amenazas existentes es iniciando los procesos diagnósticos que permitan establecer el estado actual de la seguridad dentro de la organización, teniendo en cuenta la normatividad vigente y los procesos de análisis y evaluación de riesgos. (Solarte, F., Enríquez, E., Benavidez, M., 2015)

La seguridad de la información es actualmente esencial, ya que asegura la integridad, disponibilidad y confidencialidad de la información, esto garantiza la reducción de las vulnerabilidades de la empresa, errores, o mal uso de los activos.

Según Andress, J. (2015), en un sentido general, la seguridad significa proteger nuestros activos. Esto puede significar protegerlos de los atacantes

que invaden nuestras redes, virus/gusanos, desastres naturales, condiciones ambientales adversas, fallas de energía, robo o vandalismo, o las formas más probables de ataque, en la medida de lo razonablemente posible, dadas nuestras condiciones ambientales. En los esfuerzos por asegurar nuestros activos, también debemos considerar las consecuencias de la seguridad que elegimos implementar. Hay una cita muy conocida que dice "El único sistema seguro es aquél que está apagado, en el interior de un bloque de hormigón, protegido en una habitación sellada, rodeada por guardias armados, y aun así tengo mis dudas." Aunque ciertamente podríamos decir que un sistema en tal estado podría ser considerado como seguro, seguramente no es utilizable ni productivo. A medida que aumentamos el nivel de seguridad, usualmente disminuimos el nivel de productividad. El objetivo de un plan de seguridad es encontrar el equilibrio entre protección, usabilidad y costo.

Una estrategia para brindar una adecuada protección a los activos es implementando un sistema de gestión de seguridad de información (SGSI) bajo un marco de trabajo como la ISO/IEC 27001 ya que permite tener una evaluación de los riesgos de seguridad estructurada, teniendo en cuenta las vulnerabilidades a la que está expuesta la organización lo que proporciona un marco para la correcta selección e implementación de controles u otras medidas correctivas para el tratamiento de los riesgos y a su vez, permite tener un proceso de mejora continua y es adaptable para todas las organizaciones.

El establecimiento y funcionamiento de un SGSI no reducirá por sí solo, necesariamente, el riesgo negativo de seguridad de la información. En esencia, el SGSI es una herramienta que permite a una organización controlar, sistemáticamente, el nivel de seguridad y rendimiento de la información. El sistema debe proporcionar beneficios económicos, como disminuir el tiempo de investigación, agilizar el tiempo para aprender cosas nuevas, aminorar las disputas, reducir los honorarios legales, la posible reducción de las primas de seguros, la protección de los activos de información, aumentar la conciencia sobre la seguridad de la información, confianza con clientes y otras partes interesadas. La norma ISO/IEC 27001 ayuda a proteger la confidencialidad de la información de manera que los

mantenga accesibles solo al personal autorizado, la norma preserva la integridad, exactitud e integridad de la información y la disponibilidad de información a las entidades autorizadas y la posibilidad de usarlas. Un sistema de gestión que se ha introducido en una organización para la protección de la información (Britvic, J., Prelas, A., Cingel, M., 2013).

En la presente tesis, se diseña un sistema de gestión de seguridad de la información basada en la ISO/IEC 27001 para la clínica de salud ocupacional MEDCAM Perú SAC alineados a su plan estratégico y sus objetivos de negocio.

El trabajo ha sido estructurado en cinco capítulos. El primero aborda el marco teórico, donde se desarrollan las bases teóricas del proyecto, los antecedentes a nivel global, regional y local y los términos básicos esenciales para un mejor entendimiento de la presente tesis. En el segundo, se explica sobre la metodología que se utilizó para la implementación del sistema de gestión de la seguridad de la información que se utilizó para el desarrollo del mismo. En el tercero, se documenta el desarrollo del proyecto, mostrando la solución, las actividades por cada fase, las pruebas, la aceptación del proyecto y las pruebas de implementación. En el cuarto, se analizan las pruebas y resultados de la implementación del SGSI en la empresa, en él se revisan los resultados obtenidos por cada objetivo planeado. En el quinto, se discuten los resultados comparándolos con los resultados teóricos y los obtenidos por otros investigadores.

La situación problemática, en este contexto actual, una de cuatro empresas sufre problemas de seguridad de información. En Latinoamérica, se encontró que tres de cada diez empresas, experimentó una brecha de seguridad y el 16% ha enfrentado problemas de seguridad en dispositivos móviles.

En este entorno, se debe saber que, para solucionar estos problemas, cada organización tendrá sus propias necesidades y/o requerimientos de seguridad. (Justino, Z., 2015)



Los sistemas de procesamiento de información son vulnerables a muchas amenazas que pueden infligir varios tipos de daños que dan lugar a pérdidas significativas. Este daño puede ir desde errores que dañan la integridad de la base de datos hasta incendios que destruyen complejos completos. Las pérdidas pueden provenir de las acciones de los empleados supuestamente confiados que defraudan el sistema, de los hackers externos, o de la entrada descuidada de datos. (Peltier, T., 2016)

La clínica de medicina ocupacional MEDCAM Perú SAC es una organización que maneja información muy sensible, siendo la de más alta criticidad la información de sus pacientes (como datos personales, las historias clínicas, resultado de exámenes médicos o resultados de laboratorios), estos datos deben ser resguardados y protegidos por la organización según la Ley 29733– “Ley de Protección de datos personales” , (Congreso de la República del Perú, 2011)”. De no cumplirse la organización está expuesta a multas que van desde las 5 a 100 UIT.

Asimismo, se necesita que la información de los pacientes y las de sus principales activos de información sean integras ya que son de vital importancia al momento de realizar los distintos exámenes médicos y a la hora de realizar el diagnóstico de los pacientes. A su vez, se requiere que siempre estén disponibles cuando se les necesite, ya que es parte de los servicios que ofrecen el tener la información siempre en línea y sin fecha de vencimiento. Adicional a la información de los pacientes, la clínica también debe resguardar la información crítica de los datos de sus proveedores de equipos médicos, la información de las empresas con las que trabaja o información de los recursos asignados y usados e información contable.

Actualmente, la empresa no tiene identificadas las vulnerabilidades a las que están expuestos sus activos de información, ya que si bien, cuentan con algunos mitigantes para salvaguardar sus activos de información, estos no han sido definidos bajo un marco de trabajo que permita una mejora continua, la identificación integral de sus riesgos y el establecimiento de mitigantes oportunos con la finalidad de asegurar la integridad, confidencialidad y disponibilidad de la información. Estas medidas aportan a

los objetivos de la empresa de brindar un servicio de calidad, manteniendo en reserva la información de sus clientes, asegurando la continuidad del negocio y previniendo sanciones de entidades regulatorias.

Se define el problema como la alta vulnerabilidad en los activos de información por la falta de gestión de seguridad de la información en la clínica MEDCAM Perú SAC en Lima.

Como problemas específicos se plantean los siguientes:

- Inadecuada gestión de seguridad de la información por la falta de un sistema de gestión.
- Escasos lineamientos de seguridad debido a que no se cuenta con una política de seguridad de la información.
- Ineficiente tratamiento de riesgos por falta de identificación de las amenazas y vulnerabilidad sobre los activos de información.
- Pobre conocimiento de seguridad de la información por falta de capacitación.

El objetivo general es mitigar los riesgos a los que está expuesto los activos de información de la clínica MEDCAM Perú S.A.C.

Los objetivos específicos son:

- Implementar el sistema de gestión de seguridad de información basada en la ISO/IEC 27001.
- Implementar una política de Seguridad de la Información.
- Establecer controles para el tratamiento de los riesgos identificados en base a la ISO/IEC 27002.
- Sensibilizar a los colaboradores de la empresa en temas de seguridad de la información.

La justificación teórica es que la mayoría de organizaciones tienen algunos controles para gestionar su seguridad de la información. Sin embargo, su efectividad algunas veces no es la mejor ya que son introducidas solo para solucionar problemas específicos, mientras que otras se introducen por simple convención o al azar sin haber priorizado correctamente sus procesos y

activos más importantes.

Estas políticas y controles solo tratarán ciertos aspectos de la seguridad de procesos TI o de ciertos activos y puede dejar recursos valiosos que no están plenamente identificados y que los dejará menos protegidos y vulnerables. Es por eso que es importante trabajar bajo un marco de trabajo, en este caso la ISO/IEC 27001, que aborda estas deficiencias y busca blindar a la empresa no solo con controles enfocados a los riesgos de los procesos, sino por distintos motivos como responsabilidades legales, contractuales, entre otros.

Este marco de trabajo precisa ciertos requisitos específicos que la empresa debe cumplir, lo que proporciona una gran ventaja competitiva ya que no solo asegura que los riesgos están siendo gestionados de una manera eficiente, sino que la empresa puede evidenciar a las personas interesadas, que tienen un manejo íntegro, confiable y confidencial de sus activos de información y que pueden ser formalmente auditadas y certificadas.

Como justificación práctica se plantea que uno de los activos más importantes de las empresas es la información, y actualmente los activos de información tienden a tener base tecnológica y es importante replantear los métodos de aseguramiento de estos activos que finalmente son los que permiten el cumplimiento de los objetivos del negocio.

La información manejada por la empresa MEDCAM Perú S.A.C., una clínica orientada hacia la salud ocupacional, por la naturaleza del rubro salud, la correcta gestión de la información es un proceso sumamente importante, pues se maneja información confidencial como es la información de los clientes, los procesos internos de la empresa, los resultados de los exámenes de laboratorio, las historias clínicas, entre otros. Por lo tanto, la seguridad de la información es responsabilidad de la organización.

El resultado de este proyecto asegura que la empresa, al implementar un sistema de gestión de seguridad de la información, tiene capacidad de respuesta ante los riesgos a los que están expuestos los activos de información.

Adicionalmente, la empresa garantiza el cumplimiento de la ley 29733 - Protección de Datos Personales del estado peruano, ley que en su artículo 39 indica que se deben establecer medidas de seguridad para el resguardo adecuado de los datos personales.

Según lo trabajado en el negocio, el alcance del proyecto para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) abarca los principales procesos de la empresa, los cuales han sido previamente identificados como los más críticos e importantes, en conjunto con la empresa, para el cumplimiento de los objetivos del negocio y su continuidad. El proyecto trabajó sobre los activos de información de los siguientes procesos: Captación de clientes. Atención al cliente. Procesamiento de datos. Facturación. Cobranza. Logística.

De acuerdo con las limitaciones el tiempo con el que se cuenta es escaso para el diseño e implementación del proyecto, se implementó en la empresa controles para los activos de información que presentan un riesgo crítico. Asimismo, se ejecutaron siete (7) fases metodológicas, de las 11, hasta establecer el sistema de gestión de seguridad de la información dejando de lado las fases de asignación de recursos, monitoreo, certificación y auditoría; por no ser fases necesarias para la implementación. Adicionalmente, los controles que demandan una inversión para la empresa no fueron implementados a corto plazo.

# **CAPÍTULO I**

## **MARCO TEÓRICO**

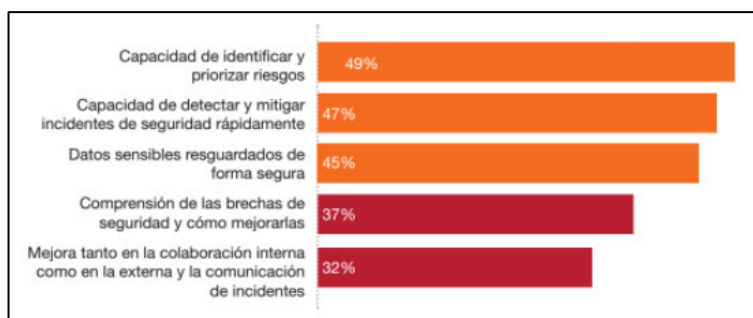
### **1.1 Antecedentes**

#### **1.1.1 Ámbito de la Seguridad de la Información**

En la actualidad, en un mundo totalmente globalizado, con una economía incrementada, el aumento de la complejidad en las infraestructuras de TI, la proliferación de dispositivos móviles y un número cada vez mayor de vulnerabilidades, no es de extrañar que las organizaciones luchen para encontrar el equilibrio para proteger sus activos de información. (Layton, T., 2016)

En estos días, el ataque a los activos de información a las empresas es cada vez más frecuente, según una encuesta a nivel global realizada por la firma de servicios profesionales PriceWaterhouseCoopers (2016), indican que año tras año los ataques cibernéticos continúan creciendo en términos de frecuencia, severidad e impacto, resultando cada vez más ineficientes, los métodos para la prevención y detección. Muchas organizaciones no saben qué hacer o no cuentan con los recursos necesarios para combatirlos. Según el estudio realizado resaltan que un programa de seguridad efectivo comienza con una estrategia y fundamentos basados en riesgos y que las compañías deben adoptar la implementación de un framework (marco de trabajo) de seguridad de la información basada en el riesgo, ya que las amenazas no vienen sólo de agentes externos sino también del personal interno, por lo que

este marco de trabajo les permite estar blindado por varios frentes. Los beneficios de la seguridad basada en un marco de trabajo que recogieron en dicha encuesta se pueden apreciar en la siguiente Figura (Ver Figura 1)



**Figura 1. Beneficios de la Seguridad de Información**

Fuente: PriceWaterHouse (2016). *Resultados de la encuesta global de la seguridad de la información.*

Como se puede apreciar, lo más destacado es que las organizaciones fueron capaces de identificar y priorizar sus riesgos a los que estaban expuestos, pero más allá de solo la evaluación de los riesgos, también pudieron hacerles frente a los incidentes de seguridad más rápidamente ya que poseen controles detectivos precisos. A su vez, permite que los datos sensibles estén resguardados correctamente y genera un proceso de mejora continua ya que se concientiza y existe una mejor comunicación entre el personal interno.

Los marcos de trabajo y las normas surgen a través del desarrollo de descripciones detalladas de características particulares de un producto o servicio por expertos de empresas e instituciones científicas. Representan un consenso sobre características tales como calidad, seguridad y fiabilidad que deben seguir siendo aplicables durante un período prolongado de tiempo y, por lo tanto, se documentan y se publican. El objetivo del desarrollo de estándares es apoyar tanto a individuos como a empresas en la adquisición de productos y servicios. Los proveedores de productos y servicios pueden aumentar su reputación al haber certificado su cumplimiento con las normas.

Dister, G., (2016), para la protección de los sistemas de información e información, las normas ISO 27000, ISO 27001 e ISO 27002 proporcionan objetivos de control, controles específicos, requisitos y directrices, con los que

la empresa puede lograr una adecuada seguridad de la información. De esta forma, la ISO 27001 permite certificar a la empresa frente a la norma, por lo que la seguridad de la información puede ser documentada como rigurosamente aplicada y gestionada de acuerdo con un estándar de organización internacionalmente reconocido.

Como menciona Capita Secure Information Systems (2015), el marco de trabajo que propone la ISO/IEC 27001 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Se tiene que tener en cuenta tres (3) cuestiones claves del estándar:

- Sus requisitos genéricos significan que es aplicable a todas las organizaciones, independientemente de su tamaño, tipo o naturaleza. Sin embargo, se adapta a las necesidades exactas de la organización a través de los controles de seguridad de la información que se identifiquen.
- Adopta un enfoque flexible y orientado hacia el riesgo.
- Es dinámico, se centra en la mejora continua y ayuda a la organización a mantenerse a la vanguardia de los cambios, tanto dentro como fuera de la organización.

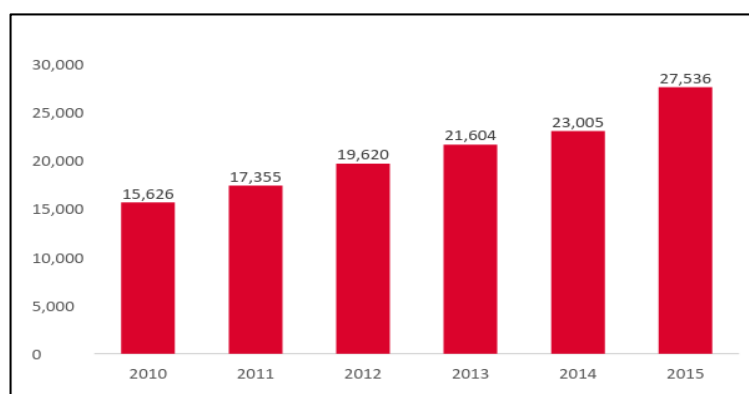
Adicionalmente, el diseño e implementación y la posterior certificación en la ISO/IEC 27001 ha contribuido a las empresas a obtener una ventaja competitiva ya que, como se comentó previamente en la justificación, evidencia a las personas interesadas que los activos que maneja la empresa cumplen los requisitos que ofrece dicha norma. A su vez, permite contar con diversos planes de acción en caso de que se produzca un incidente que pueda comprometer a la continuidad del negocio. Esto ha sido interiorizado por las empresas que ahora buscan esta certificación.

Bussiness Beam (2016), nos muestra un caso de estudio, el de Teradata, una empresa estadounidense especialista en las herramientas de data warehouse y herramientas analíticas empresariales, presente en más de 60 países del mundo. Tenía sus preocupaciones respecto a los sistemas y

datos que manejaban, ya que era información sensible de los clientes, y estos, necesitaban una garantía que la empresa contaba con servicios seguros e ininterrumpidos. Así que, para atraer más clientes y demostrar que la información de los usuarios fue resguardada, decidieron implementar un sistema de seguridad de la información. En primer lugar, se capacitaron sobre las buenas prácticas y el marco de trabajo idóneo para ellos (en este caso, la ISO/IEC 27001) y se realizó un análisis de brecha de los controles que poseía, se hizo una evaluación de sus riesgos y desarrollaron un mecanismo efectivo para calcular y minimizar sus niveles de riesgos. A su vez, se implementaron estándares que iban alineados a los objetivos y políticas del negocio. Los resultados fueron los mejores ya que obtuvieron la certificación de la ISO sin ningún inconveniente, a su vez, que se logró el objetivo principal de asegurar la información de los clientes y sensibilizar a toda la empresa en temas de seguridad.

Esta situación, a niveles regionales, puede ser analizada mediante una encuesta realizada anualmente por la Organización Internacional de Normalización, una encuesta a nivel mundial que cuenta con el apoyo de los distintos miembros del Foro Internacional de Acreditación (IAF), en el Perú representado por el INACAL (Instituto Nacional de Calidad), y nos permite tener una visión de cómo se encuentra la certificación en la ISO/IEC 27001 a nivel mundial.

Según la encuesta (International Organization for Standardization, 2016) el número de empresas certificadas a nivel mundial asciende cada año, esto se puede visualizar a continuación (Ver Figura 2)



**Figura 2. Certificaciones de ISO/IEC 27001 a nivel global**

Fuente: Organización Internacional de Normalización (2015). *The ISO Survey of management system standard certifications.*



Se observa un incremento de un 43% desde el 2010, siendo hasta la fecha del último informe (2015) 27,536, con lo que confirmamos el interés cada vez mayor de las empresas.

A su vez, se identificó que el área de Asia oriental y Pacífico (China, Japón, Corea del Norte, Corea del Sur, entre otros.) tienen las empresas con mayor número de certificaciones (Ver Tabla 1):

**Tabla 1. Certificaciones de ISO/IEC 27001 a niveles regionales**

Continentes	2010	2011	2012	2013	2014	2015
Asia Este y Pacífico	8,788	9,665	10,422	10,116	10,414	11,994
Europa	4,800	5,289	6,379	7,952	8,663	10,446
Asia Central y Sur	1,328	1,497	1,668	2,002	2,251	2,569
America del Norte	329	435	552	712	814	1,445
Medio Oriente	218	279	332	451	511	606
Centro y Sudamerica	117	150	203	272	273	347
Africa	46	40	64	99	79	11

Fuente: Organización Internacional de Normalización (2015). *The ISO Survey of management system standard certifications.*

También podemos revisar por rubros y específicamente a la que este proyecto hace referencia, al sector salud (Ver Tabla 2):

**Tabla 1 - Certificaciones de ISO/IEC 27001 a nivel de servicios**

Servicio	2010	2011	2012	2013	2014	2015
TI	3,217	3,588	4,558	5,059	4,933	5,573
Construcción	266	350	409	396	454	186
Transporte, Almacenamiento y Comunicación	184	241	288	322	327	301
Sector Finanzas	185	113	138	169	187	197
Salud y Trabajo Social	102	145	201	201	215	231
Administración Pública	79	106	155	192	191	212

Fuente: Organización Internacional de Normalización (2015). *The ISO Survey of management system standard certifications.*

A nivel regional, según un estudio realizado por la compañía ESET Latinoamérica en su reporte anual “ESET Security Report – Latinoamérica 2016” donde se consideró a empresas de distintos rubros y tamaños que pertenecen a varios países de Latinoamérica (Ver Figura 3), las preocupaciones de los encargados de la seguridad de la información en las empresas son las “Vulnerabilidades de software y sistemas” con el 58% de las respuestas afirmativas, seguido por el “Malware” (54%) y, en el tercer puesto, el “Acceso indebido la información” (46%). Tal como cita ESET Latinoamérica (2016), lo que se destaca, es que por primera vez desde que se realiza este informe, el fraude informático no ocupa el tercer lugar; ya que fue desplazado

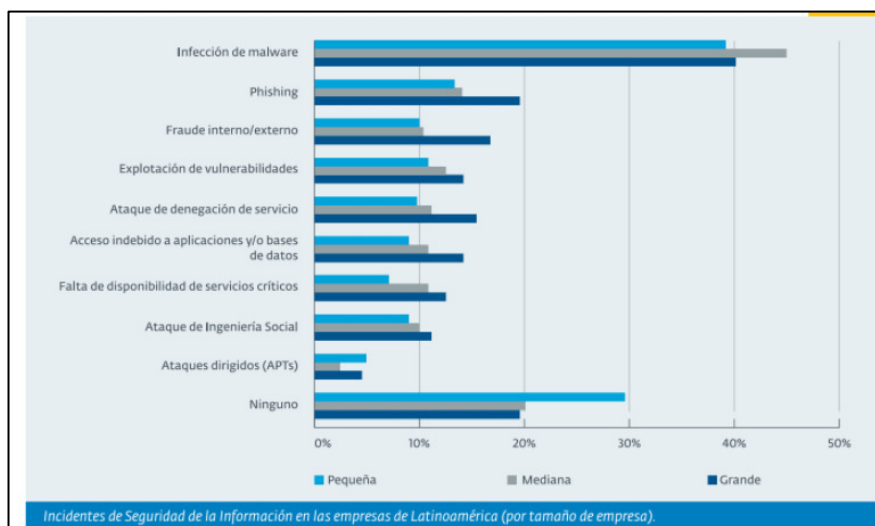
por el acceso indebido a la información. Esto se explica desde el aumento de la explotación de vulnerabilidades (la preocupación más importante), que generalmente tiene como consecuencia el acceso indebido. (Ver Figura 3)



**Figura 3. Preocupaciones de encargados de la seguridad de información en Latinoamérica**

Fuente: ESET Latinoamérica (2016). *ESET Security Report – Latinoamérica 2016*

Entre los incidentes de seguridad de información más comunes en los países de la región, se puede observar que se encuentra los fallos en los sistemas, los fraudes tanto internos como externos y falta de disponibilidad de los servicios críticos. (Ver Figura 4)



**Figura 4. Incidentes de seguridad de la información en las empresas de Latinoamérica**

Fuente: ESET Latinoamérica (2016). *ESET Security Report – Latinoamérica 2016*

Esta preocupación se ve claramente reflejada al momento de observar el número de certificaciones que están obteniendo las empresas en un sistema de gestión de seguridad de información. Se observa un incremento

del 300% desde el año 2010 hasta la fecha de la última encuesta (Ver Tabla 3).

**Tabla 2. Certificaciones de ISO/IEC 27001 a nivel de países**

Pais	2010	2011	2012	2013	2014	2015
Brazil	41	50	53	82	85	94
Colombia	23	27	58	82	78	103
Argentina	8	24	33	40	23	52
Chile	13	18	23	24	24	32
Peru	9	5	7	9	12	22
Uruguay	4	7	7	8	11	21
Costa Rica	6	7	7	10	22	4
Ecuador	1	1	3	5	7	6
Dominican Republic	1	2	3	4	3	4
Puerto Rico	2	2	2	2		0
Guatemala	1	1	1	2	3	2
Bolivia	1	3	1	1	1	1
El Salvador	1	1	1	1	1	1
Panama	1	1	2	1		0
Cuba	2			0		0
Trinidad and Tobago			1	1	1	1
Honduras		1	1	0	1	0
Barbados	1					0
Guyana	1			0		0
Jamaica	1			0		0
Venezuela					1	1
Belize						1
Saint Lucia						1
<b>Total</b>	<b>117</b>	<b>150</b>	<b>203</b>	<b>272</b>	<b>273</b>	<b>347</b>

Fuente: Organización Internacional de Normalización (2015). *The ISO Survey of management system standard certifications*.

Perú se encuentra en el quinto lugar con 22 certificaciones actualmente. Las empresas peruanas que conforman esta lista son INDECOPI, Atento, Hermes, Telefónica, entre otras.

Si bien estos datos indican el número de certificaciones a la ISO/IEC 27001, se debe ser cauteloso al asumir que solo son estas empresas las que tienen implementada la SGSI, ya que varias empresas han realizado el diseño y la implementación, mas no la certificación, pero los datos que arroja esta encuesta ayudan a ver el panorama en general.

En el ámbito local, podemos ver que el estado peruano cada vez más se preocupa por la seguridad de la información, primero con la ley de protección de datos personales (Ley N° 29733, 2011), y ahora impulsa la implementación de los SGSI principalmente de las entidades que manejan información sensible de los ciudadanos, es por esto que el 8 de enero del 2016 sale publicado en “El Peruano” la Resolución Ministerial “004-2016-PCM” que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001 – Tecnología de Información – Técnicas de Seguridad - Sistemas de Gestión de Seguridad de Información en todas las entidades integrantes del Sistema Nacional de Informática, que son los órganos informáticos de las municipalidades, de los poderes públicos y autónomos, de

todas las oficinas de informática de los ministerios, el Congreso de la República, Poder Judicial, entre otros. Cabe resaltar que las instituciones que cuenten con la certificación serán exoneradas.

La resolución indica que se tiene dos (2) años para la implementación y adecuación de la norma, pero previamente se deberá presentar a la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática) el cronograma de adecuación. Esta norma señala como opcional la certificación de la ISO/IEC 27001 y que si se desea realizar dicha certificación serán realizados con los recursos propios de la entidad.

### **1.1.2 Seguridad de la Información en el área de salud**

En la actualidad, las organizaciones sanitarias no solo prestan servicios sanitarios, sino que también tratan de competir entre sí para obtener puntuaciones altas en auditorías y acreditaciones. Uno de los enfoques que resultan útiles para mejorar la calidad de la atención de la salud es el uso de la tecnología de la información y los sistemas de información. El sistema de información del hospital es el más utilizado en los hospitales para completar las tareas diarias y para facilitar la comunicación entre los diferentes departamentos dentro y fuera de la organización. En general, el uso de sistemas de información hospitalaria tiene muchas ventajas para los proveedores de atención médica y los pacientes. Este sistema tiene potenciales para aumentar la accesibilidad de la información clínica y para mejorar la investigación clínica y de salud pública. Sin embargo, el uso de este sistema ha dado lugar a nuevos desafíos, como las preocupaciones sobre la seguridad de la información de salud. Temas como el mantenimiento de la confidencialidad y la prevención del acceso no autorizado a los datos clínicos figuran entre las principales preocupaciones que requieren atención adecuada durante todas las etapas de la entrada, el almacenamiento, el uso y la transferencia de datos. (Mehraeen, E., Ayatollah, H., Ahmadi, M., 2016).

En previas investigaciones hechas de la seguridad de información en el tratamiento de datos de salud por Sanchez, A., Fernández, J., Toval, A., Hernández, I., Sánchez, B., Carrillo, J. (2014), en las que se afirma que, las

organizaciones sanitarias, generalmente, no emplean trabajadores con habilidades en tecnologías de la información o con formación en materia de seguridad, suelen olvidar las amenazas internas a la hora de planificar la estrategia de seguridad. Esta situación se agrava en entornos abiertos a Internet, donde el número y la naturaleza de las amenazas van en aumento y están en continua evolución. Algunos ejemplos de ataques recientes en que comparten su investigación son los siguientes:

- Acceso a los datos de la hija menor de una doctora que trabajaba en un centro hospitalario, por parte de trabajadores del mismo sin consentimiento de la madre (2007). Tanto personal médico como administrativo accedieron a los datos médicos de la menor para consultar, modificar e imprimir información, sin previa autorización de su madre, trabajadora del centro.
- En 2008, un empleado de una clínica, que intentaba descargarse archivos desde el ordenador del trabajo a través de eMule, una plataforma usada para el intercambio de archivos pudo provocar que 11.300 historias clínicas, de ellas 4.000 casos de aborto, terminasen expuestas a cualquier internauta.
- Un virus se introdujo en los ordenadores de los hospitales y centros de salud madrileños. La incidencia impidió el acceso a las historias clínicas y las analíticas de los pacientes.
- Una unidad flash fue hurtada del Departamento de Personal de un Hospital Provincial de España (2010). La unidad contenía datos personales que fueron robados tras forzar la puerta de un despacho.
- Filtradas a través de Google dos (2) radiografías de pulmón de un paciente en 2011. Se tuvo que indemnizar a un paciente que, al hacer una búsqueda por Google, encontró dos (2) radiografías de pulmón que le habían realizado.

En el sector de salud peruano, debido a la constante amenaza y soportada por la norma publicada por la ONGEI, el MINSA (Ministerio de Salud del Perú) ha implementado el SGSI que propone dicha norma (Seguro Social de Salud del Perú, 2015).

En este caso, ESSALUD integró un Comité de Gestión de Seguridad de la Información conformado por las diversas áreas (Planeamiento y Desarrollo, Tecnología de Información y Comunicaciones, entre otros), con el objetivo de proponer, supervisar e implementar las políticas de seguridad de información, proponer capacitaciones para promover la importancia de la seguridad de la información, plantear metodologías de clasificación y niveles de riesgos para sus activos de información y todo esto en aras de contar con un SGSI. (Resolución de Gerencia General ESSALUD N°1504, 2015).

La empresa de estudio, MEDCAM Perú SAC, es una clínica de medicina orientada a satisfacer la necesidad, determinada por la Ley 29783 – “Ley de Seguridad y Salud en el trabajo” y su modificatoria Ley 30222, es la empresa en la cual se implementará el SGSI.

Cuenta con dos (2) locales en el distrito de Los Olivos y San Luis. Se encarga de brindar los siguientes servicios de exámenes médicos ocupacionales (EMO):

- Pre-ocupacionales: Son exámenes de carácter obligatorio que solicitan las empresas para los postulantes a un puesto de trabajo. Se busca constatar si la condición psicofísica del postulante cumple con los requerimientos exigidos.
- Periódicos-anales: Son exámenes de control que realiza la empresa para revisar la salud en la labor de sus trabajadores. A su vez, tiene la finalidad de monitorear la exposición a los factores de riesgos y su detección preventiva.
- Retiro: Cuando un trabajador cesa en el puesto laboral, se realiza exámenes con la finalidad de detectar si existe alguna secuela debido al entorno y las condiciones del trabajo al que estuvo expuesto.

Dentro de estos exámenes se realizan:

- Laboratorio Clínico
- Evaluación Médica
- Evaluación Ergonómica
- Evaluación Radiológica

- Evaluación Espirométrica
- Evaluación Oftalmológica
- Evaluación Psicológica-ocupacional, entre otros.

Actualmente, la empresa solo cuenta con unos cuantos controles manuales para resguardar su información que son respaldadas en la nube y la digitalización de algunos de sus documentos físicos.

### **1.1.3 Ley de Protección de datos**

La Ley de protección de datos personales tiene como objetivo, según precisa la Ley N°29733 (Congreso de la República del Perú, 2011), garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú (Que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar), a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen. Es decir, es una legislación que busca establecer los límites, permisos y castigos a los que se refiere la seguridad de datos personales de una persona.

A continuación, se presenta el contexto regional de leyes de protección de datos que se obtuvo en la encuesta de Ley de Protección de Datos Personales – Enfoque Práctico de Adecuación (Deloitte, 2016), los países que cuentan con una legislación, desde qué fecha están promulgadas y las que están en proyecto. (Ver Figura 5)



**Figura 5. Contexto regional de la legislación de protección de datos personales**  
Fuente: Deloitte (2016). *Ley de Protección de Datos Personales – Enfoque Práctico de Adecuación.*

Según la Ley N° 29733, La ley peruana sobre la protección de datos, menciona que los datos personales son aquella información numérica, alfabética, fotográfica, entre otros, concerniente a las personas naturales que las identifica o puedan servir para hacerlas identificables y sobre todo, para nuestro caso del proyecto, los datos personales relacionados con la salud. Es aquella información relativa a la salud pasada, presente o pronosticada, física o mental de una persona incluyendo la discapacidad o formación genética, que manejan las empresas y estén almacenados en su banco de datos, estén regulados y cumplan con ciertos principios rectores, estipulados por la ley.

- Principio de consentimiento: Cuando los datos personales sean brindados por el titular de manera expresa, con su consentimiento libre, informado e inequívoco.
- Principio de finalidad: Se debe expresar la finalidad de manera clara y sin lugar a confusión para ser usados los datos personales.
- Principio de calidad: Los datos deben ser precisos.
- Principio de seguridad: La empresa debe adoptar medidas de seguridad necesarias a fin de evitar la adulteración, pérdida, inexactitudes de origen humano o técnico.



Como afirma Deloitte, el proceso para la legislación de Protección de Datos en el Perú tiene bases desde la constitución y fue promulgada de la siguiente manera: (Ver Figura 6)

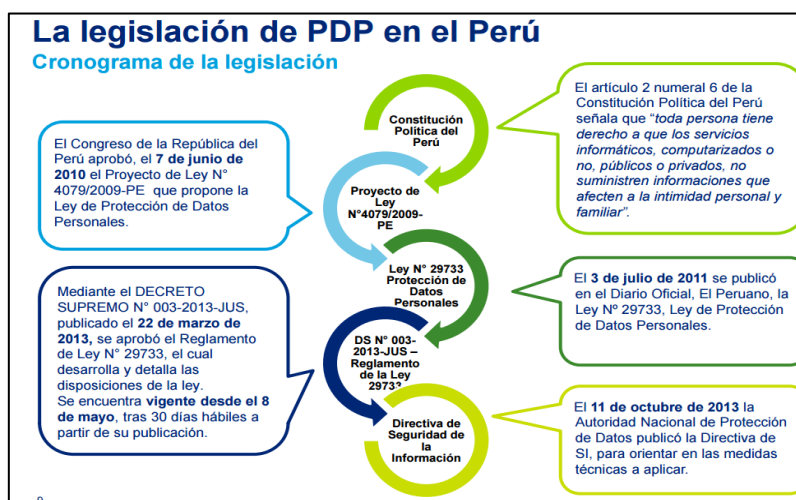


Figura 6. Cronograma de la legislación peruana

Fuente: Deloitte (2016). *Ley de Protección de Datos Personales – Enfoque Práctico de Adecuación.*

Como señala la Ley de Protección de datos personales, las organizaciones que aplican son todas las entidades públicas, privadas y las personas naturales que se encuentren en territorio peruano. Las infracciones por no cumplir con la legislación se clasifican en leve, grave y muy grave, según muestra la Tabla 4. El incumplimiento de la ley acarrea las siguientes sanciones: (Ver Tabla 5).

Tabla 3 Infracciones por incumplimiento de la ley de protección de datos

Infracciones Leves	Infracciones Graves	Infracciones Muy Graves
<ul style="list-style-type: none"> <li>Dar tratamiento a datos personales sin recabar el consentimiento de sus titulares, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley.</li> <li>No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales reconocidos en el título III, cuando legalmente proceda.</li> <li>Obstruir el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales</li> </ul>	<ul style="list-style-type: none"> <li>Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento.</li> <li>Incumplir la obligación de confidencialidad establecida en el artículo 17.</li> <li>No atender, impedir u obstaculizar, en forma sistemática, el ejercicio de los derechos del titular de datos personales reconocidos en el título III, cuando legalmente proceda.</li> <li>Obstruir, en forma sistemática, el ejercicio de la función fiscalizadora de la Autoridad Nacional de Protección de Datos Personales.</li> <li>No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales.</li> </ul>	<ul style="list-style-type: none"> <li>Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.</li> <li>Crear, modificar, cancelar o mantener bancos de datos personales sin cumplir con lo establecido por la presente Ley o su reglamento.</li> <li>Suministrar documentos o información falsa o incompleta a la Autoridad Nacional de Protección de Datos Personales.</li> <li>No cesar en el tratamiento ilícito de datos personales, cuando existiese un previo requerimiento de la Autoridad Nacional de Protección de Datos Personales para ello.</li> <li>No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales, no obstante haber sido requerido para ello por la Autoridad Nacional de Protección de Datos Personales</li> </ul>

Fuente: Deloitte (2016). *Ley de Protección de Datos Personales – Enfoque Práctico de Adecuación.*

**Tabla 4. Sanciones por incumplimiento de la ley de protección de datos**

Nivel de Infracción	Sanción Multa en S/.	Ejemplo
Leve	1,850 a 18,500	Solicitud de actualización de datos rechazada
Grave	18,501 a 185,000	Reiteradas y diversas solicitudes de actualización rechazadas
Muy grave	185,001 a 370,000	Entidad remite información falsa a la DGPDP
<b>Límite del 10% de los ingresos brutos anuales que hubiera percibido el presunto infractor durante el ejercicio anterior</b>		
<b>Multas coercitivas : Por incumplimiento de obligaciones accesorias a la sanción de multa</b>		
Nivel de Sanción	Monto de la Multa S/.	
Obligaciones accesorias a multa por infracciones Leves	740 a 7,400	
Obligaciones accesorias a multa por infracciones Graves	7,401 a 22,200	
Obligaciones accesorias a multa por infracciones Muy graves	22,201 a 37,000	
<b>La multa coercitiva es independiente de las sanciones que puedan imponerse con tal carácter y compatible con ellas.</b>		

Fuente: Deloitte (2016). *Ley de Protección de Datos Personales – Enfoque Práctico de Adecuación.*

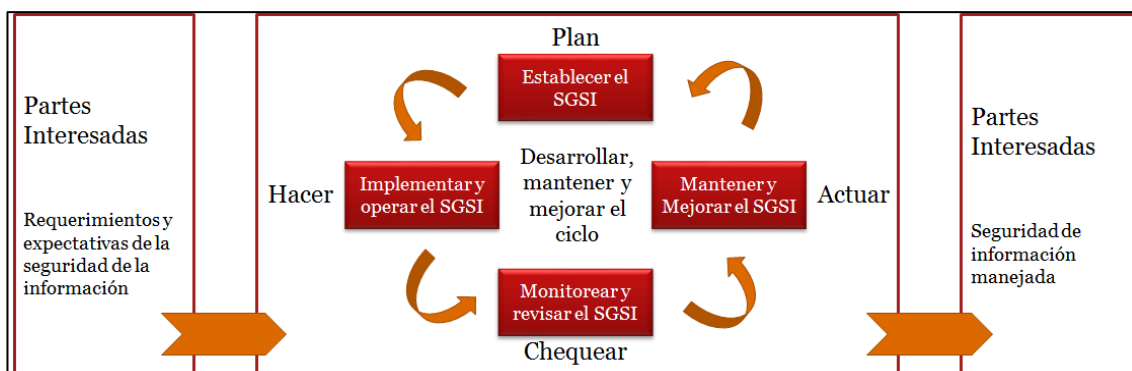
Para asegurar el cumplimiento de la ley se pueden usar diferentes métodos como el trabajar bajo el marco de trabajo de la ISO/IEC 27001. Adicionalmente, se tiene que incluir en el análisis de activos, los asociados a datos personales y al riesgo de privacidad.

## 1.2 Bases teóricas

### 1.2.1 ISO/IEC 27001: 2005

Del Estándar Internacional, publicado en el 2005 se utiliza el modelo de aplicación que recomienda para la implementación de un Sistema de Gestión de Seguridad de la Información, que se detalla a continuación: Planear-Hacer-Chequear-Actuar (PDCA), también conocido con el ciclo de Deming. Espinoza, R., (2013), explica que el estándar sigue un enfoque de procesos basado en el ciclo Deming del célebre Plan-Do-Check-Act. El modelo está basado en un enfoque racional para su desempeño y su perfeccionamiento en el tiempo. Primero se exige que el modelo siga una serie de prerequisites para que se establezca, a través de la fase denominada “Planear”. Luego de establecido el modelo, se implementa y opera, siguiendo los lineamientos de la fase “Hacer”. Luego que el modelo se ha implantado y

está funcionando, se debe monitorear y revisar durante la fase “Revisar”. Por último, se procede a la fase “actuar” y tomar los correctivos necesarios. (Ver Figura 7)



**Figura 7. Modelo PDCA aplicado a los Procesos SGSI**

Elaboración: Los autores

A continuación, se brinda un pequeño detalle de cada etapa del modelo PDCA:

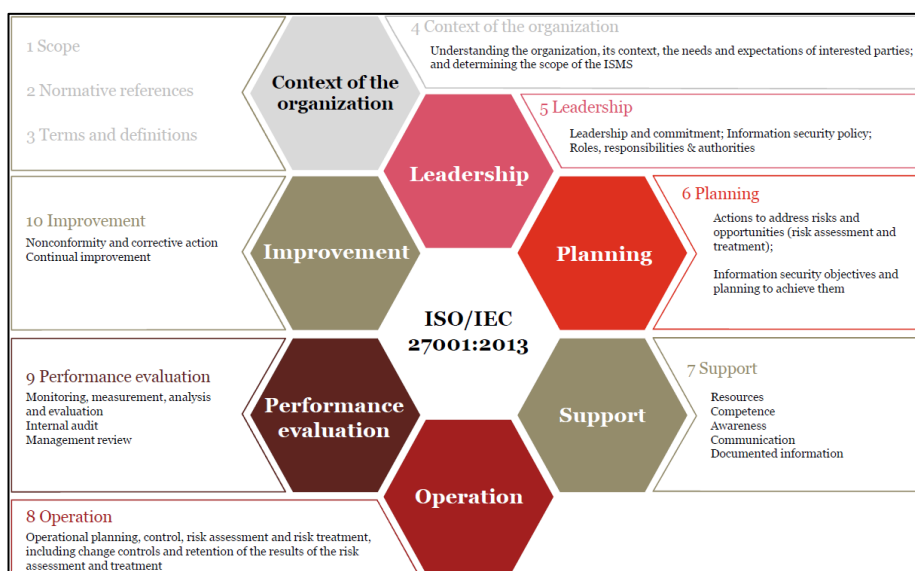
- Planear (establecer el SGSI):
  - Identificar los objetivos del negocio
  - Obtener compromiso de la alta gerencia
  - Seleccionar el alcance adecuado para la implementación
  - Definir un método para la identificación y evaluación de riesgos.
  - Elaborar un inventario de activos que se desea proteger y clasificarlos según su nivel de riesgos.
- Hacer (implementar y operar el SGSI):
  - Gestionar los riesgos y crear un plan de tratamiento de los mismos.
  - Definir políticas, controles y procedimiento para la mitigación de los riesgos.
  - Asignar los recursos y capacitar a las personas que están en el staff.
- Chequear (monitorear y revisar el SGSI):
  - Monitorear la implementación del SGSI

- Actuar (mantener y mejorar el SGSI):
  - Realizar evaluaciones periódicas.
  - Tomar acciones correctivas y preventivas.

### 1.2.2 ISO/IEC 27001: 2013

La ISO/IEC 27001:2013 explica que esta Norma Internacional especifica los requisitos para establecer, implementar, mantener y mejorar, continuamente, un sistema de gestión de la seguridad de la información dentro del contexto de la organización. El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente. (ISO/IEC 27001, 2013)

El Estándar Internacional cuenta con 10 cláusulas de las cuales las tres (3) primeras tratan sobre el contexto de la norma y los 7 restantes muestran los requisitos para la implementación del SGSI. (ISO/IEC 27001, 2013). (Ver Figura 8)



**Figura 8. Cláusulas de la ISO/IEC 2700**

Fuente: Organización Internacional de Normalización (2013). *ISO/IEC 27001*

A continuación, se detallan brevemente las 10 cláusulas:

- **Cláusula 1:** **Ámbito:** incluye requerimientos para la valoración y tratamiento de riesgos de la seguridad de la información de cualquier empresa o Compañía, (Columba Bernardo, 2017).
- **Cláusula 2:** **Referencias normativas:** Se hace una referencia normativa en parte, o en su totalidad, a la norma ISO/IEC 27000, Information Technology. Security Technology Techniques. Information Security Management Systems. Overview and Vocabulary.
- **Cláusula 3:** **Términos y definiciones:** Se aplican términos y definiciones proporcionados en ISO/IEC 27000. (ISO/IEC 27001, 2013)
- **Cláusula 4:** **Contexto de la Organización:** Se determinan aspectos como el conocimiento de la organización, comprensión de las necesidades y expectativas de las partes interesadas. (Columba Bernardo, 2017).
- **Cláusula 5:** **Liderazgo:** La alta dirección debe demostrar liderazgo y compromiso respecto al SGSI.
- **Cláusula 6:** **Planificación:** Cuando se planifica el SGSI, la organización debe considerar lo referente a comprender la organización y comprender las necesidades y expectativas de las partes interesadas para asegurar que el SGSI pueda lograr los objetivos esperados.
- **Cláusula 7:** **Soporte:** En este punto, muestra los recursos, competencias e información documentada; así como el trabajo de concientización y comunicación que debe realizar la organización para la implementación del SGSI.
- **Cláusula 8:** **Operación:** La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información. (ISO/IEC 27001, 2013)
- **Cláusula 9:** **Evaluación de desempeño:** La organización debe evaluar el desempeño de la seguridad de la información y la

efectividad del sistema de gestión de seguridad de la información determinando los métodos de monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos.

- **Cláusula 10:** Mejoras: Cuando en las evaluaciones (Cláusula 9) se identifican no conformidades, la organización debe tomar acciones correctivas, y estas deben ser apropiadas de acuerdo con los efectos de las no conformidades encontradas.

### 1.2.3 ISO/IEC 27002

La norma de seguridad de la información ISO / IEC 27002: 2013 es el "Código de prácticas para los controles de seguridad de la información". Primero fue publicado por la Organización Internacional de Normalización (ISO) y por la Comisión Electrotécnica Internacional (IEC) en diciembre de 2000 como ISO 17799. Hoy en día, la ISO / IEC 27002 forma parte de la familia/serie 27000.

El documento ofrece recomendaciones de buenas prácticas y orientación para que las organizaciones puedan seleccionar e implementar controles de seguridad de la información en el proceso de iniciar, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).

La ISO / IEC 27002 está organizada de la siguiente manera (Ver Figura 9):



**Figura 9. Cláusulas de control de la ISO/IEC 27002**

Fuente: Traducido de: Lachapelle, E., Bislimi, M. (2016). *Information Technology - Security Techniques Code of Practice for Information Security Controls*

La norma contiene 14 cláusulas de control de seguridad, que contienen un total de 35 objetivos de control y 114 controles. Las cláusulas de control son:

- **Políticas de seguridad de la información:** Aborda la necesidad de definir, publicar y revisar los diferentes tipos de políticas requeridas para la gestión de la seguridad de la información.
- **Organización de la seguridad de la información:** Trata de la necesidad de definir y asignar las funciones y responsabilidades necesarias para los procesos y actividades de gestión de la seguridad de la información.
- **Seguridad de los recursos humanos:** Aborda los controles necesarios para los procesos relacionados con la contratación del personal, su trabajo durante el empleo y después de la culminación de sus contratos.
- **Gestión de activos:** Aborda las responsabilidades requeridas que se definen y asignan para los procesos y procedimientos de

administración de activos.

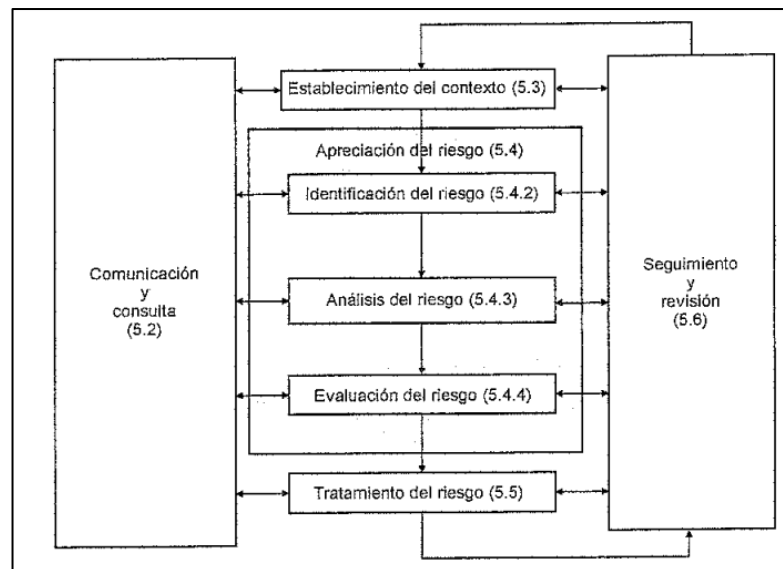
- **Control de accesos:** Trata sobre los requisitos para controlar el acceso a los activos de información y las instalaciones de procesamiento de información.
- **Criptografía:** Aborda sobre las políticas sobre los controles criptográficos para la protección de la información para garantizar el uso adecuado y eficaz de la criptografía con el fin de proteger la confidencialidad, autenticidad, integridad, no repudio y autenticación de la información.
- **Seguridad física y ambiental:** Aborda la necesidad de prevenir el acceso físico no autorizado, los daños y las interferencias a las instalaciones de información y procesamiento de información de la organización.
- **Seguridad de las operaciones:** Se refiere a la capacidad de la organización para asegurar operaciones correctas y seguras.
- **Seguridad de las comunicaciones:** Se refiere a la capacidad de la organización para garantizar la protección de la información en sistemas y aplicaciones en redes y sus instalaciones de procesamiento de información de apoyo
- **Adquisición, desarrollo y mantenimiento de sistemas:** Abarca los controles para la identificación, análisis y especificación de los requisitos de seguridad de la información, la seguridad de los servicios de aplicación en los procesos de desarrollo y soporte.
- **Relaciones con los proveedores:** Aborda los controles de las cuestiones de relación de proveedores, incluyendo aquí políticas y procedimientos de seguridad de la información.
- **Gestión de incidentes de seguridad de la información:** Abarca controles de responsabilidades y procedimientos, información de informes y debilidades de seguridad, evaluación y decisión sobre eventos de seguridad de información.



- **Aspectos de seguridad de la información en la gestión de continuidad de negocio:** Aborda la capacidad de la organización para contrarrestar las interrupciones de las operaciones normales, incluyendo la disponibilidad de instalaciones de procesamiento de información, verificar, revisar y evaluar la continuidad de la seguridad de la información.
- **Cumplimiento:** Se refiere a la capacidad de la organización para cumplir con los requisitos reglamentarios, estatutarios, contractuales y de seguridad.

#### 1.2.4 ISO/IEC 31000

La ISO/IEC 31000 es un marco de trabajo que ayuda a la gestión de los riesgos a las organizaciones, proporciona las directrices para una gestión más eficiente y no está pensada para un sector en particular, sino que puede ser aplicada a cualquier empresa sin importar el tamaño o rubro a que se dedique. El proceso de la gestión de riesgos propuesta por la ISO/IEC 31000, comprende las siguientes actividades reflejadas en la siguiente Figura: (Ver Figura 10)



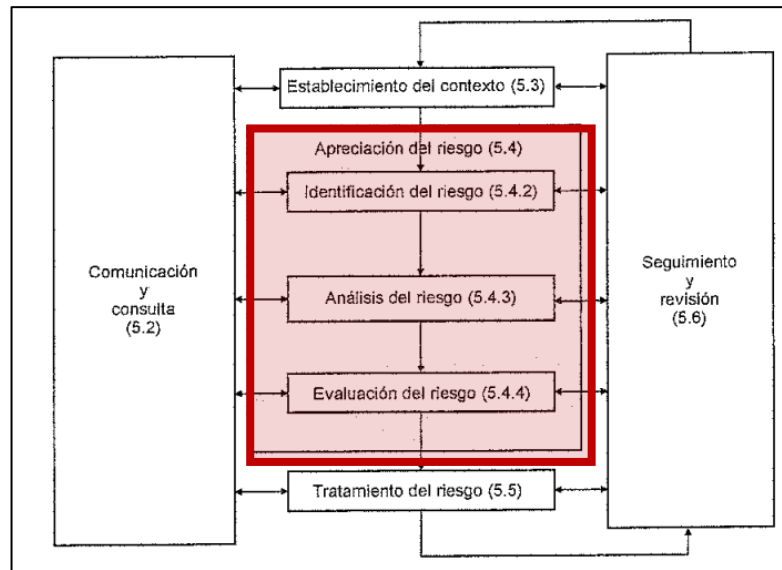
**Figura 10. Proceso de gestión de riesgos**

Fuente: Organización Internacional de Normalización (2013). *ISO/IEC 31000*

- **Comunicación y consulta:** Se debe realizar una comunicación permanente con las partes interesadas durante todo el proceso; se identifican los objetivos y se compromete a los interesados.
- **Establecimiento del contexto:** Se definen los parámetros externos e internos, alcance y criterios, todo esto enfocado en los objetivos del negocio.
- **Apreciación del riesgo:** Es la identificación, análisis y evaluación del riesgo.
- **Identificación del riesgo:** Se identifica el origen del riesgo, causas y consecuencias.
- **Análisis del riesgo:** Se busca la comprensión del riesgo, el nivel del riesgo, el impacto y la probabilidad de estos.
- **Evaluación del riesgo:** Luego de los pasos anteriores se busca cómo se debe tratar el riesgo y la prioridad de estos.
- **Tratamiento del riesgo:** Selección e implementación de controles o planes de acción para la mitigación del riesgo. Se puede evitar el riesgo al decidir no tomarlo, reducirlo, aceptarlo y retenerlo, o transferirlo con otras partes.
- **Seguimiento y revisión:** Se debe verificar, periódicamente, los controles que se tienen y realizar el seguimiento de la implementación de planes de acción. A su vez, se reportan los incidentes que puedan ocurrir o si se llegase a materializar el riesgo.

### 1.2.5 ISO/IEC 31010

La ISO/IEC 31010 fue publicada para ofrecer las mejores prácticas actuales para seleccionar y utilizar técnicas que permitan la evaluación de los riesgos. Este estándar asume que el marco de trabajo usado es la ISO/IEC 31000 y su área de aplicación sería la siguiente: (Ver Figura 11)



**Figura 11. Área de aplicación de la ISO/IEC 31010 en el proceso de gestión de riesgos**

Fuente: Organización Internacional de Normalización (2013). *ISO/IEC 31010*

Para la selección de una técnica, se debe considerar:

- Que sea justificable y apropiada para la situación actual de la organización.
- Que ofrezca resultados que permitan entender la naturaleza de los riesgos y cómo deben ser tratados.
- Debe ser trazable, repetible y verificable.
- Disponibilidad de recursos con los que se cuenta.
- Complejidad y detalle al que se quiere llegar.

### 1.2.6 ISO/IEC 27005

La ISO/IEC 27005 establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar en la aplicación satisfactoria de la seguridad de la información, basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable en todo tipo de organizaciones -por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro- que tienen la intención de gestionar los riesgos que puedan

comprometer la organización de la seguridad de la información. (Fernández, D., Pacheco, O., 2014).

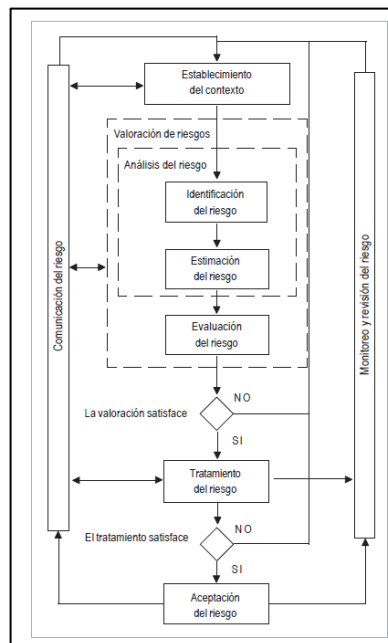
La ISO/IEC 27005 al ser parte de la familia 27000, encaja perfectamente en la implementación bajo el marco de trabajo de la ISO/IEC 27001 y va de la mano con el proceso de Plan-Do-Check-Act que se propone en este proyecto: (Ver Figura 12)

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Developing risk treatment plan Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

**Figura 12. ISO/IEC 27005 dentro de la implementación de SGSI**

Fuente: Organización Internacional de Normalización (2011). *ISO/IEC 27005*

Los pasos que establece la norma para una evaluación de riesgos son los siguientes: (Ver Figura 13)

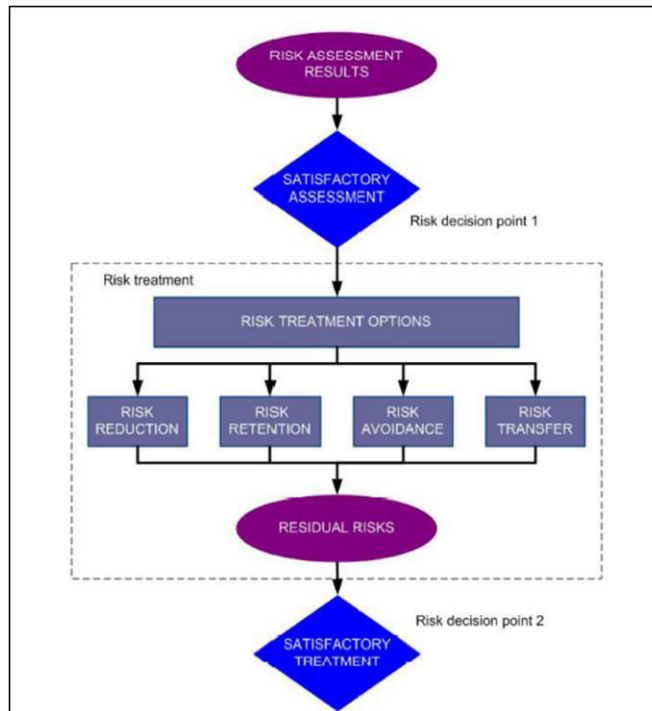


**Figura 13. Proceso de gestión de riesgo orientado a seguridad de información**

Fuente: Organización Internacional de Normalización (2011). *ISO/IEC 27005*

- **Definición del contexto organizacional interno y externo:** Al igual que el marco de la ISO/IEC 31000, se debe establecer el contexto en donde opera la empresa, tanto interna como externa. Debe estar alineado a la misión, visión, objetivos del negocio, políticas, entre otros. Para el caso externo, se deben considerar las regulaciones, economía, política, etc.
- **Identificación del riesgo:** El propósito es determinar qué podría suceder para que se origine una pérdida potencial y saber cómo, dónde o quién podría ocasionarla.
- **Identificación de activos:** Se deben identificar los activos que podrían ser afectados listándolos con los responsables de estos, lugar, función, entre otros campos que se consideren necesarios.
- **Identificación de amenazas:** La información sobre las amenazas es obtenida a través de informes de incidentes, dueños de los activos, usuarios, entre otros. Estas amenazas tienen el potencial de dañar los activos de la información, procesos y sistemas
- **Identificación de controles existentes:** Se deben identificar los controles de seguridad que se poseen para evitar trabajo y costos innecesarios.
- **Identificación de consecuencias:** La consecuencia puede ser pérdida en la eficiencia del proceso, falla en la continuidad del negocio, daño a la reputación, etc.
- **Estimación del riesgo:** La estimación del riesgo puede ser de manera cuantitativa, cualitativa o una combinación de ambas.
- **Tratamiento del riesgo:** El tratamiento de los riesgos debe ser seleccionado a base de los resultados de la evaluación del riesgo, costos de implementación de controles y beneficios.

Existen cuatro (4) opciones para realizar el tratamiento del riesgo, según señala la ISO/IEC 27005 (Ver Figura 14)



**Figura 14. Tratamiento de los riesgos**

Fuente: Organización Internacional de Normalización (2011). ISO/IEC 27005

- **Reducir el riesgo:** Se reduce la criticidad del riesgo a través de controles y planes de acción
- **Retención del riesgo:** La decisión de retener la criticidad del riesgo debido que se acepta correr el riesgo luego de un análisis de costo-beneficio o porque es inherente al negocio.
- **Evitar el riesgo:** Cuando se identifica un riesgo crítico para la organización y la implementación de controles resulta más costosa que los beneficios que se dan, se decide evitar el riesgo cambiando el proceso, actividades o condiciones en los que se opera. Si se decidiera que no vale la pena, simplemente se evita el riesgo dejando de realizar el proceso donde se genera.
- **Transferir riesgo:** El riesgo puede asegurarse o transferirse a un tercero para una gestión más eficiente.
- **Aceptación del riesgo:** El tratamiento de los riesgos debe describir cómo se deben tratar los riesgos hasta llegar a un nivel aceptable para la organización.

### 1.2.6 Activos de información

Como menciona Dutton, J. (2016), Un activo de información es cualquier pieza o colección de información almacenada en el patrimonio de la organización, definida y administrada como una sola unidad para que podamos entenderla, compartirla y protegerla eficazmente y obtener el máximo valor de ella. Es algo que no podemos reemplazar sin costo, tiempo, habilidad y recursos.

Cuando los datos e información son importantes para la organización, estos datos e información se vuelven activos críticos. Estos activos pueden estar en forma estructurada (Base de datos, evaluación de proveedores, entre otros), semi-estructurada (Archivos XML, HTML, dispositivos móviles, entre otros) o sin estructura alguna que no solo está almacenada en un servidor, sino también pueden ser dibujos, anotaciones, fotografías, etc. Los activos de información pueden ser algo tan simple como una llamada telefónica. (Borek, A., Parlikad, A. K., Webb, J., & Woodall, P., 2013)

Los activos de información pueden, a base de su naturaleza, ser de diferentes tipos:

- Información: Se refiere a información almacenada en papel (por ejemplo, contratos, correspondencia, manuales de usuario, manuales de capacitación) o electrónicamente (por ejemplo, información sobre discos duros, USB, video, teléfonos móviles, bases de datos) o cualquier otra información bien es.
- Software: Incluye sistemas operativos, aplicaciones, herramientas de desarrollo, etc.
- Activos físicos y hardware: Se refieren a cualquier activo que pueda manipular información como computadoras, dispositivos móviles, salas de servidores, etc.
- Servicios: Se refiere a los servicios de los que dependen la organización, tales como back-up, energía, iluminación, etc.

- **Personas:** Las personas son los empleados, propietarios y gerentes que llevan consigo todas las habilidades e información sobre cómo opera la empresa.
- **Intangibles:** La propiedad intelectual de la organización, reputación, marca, etc.

Según la Universidad de Southern Queensland (2015), la clasificación de activos refleja el nivel de impacto para la organización si la confidencialidad, integridad o disponibilidad está comprometida. La clasificación de los activos de información, en el contexto de seguridad de la información, es la clasificación de la información basada en su nivel de sensibilidad y el impacto en la organización si la información se divulga, altera o destruye sin autorización. La clasificación de la información ayuda a determinar qué controles de seguridad de base son apropiados para salvaguardar esa información. Toda la información puede clasificarse en uno de los tres niveles de sensibilidad:

- Nivel 1: Información pública
- Nivel 2: Información interna
- Nivel 3: Información restringida

### 1.3 Términos básicos

- **Ataque:** Intento de destruir, exponer, alterar, inhabilitar u obtener accesos no autorizados hacia algún activo.
- **Amenaza:** Posibilidad de un ataque que puede resultar un daño a la organización.
- **Análisis de riesgos:** Uso sistemático de la información para identificar las fuentes y calcular el riesgo.
- **Confidencialidad:** La propiedad de estar disponible y no sea divulgada a personas, entidades o procesos no autorizados.
- **Consecuencia:** Resultado de un evento que afecta a los objetivos.
- **Contexto externo:** Ambiente externo a la empresa en el cual busca lograr sus objetivos.
- **Contexto interno:** Entorno dentro de la empresa en la cual busca



lograr sus objetivos.

- **Control:** Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.
- **Disponibilidad:** La propiedad de estar disponible y utilizable cuando se requiera.
- **Enunciado de aplicabilidad:** Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI.
- **Evento:** Ocurrencia o cambio de un conjunto de circunstancias.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
- **Gobierno de seguridad de información:** Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas.
- **Integridad:** La propiedad de salvaguardar la exactitud e integridad de los activos.
- **Ley de Protección de Datos:** Ley que busca garantizar el derecho fundamental a la protección de los datos personales, tanto en entidades públicas, así como privadas.
- **Medicina ocupacional:** Según la Organización Mundial de la Salud (OMS), es la medicina enfocada en la salud y la seguridad de los trabajadores en su entorno laboral.
- **Riesgo:** Es la probabilidad de ocurrencia de algún evento negativo que afecte a los objetivos del negocio.
- **Seguridad de información:** Preservación de confidencialidad, integridad y disponibilidad de la información.
- **Tratamiento del riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo.

## CAPÍTULO II METODOLOGÍA

### 2.1 Materiales

A continuación, se describen los materiales a utilizarse en el presente proyecto (Ver Tabla 6).

**Tabla 6. Materiales usados en el proyecto**

Tipo de Recurso	Nombre de Recurso	Descripción
Software	Google Drive	Usado como repositorio de los documentos necesarios para el proyecto.
	MS Word	Herramienta ofimática para el desarrollo de la documentación.
	MS Excel	Herramienta ofimática que permitirá la creación de tablas, encuestas, entre otros.
	MS Visio	Herramienta que permitirá la elaboración de los flujogramas de los procesos del negocio.
	Adobe Acrobat Reader	Herramienta que permite la visualización de documentos PDF.

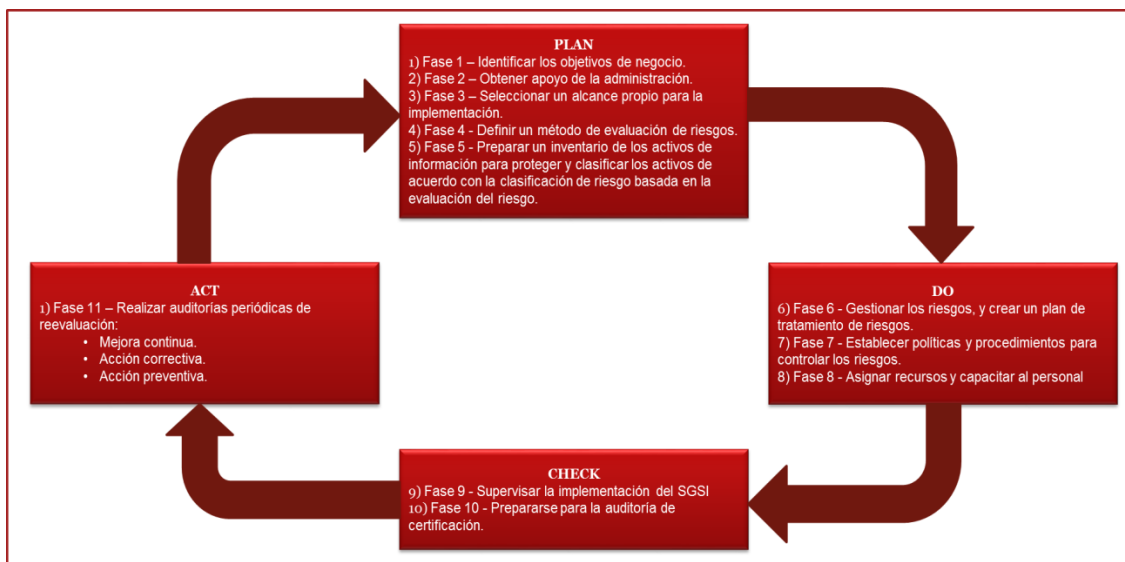
Tipo de Recurso	Nombre de Recurso	Descripción
Hardware	Laptop Personal	Computadora personal que se llevará a la empresa para poder hacer el relevamiento de los procesos y consolidar la documentación y encuestas.

Elaboración: Los autores.

## 2.2 Métodos

Como se explicó en el Capítulo I se utilizó el método Plan-Do-Check-Act o “Ciclo de Deming” sugerido por la ISO/IEC 27001:2005 Asociación de Auditoría y Control de Sistemas de Información (ISACA por sus siglas en inglés), una asociación profesional internacional centrada en la gobernanza de TI, ha definido, dentro de las cuatro (4) etapas del ciclo de Deming, 11 fases para implementar una SGSI que permitirán una fácil comprensión e implementación, así como un ahorro final de tiempo y costo.

Explica ISACA (2016), para un modelo de implementación de un SGSI, se detalla lo siguiente (Ver Figura 15):



**Figura 15. Ciclo de Deming con las fases de implementación**

Fuente: ISACA (2016). *Planning for and Implementing ISO 27001*

A continuación, se detalla las fases de implementación que propone ISACA

## Fases de implementación dentro de la metodología Plan-Do-Check-Act

A continuación, se detalla un mapeo de las 11 fases que se han definido para la implementación de un SGSI alineadas a los pasos sugeridos por la norma internacional (Ver Tabla 7). Las fases 4 y 5 requieren una metodología o guía adicional para el adecuado cumplimiento de la misma. A continuación, se detallan los lineamientos básicos y metodologías adicionales a usar:

- **Etapas 1: Planear**
- **Fase 1: Identificar los objetivos de negocio**

Las partes interesadas deben comprender, identificar y priorizar los objetivos para brindar soporte al proyecto. Los objetivos principales pueden derivarse de la misión de la empresa, la visión, el plan estratégico y los objetivos de TI. Los objetivos pueden ser la identificación de activos y efectivas evaluaciones de riesgos, determinar el apetito de riesgo, obtener ventajas competitivas, etc.

Tabla 7. Pasos para la implementación de ISO/IEC 27001

Mapeo de Pasos Sugeridos por la ISO / IEC 27001 para las Fases de Implementación	
ISO/IEC 27001:2005 Pasos Sugeridos	Fases de Implementación
Definir política de SGSI.	Fase 1 – Identificar los objetivos de negocio. Fase 2 – Obtener apoyo de la administración.
Definir el alcance del SGSI.	Fase 3 – Seleccionar un alcance propio para la implementación.
Realizar una evaluación de riesgos de seguridad.	Fase 4 - Definir un método de evaluación de riesgos.

<b>Mapeo de Pasos Sugeridos por la ISO / IEC 27001 para las Fases de Implementación</b>	
<b>ISO/IEC 27001:2005 Pasos Sugeridos</b>	<b>Fases de Implementación</b>
Gestionar el riesgo identificado.	Fase 5 - Preparar un inventario de los activos de información para proteger y clasificar los activos de acuerdo con la clasificación de riesgo basada en la evaluación del riesgo.
Seleccionar los controles a implementar y aplicar.	Fase 6 - Gestionar los riesgos, y crear un plan de tratamiento de riesgos. Fase 7 - Establecer políticas y procedimientos para controlar los riesgos.
Preparar una SOA.	Fase 8 - Asignar recursos y capacitar al personal.
<b>Mapeo de Fases de implementación para la Revisión y Registro</b>	
<b>Revisión y registro</b>	<b>Fases de Implementación</b>
Revisión de gestión y auditoría interna.	Fase 9 - Supervisar la implementación del SGSI
Registro y certificación.	Fase 10 - Prepararse para la auditoría de certificación.
Mejora del SGSI	Fase 11 – Realizar auditorías periódicas de re-evaluación: <ul style="list-style-type: none"> <li>• Mejora continua</li> <li>• Acción correctiva</li> <li>• Acción preventiva.</li> </ul>

Fuente: ISACA (2016). *Planning for and Implementing ISO 27001*

- **Fase 2: Obtener apoyo de la administración**

La gerencia o el área de administración deben estar comprometidas con el proyecto. Debe realizar un monitoreo constante, así como asegurar la mejora continua del SGSI, que puede ser a través de políticas de seguridad,

capacitaciones constantes a los empleados, definir recursos para la seguridad, entre otros.

Según Lopes I., Oliveira P. (2014), La cultura de seguridad de información ayuda a minimizar las amenazas que el comportamiento del usuario plantea a la protección de los activos de información. La importancia de crear una cultura dentro de los entornos de la organización surge del hecho de que la dimensión humana en la seguridad de la información siempre se considera el eslabón más débil.

- **Fase 3: Seleccionar el alcance adecuado**

La ISO/IEC 27001 establece cualquier ámbito de aplicación que puede abarcar todo o parte de una organización. De acuerdo con el alcance del SGSI, sólo se deben especificar los procesos, unidades de negocio o proveedores externos o contratistas que caen dentro del alcance de la implementación.

- **Fase 4: Definir un método de evaluación de riesgos**

Para cumplir con los requisitos de ISO/IEC 27001, las empresas deben definir y documentar un método de evaluación de riesgos. La norma ISO / IEC 27001 no especifica el método de evaluación de riesgos que se utilizará.

La elección de un método de evaluación de riesgos es una de las partes más importantes del establecimiento del SGSI. La ISO/IEC 27001 necesita evaluaciones de riesgo basadas en los niveles de confidencialidad, integridad y disponibilidad (CIA).

Las metodologías de análisis de riesgos ayudan a las organizaciones a tener un mayor control sobre sus activos, su valor y minimizar las amenazas que pueden impactarlas obligándolas a seleccionar medidas de seguridad que garanticen el éxito de sus procesos y una mayor competitividad en el sector en que se desenvuelven. El análisis de riesgo, a nivel empresarial, es una excelente herramienta para generar planes de contingencia y continuidad del negocio, debido a que permite a las empresas mitigar el riesgo y garantizar el

rendimiento de los sistemas informáticos. Cabe resaltar que es imposible eliminar un riesgo en su totalidad, lo que se puede hacer con la implementación de metodologías es reducirlo para que no genere ningún daño representativo al sistema informático de la organización. (Abril, A., Pulido, J., Bohada, J., 2013).

**- Técnicas de relevamiento de riesgos**

Para el relevamiento y evaluación de los riesgos se usará de base la ISO/IEC 27005 que nos da una gestión de riesgos enfocados en la seguridad de la información, a su vez, la ISO/IEC 31010, que nos brinda las mejores prácticas de relevamiento de riesgos que se pueden aplicar.

Para el relevamiento usaremos estas 3 técnicas, la elección se ve influenciada por la complejidad del problema, la cantidad de recursos necesarios, nivel de experiencia y costos, el grado de incertidumbre aceptado por la empresa, entre otros.

Para el caso de este proyecto usaremos algunas técnicas presentadas en la ISO/IEC 31010 – “Técnicas de Evaluación de Riesgos”, como por ejemplo la matriz de probabilidades e impacto.

**- Matriz de probabilidades e impacto**

La matriz de probabilidades e impacto combina los datos tanto cualitativos como cuantitativos, calificándolos en términos de consecuencia y probabilidad para una clasificación de los riesgos. Esta matriz nos permite determinar los niveles de riesgos y tener una mejor visualización de estos, a su vez, que ayuda a tener un lenguaje común sobre la medición del riesgo en toda la organización. La ISO/IEC 27005 nos da un ejemplo de cómo debería ser la matriz para determinar la criticidad de un riesgo: (Ver Figura 16)

		Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4	
	Low	1	2	3	4	5	
	Medium	2	3	4	5	6	
	High	3	4	5	6	7	
	Very High	4	5	6	7	8	

**Figura 16. Ejemplo de matriz de riesgo**

Fuente: Organización Internacional de Normalización (2011). ISO/IEC 27005

- **Fase 5: Preparar un inventario de los activos de información**

La empresa necesita crear una lista de activos de información que deben protegerse. Debe identificarse el riesgo asociado con los activos, junto con los propietarios, la ubicación, la criticidad y el valor de reposición de los activos. Una vez completada la evaluación, se identificarán los activos de información que tienen un riesgo intolerable y, por lo tanto, requieren controles. En ese momento, se crea la valorización y una posterior matriz de riesgos que indica el valor del riesgo para cada activo. Para esta fase se requiere una metodología o guía adicional a la proporcionada por la norma para la identificación y valorización de activos de información.

- **Identificación de los activos de información**

Según Aguirre, A. (2014), Se deben mapear los procesos que forman parte del alcance del proyecto, se debe realizar una serie de entrevistas para identificar a cada uno de los activos de información que están involucrados en los procesos, luego se procederá a valorarlos y asegurar cada uno de los activos, más importantes para la organización. Para la identificación de estos activos se utilizó el mapa de procesos durante cada una de las entrevistas, ya que permitió asociar los activos con una actividad del proceso.

El objetivo de esta parte del proyecto es obtener un inventario de los activos de información involucrados en el alcance del SGSI, para ello se desarrolló una metodología de valoración de activos, basada en lo propuesto por la ISO/IEC 27005:2008, en la cual se detalla cual es el procedimiento para la identificación de los mismos.

Para la realización del inventario de activos, se tomó en cuenta los siguientes datos:

- Id Activo: Un código que pueda identificar a los activos de información.
- Nombre: El nombre del activo
- Descripción: Una descripción breve de cada uno de los activos de información.
- Proceso: El proceso en el que se encuentra el activo de información



- Subproceso: Cuál es la actividad específica, dentro del proceso, en el cual se encuentra el activo de información.
  - Clasificación de activo: Si es primario o secundario, según lo definido en la metodología.
  - Sub Clasificación de Activo: Sub clasificación del activo si es software, hardware, personal, sitio u organización.
  - Propietario del activo: Quien es el dueño del activo de información
  - Ubicación: Cuál es la ubicación física o lógica del activo de información
- **Valoración de los activos de información**

Según indica la ISO/IEC 27005:2008: La decisión de utilizar una valoración cuantitativa versus una valoración cualitativa es decisión de lo que la organización prefiera, pero debe ser relevante para los activos objetos de valoración. Ambos tipos de valoración pueden ser utilizados para un mismo activo. Los posibles criterios utilizados para determinar el valor de un activo incluyen: su coste original, su costo reemplazado o de creación o su valor puede ser abstracto. Por ejemplo, el precio de la reputación de la organización.

Otra base para la valoración de los activos es el costo incurrido debido a la pérdida de confidencialidad, integridad y disponibilidad como resultado de un incidente.

- **Etapas 2: Hacer**
- **Fase 6: Gestionar los riesgos, y crear un plan de tratamiento de riesgos**

Para controlar el impacto asociado con el riesgo, la organización debe aceptar, evitar, transferir o reducir el riesgo a un nivel aceptable utilizando controles de mitigación del riesgo.

Parte de la gestión de riesgos, incorpora análisis de amenazas y vulnerabilidad y considera mitigaciones proporcionadas por controles de seguridad planeados o en su lugar. (Kissel, R., 2013).

- **Fase 7: Establecer políticas y procedimientos para controlar los riesgos**

En esta fase, se procede a realizar un análisis de los controles que proporcionan las normas y una posterior declaración de aplicabilidad, donde se justifica la implementación de controles o su exclusión. A su vez, se especifica la manera cómo se adapta a la empresa. Se necesitan declaraciones de política o un procedimiento detallado y un documento de responsabilidad para identificar las funciones de los usuarios para la implementación consistente y efectiva de políticas y procedimientos.

- **Fase 8: Asignar recursos y capacitar al personal**

El proceso del SGSI destaca uno de los compromisos importantes para la gestión: recursos suficientes para gestionar, desarrollar, mantener y aplicar el SGSI. Es esencial documentar la capacitación para la auditoría.

- **Etapa 3: Revisión**

- **Fase 9: Supervisar la implementación del SGSI**

La auditoría interna periódica es una necesidad para el monitoreo y revisión. La revisión de la auditoría interna consiste en probar los controles e identificar acciones correctivas / preventivas. Para ser eficaz, el SGSI debe ser revisado por la administración a intervalos periódicos y planificados. La revisión sigue cambios / mejoras a políticas, procedimientos, controles y decisiones de personal. Los resultados de las auditorías y las revisiones periódicas se documentan y se les debe hacer mantenimiento.

- **Fase 10: Prepararse para la auditoría de certificación**

Para que la organización sea certificada, es esencial que lleve a cabo un ciclo completo de auditorías internas, revisiones de gestión y actividades en el proceso PDCA y que conserve evidencia de las respuestas tomadas como resultado de esas revisiones y auditorías

- **Etapa 4: Actuar**
- **Fase 11: Realizar auditorías periódicas de re-evaluación**

Las revisiones de seguimiento y las auditorías periódicas confirman que la organización sigue cumpliendo con la norma. El mantenimiento de la certificación requiere auditorías periódicas de reevaluación para confirmar que el SGSI continúa funcionando como se especifica y pretende. Al igual que con cualquier otra norma ISO, ISO/IEC 27001 sigue el ciclo PDCA y ayuda a la gestión del SGSI a conocer hasta qué punto y con qué éxito ha progresado la empresa a lo largo de este ciclo.

## CAPÍTULO III DESARROLLO DEL PROYECTO

### 3.1 Cronograma de implementación

Se definió el cronograma de implementación del proyecto de la siguiente manera (Ver Tabla 8):

**Tabla 8. Cronograma de Implementación del Proyecto**

Task Mode	Task Name	Duration	Start	Finish	Resource Names
1	✦ Proyecto de Tesis	88 days	Mon 13/03/17	Mon 15/05/17	Miguel Angel Cruz / Senyi Fukusaki
2	✦ Etapa I: Planificación	49.5 days	Mon 13/03/17	Mon 17/04/17	Miguel Angel Cruz / Senyi Fukusaki
3	✦ Identificación de Objetivos de Negocio	5 days	Mon 13/03/17	Thu 16/03/17	Miguel Angel Cruz / Senyi Fukusaki
4	✦ Alinear objetivos del trabajo con objetivos de negocio	5 days	Mon 13/03/17	Thu 16/03/17	Miguel Angel Cruz / Senyi Fukusaki
5	✦ Fase 2: Obtener apoyo de la organización	5.5 days	Fri 17/03/17	Mon 20/03/17	Miguel Angel Cruz / Senyi Fukusaki
6	✦ Obtener el apoyo de la organización para el proyecto	5.5 days	Fri 17/03/17	Mon 20/03/17	Miguel Angel Cruz / Senyi Fukusaki
7	✦ Fase 3: Seleccionar el alcance adecuado	11 days	Tue 21/03/17	Tue 28/03/17	Miguel Angel Cruz / Senyi Fukusaki
8	✦ Identificar y establecer los procesos críticos de la empresa	11 days	Tue 21/03/17	Tue 28/03/17	Miguel Angel Cruz / Senyi Fukusaki
9	✦ Fase 4: Definición de método de evaluación de riesgos	12.38 days	Wed 29/03/17	Thu 06/04/17	Miguel Angel Cruz / Senyi Fukusaki
10	✦ Diseñar la metodología para la evaluación de riesgos	12.38 days	Wed 29/03/17	Thu 06/04/17	Miguel Angel Cruz / Senyi Fukusaki
11	✦ Fase 5: Inventario de Activos	15.13 days	Fri 07/04/17	Mon 17/04/17	Miguel Angel Cruz / Senyi Fukusaki
12	✦ Modelar los procesos del negocio	5 days	Fri 07/04/17	Mon 10/04/17	Miguel Angel Cruz / Senyi Fukusaki
13	✦ Identificar los activos de información	3 days	Tue 11/04/17	Thu 13/04/17	Miguel Angel Cruz / Senyi Fukusaki
14	✦ Valorizar los activos de Información	5 days	Fri 14/04/17	Mon 17/04/17	Miguel Angel Cruz / Senyi Fukusaki
15	✦ Etapa II: Hacer	38.5 days	Tue 18/04/17	Mon 15/05/17	Miguel Angel Cruz / Senyi Fukusaki
16	✦ Fase 6: Gestión de Riesgos	27.5 days	Tue 18/04/17	Sun 07/05/17	Miguel Angel Cruz / Senyi Fukusaki
17	✦ Diseñar una matriz de vulnerabilidad de activos	5 days	Tue 18/04/17	Fri 21/04/17	Miguel Angel Cruz / Senyi Fukusaki
18	✦ Diseñar matriz de riesgos	6 days	Sat 22/04/17	Wed 26/04/17	Miguel Angel Cruz / Senyi Fukusaki
19	✦ Definir controles	10 days	Thu 27/04/17	Thu 04/05/17	Miguel Angel Cruz / Senyi Fukusaki
20	✦ Establecer aplicabilidad de controles	3 days	Fri 05/05/17	Sun 07/05/17	Miguel Angel Cruz / Senyi Fukusaki
21	✦ Fase 7: Establecer política y procedimientos de control	11 days	Mon 08/05/17	Mon 15/05/17	Miguel Angel Cruz / Senyi Fukusaki
22	✦ Establecer la Política de SGSI	11 days	Mon 08/05/17	Mon 15/05/17	Miguel Angel Cruz / Senyi Fukusaki

Elaboración: Los autores.

## 3.2 Implementación del SGSI

Dentro de las cuatro (4) etapas del ciclo de Deming (Plan-Do-Check-Act) se desarrollaron las 11 fases establecidas por ISACA:

- **Etapas 1: Planear**

Esta etapa consta de cinco (5) fases en las cuales se identifican los objetivos, alcance, métodos de tratamiento de riesgo; se obtiene el respaldo del personal responsable de la empresa y se elabora el inventario de activos.

- **Fase 1: Identificar los objetivos de negocio**

A base de la misión, visión, reglamentación y los requerimientos de la organización (MEDCAM S.A.) se han determinado los siguientes objetivos bajo los cuales se desarrollará el Sistema de Gestión de Seguridad de la Información, se detallan a continuación (Ver Tabla 9):

Tabla 9. Misión, Visión y Objetivos de MEDCAM Perú SAC

MEDCAM	MEDCAM
<b>Misión</b>	<b>Objetivos de la Empresa</b>
<p>La clínica MEDCAM tiene como misión brindar servicios en salud ocupacional con calidad, calidez y profesionalismo, haciendo uso de nuestro innovador equipo tecnológico y profesional multidisciplinario, orientándonos a las necesidades y demandas de nuestros clientes contribuyendo así favorablemente en la productividad y competitividad de los mismos, así como a los constantes cambios del mercado.</p>	<ul style="list-style-type: none"> <li>• Asegurar que los activos de la información de la empresa estén debidamente respaldados, sean confiables e íntegros.</li> <li>• Adaptarse a los constantes cambios tecnológicos teniendo unas políticas y controles de seguridad flexibles.</li> <li>• Asegurar a los pacientes y empresas con las que se trabaja el compromiso de la organización con la seguridad de la información, privacidad y protección de datos personales.</li> <li>• Asegurar a los socios de negocios el estado de la organización con respecto a la seguridad de la información.</li> <li>• Preservación de la reputación y posicionamiento de la clínica entre los líderes del mercado.</li> <li>• Cumplimiento con las regulaciones de la Ley N° 30024: Ley que crea el Registro Nacional de Historias Clínicas</li> <li>• Cumplimiento con la Ley N° 29733: Ley de Protección de Datos Personales</li> </ul>
<b>Visión</b>	
<p>Ser empresa líder en servicios de salud ocupacional, reconocido por nuestro carácter innovador, tecnológico, calidad de servicio y excelencia en los servicios que brindamos satisfaciendo las necesidades de nuestros clientes, promoviendo y concientizando la prevención y promoción de la salud en el trabajo a nivel nacional.</p>	

Elaboración: Los autores.

- **Fase 2: Obtener apoyo de la Administración.**

En primer lugar, se elaboró un acta de constitución del proyecto a la clínica, donde se especificó los objetivos y el alcance, y fue presentado a la administración de MEDCAM para su aprobación (**Ver Anexo 1 – Acta de Constitución del Proyecto**).

Se elaboró una política general de la seguridad de la información en conjunto con la gerencia de la clínica, donde se definen los alcances de la seguridad en la empresa, los roles y responsabilidades y las sanciones aplicables ante cualquier violación de seguridad. Esto nos ayuda a establecer el compromiso brindado por parte de la administración. (**Ver Anexo 2 – Política General de la Seguridad de la Información**)

- **Fase 3: Seleccionar el alcance adecuado**

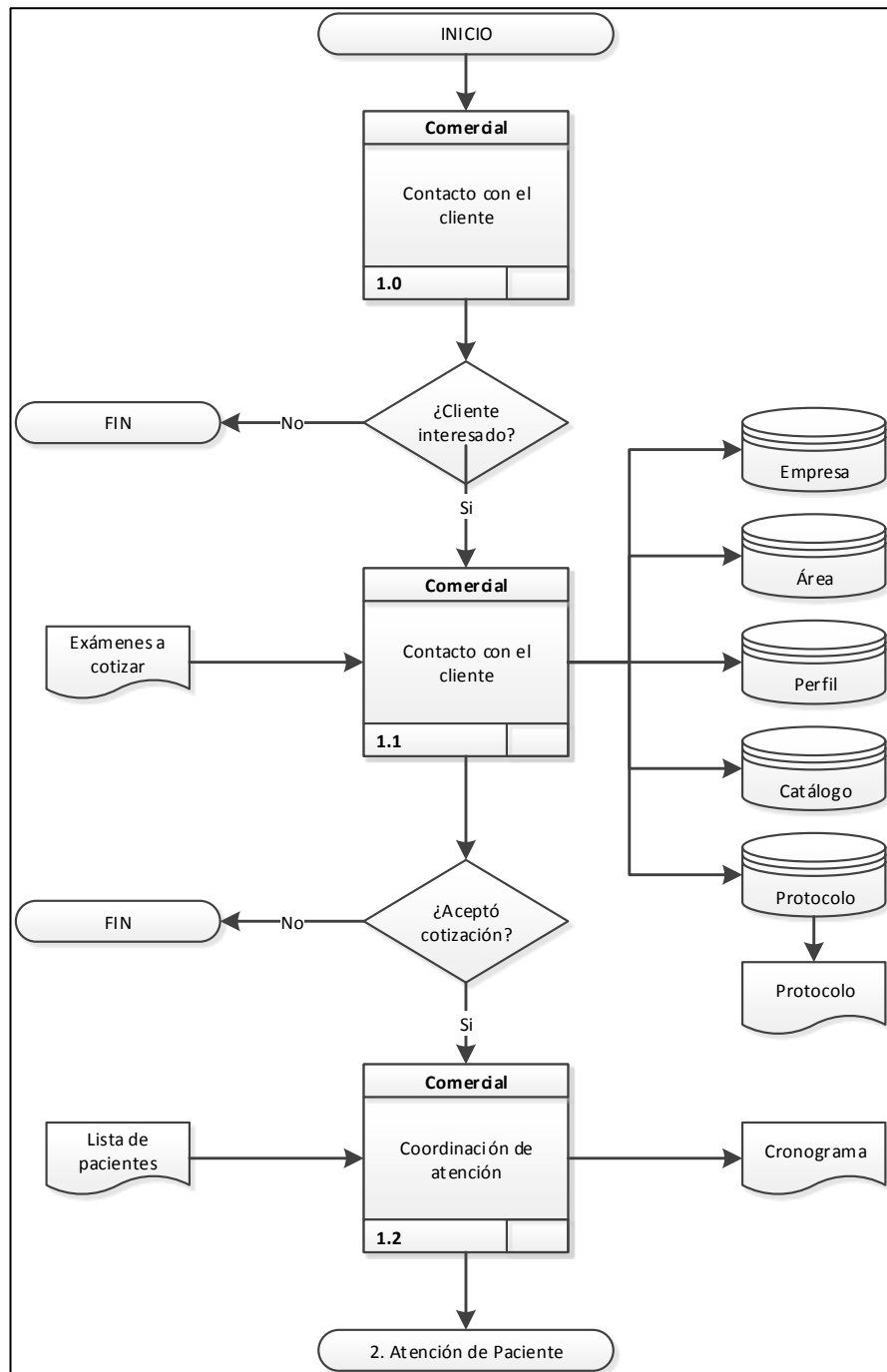
El alcance de implementación de un sistema de gestión de seguridad de la información fue determinado por la empresa a base de los objetivos de la misma. Para determinar estos, se identificaron los procesos core con los cuales la empresa considera crítico para su negocio. Los procesos que se encuentran dentro del alcance son los siguientes:

- **Captación de clientes:** Proceso mediante el cual el área comercial inicia el contacto con los clientes, si el cliente muestra interés se crea al cliente en el sistema Mediweb y se le genera un protocolo (cotización) para formalizar el servicio ofrecido. El protocolo se genera a base de las pruebas y tipos de empleados que el cliente solicita. De ser aceptado el cliente envía la lista total de empleados que serán atendidos y se coordina la atención de los pacientes, ya sea en el local la clínica o en el local del cliente. (Ver Figura 17).
- **Atención de pacientes:** Proceso en el cual el área de Admisión recibe al paciente, se realiza la toma de datos para estos ser registrados en el sistema Mediweb. Luego de registrar al paciente, y asignarles en el sistema las evaluaciones que el cliente ha solicitado realizar se crea de

manera automática la orden de atención. Una vez registrado en el sistema, se le pide llenar y dar su consentimiento en consentimientos “Consentimiento Informado de Atención” y “Consentimiento Informado Ley” en los cuales confirma que es de su conocimiento las pruebas que se realizaron y permite a MEDCAM el manejo de esta información. Finalmente, se orienta al paciente el orden en que se realiza las atenciones. (Ver Figura 18).

- **Procesamiento de datos:** Proceso en el cual el licenciado o médico es el encargado de realizar los exámenes programados y registrar los resultados en el sistema Mediweb. La persona que realiza el registro está encargada de realizar una primera revisión en el sistema. Luego, el médico auditor, responsable legal de los resultados, realiza una auditoría sobre dichos resultados en el sistema Mediweb. De existir un resultado negativo se le comunica al paciente mediante la entrega del documento “Garantía de Tratamiento Adicional” en el cual se le solicita que asegure un tratamiento en otro centro médico. Finalmente, el licenciado comunica al médico ocupacional del cliente los resultados finales, esto puede ser otorgando acceso al médico ocupacional al sistema Mediweb a los resultados de los empleados del cliente o entregando resultados impresos por paciente. (Ver Figura 19).
- **Facturación** A base de las atenciones registradas en las Órdenes de Atención en el sistema Mediweb, el facturador genera una Pre-Liquidación en la cual selecciona las órdenes que desea facturar, cabe resaltar que se pueden seleccionar las órdenes que tienen un estado auditado. El sistema Mediweb genera el cálculo de la factura con los que luego se genera la factura electrónica en la web de SUNAT. La factura electrónica es posteriormente almacenada en el sistema en formato PDF y registrada en la misma. (Ver Figura 20).
- **Logística:** Este proceso se encarga de la gestión que alimenta el kardex de entrada y salida de materiales, más específicamente de la compra de materiales determinada por requerimientos de las áreas de

negocio o por recomendaciones del sistema de reposición automática. Este proceso también se encarga del despacho de materiales para el proceso “Atención de pacientes”, el despacho es realizado si se cuenta con una solicitud por correo electrónico. (Ver Figura 22).



**Figura 17. Diagrama del proceso de captación de clientes**

Elaboración: Los autores



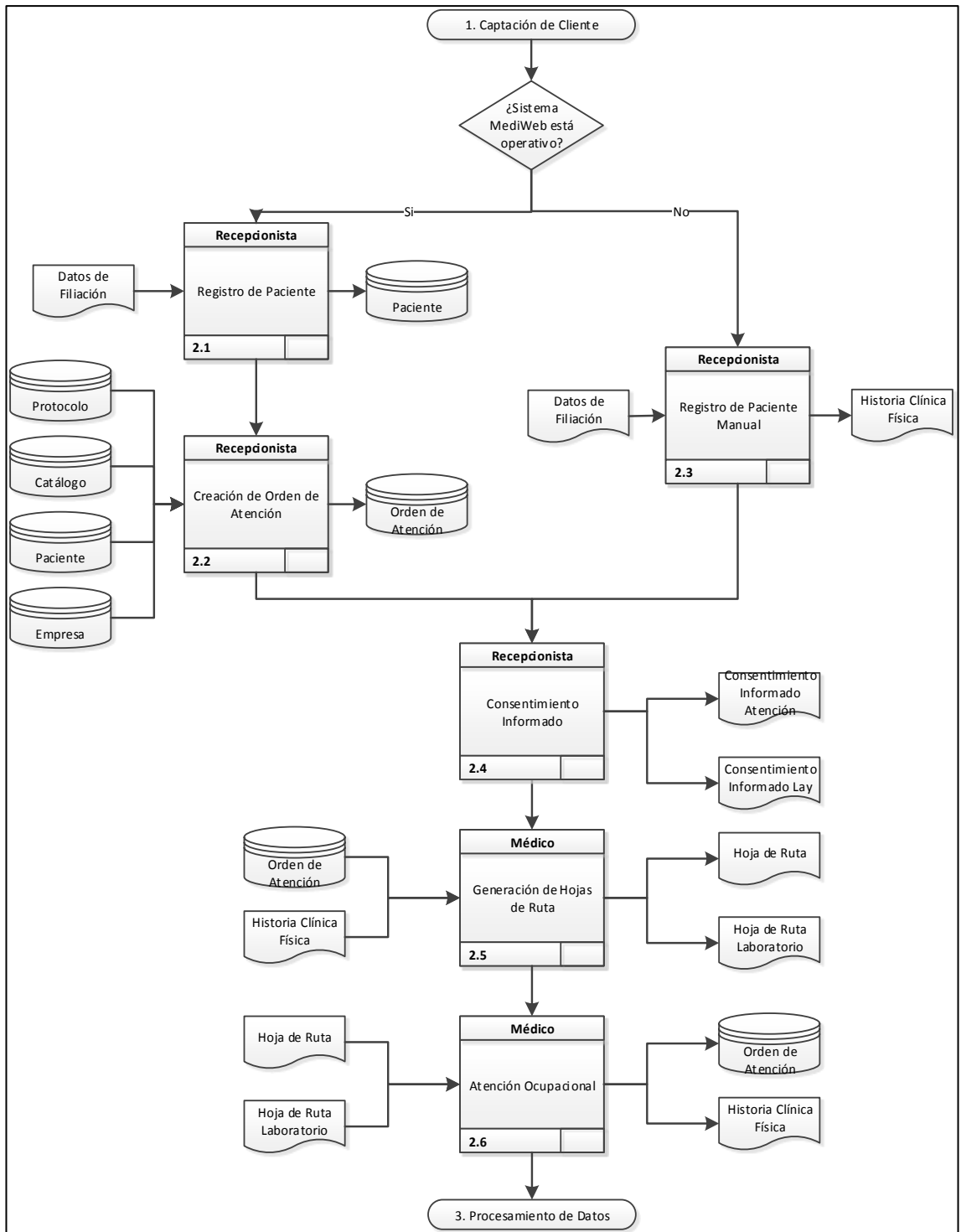
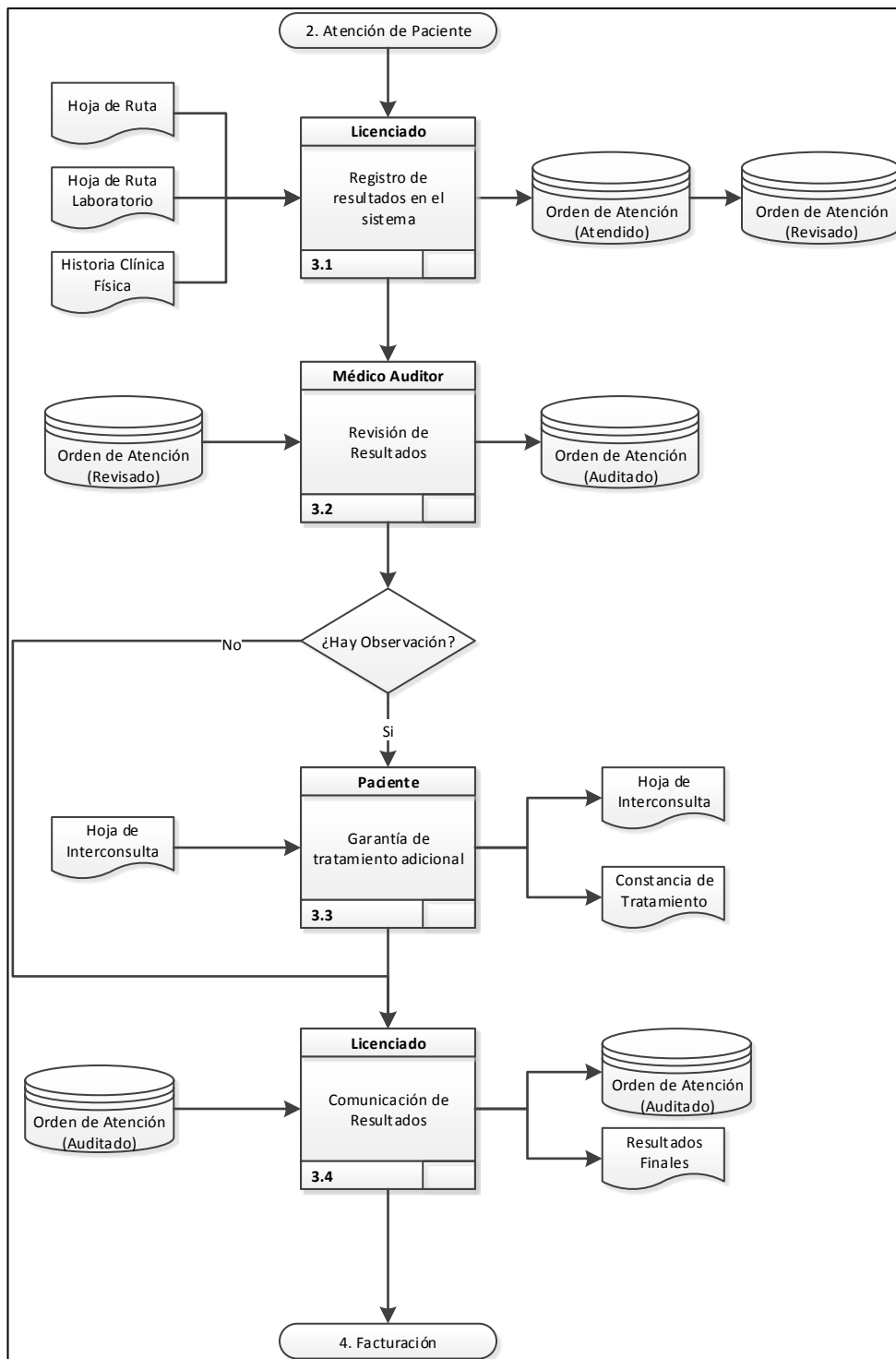


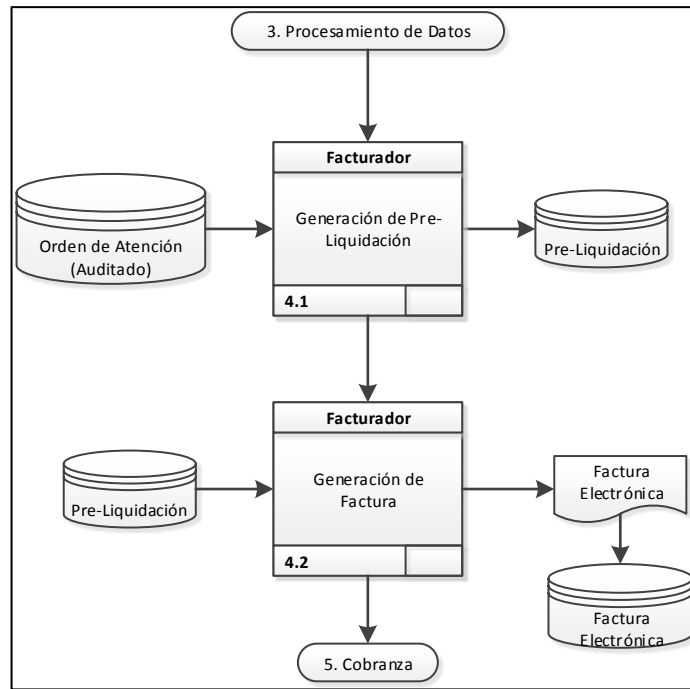
Figura 18. Diagrama del proceso de atención al cliente

Elaboración: Los autores.



**Figura 19. Diagrama del proceso de procesamiento de datos**

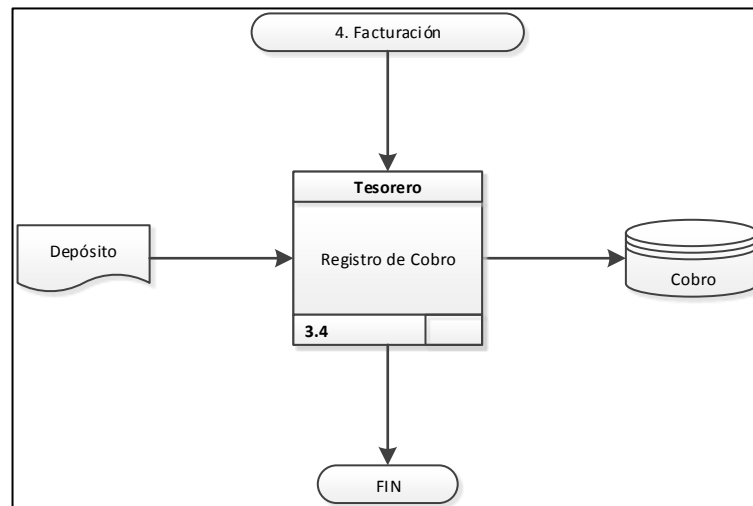
Elaboración: Los autores.



**Figura 20. Diagrama del proceso de facturación**

Elaboración: Los autores.

- **Cobranza:** Proceso en el cual se validan los depósitos del cliente en las cuentas de banco de la empresa y se procede a compensar la factura. (Ver Figura 21)



**Figura 21. Diagrama del Proceso de Cobranza**

Elaboración: Los autores

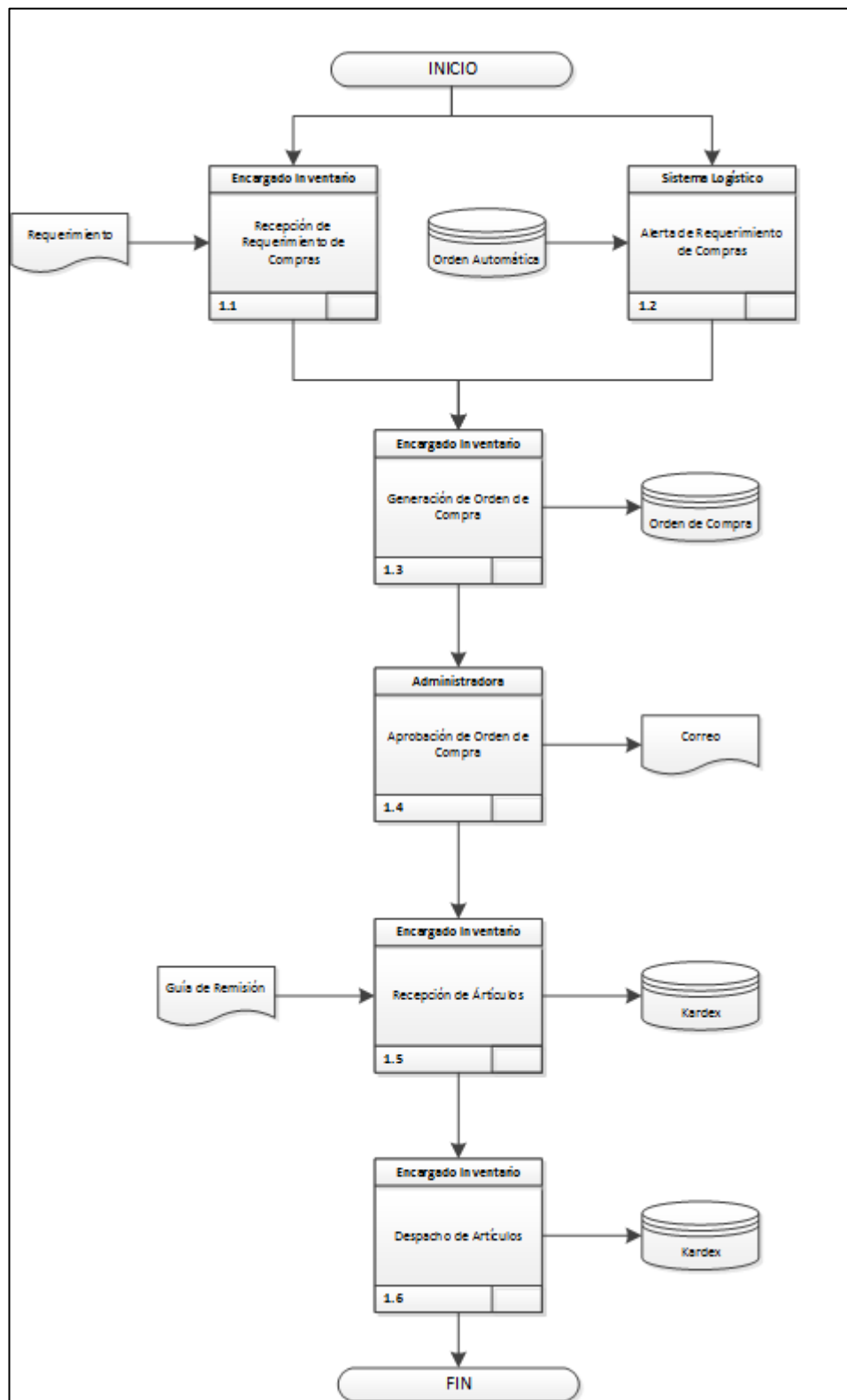


Figura 22. Diagrama del proceso de logística

Elaboración: Los autores

- **Fase 4: Definir un método de evaluación de riesgos**

En esta fase, se utilizó la ISO/IEC 27005 que nos proporcionó una lista de amenazas y vulnerabilidades para cada tipo de activo de información que se consideró relevante (Ver Anexo 4 - Lista de Amenazas y de Vulnerabilidades). Se relacionaron los activos de información con las amenazas y vulnerabilidades teniendo como resultado posibles riesgos por cada activo de información. Estos riesgos fueron evaluados a base de la criticidad que representaría su materialización y los riesgos establecidos como altos y críticos recibieron un tratamiento (respuesta por parte de la empresa).

Como se mencionó antes, para establecer la relación entre los activos de información relevantes las amenazas y vulnerabilidades obtenidas de la ISO/IEC 27005 se estableció un cuadro que relaciona los mismos (Ver Tabla 10).

**Tabla 10. Campos del Análisis de Vulnerabilidades y Amenazas**

Campo	Descripción
ID Activo	Identificador del Activo
Vulnerabilidad	Vulnerabilidad del activo
Amenaza	Amenaza expuesta del activo.

Elaboración: Los autores

Una vez relacionadas las vulnerabilidades y amenazas con los activos de información relevantes se establece el riesgo y su consecuencia, y es a base de esta consecuencia que se determina la criticidad del riesgo, los factores con los que determina la criticidad son: probabilidad e impacto.

Respecto a la probabilidad, que es la tasa de ocurrencia del riesgo, se muestra en la Tabla 11.

**Tabla 11. Criterios para la Tasa de Ocurrencia del Riesgo**

Criterios de Probabilidad	
Probabilidad	Frecuencia de Ocurrencia
Raro	Frecuencia en ocasiones excepcionales, como 1 vez cada 5 años
Improbable	Frecuencia poco probable, como 3 veces cada 5 años

Criterios de Probabilidad	
Probabilidad	Frecuencia de Ocurrencia
Posible	Frecuencia en algún momento, como 1 vez al año.
Probable	Frecuencia que ocurra de 2-3 veces al año.
Casi Certeza	Frecuencia de 4 a más veces al año.

Elaboración: Los autores.

Para evaluar el impacto que tendría el negocio si se materializaran las consecuencias, se desarrollaron características o criterios que ayudan a determinar el nivel de impacto que se tendría (Ver Tabla 12).

Cabe resaltar que, como plantea la ISO/IEC 27005, se considera el riesgo residual, que es el riesgo remanente luego de los controles que previamente se tienen, es por eso que es importante la identificación de los controles previos tal como menciona la norma.

**Tabla 12. Criterios para la determinación del impacto**

Impacto	Descripción
Bajo	Pérdida o daño catastrófico a la reputación de la organización; pérdidas financieras importantes, cobertura a nivel nacional y de forma prolongada; intervención regulatoria con sanciones por faltas muy graves; pérdida de clientes a gran escala; involucramiento directo de la alta gerencia o directorio.
Moderado	Daño sobre la empresa es mayor, riesgo inusual o inaceptable en el sector; cobertura a nivel nacional; investigación del regulador y sanciones por falta grave; involucramiento de la alta gerencia, gastos operativos de consideración; pérdidas financieras mayores.
Relevante	El impacto sobre la compañía es directo y medio, se podría incurrir en gastos operativos controlados, existen sanciones por falta leve, se expone la imagen de la organización con un impacto medio.
Alto	Riesgo aceptable en el sector; no hay daño a la reputación, no hay sanciones legales, pero si observaciones por parte de los reguladores, el impacto operacional o financiero es mínimo.
Crítico	No hay impacto directo sobre la organización, no hay daño a la reputación, no existen sanciones legales ni impacto financiero u operacional; no es percibido por los clientes pero si por los colaboradores

Fuente: Aguirre, D. (2014), Diseño de un sistema de gestión de Seguridad de Información *para servicios postales del Perú*

Para la determinación del nivel de criticidad, se toma en cuenta la probabilidad y el impacto de la ocurrencia del riesgo. A continuación, en la Tabla 13 se muestran los niveles de criticidad producto del impacto y probabilidad determinados.

Impacto	Crítico	Medio	Alto	Alto	Crítico	Crítico
	Alto	Bajo	Medio	Alto	Alto	Crítico
	Relevante	Bajo	Medio	Medio	Alto	Alto
	Moderado	Bajo	Bajo	Medio	Medio	Medio
	Bajo	Bajo	Bajo	Bajo	Bajo	Medio
		Raro	Improbable	Posible	Probable	Casi Certeza
		Probabilidad				

Elaboración: Los autores.

El apetito del riesgo es la exposición que se está dispuesto a tener por ofrecer los servicios y/o productos y que se acepta sin realizar mayor análisis. Actualmente, la empresa no cuenta con un apetito de riesgo por lo que se propone deberían aceptar riesgos “Bajo” y “Medio”, y que los riesgos “Alto” y “Crítico” deben ser controlados y mitigados inmediatamente, para reducir su criticidad a los valores aceptables.

Una vez identificados los niveles de criticidad por riesgos, se debe realizar el tratamiento de riesgo que consiste si se acepta el riesgo, se reduce, se evita o se transfiere. Según la metodología, se realiza de la siguiente manera (Ver Tabla 14):

Tabla 14. Tratamiento del Riesgo

Tratamiento de Riesgo	Descripción
Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles para que el riesgo residual pueda ser reevaluado como aceptable.
Retención del riesgo	La decisión de retener el riesgo sin medidas adicionales debe tomarse en función de la evaluación del riesgo
Evitar el riesgo	Debe evitarse la actividad o condición que da

Tratamiento de Riesgo	Descripción
	lugar al riesgo particular
Transferir el riesgo	El riesgo debe ser transferido a otra parte que pueda manejar con mayor eficacia el riesgo particular dependiendo de la evaluación del riesgo.

Elaboración: Los autores.

Finalizada la identificación (luego del análisis de amenazas y vulnerabilidades) y el respectivo análisis de riesgos, se desarrolló la matriz de riesgo que contendrá los siguientes campos (Ver Tabla 15):

**Tabla 15. Campos de la matriz de riesgos**

Campo	Descripción
ID Riesgo	Identificador del riesgo
Riesgo	Descripción del Riesgo
Consecuencias	Consecuencias de la materialización del riesgo
Probabilidad	Probabilidad de ocurrencia del riesgo
Impacto	Impacto del riesgo
Criticidad	La criticidad del riesgo, que es la combinación de Probabilidad y Consecuencia.
Tratamiento del riesgo	Tratamiento que se le dará al riesgo identificado.

Elaboración Los autores.

- **Fase 5: Preparar un inventario de los activos de información**

En esta fase, se realiza la identificación y valoración de los activos de información identificados en los procesos más críticos del negocio. En este punto, también se hace uso de la ISO/IEC 27005, en el cual se detalla el método de identificación y valoración. Esta fase es importante porque se determina cuáles son los activos de información críticos para la operatividad de los procesos.



En la identificación de los activos, se tomará en cuenta para su clasificación lo siguiente: Primario (Procesos de negocio y actividades e información) y de soporte (Hardware, Software, Redes, Personal, Sitio). Se muestran los campos para la identificación de los activos de información en la Tabla 16.

**Tabla 16. Campos de la identificación de activos**

<b>Campo</b>	<b>Descripción</b>
ID Activo	Identificador del activo.
Proceso	Proceso donde se encuentra el activo de información.
Subproceso	Sub proceso donde se encuentra el activo de información.
Nombre	Nombre del activo de información
Descripción	Descripción breve del activo de información.
Clasificación de activo	Si es Primario o de Soporte.
Sub clasificación de activo	Sub clasificación de activo de información.
Propietario del activo	Quien es el dueño del activo de información
Ubicación	Cuál es la ubicación física o lógica del activo de información

Elaboración: Los autores.

A continuación, se muestra el resultado del levantamiento de los activos de la información realizados (Ver Tabla 17).

**Tabla 17. Inventario de activos**

ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
R1	Gerente General	Responsable de fijar los objetivos y de la toma de decisiones estratégicas de la empresa.	Todos	Supervisión	Primario	Recurso humano	No aplica	Local de San Luis
R2	Administrador	Responsable de velar por el cumplimiento de las actividades de la empresa según los procesos establecidos.	Todos	Supervisión	Primario	Recurso humano	No aplica	Local de San Luis y Los Olivos
R3	Facturador	Responsable de generar las facturas y su declaratoria ante los entes reguladores.	Ingresos	Generación de Pre-Liquidación Generación de Factura	Primario	Recurso humano	No aplica	Local de San Luis y Los Olivos
R4	Médico/Técnico	Responsable de evaluar al paciente e ingresar, de ser el caso, los resultados al sistema MediWeb	Ingresos	Atención Ocupacional	Primario	Recurso humano	No aplica	Local de San Luis y Los Olivos

ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
R5	Licenciado	Responsable de registrar resultados de evaluaciones/exámenes en el sistema MediWeb y encargado de gestionar la comunicación de los mismos al cliente.	Ingresos	Registro de resultados en el sistema Comunicación de Resultados	Primario	Recurso humano	No aplica	Local de San Luis y Los Olivos
R6	Médico Auditor	Responsable de auditar los resultados de las revisiones/exámenes y hacerse responsable por los mismos.	Ingresos	Revisión de Resultados	Primario	Recurso humano	No aplica	Local de San Luis y Los Olivos
R7	Tesorero	Responsable de gestionar las cuentas por cobrar.	Ingresos	Registro de Cobro	Soporte	Recurso humano	No aplica	Local de San Luis y Los Olivos
R8	Logístico	Responsable de gestionar el inventario y el abastecimiento.	Compras y Gestión de Inventario	Gestión de Compra Recepción de Mercadería	Primario	Recurso humano	No aplica	Local de San Luis y Los Olivos

ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
S1	MediWeb	Sistema que permite la atención ocupacional y su facturación.	Ingresos	Participa en todo el proceso de ingresos.	Primario	Software	Administrador	Digital
S2	Sistema Logístico Medcam	Sistema que permite la gestión de inventario.	Gestión de Inventario	Gestión de Inventario	Primario	Software	Logístico	Digital
S3	Office	Es una suite ofimática que permite diseñar y producir documentos.	Otros	Otros	Soporte	Software	Administrador	Digital
H1	Servidor de Aplicaciones	Equipo informático que soporta las aplicaciones de negocio.	Todos	Varios	Primario	Hardware	Administrador	Local de San Luis y Los Olivos
H2	Servidor de Correos	Equipo informático que soporta la gestión de correos electrónicos.	Todos	Varios	Primario	Hardware	Administrador	Local de San Luis y Los Olivos

ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
H3	Computadora de escritorio	Equipo informático que permite a los usuarios de negocio la realización de sus funciones.	Todos	Varios	Primario	Hardware	Administrador	Local de San Luis y Los Olivos
H4	Lector biométrico	Equipo que permite la lectura de la huella digital.	Ingresos	Registro de Paciente	Primario	Hardware	Administrador	Local de San Luis y Los Olivos
H5	Fotocopiadora / Impresora	Equipo que permite obtener los documentos digitales en físicos.	Todos	Comunicación de Resultados	Soporte	Hardware	Administrador	Local de San Luis y Los Olivos
H6	Electrocardiograma	Equipo que permite la representación gráfica de la actividad eléctrica del corazón	Ingresos	Atención Ocupacional	Primario	Hardware	Administrador	Local de San Luis y Los Olivos
H7	Máquina de Rayos X	Equipo que permite la representación gráfica de la estructura ósea del paciente.	Ingresos	Atención Ocupacional	Primario	Hardware	Administrador	Local de San Luis y Los Olivos

ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
H8	Instrumento oftalmológico	Equipo que permite realizar revisiones oftalmológicas.	Ingresos	Atención Ocupacional	Primario	Hardware	Administrador	Local de San Luis y Los Olivos
H9	Instrumento de análisis de muestras	Equipo que permite evaluaciones específicas sobre las muestras de los pacientes.	Ingresos	Atención Ocupacional	Primario	Hardware	Administrador	Local de San Luis y Los Olivos
H10	Equipos de laboratorio	Equipo que permite evaluaciones químicas sobre las muestras de los pacientes.	Ingresos	Atención Ocupacional	Primario	Hardware	Administrador	Local de San Luis y Los Olivos
I1	Historia clínica	Documento médico-legal donde se recoge la información necesaria para la correcta atención de los pacientes.	Ingresos	Registro de Paciente Manual	Primario	Información	Médico Auditor	Físico
I2	Hoja de ruta	Documento que contiene los datos básicos del paciente y las especialidades en las cuales se debe	Ingresos	Generación de Hojas de ruta	Soporte	Información	Médico/Técnico	Físico

ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
		atender en su visita.						
13	Hoja de ruta Laboratorio	Documento que contiene los datos básicos del paciente y los exámenes de laboratorio que debe realizarse durante su visita.	Ingresos	Generación de Hojas de Ruta	Soporte	Información	Médico/Técnico	Físico
14	Datos de filiación	Documento que contiene los datos personales del cliente e información sobre las labores que desempeña en su centro de labores.	Ingresos	Registro de Paciente	Soporte	Información	Recepcionista	Físico
15	Consentimiento informado - ley	Documento de carácter legal en el cual el paciente autoriza a MEDCAM a realizarle exámenes que son de su conocimiento y a	Ingresos	Consentimiento Informado	Primario	Información	Recepcionista	Físico

ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
		compartir los resultados con su empleador.						
16	Consentimiento informado - atención	Documento de carácter legal en el cual el paciente confirma que la información que proporciona es real y autoriza a MEDAM a compartir los resultados con su médico ocupacional.	Ingresos	Consentimiento Informado	Primario	Información	Recepcionista	Físico
17	Hoja de interconsulta	Documento médico en el cual se detalla el resultado negativo de una evaluación médica realizada por MEDCAM, y los resultados y tratamientos realizados por un médico especialista en respuesta.	Ingresos	Garantía de tratamiento adicional	Soporte	Información	Licenciado	Físico



ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
18	Resultados finales	Documento médico en el cual se detallan los resultados de la totalidad de evaluaciones realizadas por MEDCAM.	Ingresos	Comunicación de resultados	Primario	Información	Médico Auditor	Físico
19	Factura electrónica	Documento contable que establece la responsabilidad del cliente de compensar el servicio prestado por MEDCAM.	Ingresos	Generación de factura	Primario	Información	Facturador	Físico
110	Protocolo (Cotización)	Documento mediante el cual se ofrecen los servicios de medicina ocupacional estableciendo una propuesta de evaluaciones y sus respectivos costos.	Ingresos	Contacto con el cliente	Soporte	Información	Comercial	Físico

ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
I11	Historia clínica digital	Documento médico-legal donde se recoge la información necesaria para la correcta atención de los pacientes almacenada en la aplicación MediWeb.	Ingresos	Atención Ocupacional	Primario	Información	Medico Auditor	Digital
I12	Kardex	Es un documento en el cual se registran los datos de entrada, salidas y saldos de las existencias de la empresa.	Gestión de inventario	Gestión de inventario	Primario	Información	Comercial	Digital
I13	Lista de pacientes	Documento enviado por el cliente para determinar los pacientes que serán atendidos.	Ingresos	Coordinación de atención	Primario	Información	Comercial	Digital
I14	Cronograma	Documento establecido por el MEDAM-cliente para determinar las fechas de atención de los pacientes.	Ingresos	Coordinación de atención	Soporte	Información	Comercial	Digital

ID Activo	Nombre	Descripción	Proceso	Sub-proceso	Clasificación de Activo	Sub Clasificación	Propietario de Activo	Ubicación
S1	Local de San Luis	Establecimiento en el cual se desarrollan las operaciones de la empresa, ubicado en el distrito de San Luis	Otros	Soporte de Infraestructura de todos los procesos.	Primario	Sitio	Gerencia General	Local de San Luis y Los Olivos
S2	Local de Los Olivos	Establecimiento en el cual se desarrollan las operaciones de la empresa, ubicado en el distrito de Los Olivos	Otros	Soporte de Infraestructura de todos los procesos.	Soporte	Sitio	Gerencia General	Local de San Luis y Los Olivos
Se1	Internet	Servicio que permite la interconexión de la empresa con la información, clientes y proveedores.	Todos	Envío de factura, Comunicación de resultados y Recepción de Pagos	Primario	Servicio	Administrador	Local de San Luis y Los Olivos
S4	Base de datos	Motor de base de datos para los sistema MediWeb y Sistema de Inventario	Todos	Participa en todo el proceso de ingresos y compras.	Primario	Software	Administrador	Digital

Elaboración: Los autores.

Una vez identificados claramente los activos, que están involucrados en cada proceso, se procederá a la valorización de los mismos siguiendo las dimensiones que persigue la ISO/IEC 27001, la integridad, disponibilidad y confidencialidad de los activos. Cada dimensión tendrá una escala del 1 al 4 como se muestra en la Tabla 18.

**Tabla 18 – Valores asignados a las dimensiones del activo**

Valor	Dimensiones		
	Confidencialidad	Disponibilidad	Integridad
1	Activo libre, se puede difundir y es de dominio público.	La tolerancia de que el activo no esté disponible es de 1 semana.	Los errores o modificaciones no autorizadas no generan ningún impacto al negocio.
2	Activo restringido, solo puede ser de uso interno. Si se filtra, no ocasionaría un riesgo.	La tolerancia de que el activo no esté disponible es de no más de 1 día.	Los errores o modificaciones no autorizadas generan un impacto leve al negocio.
3	Activo protegido, se debe tener controles para el acceso. Si se llega a filtrar, ocasionaría un riesgo moderado al negocio.	La tolerancia de que el activo no esté disponible es de no más de 1 hora.	Los errores o modificaciones no autorizadas generan un impacto moderado al negocio.
4	Activo confidencial, información sensible y no se puede difundir bajo ningún concepto. Su filtración ocasionaría un riesgo crítico para el negocio.	No se tolera que el activo no esté disponible.	Los errores o modificaciones no autorizadas generan un impacto crítico al negocio.

Elaboración: Los autores

Una vez identificado el nivel en cada dimensión de los activos (Ver Tabla 19), se procederá a realizar el promedio de estos para obtener el valor del activo. Según el apetito de riesgo de MEDCAM, se ha establecido que los activos con un promedio igual o mayor a 3 serán los seleccionados para realizar el análisis de riesgos, el tratamiento y la propuesta de controles, ya que son los activos de información que busca proteger la organización.

Tabla 19 – Valorización de activos

Cod	Nombre	Criterios de Valorización			Valor Final
		Confidencialidad	Disponibilidad	Integridad	
R1	Gerente general	0	2	0	1
R2	Administrador	0	3	0	1
R3	Facturador	0	3	0	1
R4	Médico/Técnico	0	4	0	1
R5	Licenciado	0	4	0	1
R6	Médico auditor	0	4	0	1
R7	Tesorero	0	2	0	1
R8	Logístico	0	3	0	1
S1	MediWeb	4	4	4	4
S2	Sistema Logístico Medcam	2	2	4	3
S3	Office	1	1	2	1
S4	Base de datos	3	3	3	3
H1	Servidor de aplicaciones	4	3	4	4
H2	Servidor de correos	2	2	2	2
H3	Computadora de escritorio	1	4	3	3
H4	Lector biométrico	1	1	1	1
H5	Fotocopiadora/Impresora	1	2	2	2
H6	Electrocardiograma	2	3	2	2
H7	Máquina de rayos X	2	3	2	2
H8	Instrumento oftalmológico	2	3	2	2
H9	Instrumento análisis de muestras	2	3	2	2
H10	Equipos de laboratorio	2	3	2	2
I1	Historia clínica	4	4	4	4
I2	Hoja de ruta	2	2	2	2
I3	Hoja de ruta laboratorio	2	2	2	2
I4	Datos de filiación	3	2	2	2
I5	Consentimiento informado - ley	2	4	3	3
I6	Consentimiento informado - atención	2	4	3	3
I7	Hoja de interconsulta	3	4	4	4
I8	Resultados finales	4	4	4	4

Cod	Nombre	Criterios de Valorización			Valor Final
		Confidencialidad	Disponibilidad	Integridad	
I9	Factura electrónica	2	2	3	2
I10	Protocolo (Cotización)	1	2	1	1
I11	Historia clínica digital	4	4	4	4
I12	Kardex	2	3	3	3
I13	Lista de pacientes	3	2	2	2
I14	Cronograma	1	2	1	1
S1	Local de San Luis	0	4	0	1
S2	Local de Los Olivos	0	4	0	1
Se1	Internet	1	2	2	2

Elaboración: Los autores

- **Etapas 2: Hacer**

En esta etapa se le da respuesta a los riesgos identificados a través del establecimiento de políticas, las cuales consideran controles, así como herramientas de capacitación, entre otras.

- **Fase 6: Gestionar los riesgos y crear un plan de tratamiento de riesgos**

Para la gestión de los riesgos, se usará la metodología seleccionada en la fase 4. Como se mencionó previamente, una vez identificados los activos y después de haberlos valorado, se debe identificar las amenazas y vulnerabilidades a los que está expuesto. El análisis se puede ver en la siguiente tabla. (Ver Tabla 20)

Tabla 20 – Amenazas y Vulnerabilidades de los Activos

ID Activo	Nombre de Activo	Vulnerabilidad	Amenaza
S1	MediWeb	Falta de finalización de sesión por parte del usuario	Abuso de derechos
		Defectos de Software	Abuso de derechos
		Defectos de Software	Mal funcionamiento del Software
		Falla en la distribución de accesos	Abuso de derechos
		Falta de Documentación	Error en el uso
		Parámetros incorrectamente configurados	Error en el uso
		Falta de Respaldos	Saturación del sistema de

ID Activo	Nombre de Activo	Vulnerabilidad	Amenaza
			información
		Falta de monitoreo de los recursos de procesamiento de información	Tratamiento ilegal de datos
		Falta de procedimiento formal para el registro y eliminación de usuarios.	Error en el uso
		Falta de procedimiento para el manejo de información clasificada	Error en el uso
S2	Sistema Logístico de MedCam	Falta de finalización de sesión por parte del usuario	Abuso de derechos
		Defectos de Software	Mal funcionamiento del Software
		Interfaz de usuario complicada	Error en el uso
		Interfaz de usuario complicada	Incumplimiento en el mantenimiento del sistema
		Falta de Documentación	Error en el uso
		Parámetros incorrectamente configurados	Error en el uso
		Falta o insuficientes pruebas de software	Mal funcionamiento del Software
		Falta de Respaldos	Saturación del sistema de información
		Especificaciones no claras o erradas para los desarrolladores	Error en el uso
		Falla en la producción de informes de gestión	Tratamiento ilegal de datos
H3	Computadoras de escritorio	Mantenimiento insuficiente	Fallo del equipo
		Falta de esquema de reemplazo periódico	Destrucción del equipo
		Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento
		Susceptibilidad a la variación de la tensión	Falla en la energía eléctrica
		Copias no controladas	Robo de documentación
		Almacenamiento sin protección	Robo de documentación
		Falta de un eficiente control de cambios	Error en el uso
		Falta de Protección física de las puertas y ventanas de la edificación	Robo de documentación
I5	Consentimiento informado - ley	Falta de procedimiento de monitoreo de recursos de procesamiento de información	Datos de fuentes no confiables
		Falta de procedimientos formales para la autorización de la información pública	Abuso de derechos
		Falta de política de limpieza de escritorio y de pantalla	Robo de documentación

ID Activo	Nombre de Activo	Vulnerabilidad	Amenaza
		Falta de procedimientos para el manejo de información clasificada	Accidente grave
		Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento
		Falta de Protección física de las puertas y ventanas de la edificación	Robo de documentación
H1	Servidor de aplicaciones	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema
		Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento
		Susceptibilidad a la variación de la tensión	Destrucción del equipo
		Falta de un eficiente control de cambios	Error en el uso
		Falta de Cuidado en la disposición final	Destrucción del equipo
		Conexión deficiente de los cables	Saturación del sistema de información
		Arquitectura insegura de red	Interceptación de señales
I1	Historia clínica	Falta de Protección física de las puertas y ventanas de la edificación	Robo de equipo
		Falta de procedimiento de monitoreo de recursos de procesamiento de información	Datos de fuentes no confiables
		Falta de procedimientos formales para la autorización de la información pública	Abuso de derechos
		Falta de política de limpieza de escritorio y de pantalla	Robo de documentación
		Falta de procedimientos para el manejo de información clasificada	Accidente grave
		Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento
		Falta de mecanismos de monitoreo	Data corrupta
		Almacenamiento sin protección	Robo de documentación
I6	Consentimiento informado - atención	Falta de procedimiento de monitoreo de recursos de procesamiento de información	Datos de fuentes no confiables
		Falta de procedimientos formales para la autorización de la información pública	Abuso de derechos
		Falta de política de limpieza de escritorio y de pantalla	Robo de documentación
		Falta de procedimientos para el manejo de información clasificada	Accidente grave
		Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento



ID Activo	Nombre de Activo	Vulnerabilidad	Amenaza
		Falta de Protección física de las puertas y ventanas de la edificación	Robo de documentación
17	Hoja interconsulta	Falta de procedimiento de monitoreo de recursos de procesamiento de información	Datos de fuentes no confiables
		Falta de procedimientos formales para la autorización de la información pública	Abuso de derechos
		Falta de política de limpieza de escritorio y de pantalla	Robo de documentación
		Falta de procedimientos para el manejo de información clasificada	Accidente grave
18	Resultados finales	Falta de procedimiento de monitoreo de recursos de procesamiento de información	Datos de fuentes no confiables
		Falta de procedimientos formales para la autorización de la información pública	Abuso de derechos
		Falta de política de limpieza de escritorio y de pantalla	Robo de documentación
		Falta de procedimientos para el manejo de información clasificada	Accidente grave
		Susceptibilidad a la humedad, polvo y suciedad	Polvo, corrosión, congelamiento
		Falta de Protección física de las puertas y ventanas de la edificación	Robo de documentación
		Almacenamiento sin protección	Robo de documentación
111	Historia clínica digital	Falta de Respaldos	Error en el uso
		Fechas Incorrectas	Incumplimiento en el mantenimiento del sistema
		Copias no controladas	Robo de documentación
		Falla en la distribución de accesos	Abuso de derechos
		Falta de política de limpieza de escritorio y de pantalla	Tratamiento ilegal de datos
		Falta de procedimiento de monitoreo de recursos de procesamiento de información	Datos de fuentes no confiables
		Falta de procedimientos formales para la autorización de la información pública	Abuso de derechos
S4	Base de datos	Falta de finalización de sesión por parte del usuario	Abuso de derechos
		Falla en la distribución de accesos	Divulgación de la información

ID Activo	Nombre de Activo	Vulnerabilidad	Amenaza
		Falta de Documentación	Error en el uso
		Parámetros incorrectamente configurados	Mal funcionamiento del Software
		Falta de mecanismos de autenticación	Data corrupta
		Tabla de contraseñas desprotegidas	Divulgación de la información
		Pobre gestión de contraseñas	Data corrupta
		Falta de Respaldos	Fallo de equipo
		Falta de Protección física	Manipulación de Software
112	Kardex	Falta de Respaldos	Error en el uso
		Fechas Incorrectas	Incumplimiento en el mantenimiento del sistema
		Copias no controladas	Robo de documentación
		Falla en la distribución de accesos	Abuso de derechos
		Falta de política de limpieza de escritorio y de pantalla	Tratamiento ilegal de datos
		Falta de procedimientos formales para la autorización de la información pública	Abuso de derechos

Elaboración: Los autores

Una vez realizado dicho análisis, se procede a la creación del mapa de riesgos y sus consecuencias, se dieron valores a la probabilidad e impacto de la ocurrencia obteniendo como resultado la criticidad de los riesgos en los procesos de negocio (Ver Tabla 21).

En respuesta a los riesgos identificados como altos y críticos se determinó como tratamiento de riesgo es establecimiento de controles y el establecimiento de políticas de seguridad que la organización debe implementar para asegurar sus activos de información (Ver Tabla 22).

Tabla 21 – Matriz de riesgos

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R1	S1	MediWeb	Acceso de usuarios no autorizados debido a que no se finalizó la sesión en el aplicativo.	Robo de Información Acceso a información no autorizada Data corrupta	Improbable	Crítico	Alto	Reducir
R2			Acceso a permisos no autorizados debido a defectos en el software	Robo de Información Acceso a información no autorizada Data corrupta	Raro	Crítico	Medio	Retener
R3			Error en el procesamiento de datos debido a defectos en el software	Data corrupta Pérdida de información	Improbable	Relevante	Medio	Retener
R4			Acceso a permisos no autorizados debido a un error en la asignación de permisos	Robo de Información Acceso a información no autorizada Inserción de data corrupta	Improbable	Crítico	Alto	Reducir
R5			Error en el uso del aplicativo debido a que no se tiene una documentación adecuada sobre las funciones del aplicativo	Data corrupta Demora en el proceso	Probable	Relevante	Alto	Reducir
R6			Error en las transacciones y uso del aplicativo debido a que no se configuró correctamente los parámetros iniciales del aplicativo	Data corrupta Demora en el proceso	Raro	Relevante	Bajo	Retener
R7			Indisponibilidad parcial o permanente del aplicativo debido a que no se cuenta con un respaldo del mismo	Indisponibilidad del aplicativo Pérdida de información	Posible	Alto	Alto	Reducir

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R8			Transacciones no autorizadas sin poder rastrear al usuario que modificó debido a que no se cuenta con un log de operaciones	Data corrupta	Posible	Relevante	Medio	Retener
R9			Acceso de usuarios que ya no están dentro de la organización debido a que no se les dio de baja cuando correspondía	Robo de información Acceso a información no autorizada Data corrupta	Posible	Crítico	Alto	Reducir
R10			Manejo incorrecto de información clasificada dentro del aplicativo debido a que no se cuenta con procedimiento para el manejo de los mismos	Acceso a información no autorizada	Improbable	Alto	Medio	Retener
R11	S2	Sistema Logístico de MedCam	Acceso de usuarios no autorizados debido a que no se finalizó la sesión en el aplicativo.	Robo de Información Acceso a información no autorizada Data corrupta	Improbable	Alto	Medio	Retener
R12			Error en el procesamiento de datos debido a defectos en el software	Data corrupta Demora en el proceso	Posible	Relevante	Medio	Retener
R13			Error en el uso del aplicativo debido a que la interfaz es muy compleja para el usuario	Data corrupta Demora en el proceso	Posible	Relevante	Medio	Retener
R14			Falta de actualización del inventario debido a que el interfaz es muy compleja	Data corrupta	Probable	Relevante	Alto	Reducir

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R15			Error en el uso del aplicativo debido a que no se tiene una documentación adecuada sobre las funciones del aplicativo	Data corrupta Demora en el proceso	Probable	Relevante	Alto	Reducir
R16			Error en las transacciones y uso del aplicativo debido a que no se configuró correctamente los parámetros iniciales del aplicativo	Data corrupta Demora en el proceso	Posible	Relevante	Medio	Retener
R17			Errores en el aplicativo o desconocimiento de funciones debido a que no se realizaron las pruebas de software al adquirir el aplicativo	Data corrupta Demora en el proceso	Posible	Relevante	Medio	Retener
R18			Indisponibilidad parcial o permanente del aplicativo debido a que no se cuenta con un respaldo del mismo	Indisponibilidad del aplicativo Pérdida de información	Posible	Relevante	Medio	Retener
R19			Interfaz, funciones desconocidas y desconocimiento del aplicativo debido a que no se especificó al proveedor las necesidades del negocio	Indisponibilidad del aplicativo Pérdida de información Demora en el proceso	Posible	Relevante	Medio	Retener
R20			Transacciones no autorizadas sin poder rastrear al usuario que modificó debido a que no se cuenta con un log de operaciones	Data corrupta	Posible	Relevante	Medio	Retener
R21			S4	Base de datos	Acceso de usuarios no autorizados debido a que no se finalizó la sesión en el aplicativo.	Robo de Información Acceso a información no autorizada Data corrupta	Improbable	Alto
R22	Acceso a permisos no autorizados debido a un error en la asignación de permisos	Robo de Información Acceso a información no autorizada Inserción de data corrupta			Improbable	Relevante	Medio	Retener

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R23			Error en el uso del aplicativo debido a que no se tiene una documentación adecuada sobre las funciones del aplicativo	Data corrupta Demora en el proceso	Improbable	Moderado	Bajo	Retener
R24			Error en las transacciones y uso del aplicativo debido a que no se configuró correctamente los parámetros del aplicativo	Data corrupta Demora en el proceso	Improbable	Moderado	Bajo	Retener
R25			Acceso de usuarios no autorizados debido a que no se cuenta con mecanismos de autenticación.	Robo de Información Acceso a información no autorizada Inserción de data corrupta	Improbable	Crítico	Alto	Reducir
R26			Acceso de usuarios no autorizados debido a que la tabla de contraseñas de la aplicación es expuesta.	Robo de Información Acceso a información no autorizada Inserción de data corrupta	Improbable	Alto	Medio	Retener
R27			Acceso de usuarios no autorizados debido a que no se cuenta con una política de contraseñas que establezca la gestión de la misma.	Robo de Información Acceso a información no autorizada Inserción de data corrupta	Improbable	Alto	Medio	Retener
R28			Indisponibilidad parcial o permanente del aplicativo debido a que no se cuenta con un respaldo del mismo	Indisponibilidad del aplicativo Pérdida de información	Improbable	Crítico	Alto	Reducir
R29			Data corrupta debido a manipulación no autorizada.	Data corrupta	Improbable	Moderado	Medio	Retener
R30	H3	Computadoras de escritorio	Malfuncionamiento de equipo debido a que no se le realizó correctamente los mantenimientos necesarios	Indisponibilidad Pérdida de Información	Posible	Relevante	Medio	Retener

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R31			Malfuncionamiento y uso de equipos obsoletos debido a que no se cuenta con un esquema de reemplazo periódico	Indisponibilidad del equipo Pérdida de Información	Posible	Relevante	Medio	Retener
R32			Malfuncionamiento de equipo debido a que el equipo no está protegido frente al polvo, corrosión y congelamiento	Indisponibilidad del equipo Pérdida de Información	Posible	Relevante	Medio	Retener
R33			Dstrucción del equipo debido a una fluctuación en la energía eléctrica	Indisponibilidad del equipo Pérdida de Información	Improbable	Relevante	Medio	Retener
R34			Robo de documentos confidenciales debido a que el equipo no cuenta con una seguridad como autenticación de usuario	Robo de Información	Probable	Alto	Alto	Reducir
R35			Robo de documentos confidenciales debido a que el equipo no almacena los documentos de una forma segura	Robo de Información	Probable	Alto	Alto	Reducir
R36			Error en el uso de los equipos debido a una mala configuración inicial del equipo	Indisponibilidad del equipo	Improbable	Relevante	Medio	Retener
R37			Robo del equipo debido a la intrusión de un tercero ya que no cuentan con una protección física eficaz	Robo de Información	Probable	Alto	Alto	Reducir
R38	15	Consentimiento informado - ley	Documento con errores deliberados de parte del paciente debido a que no se monitorea correctamente el documento	Data corrupta	Raro	Relevante	Bajo	Retener

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R39			Documento errado o con omisiones debido a que no se monitoreó correctamente el procesamiento del consentimiento informado	Data corrupta	Raro	Relevante	Bajo	Retener
R40			Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público	Robo de Información Acceso a información no autorizada	Posible	Relevante	Medio	Retener
R41			Pérdida o destrucción del documento debido a que no se cuenta con procedimientos de manejo de información sensible	Pérdida de Información	Posible	Alto	Alto	Reducir
R42			Destrucción de documento debido a que se almacenó en un almacén expuesto a la intemperie	Pérdida de Información	Posible	Alto	Alto	Reducir
R43			Robo de documentación debido a la intrusión de un tercero ya que no cuentan con una protección física eficaz	Robo de Información	Posible	Alto	Alto	Reducir
R44	I1	Historia clínica	Robo del documento debido a que no cuentan con una seguridad física eficaz	Robo de Información	Probable	Crítico	Crítico	Reducir
R45			Documento con errores deliberados de parte del paciente debido a que no se monitorea correctamente el documento	Data corrupta	Raro	Relevante	Bajo	Retener



ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R46			Documento errado o con omisiones debido a que no se monitoreó correctamente el procesamiento del consentimiento informado	Data corrupta	Raro	Relevante	Bajo	Retener
R47			Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público en el escritorio	Robo de Información Acceso a información no autorizada	Probable	Crítico	Crítico	Reducir
R48			Pérdida o destrucción del documento debido a que no se cuenta con procedimientos de manejo de información sensible	Pérdida de Información	Improbable	Crítico	Alto	Reducir
R49			Destrucción de documento debido a que se almacenó en un almacén expuesto a la intemperie	Pérdida de Información	Probable	Crítico	Crítico	Reducir
R50			Robo de documentación debido a la intrusión de un tercero ya que se encuentra en un almacén sin protección	Robo de información	Posible	Crítico	Alto	Reducir
R51			Inserción de data incorrecta debido a acciones deliberadas por parte del personal	Data corrupta	Improbable	Crítico	Alto	Reducir
R52	16	Consentimiento informado - atención	Documento con errores deliberados de parte del paciente debido a que no se monitorea correctamente el documento	Data corrupta	Raro	Relevante	Bajo	Retener

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R53			Documento errado o con omisiones debido a que no se monitoreó correctamente el procesamiento del consentimiento informado	Data corrupta	Raro	Relevante	Bajo	Retener
R54			Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público	Robo de Información Acceso a información no autorizada	Posible	Crítico	Alto	Reducir
R55			Pérdida o destrucción del documento debido a que no se cuenta con procedimientos de manejo de información sensible	Pérdida de Información	Improbable	Alto	Medio	Retener
R56			Destrucción de documento debido a que se almacenó en un almacén expuesto a la intemperie	Pérdida de Información	Posible	Alto	Alto	Reducir
R57			Robo de documentación debido a la intrusión de un tercero ya que no cuentan con una protección física eficaz	Robo de información	Posible	Crítico	Alto	Reducir
R58	17	Hoja interconsulta	Documento con errores deliberados de parte del paciente debido a que no se monitorea correctamente el documento	Data corrupta	Raro	Relevante	Bajo	Retener
R59			Documento errado o con omisiones debido a que no se monitoreó correctamente el procesamiento del consentimiento informado	Data corrupta	Raro	Relevante	Bajo	Retener
R60			Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público	Robo de Información Acceso a información no autorizada	Posible	Crítico	Alto	Reducir

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R61			Pérdida o destrucción del documento debido a que no se cuenta con procedimientos de manejo de información sensible	Pérdida de Información	Improbable	Alto	Medio	Retener
R62	18	Resultados finales	Documento con errores deliberados de parte del paciente debido a que no se monitorea correctamente el documento	Data corrupta	Raro	Relevante	Bajo	Retener
R63			Documento errado o con omisiones debido a que no se monitoreó correctamente el procesamiento del consentimiento informado	Data corrupta	Raro	Relevante	Bajo	Retener
R64			Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público	Robo de Información Acceso a información no autorizada	Probable	Crítico	Crítico	Reducir
R65			Pérdida o destrucción del documento debido a que no se cuenta con procedimientos de manejo de información sensible	Pérdida de Información	Improbable	Crítico	Alto	Reducir
R66			Destrucción de documento debido a que se almacenó en un almacén expuesto a la intemperie	Pérdida de Información	Probable	Crítico	Crítico	Reducir
R67			Robo de documentación debido a la intrusión de un tercero ya que no cuentan con una protección física eficaz	Robo de Información	Probable	Crítico	Crítico	Reducir

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R68			Robo de documentos confidenciales debido a que es almacenado en un lugar sin seguridad	Robo de Información	Posible	Crítico	Alto	Reducir
R69	I11	Historia clínica digital	Indisponibilidad parcial o permanente del documento debido a que no se cuenta con un respaldo del mismo	Indisponibilidad del aplicativo Pérdida de información	Probable	Alto	Alto	Reducir
R70			Error en el guardado y clasificación por fechas de las historias clínicas debido a que las fechas del aplicativo no esté sincronizado con el sistema operativo	Data corrupta Indisponibilidad del documento	Improbable	Alto	Medio	Retener
R71			Robo de documentación debido a que se hagan copias no autorizadas de las historias clínicas	Robo de Información	Probable	Crítico	Crítico	Reducir
R72			Acceso al documento de un tercero debido a que no se definió los accesos correctamente	Acceso a información no autorizada	Improbable	Crítico	Alto	Reducir
R73			Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público	Robo de Información Acceso a información no autorizada	Probable	Crítico	Crítico	Reducir
R74			Documento con errores deliberados de parte del paciente debido a que no se monitorea correctamente el documento por un especialista	Data corrupta	Posible	Relevante	Medio	Retener
R75			Documento errado o con omisiones debido a que no se monitoreó correctamente el procesamiento de la historia clínica	Data corrupta	Raro	Relevante	Bajo	Retener

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R76	H1	Servidor de aplicaciones	Lentitud y fallos en los sistemas debido a que no se realicen los mantenimientos necesarios	Demora en el proceso Indisponibilidad del servidor	Posible	Relevante	Medio	Retener
R77			Malfuncionamiento del servidor debido a que se encuentra expuesto a polvo, suciedad y humedad	Indisponibilidad del servidor	Posible	Relevante	Medio	Retener
R78			Destrucción del equipo debido a que no cuenta con estabilizadores necesarios	Indisponibilidad del servidor	Raro	Crítico	Medio	Retener
R79			Malfuncionamiento del servidor debido a la mala configuración inicial del servidor	Indisponibilidad del servidor	Posible	Alto	Alto	Reducir
R80			Destrucción del equipo debido a que se encuentra dispuesto en una zona no segura	Indisponibilidad del servidor	Improbable	Alto	Medio	Retener
R81			Lentitud y fallos en los sistemas debido a que no se cuenta con un sistema de enrutamiento eficiente	Indisponibilidad del servidor	Posible	Relevante	Medio	Retener
R82			Robo de información debido a que poseen una arquitectura de red muy insegura	Robo de Información	Raro	Crítico	Medio	Retener
R83			Indisponibilidad parcial o permanente de la base de datos debido a que no se cuenta con un respaldo del mismo	Indisponibilidad del equipo Pérdida de Información	Posible	Crítico	Alto	Reducir
R84			Lentitud en los sistemas o conflictos debido a que algunos servicios innecesarios estén habilitados	Data corrupta Demora en el proceso	Posible	Relevante	Medio	Retener

ID Riesgo	ID Activo	Nombre de Activo	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R85			Pérdida de información debido a que no se realicen los respaldos	Pérdida de Información	Posible	Crítico	Alto	Reducir
R86	I12	Kardex	Indisponibilidad parcial o permanente del aplicativo debido a que no se cuenta con un respaldo del mismo.	Indisponibilidad del aplicativo Pérdida de información	Posible	Relevante	Medio	Retener
R87			Error en el registro de movimientos de almacén debido a que las fechas del aplicativo no estén sincronizadas con el sistema operativo.	Data corrupta Indisponibilidad del documento	Posible	Alto	Alto	Reducir
R88			Robo de documentación debido a que se hagan copias no autorizadas de los movimientos de mercadería.	Robo de Información	Improbable	Relevante	Medio	Retener
R89			Acceso al documento de un tercero debido a que no se definió los accesos correctamente.	Acceso a información no autorizada	Raro	Relevante	Bajo	Retener
R90			Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público.	Robo de Información Acceso a información no autorizada	Improbable	Alto	Medio	Retener
R91			Usuarios no autorizados tienen acceso a información de la empresa.	Data corrupta	Posible	Relevante	Medio	Retener

Elaboración: Los autores

Tabla 22 – Controles Identificados

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC 27002:2013
R1	Acceso de usuarios no autorizados debido a que no se finalizó la sesión en el aplicativo.	Alto	A.9 Control de acceso A.11 Seguridad física y ambiental	A.9.4.3 - Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad. A.11.2.9 - Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamiento de la información debe ser adoptada.
R4	Acceso a permisos no autorizados debido a un error en la asignación de permisos	Alto	A.9 Control de acceso	A.9.2.1 - Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de accesos. A.9.2.5 - Los propietarios de los activos deben revisar los derechos de accesos de usuario a intervalos regulares.
R5	Error en el uso del aplicativo debido a que no se tiene una documentación adecuada sobre las funciones del aplicativo	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.
R7	Indisponibilidad parcial o permanente del aplicativo debido a que no se cuenta con un respaldo del mismo	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC 27002:2013
R9	Acceso de usuarios que ya no están dentro de la organización debido a que no se les dio de baja cuando correspondía	Alto	A.9 Control de acceso	A.9.2.1 - Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de accesos. A.9.2.5 - Los propietarios de los activos deben revisar los derechos de accesos de usuario a intervalos regulares.
R14	Falta de actualización del inventario debido a que el interfaz es muy compleja	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan. A.12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo apropiado.
R15	Error en el uso del aplicativo debido a que no se tiene una documentación adecuada sobre las funciones del aplicativo	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.
R25	Acceso de usuarios no autorizados debido a que no se cuenta con mecanismos de autenticación.	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.



ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC 27002:2013
R28	Indisponibilidad parcial o permanente del aplicativo debido a que no se cuenta con un respaldo del mismo	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.
R34	Robo de documentos confidenciales debido a que el equipo no cuenta con una seguridad como autenticación de usuario	Alto	A.9 Control de acceso A.11 Seguridad física y ambiental	A.9.4.3 - Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad. A.11.2.9 - Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamiento de la información debe ser adoptada.
R35	Robo de documentos confidenciales debido a que el equipo no almacena los documentos de una forma segura	Alto	A.8 Gestión de Activos	A.8.1.1 - Información, otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos de ser elaborado y mantenido. A.8.1.2 - Los activos mantenidos en el inventario deben ser propios.
R37	Robo del equipo debido a la intrusión de un tercero ya que no cuentan con una protección física eficaz	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.
R41	Pérdida o destrucción del documento debido a que no se cuenta con procedimientos de manejo de información sensible	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC 27002:2013
R42	Dstrucción de documento debido a que se almacenó en un almacén expuesto a la intemperie	Alto	A.11 Seguridad física y ambiental	A.11.1.4 - Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.
R43	Robo de documentación debido a la intrusión de un tercero ya que no cuentan con una protección física eficaz	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.
R44	Robo del documento debido a que no cuentan con una seguridad física eficaz	Crítico	A.11 Seguridad física y ambiental A.18 Cumplimiento	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado. A.18.1.4. - La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevante donde sea aplicable.
R47	Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público en el escritorio	Crítico	A.11 Seguridad física y ambiental A.18 Cumplimiento	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información. A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado. A.18.1.4. - La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevante donde sea aplicable.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC 27002:2013
R48	Pérdida o destrucción del documento debido a que no se cuenta con procedimientos de manejo de información sensible	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.
R49	Dstrucción de documento debido a que se almacenó en un almacén expuesto a la intemperie	Crítico	A.11 Seguridad física y ambiental	A.11.1.4 - Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.
R50	Robo de documentación debido a la intrusión de un tercero ya que se encuentra en un almacén sin protección	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.
R51	Inserción de data incorrecta debido a acciones deliberadas por parte del personal	Alto	A.6 Organización de la seguridad de la información	A.6.1.3 - Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.
R54	Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.
R56	Dstrucción de documento debido a que se almacenó en un almacén expuesto a la intemperie	Alto	A.11 Seguridad física y ambiental	A.11.1.4 - Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC 27002:2013
R57	Robo de documentación debido a la intrusión de un tercero ya que no cuentan con una protección física eficaz	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.
R60	Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.
R64	Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público	Crítico	A.8 Gestión de Activos A.11 Seguridad física y ambiental	A.8.3.3 - Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte. A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.
R65	Pérdida o destrucción del documento debido a que no se cuenta con procedimientos de manejo de información sensible	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.
R66	Destrucción de documento debido a que se almacenó en un almacén expuesto a la intemperie	Crítico	A.11 Seguridad física y ambiental	A.11.1.4 - Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.
R67	Robo de documentación debido a la intrusión de un tercero ya que no cuentan con una protección física eficaz	Crítico	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC 27002:2013
R68	Robo de documentos confidenciales debido a que es almacenado en un lugar sin seguridad	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.
R69	Indisponibilidad parcial o permanente del documento debido a que no se cuenta con un respaldo del mismo	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.
R71	Robo de documentación debido a que se hagan copias no autorizadas de las historias clínicas	Crítico	A.8 Gestión de Activos	A.8.3.1. - Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.
R72	Acceso al documento de un tercero debido a que no se definió los accesos correctamente	Alto	A.9 Control de acceso	A.9.2.1 - Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de accesos. A.9.2.5 - Los propietarios de los activos deben revisar los derechos de accesos de usuario a intervalos regulares.
R73	Robo de documentación o exposición a terceros debido a que se ubicó en un lugar público	Crítico	A.9 Control de acceso	A.9.3.1 - Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autenticación secreta. A.9.4.1 - El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC 27002:2013
R79	Malfuncionamiento del servidor debido a la mala configuración inicial del servidor	Alto	A.12 Seguridad de las operaciones	A.12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el mejor riesgo.
R83	Indisponibilidad parcial o permanente de la base de datos debido a que no se cuenta con un respaldo del mismo	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.
R85	Pérdida de información debido a que no se realicen los respaldos	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.
R87	Error en el registro de movimientos de almacén debido a que las fechas del aplicativo no estén sincronizadas con el sistema operativo.	Alto	A.12 Seguridad de las operaciones	A.12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el mejor riesgo.

Elaboración: Los autores

- **Fase 7: Establecer políticas y procedimientos para controlar los riesgos**

Luego de haber realizado el respectivo análisis de riesgos e identificado los controles, se diseña el documento de “Declaración de Aplicabilidad” en la cual se hizo una revisión de los 144 controles que propone la ISO/IEC 27002 y a base de criterios se determinó la aplicabilidad de cada uno de ellos a la organización. Es exigido por la ISO/IEC 27001 ya que permite asegurar que no se está omitiendo algún control y si algún control no aplicase a la empresa, se realiza la justificación. El diseño del documento se puede ver en la Tabla 23.

**Tabla 23 – Campos en la Declaración de Aplicabilidad**

<b>Campo</b>	<b>Descripción</b>
Sección	Número de Cláusula referenciada de la ISO/IEC 27001
Objetivo	Objetivo de la cláusula
Control	Descripción del control
Aplicación	SI: Si es aplicable a la empresa, No: Si no es aplicable a la empresa
Justificación de Exclusión	Justificación porque se está excluyendo el control
Justificación de Inclusión	Criterios para la selección de controles: LR: Requiemamientos Legales, CO: Obligaciones Contractuales, BR/BP: Requerimientos del negocio/Mejores Prácticas, RRA: Resultado de Análisis de Riesgos (Giraldo, L., 2016)
Adaptación a MEDCAM Perú SAC	Descripción de cómo se aplicaría el control a MEDCAM

Elaboración: Los autores

Se elaboró la declaración de aplicabilidad según los campos especificados. (Ver Tabla 24).

Tabla 24 – Declaración de aplicabilidad

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
<b>5</b>	<b>Políticas de seguridad de la información</b>								
5.1	Directrices establecidas por la dirección para la seguridad de la información								
5.1.1	Políticas para la seguridad de la información	Existen políticas de seguridad de la información pero no han sido documentadas, se debe redactar un documento que políticas para que sea distribuido y conocido por todo el personal incluido en el proceso del SGSI			X		Si	Se diseñó e implementó el documento de Política de Seguridad de la Información. <b>Control C001.</b>	
5.1.2	Revisión de las políticas para seguridad de la información	Se debe establecer un procedimiento que permita la revisión periódica de las políticas de la seguridad de la información por lo menos cada año			X		Si	Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determina el periodo de revisión de la política. <b>Control C002.</b>	
<b>6</b>	<b>Organización de la seguridad de la información</b>								
6.1	Organización interna.								
6.1.1	Roles y responsabilidades para la seguridad de información	Se deben definir roles y responsabilidades de acuerdo a las políticas de seguridad de la información a todos los que interactúen con el SGSI			X		Si	Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determinan los roles y responsabilidades respecto a la seguridad de la información. <b>Control C003.</b>	



Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
6.1.2	Separación de deberes	Se deben separar las áreas consideradas de gran importancia para que así los deberes y responsabilidades asignadas sean separadas, de esta forma se evita el uso indebido de los activos de la organización			X	X	Si	Los procesos de MEDCAM se han determinado considerando segregación en los procesos. <b>Control C004.</b>	
6.1.3	Contacto con las autoridades	En el documento de políticas de la seguridad de la información se debe contemplar un procedimiento que permita gestionar el contacto permanente con autoridades reguladoras de seguridad de la información	La organización no tiene contacto con autoridades reguladoras de los procesos de negocio.					No	
6.1.4	Contacto con grupos de interés especial	Es importante que la persona encargada de la seguridad informática gestione el contacto permanente con grupos de interés, estos pueden ser foros, chats, wiki, comunidades relacionadas con la seguridad informática, con la intención de estar actualizados en aspectos relacionados a la seguridad	Las ejecuciones en seguridad de la información no están a cargo de personal operativo de la empresa.					No	
6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en cualquier proyecto.	No representa un riesgo crítico para la empresa.					No	
6.2	Dispositivos móviles y teletrabajo.								
6.2.1	Política para dispositivos móviles	Se deben aplicar políticas para el uso adecuado de dispositivos móviles, su uso inadecuado representa grandes riesgos	Los procesos de MEDCAM no tienen participación de dispositivos móviles.					No	

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
6.2.2	Teletrabajo	La Cía. no posee empleos bajo la modalidad de teletrabajo	MEDCAM no posee este tipo de trabajadores.					No	
<b>7</b>	<b>Seguridad de los recursos humanos</b>								
7.1	Antes de asumir el empleo.								
7.1.1	Selección	Se deben realizar una exhaustiva comprobación de los antecedentes del personal como empleados, contratistas, terceros, con el fin de saber su procedencia, referencias personales, judiciales entre otras	No representa un riesgo crítico para la empresa ya que cuenta con el mismo personal por años.					No	
7.1.2	Términos y condiciones del empleo	Se debe diseñar un documento que permita a los empleados, contratistas y terceros firmar cláusulas de confidencialidad con la organización, manejo adecuado de recursos tecnológicos		X	X			Si	Se diseñó el documento Acuerdo de Confidencialidad el cual estipula que la información que corresponde a los procesos internos MEDCAM, así como la información de los pacientes atendidos por la clínica, son de carácter confidencial y la divulgación de estos conlleva castigos penales, así como la ruptura de la relación con MEDCAM. <b>Control C005.</b>
7.2	Durante la ejecución del empleo.								
7.2.1	Responsabilidades de la dirección	Se debe exigir a los empleados, contratistas y terceros el cumplimiento a cabalidad de las políticas de seguridad de la información implementadas por la Cía	No representa un riesgo crítico para la empresa.					No	

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Se debe capacitar a todo el personal en aspectos relacionados con la seguridad de la información			X		Si	El personal de MEDCAM es sensibilizado respecto a temas de seguridad de la información. <b>Control C006.</b>	
7.2.3	Proceso disciplinario	Se deben establecer políticas sobre sanciones que se aplicarán a quienes incumplan con lo descrito en las políticas de seguridad			X		Si	Se diseñó e implementó el documento de Política de Seguridad de la Información, en el cual se determinan las penalidades sobre el incumplimiento de la política. <b>Control C007.</b>	
7.3	Terminación o cambio de empleo								
7.3.1	Terminación o cambio de responsabilidades de empleo	Se debe informar a los empleados en los casos donde las responsabilidades y deberes que les fueron asignados durante el empleo, los cobijan aun cuando se realice una terminación o cambio de contrato	No representa un riesgo crítico para la empresa ya que no se realizan cambios de puestos.					No	
8	<b>Gestión de activos</b>								
8.1	Responsabilidad por los activos								
8.1.1	Inventario de activos	Se debe contar con un inventario detallado de los activos que posee la Cía			X	X	Si	Se identificó y clasificó los activos de los procesos relevantes de la organización teniendo como resultado el Inventario de Activos de Información. <b>Control C008.</b>	

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
8.1.2	Propiedad de los activos	Además de la implementación del control anterior, se debe identificar en custodia de quien se encuentra actualmente el activo			X	X	Si	El inventario de activos diseñado tiene información actualizada del propietario (responsable) del activo de información. <b>Control C009.</b>	
8.1.3	Uso aceptable de los activos	Debe existir una clausula donde los empleados se comprometan a realizar un uso aceptable de los activos de la organización			X		Si	Se diseñó e implementó la política específica de Gestión de Activos en la que se establece el uso que los empleados le deben dar a los activos de información. <b>Control C010.</b>	
8.1.4	Devolución de activos	Se debe establecer un proceso para la devolución de los activos para cuando los empleados cambien de puesto o cuando se termine su contrato			X		Si	Se diseñó e implementó la política específica de Gestión de Accesos en la que se establece el proceso de devolución de activos ante el cese del personal. <b>Control C011.</b>	
8.2	Clasificación de la información								
8.2.1	Clasificación de la información	Se debe establecer un procedimiento que permita clasificar la información de acuerdo a su valor	No representa un riesgo crítico para la empresa.					No	
8.2.2	Etiquetado de la información	La información debe estar debidamente rotulada, además esta rotulación se debe clasificar de acuerdo al valor que representa la información para la empresa	No representa un riesgo crítico para la empresa.					No	
8.2.3	Manejo de activos	Se debe contar con procedimientos que ayuden en el	Se cubrirá con el control C010.					No	

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
		adecuado manejo que se le debe dar a un activo							
8.3.1	Gestión de medios removibles	Se deben establecer políticas sobre el correcto manejo que se le deben dar a los medios removibles, puesto que estos son necesarios en el desarrollo de las labores diarias.			X	X	Si	Se diseñó e implementó la política específica de Gestión de Activos en la que se establece que los medios removibles deben ser inhabilitados en todas las computadoras de la clínica. <b>Control C012.</b>	
8.3.2	Disposición de los medios	Protección de la información cuando los medios sean destinados a labores diferentes a las actuales, se podría hablar de un procedimiento de eliminación de información en estos casos.	No aplica a la empresa.				No		
8.3.3	Transferencia de medios físicos	Definir procedimientos que permitan que la información almacenada en estos no sea divulgada, modificada o eliminada.		X		X	X	Si	Se tiene como regla en el proceso de Procesamiento que el medico ocupacional del cliente puede decepcionar los resultados de los exámenes. <b>Control C013.</b>
<b>9</b>	<b>Control de acceso</b>								
9.1	Requisitos del negocio para control de acceso								
9.1.1	Política de control de acceso	Establecer políticas que permitan el acceso a la información de acuerdo a privilegios establecidos según sus funciones			X		Si	Se diseñó e implementó la Política Específica de Gestión de Accesos. <b>Control C014.</b>	
9.1.2	Política sobre el uso de los servicios de red	Definir el acceso a la red para el desarrollo de funciones que les fueron asignadas.	No representa un riesgo crítico para la empresa ya que el acceso a la red no				No		

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
			asegura el acceso a las aplicaciones de la clínica.						
9.2	Gestión de acceso de usuarios								
9.2.1	Registro y cancelación del registro de usuarios	Todos los usuarios con acceso a sistema de información deben estar debidamente registrados, adicionalmente se debe dar de baja a los que ya no hagan parte de la organización o no hagan uso del sistema.		X	X	X	X	Si	El personal que cesa de la empresa se le debe retirar los accesos a los sistemas de información en un periodo oportuno. <b>Control C015.</b>
9.2.2	Suministro de acceso de usuarios	Implementar un procedimiento que permita a los usuarios del sistema acceder al sistema o negar el acceso a este cuando se considere necesario.				X		Si	Los ordenadores deben requerir usuarios y contraseña para el acceder a los mismos. <b>Control C016.</b>
9.2.3	Gestión de derechos de acceso privilegiado	Se deben establecer privilegios de acceso a la información de acuerdo al desempeño de sus funciones.				X		Si	Existe una revisión periódica de accesos otorgados en el sistema Mediweb. <b>Control C017.</b>
9.2.4	Gestión de información de autenticación secreta de usuarios	Esta información sólo debe ser accesada por personal con privilegios especiales				X		Si	Sólo personal autorizado tiene acceso a la Gestión de Accesos en los sistemas de información. <b>Control C018.</b>
9.2.5	Revisión de los derechos de acceso de usuarios	Monitoreo de privilegios asignados a usuarios con el fin de identificar si los privilegios asignados son adecuados para el desarrollo de sus funciones.				X	X	Si	Se cubrirá con el control <b>C017.</b>
9.2.6	Retiro o ajuste de los derechos de acceso	Se debe dar de baja o modificar los privilegios de acceso a la información en caso de traslado		X		X		Si	Se cubrirá con el control <b>C015.</b>

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
		del usuario o retiro de la organización.							
9.3	Responsabilidades de los usuarios								
9.3.1	Uso de la información de autenticación secreta	Se deben crear perfiles para el acceso a información considerada de suma importancia para la empresa			X	X	Si	Se cubrirá con el control <b>C018</b> .	
9.4	Control de acceso a sistemas y aplicaciones								
9.4.1	Restricción de acceso Información	Restringir el acceso a la información por parte de personal no autorizado.		X	X	X	X	Si	Los activos físicos críticos se encuentran en un ambiente restringido al público. <b>Control C019.</b>
9.4.2	Procedimiento de ingreso seguro	Se deben establecer procedimientos que restrinjan el acceso a la información a personal no autorizado		X	X	X		Si	Se cubrirá con el control <b>C016</b> .
9.4.3	Sistema de gestión de contraseñas	Se deben establece políticas de gestión de contraseñas como caducidad, bloqueo después de determinado número de intentos, parámetros para creación de contraseñas seguras.				X	X	Si	Los sistemas de información han sido configurados con la política de contraseña definida por la organización. <b>Control C020.</b>

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
9.4.4	Uso de programas utilitarios privilegiados	Restringir el uso de programas utilitarios ya que pueden violentar la seguridad de las contraseñas, pues algunos revelan las contraseñas, vulnerando la seguridad.	No representa un riesgo crítico para la empresa.					No	
9.4.5	Control de acceso a códigos fuente de programas	Políticas de acceso al código fuente, este sólo debe ser accesado por el personal autorizado	No aplica a la empresa.					No	
<b>10</b>	<b>Criptografía</b>								
10.1	Controles criptográficos								
10.1.1	Política sobre el uso de controles criptográficos	Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad y no repudio de la información	Se establecerán controles de criptografía fuera de una política.					No	
10.1.2	Gestión de llaves	Se deben establecer controles criptográficos que permitan la confidencialidad, disponibilidad, integridad y no repudio de la información		X		X		Si	Las tablas de información confidencial son encriptados a nivel de base de datos. <b>Control C021.</b>
<b>11</b>	<b>Seguridad física y del entorno</b>								
11.1	Áreas seguras								
11.1.1	Perímetro de seguridad física	Se debe establecer un perímetro de tal forma que los sitios donde se encuentren los activos tengan accesos restringido		X	X	X	X	Si	Se cubrirá con el control <b>C019.</b>



Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
11.1.2	Controles físicos de entrada	Se debe restringir el acceso a sitios seguros como centro de cableado, ubicación del servidor, espacios donde se encuentre información confidencial, estos sitios deben permanecer con llave.		X	X	X	X	Si	El centro de datos se encuentra con acceso restringido a personal autorizado. <b>Control C022.</b>
11.1.3	Seguridad de oficinas, recintos e instalaciones	Restringir el acceso a personal no autorizado, las áreas deben estar demarcadas dando aviso que son sitios restringidos		X	X	X		Si	En la clínica las áreas restringidas están señalizadas. <b>Control C023.</b>
11.1.4	Protección contra amenazas externas y ambientales	Se debe contar con detectores de humo y humedad, ubicación de extinguidores en sitios estratégicos, cuartos técnicos con aire acondicionado, adquisición de pólizas contra robo y desastres naturales				X	X	Si	En la clínica se han implementado medidas de seguridad ante amenazas internas como extintores, alarmas, luminarias ante falta de electricidad, etc. <b>Control C024.</b>
11.1.5	Trabajo en áreas seguras	Se deben preservar los sitios donde se encuentren activos valiosos con el fin de protegerlos contra daños intencionados	Se cubrirá con el control C013.					No	
11.1.6	Áreas de despacho y carga	Se deben designar sitios especiales para carga y despacho, lo recomendable es que estén aislados de los denominados sitios seguros o restringidos	No aplica a la empresa.					No	
11.2	Equipos								
11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados en sitios seguros, de esta forma se protegen contra robo, accesos no autorizados.		X	X	X		Si	Se cubrirá con el control <b>C022.</b>

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
11.2.2	Servicios de suministro	Se debe contar con un adecuado suministro y respaldo de energía	Se cuentan con procedimientos de continuidad de negocio.					No	
11.2.3	Seguridad del cableado	Se debe proteger el cableado eléctrico y de datos de posibles daños como interceptaciones con el fin de causar daño.	No representa un riesgo crítico para la empresa.					No	
11.2.4	Mantenimiento de equipos	Se debe contar con mantenimiento preventivo y correctivo en períodos de tiempo establecidos, con el fin de evitar daños en hardware, actualización de software.			X			Si	Los activos de hardware y software deben tener un mantenimiento anual. <b>Control C025.</b>
11.2.5	Retiro de activos	Se debe definir un procedimiento que autorice el retiro de activos de la empresa tales como equipos de cómputo, software.	No aplica a la empresa.					No	
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Aplicar la misma seguridad que se realiza a los equipos dentro de la empresa	Se cubrirá con el control C022.					No	
11.2.7	Disposición segura o reutilización de equipos	Se debe proteger la información confidencial de equipos en desuso o cuando son dados de baja.	No aplica a la empresa.					No	
11.2.8	Equipos de usuario desatendidos	Establecer políticas para equipos cuando los usuarios no están presentes, evitando así el acceso no autorizado o robo de información.		X	X	X		Si	Los sistemas de información han sido configurados con bloqueo de sesión automático. <b>Control C026.</b>
11.2.9	Política de escritorio limpio y pantalla limpia	Definir procedimientos para que los escritorios estén libres de papeles, medios de almacenamiento que puedan permitir filtración de información,		X	X	X	X	Si	Los escritorios deben permanecer libre de documentos con información confidencial. <b>Control C027.</b>

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
		además políticas de pantallas limpias.							
<b>12</b>	<b>Seguridad de las operaciones</b>								
12.1	Procedimientos operacionales y responsabilidades								
12.1.1	Procedimientos de operación documentados	Los procedimientos deben estar documentados y puestos al alcance de todos, también manuales de operaciones específicas			X	X	Si	Las políticas y documentación propia de la empresa en lo que respecta a procesos de negocio se encuentran en una carpeta compartida al cual toda la organización tiene acceso. <b>Control C028.</b>	
12.1.2	Gestión de cambios	Establecer políticas donde los cambios sean realizados por personal autorizado, además deben quedar soportados para llevar un control para evitar contratiempos.	No representa un riesgo crítico para la empresa.				No		
12.1.3	Gestión de capacidad	Se debe realizar un monitoreo de los recursos de tal forma que no afecten la operación, algunos pueden ser capacidad de banda ancha, circuitos descalibrados que afecten el fluido eléctrico, equipos de cómputo lentos.	No representa un riesgo crítico para la empresa.				No		
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Los ambientes de desarrollo prueba y operación deben estar aislados, con restricciones de acceso con el fin de evitar cambios o modificaciones no autorizadas.	No aplica a la empresa.				No		

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
12.2	Protección contra códigos maliciosos								
12.2.1	Controles contra códigos maliciosos	Los equipos de cómputo deben contar con software contra código malicioso, el cual se debe actualizar constantemente con el fin de actualizar parches que mitiguen las nuevas vulnerabilidades.			X			Si	Se revisará que los activos de software deben contar con un antivirus actualizado. <b>Control C029.</b>
12.3	Copias de respaldo								
12.3.1	Respaldo de información	Se debe realizar respaldo de la información, además se deben realizar pruebas para comprobar que estos cumplen con las políticas de respaldo-			X	X		Si	Se debe generar a los activos de software una copia de respaldo de manera mensual, esta debe ser revisada y almacenada en un lugar ajeno al centro de operaciones. <b>Control C030.</b>
12.4	Registro y seguimiento								
12.4.1	Registro de eventos	Se debe llevar un control de los eventos con el fin de establecer procedimientos que ayuden a repararlos o eliminarlos definitivamente, con el fin de que no se vuelvan a presentar	No representa un riesgo crítico para la empresa.					No	
12.4.2	Protección de la información de registro	Se debe proteger la información de registro de personal no autorizado, sólo el administrador o encargado será quien pueda tener acceso a estos, se deben realizar copias de logs.	No representa un riesgo crítico para la empresa.					No	
12.4.3	Registros del administrador y del operador	Todas las tareas que desarrollen el administrador y el operador del sistema de información deben estar registradas, además se	No representa un riesgo crítico para la empresa.					No	

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
		debe realizar un respaldo de estos registros.							
12.4.4	sincronización de relojes	Los relojes de los dispositivos que intervienen en el procesamiento de información deben estar sincronizados.	No representa un riesgo crítico para la empresa.					No	
12.5	Control de software operacional								
12.5.1	Instalación de software en sistemas operativos	La instalación de software debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas.	No representa un riesgo crítico para la empresa.					No	
12.6	Gestión de la vulnerabilidad técnica								
12.6.1	Gestión de las vulnerabilidades técnicas	Se deben establecer procedimientos que minimicen las vulnerabilidades a que están expuestos los activos tecnológicos.	La probabilidad de error en las aplicaciones de MEDCAM es mínima pues son sistemas de terceros que han demostrado estabilidad.				X	No	
12.6.2	Restricciones sobre la instalación de software	La instalación de software debe estar controlada, de tal forma que sólo las personas autorizadas puedan realizar estas tareas, además deben quedar registradas.	No representa un riesgo crítico para la empresa.					No	
12.7	Consideraciones sobre auditorías de sistemas de información								
12.7.1	Información controles de auditoría de sistemas	Se deben establecer procedimientos que permitan el buen uso de las herramientas de auditoría a los sistemas, pero	No representa un riesgo crítico para la empresa.					No	

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
		siempre procurando minimizar la interrupción del servicio a causa de estas.							
<b>13</b>	<b>Seguridad de las comunicaciones</b>								
<b>13.1</b>	<b>Gestión de la seguridad de las redes</b>								
13.1.1	Controles de redes	Se deben instalar dispositivos o software que permita controlar el acceso a la red como Firewall, lds, autenticación para su ingreso			X	X	Si	Se cuenta con un directorio activo el cual requiere autenticación para el acceso a los activos de software. <b>Control C031.</b>	
13.1.2	Seguridad de los servicios de red	Establecer controles de acceso, acuerdos de servicio en su utilización, monitoreo constante para detectar intrusos	No representa un riesgo crítico para la empresa.				No		
13.1.3	Separación en las redes	Es necesario la separación de las redes como la intranet de la red con acceso a internet, para lo cual se debe implementar un DMZ	No representa un riesgo crítico para la empresa.				No		
<b>13.2</b>	<b>Transferencia de información</b>								
13.2.1	Políticas y procedimientos de transferencia de información	Se deben establecer todas las políticas que sean necesarias para proteger la información en el momento de ser transferida (intercambio de información), permitiendo integridad y confidencialidad.	No aplica a la empresa.				No		
13.2.2	Acuerdos sobre transferencia de información	Se deben establecer controles que permitan respetar acuerdos de intercambio o transferencia de información	No aplica a la empresa.				No		

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
13.2.3	Mensajería electrónica	Deben existir controles sobre el uso adecuado de la mensajería electrónica, para ello se deben instalar programas que detecten antivirus y spam, además se debe existir capacitación sobre situaciones donde existan correos sospechosos, también políticas del uso adecuado de los recursos, en este caso uso del correo electrónico sólo para el desarrollo de las funciones asignadas.	No representa un riesgo crítico para la empresa.					No	
13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben cumplir las políticas de confidencialidad de la información, las cuáles fueron aceptadas en el momento de la firma del contrato.	Se cubrirá con el control 7.1.2					No	
<b>14</b>	<b>Adquisición, desarrollo y mantenimientos de sistemas</b>								
14.1	Requisitos de seguridad de los sistemas de información								
14.1.1	Análisis y especificación de requisitos de seguridad de la información	Las especificaciones de requisitos se deben tener en cuenta cuando se vaya a realizar un cambio o implementar un nuevo sistema de información	No aplica a la empresa.					No	
14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información	No aplica a la empresa.					No	

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
14.1.3	Protección de transacciones de los servicios de las aplicaciones	Se debe implementar seguridad en los servicios que viajan por redes públicas tales como autenticación, manejo de cookies, sesiones, pki, con el fin de garantizar la confiabilidad de la información	No aplica a la empresa.					No	
14.2	Seguridad en los procesos de desarrollo y soporte								
14.2.1	Política de desarrollo seguro	Es importante establecer políticas de código seguro en el desarrollo de software, es aquí donde se deben implementar procedimientos de seguridad como paso de variables por cabecera, sesiones, entre otros, los cuáles deben blindar el sistema de información para evitar vulnerabilidades	No aplica a la empresa.					No	
14.2.2	Procedimientos de control de cambios en sistemas	Todos los cambios que se realicen a los programas se deben documentar y quedar registrados, para lo cual se deben establecer procedimientos	No aplica a la empresa.					No	
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Se deben realizar pruebas a las aplicaciones que han sido modificadas, con el fin de evitar alteraciones en la prestación del servicio o mal funcionamiento a causa del desarrollo.	No aplica a la empresa.					No	
14.2.4	Restricciones en los cambios a los paquetes de software	Los cambios o modificaciones que se le realizan a las aplicaciones deben estar restringidos con el fin de evitar fallas no deseadas.	No aplica a la empresa.					No	



Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
14.2.5	Principios de construcción de sistemas seguros	Establecer procedimientos y políticas que permitan la construcción de aplicaciones seguras	No aplica a la empresa.					No	
14.2.6	Ambiente de desarrollo seguro	Los ambientes de desarrollo deben estar aislados y contar con todas las medidas de seguridad en cuanto a control de acceso a la información y a las instalaciones	No aplica a la empresa.					No	
14.2.7	Desarrollo contratado externamente	Cuando se adquieran sistemas externos, realizar seguimiento, es necesario validarlos antes de ponerlos en funcionamiento	No aplica a la empresa.					No	
14.2.8	Pruebas de seguridad de sistemas	Someter los sistemas a pruebas con el fin de identificar vulnerabilidades, se podría contemplar pruebas de hacking ético.	No aplica a la empresa.					No	
14.2.9	Prueba de aceptación de sistemas	Someter los sistemas a pruebas con el fin de identificar vulnerabilidades, se podría contemplar pruebas de hacking ético.	No aplica a la empresa.					No	
14.3	Datos de prueba								
14.3.1	Protección de datos de prueba	Hay que tener cuidado con los datos que se van a ingresar para realizarle pruebas a la aplicación, esto con el fin de evitar alguna fuga de información importante.	No aplica a la empresa.					No	
15	Relación con los proveedores								
15.1	Seguridad de la información en las relaciones con los proveedores								

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
15.1.1	Política de seguridad de la información para las relaciones con proveedores	Igual que con los usuarios de la organización, con los proveedores se deben establecer acuerdos de confidencialidad, control de acceso a la información, seguridad física, intercambio de información entre otros para no ver afectada la seguridad de la información.	No representa un riesgo crítico para la empresa.					No	
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Definir acuerdos de confidencialidad	No representa un riesgo crítico para la empresa.					No	
15.1.3	Cadena de suministro de tecnología de información y comunicación	Se deben establecer acuerdos que permitan mitigar los riesgos de la seguridad de la información derivados de la cadena de suministro.	No representa un riesgo crítico para la empresa.					No	
15.2	Gestión de la prestación de servicios con los proveedores								
15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.	No representa un riesgo crítico para la empresa.					No	
15.2.2	Gestión de cambios en los servicios de proveedores	Se debe contar con otras alternativas de proveedores que permitan la continuidad del servicio en caso de cambio de proveedor	No representa un riesgo crítico para la empresa.					No	
16	Gestión de incidentes de seguridad de la información								
16.1	Gestión de incidentes y mejoras en la seguridad de la información								

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
16.1.1	Responsabilidad y procedimientos	Definir procedimientos que permitan una reacción rápida ante problemas generados por causa de la seguridad de la información.			X		Si	Se diseñó e implementó el documento de Política de Gestión de Incidentes en el cual se especifica el plan de respuesta ante los incidentes de seguridad de la información. <b>Control C032.</b>	
16.1.2	Reporte de eventos de seguridad de la información	Se debe informar sobre eventos generados a causa de seguridad de la información con el fin de documentar la solución, es necesario llevar un registro de estos.			X		Si	Los incidentes de seguridad de la información serán registrados en el documento lógico "Incidentes de Seguridad de la Información" lo que permitirá trazabilidad. <b>Control C033.</b>	
16.1.3	Reporte de debilidades de seguridad de la información	Informar oportunamente sobre eventos generados, con el fin de identificar recurrencias y debilidades en seguridad de la información.			X		Si	Se cubrirá con el control <b>C033.</b>	
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Cada vez que se presente un evento de seguridad de la información es importante evaluar si será considerado como un incidente o no.	Todos los eventos serán considerados incidentes, por lo que no se hará distinción.				No		
16.1.5	Respuesta a incidentes de seguridad de la información	Se debe establecer un proceso que permita establecer los pasos a seguir para atender el incidente.			X		Si	Se diseñó e implementó el documento de Política de Gestión de Incidentes, en la cual se indica el plan de respuesta ante los incidentes acorde a su alcance. <b>Control C034.</b>	

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	La experiencia que se ha adquirido en resolver los incidentes, es pieza fundamental para reducir el impacto que pueda causar este incidente a la seguridad de la información	No representa un riesgo crítico para la empresa.					No	
16.1.7	Recolección de evidencia	Definir un procedimiento para documentar los incidentes de tal forma que exista una evidencia.			X			Si	Se ha definido un documento Excel, en una carpeta compartida, en la cual se registrarán los incidentes que se suscitarán en la organización. <b>Control C035.</b>
<b>17</b>	<b>Aspectos de seguridad de la información de la gestión de continuidad de negocio</b>								
17.1	Continuidad de seguridad de la información								
17.1.1	Planificación de la continuidad de la seguridad de la información	Definir políticas que permita la gestión de la continuidad del negocio, aunque la organización presente una crisis			X			Si	Se cubrirá con el control <b>C032.</b>
17.1.2	Implementación de la continuidad de la seguridad de la información	Implementar procedimientos que permitan la continuidad del negocio ante situaciones imprevistas que podrían causar retrasos en la operación.			X			Si	Se diseñó e implementó el documento de Política de Gestión de Incidentes, la cual cuenta con procedimiento que permite la continuidad del negocio ante eventos que no permitan la operatividad del mismo. Se cuenta con documentación física que permite la continuidad del negocio. <b>Control C036.</b>

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Realizar revisiones a los procedimientos implementados para la gestión de la continuidad del servicio para determinar si son efectivos o no.	No representa un riesgo crítico para la empresa.					No	
17.2	Redundancias								
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Es necesario establecer redundancias en las instalaciones donde se procesa la información con el fin de que no se vea afectada la disponibilidad de la información.			X			Si	El nivel de complejidad de la empresa no le permite tener un centro de datos redundante. En respuesta al riesgo se diseñó e implementó el documento de Política de Gestión de Copias de Respaldo Se cuenta con instalaciones alternas para la continuidad del negocio. <b>Control C037.</b>
18	<b>Cumplimiento</b>								
18.1	Cumplimiento de requisitos legales y contractuales								

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Definir el marco legal con el cual se debe regir la seguridad de la información.		X	X			Si	Se diseñó e implementó el documento de Política de Seguridad de la Información, en esta política se especifica las leyes que son consideradas: - Ley 26842 - 1997 - Ley General de Salud Concordada, Artículo 25.- Toda información relativa al acto médico que se realiza, tiene carácter reservado. - Ley 29733 - 2011 - Ley de Protección de Datos Personales, Artículo 16.- Seguridad del tratamiento de datos personales. Y Artículo 17.- Confidencialidad de Datos Personales. <b>Control C038.</b>
18.1.2	Derechos de propiedad intelectual	Cumplir a cabalidad las políticas de derechos de propiedad intelectual, software patentado.	No representa un riesgo crítico para la empresa.					No	
18.1.3	Protección de registros	Procedimiento que permita la custodia de los registros ante situaciones de robo, modificación, divulgación.		X	X	X		Si	Se han determinado controles preventivos que aseguran la seguridad de los registros: Controles: C014, C015, C020, C021, C026 y C031.
18.1.4	Privacidad y protección de datos personales	Cumplir con las políticas de la protección de datos personales		X	X	X	X	Si	Se han determinado controles preventivos que aseguran la seguridad de los registros: Controles: C014, C015, C020, C021, C026 y C031.
18.1.5	Reglamentación de controles criptográficos	Cumplir con las normas relacionadas con controles criptográficos	No aplica a la empresa.					No	

Sec.	Objetivo	Control	Justificación de exclusión	Justificación Inclusión				Aplicación	Adopción a MEDCAM
				LR	CO	BR/BP	RRA	Si/No	
18.2	Revisiones de seguridad de la información								
18.2.1	Revisión independiente de la seguridad de la información	Se debe revisar periódicamente el SGSI, estas revisiones deben ser adicionales a las establecidas en las políticas de seguridad de la información.	No representa un riesgo crítico para la empresa.					No	
18.2.2	Cumplimiento con las políticas y normas de seguridad	La dirección debe revisar los cumplimientos de las políticas de seguridad de la información establecidas de acuerdo a su área de responsabilidad.	No representa un riesgo crítico para la empresa.					No	
18.2.3	Revisión del cumplimiento técnico	Se deben revisar que todo el personal conoce y cumple con las políticas de seguridad de la información						Si	Se debe realizar revisiones anuales al sistema de gestión de seguridad de la información. <b>Control C039.</b>

Elaboración: Los autores

En el documento anterior se identificaron las políticas específicas que debían ser elaboradas e implementadas. Estas políticas son apoyadas por la política general de seguridad de la información. Son las siguientes:

- Política de Gestión de contraseñas
- Política de Escritorio limpio
- Política de Gestión de accesos
- Política de Gestión de incidentes de seguridad
- Política de Gestión de copias de respaldo
- Política de Gestión de activos

Estas políticas pueden apreciarse en el Anexo 3 – Políticas específicas.

### **3.3 Prueba de Efectividad de Controles**

En este rubro del proyecto, se realizaron las pruebas al Sistema de Gestión de Seguridad de la Información implementado para comprobar su correcto diseño. Las pruebas se realizaron probando la efectividad de los controles implementados.

Para realizar la efectividad de controles se debió establecer el alcance de esta revisión, para este proyecto midió la efectividad para los 39 controles producto de la implementación del SGSI. (Ver Anexo 5 - Efectividad de Controles). La prueba se basa en la validación de atributos a través del juicio experto de los involucrados en el proyecto, que son los siguientes:

- Experto 1: Tesista (Senyi Fukusaki)
- Experto 2: Tesista (Miguel Cruz)
- Experto 3: Administradora MEDCAM Perú (Karla Barbarán)

Los atributos por validar en esta prueba serán:

- Control diseñado correctamente: En este punto, se evaluará si el control está diseñado para proteger el activo de información y si sus características (periodicidad, tipo, etc.) son correctas.
- Control implementado: En este punto, los expertos evaluarán si se considera que el control, en la fecha de revisión, se implementó en la clínica.



- Eficiencia operativa: En este punto los expertos evaluarán si el control se ejecuta de manera correcta según lo establecido.

A su vez, todas las fases anteriores se verificaron y se trabajaron en conjunto con la gerencia de MEDCAM Perú SAC. Por lo que se acordó un acta de cierre que sirva como certificado de implementación del SGSI propuesto a la empresa. (Ver Anexo 8 - Acta de Cierre del Proyecto). En dicha acta se encuentra los entregables, el alcance y los acuerdos que se tuvieron con MEDCAM Perú SAC.

## **CAPÍTULO IV**

### **PRUEBAS Y RESULTADOS**

#### **4.1 Objetivo General: Mitigar los riesgos a los que está expuesto los activos de información de la clínica MEDCAM Perú SAC**

Para verificar que efectivamente se han mitigado los riesgos a los que estaban expuestos los activos de información de MEDCAM luego del desarrollo e implementación del presente proyecto, se analizará comparativamente la exposición al riesgo previo al proyecto y posterior a él. Cabe resaltar que los activos de información evaluados son los que se determinaron críticos para la organización. Ver el resultado de la valoración de activos en la Tabla 19.

La situación inicial que identificamos antes de la implementación se puede visualizar en la Matriz de riesgos (Ver Tabla 21). Posterior a la implementación de los controles se reevaluaron las exposiciones de los riesgos se realizó nuevamente la evaluación y se compara con el resultado inicial. (Ver Anexo 7 - Reevaluación Post Implementación de Controles).

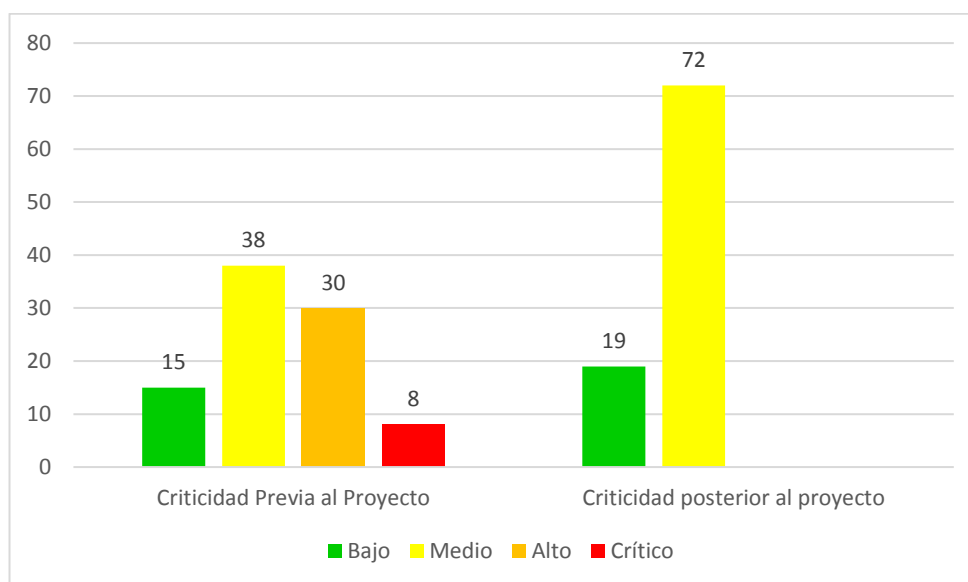
Se elaboró un cuadro resumen a partir de este análisis y se obtuvo lo siguiente. (Ver Tabla 25).

**Tabla 25 – Comparación de Criticidad**

Activos	Total Riesgos	Antes				Después			
		Bajo	Medio	Alto	Crítico	Bajo	Medio	Alto	Crítico
MediWeb	10	1	4	5	0	2	8	0	0
Servidor de Aplicaciones	10	0	7	3	0	0	10	0	0
Sistema Logístico de MedCam	10	0	8	2	0	0	10	0	0
Base de Datos	9	2	5	2	0	3	6	0	0
Computadoras de Escritorio	8	0	5	3	0	0	8	0	0
Historia Clínica	8	2	0	3	3	2	6	0	0
Historia Clínica Digital	7	1	2	2	2	1	6	0	0
Resultados Finales	7	2	0	2	3	2	5	0	0
Consentimiento Informado - Atención	6	2	1	3	0	3	3	0	0
Consentimiento Informado - Ley	6	2	1	3	0	3	3	0	0
Kardex	6	1	4	1	0	1	5	0	0
Hoja Interconsulta	4	2	1	1	0	2	2	0	0
<b>Total</b>	<b>91</b>	<b>15</b>	<b>38</b>	<b>30</b>	<b>8</b>	<b>19</b>	<b>72</b>	<b>0</b>	<b>0</b>

Elaboración: Los autores

A partir de esta información, se puede evidenciar como la criticidad de los riesgos ha bajado significativamente posterior a la implementación. (Ver Figura 23)



**Figura 23 – Comparación de la criticidad de los riesgos previo al proyecto y posterior a este.**  
Elaboración: Los autores

Se observa como los riesgos Altos y Críticos, que no estaban dentro del apetito del riesgo de la clínica, se encuentran actualmente en niveles más aceptables como Medios y Bajos. Esto nos permite afirmar y comprobar que

efectivamente se logró el objetivo de mitigar los riesgos a los que está expuesto los activos de información de la clínica.

#### 4.2 Objetivo específico 1: Implementar del sistema de gestión de seguridad de la información basado en la ISO/IEC 27001

Se diseñó e implementó el Sistema de Gestión de Seguridad de Información según los alcances establecidos al comienzo del proyecto. En primer lugar, se realizó el levantamiento de los procesos más críticos, esto permitió la correcta identificación de los activos de información que participaban dentro de estos procesos. Una vez identificados estos activos, se valorizaron según el impacto que causaba a la organización por una falta de disponibilidad, la falta de integridad y la no confidencialidad. Posteriormente, se analizaron las amenazas y vulnerabilidades a las que estaban expuestos estos activos, lo que permitió la identificación de los riesgos. Luego se identificó e implementó los controles más críticos para la mitigación de la exposición de estos activos y se implementaron las políticas específicas. A su vez, esto contribuyó a poder acercarnos a los trabajadores de la empresa para resolver sus dudas respecto a la seguridad de la información y esto ayudó a ser más fácil la sensibilización en temas de seguridad.

Se cumplió con el desarrollo y entrega (Ver Tabla 26):

**Tabla 26 – Comparación de Documentación Entregada**

Documentos	¿Lo tiene la Empresa?		Referencia
	Antes	Después	
Diagrama de procesos críticos	x	✓	Pág 41-48
Inventario de Activos	x	✓	Pág. 54
Listado de valoración de activos	x	✓	Pág. 65
Matriz de amenazas y vulnerabilidades	x	✓	Pág. 66
Matriz de riesgos	x	✓	Pág. 71
Listado de Controles de seguridad	x	✓	Pág. 83
Declaración de aplicabilidad de controles	x	✓	Pág. 92
Política general y específicas de la seguridad de la información	x	✓	Pág. 141-159

Elaboración: Los autores

Esto se puede verificar con el acta de Cierre. (Ver Anexo 8 - Acta de Cierre del Proyecto).

### 4.3 Objetivo específico 2: Implementación de una política de seguridad de la información

Se diseñó e implementó la política de seguridad de la información junto a la administración de MEDCAM Perú SAC (Ver Anexo 2 – Política General de Seguridad de la Información), donde se establecen los roles y responsabilidades, las generalidades de la seguridad y las posibles sanciones aplicables. Asimismo, se desarrollaron las políticas específicas (Ver Anexo 3 – Políticas Específicas) para cada foco de riesgo. Esta implementación ayudó a sensibilizar a los trabajadores de MEDCAM sobre la importancia que ha definido la empresa respecto a la seguridad de la información, así como tener los lineamientos que permita la protección adecuada de los activos de información en su día a día.

Asimismo, para corroborar que los colaboradores tuvieran conocimiento de esta política, se les preguntó: ¿Existe alguna política de seguridad de la información en la empresa? (Ver Figura 24). En esta pregunta, se puede observar que previo al proyecto, no existía ninguna política en las que ellos se pudieran alinear y los trabajadores eran conscientes de ello. Posterior a la implementación, los trabajadores sabían la existencia de la política general de seguridad de la información y las específicas en las que se deberían manejar en sus procedimientos diarios.

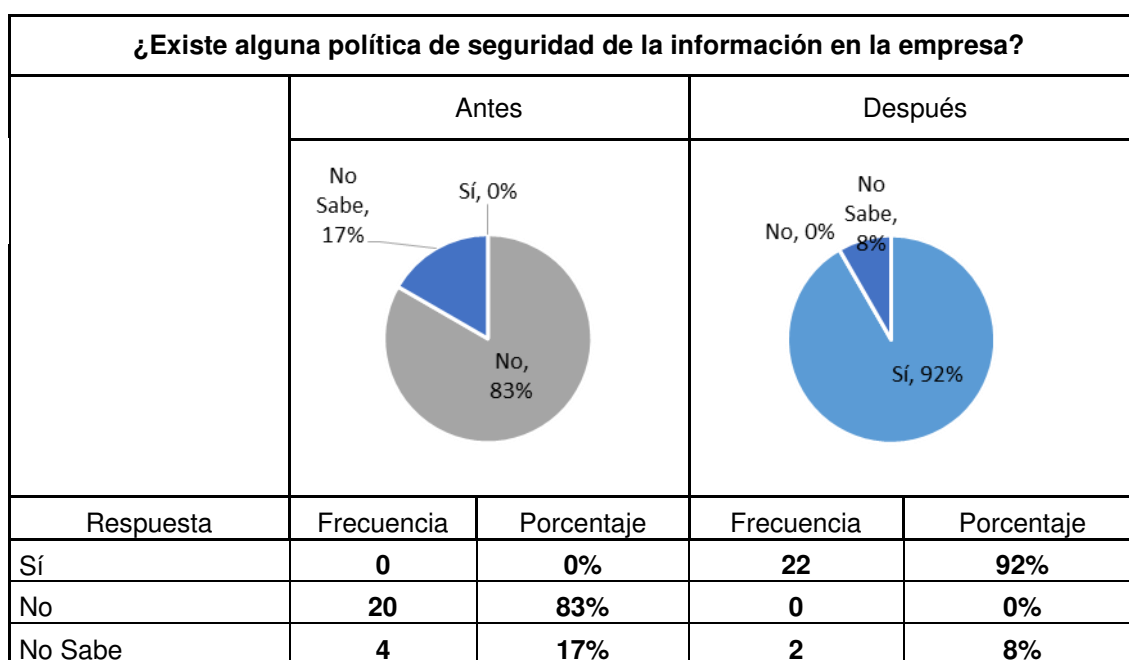


Figura 24 – Resultado de conocimiento de políticas de seguridad

Elaboración: Los autores

#### 4.4 Objetivo específico 3: Establecimiento de los controles para el tratamiento de los riesgos identificados en base a la ISO/IEC 27002

Para verificar el establecimiento de controles para los riesgos identificados, se realizó un análisis inicial donde se identificaron los controles que ya poseía la empresa (Ver Anexo 6 – Controles Previos al Proyecto). Luego del establecimiento de controles basados en la ISO/IEC 27002, se elaboró un cuadro en el cual se realizó una comparativa entre el número de controles por dominios (Dominios según la ISO/IEC 27002) entre la situación antes del proyecto y posterior a este. (Ver Tabla 27).

Tabla 27 – Comparación de Controles por Dominio

Dominios ISO/IEC 27002	Nro. Controles	
	Antes	Después
Políticas de Seguridad	0	2
Org. de la Seg. de la Información	0	2
Seg. RRHH	0	3
Gest. Activos	3	6
Control de Accesos	0	7
Criptografía	0	1
Seg. Física y del Entorno	0	6
Seg. Operaciones	2	3
Seg. Comunicaciones	0	1
Adq., Des. Y Mant. De los sistemas	0	0
Relaciones con los Proveedores	0	0
Gest. Incidentes de Seg. Inf.	1	4
Aspectos de Seg. Inf. De Gest. CdN.	2	2
Cumplimiento	1	2
<b>Total</b>	<b>9</b>	<b>39</b>

Elaboración: Los autores

Se verifica que previo al proyecto la clínica contaba con 9 controles y sin ninguna política de seguridad, luego de la implementación del SGSI cuenta con 39 controles. Es decir, los controles de seguridad incrementaron en 30, pero no solo eso, sino que los 9 previamente identificados han sido revisados y en otros casos reemplazados.

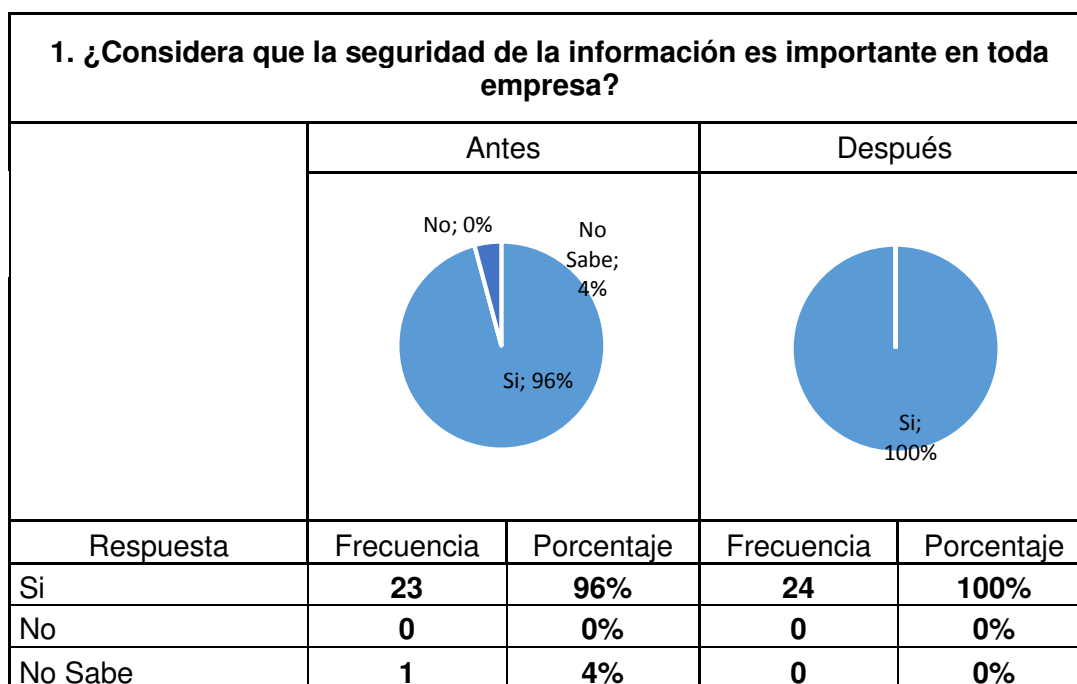
#### 4.5 Objetivo específico 4: Sensibilización a los colaboradores de la empresa en temas de seguridad de la información

El cumplimiento de este objetivo se midió a base de la comparación de

una encuesta previa a la implementación del proyecto y una posterior a esta.

Este objetivo fue de la mano junto a la implementación al SGSI, ya que para su implementación se requiere que los trabajadores sepan la importancia de la seguridad de la información en sus labores diarias. La encuesta consistía en 6 preguntas, las cuales serán analizadas a continuación.

La pregunta 1 fue: ¿Considera que la seguridad de la información es importante en toda empresa? (Ver Figura 25) Se observa que previo al proyecto, los trabajadores de MEDCAM ya consideraban que la seguridad de la información era un punto muy importante, esto ayudó a que no hubiera mucha resistencia al cambio, a la implementación de controles y políticas, ya que eran conscientes de la importancia de las mismas.



**Figura 25 – Resultados de Encuesta: Pregunta 1**

Elaboración: Los autores

La pregunta 2: ¿Conoce por qué es importante la seguridad de la información en la clínica MEDCAM Perú SAC? (Ver Figura 26). En esta pregunta, se puede ver que a pesar de que los trabajadores entendían la importancia de la seguridad de la información, no todos sabían cómo esto aplicaba a la clínica MEDCAM.

Posterior a la implementación, ya se comprendía la importancia de tener los

activos con los cuales trabajaban diariamente protegidos correctamente y como podría afectar al negocio si se llegara a producir algún incidente de seguridad como las posibles implicaciones legales, fallas en los procesos o sanciones.

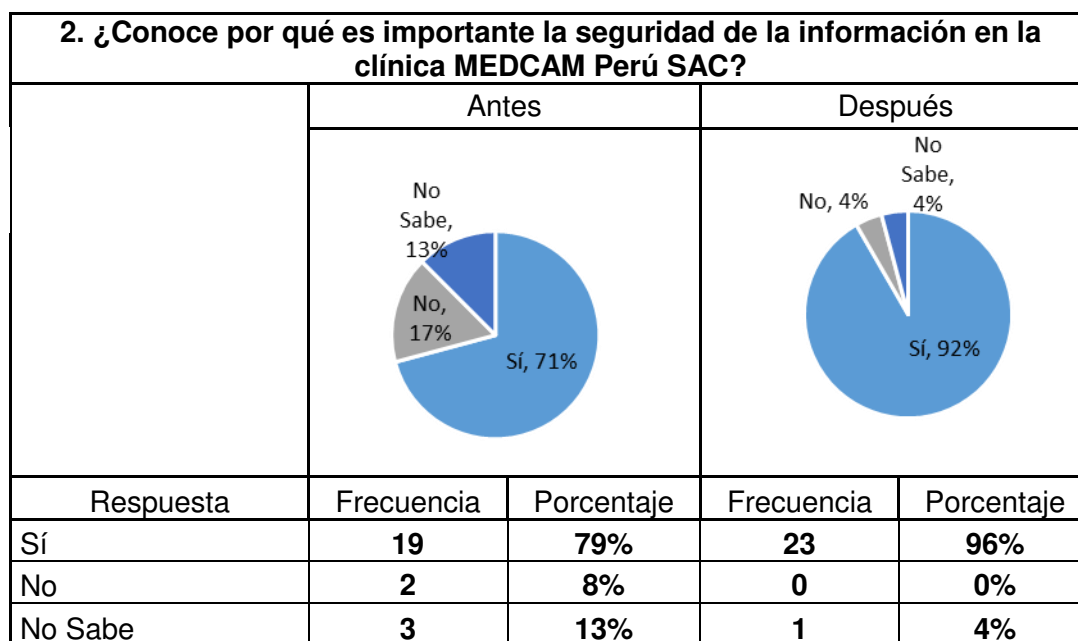


Figura 26 – Resultados de Encuesta: Pregunta 2

Elaboración: Los autores

La tercera pregunta fue: ¿Conoce las características principales que debe cumplir un activo de información respecto a su seguridad? (Ver Figura 27).

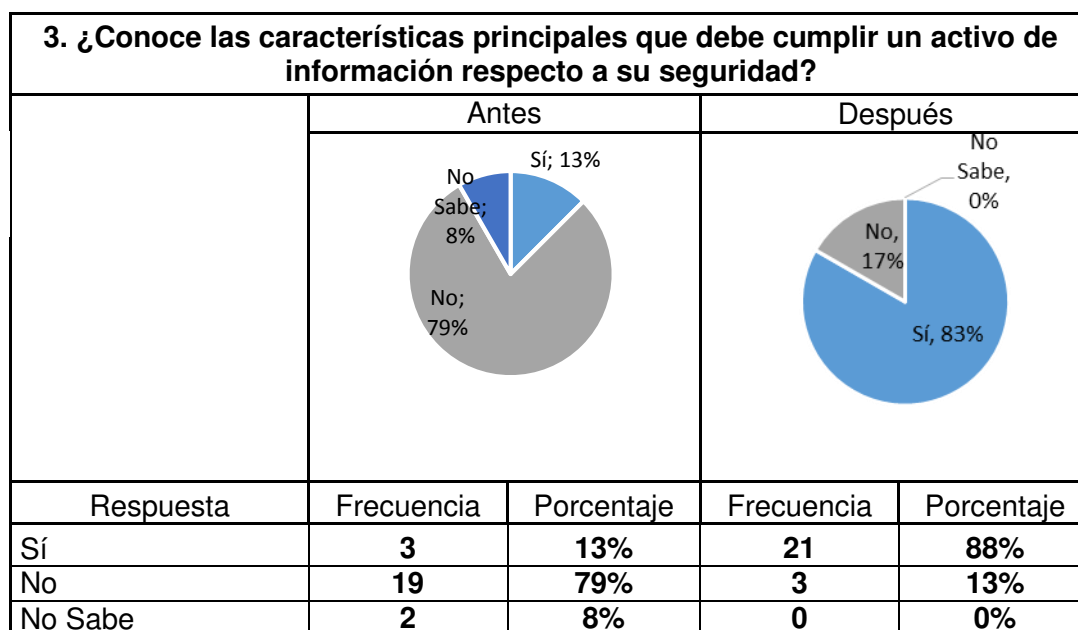


Figura 27 – Resultados de Encuesta: Pregunta 3

Elaboración: Los autores



En esta pregunta se puede observar que a pesar de que previo al proyecto consideraban la seguridad de la información importante, no sabían que las características que se buscan proteger son la confidencialidad, disponibilidad e integridad. Posterior al proyecto, la gran mayoría ya sabía las características que un sistema de gestión de seguridad de la información persigue respecto a los activos, esto ayuda al momento del relevamiento de riesgos y a la implementación de controles, ya que les permite conocer qué aspectos deben resguardar.

La pregunta 4: ¿Considera que los activos de la información de la organización están bien protegidos? (Ver Figura 28). En esta pregunta, se ve que previo al proyecto, a pesar de que no contaban con suficientes controles de seguridad y ninguna política, creían que sus activos estaban bien resguardados, lo cual era algo erróneo, ya que no conocían los riesgos a los que estaban expuestos. Posterior a la implementación, con las nuevas políticas de seguridad de la información y los controles diseñados se dieron cuenta que ahora efectivamente sus activos estaban mejor protegidos ya que había nuevos controles y planes de mitigación.

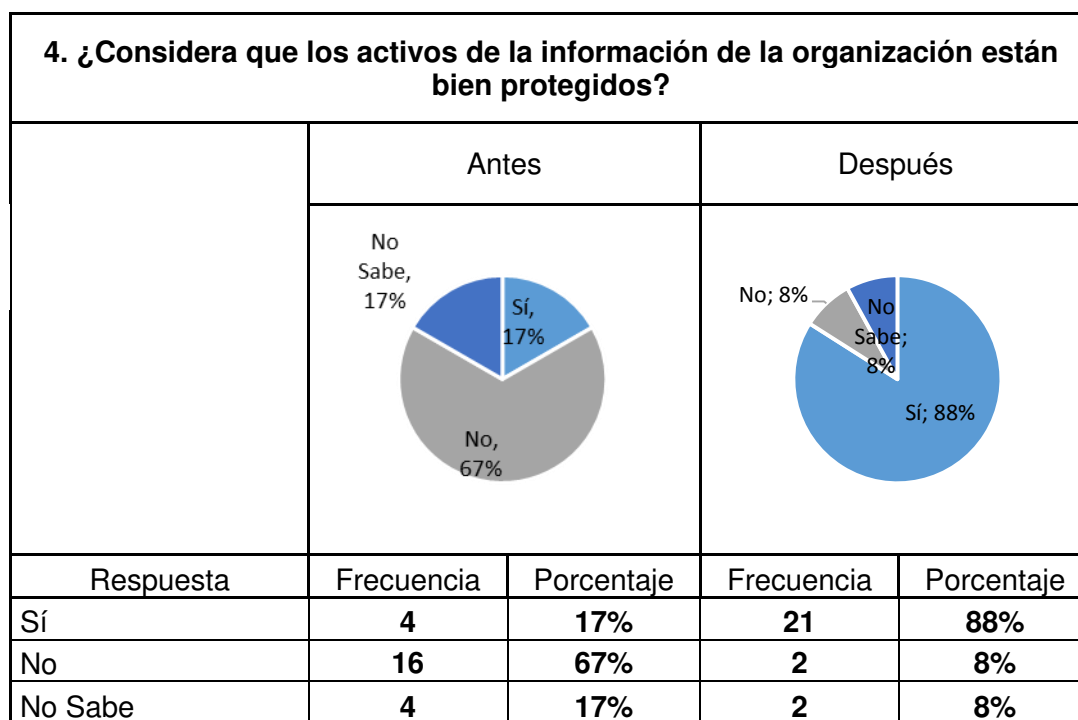
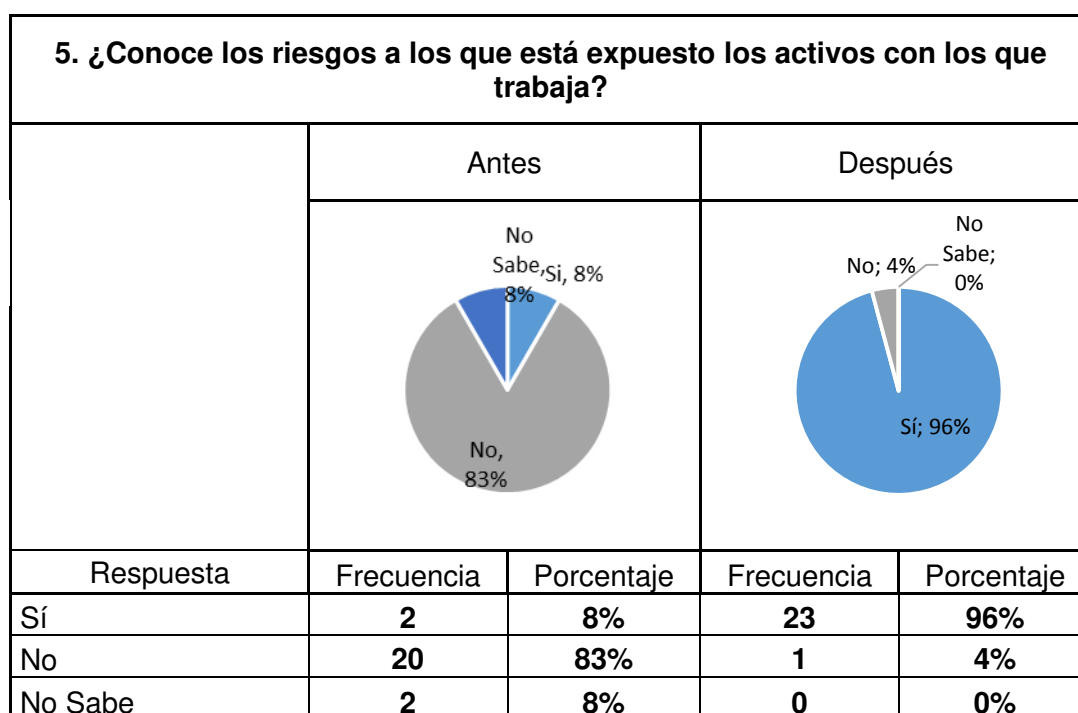


Figura 28 – Resultados de Encuesta: Pregunta 4

Elaboración: Los autores

La pregunta 5: ¿Conoce los riesgos a los que está expuesto los activos con los que trabaja? (Ver Figura 29). Se observa, en esta pregunta que previo al proyecto, los trabajadores conocían que sus activos no estaban correctamente protegidos, pero no sabían de que protegerlos, ya que no tenían un mapa de riesgos. Luego de la implementación, ya eran conscientes de las vulnerabilidades de sus activos y las posibles amenazas que podrían aprovecharse de estas.



**Figura 29 – Resultados de Encuesta: Pregunta 5**

Elaboración: Los autores

Por lo expuesto anteriormente, se puede advertir que los trabajadores de la clínica ahora están concientizados en la importancia de proteger los activos de información de la empresa frente a las amenazas a las que está expuesta y que la empresa se preocupa y hace lo posible mediante la implementación de políticas y controles que estos riesgos se mitiguen. A su vez, esta concientización ayuda a un proceso de mejora continua ya que los mismos trabajadores en su día a día pueden identificar nuevos riesgos emergentes o posibles controles.

## **CAPÍTULO V**

### **DISCUSIONES Y APLICACIONES**

#### **5.1 Discusiones**

Luego de la implementación de este proyecto se buscó contrastar los resultados con otras tesis que tuvieron como tema central la implementación de un sistema de gestión de seguridad de la información, el primer trabajo con el cual se compararemos los resultados será el de Vento, M. (2014) – “*Aplicación de Normativas de Seguridad de la Información para Systems Support & Services SA*”, donde se implementa un sistema de gestión de seguridad de la información, en una empresa de soluciones tecnológicas, en base a la ISO/IEC 27001.

En los resultados que obtuvo figuran la identificación de los activos de información y su valorización, mapeo de riesgos, declaración de aplicabilidad y la implementación de controles, lo que logró la reducción de los riesgos identificados. Esto se asemeja completamente con los resultados obtenidos en este proyecto y se ratifica que la implementación de un SGSI ayuda a la mitigación de los riesgos que se encuentran alrededor de los activos de información de cualquier tipo de empresa.

A su vez, menciona que pudo lograr la concientización de la mayoría del personal sobre temas de seguridad, al igual que este proyecto, ya que es la base para una mejora continua, así como una de las mejores prevenciones que se puede tener. Uno de los problemas que enfrentó fue que la empresa no contaba con ninguna política de seguridad, así como controles deficientes.

Estos problemas fueron similares a los encontrados al realizar este proyecto, claramente se ve que a pesar que las empresas son conocedoras de las amenazas a las que están expuestas, no tienen el conocimiento o las herramientas que les permita controlar esta situación.

Una de las recomendaciones más importantes que deja es la constante revisión y actualización de las políticas del SGSI, y controlar su cumplimiento, lo cual es básico ya que estamos en un entorno siempre cambiante y donde cada día se descubren nuevas tecnologías, es por eso que se hace la misma recomendación a MEDCAM.

Un segundo trabajo de investigación, con el cual nos pareció importante realiza la comparativa, es la de Talavera, V. (2015) – *“Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001”*, es un trabajo que se centra en la seguridad de la información de una entidad de salud al igual que este proyecto. La finalidad del proyecto es el diseño de un SGSI el cual mitigará las amenazas de los activos de información del Instituto Nacional Materno Perinatal.

Los resultados fueron el diseño e implementación de controles y políticas de seguridad de la información. Nuevamente, una de las conclusiones a la que se llegó fue que el factor humano es una de las claves para una correcta implementación de un SGSI, y que el personal de la empresa debe estar consciente que la información que manejan diariamente es confidencial y de alta importancia, al igual que los documentos que manejan los trabajadores de MEDCAM. En su proyecto advierte que los nuevos controles y cambios en el proceso pueden ser recibidos con cierto rechazo por parte de los trabajadores más antiguos ya que puede ser percibido como una amenaza. Para nuestro proyecto este rechazo no fue experimentado ya que contábamos con el total apoyo de la administración de la clínica y de los trabajadores, ya que comprendían que estos nuevos cambios eran necesarios ya que, adicionalmente de brindarles mayor seguridad en sus procesos, les daba una ventaja competitiva frente a las otras clínicas, y que su colaboración era esencial para que se llevara a cabo una correcta implementación del SGSI.

Una recomendación del proyecto es que se considere la implementación de un sistema de gestión de continuidad de negocio, lo que tiene mucho sentido ya que complementa al SGSI, pues este responde ante posibles escenarios que no permiten el desarrollo normal del negocio, por lo que queda como una recomendación aplicable a MEDCAM.

Otra recomendación que brinda es la digitalización de historias clínicas para un mejor respaldo de información; en nuestro caso, MEDCAM ya cuenta con historias clínicas digitales, pero no poseía los controles necesarios para asegurar este activo, por lo que se identificó como un activo crítico y se implementaron las estrategias de mitigación necesarias.

Como observamos en ambos proyectos, se consideró que la mejor manera de asegurar los activos de información es la implementación de un sistema de gestión de seguridad de la información ya que se logró reducir las amenazas sobre los activos asegurando la integridad, disponibilidad y confidencialidad de los mismos. De este análisis se deriva que el cumplimiento del objetivo principal, el de la mitigación de riesgos de los activos de información de MEDCAM, se realizó de un modo adecuado obteniendo resultados similares al de otros investigadores.

La medición de los resultados del proyecto respecto a los objetivos inicialmente indicados se puede apreciar en la siguiente Tabla (Ver Tabla 28).

**Tabla 28 – Objetivos asociados a sus pruebas y resultados**

<b>Nro</b>	<b>Objetivo General</b>	<b>Pruebas y Resultados</b>
4.1	Mitigar los riesgos a los que está expuesto los activos de información de la clínica MEDCAM Perú S.A.C.	Comparativa de exposición al riesgo de los activos de información previa al proyecto y posterior a este.
<b>Nro</b>	<b>Objetivos Específicos</b>	<b>Pruebas y Resultados</b>
4.2	Implementar el sistema de gestión de seguridad de información basada en la ISO/IEC 27001	Documentación requerida por la ISO/IEC 27001

Nro	Objetivos Específicos	Pruebas y Resultados
4.2	Implementar el sistema de gestión de seguridad de información basada en la ISO/IEC 27001	Documentación requerida por la ISO/IEC 27001
4.3	Implementar una política de Seguridad de la Información	Documentación e implementación de la política de seguridad de la información en la empresa.
4.4	Establecer controles para el tratamiento de los riesgos identificados en base a la ISO/IEC 27002	Comparativa de controles actuales y previos al proyecto
4.5	Sensibilizar a los colaboradores de la empresa en temas de seguridad de la información.	Encuesta sobre conocimiento respecto a la seguridad de la información.

Elaboración: Los autores

## 5.2 Aplicaciones

Un Sistema de Gestión de Seguridad de la Información puede ser aplicado a cualquier empresa sin importar el tamaño ni el rubro al que se dedique, como lo observamos en el punto anterior donde se analizaron trabajos de una empresa de solución tecnológica y una de un instituto estatal de salud, ya que es adaptable a las necesidades de cada negocio. Si bien es cierto, que en una empresa pequeña los presupuestos pueden ser más ajustados, esto no es necesariamente un impedimento para la implementación del SGSI, ya que se puede priorizar los procesos, servicios o productos que se desea proteger o que la empresa considere fundamentales, reduciendo los posibles gastos de controles no tan necesarios o políticas que no benefician directamente a las necesidades de la empresa. Para este proyecto el SGSI se aplicó en los procesos de compras e ingresos, considerando los sub-procesos que estos abarquen.

## **CONCLUSIONES**

1. Se logró la mitigación de los riesgos a los que estaban expuestos los activos de información de la clínica, a través de la identificación, diseño e implementación de controles para los riesgos más críticos.
2. La implementación del Sistema de Gestión de Seguridad de la Información fue la base para lograr el cumplimiento del objetivo principal. La implementación se logró a través del diseño e implementación de políticas para gestionar eficientemente el acceso a la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información logrando minimizar los riesgos de seguridad de la información.
3. El desarrollo e implementación de la Política de Seguridad de la Información fue importante ya que demostró el compromiso de la administración con la seguridad de la información, además de asignar roles y responsabilidades, estableció los lineamientos en los cuales se debe manejar la empresa y que deben ser seguidos por los trabajadores en sus labores diarias.
4. Luego de las evaluaciones realizadas concluimos que el establecimiento de controles es el tratamiento de riesgo idóneo para MEDCAM Perú, estos fueron diseñados en base a variables como el costo de la implementación, la efectividad para la mitigación del riesgo

identificado y el análisis de costo-beneficio.

5. La sensibilización del personal en temas de seguridad es vital para que el SGSI se pueda implementar en la organización y madure junto con esta. Ahora, los trabajadores de la clínica son conscientes que la información que ellos manejan es confidencial y que deben velar por su integridad total. Sensibilizar en temas de seguridad de la información, robustece al sistema implementado y genera una mejora continua. Esto también permitió que fuese más sencilla la implementación del SGSI.



## **RECOMENDACIONES**

1. Es necesario ampliar el Sistema de Gestión de Seguridad de la Información a los demás procesos de la clínica, que no han sido cubiertos por el SGSI, para cubrir todos los frentes a los que está expuesto.
2. Aplicar un mantenimiento periódico a las políticas de seguridad, ya que nos encontramos en un entorno totalmente cambiante donde se introducen nuevas tecnologías y las amenazas pueden variar.
3. Se sugiere implementar los controles que representan un gasto financiero para la organización; son medidas que garantizan la seguridad de los activos y aseguran la continuidad del negocio.
4. Agendar capacitaciones en temas de seguridad de la información a los nuevos trabajadores de la empresa y realizar un monitoreo periódico para ver el cumplimiento de las políticas y controles establecidos.
5. La empresa debe evaluar la factibilidad de la implementación de un plan de continuidad de negocios, que permita la recuperación total o parcial de sus actividades ante un escenario de interrupción de sus procesos.
6. Evaluar y certificar los procesos de la empresa bajo la ISO/IEC 27001.

## FUENTES DE INFORMACIÓN

### **Bibliográficas:**

**Abril, A., Pulido, J., Bohada, J (2013).** *Análisis de Riesgos en Seguridad de la Información.* Boyacá, Colombia. Fundación Universitaria Juan de Castellanos.

**Aguirre, A. (2014).** *Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A.* Lima, Perú. Pontificia Universidad Católica del Perú.

**Andress, J. (2015).** *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.* Massachusetts, Estados Unidos de América. Elsevier.

**Borek, A., Parlikad, A. K., Webb, J., & Woodall, P. (2013).** *Total information risk management: maximizing the value of data and information assets.* Massachusetts, Estados Unidos de América. Elsevier.

**Capita Secure Information Systems (2015).** *Benefits of ISO27001.* Chippenham, Reino Unido. Capita PLC.

**Columba, Bernardo (2017).** *Diseño de un sistema de Gestión de Seguridad de la Información, Basado en la Norma ISO/IEC 27001:2013 para la compañía ARONEM AIR Cargo S.A.*, Quito, Ecuador: Escuela Politécnica Nacional.

**Congreso de la República del Perú (2011).** *Ley N°29733 - Ley de Protección de Datos Personales.* Lima, Perú. Diario El Peruano.

**Dutton, J. (2016).** *Identifying assets for conducting an asset-based information security risk assessment.* Londres, Reino Unido. Portal Vigilant Software

**ESET Latinoamérica (2016).** ESET Security Report Latinoamérica 2016. ESET. Portal Web de ESET Latinoamérica.

**Espinoza, R. (2013).** *Análisis y Diseño de un Sistema de Gestión de Seguridad de Información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo.* Lima, Perú. Pontificia Universidad Católica del Perú.

**Fernandez, D., Pacheco, O. (2014).** *Mejora de Seguridad de Información en la Comandancia de Operaciones Guardacostas basada en la Norma Técnica Peruana NTP-ISO/IEC 27001:2008.* Lima, Perú. Universidad San Martín de Porres.

**Giraldo, L. (2016).** *Análisis para la Implementación de un Sistema de Gestión de la Seguridad de la Información según la Norma ISO 27001 en la empresa SERVIDOC S.A.* Cali, Colombia. Universidad Nacional Abierta y a Distancia Colombia.

**ISACA (2016).** *Planning for and Implementing ISO 27001.* ISACA Journal.

**ISO/IEC 27000 (2016).** *ISO/IEC 27000:2016 Tecnología de la Información – Técnicas de seguridad – Sistema de gestión de seguridad de la información – Vista general y vocabulario.* Génova, Suiza: ISO/IEC.

**ISO/IEC 27001 (2013).** *ISO/IEC 27001:2013 Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.* Génova, Suiza: ISO/IEC.

**ISO/IEC 27002 (2013).** *ISO/IEC 27002:2013 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.* Génova, Suiza: ISO/IEC.

**ISO/IEC 27005 (2011).** *ISO/IEC 27005:2011 Tecnología de la Información – Técnicas de seguridad – Gestión de Riesgos de la Seguridad de Información.* Génova, Suiza: ISO/IEC.

**ISO/IEC 31000 (2013).** *Gestión del Riesgo – Principios y directrices.* Génova, Suiza: ISO/IEC.

**Justino, Z. (2015).** *Diseño de un Sistema de Gestión de Seguridad de Información para una empresa Inmobiliaria alineada a la norma ISO/IEC 27001:2013.* Lima, Perú. Pontificia Universidad Católica del Perú.

**Kissel, R. (2013).** *Glossary of Key Information Security Terms.* Maryland, Estados Unidos de América. National Institute of Standards and Technology.

**Lachapelle, E., Bislimi, M. (2016).** *Information Technology - Security Techniques Code Of Practice For Information Security Controls.* Quebec, Canada. PECB.

**Layton, T. (2016).** *Information Security: Design, Implementation, Measurement and Compliance.* Florida, Estados Unidos de América. CRC Press.

**Lopes I., Oliveira P. (2014).** *Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises.* Braga, Portugal- Springer International Publishing.

**Mehraeen, E., Ayatollah, H., Ahmadi, M. (2016).** *Health Information Security in Hospitals: The Application of Security Safeguards.* Tehran, Iran. Universidad de Tehran.

**Peltier, T. (2016).** *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management.* Florida, Estados Unidos de América. CRC Press.

**PriceWaterHouse (2016).** *Resultados de la Encuesta Global de Seguridad de la Información.* Buenos Aires, Argentina. PwC Argentina.

**Resolución de Gerencia General ESSALUD N°1504 (2015).** *Conformación de Comité de Gestión de Seguridad de la Información en ESSALUD.* MINSA. Portal Institucional de ESSALUD.

**Sanchez, A., Fernández, J., Toval, A., Hernandez, I., Sánchez, B., Carrillo, J. (2014).** *Guía de Buenas Prácticas de Seguridad Informática en el Tratamiento de Datos de Salud para el Personal Sanitario en Atención Primaria.* Murcia, España. Elsevier.

**Solarte, F., Enriquez, E., Benavidez, M. (2015)** *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.* Guayaquil, Ecuador: Revista Tecnológica ESPOL.

**Talavera, V. (2015).** *Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de Salud de acuerdo a la ISO/IEC 27001:2013.* Lima, Perú. Pontificia Universidad Católica del Perú.

**Vento, M. (2014).** *Aplicación de Normativas de Seguridad de Información para System Support & Services S.A.* Lima, Perú. Universidad San Martín de Porres.

**Electrónicas:**

**Britvic, J., Prelas, A., Cingel, M. (2013).** *Integration Possibilities of ISO 9001:2008 Quality Management System with ISO 27001*. Recuperado de: <http://www.efos.unios.hr/repec/osi/eecytt/PDF/EconomyofeasternCroatiayest erdaytodaytomorrow02/eecytt0242.pdf>.

**Bussiness Beam (2016).** *Implementing ISO 27001 ISMS at Teradata Global Consulting Center*. Recuperado de: <https://www.businessbeam.com/casestudy-teradata>.

**Deloitte (2016).** *Ley de Protección de Datos Personales – Enfoque Práctico de Adecuación*. Lima, Perú. Recuperado de: [https://www2.deloitte.com/pe/es/pages/risk/articles/data\\_law\\_protection.html](https://www2.deloitte.com/pe/es/pages/risk/articles/data_law_protection.html)

**International Organization for Standardization (2016).** *ISO Survey 2015*. Recuperado de: <https://www.iso.org/the-iso-survey.html>

**Universidad de Southern Queenslad (2015).** *Information Asset and Security Classification Procedura*. Recuperado de: <http://policy.usq.edu.au/documents/13931PL>

**Tu, Z., Yuan, Y. (2014).** *Critical Success Factors Analysis on Effective Information Security Management: A Literature Review*. Recuperado de: <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1158&context=amcis2014>

## **ANEXOS**

Anexo 1 – Acta de constitución del Proyecto

Anexo 2 – Política general de seguridad de información

Anexo 3 – Políticas generales

Anexo 4 – Lista de amenazas y de vulnerabilidades

Anexo 5 – Efectividad de controles

Anexo 6 – Controles previos del proyecto

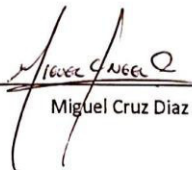
Anexo 7 – Reevaluación post implementación de controles

Anexo 8 – Acta de cierre del proyecto

## ANEXO 1 – Acta de constitución del proyecto

Acta de Constitución del proyecto			
<b>A. Información General</b>			
<b>Nombre del Proyecto:</b>	DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM PERU SAC	<b>Fecha de Preparación:</b>	24/03/2017
<b>Preparado Por:</b>	Senyi Fukusaki Infantas Miguel Cruz Diaz	<b>Autorizado Por:</b>	Administración de clínica MEDCAM Perú SAC
<b>B. Necesidad del Proyecto</b>			
<ul style="list-style-type: none"> <li>• Mitigar los riesgos a los que está expuestos los activos de información de la clínica MEDCAM Perú S.A.C.</li> </ul>			
<b>C. Objetivos del Proyecto</b>			
<ul style="list-style-type: none"> <li>• Implementar el sistema de gestión de seguridad de información basada en la ISO/IEC 27001.</li> <li>• Implementar una política de Seguridad de la Información.</li> <li>• Establecer controles para el tratamiento de los riesgos identificados en base a la ISO 27002.</li> <li>• Establecer una cultura de seguridad de información</li> </ul>			
<b>D. Alcance del proyecto</b>			
<ul style="list-style-type: none"> <li>• Proceso de ingresos</li> <li>• Proceso logístico</li> </ul>			

  
 Senyi Fukusaki Infantas

  
 Miguel Cruz Diaz

  
 Administración clínica MEDCAM  
 Perú SAC



## ANEXO 2 - Política general de seguridad de la información

	Versión 1.0
	Autor(es): Senyi Fukusaki I. Miguel Angel Cruz D.
	Fecha: 02/05/2017
<b>Política General de la Seguridad de la Información</b>	

### 1. Resumen

En la presente política se describe de forma general los lineamientos de seguridad en los que se debe manejar la empresa, tratamiento de los activos según su categoría, los roles y responsabilidades de la seguridad y las posibles sanciones a las que están expuestos por el incumplimiento de estas políticas de seguridad.

### 2. Objetivo

Establecer lineamientos para la gestión de la seguridad de la información que permita la protección adecuada de los activos de información frente a las amenazas a las cuales se encuentra expuesta la organización, tanto internas como externas, deliberadas o accidentales con la finalidad de asegurar la integridad, disponibilidad y confidencialidad de la información.

### 3. Alcance

La siguiente política de seguridad de la información es aplicable a toda la organización, empleados, entidades y profesionales contratados bajo otras modalidades. Este documento debe ser revisado y actualizado periódicamente según se crea conveniente respecto a cambios significativos dentro de la organización como el uso de nuevas tecnologías, nuevos servicios, cambios en la infraestructura, entre otros. A su vez, se toman consideraciones para el cumplimiento de la Ley 30024 – Ley que crea el registro nacional de historias clínicas electrónicas, la Ley 29733 – Ley de Protección de Datos Personales y la Ley 26842 - Ley General de Salud



#### 4. Generalidades

- MEDCAM Perú SAC reconoce la importancia de la información y de los sistemas de información, así como la necesidad disminuir las vulnerabilidades y protegerlas de las amenazas a las que se encuentran expuestos ya que puede constituir un peligro a la continuidad del negocio o daños muy importantes si se produjera una pérdida irreversible de datos. A su vez, por estar así establecidos en la legislación peruana en los que hace hincapié en la seguridad de los datos personales y en defensa de los intereses de los clientes, empleados y otros posibles afectados.
- Los accesos y usos de la información, estarán alineadas a las normativas internas, reglas, estándares y procedimientos de MEDCAM Perú SAC.
- Los empleados deben tener conocimiento de las políticas, normas, reglas, estándares y procedimientos y de igual manera, deberán conocer los documentos de seguridad que hagan referencia a datos de carácter personal.
- Se deberá contar con una adecuada segregación de funciones y revisión de las operaciones o transacciones que se realicen que permitan la identificación de la persona, cuando lo hizo y donde.
- Para la prevención de fraudes, delitos, errores u omisiones, se fomentará la difusión de la información y se promoverá una cultura de seguridad de información entre los colaboradores.
- Cada rol de usuario solo podrá realizar las tareas y acceder a datos necesarios y previamente autorizados.
- Se establecerán los medios necesarios y adecuados para proteger a las personas, datos, software, hardware, documentación y en general cualquier activo de seguridad de la información de MEDCAM Perú SAC.
- En caso de baja de un empleado se deberá entregar llaves, tarjetas de acceso, usuarios, equipos o cualquier tipo de información entregados o recopilados en sus funciones realizadas en MEDCAM Perú SAC. Si hubiera algún indicio de que no se devolvió toda la información, se analizará si ha podido realizar copias digitales o físicas, o haber introducido datos erróneos a la información de la empresa.
- La información debe clasificarse en alguno de los siguientes niveles:



- Activo Libre, se puede difundir y es de dominio público.
- Activo Restringido, solo puede debe ser de uso interno. Si se filtra, no ocasionaría no ocasionaría un riesgo.
- Activo Protegido, se debe tener controles para el acceso. Si se llega a filtrar, ocasionaría un riesgo moderado al negocio.
- Activo Confidencial, información sensible y no se puede difundir bajo ningún concepto. Su filtración ocasionaría un riesgo crítico para el negocio.
- Las zonas restringidas de la clínica deben contar con controles para impedir el daño o pérdida de información.
- Los puertos para medios removibles serán desactivados en todas las computadoras de la clínica. Si se requiere el uso del algún medio removible, debe justificarse a la administración.
- Se debe tener conocimiento y comunicar las políticas específicas de seguridad a todos los trabajadores de la clínica. Ante cualquier actualización, también debe ser comunicado especificando los cambios realizados.
- Se debe tener un proceso periódico para el inventariado de los activos de información de la empresa, según crea conveniente la administración de la clínica.
- La política general de seguridad de la información y las políticas específicas, deben ser revisadas al menos 1 vez al año para su actualización.

## 5. Responsabilidades

La responsabilidad de la seguridad de la información es de la gerencia general y el área de administración según sea el caso. Esto no niega que cada empleado deba asumir su responsabilidad respecto a los medios que utiliza, según los puntos que se indican las políticas, sus normas y procedimientos.

## 6. Sanciones

La violación de un control de seguridad o de la presente política justifica la aplicación de sanciones disciplinarias de acuerdo al reglamento interno de trabajo de la clínica, las cuales serán aplicadas teniendo en consideración lo





siguiente: Naturaleza y gravedad de falta, antecedentes del empleado, reincidencia y circunstancias en que se cometió la falta. La administración de la clínica es la encargada de determinar la gravedad de las faltas.

De acuerdo a la gravedad de la falta cometida, la gerencia podrá aplicar cualquiera de las siguientes sanciones:

- Amonestación verbal
- Amonestación por escrito
- Suspensión de labores
- Despido

Las amonestaciones verbales se impondrán a los trabajadores que comentan faltas por primera vez y que sean faltas leves.

Las amonestaciones por escrito se impondrán a los trabajadores que sean reincidentes en faltas leves o si realizan faltas que se considere que debe haber una amonestación más que verbal.

La suspensión de labores se impondrá a los trabajadores que hayan sido amonestados de manera reiterativa tanto verbal como escrita o que cometan faltas que no constituyan causal de despido.

Las sanciones no necesariamente se impondrán de forma progresiva. La gravedad de la falta determinará la sanción a imponerse.

## **7. Políticas Específicas**

Las políticas específicas de Seguridad deben estar alineadas y están soportadas bajo la política general de seguridad. Estas políticas son las siguientes:

- Política de Gestión de Contraseñas
- Política de Escritorio Limpio
- Política de Gestión de Accesos
- Política de Gestión de Incidentes
- Política de Gestión de Copias de Respaldo
- Política de Gestión de Activos



**ANEXO 3 – Políticas específicas**  
**Política de Gestión de Contraseñas**

	Versión 1.0
	Autor(es): Senyi Fukusaki I. Miguel Ángel Cruz D.
	Fecha: 02/05/2017
<b>Política de Gestión de Contraseñas</b>	

### 1. Resumen

En el presente documento se definirán una serie de lineamientos que deberá usarse como requisito mínimo en lo que concierne la gestión de contraseñas. Este es un aspecto muy importante en la seguridad de la información, ya que si se vulnera y permite el acceso a personas no autorizadas, compromete la seguridad de los activos digitales de la clínica.

### 2. Objetivo

La siguiente política de seguridad tiene como objetivo mitigar el riesgo de accesos no autorizados mediante el establecimiento de estándares para la creación de contraseñas y su respectivo mantenimiento.

### 3. Alcance

El alcance de la política incluye a todas las cuentas de usuarios que accedan a los dominios de la clínica, como el inicio de sesión en los sistemas operativos, cuentas de correo electrónico, aplicativos informáticos entre otros.

### 4. Creación de Contraseñas

- Las contraseñas de los usuarios deben tener al menos 8 caracteres.
- Las contraseñas deben estar compuesta por las siguientes características:
  - Letras mayúsculas
  - Caracteres no alfabéticos (¡, #, \$, %, &, !, @')

- Números
- Las contraseñas no deben ser palabras fácilmente identificables como el nombre del usuario, fechas de cumpleaños, nombre de mascotas entre otros.
- Las contraseñas de distintas aplicaciones no deben ser iguales.
- Las contraseñas usadas dentro del ámbito laboral no deben ser iguales a las usadas para fines personales.

## **5. Gestión de Contraseñas de Usuarios**

- Las contraseñas deben ser cambiadas máximo cada 90 días.
- No usar la característica de “Recordar contraseña” presente en la mayoría de navegadores de internet.
- La contraseña del usuario no debe ser almacenada en ningún documento físico ni digital.
- No se debe compartir la contraseña con ningún usuario.
- Si la contraseña es solicitada por algún miembro de la empresa o un agente externo, informar inmediatamente a la administración de MEDCAM.
- Si el usuario olvida o pierde la contraseña, deberá ser solicitada a una renovación a la Administración.

## **6. Gestión de Contraseñas para Desarrolladores**

- Las contraseñas gestionadas por las aplicaciones o sistemas operativos de la empresa deben ser correctamente encriptados y no ser guardadas como texto plano.
- Si se cuenta con acceso remoto a la red de la empresa, esta debe ser gestionadas a través de un VPN (Virtual Private Network) a través de contraseñas o tokens de seguridad.
- Los campos usados como contraseñas dentro de aplicaciones usadas por la empresa, no deben mostrar explícitamente los caracteres ingresados, en su defecto, se debe mostrar caracteres no alfabéticos (\*, \_, @).

## **7. Roles y Responsabilidades**

Los roles y responsabilidades son las definidas en el punto 5 de la **Política general de seguridad de la información**.

## **8. Sanciones**

Las sanciones aplicables son las definidas en el punto 6 de la Política General de la Seguridad de la Información.

## Política de Escritorio Limpio

	Versión 1.0
	Autor(es): Senyi Fukusaki I. Miguel Ángel Cruz D.
	Fecha: 02/05/2017
<b>Política de Escritorio Limpio</b>	

### 1. Resumen

En el presente documento se definirán una política de escritorio limpio, que asegura que todos los documentos o información confidencial no estén visibles ni sean manipulados por un tercero cuando el trabajador no se encuentra en su área de trabajo. Esta es una política realmente importante ya que ayuda reducir significativamente las posibles filtraciones o alteración de información de los activos de la empresa.

### 2. Objetivo

La siguiente política de seguridad tiene como objetivo que la información solo sea visualizada y modificada por el personal autorizado, mediante el establecimiento de criterios que los trabajadores deben cumplir cuando no se encuentren en su área de trabajo.

### 3. Alcance

El alcance de la política incluye a todos los trabajadores de la clínica.

### 4. Criterios de Escritorio Limpio

- Se debe bloquear la computadora al momento de ausentarse de su estación de trabajo y al final del día deben ser apagados.
- Los documentos, archivos o dispositivos electrónicos sensibles no deben estar expuestos en el escritorio del trabajador cuando este no se encuentre



en su estación de trabajo y al final del día deben guardar la información en su respectivo almacén o en su escritorio bajo llave.

- Las llaves usadas para las gavetas del escritorio o de los almacenes no deben ser descuidadas en ningún momento por el trabajador.
- Las computadoras personales deben ser ancladas cuando el trabajador no se encuentre en su estación de trabajo.
- Los documentos sensibles que sean desechados, deben ser debidamente destruidos sin la posibilidad de una posible reconstrucción.
- Las impresiones o mensajes de fax, deben ser inmediatamente recogidas para evitar que un tercero se apodere del documento.
- Cuando un tercero, que no cuente con los permisos de visualización o modificación de ciertos documentos, se acerque a la estación de trabajo, no se debe mostrar archivos abiertos en la pantalla de la computadora.

## **5. Monitoreo**

- Al finalizar el día se hará un repaso por todas las estaciones de trabajo para verificar que efectivamente estos criterios están siendo seguidos por los trabajadores.
- Si se detecta algún documento, archivo o dispositivo electrónico, será almacenado por la administración de la clínica hasta el día siguiente. Para la devolución de estos documentos, archivos o dispositivos electrónicos, el trabajador debe acercarse a la administración mostrando la conformidad de su jefatura directa.

## **6. Roles y Responsabilidades**

Los roles y responsabilidades son las definidas en el punto 5 de la **Política general de seguridad de la información**.

## **7. Sanciones**

Las sanciones aplicables son las definidas en el punto 6 de la Política General de la Seguridad de la Información.

## Política de Gestión de Accesos

	Versión 1.0
	Autor(es): Senyi Fukusaki I. Miguel Ángel Cruz D.
	Fecha: 02/05/2017
<b>Política de Gestión de Accesos</b>	

### 1. Resumen

En el presente documento se detallará la gestión de accesos a los sistemas de la clínica, sus activos de información, el manejo de los usuarios y el monitoreo que se debe tener de estos.

### 2. Objetivo

La siguiente política de seguridad tiene como objetivo definir la gestión del control de accesos a los activos de información de la clínica.

### 3. Alcance

Esta política aplica a toda la información suministrada por la clínica, ya sea a través de documentos físicos, carpetas compartidas, bases de dato, aplicaciones, entre otros y para quienes las administran y hacen uso de estas.

### 4. Acceso a la Información

- Los trabajadores de la clínica solo deberán tener acceso a los activos de información que sean necesarios para el cumplimiento de sus funciones dentro de la clínica.
- A todos los trabajadores que ingresen a la clínica se les generará un usuario para que ingresen a las aplicaciones y computadoras que se les asigne, y una contraseña que deberá cumplir los lineamientos de la **Política de Gestión de Contraseñas**. A su vez, se le brindará la documentación necesaria para el manejo de los activos asignados.

- Los activos de información a los que tendrá acceso los usuarios por las funciones que realizan serán definidos por la jefatura directa y el área de administración de la clínica. Finalmente, el dueño del activo tendrá que dar la aprobación final para conceder los permisos requeridos.
- Si se requiere dar acceso a un tercero por temas de auditoría, consultoría, entre otros, primero deberá ser aprobado por la administración de la clínica y el dueño del activo y posteriormente deberá firmarse un acuerdo de confidencialidad.
- Para los aplicativos y sistemas de la clínica, deberá designarse un único administrador que tenga los permisos de brindar los accesos a los usuarios.

## **5. Mantenimiento de los accesos**

- Se debe realizar un mantenimiento periódico de los accesos a los distintos activos de información. Este mantenimiento debe realizarse por lo menos una vez cada seis meses.
- Los accesos brindados a terceros, deben ser retirados una vez terminada la auditoría, consultoría o según corresponda.
- A los terceros y/o trabajadores que cambien de funciones, se debe evaluar si mantendrán los accesos previos y la documentación que actualmente poseen. De no ser el caso, se debe hacer devolución de la información y documentación, y a su vez, la actualización de los permisos que tenga.
- A los terceros y/o trabajadores que cesen sus funciones de la clínica, deberán devolver toda documentación que se le haya brindado y se le debe retirar los accesos inmediatamente.

## **6. Segregación de Funciones**

- Los accesos que se brindan deben ser individuales y no por grupos de usuarios.
- Los accesos a los usuarios deben estar basadas en una segregación de funciones, es decir, que no puede tener acceso a todas las operaciones / funciones / transacciones de algún proceso del negocio.

## **7. Roles y Responsabilidades**

Los roles y responsabilidades son las definidas en el punto 5 de la **Política general de seguridad de la información**.

## **8. Sanciones**

Las sanciones aplicables son las definidas en el punto 6 de la Política General de la Seguridad de la Información.

## Política de Gestión de Incidentes de Seguridad

	Versión 1.0
	Autor(es): Senyi Fukusaki I. Miguel Ángel Cruz D.
	Fecha: 02/05/2017
<b>Política de Gestión de Incidentes de Seguridad</b>	

### 1. Resumen

En el presente documento se presenta los lineamientos a seguir en caso se presente algún incidente de seguridad de información.

### 2. Objetivo

La siguiente política de seguridad tiene como objetivo establecer lineamientos generales para la gestión de incidentes de seguridad para reducir el impacto en la clínica.

### 3. Alcance

El alcance de la política incluye a todos los trabajadores de la clínica.

### 4. Gestión de Incidentes

- Todo trabajador de la clínica tiene la responsabilidad de comunicar algún incidente de seguridad que sea de su conocimiento, a los responsables de la seguridad en la clínica y a su jefatura directa.
- Todos los incidentes reportados serán clasificados para determinar si se trata de un incidente de seguridad, la gravedad, los procedimientos y plan de respuesta deben ser determinados por los responsables de seguridad.
- Se debe establecer procedimientos para incidentes de seguridad y establecer las coordinaciones necesarias con instituciones como Bomberos, Policías, Servicios Médicos, entre otros, según corresponda.

- Los responsables de seguridad, deben registrar todos los incidentes de seguridad de información detectados detallando como mínimo:
  - Nombre del Activo afectado
  - Detalle del incidente de seguridad
  - Riesgo asociado al incidente
  - Controles asociados al incidente
  - Comportamiento de los controles durante el incidente
  - Impacto Financiero / Legal / Reputacional del incidente
  - Planes de Acción
- Los incidentes de seguridad graves deben ser informado a todas las gerencias y administración de la clínica, detallando el evento, el impacto hacia el negocio y los planes de acción.
- Los incidentes de seguridad considerados como graves, deben ser inmediatamente analizados para determinar si se está violando alguna ley existente.
- Una vez superado el incidente, se debe monitorear los controles asociados al incidente de seguridad, para determinar la efectividad del control y establecer si se realizó el cumplimiento de este.
- Una vez superado el incidente, se debe evaluar si se trata de un nuevo riesgo o si es un riesgo conocido. Si es nuevo, se debe proceder a realizar una evaluación del riesgo. Si es un riesgo conocido, se debe analizar si está dentro del apetito del riesgo o necesita ser reclasificado aumentando o disminuyendo su impacto.

## **7. Roles y Responsabilidades**

Los roles y responsabilidades son las definidas en el punto 5 de la **Política general de seguridad de la información**.

## **8. Sanciones**

Las sanciones aplicables son las definidas en el punto 6 de la Política General de la Seguridad de la Información.

## Política de Gestión de Copias de Respaldo

	Versión 1.0
	Autor(es): Senyi Fukusaki I. Miguel Ángel Cruz D.
	Fecha: 02/05/2017
<b>Política de Gestión de Copias de Respaldo</b>	

### 1. Resumen

En el presente documento se presenta los lineamientos a seguir para realizar copias de respaldo o hacer uso de estas.

### 2. Objetivo

La siguiente política de seguridad tiene como objetivo establecer lineamientos generales para la gestión de copias de respaldo de los aplicativos, base de datos y documentos.

### 3. Alcance

Esta política aplica a toda la información suministrada por la clínica, ya sea a través de documentos físicos, carpetas compartidas, bases de dato, aplicaciones, entre otros y para quienes las administran y hacen uso de estas.

### 4. Gestión de Incidentes

- Se realizarán copias de seguridad de la base de datos un mínimo de 1 vez a la semana.
- Se realizará copias de seguridad de los documentos digitales mínimo 1 vez al día.
- Las copias de seguridad deben ser realizadas de manera automática no manual, guardando versiones por fechas y no reemplazándolas en cada copia.

- Las copias de respaldo no deben ser realizados dentro de los mismos servidores ni dentro del mismo local donde estos se encuentran.
- Si se desea realizar una restauración parcial o completa de la información, esta debe ser solicitada a los encargados de seguridad e informado a la jefatura directa.
- Toda copia de respaldo debe estar debidamente encriptado.

## **7. Roles y Responsabilidades**

Los roles y responsabilidades son las definidas en el punto 5 de la **Política general de seguridad de la información**.

## **8. Sanciones**

Las sanciones aplicables son las definidas en el punto 6 de la Política General de la Seguridad de la Información.



## Política de Gestión de Activos

	Versión 1.0
	Autor(es): Senyi Fukusaki I. Miguel Ángel Cruz D.
	Fecha: 02/05/2017
<b>Política de Gestión de Activos</b>	

### 1. Resumen

En el presente documento se presenta los lineamientos a seguir la gestión de activos de información de la clínica.

### 2. Objetivo

La siguiente política de seguridad tiene como objetivo establecer lineamientos generales para la gestión de los activos de la clínica previniendo su pérdida de integridad, disponibilidad y confidencialidad.

### 3. Alcance

Esta política aplica a toda la información suministrada por la clínica, ya sea a través de documentos físicos, carpetas compartidas, bases de dato, aplicaciones, entre otros y para quienes las administran y hacen uso de estas.

### 4. Seguridad de Información Digital

- Se debe tener conocimiento de las políticas, normas, reglas, estándares y procedimientos en el uso de todo activo de información de manera digital.
- Las aplicaciones utilizadas para realizar comunicaciones electrónicas serán otorgados por MEDCAM Perú SAC. No podrá utilizar ningún software adicional, de ser necesario deberán comunicarse al respectivo inmediato superior.

- El intercambio de información laboral con pacientes, clientes, proveedores o terceros deben ser realizados con los recursos entregados por la clínica. El uso de correos personales está prohibido.
- Está prohibido interceptar, divulgar o leer comunicaciones electrónicas sin la autorización del dueño de la información.
- El acceso a internet para actividades que no estén dentro de las funciones del colaborador debe ser moderado.
- No almacenar información restringida en dispositivos móviles.
- Todo documento que sea clasificado como confidencial deberá estar debidamente encriptado.
- Se debe contar con antivirus, cortafuegos un programa de encriptación en todas las computadoras de la clínica sin excepción.
- Los medios removibles deben ser inhabilitados en todas las computadoras de la clínica. Si se necesita el uso de algún medio removible, se debe solicitar a la administración con su respectiva justificación.
- El lugar donde se almacena la información digital debe tener un mantenimiento de mínimo 1 vez cada 6 meses.
- Para evitar comprometer información de forma accidental, se debe tener en cuenta lo siguiente:
  - Evitar abrir correos sospechosos o de destinatarios desconocidos.
  - Bloquear la pantalla del computador cuando no se encuentre en el área de trabajo.
  - Eliminar completamente documentación digital.

## **5. Seguridad Física y de sitio**

- Se debe tener conocimiento de las políticas, normas, reglas, estándares y procedimientos en el uso de todo activo de información física y de sitio.
- El acceso a las áreas administrativas solo estará permitido para empleados, mientras las áreas de consultas, laboratorios, exámenes, área de espera serán permitidos para empleados, clientes y pacientes.

- De existir la necesidad de eliminar un documento con datos confidenciales deben ser destruidos de tal manera que la información en esta sea irrecuperable.
- Los escritorios administrativos deben quedar vacíos (sin ningún documento a la vista) cuando el colaborador no se encuentre en el lugar.
- Las gavetas asignadas para cada empleado deben estar cerradas bajo llave.
- Los documentos que sean generales de la empresa (Kardex, Historias clínicas, entre otros) serán almacenados dentro de un almacén asignado bajo llave.
- El lugar donde se almacena la información debe tener un mantenimiento de mínimo 1 vez al año.

## **6. Roles y Responsabilidades**

Los roles y responsabilidades son las definidas en el punto 5 de la **Política general de seguridad de la información**.

## **7. Sanciones**

Las sanciones aplicables son las definidas en el punto 6 de la Política General de la Seguridad de la Información.

## ANEXO 4 - Lista de amenazas y vulnerabilidades

### Lista de Amenazas:

La ISO 27005 menciona una lista de amenazas, que serán usadas en el proyecto para determinar la matriz de riesgos. El origen de las amenazas puede ser Deliberado (D), Accidental (A) o Ambiental (E). A es usado para acciones humanas que pueden dañar los activos de manera accidental y E es usado para las acciones que no son de origen humano.

Tipo	Amenaza	Origen
Daño Físico	Fuego	A,D,E
	Daño por Agua	A,D,E
	Contaminación	A,D,E
	Accidente	A,D,E
	Destrucción de Equipos	A,D,E
Eventos Naturales	Polvo, Corrosión, Congelamiento	A,D,E
	Fenómenos climáticos	E
	Fenómenos Sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos Meteorológicos	E
Fallo de Servicios esenciales	Inundaciones	E
	Falla en el aire acondicionado o suministro de Agua	A,D
	Falla en Energía eléctrica	A,D,E
Radiación	Falla en los equipos de telecomunicaciones	A,D
	Radiación electromagnética	A,D,E
	Radiación térmica	A,D,E
Compromiso de la información	Pulsos electromagnéticos	A,D,E
	Intercepción de señales	D
	Espionaje	D
	Monitoreo ilegal	D
	Robo de documentos	D
	Robo de Equipos	D
	Recuperación de equipos desechados	D
	Divulgación de información	A,D
	Datos de fuentes no confiables	A,D
	Manipulación de Hardware	D
	Manipulación de Software	A,D
Detección de posición	D	
Fallas Técnicas	Fallo de equipo	A
	Mal Funcionamiento de Equipo	A
	Saturación de los sistemas de información	A,D
	Malfuncionamiento de Software	A
	Falta de mantenimiento de software	A,D

Tipo	Amenaza	Origen
Acciones no autorizadas	Uso no autorizado de los equipos	D
	Copia fraudulenta de Software	D
	Uso de software pirata	A,D
	Data corrupta	D
	Proceso ilegal de data	D
Compromiso de funciones	Error en el uso	A
	Abuso de derecho	A,D
	Falsificación de derecho	D
	Negación de accesos	D
	No disponibilidad de personal	A,D,E

Lista de Vulnerabilidades:

Tipo	Vulnerabilidad
Hardware	Mantenimiento insuficiente / Fallo en la Instalación de dispositivos de almacenamiento
	Falta de reemplazo periódico
	Susceptibilidad al polvo, humedad y suciedad
	Sensibilidad a la radiación electromagnética
	Falta de un eficiente control de cambios
	Susceptible de cambio de voltaje / Susceptible al cambio de temperatura
	Almacenamiento desprotegido
	Falta de cuidado en la disposición del hardware
	Copia no controlada
Software	Prueba de software no existente
	Defectos del software
	Falta de finalización de sesión por parte del usuario
	Uso o reutilización de los medios de almacenamiento sin borrado adecuado
	Falta de Prueba de Auditoría
	Falla en la distribución de accesos
	Uso de aplicaciones a datos errados en término de tiempo
	Interfaz de usuario compleja
	Falta de documentación
	Parámetros incorrectamente configurados
	Fechas incorrectas
	Falta de mecanismo de autenticación

Tipo	Vulnerabilidad
	Tabla de contraseñas desprotegida
	Pobre gestión de contraseñas
	Servicios innecesarios habilitados
	Software nuevo o inmaduro
	Especificaciones incompletas o nada clara de los desarrolladores
	Falta de control de cambios
	Descarga y uso no controlado de Software
	Falta de respaldos
	Falta de protección física del edificio
	Falla en los reportes de gestión
Red	Falta de Prueba de envío o recibimiento de mensajes
	Líneas de comunicación no protegidas
	Tráfico sensible no protegidos
	Pobre cableado
	Punto único de falla
	Falta de autenticación de quien envía y recibe
	Arquitectura de red insegura
	Transferencia de contraseñas autorizadas
	Gestión inadecuada de red
	Conexiones públicas de red no autorizadas.
Personal	Ausencia de personal
	Proceso inadecuado de contratación
	Seguridad enseñada insuficientemente
	Uso incorrecto de Software y Hardware
	Cultura de seguridad insuficiente
	Falta de mecanismo de monitoreo
	Trabajo no supervisado del personal externo
Falta de política en el uso de líneas de comunicaciones.	
Sitio	Uso inadecuado de acceso físico a las edificaciones
	Ubicación en un área susceptible de desastres
	Red energética inestable
	Falta de protección física del edificio, puerta y ventanas
Organización	Falta de procedimiento formal para el registro y eliminación de usuarios.
	Falta de procedimiento formal de la revisión de los accesos de los usuarios
	Falta o insuficiencia de disposición en los contratos con

Tipo	Vulnerabilidad
	los clientes.
	Falta de monitoreo de los recursos de procesamiento de información.
	Falta de auditorías periódicas.
	Falta de procedimiento de identificación y evaluación de riesgos.
	Falta de reportes de errores y fallos en los logs de administrador y operadores.
	Respuesta inadecuada de mantenimiento de servicio
	Falta de Acuerdos de nivel de servicios
	Falta de procedimientos de control de cambio
	Falta de procedimientos formales para la revisión de la documentación del SGSI.
	Falta de procedimientos formales para la autorización de la información pública
	Falta de responsabilidades en SGSI
	Falta de planes de continuidad de negocios
	Falta de política de uso de correos
	Falta de procedimientos formales para el uso de nuevos software
	Falta de logs en el administrador y operadores
	Falta de procedimiento para el manejo de información clasificada
	Falta de información de la responsabilidad de la seguridad en la descripción de los puestos
	Falta de procesos disciplinarios en caso de un incidente de seguridad
	Falta de política para el uso de computadoras portátiles
	Falta de control de activos fuera de la organización
	Falta de política de limpieza de escritorio y de pantalla
	Falta de autorización en los procesos de la información
	Falta de mecanismos de monitoreo
	Falta de revisión por parte de la gerencia
	Falta de procedimiento para reporte de debilidades en la seguridad
	Falta de procedimiento del cumplimiento de disposiciones de derechos de autor

## ANEXO 5 – Efectividad de controles

Datos del Control					
<b>Cod Control</b>	C001	<b>Cod Control ISO</b>	5.1.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Anual
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	No	No	No	0	
<b>Resultado final</b>					<b>66.67</b>
<b>Justificación (Si el resultado es negativo)</b>	El control se ha definido con periodicidad anual, por lo que no se ejecutado hasta el momento.				
<b>Evidencia</b>	No aplica				
<b>Resultado</b>	Efectividad no puede ser evaluada.				
Datos del Control					
<b>Cod Control</b>	C002	<b>Cod Control ISO</b>	5.1.2		
<b>Naturaleza</b>	Detectivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Anual
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	No	No	No	0	
<b>Resultado final</b>					<b>66.67</b>
<b>Justificación (Si el resultado es negativo)</b>	El control se ha definido con periodicidad anual, por lo que no se ejecutado hasta el momento.				
<b>Evidencia</b>	No aplica				
<b>Resultado</b>	Efectividad no puede ser evaluada.				
Datos del Control					
<b>Cod Control</b>	C003	<b>Cod Control ISO</b>	6.1.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Anual
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	0	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Política de Seguridad de la Información				
<b>Resultado</b>	Control efectivo.				



Datos del Control					
<b>Cod Control</b>	C004	<b>Cod Control ISO</b>	6.1.2		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Anual
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	0	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Flujo de Procesos				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C005	<b>Cod Control ISO</b>	7.1.2		
<b>Naturaleza</b>	Detectivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Anual
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	No	No	No	0	
<b>Resultado final</b>					<b>66.67</b>
<b>Justificación (Si el resultado es negativo)</b>	El control se ha definido con periodicidad anual, por lo que no se ejecutado hasta el momento.				
<b>Evidencia</b>	Acuerdo de Confidencialidad				
<b>Resultado</b>	Efectividad no puede ser evaluada.				
Datos del Control					
<b>Cod Control</b>	C006	<b>Cod Control ISO</b>	7.2.2		
<b>Naturaleza</b>	Detectivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	0	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica.				
<b>Evidencia</b>	Resultados de encuesta.				
<b>Resultado</b>	Control efectivo.				

Datos del Control					
<b>Cod Control</b>	C007	<b>Cod Control ISO</b>	7.2.3		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Política de Seguridad de la Información				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C008	<b>Cod Control ISO</b>	8.1.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Inventario de Activos de Información				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C009	<b>Cod Control ISO</b>	8.1.2		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Inventario de Activos de Información				
<b>Resultado</b>	Control efectivo.				

Datos del Control					
<b>Cod Control</b>	C010	<b>Cod Control ISO</b>	8.1.3		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Política Especifica: Gestión de Activos				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C011	<b>Cod Control ISO</b>	8.1.4		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Política Especifica: Gestión de Accesos				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C012	<b>Cod Control ISO</b>	8.3.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Automático	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Captura de pantalla de no reconocimiento de dispositivos.				
<b>Resultado</b>	Control efectivo.				

Datos del Control					
<b>Cod Control</b>	C013	<b>Cod Control ISO</b>	8.3.3		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Flujo de Proceso: Procesamiento de Datos				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C014	<b>Cod Control ISO</b>	9.1.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Política Específica: Gestión de Accesos				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C015	<b>Cod Control ISO</b>	9.2.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Fecha de cese vs. Fecha de baja en el sistema.				
<b>Resultado</b>	Control efectivo.				

Datos del Control					
<b>Cod Control</b>	C016	<b>Cod Control ISO</b>	9.2.2		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Automático	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Pantalla de configuración.				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C017	<b>Cod Control ISO</b>	9.2.3		
<b>Naturaleza</b>	Detectivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Semestral
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	No	No	No	0	
<b>Resultado final</b>					<b>66.67</b>
<b>Justificación (Si el resultado es negativo)</b>	El control se ha definido con periodicidad semestral, por lo que no se ejecutado hasta el momento.				
<b>Evidencia</b>	No aplica				
<b>Resultado</b>	Efectividad no puede ser evaluada.				
Datos del Control					
<b>Cod Control</b>	C018	<b>Cod Control ISO</b>	9.2.4		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Automático	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Pantalla de configuración.				
<b>Resultado</b>	Control efectivo.				

Datos del Control					
<b>Cod Control</b>	C019	<b>Cod Control ISO</b>	9.4.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Imagen del lugar restringido.				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C020	<b>Cod Control ISO</b>	9.4.3		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Automático	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Pantalla de configuración.				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C021	<b>Cod Control ISO</b>	10.1.2		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Automático	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Pantalla de configuración.				
<b>Resultado</b>	Control efectivo.				

Datos del Control					
<b>Cod Control</b>	C022	<b>Cod Control ISO</b>	11.1.2		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	No	No	No	0	
Eficacia Operativa? (40%)	No	No	Si	40	
<b>Resultado final</b>					<b>46.67</b>
<b>Justificación (Si el resultado es negativo)</b>	La organización no ha implementado seguridad alrededor del centro de datos de la empresa.				
<b>Evidencia</b>	No aplica.				
<b>Resultado</b>	Control inefectivo.				
Datos del Control					
<b>Cod Control</b>	C023	<b>Cod Control ISO</b>	11.1.3		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Foto de señalización.				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C024	<b>Cod Control ISO</b>	11.1.4		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Foto de extinguidores, señalización, luminarias, etc.				
<b>Resultado</b>	Control efectivo.				

Datos del Control					
<b>Cod Control</b>	C025	<b>Cod Control ISO</b>	11.2.4		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Anual
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	No	No	No	0	
<b>Resultado final</b>					<b>66.67</b>
<b>Justificación (Si el resultado es negativo)</b>	El control se ha definido con periodicidad anual, por lo que no se ejecutado hasta el momento.				
<b>Evidencia</b>	No aplica				
<b>Resultado</b>	Efectividad no puede ser evaluada.				
Datos del Control					
<b>Cod Control</b>	C026	<b>Cod Control ISO</b>	11.2.8		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Pantalla de configuración.				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C027	<b>Cod Control ISO</b>	11.2.9		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Bimestral
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	No	No	No	0	
<b>Resultado final</b>					<b>66.67</b>
<b>Justificación (Si el resultado es negativo)</b>	El control se ha definido con periodicidad mensual, por lo que no se ha ejecutado a la fecha.				
<b>Evidencia</b>	No aplica				
<b>Resultado</b>	Efectividad no puede ser evaluada.				



Datos del Control					
<b>Cod Control</b>	C028	<b>Cod Control ISO</b>	12.1.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	Si	Si	Si	100	
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Pantalla de carpeta con políticas				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C029	<b>Cod Control ISO</b>	12.2.1		
<b>Naturaleza</b>	Detectivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Anual
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	No	No	No	0	
<b>Resultado final</b>					<b>66.67</b>
<b>Justificación (Si el resultado es negativo)</b>	El control se ha definido con periodicidad anual, por lo que no se ejecutado hasta el momento.				
<b>Evidencia</b>	No aplica				
<b>Resultado</b>	Efectividad no puede ser evaluada.				
Datos del Control					
<b>Cod Control</b>	C030	<b>Cod Control ISO</b>	12.3.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	Mensual
Evaluación					
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>	
Control Diseñado correctamente? (30%)	Si	Si	Si	100	
Control Implementado? (30%)	Si	Si	Si	100	
Eficacia Operativa? (40%)	No	No	No	0	
<b>Resultado final</b>					<b>66.67</b>
<b>Justificación (Si el resultado es negativo)</b>	El control se ha definido con periodicidad mensual, por lo que no se ha ejecutado a la fecha.				
<b>Evidencia</b>	No aplica				
<b>Resultado</b>	Efectividad no puede ser evaluada.				

Datos del Control				
<b>Cod Control</b>	C031	<b>Cod Control ISO</b>	13.1.1	
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Automático	<b>Frecuencia</b> A demanda
Evaluación				
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>
Control Diseñado correctamente? (30%)	Si	Si	Si	100
Control Implementado? (30%)	No	No	No	0
Eficacia Operativa? (40%)	No	No	No	0
<b>Resultado final</b>				<b>33.33</b>
<b>Justificación (Si el resultado es negativo)</b>	Se cuenta con presupuesto para la implementación en el segundo semestre del año. La organización no ha implementado el directorio activo al momento de la revisión.			
<b>Evidencia</b>	No aplica.			
<b>Resultado</b>	Control inefectivo.			
Datos del Control				
<b>Cod Control</b>	C032	<b>Cod Control ISO</b>	16.1.1	
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b> No aplica
Evaluación				
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>
Control Diseñado correctamente? (30%)	Si	Si	Si	100
Control Implementado? (30%)	Si	Si	Si	100
Eficacia Operativa? (40%)	Si	Si	Si	0
<b>Resultado final</b>				<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica			
<b>Evidencia</b>	Política Específica: Gestión de Incidentes			
<b>Resultado</b>	Control efectivo.			
Datos del Control				
<b>Cod Control</b>	C034	<b>Cod Control ISO</b>	16.1.5	
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b> No aplica
Evaluación				
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>
Control Diseñado correctamente? (30%)	Si	Si	Si	100
Control Implementado? (30%)	Si	Si	Si	100
Eficacia Operativa? (40%)	Si	Si	Si	0
<b>Resultado final</b>				<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica			
<b>Evidencia</b>	Política Específica: Gestión de Incidentes			
<b>Resultado</b>	Control efectivo.			

Datos del Control					
<b>Cod Control</b>	C035	<b>Cod Control ISO</b>	16.1.7		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>		<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>
Control Diseñado correctamente? (30%)		Si	Si	Si	100
Control Implementado? (30%)		Si	Si	Si	100
Eficacia Operativa? (40%)		Si	Si	Si	100
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Pantalla de documento compartido.				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C036	<b>Cod Control ISO</b>	17.1.2		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	No aplica
Evaluación					
<b>Indicador</b>		<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>
Control Diseñado correctamente? (30%)		Si	Si	Si	100
Control Implementado? (30%)		Si	Si	Si	100
Eficacia Operativa? (40%)		Si	Si	Si	0
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Historial Clínica Física				
<b>Resultado</b>	Control efectivo.				
Datos del Control					
<b>Cod Control</b>	C037	<b>Cod Control ISO</b>	17.2.1		
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b>	A demanda
Evaluación					
<b>Indicador</b>		<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>
Control Diseñado correctamente? (30%)		Si	Si	Si	100
Control Implementado? (30%)		Si	Si	Si	100
Eficacia Operativa? (40%)		Si	Si	Si	100
<b>Resultado final</b>					<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica				
<b>Evidencia</b>	Evidencia de sitio alterno.				
<b>Resultado</b>	Control efectivo.				

Datos del Control				
<b>Cod Control</b>	C038	<b>Cod Control ISO</b>	18.1.1	
<b>Naturaleza</b>	Preventivo	<b>Tipo</b>	Manual	<b>Frecuencia</b> No aplica
Evaluación				
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>
Control Diseñado correctamente? (30%)	Si	Si	Si	100
Control Implementado? (30%)	Si	Si	Si	100
Eficacia Operativa? (40%)	Si	Si	Si	0
<b>Resultado final</b>				<b>100.00</b>
<b>Justificación (Si el resultado es negativo)</b>	No aplica			
<b>Evidencia</b>	Política de Seguridad de la Información			
<b>Resultado</b>	Control efectivo.			
Datos del Control				
<b>Cod Control</b>	C039	<b>Cod Control ISO</b>	18.2.3	
<b>Naturaleza</b>	Detectivo	<b>Tipo</b>	Manual	<b>Frecuencia</b> Anual
Evaluación				
<b>Indicador</b>	<b>Experto 1</b>	<b>Experto 2</b>	<b>Experto 3</b>	<b>Resultado</b>
Control Diseñado correctamente? (30%)	Si	Si	Si	100
Control Implementado? (30%)	Si	Si	Si	100
Eficacia Operativa? (40%)	No	No	No	0
<b>Resultado final</b>				<b>66.67</b>
<b>Justificación (Si el resultado es negativo)</b>	El control se ha ejecutado hasta el momento pues tiene frecuencia anual.			
<b>Evidencia</b>	No aplica			
<b>Resultado</b>	Efectividad no puede ser evaluada.			

## ANEXO 6 – Controles previos al proyecto

Sección	Control ISO/IEC 27002	Objetivo de Control	Control	Situación Previa a la implementación
9. Control de acceso	9.2.2	Suministro de acceso de usuarios	Implementar un procedimiento que permita a los usuarios del sistema acceder al sistema o negar el acceso a este cuando se considere necesario.	Control implementado: Se cuenta con un proceso en el cual se otorgan en los sistemas de información de MEDCAM el acceso por perfiles en base a las responsabilidades de los usuarios.
9. Control de acceso	9.3.1	Uso de la información de autenticación secreta	Se deben crear perfiles para el acceso a información considerada de suma importancia para la empresa	Control en proceso: Se otorga accesos a los sistemas de información están segregados en base a funciones, pero no se cuenta con un matriz de perfiles por puesto.
9. Control de acceso	9.4.1	Restricción de acceso Información	Restringir el acceso a la información por parte de personal no autorizado.	Control en proceso: Los accesos otorgados se delimita a información específica en base a las funciones de los usuarios.
12. Seguridad de las operaciones	12.2.1	Controles contra códigos maliciosos	Los equipos de cómputo deben contar con software contra código malicioso, el cual se debe actualizar constantemente con el fin actualizar parches que mitiguen las nuevas vulnerabilidades.	Control en proceso: No todos los equipos cuentan antivirus actualizado.
12. Seguridad de las operaciones	12.3.1	Respaldo de información	Se debe realizar respaldo de la información, además se deben realizar pruebas para comprobar que estos cumplen con las políticas de respaldo-	Control en proceso: Se ejecutan copias de respaldo, pero estas no son almacenadas en un lugar distinto al de las operaciones.
16. Gestión de incidentes de seguridad de la información	16.1.5	Respuesta a incidentes de seguridad de la información	Se debe establecer un proceso que permita establecer los pasos a seguir para atender el incidente.	Control en proceso: El personal conoce empíricamente las acciones de respuesta en base a experiencias difundidas por la administración.

Sección	Control ISO/IEC 27002	Objetivo de Control	Control	Situación Previa a la implementación
17. Aspectos de seguridad de la información de la gestión de continuidad de negocio	17.1.2	Implementación de la continuidad de la seguridad de la información	Implementar procedimientos que permitan la continuidad del negocio ante situaciones imprevistas que podrían causar retrasos en la operación.	Control en proceso: Se cuentan con reemplazos físicos (historias clínicas físicas) ante la inhabilitación de equipos electrónicos.
17. Aspectos de seguridad de la información de la gestión de continuidad de negocio	17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Es necesario establecer redundancias en las instalaciones donde se procesa la información con el fin de que no se vea afectada la disponibilidad de la información.	Control implementado: Se cuenta con instalaciones alternas en las cuales se pueden continuar con las operaciones de la empresa en caso de inhabilitación de una de las instalaciones.
18. Cumplimiento	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Definir el marco legal con el cual se debe regir la seguridad de la información.	Control en proceso: Se han determinado documentos que son aceptados y firmados por los pacientes en los cuales aceptan y dan su consentimiento sobre el tratamiento de la información médica en base a la Ley 26842 - Ley General de Salud.

### ANEXO 7 – Reevaluación post implementación de controles

ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
R1	MediWeb	Improbable	Crítico	Alto	A.9 Control de acceso A.11 Seguridad física y ambiental	A.9.4.3 - Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad. A.11.2.9 - Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamiento de la información debe ser adoptada.	Raro	Crítico	Medio
R4	MediWeb	Improbable	Crítico	Alto	A.9 Control de acceso	A.9.2.1 - Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de accesos. A.9.2.5 - Los propietarios de los activos deben revisar los derechos de accesos de usuario a intervalos regulares.	Raro	Crítico	Medio
R5	MediWeb	Probable	Relevante	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.	Improbable	Relevante	Medio

ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
R7	MediWeb	Posible	Alto	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	Raro	Alto	Bajo
R9	MediWeb	Posible	Crítico	Alto	A.9 Control de acceso	A.9.2.1 - Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de accesos. A.9.2.5 - Los propietarios de los activos deben revisar los derechos de accesos de usuario a intervalos regulares.	Raro	Crítico	Medio
R14	Sistema Logístico de MedCam	Probable	Relevante	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan. A.12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo apropiado.	Improbable	Relevante	Medio



ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
R15	Sistema Logístico de MedCam	Probable	Relevante	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.	Improbable	Relevante	Medio
R25	Base de Datos	Improbable	Crítico	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.	Raro	Crítico	Medio
R28	Base de Datos	Improbable	Crítico	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Se debe realizar respaldo de la información, además se deben realizar pruebas para comprobar que estos cumplen con las políticas de respaldo-	Raro	Crítico	Medio
R34	Computadoras de Escritorio	Probable	Alto	Alto	A.9 Control de acceso A.11 Seguridad física y ambiental	A.9.4.3 - Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad. A.11.2.9 - Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamiento de la información debe ser adoptada.	Improbable	Alto	Medio

ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
R35	Computadoras de Escritorio	Probable	Alto	Alto	A.8 Gestión de Activos	A.8.1.1 - Información, otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos de ser elaborado y mantenido. A.8.1.2 - Los activos mantenidos en el inventario deben ser propios.	Improbable	Alto	Medio
R37	Computadoras de Escritorio	Probable	Alto	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.	Improbable	Alto	Medio
R41	Consentimiento Informado - Ley	Posible	Alto	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.	Improbable	Alto	Medio
R42	Consentimiento Informado - Ley	Posible	Alto	Alto	A.11 Seguridad física y ambiental	A.11.1.4 - Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	Raro	Alto	Bajo
R43	Consentimiento Informado - Ley	Posible	Alto	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.	Improbable	Alto	Medio

ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
R44	Historia Clínica	Probable	Crítico	Crítico	A.11 Seguridad física y ambiental A.18 Cumplimiento	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado. A.18.1.4. - La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevante donde sea aplicable.	Raro	Crítico	Medio
R47	Historia Clínica	Probable	Crítico	Crítico	A.11 Seguridad física y ambiental A.18 Cumplimiento	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información. A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado. A.18.1.4. - La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevante donde sea aplicable.	Raro	Crítico	Medio
R48	Historia Clínica	Improbable	Crítico	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e	Raro	Crítico	Medio

ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
						instalaciones de procesamiento de información.			
R49	Historia Clínica	Probable	Crítico	Crítico	A.11 Seguridad física y ambiental	A.11.1.4 - Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	Raro	Crítico	Medio
R50	Historia Clínica	Posible	Crítico	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.	Raro	Crítico	Medio
R51	Historia Clínica	Improbable	Crítico	Alto	A.6 Organización de la seguridad de la información	A.6.1.3 - Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.	Raro	Crítico	Medio
R54	Consentimiento Informado - Atención	Posible	Crítico	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.	Raro	Crítico	Medio
R56	Consentimiento Informado - Atención	Posible	Alto	Alto	A.11 Seguridad física y ambiental	A.11.1.4 - Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	Raro	Alto	Bajo

ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
R57	Consentimiento Informado - Atención	Posible	Crítico	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.	Raro	Crítico	Medio
R60	Hoja Interconsulta	Posible	Crítico	Alto	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.	Raro	Crítico	Medio
R64	Resultados Finales	Probable	Crítico	Crítico	A.8 Gestión de Activos A.11 Seguridad física y ambiental	A.8.3.3 - Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte. A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.	Raro	Crítico	Medio
R65	Resultados Finales	Improbable	Crítico	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.	Raro	Crítico	Medio
R66	Resultados Finales	Probable	Crítico	Crítico	A.11 Seguridad física y ambiental	A.11.1.4 - Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	Raro	Crítico	Medio

ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
R67	Resultados Finales	Probable	Crítico	Crítico	A.11 Seguridad física y ambiental	A.11.1.2 - Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite acceso sólo al personal autorizado.	Raro	Crítico	Medio
R68	Resultados Finales	Posible	Crítico	Alto	A.11 Seguridad física y ambiental	A.11.1.1 - Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de información.	Raro	Crítico	Medio
R69	Historia Clínica Digital	Probable	Alto	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	Improbable	Alto	Medio
R71	Historia Clínica Digital	Probable	Crítico	Crítico	A.8 Gestión de Activos	A.8.3.1. - Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.	Raro	Crítico	Medio
R72	Historia Clínica Digital	Improbable	Crítico	Alto	A.9 Control de acceso	A.9.2.1 - Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de accesos. A.9.2.5 - Los propietarios de los activos deben revisar los derechos de accesos de usuario a intervalos regulares.	Raro	Crítico	Medio

ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
R73	Historia Clínica Digital	Probable	Crítico	Crítico	A.9 Control de acceso	A.9.3.1 - Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autenticación secreta. A.9.4.1 - El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.	Raro	Crítico	Medio
R79	Servidor de Aplicaciones	Posible	Alto	Alto	A.12 Seguridad de las operaciones	A.12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el mejor riesgo.	Improbable	Alto	Medio
R83	Servidor de Aplicaciones	Posible	Crítico	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	Raro	Crítico	Medio

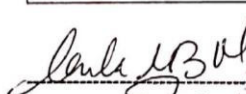
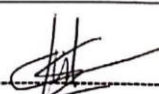
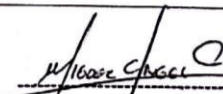
ID Riesgo	Activo	Prob.	Consec.	Criticidad	Cláusula	Controles ISO/IEC 27002:2013	Prob. luego de Control	Consec. luego de Control	Criticidad luego de Control
R85	Servidor de Aplicaciones	Posible	Crítico	Alto	A.12 Seguridad de las operaciones	A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	Raro	Crítico	Medio
R87	Kardex	Posible	Alto	Alto	A.12 Seguridad de las operaciones	A.12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el mejor riesgo.	Posible	Relevante	Medio



## ANEXO 8 – Acta de cierre del proyecto

### ACTA DE CIERRE Y ENTREGA DEL PROYECTO

<b>Título del Proyecto</b> DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM PERU SAC	
<b>Objetivos Finales del Proyecto</b> <i>Objetivo general</i>  Mitigar los riesgos a los que está expuestos los activos de información de la clínica MEDCAM Perú S.A.C.  <i>Objetivos específicos</i> <ul style="list-style-type: none"> <li>Implementar el sistema de gestión de seguridad de información basada en la ISO/IEC 27001.</li> <li>Implementar una política de Seguridad de la Información.</li> <li>Establecer controles para el tratamiento de los riesgos identificados en base a la ISO 27002.</li> <li>Establecer una cultura de seguridad de información</li> </ul>	
<b>Fecha de entrega del Proyecto:</b> 27/05/2017	<b>Fecha de Inicio del Proyecto:</b> 13/03/2017
<b>Entregables generados por el proyecto:</b> <ul style="list-style-type: none"> <li>Política de Seguridad de la Información</li> <li>Inventario de Activos</li> <li>Matriz de Amenazas y Vulnerabilidades</li> <li>Valoración de Activos</li> <li>Matriz de Riesgos</li> <li>Listado de controles</li> <li>Declaración de Aplicabilidad</li> </ul>	<b>Costo Final del Proyecto en SOLES</b> El proyecto no representó costo alguno para la empresa.
<b>Logros del proyecto:</b> <ul style="list-style-type: none"> <li>Lograr la mitigación de los riesgos a los que estaban expuestos los activos más críticos de la empresa.</li> <li>Establecer una cultura de seguridad en la empresa.</li> </ul>	
<b>Beneficiario del Proyecto:</b> MEDCAM Perú S.A.C.	
<b>Comentarios Generales:</b> La importancia de implementar un sistema de gestión de seguridad de la información basado en estándares de buenas prácticas, como la familia ISO/IEC 27000, así como un personal de experiencia en lo relacionado a control interno asegura la correcta implementación del mismo.	

 Administradora MEDCAM Carla Barbarán V.	 Integrante Proyecto Senyi Fukusaki I.	 Integrante Proyecto Miguel A. Cruz D.
-----------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------