



# Universidad **Mariana**

Seguridad de la información basada en la norma ISO/IEC 27001 para la Clínica Proinsalud de la  
Ciudad de Pasto

Carlos Fernando Delgado Martínez  
Daniel Alejandro Solarte Criollo  
Nicolas Alexander Muñoz Jamauca

Universidad Mariana  
Facultad de Ingeniería  
Programa de Ingeniería de Sistemas  
San Juan de Pasto

2023

Seguridad de la información basada en la norma ISO/IEC 27001 para la Clínica Proinsalud de la  
Ciudad de Pasto.

Carlos Fernando Delgado Martínez

Daniel Alejandro Solarte Criollo

Nicolas Alexander Muñoz Jamauca

Informe de investigación para optar al título de Ingeniero de Sistemas

MSc. José Javier Villalba Romero

Asesor

Universidad Mariana

Facultad de Ingeniería

Programa de Ingeniería de Sistemas

San Juan de Pasto

2023

Artículo 71: los conceptos, afirmaciones y opiniones emitidos en el Trabajo de Grado son responsabilidad única y exclusiva del (los) Educando (s)

Reglamento de Investigaciones y Publicaciones, 2007  
Universidad Mariana

## **Dedicatoria**

A mis amados padres Carlos Delgado y Ruby Martínez ya que fueron el pilar fundamental en mi educación brindándome las mejores enseñanzas en base a su esfuerzo, por su perseverancia para que el futuro de sus hijos sea lleno de éxitos, por su apoyo incondicional para lograr mis metas y llegar a ser un profesional. A mi familia por su motivación para que llegue a ser un profesional, por formar parte de los cimientos en mi formación académica y por enseñarme a valorar el esfuerzo de mis padres y por último y no menos importante a mi esposa Adriana Mora y mi hija Laura ya que ellas me regalaron el último empujoncito para ser un gran profesional

Carlos Fernando Delgado Martínez

## **Agradecimientos**

Primeramente, a nuestro Dios ya que él nunca me abandono en los momentos difíciles que se aparecieron en mi vida, por hacerme un hombre de bien dándome a conocer que en esta vida siempre vamos a contar con él y sobre todo con su amor infinito. A mi madre y padre Rubiela y Carlos por su infinito amor, paciencia, dedicación que gracias a ello me ha hecho un hombre sabio. A mi hija Laura, a mis hermanos por ser mi inspiración de ser un profesional y ejemplo a seguir de nuestra familia. Gracias a mis tíos por sus palabras motivadoras de ser “Alguien en la vida”, de que uno de la familia tiene que ser el ejemplo y motivación de las siguientes generaciones. Gracias a mi tutor Ing. Javier Villalba por compartir su conocimiento y don de persona durante mi vida académica en la universidad y especialmente en este trabajo. Carlos Fernando Delgado

## Contenido

Introducción .....	15
1. Elementos del proceso investigativo .....	17
1.1. Antecedentes y estado del conocimiento.....	17
1.1.1. Antecedentes internacionales .....	17
1.1.2. Antecedentes nacionales.....	18
1.2. Título .....	19
1.3. Problema de investigación .....	19
1.3.1. Descripción del problema.....	19
1.3.2. Formulación del problema .....	21
1.4. Objetivos .....	22
1.4.1. Objetivo general .....	22
1.4.2. Objetivos específicos.....	22
1.5. Justificación.....	22
1.6. Marcos de referencia .....	24
1.6.1. Marco teórico - conceptual.....	24
1.6.1.1. ISO/IEC 27001 .....	29
1.6.1.2. Modelo PHVA.....	30
1.6.1.3. Metodología Magerit.....	31
1.6.2. Marco legal.....	32
1.6.3. Marco contextual.....	34
1.7. Metodología .....	37
1.7.1. Paradigma de investigación.....	37
1.7.2. Enfoque de investigación .....	37
1.7.3. Tipo de investigación .....	37
1.7.4. La línea de investigación.....	37
1.7.5. Áreas Temáticas de investigación .....	38
1.7.6. Población y muestra .....	38
1.8. Presupuesto.....	42
1.9. Cronograma.....	44

1.10. Productos esperados .....	46
2. Desarrollo del proceso investigativo .....	47
2.1. Activos informáticos, procesos y servicios de las áreas de la Clínica Proinsalud .....	47
2.1.1. Dirección subgerencia administrativa y financiera .....	47
2.1.1.1. Talento humano. ....	47
2.1.1.2. Contabilidad. ....	52
2.1.1.3. Facturación. ....	55
2.1.1.3.1. Factura o documento de cobro equivalente de venta por prestación de servicios. 1. Nota Débito Cliente. 2. Nota Crédito Cliente .....	55
2.1.1.3.2. Insumos y productos del proceso de facturación. Entradas: a. Un contrato o convenio y un manual de tarifas, Varios contratos pueden utilizar un mismo manual de tarifas. ....	55
2.1.1.4. Cartera. ....	60
2.1.1.5. Suministros. ....	63
2.1.1.6. Pagaduría. ....	65
2.1.1.7. Registro y control. ....	67
2.1.1.8. Área de sistemas .....	69
2.1.2. Dirección clínica .....	74
2.1.2.1. Urgencias. ....	74
2.1.2.2. Hospitalización. ....	79
2.1.2.3. Quirófano. ....	83
2.1.2.4. Unidad de Cuidado Intensivo (UCI). ....	87
2.2. Análisis y evaluación de amenazas, riesgos y vulnerabilidades con metodología Magerit ....	91
2.2.1. Análisis de vulnerabilidades riesgos y amenazas aplicando criterios de valoración por color del valor y las dimensiones de seguridad .....	94
2.2.2. Área pagaduría .....	94
2.2.2.1. Amenazas por desastre natural. ....	94
2.2.2.2. Amenazas por origen industrial. ....	96
2.2.2.3. Amenazas por errores y fallos no intencionados. ....	99
2.2.2.4. Amenazas por ataques intencionados. ....	102
2.2.3. Área facturación .....	105
2.2.3.1. Amenazas por desastre natural. ....	105

2.2.3.2. Amenazas por origen industrial.....	107
2.2.3.3. Amenazas por errores y fallos no intencionados.....	110
2.2.3.4. Amenazas por ataques intencionados.....	113
2.2.4. Área sistemas.....	117
2.2.5. Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 .	126
2.2.5.1. Política institucional de seguridad de la información en la Clínica Proinsalud S.A. ....	126
2.2.5.1.1. Objetivo.....	127
2.2.5.1.2. Estrategia 1.....	127
2.2.5.1.3. Estrategia 2.....	127
2.2.5.1.4. Estrategia 3.....	128
2.2.5.1.5. Estrategia 4.....	129
2.2.5.1.6. Estrategia 5.....	129
2.2.5.2. Objetivos de control y controles. Anexo A de la ISO 27001 a implementarse en la Clínica Proinsalud S.A.....	130
2.2.5.3. Política táctica de seguridad de la información en el área de recursos humanos. ....	132
2.2.5.3.1. Objetivo.....	132
2.2.5.3.2. Estrategia 1.....	132
2.2.5.3.3. Estrategia 2.....	132
2.2.5.3.4. Estrategia 3.....	133
2.2.5.3.5. Estrategia 4.....	134
2.2.5.4. Objetivos de control y controles. Anexo A de la ISO 27001 a implementarse en la Clínica Proinsalud s en el área de recursos humanos. ....	134
2.2.5.5. Política táctica de seguridad de la información en el área de administración financiera. ....	136
2.2.5.5.1. Objetivo.....	136
2.2.5.5.2. Estrategia 1.....	137
2.2.5.5.3. Estrategia 2.....	137
2.2.5.5.4. Estrategia 3.....	138
2.2.5.6. Objetivos de control y controles. Anexo A de la ISO 27001 a implementarse en la Clínica Proinsalud S.A. en el área de financiera gestión de activos.....	139
2.2.5.7. Política táctica de seguridad de la información en el área de sistemas. ....	141



2.2.5.7.1. Objetivo.....	141
2.2.5.7.2. Estrategia 1.....	141
2.2.5.7.3. Estrategia 2.....	142
2.2.5.7.4. Estrategia 3.....	143
2.2.5.8. Objetivos de control y controles. Anexo A de la ISO 27001 a implementarse en la Clínica Proinsalud S.A. en el área de sistemas.....	144
3. Conclusiones.....	149
4. Recomendaciones.....	151
Referencias bibliográficas.....	152

## Índice de Tablas

Tabla 1. Análisis de ataques en año 2021 .....	20
Tabla 2. Proceso de investigación .....	39
Tabla 3. Variables e hipótesis .....	41
Tabla 4. Rubros totales .....	42
Tabla 5. Costos totales de los investigadores de la investigación .....	42
Tabla 6. Rubros materiales .....	42
Tabla 7. Equipos tecnológicos.....	43
Tabla 8. Otros rubros.....	43
Tabla 9. Fecha de actividades.....	44
Tabla 10. Inventario del área de recursos humano .....	49
Tabla 11. Inventario del área de contabilidad.....	53
Tabla 12. Inventario del área de facturación .....	57
Tabla 13. Inventario del área de cartera .....	62
Tabla 14. Inventario del área de suministros.....	64
Tabla 15. Inventario del área de pagaduría.....	66
Tabla 16. Inventario del área de registro y control.....	68
Tabla 17. Inventario del área de sistemas.....	71
Tabla 18. Inventario del área de urgencias .....	75
Tabla 19. Inventario del área de hospitalización.....	80
Tabla 20. Inventario del área de Quirófano.....	84
Tabla 21. Inventario del área de UCI. ....	88
Tabla 22. Tipos de riesgos .....	91
Tabla 23. Criterios de valoración .....	93
Tabla 24. Dimensiones de seguridad.....	93
Tabla 25. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	95
Tabla 26. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	98
Tabla 27. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	101
Tabla 28. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	104
Tabla 29. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	106

Tabla 30. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	109
Tabla 31. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	112
Tabla 32. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	115
Tabla 33. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	117
Tabla 34. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	120
Tabla 35. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	122
Tabla 36. Indicadores de los tipos de impacto de las tablas analizadas con Magerit.....	125
Tabla 37. Acciones y responsables con su tiempo empleado en días.....	127
Tabla 38. Acciones y responsables con su tiempo empleado en días.....	128
Tabla 39. Acciones y responsables con su tiempo empleado en días.....	128
Tabla 40. Acciones y responsables con su tiempo empleado en días.....	129
Tabla 41. Acciones y responsables con su tiempo empleado en días.....	129
Tabla 42. Orientación de la dirección para la gestión de la seguridad de la información.....	130
Tabla 43. Organización de la seguridad de la información.....	131
Tabla 44. Acciones y responsables con su tiempo empleado en días.....	132
Tabla 45. Acciones y responsables con su tiempo empleado en días.....	133
Tabla 46. Acciones y responsables con su tiempo empleado en días.....	133
Tabla 47. Acciones y responsables con su tiempo empleado en días.....	134
Tabla 48. Seguridad de los recursos humanos. Antes de asumir el empleo.....	134
Tabla 49. Seguridad de los recursos humanos. Durante la ejecución del empleo.....	135
Tabla 50. Seguridad de los recursos humanos. Con la terminación y cambio de empleo.....	136
Tabla 51. Copias de respaldo.....	136
Tabla 52. Acciones y responsables con su tiempo empleado en días.....	137
Tabla 53. Acciones y responsables con su tiempo empleado en días.....	137
Tabla 54. Acciones y responsables con su tiempo empleado en días.....	138
Tabla 55. Responsabilidad por los activos.....	139
Tabla 56. Clasificación de la información.....	139
Tabla 57. Seguridad física y del entorno.....	140
Tabla 58. Copias de respaldo.....	141
Tabla 59. Acciones y responsables con su tiempo empleado en días.....	142
Tabla 60. Acciones y responsables con su tiempo empleado en días.....	142

Tabla 61. Acciones y responsables con su tiempo empleado en días.....	143
Tabla 62. Responsabilidad por los activos .....	144
Tabla 63. Clasificación de la información.....	144
Tabla 64. Control de acceso .....	145
Tabla 65. Gestión de acceso de usuarios .....	146
Tabla 66. Seguridad física y del entorno .....	146
Tabla 67. Equipos.....	147
Tabla 68. Copias de respaldo.....	148

## Índice de figuras

Figura 1. Modelo PHVA con la implementación de un SGSI.....	31
Figura 2. Ciclo de la metodología Magerit .....	32
Figura 3. Ubicación satelital de la Clínica Proinsalud .....	34
Figura 4. Organigrama de general de la Clínica Proinsalud.....	35
Figura 5. Organigrama del área de sistemas de la Clínica Proinsalud .....	36
Figura 6. Área de recursos humanos .....	48
Figura 7. Área de contabilidad .....	52
Figura 8. Figura del área de facturación.....	56
Figura 9. Área de cartera .....	61
Figura 10. Área de desarrollo departamento de sistemas.....	70
Figura 11. Área de urgencias.....	74
Figura 12. Área de hospitalización.....	79
Figura 13. Área de quirófano .....	83
Figura 14. Área de UCI.....	87
Figura 15. Zonas de riesgos con respecto al impacto y la probabilidad.....	92
Figura 16. Análisis de Amenazas y riesgos del área de pagaduría. ....	95
Figura 17. Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas .....	96
Figura 18 .Análisis de Amenazas y riesgos por origen industrial del área de pagaduría. ....	97
Figura 19. Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas .....	98
Figura 20. Análisis de amenazas y riesgos por errores y fallos no intencionados. Área de Contabilidad .....	100
Figura 21. Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas .....	102
Figura 22. Análisis de Amenazas y riesgos por ataques intencionados del área de Pagaduría ....	103
Figura 23. Mapas de calor de los impactos con respecto a la tabla de amenazas y riesgos por ataques intencionados del área de Pagaduría y sus respectivas amenazas .....	105
Figura 24. Análisis de Amenazas y riesgos por desastres naturales del área de facturación .....	106

Figura 25. Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas .....	107
Figura 26. Análisis de Amenazas y riesgos por origen industrial del área de facturación .....	108
Figura 27. Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas .....	109
Figura 28. Análisis de Amenazas y riesgos por errores y fallos no intencionados del área de facturación.....	111
Figura 29. Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas .....	112
Figura 30. Análisis de Amenazas y riesgos por ataques intencionados del área de Contabilidad	114
Figura 31. Mapas de calor de los impactos con respecto a la tabla de ataques intencionados y sus respectivas amenazas.....	116
Figura 32. Análisis de Amenazas y riesgos por desastre natural del área de Sistemas .....	117
Figura 33. Mapas de calor de los impactos con respecto a la tabla de desastre natural y sus respectivas amenazas.....	118
Figura 34. Análisis de Amenazas y riesgos por origen industrial del área de Sistemas.....	119
Figura 35. Mapas de calor de los impactos con respecto a la tabla de origen industrial y sus amenazas .....	120
Figura 36. Análisis de Amenazas y riesgos por errores y fallos no intencionados del área de Sistemas.....	121
Figura 37. Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas .....	123
Figura 38. Análisis de Amenazas y riesgos por ataques intencionados del área de Sistemas.....	124
Figura 39. Mapas de calor de los impactos con respecto a la tabla de ataques intencionados y sus respectivas amenazas.....	126

## **Introducción**

Hoy en día la información es uno de los activos más importantes y esenciales para cualquier organización ya que esta adquiere valor cuando es utilizada en forma adecuada, responsable y segura. La confidencialidad, la protección y la disponibilidad de la información de las empresas representan una tarea ardua al momento de garantizar su integridad y confidencialidad. Razón por la cual la información ha llegado a ser uno de los activos más valiosos en las empresas de hoy en día. La protección de la información en el ámbito de la salud es esencial para garantizar la privacidad y la confidencialidad de los pacientes.

En esta presente investigación se aborda la implementación de medidas de seguridad de la información basadas en la norma ISO/IEC 27001 en la Clínica Proinsalud S.A de la Ciudad de Pasto, con el fin de fortalecer la protección de los datos sensibles y prevenir posibles brechas de seguridad. La Clínica Proinsalud S.A desempeña un papel vital en el cuidado de la salud de la comunidad de la Ciudad de Pasto. Sin embargo, en un entorno digitalizado, la seguridad de la información se ha vuelto un aspecto crucial. La norma ISO/IEC 27001 ofrece un enfoque sistemático para el SGSI, brindando lineamientos para identificar riesgos y establecer controles efectivos.

La Clínica Proinsalud S.A preocupada por la seguridad de los mismos inicia el proyecto de implementación de la ISO /IEC27001 que busca salvaguardar la información de sus usuarios basados en la metodología MAGERIT y la norma ISO/IEC27001.

La metodología adoptada consistió en la evaluación de riesgos, la identificación de activos críticos de información, la definición de políticas de seguridad y la implementación de controles específicos. Se siguieron los principios y recomendaciones de las normas ISO/IEC 27001, adaptadas a las necesidades y contextos de la Clínica Proinsalud S.A.

Con lo anterior permitirá que la clínica Proinsalud S.A cuente con una implementación de medidas de seguridad basadas en ISO/IEC 27001 dicha implementación ha tenido un impacto positivo. Se establecieron Políticas Institucionales y Políticas de Seguridad para el acceso a los

registros por parte de los funcionarios de la institución, la protección de contraseñas y la gestión de respaldos de información. La implementación de la norma ISO/IEC 27001 en la Clínica Proinsalud ha demostrado ser un paso necesario en la protección de la información y la prevención de amenazas cibernéticas. Sin embargo, se han identificado desafíos como la capacitación continua del personal y la necesidad de adaptarse a las evoluciones tecnológicas y de seguridad. La implementación de la norma ISO/IEC 27001 ha fortalecido la seguridad de la información en la Clínica Proinsalud, mejorando la confidencialidad y la integridad de los datos. Esta iniciativa no solo protege a los pacientes, sino que también contribuye a la confianza y la reputación de la Clínica en la Ciudad de Pasto. La adaptación constante y la mejora continua son esenciales para mantener una seguridad sólida en un entorno en constante cambio.



## **1. Elementos del proceso investigativo**

### **1.1. Antecedentes y estado del conocimiento**

Como soporte al proceso investigativo se revisan algunos antecedentes que se han implementado a nivel local, nacional e internacional y se relacionan a continuación.

#### ***1.1.1. Antecedentes internacionales***

El proyecto elaboración de plan de implementación de la ISO/IEC 27001:2013 en la empresa Recycle S.A ubicada en varios países de Europa de Garrido (2018) muestra el proceso realizado para elaboración del Plan de Implementación de la ISO/IEC 27001:2013 en una multinacional dedicada al reciclaje de residuos industriales, aunque consientes con la necesidad de asegurar adecuadamente sus sistemas de información, no contaba hasta el momento con un SGSI. El proyecto recoge las tareas realizadas para sentar las bases para la implantación del SGSI, y genera una serie de entregables que formarán parte del sistema de gestión documental del SGSI. Este estudio muestra la necesidad de asegurar adecuadamente sus sistemas de información por lo cual sirve como guía a seguir ya que en el presente estudio también se debe salvaguardar la información de una empresa. Este proyecto difiere del planteado ya que se desarrolló en una empresa de reciclaje mientras que la propuesta se implementará en una clínica.

Este proyecto se asemeja al propuesto en el uso de la Norma ISO/IEC 27001 en salvaguarda de la información de la empresa y los beneficios que esta genera en la seguridad de los datos.

El proyecto 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 Perú, realizado por Talavera (2015) en el Instituto Nacional Materno Perinatal, indica el proceso realizado mediante la implementación de la norma ISO/IEC 27001:2013 en una entidad estatal de salud, la cual maneja información sobre sus pacientes que permite mantener y actualizar un historial de atenciones que es contenido en la historia clínica en donde contiene información personal que identifica al paciente y esta deberá ser protegida para poder garantizar la correcta atención de los pacientes, para evitar la fuga de

información que puede ser manipulada de manera maliciosa. El proyecto comprenderá la elaboración de la documentación necesaria para establecer controles que permitan mitigar los riesgos identificados, también se realizó un análisis de los riesgos presentes en la situación actual y que constituyan una posible amenaza directa o indirecta para los activos de la información. Con respecto al proyecto propuesto, esta investigación tiene una similitud muy importante en el uso de la norma ISO/IEC 27001:2013, en donde es muy claro lo que se va a realizar en el estudio de la Clínica Proinsalud hacia un análisis y protección de los datos de los pacientes.

### ***1.1.2. Antecedentes nacionales***

El proyecto plan de implementación del SGSI basado en la norma ISO 27001:2013 de la empresa Textilera S.A en Girardota, ubicada en la Ciudad de Medellín de la autora Maya (2016), detalla los objetivos, la importancia, la expectativa del Sistema de Gestión de la Seguridad de la Información y la metodología relacionada con la planeación, descripción, concepto e identificación y creación del modelo de seguridad de la información para la empresa Textilera S.A., basado en la norma ISO 27001:2013. “El principal objetivo es sentar las bases del proceso de mejora continua y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales” (Maya, 2016, p. 4). El proyecto plantea el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información). Este proyecto se asemeja al proyecto en curso debido a que fundamenta los procesos basados en la norma para la implementación de la ISO/IEC 27001, se diferencia debido a que los procesos de una empresa de textiles manejan diferentes actividades que una entidad de salud partiendo desde la interacción con sus usuarios Este proyecto le aporta a la investigación ya que permite asimilar los conocimientos de roles y las normas a aplicar una vez se despliegue la ISO/IEC 27001.

El proyecto diseño de un sistema de gestión de seguridad de información bajo la norma iso27001:2013 el cual fue realizado en la ciudad de Timana ubicada en el departamento del Huila del autor Reyes (2019). El objeto de este trabajo es “realizar el inventario de los diferentes activos informáticos, priorizar los datos, realizar el estudio de riesgos de la información, establecer políticas y controles que garanticen la protección de información mediante el modelo ISO/IEC 27001” (Reyes, 2019, p. 16) minimizando riesgos identificados al interior de la

empresa. El presente proyecto sirve como un documento ilustrativo ya que se realiza el estudio dentro de una clínica para tener en cuenta las normativas que se detectaron en dicho estudio como también identificar, compilar los activos y priorizar los datos.

El proyecto análisis de riesgos de seguridad de la información basado en la metodología Magerit para el área de datacenter de una entidad promotora de salud realizado en una EPS de la capital de Colombia de los autores Guamanga y Perilla (2015). El propósito principal es:

Asegurar el análisis de riesgos permitió determinar a que está expuesta la EPS y estimar el nivel de impacto en caso de materializarse. Este análisis también permitió implementar una metodología para el levantamiento de activos, identificación de amenazas y efectividad de controles implementados universidad piloto de Colombia. (Guamanga y Perilla, 2015, p. 49)

Los antecedentes anteriores sirven de referente para identificar la importancia y cómo funciona la metodología Magerit en una I.P.S. Se resalta que el presente proyecto será basado en una IPS. Esta genera historias clínicas de las atenciones de sus pacientes y velar por la seguridad y confidencialidad de esta información.

## **1.2. Título**

Seguridad de la información usando la norma ISO/IEC 27001 para la Clínica Proinsalud S.A de la Ciudad de San Juan de Pasto.

## **1.3. Problema de investigación**

### ***1.3.1. Descripción del problema***

Hoy en día la seguridad de los datos está en un crecimiento exponencial, dado a que los ataques informáticos se presentan de cualquier forma y en cualquier lugar, ya sea desde el quebramiento de la seguridad y protección de las cuentas personales hasta el hurto de información entre las entidades organizacionales.

La compañía de seguridad informática ESET presenta anualmente un análisis de ataques realizados a empresas de distintos países que tiene como convenio a la compañía de seguridad. Según ESET Security Report (2021) el estudio en Latinoamérica 2021 es el resultado de consultas y encuestas realizadas a cerca de mil ejecutivos y representantes de empresas de 17 países de la región. A continuación, se destaca los principales hallazgos.

**Tabla 1**

*Análisis de ataques en año 2021*

<b>Inseguridad de empresas</b>	
Códigos maliciosos	El 64% de las empresas han temido por códigos maliciosos
Robo de información	El 60% de las empresas han presentado robo de información personal
Acceso indebido a los sistemas	El 56% han presentado acceso indebido a la información de las empresas
Privacidad de la información	El 45% de la privacidad de información ha sido manipulada por intrusos
Falta de disponibilidad de servicios críticos	El 27% de las empresas han sido afectadas por la falta de experiencia en servicios críticos como la seguridad de la información
Uso inapropiado de infraestructura	El 20% de las empresas han tenido uso inapropiado en su infraestructura

*Nota.* datos correspondientes al año 2021. Fuente: ESET Security Report (2021)

La Clínica Proinsalud (2022) es una entidad privada que presta sus servicios de salud a la población del magisterio de Nariño, hoy en día cuenta con 680 trabajadores entre directivos, administrativos y asistenciales, quienes hacen uso de forma regular de los medios de información para consultar datos. Para ello, usa software, redes, sistemas informáticos. Cuenta con unas dependencias del área de sistemas que son infraestructura, desarrollo y soporte, las cuales brindan apoyo a cualquier requerimiento de su organización tecnológica las 24 horas del día.

La Clínica Proinsalud (2022) realiza sus procesos de funcionamiento apoyados en tecnologías de información, esto le permite un manejo de datos e información de manera más eficiente,

Cada una de las dependencias del área de sistemas posee sus funciones y asistencias en la entidad, con el fin de mantener un óptimo desempeño en los servicios tecnológicos, así mismo cuenta con sistemas, procedimientos, técnicas y estándares que ofrezcan y salvaguarden los activos de información en donde les brinde integridad, confidencialidad y disponibilidad en sus soluciones.

Cabe mencionar que la empresa posee un canal de internet de 100 megas en ancho de banda dedicado para poder dar desarrollo a sus actividades rutinarias. Como son las conexiones a sus sedes en los diferentes municipios del departamento de Nariño.

En la actualidad la Clínica Proinsalud presenta falencias en los servidores se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas, no se cuenta con planos de la red de comunicaciones, algunos equipos de cómputo no cuentan con sistemas de antivirus actualizado, debido al alto flujo en la oficina de nómina y facturación, la alimentación de la información en el sistema en ocasiones la diligencia personal de contratos de aprendizaje lo cual conlleva que una mala manipulación de la información podría acarrear problemas legales, existe un Cortafuegos Cisco mx86, este no cuenta con reglas implementadas para la autorización o denegación de conexiones o transmisión de datos.

Lo anterior ha ocasionado problemas como el ataque sufrido en el mes de agosto del año 2018 debido a esto se dejó de brindar servicio de aplicativos por lapso de 14 horas. El no licenciamiento de todos los equipos con el antivirus hace que se dejen equipos vulnerables los cuales han sido atacados. Los equipos presentan lentitud en el manejo. Lo cual conlleva a una mala prestación en el servicio frente a los usuarios.

### ***1.3.2. Formulación del problema***

¿Cómo asegurar los activos de información en la Clínica Proinsalud que garanticen su seguridad

en el manejo de la información?

## **1.4. Objetivos**

### ***1.4.1. Objetivo general***

Asegurar los activos de información en la Clínica Proinsalud mediante la implementación de un Sistema de Gestión de Seguridad de la Información SGSI basados en el estándar NTC-ISO/IEC 27001.

### ***1.4.2. Objetivos específicos***

- Identificar los activos informáticos, procesos y servicios soportados por la oficina de Tecnologías de Información de la Clínica Proinsalud.
- Analizar y evaluar amenazas, riesgos y vulnerabilidades desde la metodología Magerit.
- Diseñar el Sistema de Gestión de Seguridad de la Información Basado en la norma ISO/IEC 27001.
- Evaluar el Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) en la Clínica Proinsalud de la ciudad de San Juan de Pasto.

## **1.5. Justificación**

Los datos e información de las empresas son la mayor preocupación en la actualidad esto se debe a que se encuentran sujetos a pérdida de información. El presente proyecto es presentado conociendo las falencias y necesidades que se observan en la seguridad sobre los insumos informáticos de la Clínica Proinsalud y así identificar vulnerabilidades guiados por el estándar ISO/IEC 27001 con la cual se logrará implementar un sistema que permita definir políticas de seguridad de la información y así garantizar la integridad, la disponibilidad y confidencialidad de

la información.

De acuerdo a lo anterior se define que los activos de la información tanto físicos como lógicos deben ser protegidos adecuadamente mediante la implementación de los procesos, protocolos y políticas.

La Clínica Proinsalud tendrá como nuevos objetivos salvaguardar la información aplicando las recomendaciones que se definan como insumo en el cumplimiento de las políticas basadas en el estándar ISO/IEC 27001 empleando las nuevas prácticas de la seguridad de la información sugeridas en dicho modelo para poder generar conciencia al interior del establecimiento de salud sobre los riesgos al ser manipulada de una manera errónea.

Esta investigación se basa en la norma ISO/IEC 27001 junto con la metodología Magerit, que permite identificar riesgos, vulnerabilidades y amenazas para luego gestionarlos y minimizar su impacto, los cuales pretende garantizar que la información de los usuarios ya sea auditiva, visual, tangible y electrónica este excepta de que sea destruida, usada inadecuadamente, perdida y corrupta, como también prevenir un incidente de seguridad de la información que de una u otra manera tiene impactos negativos hacia la Clínica Proinsalud estos incidentes se presentan cuando no está disponible la información o incluso cuando la integridad de esta sea corrupta o incompleta y por último la confidencialidad de los datos sea expuesta a personas que no deberían tener acceso y que esta pueda llegar a ser utilizada de manera inadecuada.

Este proyecto resalta la importancia de tener un estándar de Sistema de Gestión de la Seguridad de la Información, por lo tanto, gracias a este sistema la Clínica Proinsalud S.A puede evitar problemas legales de pérdida o manipulación de historias, permitiendo que la empresa vele por la integridad de su información, resaltando también que los usuarios y funcionarios de la Clínica se verán beneficiados por la confidencialidad de su información.

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad,

conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

## **1.6. Marcos de referencia**

### ***1.6.1. Marco teórico - conceptual***

El proyecto se soporta en conceptos y teorías de las normas las cuales desde el pensamiento de los autores y basados en el conocimiento científico son fundamentales para el desarrollo de la investigación.

Con la inclusión de nuevas tecnologías y la masificación de la información viajando por diferentes canales, se hace evidente que el perfil de riesgos para las personas y empresas también cambia, incrementando el nivel de riesgos de la información en sus tres aspectos fundamentales, disponibilidad, integridad y confidencialidad.

En la actualidad las empresas tienen áreas especializadas en la mitigación de los riesgos, elaborando estrategias para la gestión de dichos riesgos.

Este proyecto se apoyó en avances de los planes de gestión de riesgos ya aplicados en algunas empresas siguiendo como directriz las normas ISO/IEC 27001 las cuales suministran directrices para la gestión de riesgos. Aunque las normas ISO son el estándar internacional, no se dejaron de lado otras metodologías de análisis de riesgos, como es el caso de Magerit, cabe resaltar que estas metodologías usan elementos transversales en el análisis y gestión de riesgos, los cuales se describen a continuación.

**Activo.** “Son aquellos recursos (Hardware y Software) con los que cuenta una empresa. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información” (Orozco, 2013, p. 2). En el presente caso de estudio los activos de la clínica Proinsalud en la parte de hardware serían los servidores, computadores, impresoras, entre otros, y por el lado de software encontraríamos el aplicativo SIMA y SIIGO los cuales son los encargados



de crear guardar y salvaguardar toda la documentación de la Clínica.

Los Activos Informáticos son una parte fundamental de los negocios y garantizan su continuidad o competitividad. Se debe tener en cuenta que es crucial protegerlos para mantener seguras las claves y la información de los distintos proyectos empresariales o personales. Se defiende ante posibles daños y alteraciones en los datos. (Perito Judicial Group, 2021, párr. 5-6)

Bajo esta gestión se persigue dar cumplimiento a cuatro puntos claves acerca de los activos de información:

**Inventario de activos.** “Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos de información importantes de la organización” (Ministerio de Tecnologías de la Información y Comunicaciones, 2016, p. 6).

**Propiedad de los activos.** “Todos los activos de información deben ser “propiedad” de una parte designada de la Organización. En este sentido el propietario del activo definirá y garantizará los controles para la adecuada protección del activo” (Ministerio de Tecnologías de la Información y Comunicaciones, 2016, p. 6).

**Directrices de clasificación de activos.** “La información debe clasificarse en términos de su valor, de los requisitos legales, de su sensibilidad y la importancia para la organización” (Eduba, 2022, párr. 12).

**Tratamiento de activos.** A la información debe dársele un manejo adecuado. Se debe establecer con base en las mejores prácticas de seguridad, que controles mínimos deben ser aplicados a los activos para su adecuado manejo, dependiendo del nivel de clasificación en el cual hayan sido catalogados. (Eduba, 2022, párr. 13)

Aunque no es un requisito de la norma ISO 27001, es deseable determinar la importancia de los activos de información, lo que se puede hacer a través de tres variables: aplicación de la

Confidencialidad, Integridad y Disponibilidad, también conocida como “CID”:

**Confidencialidad.** Es información importante y confidencial, como su nombre lo indica, en la continuidad de la empresa. Si se divulga, podría tener graves consecuencias para la organización, poner en peligro su reputación y generar amenazas importantes (Grupo Ático, 2022).

**Integridad.** La información propietaria debe ser completa y legal, por lo que no debe ser alterada por ningún motivo ni manipulada por ningún tercero ya que esto provocará errores en el sistema (Grupo Ático, 2022).

**Disponibilidad.** La capacidad de acceder a la información según sea necesario. Si el activo no está disponible, puede hacer que la empresa detenga la producción (Grupo Ático, 2022).

**Vulnerabilidad.** Debilidad inherente al activo, su presencia no causa daño por sí misma, ya que necesita presentar una amenaza que la comprometa en el presente caso de estudios serían las ausencias de políticas de seguridad lo cual conlleva a. un mal manejo y a una pérdida de información. Por otro lado, la falta de control de acceso al Datacenter indica la falencia que se tiene en la presencia de políticas de seguridad (Grupo Ático, 2022).

**Tipos de vulnerabilidades.** Hay dos formas de detectar vulnerabilidades existentes, como se indica en la publicación titulada *puerta trasera a la vulnerabilidad* de Campus Ciber Seguridad (2021), se destacan dos formas, el primero surge del estudio de los ciberdelincuentes tratando de aprovecharlo al máximo hasta que se despliega la vulnerabilidad y se desarrollan los parches correspondientes. El segundo método es publicar en grupos de piratería como The Shadow Brokers (Los Intermediarios en la sombra). Es cierto que un agujero de seguridad tiene la capacidad de destruir todo un sistema en pocos minutos, por lo que para intentar prevenirlo es necesario realizar pruebas de penetración para reducir los riesgos.

**Error en la gestión de recursos.** La Clínica Proinsalud S.A está expuesta y se debe tener extremo cuidado en este tipo de errores que corresponden a una aplicación que permite el uso excesivo de los recursos, afectando su disponibilidad.

**Amenaza.** Circunstancia o evento que tiene el potencial de causar daño a un activo. “16,7 millones de consumidores experimentaron robo de identidad en 2017 (JavelinStrategy), pero queda mucho por mejorar ya que, según un estudio de 2018 de Juniper Research, los ciberdelincuentes se apropiarán de cerca de 33 mil millones de registros en 2023” (Pérez, 2019, párr. 3).

El estudio de Instituto Ponemon para IBM sobre el coste de un incumplimiento de datos realizado en 2018 revela que el coste promedio de la violación de datos a empresas de todo el mundo es de 3.86 millones de dólares y el tiempo promedio que se tarda en identificar una violación de datos es de 196 días. (Pérez, 2019, párr. 4)

El primer paso para evitar las consecuencias de estos ataques es conocer los tipos de amenazas informáticas que existen. Son los siguientes:

**Spam.** Es correo basura digital comunicaciones no solicitadas que se envían de forma masiva por Internet o mediante otros sistemas de mensajería electrónica. Más allá de la molestia y el tiempo que se pierde a causa de los mensajes no deseados, el spam puede causar daños significativos, infectando las computadoras de los usuarios con software malicioso capaz de dañar los sistemas y robar información personal. También puede consumir recursos de la red (Angelino, 2022).

**Farming.** Consiste en disfrazar sitios web falsos como si fueran auténticos para obtener así la información que se introduzca en ellos (Kaspersky, 2023).

**Phishing.** “El phishing es una técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial” (Avast, 2022, párr. 1). Ya sea que se realice por correo electrónico, redes sociales, SMS o cualquier otro sistema, todos los ataques de phishing siguen los mismos principios básicos. Los atacantes envían comunicaciones dirigidas para convencer a las víctimas de que hagan clic en enlaces, descarguen archivos adjuntos, envíen la información solicitada o incluso realicen pagos. La naturaleza del engaño se deja a la imaginación y habilidad del atacante. Con la llegada de las

redes sociales, los estafadores tienen acceso a más información personal sobre sus objetivos que nunca. Armados con estos datos, pueden ajustar los ataques en función de las necesidades, los deseos y las circunstancias de la vida del objetivo, creando una pantalla más convincente. En estos casos, las redes sociales permiten una ingeniería social más robusta.

**Ransomware.** Es una de las amenazas de ciberseguridad de más rápido crecimiento. Una vez que infecta el sistema y la computadora, bloquea los archivos y requiere un pago para abrirlos; También puede amenazar con filtrar datos y, por lo tanto, aumentar la presión (We Live Security, 2021). Se debe tener en cuenta los dos tipos de ransomware:

**Bloquear ransomware.** Este tipo de ransomware está diseñado para bloquear funciones básicas de la computadora (We Live Security, 2021).

**Cifrado de ransomware.** Este tipo de ransomware está diseñado para cifrar los archivos más importantes de la víctima, como documentos, fotos y videos (We Live Security, 2021).

**Riesgo.** “Los riesgos informáticos son aquellas amenazas o vulnerabilidades a las cuales está expuesta la información almacenada en un computador o un dispositivo con la capacidad de almacenar información” (Rent Advisor, 2022, párr. 1).

Las empresas y los establecimientos comerciales son las víctimas más frecuentes del robo de la información, que puede traducirse en graves delitos como la suplantación de identidad, desfalcos y hurtos al bien, ya que los riesgos informáticos a los cuales están expuestos este tipo de establecimientos es mucho más elevado que los hogares y los dispositivos tecnológicos que allí se encuentran (Gallardo, 2016). Existen varios tipos de riesgos informáticos a los cuales puede estar expuesta tu compañía o tu negocio:

“Relación: Por personas cercanas a la compañía. Acceso: Claves de seguridad débiles. Utilidad: Mal uso de la tecnología. Infraestructura: Hurtos de activos como aparatos tecnológicos. Seguridad integral: Sistemas de seguridad privada y CCTV (Circuitos cerrados de televisión)” (Rent Advisor, 2022, párr. 5).

Estos son alguno de los riesgos más comunes dentro de la Clínica Proinsalud y muchas veces suele ser por desconocimiento de los funcionarios que utilizan las plataformas informáticas.

**Mitigación.** Reducción de riesgos con baja probabilidad de que suceda un imprevisto.

Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. (Soluciones Pilar, 2022, párr. 2)

Los riesgos de seguridad de información deben ser considerados en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas, etcétera y los clientes deben ser identificados para lograr una imagen global y completa de estos riesgos dentro de la Clínica Proinsalud S.A.

“Cada organización tiene una misión. En esta era digital, las organizaciones que utilizan sistemas tecnológicos para automatizar sus procesos o información deben de ser conscientes de que la administración del riesgo informático juega un rol crítico” (Gadeas et al., 2010, p. 15).

**1.6.1.1. ISO/IEC 27001.** La norma ISO/IEC 27001 es importante y fundamental en la implementación de una empresa ya que por medio de esta se puede salvaguardar la información según Guzmán (2015) la norma principal de la serie ISO/EIC 27000 se puede aplicar a cualquier tipo de organización, sin importar su tamaño o su actividad comercial. La Norma contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información, documentado dentro del contexto global de los riesgos de negocio de la organización.

Esta norma habla y vela por la importancia de la información dentro de las instituciones ya que por medio de esta se realiza la toma de decisiones empresariales.

**1.6.1.2. Modelo PHVA.** Es un modelo que se conforma por cuatro pasos que son:

**Planificar.** En la etapa de planificación se establecen objetivos y se identifican los procesos necesarios para lograr unos determinados resultados de acuerdo a las políticas de la organización. En esta etapa se determinan también los parámetros de medición que se van a utilizar para controlar y seguir el proceso. (Argos, 2021, párr. 6)

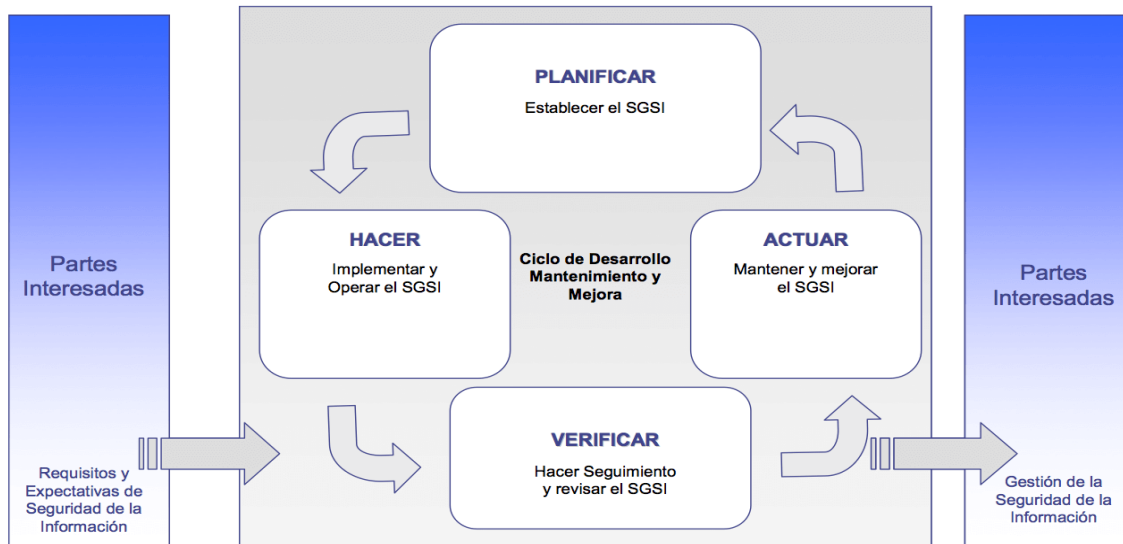
**Hacer.** Consiste en la implementación de los cambios o acciones necesarias para lograr las mejoras planteadas. Con el objeto de ganar en eficacia y poder corregir fácilmente posibles errores en la ejecución, normalmente se desarrolla un plan piloto a modo de prueba o testeo. (Argos, 2021, párr. 7)

**Verificar.** “Una vez se ha puesto en marcha el plan de mejoras, se establece un periodo de prueba para medir y valorar la efectividad de los cambios. Se trata de una fase de regulación y ajuste” (Argos, 2021, párr. 8).

**Actuar.** Realizadas las mediciones, en el caso de que los resultados no se ajusten a las expectativas y objetivos predefinidos, se realizan las correcciones y modificaciones necesarias. Por otro lado, se toman las decisiones y acciones pertinentes para mejorar continuamente el desarrollo de los procesos. (Argos, 2021, párr. 9)

**Figura 1**

*Modelo PHVA con la implementación de un SGSI*



*Nota.* En el diagrama se muestra el ciclo del modelo PHVA mediante el cual se establecerá, implementará, revisará y mejorará un SGSI en una empresa.

**1.6.1.3. Metodología Magerit.** Es una metodología para el análisis y la gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica (CSAE). Esta metodología es abierta al público y cualquier persona puede hacer uso de la misma sin necesidad de solicitar autorización del Ministerio de Administraciones Públicas de España (Rodríguez y Peralta, 2013).

Magerit es una metodología de carácter público que puede ser utilizada libremente y no requiere autorización previa. Interesa principalmente a las entidades en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) para satisfacer el principio de la gestión de la seguridad basada en riesgos, así como el requisito de análisis y gestión de riesgos, considerando la dependencia de las tecnologías de la información para cumplir misiones, prestar servicios y alcanzar los objetivos de la organización (Rodríguez y Peralta, 2013).

**Figura 2**

*Ciclo de la metodología Magerit*



*Nota.* En el diagrama muestra el ciclo de la metodología Magerit usa para observar a que están expuestos la información Magerit 3.0: método de análisis de riesgos. Fuente: Moncayo et al. (2014).

### **1.6.2. Marco legal**

De acuerdo a las leyes colombianas los Institutos Prestadores de Salud (IPS) están obligadas a cumplir con ciertas condiciones en el manejo de su información y brindar los mecanismos apropiados para garantizar la integridad, disponibilidad y confidencialidad de la información de sus beneficiarios o afiliados. La Resolución 1995 (1999), del Ministerio de Salud establece las normas para el manejo de la historia clínica. Dentro de esta norma se pueden encontrar varios artículos que de manera general imparten directrices a todas las IPS de Colombia, entre estos los más importantes son:

**Artículo 16.** Trata de la seguridad que debe tener la IPS en el lugar donde almacene las historias clínicas, además de velar por la conservación de la misma. También ordena que el lugar en donde se almacenen solo podrá ser accedido por personal autorizado con el fin de garantizar la integridad de las historias clínicas (Resolución 1995 de 1999).



**Artículo 17.** Define las condiciones físicas en las cuales se deben almacenar las historias clínicas, siguiendo los parámetros establece el Archivo General de la Nación (Resolución 1995 de 1999).

**Artículo 18.** Enuncia los medios técnicos que se usan para el registro y conservación de las historias clínicas. Este artículo deja de lado los documentos físicos y se enfoca en los sistemas automatizados que procesan la información que se almacena en la historia clínica y todo lo que intervenga en este proceso, incluyendo personas y equipos. Para lo anterior se imparten ciertas condiciones: equipos, sistemas y sus respectivos soportes deben tener mecanismos de seguridad, con el fin de que no se alteren sin autorización las historias clínicas una vez sean guardadas. La historia clínica se debe proteger por mecanismos de seguridad que impidan que se elimine o destruya de forma accidental o intencionada. Los sistemas deben identificar al personal responsable de cargar datos a las historias clínicas, por medio de códigos o identificadores únicos, de manera que se conozca con certeza la persona que realizó algún cambio, la fecha y hora del mismo (Resolución 1995 de 1999).

Las IPS por estar siendo operadas bajo la responsabilidad de personas naturales y por ser un servicio al público deben estar reglamentadas por las siguientes normas:

La Ley 65-00 de 2000 sobre Derecho de Autor y su reglamento de aplicación, así como la Ley 424-06 de 2006, protegen los derechos de los autores, al igual que los derechos afines de los artistas intérpretes o ejecutantes.

La Ley de Protección de Datos Personales o Ley 1581 de 2012, reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

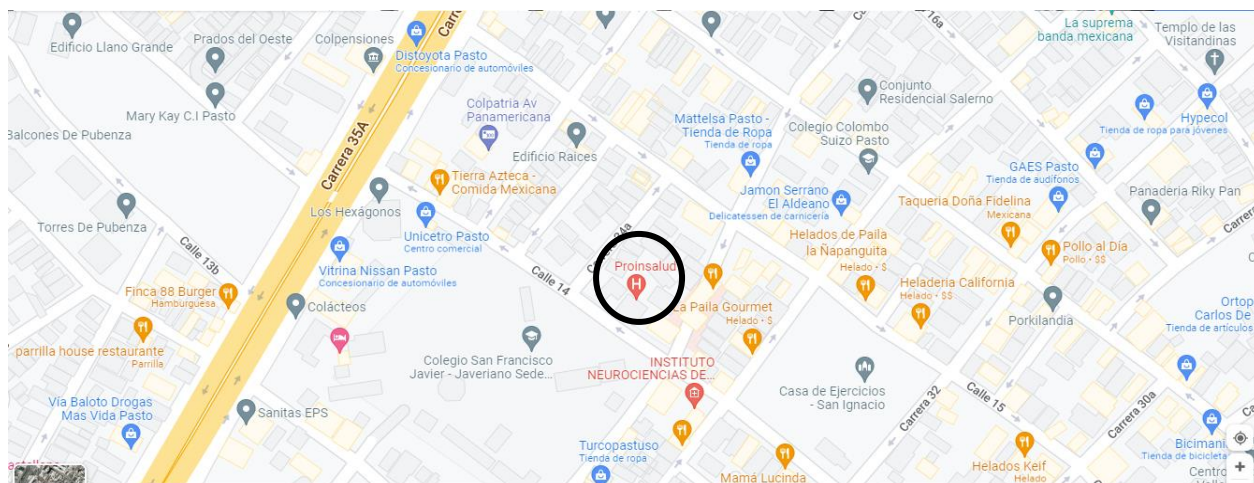
### 1.6.3. Marco contextual

Este trabajo se realizará en la Clínica Proinsalud (2021) la cual es una institución de salud, bajo la modalidad de servicios de salud con sede en Pasto (Nariño). La clínica presta los servicios en salud de urgencias, hospitalización, consulta externa, imagenología, quimioterapia, quirófanos, laboratorio clínico, UCIA, UCIN y consulta especializada.

La Clínica Proinsalud (2021) cuenta con código de habilitación aprobado por el Instituto Departamental de Salud de Nariño, según licencia de habilitación 520010066901, la clínica se encuentra ubicada en la calle 14 # 33 – 24 del Barrio San Ignacio del municipio de Pasto, Departamento de Nariño.

### Figura 3

Ubicación satelital de la Clínica Proinsalud

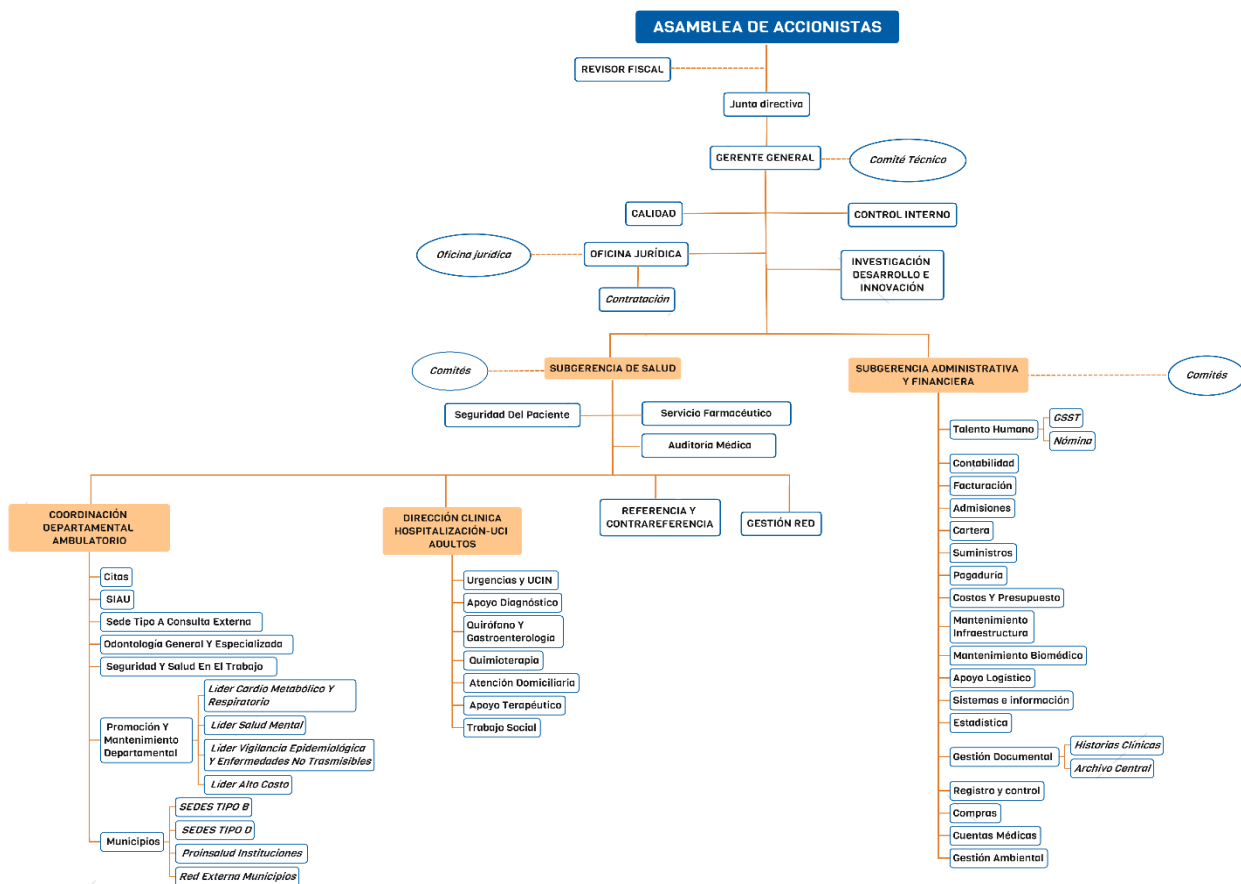


Fuente: Google Maps (2023)

La función principal de Clínica Proinsalud (2021), es prestar servicios de salud con personal capacitado y tecnificado con proyección laboral y empresarial. La Clínica Proinsalud (2021) es pionera en el sur de Colombia en la prestación de servicios de salud a los docentes del magisterio de Nariño, capacitando y desarrollando al personal humano, para fomenta la fuerza laboral de sus más de 600 empleados en la jornada de la mañana, tarde y noche.

En el organigrama (Ver figura 4) se muestra la representación gráfica de la Clínica Proinsalud, a través del diagrama jerárquico y funcional se observa que actualmente toda la estructura de la institución, depende de la Asamblea de Accionistas; quienes son los únicos responsables en la toma de decisiones en cumplimiento de las metas propuestas y poder así lograr los objetivos trazados.

**Figura 4**  
Organigrama de general de la Clínica Proinsalud



*Nota.* Estructura organizacional de la clínica Proinsalud la cual muestra como está conformada por sus respectivas áreas. Fuente: Clínica Proinsalud (2021)

Área de Sistemas se encuentra conformado por un grupo de ingenieros de sistemas y tecnólogos que se agrupan en diferentes tareas afines como son desarrollo, soporte técnico, tecnologías de la Información, redes y telecomunicaciones. En el área de Desarrollo de Software se realizan las actividades pertinentes al análisis, diseño codificación e implementación y

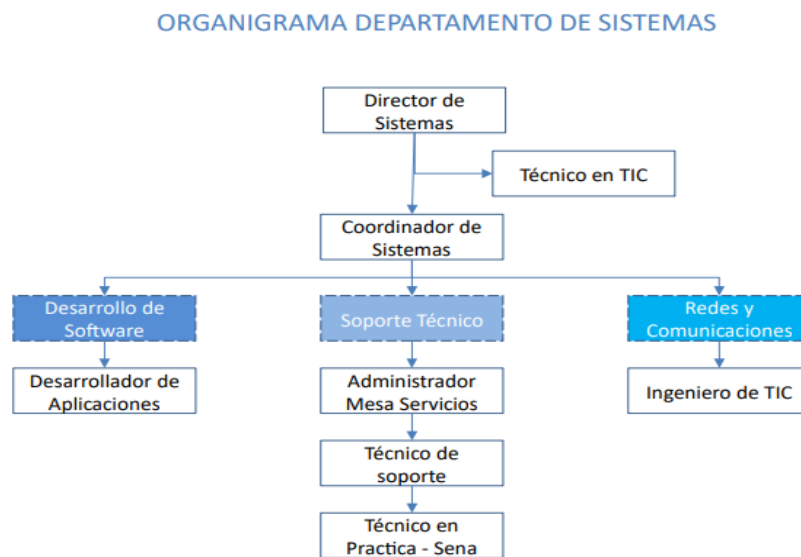
mantenimiento de aplicaciones en producción las cuales brindan una estabilidad para la gestión de la información en las diferentes áreas de la Clínica Proinsalud (2021).

El área de Soporte Técnico se encarga por velar la integridad de los equipos de cómputo y velar por que estos se encuentren en perfecto funcionamiento para garantizar agilidad de sus procesos, buscando una buena prestación de los servicios de las diferentes áreas de la Clínica frente a sus Usuarios (Clínica Proinsalud, 2021). Otra de sus áreas es la de Tecnología de la Información la cual se enfoca a la integración, implantación, operación y administración de sistemas informáticos empleando como herramienta principal las tecnologías computacionales, así como también operar y administrar las comunicaciones y telecomunicaciones de la Clínica Proinsalud (2021).

Por último, el área de Redes y Telecomunicaciones los cuales son los encargados de velar por la conectividad dentro de la institución de todos los equipos de cómputo e instalación de cámaras de seguridad (Clínica Proinsalud, 2021). Se evidencia la distribución del área de sistemas en el siguiente organigrama del área.

**Figura 5**

*Organigrama del área de sistemas de la Clínica Proinsalud*



*Nota.* Estructura organizacional del área de sistemas. Fuente: Clínica Proinsalud (2021)

## **1.7. Metodología**

### ***1.7.1. Paradigma de investigación***

La presente investigación se ubica dentro del paradigma cuantitativo como también cualitativo. Según Monje (2011) el enfoque cuantitativo plantea la obtención de datos, verificación de hipótesis y teorías como también por el uso de técnicas de conteo, medición y razonamiento abstracto. De la misma manera se enmarcará en un paradigma cualitativo por que se van a desarrollar diagnósticos, tipos de análisis. Según Landeau (2007) la finalidad del paradigma cualitativo es encontrar una teoría con la que se pueda probar, con razones convincentes, la efectividad de los datos.

### ***1.7.2. Enfoque de investigación***

La investigación sigue el enfoque empírico analítico ya que se busca conocer de manera objetiva, externa y efectiva las causas, efectos y síntomas de problemas para analizarlos predecirlos y por último contrarrestarlos. Cifuentes (2011) afirma que el enfoque empírico analítico se inclina por la medición, la muestra y la representatividad de los datos, los cuales tiene que tener validez.

### ***1.7.3. Tipo de investigación***

La investigación es descriptiva ya que según Tamayo y Tamayo (2004) esta investigación comprende la descripción, registro, análisis como también las características de los datos y la descripción precisa, lo cual se realizará en las diferentes etapas del proceso investigativo.

### ***1.7.4. La línea de investigación***

Se ubica dentro de Ingeniería, Informática y computación.

### ***1.7.5. Áreas Temáticas de investigación***

La investigación se ubica en el área de Tecnologías de Información y comunicación (TIC).

### ***1.7.6. Población y muestra***

La población a estudiar son las diferentes áreas de la Clínica Proinsalud las cuales son el área de recursos humanos, pagaduría, jurídica, contabilidad, cartera, auditoria y, referencia y contra referencia.

No obstante, para efectos de la investigación se tomará la muestra relacionada con el área de sistemas la cual cuenta desarrollo, soporte técnico, tecnologías de la información y, redes y telecomunicaciones.

**Tabla 2***Proceso de investigación*

<b>Objetivos específicos</b>	<b>Fuente</b>	<b>Técnica de recolección</b>	<b>Instrumento</b>	<b>Técnica de Procesamiento</b>	<b>Resultado</b>
Identificar los activos informáticos, procesos y servicios soportados por la oficina de Tecnologías de Información de la Clínica Proinsalud	Inventario de equipos de cómputo y funcionarios de la clínica.	Revisión documental y observación directa.	Bitácora de campo	Análisis documental	Documento con tabla de activos informáticos del área.
Analizar y evaluar amenazas, riesgos y vulnerabilidades del área desde la metodología Magerit.	Área de Sistemas Proinsalud	Observación y encuesta	Cuestionario y lista de chequeo	Análisis documental	Documento con cuadro de riesgos, amenazas y vulnerabilidades del área
Diseñar el Sistema de Gestión de	Norma ISO/IEC 27001	Revisión documental	Ficha de revisión documental	Análisis documental	Documento con Diseño del Sistema

Objetivos específicos	Fuente	Técnica de recolección	Instrumento	Técnica de Procesamiento	Resultado
Seguridad de la Información Basado en la norma ISO/IEC 27001.					de Gestión de Seguridad de la Información en Proinsalud.
Evaluar el Diseño del Sistema de Gestión de Seguridad de la Información (SGSI). En la Clínica Proinsalud de la ciudad de San Juan de Pasto.	Área de sistemas	Validación en campo	Lista de chequeo	Análisis documental	Matriz con debilidades fortalezas del sistema.



**Tabla 3**

*Variables e hipótesis*

<b>Variable</b>	<b>Descripción</b>	<b>Tipo de Variable</b>	<b>Objetivo específico</b>	<b>Indicador</b>	<b>Naturaleza</b>	<b>Fuente</b>	<b>Tr*</b>	<b>Ta**</b>
Eficiencia	Esta variable es utilizada como indicador para medir el SGSI en la Clínica Proinsalud	Dependiente	Evaluar la efectividad del SGSI	100 % de la lista de chequeo en el cumplimiento del SGSI	Cuantitativa	Desarrolladores	Lista de chequeo	Cuantitativa
Vulnerabilidad	Esta variable es usada para identificar el grado de amenazas y riesgos informáticos en la Clínica Proinsalud.	Dependiente	Evaluar amenazas, riesgos en información de la Clínica Proinsalud	100 % de vulnerabilidades identificadas	Cuantitativa	Desarrolladores	Cuestionario de auditoria	Cuantitativa

## 1.8. Presupuesto

**Tabla 4**

*Rubros totales*

<b>Rubros</b>	<b>Total (\$)</b>
Inversión en personal	6.333.080
Rubros	1.970.000
<b>Total</b>	<b>\$8.303.080</b>

**Tabla 5**

*Costos totales de los investigadores de la investigación*

<b>Nombre investigador</b>	<b>Vr. Horas investigador</b>	<b>Dedicación</b>	<b>Valor</b>
		<b>Número total de horas</b>	
Nicolas Muñoz	8.333	240	1.999.920
Daniel Solarte	8.333	240	1.999.920
Carlos Delgado	8.333	240	1.999.920
Javier Villalba	16.666	20	333.320
<b>Total</b>			<b>6.333.080</b>
Vr horas investigador Docente		4 SMDLV/8	\$ 16.666
Vr horas investigador Estudiante		2 SMDLV/8	\$ 8.333

**Tabla 6**

*Rubros materiales*

<b>Rubro</b>	<b>Justificación</b>	<b>Valor total</b>
Resma de papel	Obtención de la información de manera tangible	70.000
Lapiceros	Escribir información pertinente al caso de estudio.	20.000
Borradores	Este recurso es esencial para poder anotaciones de los casos de	10.000

<b>Rubro</b>	<b>Justificación</b>	<b>Valor total</b>
	estudio.	
Libretas	Capturar información relevante del caso de estudio	100.000
Toner	Cambio de toner de la impresora para mejorar calidad de impresión	250.000
<b>Total</b>		<b>450.000</b>

**Tabla 7**

*Equipos tecnológicos*

<b>Rubro</b>	<b>Justificación</b>	<b>Valor total</b>
Depreciación equipos de computo	Desgaste y pérdida de valor de los equipos de cómputo con el tiempo y el uso.	300.000
Depreciación de impresora	Desgaste y pérdida de valor de los equipos de cómputo con el tiempo y el uso.	150.000
<b>Total</b>		<b>450.000</b>

**Tabla 8**

*Otros rubros*

<b>Rubro</b>	<b>Justificación</b>	<b>Valor total</b>
Salidas de campo (20)	Se harán visitas previamente la clínica para la recolección de información, auditorías, capacitaciones	320.000
Eventos académicos	Este evento se divulgará en un evento académico, para lo cual se costea inscripción	500.000
Publicación	Los resultados de la investigación se publicarán en revista.	150.000
<b>Total</b>		<b>970.000</b>

## 1.9. Cronograma

**Tabla 9**

*Fecha de actividades*

Actividades	Tiempo en semanas																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Identificar los activos informáticos, procesos y servicios soportados por la oficina de Tecnologías de Información de la Clínica Proinsalud																				
Realizar inventario de Activos.	X	X																		
Inventario de procesos de la clínica.				X																
Identificar prioridades de cada proceso con sus dueños		X	X																	
Analizar y evaluar amenazas, riesgos y vulnerabilidades desde la metodología Magerit.																				
Identificar amenazas y riesgos existentes				X	X															
Recopilar y analizar las vulnerabilidades encontradas.						X	X	X												
Diseñar el Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001.																				
Identificar estrategias para el tratamiento de los riesgos.								X	X	X										
Implementar técnicas para el tratamiento de los riesgos										X	X	X								
Crear políticas para el tratamiento de los riesgos.													X	X						

Actividades	Tiempo en semanas																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Brindar controles recomendados.															X	X				
Asignación de responsabilidades.																X				
Evaluar el Diseño del Sistema de Gestión de Seguridad de la Información (SGSI). Clínica Proinsalud de Pasto.																				
Evaluación del tratamiento de los riesgos.																	X			
Verificación de metodología implementada.																		X		
Resumen de resultados.																			X	
Conclusiones																				X

### **1.10. Productos esperados**

Se entregará un documento con todos los resultados de la investigación acorde con los lineamientos de la Universidad Mariana.

Se entregará un artículo científico el cual será publicado en una revista reconocida.

Los resultados de la investigación se presentarán en un evento de carácter nacional o internacional que permita su divulgación.

## 2. Desarrollo del proceso investigativo

### 2.1. Activos informáticos, procesos y servicios de las áreas de la Clínica Proinsalud

A continuación, se describen los activos, procesos y servicios de las diferentes áreas de la Clínica Proinsalud.

#### 2.1.1. Dirección subgerencia administrativa y financiera

Es la encargada de gestionar el personal y los recursos financieros de la entidad, ya que en esta dirección recae la toma de decisiones para optimizar el capital económico y con ello la toma de decisiones, estas deben ser coherentes con las inversiones que puede realizar La Clínica Proinsalud S.A. Esta área cuenta con las siguientes dependencias:

**2.1.1.1. Talento humano.** El departamento de Talento Humano de la Clínica Proinsalud, planea, coordina, ejecuta y presta orientaciones técnicas sobre actividades de administración de personal, entrenamiento y formación, bienestar social, seguridad y salud ocupacional, basado en las políticas, directrices y normas legales y de la empresa, Esta área cuenta con una infraestructura la cual está ubicada en el segundo piso de la Clínica Proinsalud compuesta por seis puestos de trabajo como lo muestra la figura 6, dentro en ella se encuentran 9 equipos de cómputo los cuales están repartidos en las distintos puestos de trabajo estos equipos cuentan con programas de software y unas características que están descritas en la tabla 10. Dentro de los aspectos más relevantes que se deben tener en cuenta para el desarrollo de las actividades son:

Administración de personal: Asegurar que la Clínica Proinsalud cumple y aplica las legislaciones del trabajo y obligaciones tributarias y sociales.

Entrenamiento y Formación: Desarrollar planes de capacitación y formación orientados a mejorar la competencia de los trabajadores y al desarrollo del potencial humano.

Bienestar social: Ejecutar acciones integradas que ayuden a preservar la calidad de vida del

trabajador, mejorar su estado de salud física y emocional a través de recreación y deportes eventos socio – culturales, atención y acompañamiento social, administración de convenios (planes de salud, seguros de vida) y capacitaciones preventivas

Reclutamiento y Selección: Implementar acciones necesarias para entregar a las diferentes dependencias (administrativas / operacionales) personal competente y capacitado que contribuya al cumplimiento de la visión, objetivos y metas de la empresa.

Seguridad y salud Ocupacional: Crear políticas y controles que minimicen los riesgos de accidentes que atentan contra la salud de los trabajadores en cada puesto de trabajo de la Clínica Proinsalud.

### **Figura 6**

*Área de recursos humanos*



*Nota.* La figura corresponde a los equipos de cómputo los cuales están ubicados en el área de talento humano.



**Tabla 10***Inventario del área de recursos humano*

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
NOMAUX 02	1301102	Administrativa > rhumanos 2 piso	8CC0410 KVVW	HP All-in-One 24-dd0xxx	Win 10 pro	22/07/2022 12:05	AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx	8 Gb	Siigo Sima /radicador de cuentas Ofimatica siigo nomina outlook messenger
Reccoord	1300837	Administrativa > rhumanos 2 piso	MXL248 0KT9	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	30/03/2022 13:48	Intel(R) Core(TM) i3- 3220 CPU @ 3.30GHz	4 Gb	Ofimática Sima/evaluación de desempeño outlook messenger
RECHUM 01	1300811	Administrativa > rhumanos 2 piso	MXL248 0KTG	HP Compaq Pro 4300 AiO 20 PC	Win 10 pro	1/08/2022 1:31	Intel(R) Core(TM) i3- 3220 CPU @ 3.30GHz	4 Gb	huellero de marcaciones Ofimatica SIMA creacion de usuarios radicador de cuentas outlook messenger

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
RECURS OSH UMAUX0 1	1300948	Administrativa > rhumanos 2 piso	1300948	MS-7A15	Win 10 pro	1/08/2022 1:28	Intel(R) Core(TM) i7- 7700 CPU @ 3.60GHz	8 Gb	Ofimatica Sima / radicador de cuentas outlook messenger siigo nomina
rhaux01	1300828	Administrativa > rhumanos 2 piso	MXL248 0KTD	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	1/08/2022 1:31	Intel(R) Core(TM) i3- 3220 CPU @ 3.30GHz	6 Gb	Ofimatica Sima / radicador de cuentas outlook messenger siigo nomina
RHAUX0 3	1300227	Administrativa > rhumanos 2 piso		MS-7255 V2.0	Win 7 pro	1/08/2022 1:30	Intel(R) Pentium(R) Dual CPU E2160 @ 1.80GHz	2 Gb	Ofimatica Sima / radicador de cuentas outlook messenger siigo nomina
RHAUX0 4	1301191	Administrativa > rhumanos 2 piso	1CZ1290 DDF	HP ProDesk 400 G7 Small Form Factor PC	Win 10 pro	16/08/2022 17:30	Intel(R) Core(TM) i5- 10500 CPU @ 3.10GHz	8 Gb	Ofimatica Sima / radicador de cuentas outlook messenger siigo nomina
rhnom01	900200526	Administrativa > rhumanos 2	MXL527 1GSR	HP ProOne 400 G1 AiO	Win 8.1	23/03/2022 13:44	Intel(R) Core(TM) i7-	8 Gb	Ofimatica Sima / radicador de

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
		piso			pro		4770T CPU @ 2.50GHz		cuentas outlook messenger siigo nomina
RHNON0 2	1300027	Administrativa > rhumanos 2 piso	1300027	OEM	Win 7 pro	21/02/2022 12:32	Intel(R) Celeron(R) CPU 430 @ 1.80GHz	2 Gb	Ofimatica Sima / radicador de cuentas outlook messenger siigo nomina escaneer

**2.1.1.2. Contabilidad.** El área de contabilidad en la Clínica Proinsalud es la responsable de instrumentar y operar las políticas, normas, sistemas y procedimientos necesarios para garantizar la exactitud y seguridad en la captación y registro de las operaciones financieras, presupuestarias y de consecución de metas de la empresa. Es decir que contabilidad es el área de control de gastos e ingresos y de la situación financiera de la empresa, además de saber los cobros y pagos pendientes, dentro de la infraestructura de la Clínica esta área se encuentra situada en el tercer piso, es una de las áreas que cuenta con más puestos de trabajo debido a la importancia que esta presenta dentro de la Clínica se puede evidenciar la estructura dentro del área en la figura 7, cuenta con 6 equipos de cómputo los cuales cuentan con un serial, unas características y software instalados esta información esta detallada en la tabla 11.

Sus funciones principales son control de libros contables: se encuentra con los libros de registro, donde aparecen las facturas emitidas y recibidas, el registro de los bienes de inversión, el cierre del ejercicio: aquí se ocupa de preparar, balance, cuenta de pérdidas y ganancias, memoria de cuentas, las obligaciones registrales: la legalización y el depósito de libros y cuentas, la preparación de impuestos y tareas del departamento de contabilidad. Además de todo esto, entre las funciones de un contable administrativo destaca que es el responsable de diseñar el Plan General Contable (PGC) de la empresa. El PGC es un documento que sirve de guía a la hora de llevar a cabo todas las funciones asignadas al área de contabilidad, de esta forma este actúa ordenada y coherente.

### **Figura 7**

*Área de contabilidad*



*Nota.* La figura corresponde a los equipos de cómputo los cuales están ubicados en el área de contabilidad.

**Tabla 11***Inventario del área de contabilidad*

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
caraux02	1300957	Administrativa > contabilidad 3 piso	1300957	MS-7A15	Win 10 pro	1/08/2022 2:11	Intel(R) Core(TM) i7- 7700 CPU @ 3.60GHz	8 Gb	Siigo, Ofimatica, Otllockmessenger Sima /Facturacion/radica dor de cuentas
CONAUX0 1	900200523	Administrativa > contabilidad 3 piso	MXL5271 GT6	HP ProOne 400 G1 AiO	Win 8.1 pro	28/03/2022 8:58	Intel(R) Core(TM) i7- 4770T CPU @ 2.50GHz	8 Gb	Siigo, Ofimatica, Otllockmessenger Sima /Facturacion/radica dor de cuentas
CONAUX0 3	1300950	Administrativa > contabilidad 3 piso	1300950	MS-7A15	Win 10 pro	1/08/2022 2:10	Intel(R) Core(TM) i7- 7700 CPU @ 3.60GHz	8 Gb	Siigo, Ofimatica, Otllockmessenger Sima /Facturacion/radica dor de cuentas
conaux04	1300814	Administrativa > contabilidad 3 piso	MXL2480 KXM	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	1/08/2022 2:11	Intel(R) Core(TM) i3- 3220 CPU @ 3.30GHz	4 Gb	Siigo, Ofimatica, Otllockmessenger Sima /Facturacion/radica

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
									dor de cuentas
CONTACO ORD	1301195	Administrativa > contabilidad 3 piso	8CC13226 PR	HP 200 G4 22 All-in- One PC	Win 10 pro	30/03/2022 16:39	Intel(R) Core(TM) i5- 10210U CPU @ 1.60GHz	8 Gb	Siigo, Ofimatica, Otlookmessenger Sima /Facturacion/radica dor de cuentas
FISCAL01	1301106	Administrativa > contabilidad 3 piso	8CC0410 KW5	HP All-in- One 24- dd0xxx	Win 10 pro	6/04/2022 20:07	AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx	8 Gb	Siigo, Ofimatica, Otlookmessenger Sima /Facturacion/radica dor de cuentas

*Nota.* En la tabla se describe hardware como software de los equipos de cómputo del área de contabilidad de la Clínica Proinsalud con sus respectivas ubicaciones.

**2.1.1.3. Facturación.** El área de Facturación de la Clínica Proinsalud está ubicada en el primer piso cuenta con un espacio reducido donde están ubicados los puestos de trabajo dentro de estos están incluidos impresoras y equipos de cómputo en la figura 8 se observa la distribución de los puestos de trabajo, en seguida en la tabla 13 se puede evidenciar el inventario de los equipos como también sus características y software instalados. El área de facturación está relacionada con el proceso de admisiones; su objetivo básico es realizar el seguimiento al paciente desde su ingreso a la Clínica hasta el egreso de esta, al tiempo que realiza un registro de cada uno de los servicios prestados durante la estancia del paciente, para finalmente producir un documento equivalente de cobro o factura de venta de servicios. Esta área debe enviar hacia contabilidad, como mínimo, los siguientes documentos con sus respectivos atributos:

**2.1.1.3.1. Factura o documento de cobro equivalente de venta por prestación de servicios.** 1. Nota Débito Cliente. 2. Nota Crédito Cliente

**2.1.1.3.2. Insumos y productos del proceso de facturación.** Entradas: a. Un contrato o convenio y un manual de tarifas, Varios contratos pueden utilizar un mismo manual de tarifas.

La Clínica Proinsalud en que informan los procedimientos, exámenes y suministros que fueron realizados o aplicados a un paciente. Registro individual de Prestación de Servicios RIPS.

Salidas: a. La principal salida de un área de facturación es la factura individual por paciente por concepto de servicios prestados al mismo. Esta debe cumplir estrictamente los requisitos legales y contractuales en cuanto a presentación, soportes, fechas, liquidación y formatos, entre otros.

b. También una IPS requiere internamente información que se genera en facturación y que debe ser distribuida bajo unos requisitos precisos. Esta información está compuesta de reportes a la gerencia, a las áreas administrativas y a las áreas misionales.

**Figura 8**

*Figura del área de facturación*



*Nota.* La figura corresponde a los equipos de cómputo los cuales están ubicados en el área de facturación.



**Tabla 12***Inventario del área de facturación*

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
FACAU X07	1300636	Administrativa > facturacion 1 piso	1300636	G31-M7 TE	Win 7 pro	31/03/2022 11:23	Pentium(R) Dual-Core CPU E5400 @ 2.70GHz	2 Gb	Sima / facturacion /consukltas generales/ derechos / autorizaciones ofimatica outlook messenger antivirus sophos
FACTAU X001	1300817	Administrativa > facturacion 1 piso	MXL248 0KTC	HP Compaq Pro 4300 AiO 20 PC	Win 10 pro	9/05/2022 16:55	Intel(R) Core(TM) i3- 3220 CPU @ 3.30GHz	4 Gb	Sima / facturacion /consukltas generales/ derechos / autorizaciones ofimatica outlook messenger antivirus sophos
factucin	1300841	Administrativa > facturacion 1 piso	MXL248 0KTP	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	1/08/2022 0:59	Intel(R) Core(TM) i3- 3220 CPU @ 3.30GHz	4 Gb	Sima / facturacion /consukltas generales/ derechos / autorizaciones ofimatica outlook messenger antivirus sophos

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
FACTUC OORD	1301197	Administrativa > facturacion 1 piso	8CC1322 66B	HP 200 G4 22 All-in-One PC	Win 10 pro	27/01/2022 16:07	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz	8 Gb	Sima / facturacion /consukltas generales/ derechos / autorizaciones/ generador de reportes ofimatica outlook messenger antivirus sophos
FACTUC OORD02	1300697	Administrativa > facturacion 1 piso	JAY791 QCB00 236	300E4C/ 300E5C/ 300E7C	Win 10 pro	24/03/2022 17:41	Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz	4 Gb	Sima / facturacion /consukltas generales/ derechos / autorizaciones ofimatica outlook messenger antivirus sophos
Factucos01	900200338	Administrativa > facturacion 1 piso	MXL333 0L38	HP Pro3500 Series	Win 10 pro	1/08/2022 2:24	Intel(R) Core(TM) i5-3470 CPU @ 3.20GHz	4 Gb	Sima / facturacion /consukltas generales/ derechos / autorizaciones ofimatica outlook messenger antivirus sophos
FACTV ENT01	1300605	Administrativa > facturacion 1	MXL009 03Z5	Compaq 505B	Win 7 pro	1/08/2022 1:53	AMD Athlon(tm) II X2 215	4 Gb	Sima / facturacion /consukltas generales/

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
		piso		Microto wer PC			Processor		derechos / autorizaciones ofimatica outlook messenger antivirus sophos
Facucia 01	900100029	Clinica > facturacion 4 piso	MXL605 11MZ	HP ProDesk 400 G2.5 SFF	Win 10 pro	1/08/2022 2:24	Intel(R) Core(TM) i7- 4790S CPU @ 3.20GHz	8 Gb	Sima / facturacion /consuktas generales/ derechos / autorizaciones ofimatica outlook messenger antivirus sophos
Portátil 4 Prestamo	1300696	Administrativa > facturacion 1 piso	JAY791 QCB07 868	300E4C/ 300E5C/ 300E7C	Win 10 pro	24/03/2022 17:41	Intel(R) Core(TM) i5- 3210M CPU @ 2.50GHz	4 Gb	Sima / facturacion /consuktas generales/ derechos / autorizaciones ofimatica outlook messenger antivirus sophos

*Nota.* Datos tomados del área de recursos humanos de la Clínica Proinsalud que corresponde a los equipos de cómputo con sus respectivas características de hardware como software y su ubicación.

**2.1.1.4. Cartera.** El área de cartera de la Clínica Proinsalud se encuentra en el tercer piso, es un área más pequeña como se muestra en la figura 9, cuenta con tan solo 3 equipos de cómputo estos están descritos en la tabla 13, Esta área se encarga de gestionar las deudas que los clientes tienen con la Clínica, la oficina de cartera en la Clínica Proinsalud es la encargada de recuperar las deudas a ser gestionadas.

Obligando a que las instituciones del sector salud diseñen nuevas propuestas para recuperar y organizar la morosidad existente. Actualmente, situaciones como el incumplimiento en el pago por el Estado y de las EPS a las IPS ha ocasionado que se acreciente el riesgo de inviabilidad financiera por la presencia de mayores niveles de endeudamiento e incumplimiento con las entidades financieras, el Estado, proveedores, empleados y contratistas, aunque cabe señalar que una de las problemáticas de cartera del sector hospitalario corresponde a la desactualización y desorganización de la misma.

Es por eso que en el Clínica Proinsalud el sistema de gestión de cartera optimiza los procesos administrativos en lo que concierne a la recuperación de la misma. Por tal motivo, para identificar las causas y proponer posibles soluciones a dicho problema, es responsabilidad de todas las instituciones prestadoras de servicio de salud, brindar a sus usuarios servicios de la mejor calidad, en condiciones de oportunidad y eficiencia que garantice la suficiente atención para el mejoramiento de la salud de la población colombiana. Por tal motivo, las organizaciones de salud contratan personal calificado, equipos e instalaciones en condiciones idóneas para la prestación del servicio.

**Figura 9**

*Área de cartera*



*Nota.* La figura corresponde a los equipos de cómputo los cuales están ubicados en el área de cartera.

**Tabla 13***Inventario del área de cartera*

Nombre	Número de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
carcoor	1300859	Administrativa > cartera 3 piso	MXL248 0KWQ	HP Compaq Pro 4300 AiO 20 PC	Win 10 pro	1/08/2022 2:13	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	4 Gb	Ofimatica outlook meseenger Siigo
CARTER AUX03	1301196	Administrativa > cartera 3 piso	8CC1322 689	HP AiO 22 G4	Win 10 pro	1/04/2022 11:17	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz	8 Gb	Ofimatica outlook meseenger Siigo
cosaux02	900200531	Administrativa > cartera 3 piso	MXL527 1GVC	HP ProOne 400 G1 AiO	Win 8.1 pro	1/08/2022 2:14	Intel(R) Core(TM) i7-4770T CPU @ 2.50GHz	8 Gb	Ofimatica outlook meseenger Siigo Generador de reportes sima

*Nota.* Datos tomados del área de recursos humanos de la Clínica Proinsalud que corresponde a los equipos de cómputo con sus respectivas características de hardware como software y su ubicación.

**2.1.1.5. Suministros.** En la Clínica Proinsalud el área de suministros está ubicada en el parqueadero el cual está en el sótano de la clínica es un área de dimensiones muy reducidas, esta cuenta 2 quipos de cómputo en los cuales se registran las entradas de la Clínica las características de los equipos están registradas en la tabla 14. Esta área es de suma importancia ya que por medio de esta área la clínica obtiene su dotación física y de materiales pertinente para una buena prestación de su servicio. esta área es la encargada de decepcionar todas las compras e ingresarlas a los activos de la Clínica Proinsalud por medio del software sigo quien genera una placa de identificación del producto dentro de los activos de la institución. también es la encargada de velar por que los activos de la Clínica Proinsalud se encuentren en óptimas condiciones y se encuentren dentro de la institución ya que es el área encargada de realizar inventarios periódicos y velar por los activos de la Clínica Proinsalud.

**Tabla 14***Inventario del área de suministros*

Nombre	Número de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
sumact01	1300879	Clinica > suministros - parqueadero	MXL7032X1X	HP ProOne 400 G2 20-in Non- Touch AiO	Win 10 pro	12/05/2022 12:13	Intel(R) Core(TM) i5- 6500 CPU @ 3.20GHz	8 Gb	Siigo Outlook messenger Ofimatica Sima / radicador de cuentas generador de plaquetas de inventario
Sumcoord01	900200528	Clinica > suministros - parqueadero	MXL5271GTB	HP ProOne 400 G1 AiO	Win 10 pro	1/08/2022 0:12	Intel(R) Core(TM) i7- 4770T CPU @ 2.50GHz	8 Gb	Siigo Outlook messenger Ofimatica Sima / radicador de cuentas generador de plaquetas de inventario

*Nota.* En la tabla se describe hardware como software de los equipos de cómputo del área de contabilidad de la Clínica Proinsalud con sus respectivas ubicaciones.



**2.1.1.6. Pagaduría.** El área de pagaduría de la Clínica es el departamento encargado de gestionar los pagos y las facturas relacionadas con los servicios médicos prestados a los pacientes.

En este caso, esta área se encuentra ubicada en un segundo piso y cuenta con 3 equipos de cómputo, es un espacio dedicado exclusivamente a tareas administrativas y contables. Los equipos están equipados con software especializado en gestión de facturación y pagos, así como herramientas de ofimática estándar como procesadores de texto, hojas de cálculo y programas de correo electrónico como muestra la tabla 12.

En esta área, los empleados pueden llevar a cabo una variedad de tareas, como procesar y enviar facturas a los pacientes, verificar y registrar pagos, mantener registros financieros precisos y actualizar bases de datos de pacientes y aseguradoras. Además, pueden comunicarse con otros departamentos de la clínica para coordinar el procesamiento de pagos y resolver cualquier problema relacionado con la facturación y los pagos.

**Tabla 15***Inventario del área de pagaduría*

Nombre	Número de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
PAGAU X01	1301180	Administrativa > pagaduría 2 piso	1CZ1290 DMR	HP ProDesk 400 G7 Small Form Factor PC	Win 10 pro	31/03/2022 11:56	Intel(R) Core(TM) i5- 10500 CPU @ 3.10GHz	8 Gb	Ofimatica Siigo Coneccion bancos sima /radicado de cuentas
pagaux0 2	1300819	Administrativa > pagaduría 2 piso	MXL248 0KW4	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	1/08/2022 1:38	Intel(R) Core(TM) i3- 3220 CPU @ 3.30GHz	6 Gb	Ofimatica Siigo Coneccion bancos sima /radicado de cuentas
pagcoor d01	900200507	Administrativa > pagaduría 2 piso	9002005 07	HP ProOne 400 G1 AiO	Win 8.1 pro	1/08/2022 1:39	Intel(R) Core(TM) i7- 4770T CPU @ 2.50GHz	8 Gb	Ofimatica Siigo Coneccion bancos sima /radicado de cuentas

*Nota.* Datos tomados del área de recursos humanos de la Clínica Proinsalud que corresponde a los equipos de cómputo con sus respectivas características de hardware como software y su ubicación.

**2.1.1.7. Registro y control.** El área de registro y control en una clínica es el departamento encargado de mantener un registro preciso y actualizado de todos los pacientes, citas y servicios médicos prestados. En este caso, esta área se encuentra ubicada en un segundo piso y cuenta con 3 equipos de cómputo con software especializado para el área como se muestra en la tabla 16.

En esta área, los empleados pueden llevar a cabo una variedad de tareas, como registrar la información de los pacientes, programar citas y mantener un registro detallado de los servicios médicos prestados a cada paciente. Además, pueden trabajar en conjunto con otros departamentos de la clínica para coordinar la atención de los pacientes y asegurarse de que se sigan los procedimientos adecuados.

Esta área de registro y control es la responsable de la gestión de los pagos y facturación, trabajando en estrecha colaboración con el departamento de pagaduría para garantizar que los pacientes reciban facturas precisas y oportunas por los servicios médicos prestados.

**Tabla 16***Inventario del área de registro y control*

Nombre	Número de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
regiycon02	900200509	Administrativa > registro 2 piso	MXL527 1GV6	HP ProOne 400 G1 AiO	Win 8.1 pro	1/08/2022 2:32	Intel(R) Core(TM) i7-4770T CPU @ 2.50GHz	8 Gb	Sima / RYC / Derechos Ofimatica, Sophos
rycaux01	1300902	Administrativa > registro 2 piso	8CC7340 782	24-g209la	Win 10 pro	1/08/2022 2:31	Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz	4 Gb	Sima / RYC / Derechos Ofimatica, Sophos / escanner
ryccoor	1300826	Administrativa > registro 2 piso	MXL248 0KXQ	HP Compaq Pro 4300 AiO 20 PC	Win 10 pro	1/08/2022 2:32	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	4 Gb	Sima / RYC / Derechos Ofimatica, Sophos generador de informes

*Nota.* En la tabla se describe hardware como software de los equipos de cómputo del área de contabilidad de la Clínica Proinsalud con sus respectivas ubicaciones.

**2.1.1.8. Área de sistemas.** La oficina de sistemas de la Clínica Proinsalud se encuentra ubicada en el tercer piso de la casa de Referencia y Contra referencia esta dependencia cuenta con una estructura un poco amplia se divide en dos partes una de ella es la parte de desarrollo y mantenimiento como se muestra en la figura 10, el inventario de los equipos está plasmada en la tabla 17. Esta área se encuentra conformada organizacionalmente de la siguiente forma:

- 1 cuenta con un director de Área
- 1 cuenta con un coordinador de área
- 2 ingenieros T.I
- 1 ingeniero de redes.
- 3 técnicos.

Estos funcionarios dentro de la Clínica Proinsalud tienen unos roles ya definidos:

El director de área es el encargado de Organizar las reuniones y velar por el cumplimiento de los requerimientos que se le solicitan al área de sistemas.

Director de sistemas se encargará por velar que el grupo de sistemas cumpla a cabalidad sus funciones y sus tareas asignadas,

Ingenieros T.I se encargará por velar por la integridad de la seguridad de la información, por qué se cuenta con seguridad perimetral, velar por el correcto funcionamiento de los servidores que pertenecen a la Clínica Proinsalud, capacitar en la aplicativa sima y velar por que este se encuentre en funcionamiento.

Ingeniero de redes es el encargado de velar por la conexión de las diferentes área e instalación de cámaras de seguridad.

Los técnicos se encargará por velar por el perfecto funcionamiento de los equipos de cómputo tanto en su parte de hardware como software, son los que realizan los mantenimientos preventivos programados por los Ing. T.I

El área de Sistemas de Proinsalud. Son un equipo de trabajo que hace posible que la entidad cuente con herramientas y servicios de tecnología e información necesarios para poder cumplir los objetivos de servicio de la Clínica Proinsalud.

Las líneas de acción del área de sistemas de la clínica Proinsalud son las siguientes:

Sistemas de información: Se garantiza el desarrollo, soporte y mantenimiento de los sistemas de información Sima, SIIGO, WEPS, OVIYAM, SIGE esenciales para llevar a cabo los procesos de la entidad.

Servicios tecnológicos: estos están organizados para garantizar la implementación mantenimiento y soporte de los recursos tecnológicos.

### **Figura 10**

*Área de desarrollo departamento de sistemas*



*Nota.* La figura corresponde a los equipos de cómputo los cuales están ubicados en el área de desarrollo departamento de sistemas.

**Tabla 17***Inventario del área de sistemas*

Nombre	Número de inventario	Localización	Fabricador	Número de serie	Tipo	Modelo	Sistema operativo - Nombre	Componentes - Procesador	Memoria
DESKTOP-K94BF5S	1301088	Administrativa > sistemas 3 piso	HP	8CC0281C 0Q	All in One	HP All-in-One	Win 10 pro	Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz	8 Gb
HOME CAR ECOOR	1301190	Administrativa > sistemas 3 piso	HP	1CZ1290D 70	DESKT OP	HP ProDesk 400 G7 Small Form Factor PC	Win 10 pro	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	8 Gb
Portátil 5 préstamo	1300776	Administrativa > sistemas 3 piso	LENOVO	YB057839 22	LAPTO P	Lenovo G40-70	Win 10 pro	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	8 Gb
Portatil 6 prestamo	1300897	Administrativa > sistemas 3 piso	HP	CND7197 TJP	LAPTO P	HP Laptop 15-bs0xx	Win 10 pro	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	8 Gb
SISDIRECT OR	1301184	Administrativa > sistemas 3 piso	HP	1CZ1290D CT	DESKT OP	HP ProDesk 400 G7 Small Form Factor PC	Win 10 pro	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	8 Gb
SISPRO01	1301183	Administrativa >	HP	1CZ1290D	DESKT	HP ProDesk	Win 10 pro	Intel(R) Core(TM)	8 Gb

Nombre	Número de inventario	Localización	Fabricador	Número de serie	Tipo	Modelo	Sistema operativo - Nombre	Componentes - Procesador	Memoria
		sistemas 3 piso		NT	OP	400 G7 Small Form Factor PC		i5-10500 CPU @ 3.10GHz	
SISPRO02	1301182	Administrativa > sistemas 3 piso	HP	1CZ1290D NQ	DESKT OP	HP ProDesk 400 G7 Small Form Factor PC	Win 10 pro	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	8 Gb
SISPRO05	1301186	Administrativa > sistemas 3 piso	HP	1CZ1290D N2	DESKT OP	HP ProDesk 400 G7 Small Form Factor PC	Win 10 pro	Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz	8 Gb
SISSOPORT E10	MXL5271GS V	Administrativa > sistemas 3 piso	Hewlett- Packard	MXL5271 GSV	DESKT OP	HP ProOne 400 G1 AiO	Win 10 pro	Intel(R) Core(TM) i7-4770T CPU @ 2.50GHz	8 Gb
SistemasSop 01	900200512	Administrativa > sistemas 3 piso	Hewlett- Packard	MXL5271 GVN	All in One	HP ProOne 400 G1 AiO	Win 10 pro	Intel(R) Core(TM) i7-4770T CPU @ 2.50GHz	8 Gb
Sopaux03	900200514	Administrativa > sistemas 3 piso	Hewlett- Packard	MXL5271 GVD	DESKT OP	HP ProOne 400 G1 AiO	Win 10 pro	Intel(R) Core(TM) i7-4770T CPU @ 2.50GHz	8 Gb
soporte1	900200587	Administrativa >	HP	MXL7253	All in	HP ProOne	Win 10 pro	Intel(R) Core(TM)	8 Gb



Nombre	Número de inventario	Localización	Fabricador	Número de serie	Tipo	Modelo	Sistema operativo - Nombre	Componentes - Procesador	Memoria
		sistemas 3 piso		CFD	One	400 G2 20- in Non- Touch AiO		i7-6700T CPU @ 2.80GHz	
srvchat	900100033	Clinica > sistemas bodega -parquadero	HP	MXL6050 ZS2	DESKT OP	HP ProDesk 400 G2.5 SFF	Win 10 pro	Intel(R) Core(TM) i7-4790S CPU @ 3.20GHz	8 Gb
DESKTOP- K94BF5S	1301088	Administrativa > sistemas 3 piso	HP	MXL6050 ZS2	DESKT OP	HP ProDesk 400 G2.5 SFF	Win 8.1 Pro	Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz	8gb

*Nota.* En la tabla se describe hardware como software de los equipos de cómputo del área de Sistemas de la Clínica Proinsalud con sus respectivas ubicaciones.

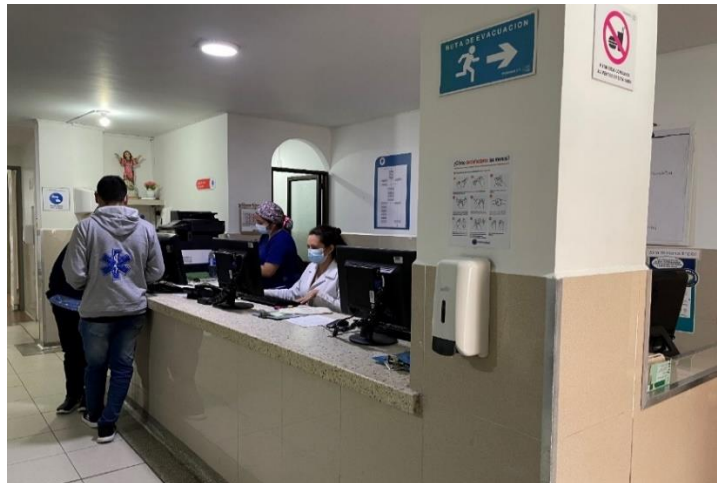
## 2.1.2. Dirección clínica

**2.1.2.1. Urgencias.** El servicio de urgencias de la Clínica Proinsalud ubicada en el primer piso cuenta con 5 equipos en la estación de enfermería como se evidencia en la figura 11 y 4 consultorios médicos estos equipos tienen unos programas de software instalados y unas características específicas como S.O todas estas características se encuentran alojadas en la tabla 18 brinda atención las 24 horas, a través de especialistas calificados y alta tecnología para la atención de los usuarios y grupos familiares pertenecientes al magisterio de Nariño.

El servicio de urgencias de la Clínica Proinsalud se encuentra ubicado por la carrera 34 # 14 - 37 del barrio san Ignacio de la ciudad de Pasto. Cuenta con un grupo de profesionales idóneos con gran experiencia en manejo de situaciones críticas y problemas de salud de alta gravedad y complejidad. Los médicos generales, enfermeros y demás personal asistencial y administrativo de la Clínica Proinsalud S.A los cuales apoyan la labor del servicio de urgencias de la Clínica, cuentan con una formación profesional y humana. La Clínica cuenta con el apoyo de todas las especialidades médicas y quirúrgicas disponibles en la Clínica, permitiendo la toma de decisiones en las que se requiera de su presencia lo cual permite brindar una atención segura y de calidad.

### Figura 11

Área de urgencias



*Nota.* La figura corresponde a los equipos de cómputo los cuales están ubicados en el área de urgencias.

**Tabla 18***Inventario del área de urgencias*

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
FACTUR VENTANA I002	900200171	Clinica > urgencias 1 piso	MXL2480KXH_001	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	26/08/2022 9:56	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	4 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shapos outlook messenger
ORIENT A DOR01	1300606	Clinica > urgencias 1 piso	MXL00903Z1	Compaq 505B Microtower PC	Win 7 pro	5/04/2022 18:36	AMD Athlon(tm) II X2 215 Processor	2 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shapos outlook messenger
TABLET COMP UTER 01	1301164	Clinica > urgencias 1 piso	HGAK5BC7	Lenovo TB-X505L	And 9	13/10/2021 15:38		8 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shapos outlook messenger
URG-EST01	1301140	Clinica > urgencias 1 piso	MJ0DZX4R	ThinkCentre M70q	Win 10 pro	25/03/2022 19:53	Intel(R) Core(TM) i5-10400T CPU @ 2.00GHz	8 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shapos outlook

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
									messenger
URG-EST03	1301141	Clinica > urgencias 1 piso	MJ0DZX 31	ThinkCentre M70q	Win 10 pro	31/03/2022 10:02	Intel(R) Core(TM) i5-10400T CPU @ 2.00GHz	8 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shopos outlook messenger
URG-EST04	1301123	Clinica > urgencias 1 piso	MJ0DZX 2V	ThinkCentre M70q	Win 10 pro	1/05/2022 7:04	Intel(R) Core(TM) i5-10400T CPU @ 2.00GHz	8 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shopos outlook messenger
urg109	1300863	Clinica > urgencias 1 piso	MXL248 0KW6	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	1/08/2022 0:33	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	4 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shopos outlook messenger
urg111	1300800	Clinica > urgencias 1 piso	S1H049 AR	ThinkCentre E73z	Win 7 pro	1/08/2022 0:29	Intel(R) Core(TM) i5-4460T CPU @ 1.90GHz	4 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shopos outlook messenger
URG113	1300835	Clinica >	MXL248	HP	Win 7	1/08/2022	Intel(R)	4 Gb	Sima /consulta médica

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
		urgencias 1 piso	0KXT	Compaq Pro 4300 AiO 20 PC	pro	0:31	Core(TM) i3- 3220 CPU @ 3.30GHz		ambulatoria derechos triage historia de evolucion ofimatica shopos outlook messenger
URGAD M01	900200515	Clinica > urgencias 1 piso	MXL527 1GV3	HP ProOne 400 G1 AiO	Win 10 pro	1/08/2022 0:23	Intel(R) Core(TM) i7- 4770T CPU @ 2.50GHz	8 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shopos outlook messenger
URGCAR ES04	1300476	Clinica > urgencias 1 piso	1300476	OEM	Win 7 pro	21/02/2022 12:31	Intel(R) Core(TM)2 Duo CPU E7400 @ 2.80GHz	2 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shopos outlook messenger
URGCAR EST	1300809	Clinica > urgencias 1 piso	MXL248 0KT1	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	1/08/2022 0:31	Intel(R) Core(TM) i3- 3220 CPU @ 3.30GHz	4 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shopos outlook messenger
URGCO O RD	900200584	Clinica > urgencias 1 piso	MXL725 3CDQ	HP ProOne 400 G2	Win 10 pro	9/05/2022 17:00	Intel(R) Core(TM) i7- 6700T CPU @	8 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
				20-in Non-Touch AiO			2.80GHz		ofimatica shopos outlook messenger generador de informes
URGTRI AGE	900200170	Clinica > urgencias 1 piso	MXL122 1JBC	HP Omni Pro110 AiO PC	Win 10 pro	16/08/2022 10:39	Pentium(R) Dual-Core CPU E5800 @ 3.20GHz	4 Gb	Sima /consulta médica ambulatoria derechos triage historia de evolucion ofimatica shopos outlook messenger

*Nota.* Datos tomados del área de recursos humanos de la Clínica Proinsalud que corresponde a los equipos de cómputo con sus respectivas características de hardware como software y su ubicación.

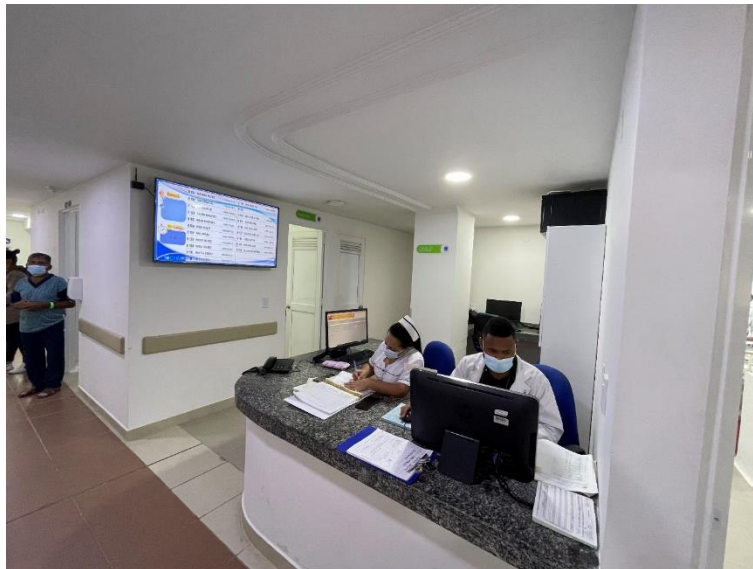
**2.1.2.2. Hospitalización.** Cuidado personalizado que hace parte del modelo de atención médica requerido en toda la estancia hospitalaria.

La Clínica Proinsalud S.A cuenta con 3 pisos de hospitalización los cuales se dividen en área de quirúrgicas, área de medicina interna, área de ginecología como se muestra en la figura 12. Las instalaciones son confortables para brindar atención a los usuarios adultos y al binomio madre-hijo, en habitaciones unipersonales y bipersonales. El personal está altamente calificado en la atención de especialidades quirúrgicas y clínicas, así como subespecialidades de adultos y pediátricos, con lo cual se garantiza un servicio en salud con los más altos estándares de calidad y humanismo.

La Clínica Proinsalud S.A ofrece el servicio de hospitalización para adultos, servicios de maternidad y unidades de cuidado intensivo médica, y neonatal.

### Figura 12

*Área de hospitalización*



*Nota.* La figura corresponde a los equipos de cómputo los cuales están ubicados en el área de urgencias.

**Tabla 19***Inventario del área de hospitalización*

Nombre	Número de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
Fac1piso	1300178	Clinica > ginecologia 1 piso	UYVA82 316290	OEM	Win 7 pro	1/08/2022 0:27	Intel(R) Core(TM)2 Duo CPU E7200 @ 2.53GHz	2 Gb	Sima / Facturacion consultas generales derechos sophos outlook messenger
FACUAU X002	123456	Clinica > ginecologia 1 piso	MXL246 7KTR	HP Compaq Pro 4300 AiO 20 PC	Win 10 pro	11/03/2022 13:31	Intel(R) Core(TM)2 Duo CPU T6570 @ 2.10GHz	3 Gb	Sima / Facturacion consultas generales derechos sophos outlook messenger
HOSP1M ED	900200527	Clinica > ginecologia 1 piso	MXL527 1GSZ	HP ProOne 400 G1 AiO	Win 10 pro	1/08/2022 0:24	Intel(R) Core(TM) i7- 4770T CPU @ 2.50GHz	8 Gb	Sima historia de evolucion oviyam outlook messenger sophos consultas generales
HOSP1_A UX01	1301121	Clinica > ginecologia 1 piso	MJ0DZX 33	ThinkCentre M70q	Win 10 pro	11/03/2022 13:38	Intel(R) Core(TM) i5- 10400T CPU @ 2.00GHz	8 Gb	Sima historia de evolucion oviyam outlook messenger sophos consultas



Nombre	Número de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
									generales
HOSPI_A UX02	1301123	Clinica > ginecologia 1 piso	MJ0DZX 36	ThinkCentre M70q	Win 10 pro	11/03/2022 20:00	Intel(R) Core(TM) i5- 10400T CPU @ 2.00GHz	8 Gb	Sima historia de evolucion oviyam outlook messenger sophos consultas generales
HOSPIA UX01	1301121	Clinica > ginecologia 1 piso	MJ0D2X 33	Lenovo CPU thinkcentre core I5	Win 10 pro	9/09/2021 17:20			Sima historia de evolucion oviyam outlook messenger sophos consultas generales
HOSPIA UX03	1301128	Clinica > ginecologia 1 piso	MJ0DZX 2Q	ThinkCentre M70q	Win 10 pro	25/08/2022 11:06	Intel(R) Core(TM) i5- 10400T CPU @ 2.00GHz	8 Gb	Sima historia de evolucion oviyam outlook messenger sophos consultas generales
HOS2AU X02	1301122	Clinica > hospitalizacion 2 piso	MJ0DZX 38	ThinkCentre M70q	Win 10 pro	22/03/2022 14:02	Intel(R) Core(TM) i5- 10400T CPU @ 2.00GHz	8 Gb	Sima historia de evolucion oviyam outlook messenger sophos consultas generales
HOSP2A	1301129	Clinica >	MJ0DZX	ThinkCentre	Win	1/05/2022	Intel(R)	8 Gb	Sima historia de

Nombre	Número de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
UX01		hospitalizacion 2 piso	3D	M70q	10 pro	9:00	Core(TM) i5- 10400T CPU @ 2.00GHz		evolucion outlook sophos generales oviyam messenger consultas
HOSP2JE F	1300865	Clinica > hospitalizacion 2 piso	MXL248 0KTR	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	9/05/2022 16:57	Intel(R) Core(TM) i3- 3220 CPU @ 3.30GHz	6 Gb	Sima historia de evolucion outlook sophos generales oviyam messenger consultas

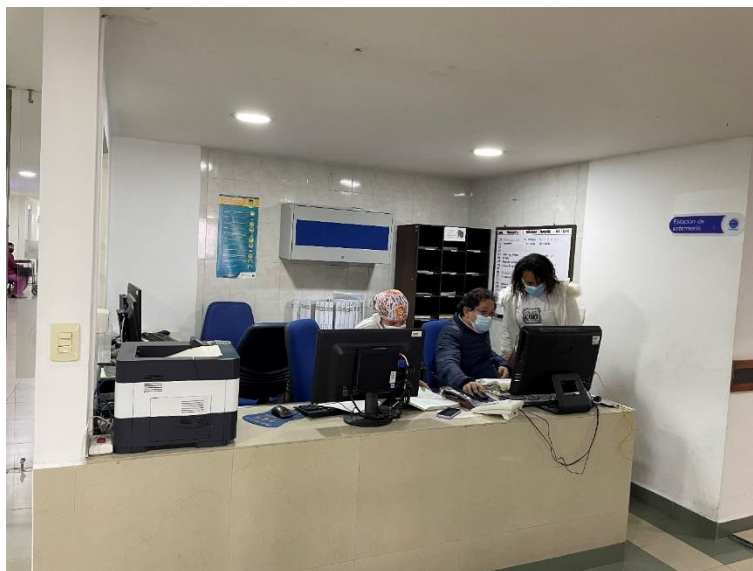
*Nota.* Datos tomados del área de hospitalización de la Clínica Proinsalud que corresponde a los equipos de cómputo con sus respectivas características de hardware como software y su ubicación.

**2.1.2.3. Quirófano.** El área de quirófano de la Clínica Proinsalud ubicada en el tercer piso, cuenta con un acceso directo a la unidad de cuidados intensivos, quirófano cuenta con una estación medica como se muestra en la figura 13, el inventario de los equipos de quirófano se puede evidenciar en la tabla 20. El área cuenta con profesionales idóneos en todas las especialidades quirúrgicas. Sus procesos estandarizados de calidad, seguridad y manejo de dolor, contribuyen a la pronta recuperación de los pacientes.

Todas las cirugías, la mayoría de alta complejidad, se realizan con técnicas quirúrgicas y anestésicas avanzadas y seguras que permiten que la mayor parte del posoperatorio de los pacientes.

### Figura 13

*Área de quirófano*



*Nota.* La figura corresponde a los equipos de cómputo los cuales están ubicados en el área de quirófano.

**Tabla 20***Inventario del área de Quirófano*

Nombre	Número de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
ESTQX02	900200169	Clinica > quirófano 3 piso	MXL12 70BQH	HP Omni Pro110 AiO PC	Win 7 pro	1/08/2022 0:54	Pentium(R) Dual-Core CPU E5800 @ 3.20GHz	4 Gb	Sima / consulta médica ambulatoria quirófano historia de evolucion ofimatica sophos outlook messenger
Facqux01	1300189	Clinica > quirófano 3 piso	MXL92 00HQK	HP Compaq dx2400 Microtower	Win 7 pro	1/08/2022 0:50	Pentium(R) Dual-Core CPU E5200 @ 2.50GHz	4 Gb	Sima / facturacion derechos consultas generales ofomatica outlook messenger
faroste01	1300117	Clinica > quirófano 3 piso		N68S3B	Win 7 pro	1/08/2022 0:50	AMD Sempron(tm) 130 Processor	2 Gb	Sima / consulta médica ambulatoria quirófano historia de evolucion ofimatica sophos outlook messenger
Quiraux01	900200146	Clinica > quirófano 3	MXL1 221J6Y	HP Omni Pro110 AiO PC	Win 7 pro	22/08/2022 22:51	Pentium(R) Dual-Core CPU	4 Gb	Sima / consulta médica ambulatoria

Nombre	Número de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
		piso					E5800 @ 3.20GHz		quirofano historia de evolucion ofimatica sophos outlook messenger
Quirjefe	1300868	Clinica > quirofono 3 piso	MXL24 80KXS	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	1/08/2022 0:52	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	4 Gb	Sima / consulta médica ambulatoria quirofono historia de evolucion ofimatica sophos outlook messenger generador de informes
QUIROFA NO02	1301126	Clinica > quirofono 3 piso	MJ0DZX 37	ThinkCentre M70q	Win 10 pro	24/03/2022 18:18	Intel(R) Core(TM) i5-10400T CPU @ 2.00GHz	8 Gb	Sima / consulta médica ambulatoria quirofono historia de evolucion ofimatica sophos outlook messenger
QUIROFA NO03	1301127	Clinica > quirofono 3 piso	MJ0DZX 5S	ThinkCentre M70q	Win 10 pro	11/03/2022 13:00	Intel(R) Core(TM) i5-10400T CPU @ 2.00GHz	8 Gb	Sima / consulta médica ambulatoria quirofono historia de evolucion ofimatica

Nombre	Número de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
									sophos outlook messenger
QXAUX01	1300822	Clinica > quirofono 3 piso	MXL248 0KTH	HP Compaq Pro 4300 AiO 20 PC	Win 7 pro	1/08/2022 0:54	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	4 Gb	Sima / consulta médica ambulatoria quirofono historia de evolucion ofimatica sophos outlook messenger
qxaux02	900200163	Clinica > quirofono 3 piso	MXL12 21J7R	HP Omni Pro110 AiO PC	Win 7 pro	1/08/2022 0:53	Pentium(R) Dual-Core CPU E5800 @ 3.20GHz	4 Gb	Sima / consulta médica ambulatoria quirofono historia de evolucion ofimatica sophos outlook messenger
QXPREST AMO	1301062	Clinica > quirofono 3 piso	K2N0CX 06M847 09A	VivoBook_AS US Laptop X505ZA_X505 ZA	Win 10 hom	9/08/2022 15:43	AMD Ryzen 5 2500U with Radeon Vega Mobile Gfx	8 Gb	ima / consulta médica ambulatoria quirofono historia de evolucion ofimatica sophos outlook messenger

*Nota.* Datos tomados del área de quirófano de la Clínica Proinsalud que corresponde a los equipos de cómputo con sus respectivas características de hardware como software y su ubicación

**2.1.2.4. Unidad de Cuidado Intensivo (UCI).** El departamento UCI ubicada en el tercer piso tiene un espacio de 3 tres equipos de cómputo encargados de la recepción de los pacientes como se muestra la figura 14, otra área que se encarga del monitoreo que se compone de 6 equipos de cómputo las características de los equipos que componen toda el área están descritos en la tabla 21. La unidad de cuidados intensivos se encarga de una atención especial con problemas de salud de diagnósticos mortales ya que los pacientes que ingresan a esta área necesitan de monitoreo y tratamientos constantes. (este departamento esta dividido en dos áreas uno para personas mayores y el otro para bebés recién nacidos).

El área de Unidad de Cuidado Intensivo (UCI) en una clínica es un espacio especializado diseñado para brindar atención médica crítica y supervisión continua a pacientes que requieren cuidados intensivos. La UCI está diseñada para tratar a pacientes con enfermedades graves o lesiones que ponen en peligro su vida, y por lo tanto requieren una atención médica especializada y personalizada. El objetivo principal de la UCI es proporcionar una atención médica avanzada y altamente especializada a pacientes con afecciones graves o que están en peligro de vida.

#### **Figura 14**

*Área de UCI*



*Nota.* La figura corresponde a los equipos de cómputo los cuales están ubicados en el área de quirófano.

**Tabla 21***Inventario del área de UCI.*

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.O	Última actualización	Componentes - Procesador	Memoria	Programas
UciAdultos001	1300999	Clinica > uci adultos 3 piso	S1H052YU	10QH0006LS	Win 10 pro	1/08/2022 0:43	Intel(R) Core(TM) i5-7400 CPU @ 3.00GHz	4 Gb	Sima / historia de evolucion / oviyam / Ofimatica / sophos /outlook messenger
UCIAJE FE01	1301093	Clinica > uci adultos 3 piso	8CC02908BV	HP All-in-One	Win 10 hom	12/08/2022 10:13	Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz	8 Gb	Sima / historia de evolucion / oviyam / Ofimatica / sophos /outlook messenger
UCIAM ED01	1301144	Clinica > uci adultos 3 piso	MJ0DZX64	ThinkCentre M70q	Win 10 pro	10/03/2022 17:02	Intel(R) Core(TM) i5-10400T CPU @ 2.00GHz	8 Gb	Sima / historia de evolucion / oviyam / Ofimatica / sophos /outlook messenger
uciint01	1300858	Clinica > uci adultos 3 piso	MXL2480KX F	HP Compaq Pro 4300 AiO 20 PC	Win 10 pro	7/08/2022 13:02	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	4 Gb	Sima / historia de evolucion / oviyam / Ofimatica / sophos /outlook messenger



Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
									messenger
UCINAU X01	1300798	Clinica > uci neonatos 3 piso	S1H049LS	ThinkCentre E73z	Win 10 pro	1/08/2022 0:47	Intel(R) Core(TM) i5- 4460T CPU @ 1.90GHz	4 Gb	Sima / historia de evolucion / oviyam / Ofimatica / sophos /outlook messenger
UCINAU X02	1301138	Clinica > uci neonatos 3 piso	MJ0DZX2W	ThinkCentre M70q	Win 10 pro	25/03/2022 13:04	Intel(R) Core(TM) i5- 10400T CPU @ 2.00GHz	8 Gb	Sima / historia de evolucion / oviyam / Ofimatica / sophos /outlook messenger
UCINAU X03	900200202	Clinica > uci neonatos 3 piso	MXL1210FS B	HP Omni Pro110 AiO PC	Win 10 pro	1/08/2022 0:45	Pentium(R) Dual-Core CPU E5800 @ 3.20GHz	4 Gb	Sima / historia de evolucion / oviyam / Ofimatica / sophos /outlook messenger
UCINJE FE01	1300892	Clinica > uci neonatos 3 piso	MXL70330N R	HP ProOne 400 G2 20-in Non-Touch AiO	Win 10 pro	1/08/2022 0:46	Intel(R) Core(TM) i5- 6500 CPU @ 3.20GHz	8 Gb	Sima / historia de evolucion / oviyam / Ofimatica / sophos /outlook messenger
UCITER	1300833	Clinica > uci	MXL2480K	HP Compaq	Win	9/05/2022	Intel(R)	4 Gb	Sima / historia de

Nombre	No. de inventario	Localización	Número de serie	Modelo	S.0	Última actualización	Componentes - Procesador	Memoria	Programas
	01	adultos 3 piso	WW	Pro 4300 AiO 20 PC	10 pro	16:49	Core(TM) i3- 3220 CPU @ 3.30GHz		evolucion / oviyam / Ofimatica / sophos /outlook messenger

*Nota.* Datos tomados del área de UCI de la Clínica Proinsalud que corresponde a los equipos de cómputo con sus respectivas características de hardware como software y su ubicación.





## 2.2. Análisis y evaluación de amenazas, riesgos y vulnerabilidades con metodología Magerit

La metodología Magerit ha sido empleada en la Clínica Proinsalud para identificar los activos importantes, evaluar su valor y determinar el nivel de riesgo asociado con su posible deterioro. Para llevar a cabo este proceso, se ha comenzado por realizar un inventario de los equipos de las diferentes áreas de la clínica. Posteriormente, se ha procedido a aplicar la metodología para llevar a cabo un análisis detallado de los activos.

En este sentido, se han investigado los diferentes aspectos que conforman la metodología Magerit, permitiendo valorar las distintas dimensiones de seguridad de los equipos, como sus aplicaciones, información y bases de datos. De esta manera, se han obtenido resultados precisos y detallados acerca del nivel de riesgo asociado con cada uno de los activos, lo que permitirá a la clínica Proinsalud tomar decisiones informadas y eficaces para garantizar la seguridad y protección de sus recursos. En la tabla 22 se determina el tipo de riesgo de dichos activos.

**Tabla 22**

*Tipos de riesgos*

Tipos	Concepto	Color
Tipo de riesgo 9-10	Riesgos muy probables y de muy alto impacto.	
Tipo de riesgo 2-3-4-5	Este tipo de riesgo cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo.	
Tipo de riesgo 0-1	Son riesgos improbables y de bajo impacto.	
Tipo de riesgo 6-7-8	Riesgos improbables, pero de muy alto impacto	

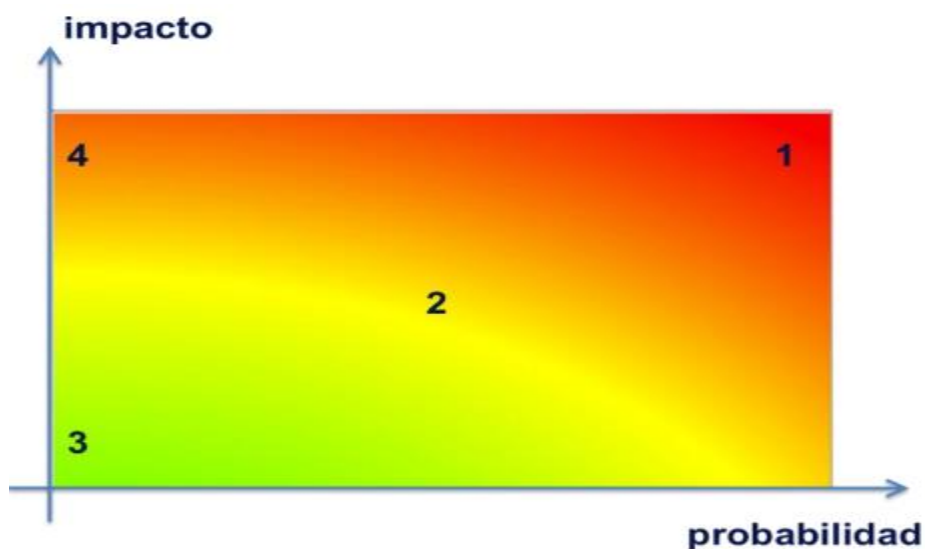
*Nota.* la tabla representa los riesgos que se pueden encontrar a la hora de analizar software como hardware.

Una vez identificados los riesgos de los activos se procede a determinar el nivel de amenaza que puede llegar a afectar los activos, teniendo en cuenta que los tipos de amenazas son de origen natural, origen industrial, fallas en las aplicaciones y origen humano.

En la figura 15 se observa los sectores por color dependiendo en impacto que vaya a tener los activos al no tener salvaguardas la cual mitiga la probabilidad de sufrir daños.

**Figura 15**

*Zonas de riesgos con respecto al impacto y la probabilidad*



*Nota.* La figura muestra los sectores por color dependiendo en impacto que vaya a tener los activos al no tener salvaguardas la cual mitiga la probabilidad de sufrir daños.

En esta figura cada número corresponde a una zona, es decir:

- Zona 1: Riesgo crítico con alta probabilidad de impacto
- Zona 2: Riesgo improbables y con impacto medio
- Zona 3: Riesgo improbable y con impacto bajo
- Zona 4: riesgo improbable y con impacto muy alto

Al ubicar las zonas de riesgo se procede a se determina que salvaguardas o controles existen actualmente en la Clínica Proinsalud y ver qué nivel de riesgo posee cada área. Al identificar los controles y salvaguardas se procede a determinar criterios de evaluación de la metodología Magerit en donde se asigna en una escala de 0 a 10 para valorar los activos teóricamente como muestra en la tabla 23.

**Tabla 23***Criterios de valoración*

Valor	Daño	Criterio
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

*Nota.* La tabla representa una evaluación en una escala de 0 a 10 de los riesgos que puede sufrir hardware y software mediante las dimensiones de seguridad.

La seguridad es la capacidad de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos de los servicios que dichos y sistemas ofrecen o hacen accesibles (Magerit, 2012). Mediante estos criterios se mide la fiabilidad de la información a continuación en grafica se ilustra los criterios de la dimensión de seguridad.

**Tabla 24***Dimensiones de seguridad*

D	Disponibilidad
I	Integridad
C	Confidencialidad
A	Autenticidad
T	Trazabilidad

*Nota.* estas dimensiones de seguridad caracterizan a los activos para un mayor entendimiento a la hora de aplicar la metodología Magerit.

### ***2.2.1. Análisis de vulnerabilidades riesgos y amenazas aplicando criterios de valoración por color del valor y las dimensiones de seguridad***

Por medio de la metodología Magerit y tomando esta como herramienta de evaluación hacia los criterios de seguridad de la información en La Clínica Proinsalud pudimos realizar una lista de verificación de las incidencias más comunes estandarizadas por la metodología Magerit para de esta forma determinar y evaluar el riesgo de la información. Teniendo en cuenta el valor de amenazas enmarcados en la metodología. los cuales son. Impacto potencial el cual representa el posible daño que puede suceder, impacto actual se representa lo que está sucediendo en el momento y el impacto repercutido es el daño que puede causar afectaciones a los demás activos, estas amenazas se miden con las dimensiones de seguridad que en este caso fueron elegidas las tres más importantes que son Disponibilidad, integridad y confidencialidad.

Al tener en cuenta la identificación de amenazas de la metodología en la cada área a estudiar se dividieron en cuatro tablas en las cuales representa una diferente amenaza sobre los activos.

### ***2.2.2. Área pagaduría***

**2.2.2.1. Amenazas por desastre natural.** La presente tabla de la metodología Magerit es muy importante para la evaluación del riesgo de la información de la Clínica Proinsalud. Es de suma importancia ya que la ciudad de san juan de pasto se encuentra en un riesgo inminente a desastre natural por inferencia del Volcán Galeras.

Por lo tanto, se procede a realizar un análisis detallado de todas las injerencias naturales que puedan afectar el normal desarrollo de la información el diligenciamiento el orden y la gestión de dicha información.

En el área de pagaduría se evidencia el riesgo de desastres naturales donde se puede evidenciar que el riesgo más crítico es sobre las instalaciones ya que como todos sabemos la Clínica Proinsalud se encuentra ubicada en la ciudad de pasto la cual está en un alto riesgo de erupción volcánica

**Figura 16**




Análisis de Amenazas y riesgos del área de pagaduría.

AREA PAGADURIA AMENAZAS POR DESASTRE NATURAL									
[N]Desastres naturales	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[N1] fuego d									
[HW] equipos informáticos (hardware)	2			0			10		
[Media] soportes de información	2			0			10		
[AUX] equipamiento auxiliar	2			0			10		
[L] instalaciones	2			0			10		
[N2] Daños por agua d									
[HW] equipos informáticos (hardware)	2			0			10		
[Media] soportes de información	2			0			10		
[AUX] equipamiento auxiliar	2			0			10		
[L] instalaciones	2			0			10		
[N.*] Desastres naturales d									
[HW] equipos informáticos (hardware)	8			0			10		
[Media] soportes de información	3			0			10		
[AUX] equipamiento auxiliar	2			0			10		
[L] instalaciones	10			0			10		

Nota. los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de contabilidad de La Clínica Proinsalud.

**Tabla 25**

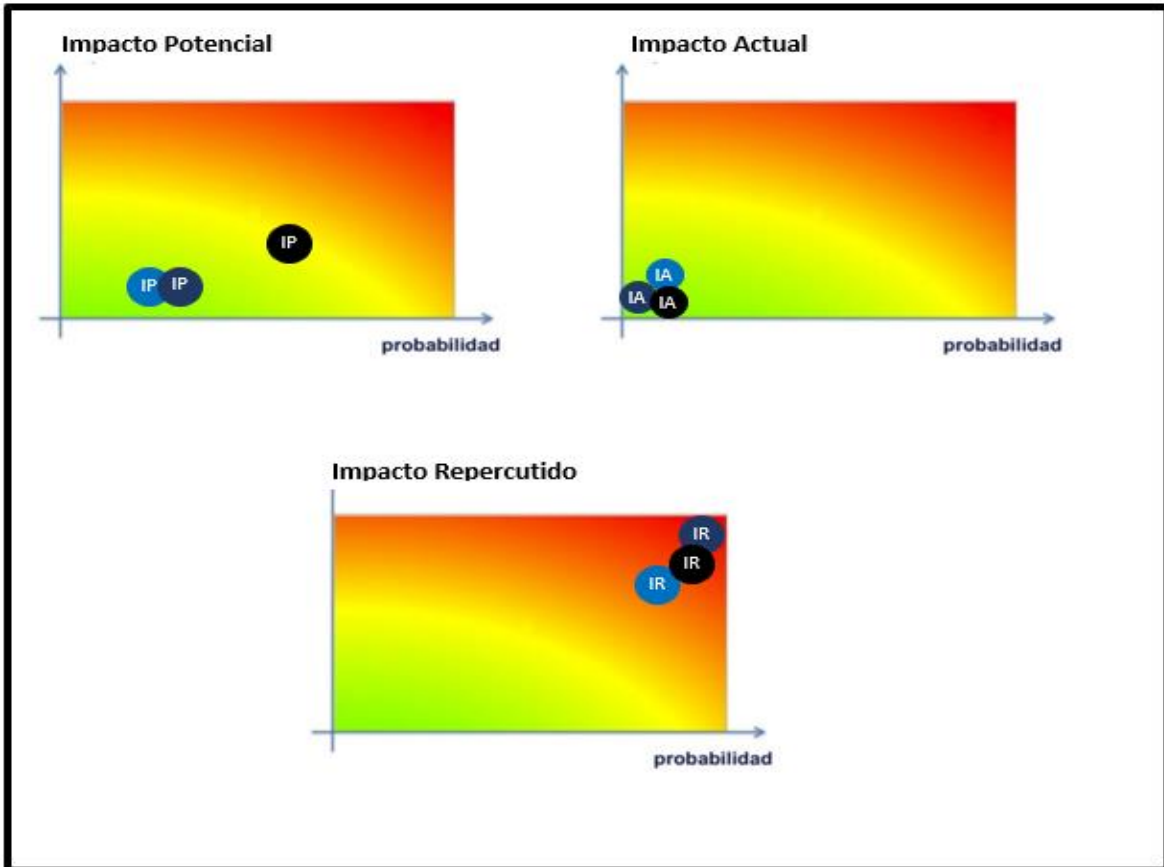
Indicadores de los tipos de impacto de las tablas analizadas con Magerit.

Desastres naturales		Tipos de impacto	
	Daños por fuego	<b>IP</b>	Impacto Potencial
	Daños por agua	<b>IA</b>	Impacto Actual
	Desastres naturales	<b>IR</b>	Impacto Repercutido

Nota. En la tabla se muestra cada uno de las amenazas por desastres naturales de acuerdo al tipo de impacto analizado con la mitología Magerit.

**Figura 17**

*Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas*



El anterior mapa de calor muestra las amenazas por desastre natural en el área de pagaduría de la Clínica Poin salud, evaluando los riesgos teniendo en cuenta los impactos. Se puede observar que, para el impacto potencial, los riesgos se encuentran controlados y estables, al igual que para el impacto actual. Sin embargo, el mapa de calor muestra que, para el impacto repercutido, existen grandes falencias y se presenta un riesgo crítico de pérdida de información por los ítems evaluados.

**2.2.2.2. Amenazas por origen industrial.** La presente tabla de la metodología Magerit donde se aborda los riesgos del origen industrial es en la cual se realiza una evaluación de los riesgos por incidencia o dependencia del hombre para de esta manera evaluar y mitigar las



posibles falencias al que se encuentra expuesto por el actuar de la mano de trabajo humana.

En el área de pagaduría de la clínica Proinsalud podemos observar que unos de los puntos críticos que nos arroja la tabla son las instalaciones eléctricas, como también los soportes de información los cuales se evidencia que son las copias de seguridad realizadas por cada uno de los empleados de la Clínica Proinsalud.

**Figura 18**








*Análisis de Amenazas y riesgos por origen industrial del área de pagaduría.*

AREA PAGADURIA AMENAZAS POR ORIGEN INDUSTRIAL									
[I]Origen industrial	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[11] fuego d									
[HW] equipos informáticos (hardware)	2			0			10		
[Media] soportes de información	9			6			10		
[AUX] equipamiento auxiliar	9			10			10		
[L] instalaciones	10			0			10		
[12] Daños por agua d									
[HW] equipos informáticos (hardware)	10			8			10		
[Media] soportes de información	10			9			10		
[AUX] equipamiento auxiliar	8			10			10		
[L] instalaciones	10			0			10		
[13] Contaminación mecánica d									
[HW] equipos informáticos (hardware)	8			9			10		
[Media] soportes de información	9			6			10		
[AUX] equipamiento auxiliar	6			4			10		
[15] Avería de origen físico o lógico									
[HW] equipos informáticos (hardware)	9			10			10		
[HS] equipos informáticos (software)	8			8			10		
[Media] soportes de información	6			5			8		
[AUX] equipamiento auxiliar	3			3			6		
[16] Corte del suministro eléctrico d									
[HW] equipos informáticos (hardware)	7			5			10		
[Media] soportes de información	3			2			7		
[AUX] equipamiento auxiliar	2			2			7		
[18] Fallo de servicios de comunicaciones									
[COM]redes de cominucaciones	10			10			10		
[111] Emanaciones electromagnéticas c									
[HW] equipos informáticos (hardware)			2			0			10
[HS] equipos informáticos (software)			2			0			10
[Media] soportes de información			2			0			10
[AUX] equipamiento auxiliar			2			0			10

*Nota.* los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de contabilidad de La Clínica Proinsalud.

**Tabla 26**

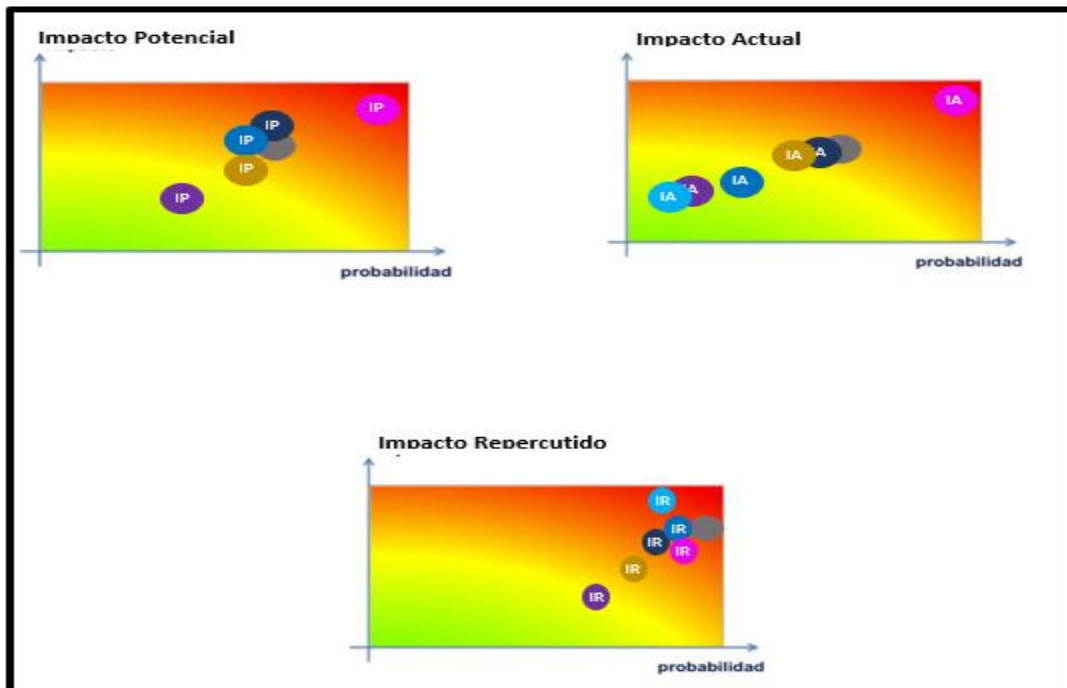
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit.*

Origen industrial		Tipos de impacto	
	Daños por fuego	IP	Impacto Potencial
	Daños por agua	IA	Impacto Actual
	Contaminación Mecánica	IR	Impacto Repercutido
	Avería de origen físico o lógico		
	Corto del suministro eléctrico		
	Fallo de servicio de comunicaciones		
	Emanaciones Electromagnéticas		

*Nota.* En la tabla se muestra cada uno de las amenazas por errores y fallos no intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit.

**Figura 19**

*Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas*



El mapa de calor anterior muestra las amenazas por origen industrial en el área de pagaduría de la Clínica Poin salud, evaluando los riesgos y teniendo en cuenta los impactos. Se puede observar que, para el impacto potencial, los riesgos se encuentran por mejorar, ya que existe un alto riesgo de pérdida de información. Para el impacto repercutido, se presentan grandes falencias y existe un riesgo crítico de pérdida de información por los ítems evaluados.

**2.2.2.3. Amenazas por errores y fallos no intencionados.** La presente tabla indica los riesgos más comunes que se pueden presentar en una entidad estos riesgos se presentan de unos fallos no intencionados o que no dependen del obrar humano.

En la clínica Proinsalud se evidencia este tipo de fallos según el análisis realizado en los aplicativos los cuales pueden tener fallas y no arrojar los datos estadísticamente adecuados lo que conlleva a una toma de decisiones gerenciales erróneas. Un punto a tener en cuenta en estos fallos no intencionados son los equipos de red que puede dejar de prestar servicio en momentos puntuales así se les esté realizando una revisión periódica y un mantenimiento programado en cronograma de mantenimientos.

**Figura 20**












*Análisis de amenazas y riesgos por errores y fallos no intencionados. Área de Contabilidad*

AREA PAGADURIA AMENAZAS POR ERRORES Y FALLOS NO INTENCIONADOS									
[E] Errores y fallos no intencionados	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[E1] Errores de los usuarios									
[D] datos / información 3	7	9	3	7	8	5	6	5	3
[keys] claves criptográficas 3	6	5	7	9	9	4	7	6	5
[S] servicios 3	5	6	8	6	7	5	8	7	6
[SW] aplicaciones (software) 3	8	9	6	9	8	4	8	7	5
[Media] soportes de información 3	7	8	9	8	6	4	7	8	4
[E3] Errores de monitorización (log)									
[E4] Errores de configuración in		8			6			9	
[D.conf] datos de configuración in		7			4			9	
[E8] Difusión de software dañino									
[SW] aplicaciones (software) 3	10	10	10	8	9	9	10	10	10
[E9] Errores de [re-]encaminamiento									
[S] servicios c			4			4			6
[SW] aplicaciones (software) c			6			2			9
[COM]redes de comunicaciones c			9			2			10
[E14] Escapes de información c			9			5			10
[E15] Alteración accidental de la información									
[D] datos / información i		9			10			10	
[keys] claves criptográficas i		2			10			10	
[S] servicios i		3			6			10	
[SW] aplicaciones (software) i		9			8			10	
[E18] Destrucción de información									
[D] datos / información d	8			10			10		
[S] servicios d	7			6			10		
[SW] aplicaciones (software) d	9			4			10		
[COM]redes de comunicaciones d	9			5			10		
[Media] soportes de información d	9			10			10		
[E19] Fugas de información									
[D] datos / información c			10			10			10
[keys] claves criptográficas c			10			2			9
[S] servicios c			5			5			8
[SW] aplicaciones (software) c			7			2			8
[COM]redes de comunicaciones c			4			10			8
[Media] soportes de información c			5			5			10
[L] instalaciones c			10			3			7
[P] personal c			10			4			10
[E20] Vulnerabilidades de los programas (software)									
[SW] aplicaciones (software) 3	10	10	10	10	8	10	10	10	10
[E.21] Errores de mantenimiento / actualización de programas (software)									
[SW] aplicaciones (software) i d	8	6		8	9		10	10	
[E24] Caída del sistema por agotamiento de recursos									
[S] servicios d	10			10			10		
[HW] equipos informáticos (hardware) d	9			6			10		
[COM]redes de comunicaciones d	9			9			10		

*Nota.* los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de contabilidad de La Clínica Proinsalud.

**Tabla 27**

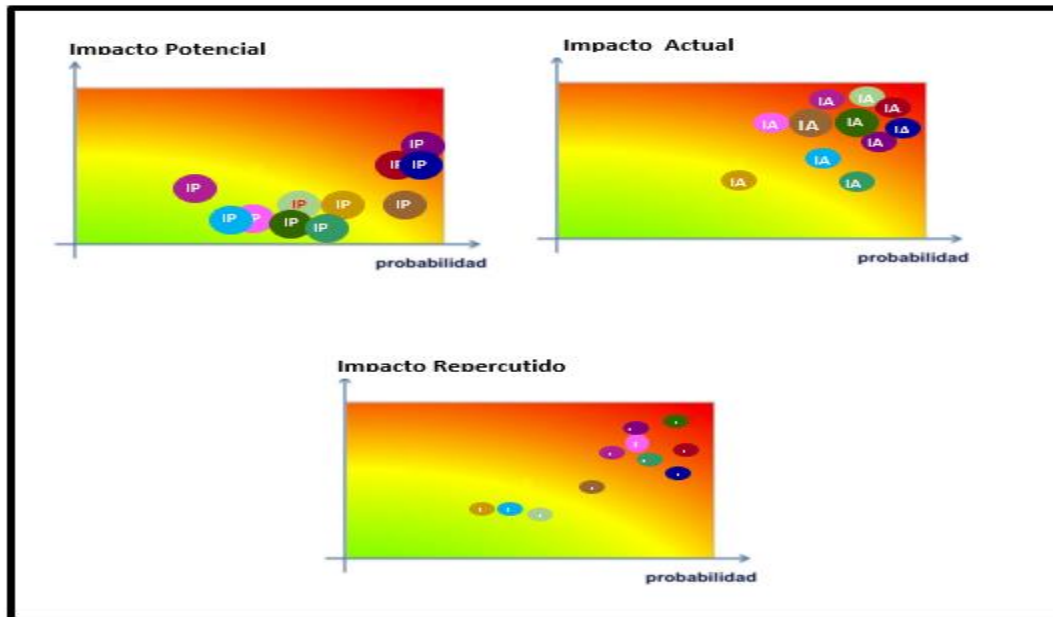
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit.*

<b>Errores y fallos no intencionados</b>		<b>Tipos de impacto</b>	
	Errores de los usuarios	<b>IP</b>	Impacto Potencial
	Errores de monitorización	<b>IA</b>	Impacto Actual
	Difusión de software dañino	<b>IR</b>	Impacto Repercutido
	Errores de Reencaminamiento		
	Escapes de información		
	Alteración accidental de la información		
	Destrucción de información		
	Fugas de información		
	Vulnerabilidades de los programas		
	Errores de mantenimiento		
	Caída del sistema por agotamiento de recursos		

*Nota.* En la tabla se muestra cada uno de las amenazas por errores y fallos no intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit.

**Figura 21**

*Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas*



El anterior mapa de calor muestra las amenazas por errores y fallos no intencionados en el área de pagaduría de la Clínica Proinsalud evaluando los riesgos se tiene en cuenta los impactos ya que se evidencia que para el impacto potencial los riesgos se encuentran un poco fuera de control yéndose más a un alto riesgo de pérdida de información.

**2.2.2.4. Amenazas por ataques intencionados.** La presente tabla de la metodología Magerit arroja los posibles riesgos que puede tener una entidad frente ataques internos o externos malintencionados y da un panorama que ayuda a mitigar por medio de protocolos y normativas la mitigación del riesgo.

Después de la evaluación realizada en el área de pagaduría se observar que un riesgo muy alto se tiene en ataques o manipulación de la información ya que esta área es la encargada de realizar pagos a los proveedores. Y una manipulación de la información obligatoria a realizar un pago indebido, resalta que se debe tener claves encriptadas lo que brindara una mayor seguridad en

movimientos bancarios los cuales deben estar estandarizados para mitigar los riesgos en el robo de la información.

**Figura 22**

















*Análisis de Amenazas y riesgos por ataques intencionados del área de Pagaduría*

AREA PAGADURIA AMENAZAS POR ATAQUES INTENCIONADOS									
[A] Ataques intencionados	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[A.3] Manipulación de los registros de actividad (log)									
[D.log] registros de actividad i		3			1			8	
[A.4] Manipulación de la configuración									
[D.log] registros de actividad 3	7	7	10	2	2	2	8	9	6
[A5] Suplantación de la identidad del usuario									
[D] datos / información 3	10	10	10	1	1	1	10	10	10
[keys] claves criptográficas 3	10	10	10	1	1	1	10	10	10
[S] servicios 3	10	10	10	1	1	1	10	10	10
[SW] aplicaciones (software) 3	10	10	10	1	1	1	10	10	10
[COM]redes de comunicaciones 3	10	10	10	1	1	1	10	10	10
[A6] Abuso de privilegios de acceso									
[D] datos / información 3	10	10	10	1	1	1	9	9	9
[keys] claves criptográficas 3	9	10	9	6	8	10	10	8	7
[S] servicios 3	7	6	9	0	0	0	8	6	5
[SW] aplicaciones (software) 3	10	10	10	7	5	10	9	8	10
[COM]redes de comunicaciones 3	9	10	9	5	5	5	10	10	10
[HW] equipos informáticos (hardware) 3	7	6	10	2	2	2	10	10	10
[A7] Uso no previsto									
[D] datos / información 3				0	0	0			
[keys] claves criptográficas 3				0	0	0			
[S] servicios 3				0	0	0			
[SW] aplicaciones (software) 3				0	0	0			
[COM]redes de comunicaciones 3				0	0	0			
[HW] equipos informáticos (hardware) 3				0	0	0			
[Media] soportes de información 3				0	0	0			
[AUX] equipamiento auxiliar 3				0	0	0			
[A8] Difusión de software dañino									
[SW] aplicaciones (software) 3	10	10	10	2	2	2	10	10	10
[A11] Acceso no autorizado									
[D] datos / información ci		10	10		6	8	10	10	10
[keys] claves criptográficas ci		8	10		3	5		8	10
[S] servicios ci		8	7		6	8		8	8
[SW] aplicaciones (software) ci		9	9		3	6		7	10
[COM]redes de comunicaciones ci		6	6		9	9		7	5
[HW] equipos informáticos (hardware) ci		9	10		10	10		10	9
[Media] soportes de información ci		6	9		3	2		7	9
[AUX] equipamiento auxiliar ci		7	9		9	8		8	10
[A12] Análisis de tráfico									
[COM]redes de comunicaciones c			8			5			7
[A15] Modificación deliberada de la información									
[D] datos / información i		10			9			9	
[keys] claves criptográficas i		9			9			9	
[S] servicios i		9			5			9	
[SW] aplicaciones (software) i		6			4			9	
[COM]redes de comunicaciones i		10			9			9	
[Media] soportes de información i		9			10			9	
[A18] Destrucción de información d									
[D] datos / información	10			9			10		
[S] servicios	8			6			10		
[SW] aplicaciones (software)	8			6			10		
[COM]redes de comunicaciones	8			0			10		
[Media] soportes de información	10			10			10		
[A19] Divulgación de información c									
[D] datos / información			8			9			10
[keys] claves criptográficas			6			5			10
[S] servicios			9			4			9
[SW] aplicaciones (software)			6			2			9
[COM]redes de comunicaciones			8			4			9
[Media] soportes de información			9			2			10
[A22] Manipulación de programas 3									
[SW] aplicaciones (software)	9	9	10	5	3	5	10	10	10
[A23] Manipulación de los equipos cd									
[AUX] equipamiento auxiliar	5		7	2		4	9		9
[COM]redes de comunicaciones	8		6	6		8	10		10
[HW] equipos	9		9	8		8	10		10
[A25] Robo cd									
[HW] equipos informáticos (hardware)	9		9	2		3	10		10
[AUX] equipamiento auxiliar	4		3	0		0	4		3
[Media] soportes de información	6		6	6		8	8		9
[A29] Extorsión 3									
[HW] equipos informáticos (hardware)	10	10	10	3	3	3	10	10	10
[P] personal interno	6	5	2	1	1	1	10	10	10
[A30] Ingeniería social 3									
[P] personal interno	10	10	10	10	10	10	10	10	10

Nota. los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de sistemas de la Clínica Proinsalud.

**Tabla 28**

*Indicadores de los tipos de impacto de las tablas analizadas con Magerit.*

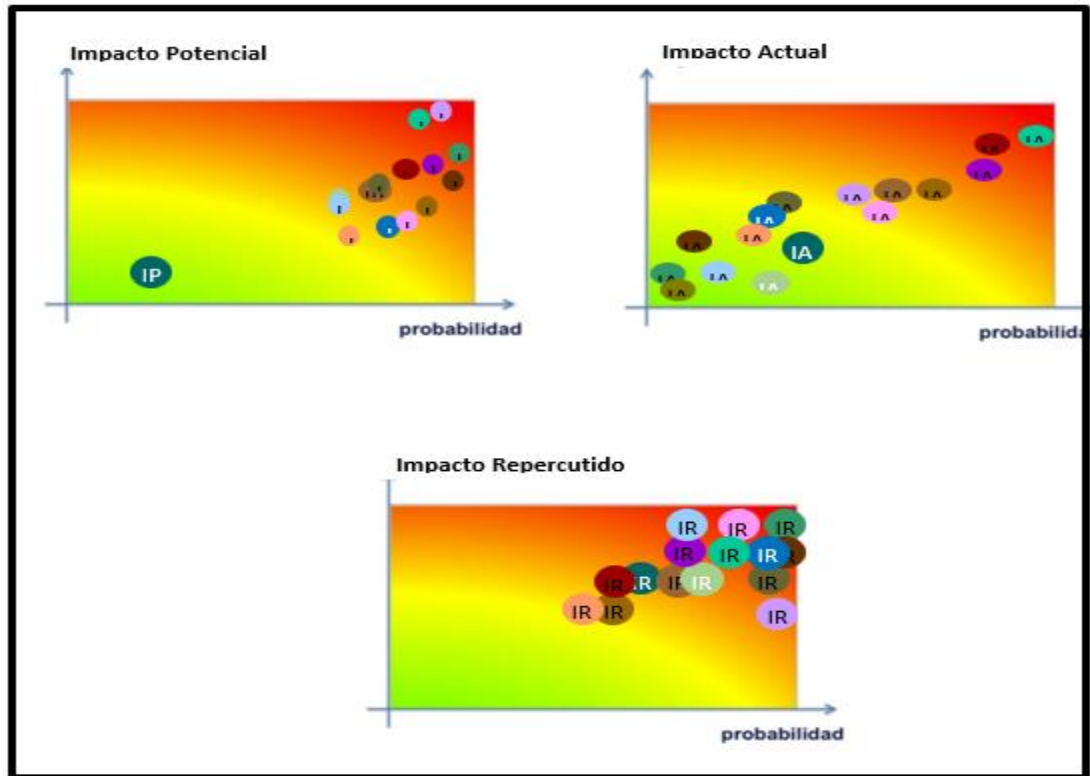
	<b>Amenazas por ataques intencionados</b>	<b>Tipos de impacto</b>
	Manipulación de los registros de actividad	<b>IP</b> Impacto Potencial
	Manipulación de la configuración	<b>IA</b> Impacto Actual
	Suplantación de la identidad del usuario	<b>IR</b> Impacto Repercutido
	Abuso de privilegios de acceso	
	Uso no previsto	
	Difusión de software dañino	
	Acceso no autorizado	
	Análisis de tráfico	
	Modificación deliberada de la información	
	Destrucción de información	
	Divulgación de información	
	Manipulación de programas	
	Manipulación de los equipos	
	Robo	
	Extorsión	
	Ingeniería social	

*Nota.* En la tabla se muestra cada uno de las amenazas o ataques intencionados de acuerdo el tipo de impacto analizado con la mitología Magerit.



**Figura 23**

*Mapas de calor de los impactos con respecto a la tabla de amenazas y riesgos por ataques intencionados del área de Pagaduría y sus respectivas amenazas*



El anterior mapa de calor muestra las amenazas por errores y fallos intencionados en el área de pagaduría de la Clínica Poinosalud evaluando los riesgos se tiene en cuenta los impactos ya que se observa que los riesgos se encuentran fuera de control esto conllevando a una pérdida de información inminente.

### 2.2.3. Área facturación

**2.2.3.1. Amenazas por desastre natural.** El área de facturación en la actualidad no presenta falencias con respecto de que el fuego acabe con recursos de los activos e incluso de que el agua afecte a los activos, ya que está en un lugar seguro.

Sin embargo, no está excepta de un desastre natural como puede ser una tormenta eléctrica, un

terremoto o daños que el volcán galeras puede causar a las instalaciones en general, mediante la metodología Magerit se tomaron varios análisis y datos que fueron útiles a la hora de calificar cada tipo que se encuentra situado en la siguiente figura.

**Figura 24**




*Análisis de Amenazas y riesgos por desastres naturales del área de facturación*

AREA FACTURACION AMENAZAS POR DESASTRE NATURAL									
[N]Desastres naturales	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[N1] fuego d									
[HW] equipos informáticos (hardware)	2			0	0	0	10		
[Media] soportes de información	2			0	0	0	9		
[AUX] equipamiento auxiliar	2			0	0	0	9		
[L] instalaciones	3			0	0	0	10		
[N2] Daños por agua d									
[HW] equipos informáticos (hardware)	2			0	0	0	10		
[Media] soportes de información	2			0	0	0	9		
[AUX] equipamiento auxiliar	3			0	0	0	9		
[L] instalaciones	3			0	0	0	10		
[N.*] Desastres naturales d									
[HW] equipos informáticos (hardware)	3			0	0	0	10		
[Media] soportes de información	2			0	0	0	9		
[AUX] equipamiento auxiliar	3			0	0	0	9		
[L] instalaciones	2			0	0	0	10		

*Nota.* los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de contabilidad de La Clínica Proinsalud.

**Tabla 29**

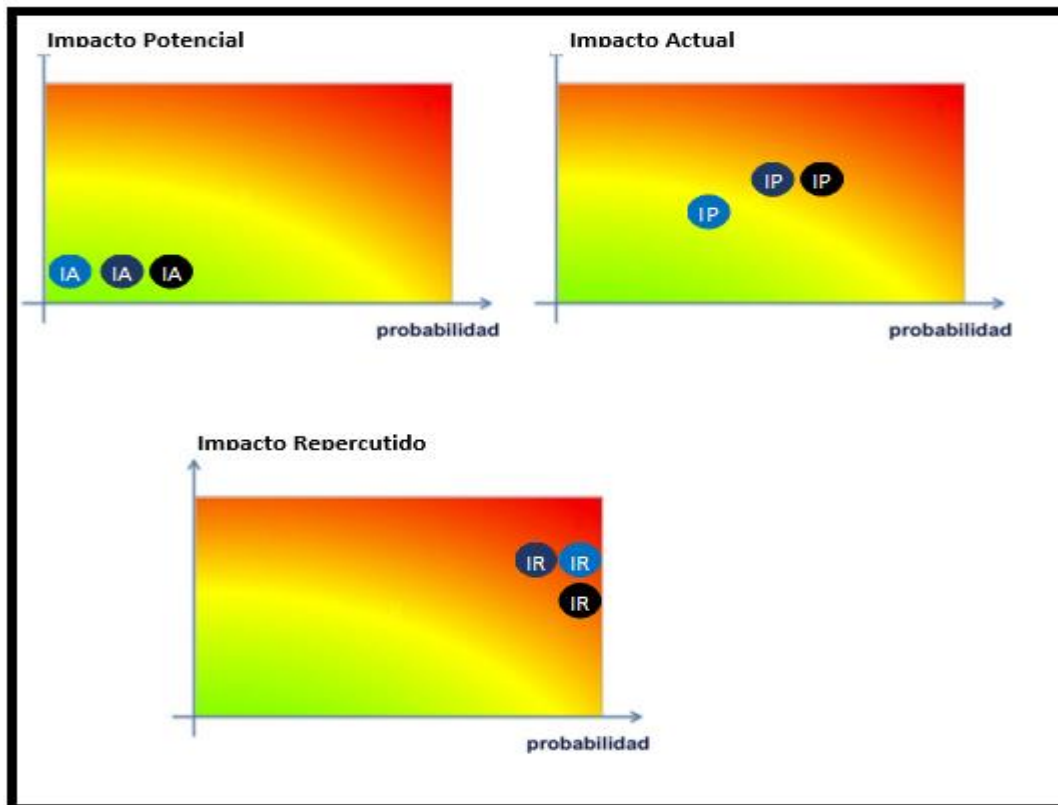
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit*

	Desastres naturales		Tipos de impacto
	Daños por fuego	<b>IP</b>	Impacto Potencial
	Daños por agua	<b>IA</b>	Impacto Actual
	Desastres naturales	<b>IR</b>	Impacto Repercutido

*Nota.* En la tabla se muestra cada uno de las amenazas por errores y fallos no intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit

**Figura 25**

*Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas*



El área de facturación con respecto a las amenazas por fallos no intencionados se encuentra en un estado crítico debido a que hay niveles en alto riesgo, por lo tanto, debe ser abordado de inmediato llevando a cabo que la fuente de riesgo donde presenta mayor inconveniente es errores de los usuarios, para ello una de las posibles soluciones se debe incluir medidas educativas y tecnológicas para minimizar la probabilidad de que los usuarios cometan errores y reducir el impacto en el sistema en caso de que los errores ocurran.

**2.2.3.2. Amenazas por origen industrial.** Las amenazas causadas por origen industrial son aquellas que vienen deliberadas por las actividades de personas externas como internas a la Clínica Proinsalud, una amenaza de estas puede ser actividades como el arreglo de una tubería o incluso la inundación por el taponamiento de alcantarillado.

Otro peligro que están expuestos los activos son arreglos internos como la soldadura la cual puede ser inflamable y ocasionar un incendio el cual pondría en peligro los activos. Después de analizar el área de facturación con la metodología Magerit se evidencia falencias, amenazas y vulnerabilidades que están presentes las cuales están enmarcadas en la siguiente figura:

**Figura 26**


*Análisis de Amenazas y riesgos por origen industrial del área de facturación*

AREA FACTURACION AMENAZAS POR ORIGEN INDUSTRIAL									
[I]Origen industrial	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[I1] fuego d									
[HW] equipos informáticos (hardware)	3			0			10		
[Media] soportes de información	10			5			10		
[AUX] equipamiento auxiliar	10			9			10		
[L] instalaciones	10			0			10		
[I2] Daños por agua d									
[HW] equipos informáticos (hardware)	10			9					
[Media] soportes de información	10			9			10		
[AUX] equipamiento auxiliar	10			9			10		
[L] instalaciones	10			0					
[I3] Contaminacion mecanica d									
[HW] equipos informáticos (hardware)	3			8			3		
[Media] soportes de información	5			7			8		
[AUX] equipamiento auxiliar	2			7			8		
[I5] Avería de origen físico o lógico									
[HW] equipos informáticos (hardware)	9			9			9		
[HS] equipos informáticos (software)	9			9			9		
[Media] soportes de información	10			4			7		
[AUX] equipamiento auxiliar	3			3			10		
[I6] Corte del suministro eléctrico d									
[HW] equipos informáticos (hardware)	4			3			2		
[Media] soportes de información	2			2			4		
[AUX] equipamiento auxiliar	7			2			7		
[I8] Fallo de servicios de comunicaciones									
[COM]redes de cominucaciones	6			1			6		
[I11] Emanaciones electromagnéticas c									
[HW] equipos informáticos (hardware)	9					0			9
[HS] equipos informáticos (software)	6					0			9
[Media] soportes de información	10					0			10
[AUX] equipamiento auxiliar	10					0			10

*Nota.* los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de contabilidad de La Clínica Proinsalud.

**Tabla 30**

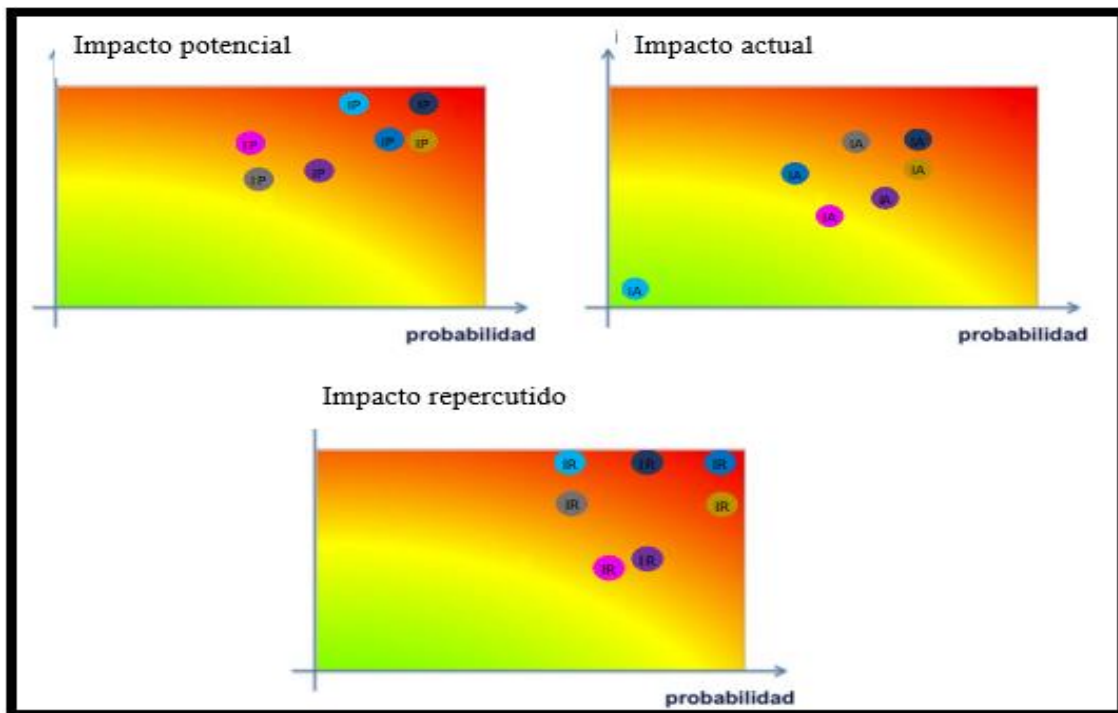
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit.*

Origen industrial		Tipos de impacto	
	Daños por fuego	<b>IP</b>	Impacto Potencial
	Daños por agua	<b>IA</b>	Impacto Actual
	Contaminación Mecánica	<b>IR</b>	Impacto Repercutido
	Avería de origen físico o lógico		
	Corto del suministro eléctrico		
	Fallo de servicio de comunicaciones		
	Emanaciones Electromagnéticas		

*Nota.* En la tabla se muestra cada uno de las amenazas por errores y fallos no intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit

**Figura 27**

*Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas*



El área de facturación con respecto a las amenazas por origen industrial se encuentra en un estado crítico debido que hay niveles en alto riesgo, por lo tanto, debe ser abordado de inmediato llevando a cabo cual es la principal fuente de riesgo e implementar la solución identificada y realizar un seguimiento para asegurarse de que el riesgo se haya eliminado o mitigado.

**2.2.3.3. Amenazas por errores y fallos no intencionados.** Con el análisis realizado al área de facturación apoyados de la metodología Magerit el estudio presenta desfases muy altos en la probabilidad de riesgos de los activos de información debido a los fallos no intencionados que ya han ocasionado pérdidas, amenazas a la hora del personal de la clínica usa equivocadamente los servicios, datos entre otros.

De esta misma manera se ve afectados los escapes de información la cual hace referencia a que la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.

**Figura 28**

*Análisis de Amenazas y riesgos por errores y fallos no intencionados del área de facturación*

AREA FACTURACION AMENAZAS POR ERRORES Y FALLOS NO INTENCIONADOS									
[E] Errores y fallos no intencionados	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[E1] Errores de los usuarios									
[D] datos / información 3	10	10	10	6	6	5	10	10	10
[keys] claves criptográficas 3	10	10	10	9	7	6	10	10	10
[S] servicios 3	10	10	10	9	6	7	10	10	10
[SW] aplicaciones (software) 3	10	10	10	9	5	6	10	10	10
[Media] soportes de información 3	10	10	10	5	5	6	10	10	10
[E3] Errores de monitorización (log)									
[E4] Errores de configuración in		10	10		3			10	
[D.conf] datos de configuración in		10	10		3			10	
[E8] Difusión de software dañino									
[SW] aplicaciones (software) 3	10	10	10	1	1	1	10	10	10
[E9] Errores de [re-]encaminamiento									
[S] servicios c			8			3			8
[SW] aplicaciones (software) c			6			5			6
[COM]redes de comunicaciones c			7			3			7
[E14] Escapes de información c			9			2			9
[E15] Alteración accidental de la información									
[D] datos / información i		10			8			10	
[keys] claves criptográficas i		10			9			10	
[S] servicios i		8			7			8	
[SW] aplicaciones (software) i		9			5			9	
[E18] Destrucción de información									
[D] datos / información d	7			9			7		
[S] servicios d	5			9			5		
[SW] aplicaciones (software) d	6			6			6		
[COM]redes de comunicaciones d	9			5			9		
[Media] soportes de información d	9			2			9		
[E19] Fugas de información									
[D] datos / información c			10			9			10
[keys] claves criptográficas c			10			8			10
[S] servicios c			6			7			6
[SW] aplicaciones (software) c			10			4			10
[COM]redes de comunicaciones c			10			5			10
[Media] soportes de información c			10			6			10
[L] instalaciones c			5			8			5
[P] personal c			7			3			7
[E20] Vulnerabilidades de los programas (software)									
[SW] aplicaciones (software) 3	10	10	10	9	5	8	10	10	10
[E.21] Errores de mantenimiento / actualización de									
[SW] aplicaciones (software) i d	9	9		9	9		9	9	9
[E24] Caída del sistema por agotamiento de recursos									
[S] servicios d	9			9			10		
[HW] equipos informáticos (hardware) d	9			9			10		
[COM]redes de comunicaciones d	6			9			10		

*Nota.* los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de contabilidad de La Clínica Proinsalud.

**Tabla 31**

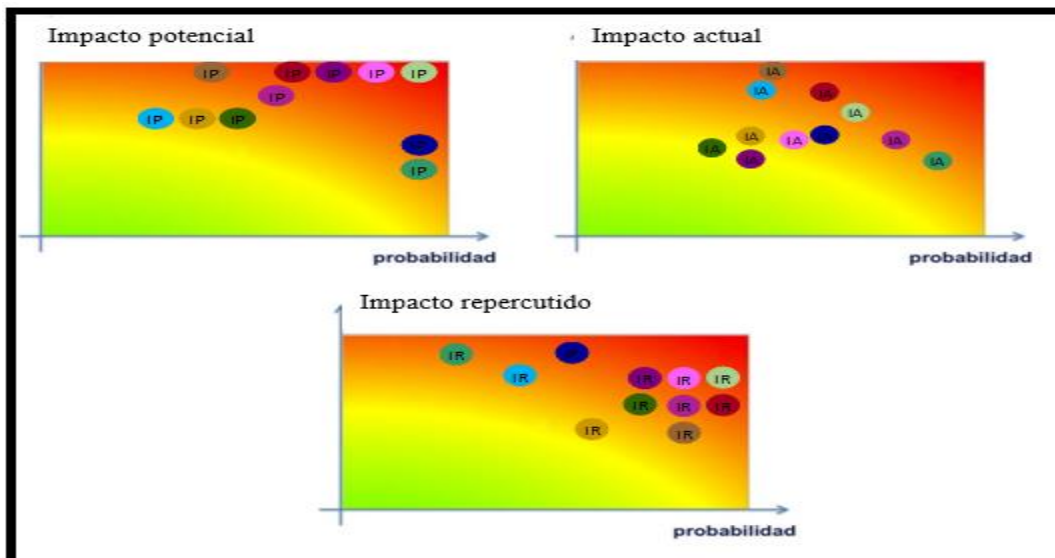
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit*

	<b>Errores y fallos no intencionados</b>	<b>Tipos de impacto</b>
●	Errores de los usuarios	<b>IP</b> Impacto Potencial
●	Errores de monitorización	<b>IA</b> Impacto Actual
●	Difusión de software dañino	<b>IR</b> Impacto Repercutido
●	Errores de Re encaminamiento	
●	Escapes de información	
●	Alteración accidental de la información	
●	Destrucción de información	
●	Fugas de información	
●	Vulnerabilidades de los programas	
●	Errores de mantenimiento	
●	Caída del sistema por agotamiento de recursos	

*Nota.* En la tabla se muestra cada uno de las amenazas por errores y fallos no intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit.

**Figura 29**

*Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas*





El área de facturación con respecto a las amenazas por fallos no intencionados se encuentra en un estado crítico debido a que hay niveles en alto riesgo, por lo tanto, debe ser abordado de inmediato llevando a cabo que la fuente de riesgo donde presenta mayor inconveniente es errores de los usuarios.

Para ello una de las posibles soluciones se debe incluir medidas educativas y tecnológicas para minimizar la probabilidad de que los usuarios cometan errores y reducir el impacto en el sistema en caso de que los errores ocurran.

**2.2.3.4. Amenazas por ataques intencionados.** En la siguiente tabla se describe las vulnerabilidades que están presentes en el área de facturación la cual tiene una alta probabilidad de amenaza e impacto hacia los activos de información de la Clínica Proinsalud, los ataques que se presentaron en la clínica fueron registrados en la tabla con un puntaje alto debido a que causaron algunos daños dentro del área, uno de los tipos que más se presentó con frecuencia fueron el acceso no autorizado que hace referencia ataques los cuales acceden a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

**Figura 30**

















*Análisis de Amenazas y riesgos por ataques intencionados del área de Contabilidad*

AREA FACTURACION AMENAZAS POR ATAQUES INTENCIONADOS									
	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[A] Ataques intencionados									
[A.3] Manipulación de los registros de actividad (log)									
[D.log] registros de actividad i	10	10	10	2	1	2	10	10	10
[A.4] Manipulación de la configuración									
[D.log] registros de actividad 3	10	10	10	2	3	2	10	10	10
[A5] Suplantación de la identidad del usuario									
[D] datos / información 3	10	10	10	2	1	2	10	10	10
[keys] claves criptográficas 3	10	10	10	1	1	1	10	10	10
[S] servicios 3	10	10	10	1	1	1	10	10	10
[SW] aplicaciones (software) 3	10	10	10	1	1	1	10	10	10
[COM]redes de comunicaciones 3	10	10	10	1	1	1	10	10	10
[A6] Abuso de privilegios de acceso									
[D] datos / información 3	8	8	8	1	1	1	8	8	8
[keys] claves criptográficas 3	8	7	6	4	4	10	8	5	6
[S] servicios 3	7	7	7	0	0	0	5	4	5
[SW] aplicaciones (software) 3	9	9	9	1	1	10	4	5	9
[COM]redes de comunicaciones 3	10	10	10	4	5	6	10	10	10
[HW] equipos informáticos (hardware) 3	10	10	10	1	1	1	10	10	10
[A7] Uso no previsto									
[D] datos / información 3				0	0	0			
[keys] claves criptográficas 3				0	0	0			
[S] servicios 3				0	0	0			
[SW] aplicaciones (software) 3				0	0	0			
[COM]redes de comunicaciones 3				0	0	0			
[HW] equipos informáticos (hardware) 3				0	0	0			
[Media] soportes de información 3				0	0	0			
[AUX] equipamiento auxiliar 3				0	0	0			
[A8] Difusión de software dañino									
[SW] aplicaciones (software) 3	10	10	10	1	1	1	10	10	10
[A11] Acceso no autorizado									
[D] datos / información ci		10	10		6	8	10	10	10
[keys] claves criptográficas ci		10	10		1	4		10	10
[S] servicios ci		10	10		3	2		10	10
[SW] aplicaciones (software) ci		10	10		4	7		10	10
[COM]redes de comunicaciones ci		10	10		5	8		10	10
[HW] equipos informáticos (hardware) ci		9	9		5	1		9	9
[Media] soportes de información ci		9	9		8	9		9	9
[AUX] equipamiento auxiliar ci		10	10		1	4		10	10
[A12] Análisis de tráfico									
[COM]redes de comunicaciones c		9	9			4		9	9
[A15] Modificación deliberada de la información									
[D] datos / información i		9			1			3	
[keys] claves criptográficas i		9			1			4	
[S] servicios i		9			1			5	
[SW] aplicaciones (software) i		9			1			9	
[COM]redes de comunicaciones i		10			1			10	
[Media] soportes de información i		10			0			10	
[A18] Destrucción de información d									
[D] datos / información	10			9			10		
[S] servicios	9			8			9		
[SW] aplicaciones (software)	8			4			8		
[COM]redes de comunicaciones	10			4			10		
[Media] soportes de información	9			3			9		
[A19] Divulgación de información c									
[D] datos / información			10		1				10
[keys] claves criptográficas			10		2				10
[S] servicios			9		5				9
[SW] aplicaciones (software)			10		5				10
[COM]redes de comunicaciones			10		1				10
[Media] soportes de información			9		1				9
[A22] Manipulación de programas 3									
[SW] aplicaciones (software)	9	9	10	2	3	2	9	9	10
[A23] Manipulación de los equipos cd									
[AUX] equipamiento auxiliar	9		9	2		3	9		9
[COM]redes de comunicaciones	10		10	2		3	10		10
[HW] equipos	9		9	3		2	9		9
[A25] Robo cd									
[HW] equipos informáticos (hardware)	10		10	3		3	10		10
[AUX] equipamiento auxiliar	10		10	0		0	10		10
[Media] soportes de información	9		9	1		2	9		9
[A29] Extorsión 3									
[HW] equipos informáticos (hardware)	10	10	10	1	1	1	10	10	10
[P] personal interno	9	8	8	1	1	1	9	8	8
[A30] Ingeniería social 3									
[P] personal interno	10	10	10	1	1	1	10	10	10

Nota. los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de contabilidad de La Clínica Proinsalud.

**Tabla 32**

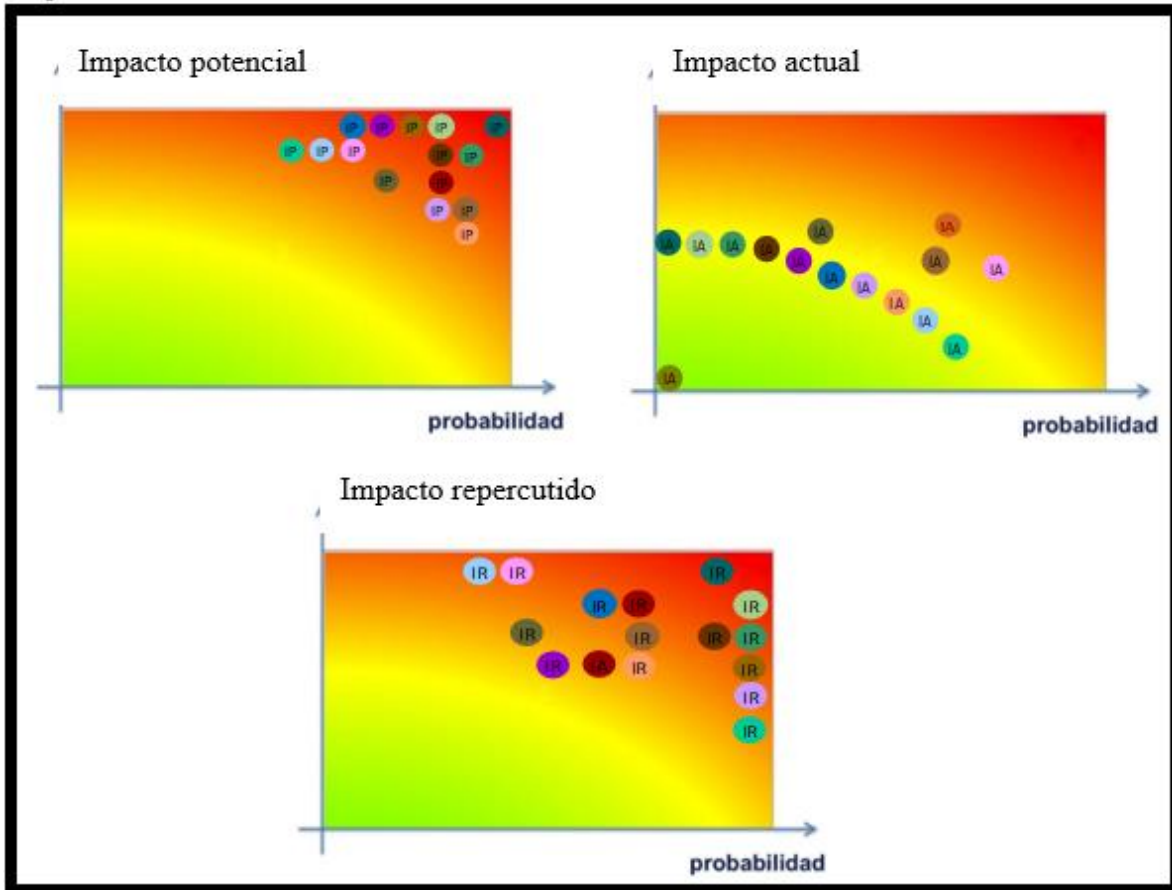
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit*

<b>Amenazas por ataques intencionados</b>		<b>Tipos de impacto</b>	
	Manipulación de los registros de actividad	<b>IP</b>	Impacto Potencial
	Manipulación de la configuración	<b>IA</b>	Impacto Actual
	Suplantación de la identidad del usuario	<b>IR</b>	Impacto Repercutido
	Abuso de privilegios de acceso		
	Uso no previsto		
	Difusión de software dañino		
	Acceso no autorizado		
	Análisis de tráfico		
	Modificación deliberada de la información		
	Destrucción de información		
	Divulgación de información		
	Manipulación de programas		
	Manipulación de los equipos		
	Robo		
	Extorsión		
	Ingeniería social		

*Nota.* En la tabla se muestra cada uno de las amenazas por errores y fallos no intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit.

**Figura 31**

*Mapas de calor de los impactos con respecto a la tabla de ataques intencionados y sus respectivas amenazas*



El área de facturación con respecto a las amenazas por ataques intencionados se encuentra en un estado crítico debido a que hay niveles en alto riesgo, por lo tanto, debe ser abordado de inmediato determinando cual es la causa principal de estos ataques, como evaluar la amenaza y para ello una vez que se hayan identificado las soluciones adecuadas, se deben implementar y llevar a cabo de forma efectiva un seguimiento para que esto no vuelva a ocurrir en la actualidad.

## 2.2.4. Área sistemas

**Figura 32**




*Análisis de Amenazas y riesgos por desastre natural del área de Sistemas*

AREA SISTEMAS AMENAZAS POR DESASTRE NATURAL									
[N]Desastres naturales	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[N1] fuego d									
[HW] equipos informáticos (hardware)	7			0			10		
[Media] soportes de información	7			0			10		
[AUX] equipamiento auxiliar	7			0			10		
[L] instalaciones	7			0			10		
[N2] Daños por agua d									
[HW] equipos informáticos (hardware)	7			2			10		
[Media] soportes de información	7			2			10		
[AUX] equipamiento auxiliar	2			2			10		
[L] instalaciones	7			2			10		
[N.*] Desastres naturales d									
[HW] equipos informáticos (hardware)	10			0			10		
[Media] soportes de información	10			0			10		
[AUX] equipamiento auxiliar	10			0			10		
[L] instalaciones	10			0			10		

*Nota.* los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de sistemas de la Clínica Proinsalud.

**Tabla 33**

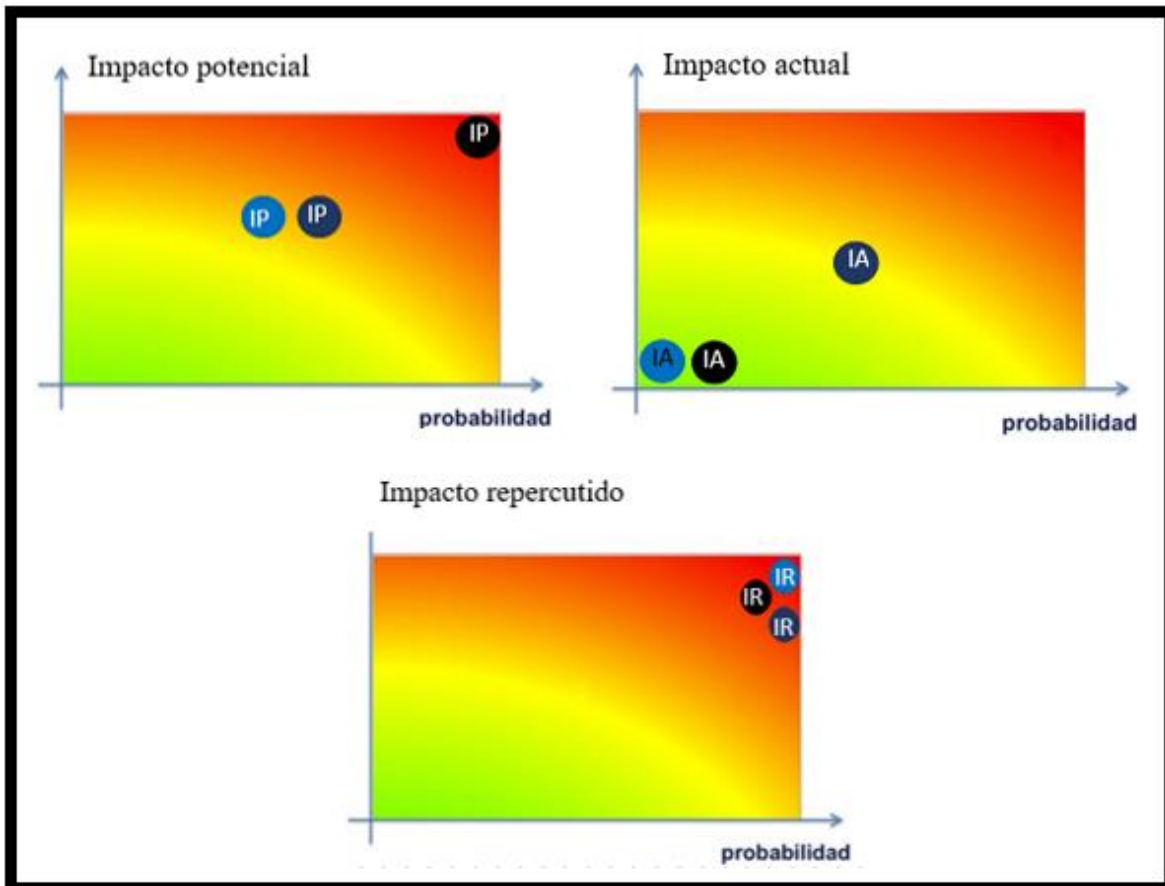
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit.*

	Desastres naturales		Tipos de impacto
	Daños por fuego	<b>IP</b>	Impacto Potencial
	Daños por agua	<b>IA</b>	Impacto Actual
	Desastres naturales	<b>IR</b>	Impacto Repercutido

*Nota.* En la tabla se muestra cada uno de las amenazas por errores y fallos no intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit.

**Figura 33**

*Mapas de calor de los impactos con respecto a la tabla de desastre natural y sus respectivas amenazas*



El área de sistemas con respecto a las amenazas por desastre natural se encuentra en un estado medio de nivel de riesgo, por lo tanto, debe ser abordado lo antes posible para minimizar su impacto, principalmente se determina cual es la causa principal, evaluar la probabilidad de que el riesgo ocurra y el impacto que tendría en el sistema para así determinar una solución para mitigar el impacto.

Se debe destacar que la gestión de riesgos es un proceso continuo y dinámico, por lo que se debe llevar a cabo una monitorización constante del sistema para asegurarse de que se mantiene seguro y protegido.

**Figura 34**








*Análisis de Amenazas y riesgos por origen industrial del área de Sistemas*

AREA SISTEMAS AMENAZAS POR ORIGEN INDUSTRIAL									
[I]Origen industrial	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[I1] fuego d									
[HW] equipos informáticos (hardware)	2			0			10		
[Media] soportes de información	2			0			10		
[AUX] equipamiento auxiliar	2			5			10		
[L] instalaciones	2			0			10		
[I2] Daños por agua d									
[HW] equipos informáticos (hardware)	6			5			10		
[Media] soportes de información	3			0			10		
[AUX] equipamiento auxiliar	6			0			10		
[L] instalaciones	3			0			10		
[I3] Contaminación mecánica d									
[HW] equipos informáticos (hardware)	4			5			10		
[Media] soportes de información	6			4			10		
[AUX] equipamiento auxiliar	4			5			10		
[I5] Avería de origen físico o lógico									
[HW] equipos informáticos (hardware)	6			8			10		
[HS] equipos informáticos (software)	5			5			10		
[Media] soportes de información	6			8			10		
[AUX] equipamiento auxiliar	5			5			10		
[I6] Corte del suministro eléctrico d									
[HW] equipos informáticos (hardware)	2			4			10		
[Media] soportes de información	2			4			10		
[AUX] equipamiento auxiliar	2			4			10		
[I8] Fallo de servicios de comunicaciones									
[COM]redes de cominucaciones	9			5			10		
[I11] Emanaciones electromagnéticas c									
[HW] equipos informáticos (hardware)			2			0			10
[HS] equipos informáticos (software)			2			0			10
[Media] soportes de información			2			0			10
[AUX] equipamiento auxiliar			2			0			10

*Nota.* los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de sistemas de la Clínica Proinsalud.

**Tabla 34**

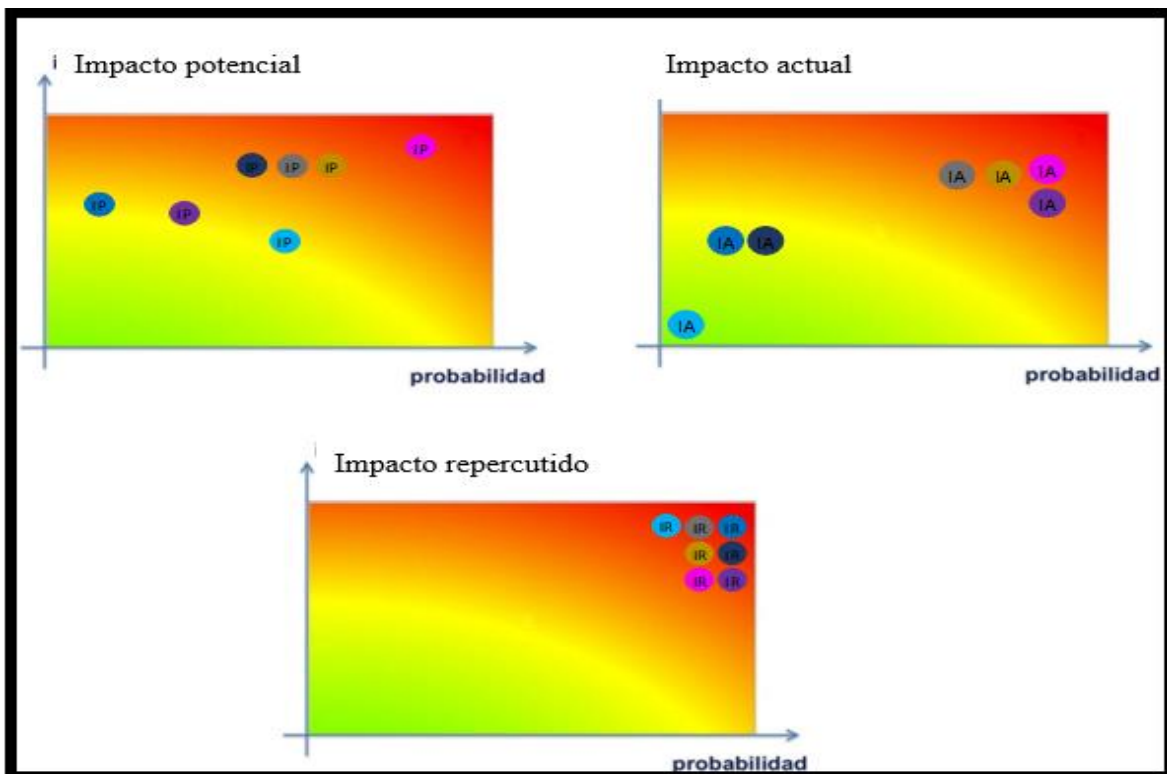
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit.*

Origen industrial		Tipos de impacto	
	Daños por fuego	<b>IP</b>	Impacto Potencial
	Daños por agua	<b>IA</b>	Impacto Actual
	Contaminación Mecánica	<b>IR</b>	Impacto Repercutido
	Avería de origen físico o lógico		
	Corto del suministro eléctrico		
	Fallo de servicio de comunicaciones		
	Emanaciones Electromagnéticas		

*Nota.* En la tabla se muestra cada uno de las amenazas por errores y fallos no intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit.

**Figura 35**

*Mapas de calor de los impactos con respecto a la tabla de origen industrial y sus amenazas*





El área de sistemas con respecto a las amenazas por origen industrial se encuentra en un estado medio de nivel de riesgo, por lo tanto, debe ser abordado lo antes posible para minimizar su impacto, para ello es importante determinar cuál es su fuente principal de riesgo, evaluar la probabilidad de que el riesgo ocurra y el impacto que tendría en el sistema para así determinar una solución para mitigar el impacto. Es importante destacar que, en este tipo de riesgos, es fundamental cumplir con las regulaciones y legislaciones ambientales y de seguridad en el trabajo.

**Figura 36**












*Análisis de Amenazas y riesgos por errores y fallos no intencionados del área de Sistemas*

AREA SISTEMAS POR ERRORES Y FALLOS NO INTENCIONADOS									
[E] Errores y fallos no intencionados	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[E1] Errores de los usuarios									
[D] datos / información 3	2	2	2	2	2	2	8	8	9
[keys] claves criptográficas 3	2	4	4	0	2	2	7	8	8
[S] servicios 3	4	4	2	2	0	0	9	8	7
[SW] aplicaciones (software) 3	2	2	2	2	2	2	8	7	9
[Media] soportes de información 3	4	2	4	2	0	0	7	8	8
[E3] Errores de monitorización (log)									
[E4] Errores de configuración in		9			9			9	
[D.conf] datos de configuración in		9			9			9	
[E8] Difusión de software dañino									
[SW] aplicaciones (software) 3	4	4	4	2	2	2	9	9	9
[E9] Errores de [re-]encaminamiento									
[S] servicios c			7			6			9
[SW] aplicaciones (software) c			7			6			9
[COM]redes de comunicaciones c			7			6			9
[E14] Escapes de información c			2			0			9
[E15] Alteración accidental de la información									
[D] datos / información i		8			0			9	
[keys] claves criptográficas i		8			0			9	
[S] servicios i		8			0			9	
[SW] aplicaciones (software) i		8			0			9	
[E18] Destrucción de información									
[D] datos / información d	9			0			9		
[S] servicios d	9			0			9		
[SW] aplicaciones (software) d	9			0			9		
[COM]redes de comunicaciones d	9			0			9		
[Media] soportes de información d	9			0			9		
[E19] Fugas de información									
[D] datos / información c			2			0			9
[keys] claves criptográficas c			2			0			9
[S] servicios c			2			0			9
[SW] aplicaciones (software) c			2			0			9
[COM]redes de comunicaciones c			2			0			9
[Media] soportes de información c			2			0			9
[L] instalaciones c			2			0			9
[P] personal c			2			0			9
[E20] Vulnerabilidades de los programas (software)									
[SW] aplicaciones (software) 3	5	5	5	2	2	2	10	10	10
[E.21] Errores de mantenimiento / actualización de									
[SW] aplicaciones (software) i d	9	9		6	6		10	10	
[E24] Caída del sistema por agotamiento de recursos									
[S] servicios d	9			6			10		
[HW] equipos informáticos (hardware) d	3			2			10		
[COM]redes de comunicaciones d	10			8			10		

*Nota.* los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de contabilidad de La Clínica Proinsalud.

**Tabla 35**

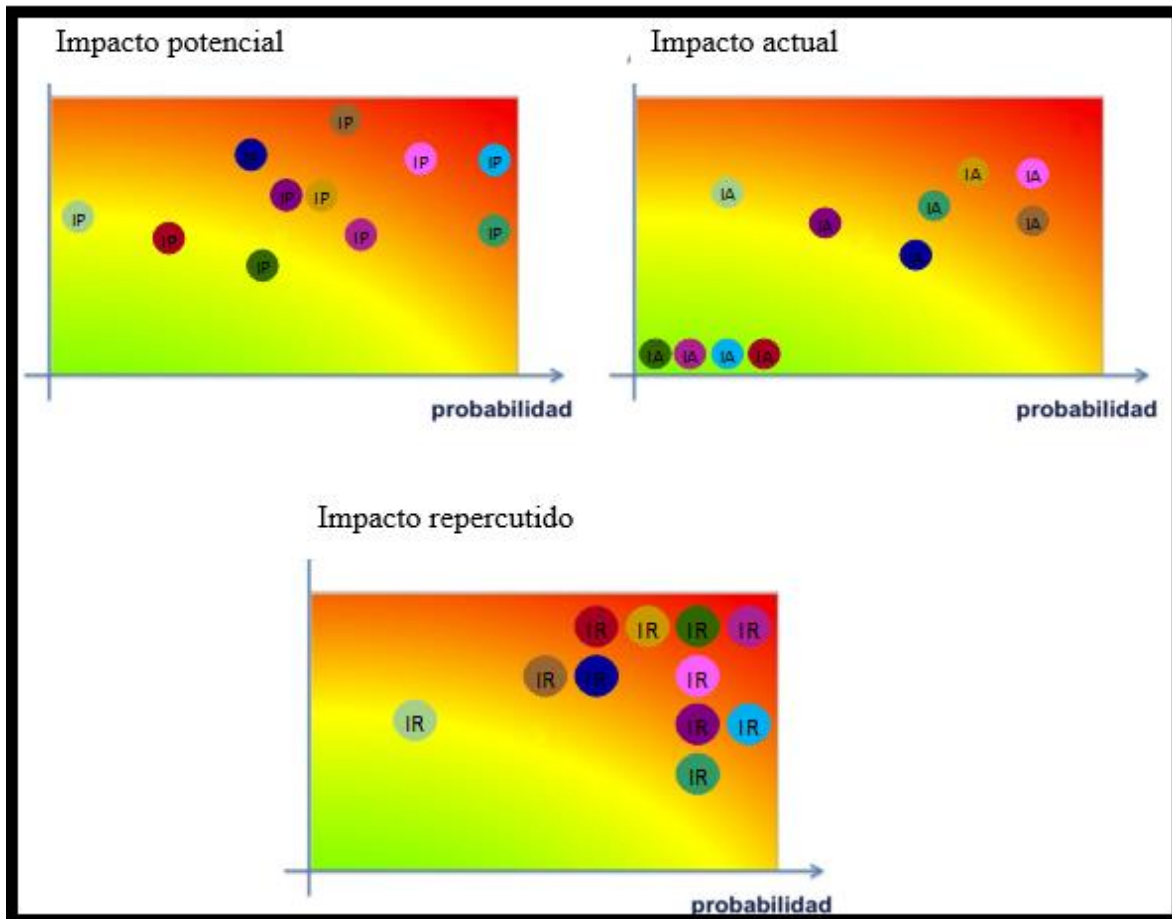
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit.*

<b>Errores y fallos no intencionados</b>		<b>Tipos de impacto</b>	
	Errores de los usuarios	<b>IP</b>	Impacto Potencial
	Errores de monitorización	<b>IA</b>	Impacto Actual
	Difusión de software dañino	<b>IR</b>	Impacto Repercutido
	Errores de Reencaminamiento		
	Escapes de información		
	Alteración accidental de la información		
	Destrucción de información		
	Fugas de información		
	Vulnerabilidades de los programas		
	Errores de mantenimiento		
	Caída del sistema por agotamiento de recursos		

*Nota.* En la tabla se muestra cada uno de las amenazas por errores y fallos no intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit.

**Figura 37**

Mapas de calor de los impactos con respecto a la tabla de errores y fallos no intencionados y sus respectivas amenazas



El área de sistemas con respecto a las amenazas por fallos no intencionados se encuentra en un estado medio de nivel de riesgo, llevando a cabo que una de las causas principales son los errores de los usuarios, por lo tanto, debe ser abordado lo antes posible para minimizar su posible impacto, se debe evaluar la probabilidad de que el riesgo ocurra y el impacto que tendría en el sistema para así determinar una solución para mitigar el impacto. Cabe destacar que la gestión de riesgos relacionados con los errores de los usuarios debe incluir medidas educativas y tecnológicas para minimizar la probabilidad de que los usuarios cometan errores y reducir el impacto en el sistema en caso de que los errores ocurran.

Figura 38

















Análisis de Amenazas y riesgos por ataques intencionados del área de Sistemas

AREA SISTEMAS POR ATAQUES INTENCIONADOS									
	Impacto Potencial			Impacto actual			Impacto Repercutido		
	D	I	C	D	I	C	D	I	C
[A] Ataques intencionados									
[A.3] Manipulación de los registros de actividad (log)									
[D.log] registros de actividad i		2			0			9	
[A.4] Manipulación de la configuración									
[D.log] registros de actividad 3	3	3	3	0	0	0	10	10	10
[A5] Suplantación de la identidad del usuario									
[D] datos / información 3	8	8	8	3	2	2	10	10	10
[keys] claves criptográficas 3	8	8	8	3	2	2	10	10	10
[S] servicios 3	8	8	8	2	5	2	10	10	10
[SW] aplicaciones (software) 3	8	8	8	2	5	2	10	10	10
[COM]redes de comunicaciones 3	8	8	8	2	2	2	10	10	10
[A6] Abuso de privilegios de acceso									
[D] datos / información 3	6	3	3	2	3	2	8	8	8
[keys] claves criptográficas 3	3	3	3	2	3	2	8	8	8
[S] servicios 3	3	6	6	2	2	3	8	8	8
[SW] aplicaciones (software) 3	3	3	6	2	2	3	8	8	8
[COM]redes de comunicaciones 3	3	3	3	2	2	2	8	8	8
[HW] equipos informáticos (hardware) 3	3	6	3	2	2	2	8	8	8
[A7] Uso no previsto									
[D] datos / información 3	5	5	5	3	2	3	9	9	9
[keys] claves criptográficas 3	5	5	5	3	2	3	9	9	10
[S] servicios 3	5	6	5	3	3	3	9	9	10
[SW] aplicaciones (software) 3	5	5	5	3	3	3	9	9	9
[COM]redes de comunicaciones 3	5	6	5	3	3	2	10	9	9
[HW] equipos informáticos (hardware) 3	5	5	5	3	2	2	10	9	9
[Media] soportes de información 3	5	6	5	3	2	3	10	9	10
[AUX] equipamiento auxiliar 3	5	5	5	3	3	3	9	9	10
[A8] Difusión de software dañino									
[SW] aplicaciones (software) 3	6	6	6	0	0	0	10	10	10
[A11] Acceso no autorizado									
[D] datos / información ci		5	5		0	0		10	10
[keys] claves criptográficas ci		5	5		0	0		10	10
[S] servicios ci		5	5		0	0		10	10
[SW] aplicaciones (software) ci		5	5		0	0		10	10
[COM]redes de comunicaciones ci		5	5		0	0		10	10
[HW] equipos informáticos (hardware) ci		5	5		0	0		10	10
[Media] soportes de información ci		5	5		0	0		10	10
[AUX] equipamiento auxiliar ci		5	5		0	0		10	10
[A12] Análisis de tráfico									
[COM]redes de comunicaciones c			9			4			10
[A15] Modificación deliberada de la información									
[D] datos / información i		3			0			10	
[keys] claves criptográficas i		3			0			10	
[S] servicios i		3			0			10	
[SW] aplicaciones (software) i		3			0			10	
[COM]redes de comunicaciones i		3			0			10	
[Media] soportes de información i		3			0			10	
[A18] Destrucción de información d									
[D] datos / información	8				2			10	
[S] servicios	6				2			10	
[SW] aplicaciones (software)	8				3			10	
[COM]redes de comunicaciones	6				2			10	
[Media] soportes de información	8				3			10	
[A19] Divulgación de información c									
[D] datos / información			3			4			8
[keys] claves criptográficas			3			3			4
[S] servicios			2			2			8
[SW] aplicaciones (software)			3			3			8
[COM]redes de comunicaciones			2			4			8
[Media] soportes de información			3			2			4
[A22] Manipulación de programas 3									
[SW] aplicaciones (software)	6	6	6	2	2	2	10	10	10
[A23] Manipulación de los equipos cd									
[AUX] equipamiento auxiliar	9		9	4		6	9		10
[COM]redes de comunicaciones	9		9	2		2	9		10
[HW] equipos	9		9	4		4	9		10
[A25] Robo cd									
[HW] equipos informáticos (hardware)	10		10	4		4	10		10
[AUX] equipamiento auxiliar	8		8	4		4	10		10
[Media] soportes de información	10		8	4		4	10		10
[A29] Extorsión 3									
[HW] equipos informáticos (hardware)	9	8	9	2	4	2	10		10
[P] personal interno	9	8	9	8	4	6	10		10
[A30] Ingeniería social 3									
[P] personal interno	8	8	8	6	4	4	9	10	10

Nota. los datos obtenidos fueron tomados directamente desde recolección de información mediante visita técnica visual al área de contabilidad de La Clínica Proinsalud.

**Tabla 36**

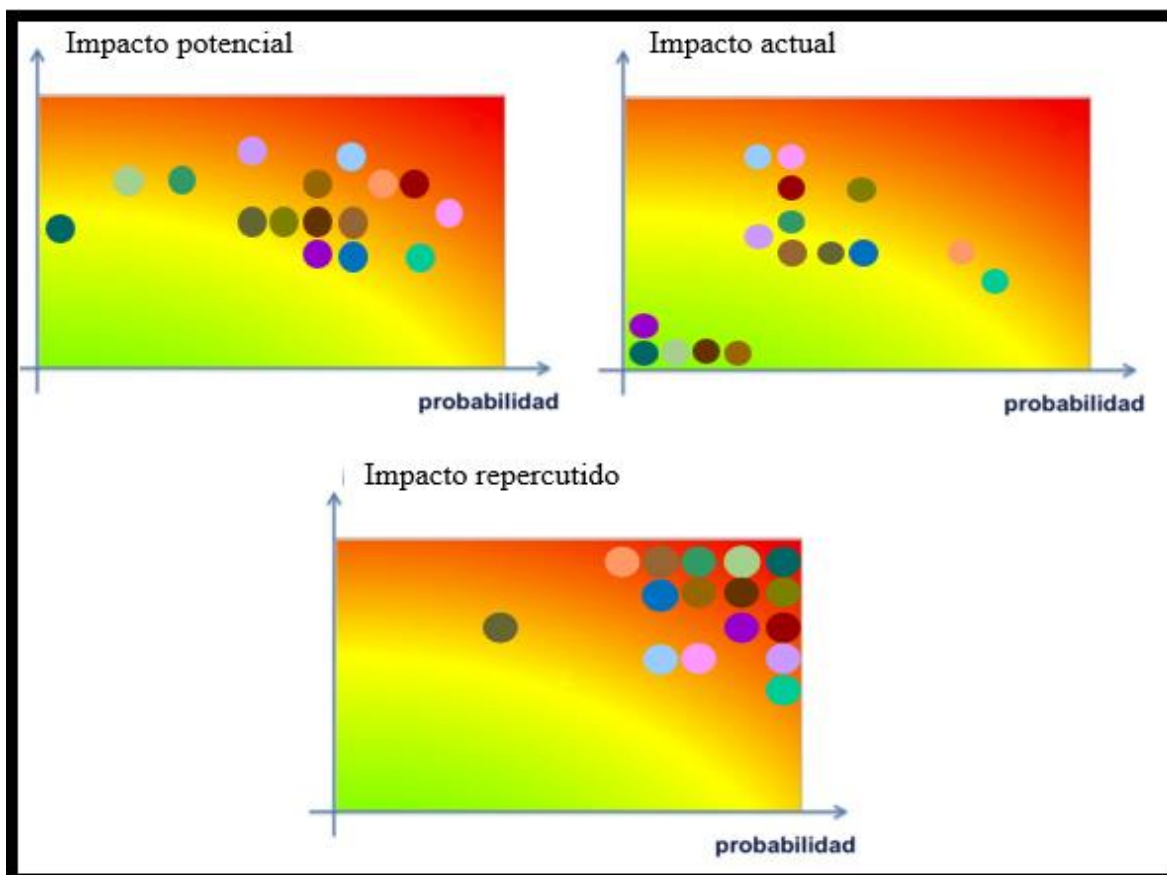
*Indicadores de los tipos de impacto de las tablas analizadas con Magerit.*

<b>Amenazas por ataques intencionados</b>		<b>Tipos de impacto</b>	
	Manipulación de los registros de actividad	<b>IP</b>	Impacto Potencial
	Manipulación de la configuración	<b>IA</b>	Impacto Actual
	Suplantación de la identidad del usuario	<b>IR</b>	Impacto Repercutido
	Abuso de privilegios de acceso		
	Uso no previsto		
	Difusión de software dañino		
	Acceso no autorizado		
	Análisis de tráfico		
	Modificación deliberada de la información		
	Destrucción de información		
	Divulgación de información		
	Manipulación de programas		
	Manipulación de los equipos		
	Robo		
	Extorsión		
	Ingeniería social		

*Nota.* En la tabla se muestra cada uno de las amenazas o ataques intencionados de acuerdo el tipo de impacto analizado con la metodología Magerit.

**Figura 39**

*Mapas de calor de los impactos con respecto a la tabla de ataques intencionados y sus respectivas amenazas*



El área de sistemas con respecto a las amenazas por fallos no intencionados se encuentra en un estado alto de nivel de riesgo, por lo tanto, debe ser abordado lo antes posible para minimizar su posible impacto, se debe evaluar la probabilidad de que el riesgo ocurra y el impacto que tendría en el sistema para así determinar una solución para mitigar el impacto.

### **2.2.5. Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001**

**2.2.5.1. Política institucional de seguridad de la información en la Clínica Proinsalud S.A.** La Clínica Proinsalud S.A se compromete con la seguridad de la información a partir de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la

norma ISO /IEC 27001 que permitirá controlar, mitigar amenazas vulnerabilidades y el robo de información a nivel institucional.

**2.2.5.1.1. Objetivo.** Implementar el Sistema de Gestión de Seguridad de la Información (SGSI) en la Clínica Proinsalud S.A que garantice la continuidad del negocio la satisfacción de las necesidades y expectativas de los usuarios y otras partes interesadas.

**2.2.5.1.2. Estrategia 1.** Implementar Y desplegar el Sistema de Gestión de Seguridad de la Información (SGSI) en la Clínica Proinsalud S.A.

**Tabla 37**

*Acciones y responsables con su tiempo empleado en días.*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
La Gerencia de la Clínica Proinsalud S.A debe elaborar una circular con el fin de informar la socialización del Sistema de Gestión de Seguridad de la Información.	Alta Dirección o Gerencia	1
Establecer un equipo Líder del proyecto de implementar Sistema de Gestión de Seguridad de la Información (SGSI).	Alta Dirección o Gerencia	2

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.1.3. Estrategia 2.** Socializar y divulgar el Sistema de Gestión de Seguridad de la Información donde se dé a conocer los riesgos y vulnerabilidades de las diferentes áreas de la Clínica Proinsalud S.A.

**Tabla 38***Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
Identificar el público a quienes se les va a dirigir la socialización y divulgación del Sistema de Gestión de Seguridad de la Información (SGSI). Pueden ser directivos, empleados, usuarios y proveedores de la Clínica Proinsalud S.A	Equipo designado por la Alta Dirección	5
Socializar el Sistema de Gestión de Seguridad de la Información (SGSI) a través de medios oficiales de comunicación de la Clínica Proinsalud S.A como los son Carteleras, página web y la intraweb.	Equipo designado por la Alta Dirección	10

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.1.4. Estrategia 3.** Sensibilizar y concientizar la importancia de salvaguardar los activos críticos de información: La Clínica debe identificar qué información es crítica y requiere un nivel más alto de protección.

**Tabla 39***Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
Socialización del SGSI en las áreas funcionales de la clínica y sus activos críticos.	Responsable de implementación del SGSI	5
Sensibilización y divulgación del análisis de vulnerabilidades y riesgos al personal de las áreas de la Clínica Proinsalud S.A.	Responsable de implementación del SGSI	5

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.



**2.2.5.1.5. Estrategia 4.** Implementar y socializar las medidas de seguridad físicas. Es importante que la Clínica implemente medidas de seguridad físicas para proteger la información, como el control de acceso a los espacios donde se almacena la información crítica, la instalación de sistemas de vigilancia y alarmas, y la protección contra incendios y otros desastres naturales.

**Tabla 40**

*Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo(Días)</b>
Implementación de controles de seguridad por parte de la Clínica Proinsalud S.A para salvaguardar los activos de las áreas de la institución.	Responsable de implementación del SGSI	20
Asignación de responsabilidades y roles por parte de las áreas de la Clínica Proinsalud S.A para la manipulación de la información de cada área.	Equipo designado por la Alta Dirección	10

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.1.6. Estrategia 5.** Plan de capacitación y fomentar la cultura de la seguridad de la información en la Clínica Proinsalud S.A.

**Tabla 41**

*Acciones y responsables con su tiempo empleado en días.*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo(Días)</b>
Elaboración del plan que incluye programación y cronograma de actividades.	Responsable de implementación del SGSI	15
Ruta a seguir para reportar incidentes suscitados con el manejo y protección de la información dentro de la Clínica Proinsalud S.A.	Responsable de implementación del SGSI	5
Organizar capacitaciones por medio de área de	Responsable de	15

Acciones	Responsable	Tiempo(Dias)
sistemas del correcto manejo de la información dentro de la Clínica Proinsalud S.A	implementación del SGSI	

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

### 2.2.5.2. Objetivos de control y controles. Anexo A de la ISO 27001 a implementarse en la Clínica Proinsalud S.A.

**Tabla 42**

*Orientación de la dirección para la gestión de la seguridad de la información*

<b>Orientación de la dirección de la Clínica Proinsalud S.A para la gestión de la seguridad de la información</b>	
<b>Objetivo:</b> Implementar el Sistema de Gestión de Seguridad de la Información (SGSI) en la Clínica Proinsalud S:A que garantice la continuidad del negocio la satisfacción de las necesidades y expectativas de los usuarios y otras partes interesadas.	
Políticas para la seguridad de la información	<b>Control</b> Se definirá un conjunto de políticas para la seguridad de la información, aprobada por la dirección de la Clínica Proinsalud.
Revisión de las políticas para la seguridad de la información	<b>Control</b> Se realizará revisiones periódicas Planificadas para optimizar y llevar sus procesos de seguridad de la información hacia una mejora continua.
Copias de Seguridad	<b>Control</b> En el área se deberá realizar copias de seguridad con una periodicidad no mayor a un mes de la información que se considere importante y esta será alojada en la NAS de almacenamiento de la Clínica Proinsalud.

**Tabla 43**

*Organización de la seguridad de la información*

<b>Organización interna</b>	
<b>Objetivo:</b> Implementar el Sistema de Gestión de Seguridad de la Información (SGSI) en la Clínica Proinsalud S:A que garantice la continuidad del negocio la satisfacción de las necesidades y expectativas de los usuarios y otras partes interesadas.	
Roles y responsabilidades para la seguridad de la información	<b>Control</b> Se definirá y asignará a funcionarios de la Clínica Proinsalud todas las responsabilidades para velar por la seguridad de la información.
Separación de deberes	<b>Control</b> Se implementará los deberes y áreas de responsabilidad en el uso indebido de los activos de la organización.
Evaluación de riesgos	<b>Control</b> Se implementarán medidas para tratar los riesgos identificados.
<b>Dispositivos móviles y teletrabajo</b>	
<b>Objetivo:</b> Implementar el Sistema de Gestión de Seguridad de la Información (SGSI) en la Clínica Proinsalud S.A que garantice la continuidad del negocio la satisfacción de las necesidades y expectativas de los usuarios y otras partes interesadas.	
Política para dispositivos móviles	<b>Control</b> Se implementarán políticas y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles en la Clínica Proinsalud S.A.
Teletrabajo	<b>Control</b> Se implementarán políticas y medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, y que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

**2.2.5.3. Política táctica de seguridad de la información en el área de recursos humanos.**

El área de Recursos Humanos de la Clínica Proinsalud S.A se compromete en concientizar y dar a conocer a los funcionarios de la clínica la importancia del Sistema de Gestión de Seguridad de la Información (SGSI).

**2.2.5.3.1. Objetivo.** Mitigar y fortalecer la falta de conocimiento del personal de la Clínica Proinsalud S.A ante incidentes o inconvenientes suscitados en la seguridad de la información.

**2.2.5.3.2. Estrategia 1.** Realizar y planear un cronograma de capacitaciones dirigidas a todos los funcionarios y áreas de la Clínica Proinsalud S.A, incluyendo al personal involucrado con historias clínicas y demás activos de información.

**Tabla 44**

*Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
La Gerencia de la Clínica Proinsalud generará convocatorias de capacitación en seguridad informática con personal idóneo y experto.	Alta Dirección o Gerencia	5
Los funcionarios de la Clínica Proinsalud sin excepción deben asistir a las capacitaciones y es obligación cumplir con la totalidad de las horas establecidas para tal fin.	Responsable de implementación del SGSI	30

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.3.3. Estrategia 2.** Socializar las posibles vulnerabilidades del área de recursos humanos de la Clínica Proinsalud S.A. Para el correcto proceso de la información.

**Tabla 45***Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
El área de Sistemas de la Clínica Proinsalud, debe distinguir acciones o procedimientos realizados por los funcionarios del área de recursos humanos que representen riesgo para los activos de información.	Responsable de implementación del SGSI y área de sistemas	30
La Clínica Proinsalud listara acciones o procedimientos realizados de manera incorrecta con el fin de generar un cronograma de capacitación para mejora de procesos a cada área de la clínica	Responsable de implementación del SGSI	30

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.3.4. Estrategia 3.** Evaluar con las áreas los puntos críticos encontrados en metodología Magerit.

**Tabla 46***Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
Familiarizarse con la metodología Magerit: Estudia y comprende en detalle los conceptos y procesos que abarca la metodología Magerit.	Responsable de implementación del SGSI	8
Priorización y planificación la información relevante, prioriza los puntos críticos identificados en función de su impacto y probabilidad de ocurrencia. Desarrolla un plan de acción que establezca las medidas necesarias para abordar cada punto crítico, asignando responsabilidades y plazos	Responsable de implementación del SGSI	30

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.3.5. Estrategia 4.** Concientizar y socializar a los funcionarios de la Clínica Proinsalud S.A la Confidencialidad de la información dentro de una entidad de salud.

**Tabla 47**

*Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
Definir la confidencialidad de la información, es importante que los funcionarios de la Clínica Proinsalud S.A comprendan información confidencial y por qué es importante protegerla.	Responsable de implementación del SGSI	30
Las políticas y procedimientos de confidencialidad deben ser comunicados de manera clara y efectiva a los empleados, a los pacientes y sus familias.	Responsable de implementación del SGSI	15
Monitorear el cumplimiento de las políticas de confidencialidad de la Clínica Proinsalud S.A.	Responsable de implementación del SGSI	10

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.4. Objetivos de control y controles. Anexo A de la ISO 27001 a implementarse en la Clínica Proinsalud s en el área de recursos humanos.**

**Tabla 48**

*Seguridad de los recursos humanos. Antes de asumir el empleo*

<b>Antes de asumir el empleo en la Clínica Proinsalud S.A</b>	
<b>Objetivo:</b> Mitigar y fortalecer la falta de conocimiento del personal de la Clínica Proinsalud S.A ante incidentes o inconvenientes suscitados en la seguridad de la información.	
Selección	<b>Control</b>
	Será de obligatorio cumplimiento para el área de Recursos Humanos de la

	Clínica Proinsalud la verificación de los antecedentes de todos los candidatos a un empleo. Se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes.
Términos y condiciones del empleo	<b>Control</b> Se tendrán acuerdos contractuales con empleados y contratistas donde se establezca sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

**Tabla 49**

*Seguridad de los recursos humanos. Durante la ejecución del empleo*

<b>Durante la ejecución del empleo</b>	
<b>Objetivo:</b> Mitigar y fortalecer la falta de conocimiento del personal de la Clínica Proinsalud S.A ante incidentes o inconvenientes suscitados en la seguridad de la información.	
Responsabilidades de la dirección	<b>Control</b> El área de recursos Humanos exigirá a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
Toma de conciencia, educación y formación en la seguridad de la información	<b>Control</b> Todos los empleados de la Clínica Proinsalud S.A, y en donde sea pertinente, los contratistas, deberán recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
Proceso disciplinario	<b>Control</b> Se contara con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

**Tabla 50**

*Seguridad de los recursos humanos. Con la terminación y cambio de empleo*

<b>Terminación y cambio de empleo</b>	
<b>Objetivo:</b> Mitigar y fortalecer la falta de conocimiento del personal de la Clínica Proinsalud S.A ante incidentes o inconvenientes suscitados en la seguridad de la información.	
Terminación o cambio de responsabilidades de empleo	<b>Control</b> El área de Recursos Humanos será responsable de la socialización de la responsabilidad y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo y estos son de obligatorio cumplimiento deben hacer cumplir.

**Tabla 51**

*Copias de respaldo*

<b>Copias de respaldo</b>	
<b>Objetivo:</b> Mitigar y fortalecer la falta de conocimiento del personal de la Clínica Proinsalud S.A ante incidentes o inconvenientes suscitados en la seguridad de la información.	
Respaldo de la información	<b>Control</b> En el área se deberá realizar copias de seguridad con una periodicidad no mayor a un mes de la información que se considere importante y esta será alojada en la NAS de almacenamiento de la Clínica Proinsalud

**2.2.5.5. Política táctica de seguridad de la información en el área de administración financiera.** La Administración Financiera será responsable de garantizar que los datos financieros de la clínica se manejen de manera segura y protegida en todo momento. Esto incluye la creación, transmisión, almacenamiento, acceso y eliminación de los datos financieros.

**2.2.5.5.1. Objetivo.** Garantizar la seguridad y protección de los datos financieros de la clínica



Proinsalud a través de la implementación de controles de seguridad adecuados y el cumplimiento de los requisitos establecidos en Sistema de Gestión de Seguridad de la Información en la clínica Proinsalud. S. A.

**2.2.5.5.2. Estrategia 1.** Implementar el Sistema de Gestión de Seguridad de la Información en el área financiera para asegurar la confidencialidad, integridad y disponibilidad de la información y resistir amenazas internas y externas.

**Tabla 52**

*Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo(Días)</b>
Capacitar al personal del área financiera en los procedimientos de contingencia	Responsable de implementación del SGSI	15
Desarrollar políticas y procedimientos de seguridad: Define políticas y procedimientos de seguridad específicos para el área financiera.	Responsable de implementación del SGSI	10

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.5.3. Estrategia 2.** Implementar controles de acceso y protección de la información en el área financiera con el fin de prevenir el acceso no autorizado, la modificación o la eliminación de información financiera sensible y crítica.

**Tabla 53**

*Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
Incluir la implementación de medidas de seguridad física.	Responsable de implementación del SGSI y área de Sistemas	10
Implementación de controles de seguridad	Responsable de implementación	10

Acciones	Responsable	Tiempo (Días)
lógicos.	del SGSI y área de Sistemas	
Definir políticas y procedimientos de acceso y uso de la información financiera.	Responsable de implementación del SGSI	15

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.5.4. Estrategia 3.** Implementar una gestión de vulnerabilidades para identificar, priorizar y remediar las vulnerabilidades de seguridad en el área financiera y así proteger los activos de información críticos.

**Tabla 54**

*Acciones y responsables con su tiempo empleado en días*

Acciones	Responsable	Tiempo (Días)
Realizar una análisis y verificación de seguridad de los sistemas financieros y aplicaciones críticas para identificar y evaluar posibles vulnerabilidades de seguridad	Responsable de implementación del SGSI	15
Monitorear y mantener: Es importante mantener la gestión de vulnerabilidades como un proceso continuo para garantizar que se sigan identificando, evaluando y remediando las vulnerabilidades de seguridad en el área financiera.	Responsable de implementación del SGSI	15

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.6. Objetivos de control y controles. Anexo A de la ISO 27001 a implementarse en la Clínica Proinsalud S.A. en el área de financiera gestión de activos**

**Tabla 55**

*Responsabilidad por los activos*

<b>Responsabilidad por los activos</b>	
<b>Objetivo:</b> Garantizar la seguridad y protección de los datos financieros de la clínica Proinsalud a través de la implementación de controles de seguridad adecuados y el cumplimiento de los requisitos establecidos en Sistema de Gestión de Seguridad de la Información en la clínica Proinsalud . S. A.	
Inventario de activos	<b>Control</b> Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
Propiedad de los activos	<b>Control</b> Los activos mantenidos en el inventario deben tener un propietario.
Devolución de activos	<b>Control</b> Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

**Tabla 56**

*Clasificación de la información*

<b>Clasificación de la información</b>	
<b>Objetivo:</b> Garantizar la seguridad y protección de los datos financieros de la clínica Proinsalud a través de la implementación de controles de seguridad adecuados y el cumplimiento de los requisitos establecidos en Sistema de Gestión de Seguridad de la Información en la clínica Proinsalud . S. A.	
Clasificación	de la <b>Control</b>

información	La información se debe clasificar en función de los requisitos legales, valor, Criticidad y susceptibilidad a divulgación o a modificación no autorizada.
Etiquetado de la información	<b>Control</b> Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la Clínica Proinsalud S.A.
Manejo de activos	<b>Control</b> Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la Clínica Proinsalud S.A.

**Tabla 57**

*Seguridad física y del entorno*

**Seguridad física y del entorno**

**Objetivo:** Garantizar la seguridad y protección de los datos financieros de la clínica Proinsalud a través de la implementación de controles de seguridad adecuados y el cumplimiento de los requisitos establecidos en Sistema de Gestión de Seguridad de la Información en la clínica Proinsalud . S. A.

Controles de acceso físicos	<b>Control</b> Se implementará controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado
Seguridad de oficinas, recintos e instalaciones	<b>Control</b> Se aplicará seguridad física a oficinas, recintos e instalaciones.
Protección contra amenazas externas y ambientales	<b>Control</b> Se aplicará protección física contra desastres naturales, ataques Maliciosos o accidentes.

**Tabla 58**

*Copias de respaldo*

<b>Copias de respaldo</b>	
<b>Objetivo:</b> Garantizar la seguridad y protección de los datos financieros de la clínica Proinsalud a través de la implementación de controles de seguridad adecuados y el cumplimiento de los requisitos establecidos en Sistema de Gestión de Seguridad de la Información en la clínica Proinsalud . S. A.	
Respaldo de la información	<p><b>Control</b></p> <p>En el área se deberá realizar copias de seguridad con una periodicidad no mayor a un mes de la información que se considere importante y esta será alojada en la NAS de almacenamiento de la Clínica Proinsalud.</p>

**2.2.5.7. Política táctica de seguridad de la información en el área de sistemas.** La Clínica Proinsalud S.A se compromete con la seguridad de la información en su área de sistemas a partir de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001. El SGSI permitirá controlar, mitigar amenazas, vulnerabilidades y el robo de información.

**2.2.5.7.1. Objetivo.** El objetivo de esta política es establecer medidas tácticas de Seguridad de la Información basadas en la norma ISO 27001 para el Área de Sistemas de la Clínica Proinsalud, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información, mitigar los riesgos identificados en el análisis MAGERIT y garantizar la continuidad del servicio en el área de sistemas.

**2.2.5.7.2. Estrategia 1.** Implementar controles de seguridad de la información que permitan reducir los riesgos identificados en el análisis MAGERIT y cumplir con los requisitos establecidos en la norma ISO 27001.

**Tabla 59***Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
Realizar un análisis detallado de los riesgos identificados en el análisis MAGERIT y definir cuáles son los riesgos críticos que requieren una atención inmediata.	Responsable de implementación del SGSI	30
Capacitar a todo el personal del área de sistemas en la importancia de la seguridad de la información y cómo pueden contribuir a su protección. Esto puede incluir la formación sobre la política de seguridad de la información de la organización, los procedimientos de seguridad, y las prácticas seguras de trabajo.	Responsable de implementación del SGSI	30

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.7.3. Estrategia 2.** Divulgar un sistema de gestión de accesos y autorizaciones para todas las aplicaciones del área de sistemas puede ayudar a mejorar la seguridad de la información de la Clínica Proinsalud S.A.

**Tabla 60***Acciones y responsables con su tiempo empleado en días*

<b>Acciones</b>	<b>Responsable</b>	<b>Tiempo (Días)</b>
Se establecerá un proceso de monitoreo constante de los sistemas y aplicaciones críticas, con la implementación de herramientas de monitoreo y alertas tempranas para identificar posibles errores de forma proactiva y tomar acciones correctivas de manera oportuna.	Responsable de implementación del SGSI	30
Implementar herramientas de monitoreo y alertas tempranas en los sistemas y aplicaciones críticas del área	Responsable de implementación	30

Acciones	Responsable	Tiempo (Días)
de sistemas, para identificar posibles errores de forma proactiva y tomar acciones correctivas de manera oportuna.	del SGSI	
Realizar una evaluación de riesgos y vulnerabilidades en todas las aplicaciones del área de sistemas para identificar los puntos críticos de acceso y determinar los permisos de acceso necesarios para cada uno.	Responsable de implementación del SGSI	20

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.7.4. Estrategia 3.** La estrategia garantiza la disponibilidad de los servidores críticos para el correcto funcionamiento de la Clínica mediante la implementación de medidas de alta disponibilidad y recuperación ante desastres.

**Tabla 61**

*Acciones y responsables con su tiempo empleado en días.*

Acciones	Responsable	Tiempo (Días)
Identificar y priorizar los sistemas y aplicaciones críticos para la Clínica, y asegurarse de que estén protegidos con medidas adicionales de alta disponibilidad y recuperación ante desastres	Responsable de implementación del SGSI	15
Se implementarán políticas de gestión de capacidad y recursos en los sistemas y servidores para evitar la caída por agotamiento de recursos, como la memoria, el almacenamiento y la capacidad de procesamiento. Se establecerán mecanismos de monitoreo y alertas tempranas para identificar y mitigar posibles situaciones de agotamiento de recursos.	Responsable de implementación del SGSI	30

*Nota.* En la tabla se muestra las acciones con sus respectivos responsables y el tiempo en la cual se empleará en cumplir dicha estrategia.

**2.2.5.8. Objetivos de control y controles. Anexo A de la ISO 27001 a implementarse en la Clínica Proinsalud S.A. en el área de sistemas.**

**Tabla 62**

*Responsabilidad por los activos*

---

<b>Responsabilidad por los activos</b>	
<b>Objetivo:</b> El objetivo de esta política es establecer medidas tácticas de seguridad de la información basadas en la norma ISO 27001 para el Área de Sistemas de la Clínica Proinsalud, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información, mitigar los riesgos identificados en el análisis MAGERIT y garantizar la continuidad del servicio en el área de sistemas.	
Inventario de activos	<b>Control</b> Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
Propiedad de los activos	<b>Control</b> Los activos mantenidos en el inventario deben tener un propietario.
Devolución de activos	<b>Control</b> Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

---

**Tabla 63**

*Clasificación de la información*

---

<b>Clasificación de la información</b>	
<b>Objetivo:</b> El objetivo de esta política es establecer medidas tácticas de seguridad de la información basadas en la norma ISO 27001 para el Área de Sistemas de la Clínica Proinsalud, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información, mitigar los riesgos identificados en el análisis MAGERIT y garantizar la	

---



---

continuidad del servicio en el área de sistemas.	
Clasificación de la información	<b>Control</b> La información se debe clasificar en función de los requisitos legales, valor, Criticidad y susceptibilidad a divulgación o a modificación no autorizada.
Etiquetado de la información	<b>Control</b> Se desarrollará e implementará un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la Clínica Proinsalud S.A.
Manejo de activos	<b>Control</b> Se desarrollará e implementará procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la Clínica Proinsalud S.A.

---

## Tabla 64

### *Control de acceso*

---

<b>Requisitos del negocio para control de acceso</b>	
<b>Objetivo:</b>	El objetivo de esta política es establecer medidas tácticas de seguridad de la información basadas en la norma ISO 27001 para el Área de Sistemas de la Clínica Proinsalud, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información, mitigar los riesgos identificados en el análisis MAGERIT y garantizar la continuidad del servicio en el área de sistemas.
Política de control de acceso	<b>Control</b> Se establecerá documentará y revisará una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
Acceso a redes y a servicios en red	<b>Control</b> Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

---

**Tabla 65**

*Gestión de acceso de usuarios*

<b>Gestión de acceso de usuarios</b>	
<b>Objetivo:</b> El objetivo de esta política es establecer medidas tácticas de seguridad de la información basadas en la norma ISO 27001 para el Área de Sistemas de la Clínica Proinsalud, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información, mitigar los riesgos identificados en el análisis MAGERIT y garantizar la continuidad del servicio en el área de sistemas.	
Registro y cancelación del registro de usuarios	<b>Control</b> El área de Sistemas de la Clínica Proinsalud S.A debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
Suministro de acceso de usuarios	<b>Control</b> El área de Sistemas de la Clínica Proinsalud S.A debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
Gestión de derechos de acceso privilegiado	<b>Control</b> Se restringirá y controlara la asignación y uso de derechos de acceso privilegiado.

**Tabla 66**

*Seguridad física y del entorno*

<b>Seguridad física y del entorno</b>	
<b>Objetivo:</b> El objetivo de esta política es establecer medidas tácticas de seguridad de la información basadas en la norma ISO 27001 para el Área de Sistemas de la Clínica Proinsalud, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información, mitigar los riesgos identificados en el análisis MAGERIT y garantizar la	

continuidad del servicio en el área de sistemas	
Controles de acceso físicos	<b>Control</b> Se instalarán controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado
Seguridad de oficinas, recintos e instalaciones	<b>Control</b> Se aplicará seguridad física a oficinas, recintos e instalaciones.
Protección contra amenazas externas y ambientales	<b>Control</b> Se aplicará protección física contra desastres naturales, ataques maliciosos o accidentes.

**Tabla 67**

*Equipos*

<b>Equipos</b>	
<b>Objetivo:</b> El objetivo de esta política es establecer medidas tácticas de seguridad de la información basadas en la norma ISO 27001 para el Área de Sistemas de la Clínica Proinsalud, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información, mitigar los riesgos identificados en el análisis MAGERIT y garantizar la continuidad del servicio en el área de sistemas	
Ubicación y protección de los equipos	<b>Control</b> Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
Servicios de suministro	<b>Control</b> Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
Mantenimiento de equipos	<b>Control</b> Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

**Tabla 68**

*Copias de respaldo*

---

<b>Copias de respaldo</b>	
<b>Objetivo:</b> El objetivo de esta política es establecer medidas tácticas de seguridad de la información basadas en la norma ISO 27001 para el Área de Sistemas de la Clínica Proinsalud, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información, mitigar los riesgos identificados en el análisis MAGERIT y garantizar la continuidad del servicio en el área de sistemas	
Respaldo de la información	<b>Control</b> En el área se deberá realizar copias de seguridad con una periodicidad no mayor a un mes de la información que se considere importante y esta será alojada en la NAS de almacenamiento de la Clínica Proinsalud

---

Análisis y evaluación de amenazas, riesgos y vulnerabilidades del área de TI desde la metodología Magerit.

### **3. Conclusiones**

El trabajo de grado realizado en la Clínica Proinsalud sirvió para fortalecer la seguridad de la información y la gestión de activos tecnológicos, con la aplicación de los objetivos plasmado en el trabajo se obtuvieron conclusiones e información que destacan la importancia de garantizar la protección de la información para la continuidad de los servicios.

Mediante la investigación se logró realizar una revisión de la norma ISO/IEC 27001 la cual permitió establecer lineamientos como también políticas, estrategias adecuadas para SGSI de la Clínica Proinsalud.

Con el uso de la metodología Magerit se identificó sectores de riesgo de la clínica Proinsalud. Por medio de los mapas de calor generados a partir del estudio y el análisis de la documentación de esta metodología se logró determinar donde se concreta las mayores vulnerabilidades y amenazas, con la información obtenida se logra tomar decisiones para priorizar las acciones y la mejora de la seguridad en puntos más críticos.

Se realiza un inventario de los equipos. Con esto la clínica Proinsalud tiene un control de sus activos tecnológicos al conocer la ubicación y el estado de cada equipo, así como la información de hardware y software, mediante esto se pudo implementar medidas preventivas y correctivas específicas para asegurar la protección de estos activos a posibles amenazas e incidentes

Por medio de la norma ISO/IEC 27001 se desarrollaron políticas y estrategias de seguridad de la información de manera estructurada, estas políticas han establecido directrices para el manejo adecuado de la información las responsabilidades del personal el acceso a los datos y la gestión de incidentes. Las políticas fortalecen la seguridad en la organización y promueve conciencia sobre la importancia de proteger la información en la red.

En la investigación se combina la metodología Magerit y la norma ISO/IEC 27001 para generar una mejora continua y adaptabilidad al SGSI adecuando el ciclo PHVA, analizando los resultados obtenidos y los avances que se realizaron la clínica Proinsalud puede ajustar sus

políticas y estrategias asegurando que sigan siendo efectivas entre cambios tecnológicos y nuevas amenazas que se surgen a diario.

La aplicación de la metodología Magerit junto con la norma ISO/IEC 27001 fue una investigación sólida ya que fortalece la seguridad de la información en la clínica Proinsalud la identificación de sectores de riesgo la protección de activos y el enfoque a la mejora continua y adaptabilidad han permitido la creación de políticas y estrategias como también salvaguardas para proteger la confidencialidad integridad y disponibilidad de los activos.

#### **4. Recomendaciones**

De la investigación realizada, se propone las siguientes recomendaciones para mitigar el índice de amenazas y riesgos de la información de la Clínica Proinsalud. S.A

Implementar lineamientos y políticas institucionales adecuadas para el SGSI de la Clínica Proinsalud S.A, con el fin de concientizar y establecer criterios sobre la seguridad de la información a todo el personal de la Clínica.

Estructurar un proceso para identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información en la Clínica Proinsalud S.A, con el objetivo de fortalecer la seguridad informática de la entidad.

Determinar contraseñas encriptadas para salvaguardar la información de cada área de la Clínica Proinsalud, para evitar acceso a los activos empresariales.

Capacitación al personal de la Clínica Proinsalud. S.A periódicamente en temas de Seguridad de la Información con el fin de que tengan los conocimientos necesarios para una posible necesidad y comprobar si se está cumpliendo con las políticas de seguridad por parte de los empleados.

## Referencias bibliográficas

- Angelino, A. (2022). *¿Cómo hago para que los correos no me lleguen a la bandeja de correos no deseados?* <https://www.harasdadinco.cl/como-hago-para-que-los-correos-no-me-lleguen-a-la-bandeja-de-correos-no-deseados/#>
- Argos. (2021). *Ciclo PHVA: 4 pasos para realizar proyectos de calidad en la construcción.* <https://colombia.argos.co/ciclo-phva-4-pasos-para-realizar-proyectos-de-calidad-en-la-construccion/>
- Avast. (2022). <https://www.avast.com/es-es/c-phishing>. Guía esencial del phishing: cómo funciona y cómo defenderse
- Campus Ciber Seguridad. (2021). *La puerta trasera de una vulnerabilidad.* <https://www.campusciberseguridad.com/blog/item/101-la-puerta-trasera-de-una-vulnerabilidad>
- Cifuentes, R. (2011). *Diseño de proyectos de investigación cualitativa.* Noveduc.
- Clínica Proinsalud. (2021). *Manual de Procesos Clínica Proinsalud.* Archivo interno.
- Clínica Proinsalud. (2022). *Nuestra institución.* <https://www.proinsalud.co/historia.php>
- Eduba. (2022). *Activos de información.* <https://www.eduba.gov.co/index.php/eduba/gestion-documental/activos-de-informacion>
- ESET Security Report. (2021). *Reporte para Latinoamérica.* <https://web-assets.esetstatic.com/wls/2021/06/ESET-security-report-LATAM2021.pdf>
- Gadeas, E., Martínez, M., & Stonestreet, C. (2010). *Análisis y gestión de riesgos.* <https://es.slideshare.net/123jou/analisis-y-gestion-de-riesgos-23999887>



- Gallardo, G. (2016). *Seguridad en Los sistemas de información*. IT Campus Academy.
- Garrido, C. (2018). *Elaboración de plan de implementación de la ISO/IEC 27001:2023*. [Tesis de maestría, Universidad Autónoma de Barcelona] Repositorio UOC: <https://openaccess.uoc.edu/bitstream/10609/88265/10/cgarridocaTFM0119memoria.pdf>
- Google Maps. (2023). *Ubicación satelital de la Clínica Proinsalud*. <https://n9.cl/dltc0>
- Grupo Ático. (2022). *Confidencialidad, integridad y disponibilidad de los datos*. <https://protecciondatos-lopd.com/empresas/confidencialidad-integridad-disponibilidad/>
- Guamanga, C., & Perilla, C. (2015). *Análisis de riesgos de seguridad de la información basado en la metodología Magerit para el área de datacenter de una entidad promotora de salud*. [Tesis de especialización, Universidad Piloto de Colombia] Repositorio Unipiloto: <http://repository.unipiloto.edu.co/handle/20.500.12277/2752?show=full>
- Guzmán, C. (2015). *Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso*. [Tesis de especialización, Institución Universitaria Politécnico Grancolombiano] Alejandría Poligran: <https://alejandria.poligran.edu.co/handle/10823/654>
- Kaspersky. (2023). *¿Qué es el pharming y cómo evitarlo?* <https://latam.kaspersky.com/resource-center/definitions/pharming>
- Landeau, R. (2007). *Elaboración de trabajos de investigación*. Editorial Alfa.
- Ley 1273 de 2009. (2009, 5 de enero). Congreso de Colombia. Diario Oficial No. 47.223: [http://www.secretariassenado.gov.co/senado/basedoc/ley\\_1273\\_2009.html](http://www.secretariassenado.gov.co/senado/basedoc/ley_1273_2009.html)
- Ley 1581 de 2012. (2012, 17 de octubre). Congreso de Colombia. Diario Oficial No. 48.587: [https://www.funcionpublica.gov.co/eva/gestornormativo/norma\\_pdf.php?i=49981](https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981)

Ley 424-06 de 2006. (2006, 20 de noviembre). Congreso Nacional de República Dominicana:  
<https://opac.pucmm.edu.do/virtuales/elibros/LeyNo424-06.pdf>

Ley 65-00 del 2000. (2000, 26 de julio). Congreso Nacional de República Dominicana:  
<https://www.egeda.do/documentos/Ley%20No.65-00%20sobre%20Derecho%20de%20Autor.pdf>

Magerit. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Versión 3*.  
<https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>

Maya, P. (2016). *Plan de implementación del SGSI basado en la norma ISO 27001:2013 de la empresa Textilera S.A en Girardota*. [Tesis de maestría, Universitat Oberta de Catalunya] Repositorio UOC:  
<https://openaccess.uoc.edu/bitstream/10609/53466/8/pmayaaTFM0616memoria.pdf>

Ministerio de Tecnologías de la Información y Comunicaciones. (2016). *Guía para la gestión y clasificación de activos de información*. [https://www.mintic.gov.co/gestionti/615/articulos-5482\\_G5\\_Gestion\\_Clasificacion.pdf](https://www.mintic.gov.co/gestionti/615/articulos-5482_G5_Gestion_Clasificacion.pdf)

Moncayo, E., Campaña, M., & Solís, F. (2014). *Diseño de un sistema de gestión en control y seguridad basado en la norma Basc para la empresa de transportes y servicios asociados SYTSA CCÍA LTDA*. [Tesis de pregrado, Universidad de las Fuerzas Armadas de Ecuador] Repositorio ESPE: <http://repositorio.espe.edu.ec/xmlui/handle/21000/8988>

Monje, C. (2011). *Metodología de la investigación. Cualitativa y cuantitativa. Guía didáctica*. Universidad Surcolombiana: <https://www.uv.mx/rmipe/files/2017/02/Guia-didactica-metodologia-de-la-investigacion.pdf>

Orozco, M. (2013). *Activos Informáticos*. <https://es.slideshare.net/meztli9/16-activos-inf>

Pérez, A. (2019). *10 amenazas informáticas en el punto de mira*.  
<https://www.obsbusiness.school/blog/10-amenazas-informaticas-en-el-punto-de-mira#>

Perito Judicial Group. (2021). *Activos Informáticos: Las 7 claves que tienes que conocer*.  
<https://peritojudicial.com/activos-informaticos/>

Rent Advisor. (2022). *¿Sabes cuáles son los riesgos informáticos a los que está expuesta tu empresa?* <https://www.rentadvisor.com.co/riesgos-informaticos/>

Resolución 1995 de 1999. (1999, 8 de julio). Ministerio de Salud:  
[https://www.minsalud.gov.co/Normatividad\\_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf](https://www.minsalud.gov.co/Normatividad_Nuevo/RESOLUCI%C3%93N%201995%20DE%201999.pdf)

Reyes, J. (2019). *Diseño de un sistema de gestión de seguridad de información bajo la Norma ISO 27001:2013 en la E.P.S Asmet Salud*. [Tesis de especialización, Universidad Nacional Abierta y a Distancia] Repositorio UNAD: <https://repository.unad.edu.co/handle/10596/27057>

Rodríguez, J., & Peralta, I. (2013). *Gestión de Riesgos. Magerit*. tiThink.

Soluciones Pilar. (2022). *Análisis de riesgos*. <https://pilar.ccn-cert.cni.es/index.php/analisis-de-riesgos/analisis-de-riesgos-pilar>

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*. [Tesis de pregrado, Pontificia Universidad Católica del Perú] Tesis PUCP:  
<https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6092>

Tamayo y Tamayo, M. (2004). *El proceso de la investigación científica*. Editorial Limusa.

We Live Security. (2021). *Ransomware: qué es y cómo funciona*.  
<https://www.welivesecurity.com/la-es/2021/05/21/que-es-ransomware/>