

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN EN SEGURIDAD DE LA
INFORMACIÓN PARA EL HOSPITAL AGUA DE DIOS

ANDRÉS CÁRDENAS HERNÁNDEZ

DANIEL HERNÁN CASTAÑEDA MONTES



FACULTAD DE CIENCIAS SOCIALES Y EMPRESARIALES

ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS

BOGOTÁ D.C. SEMESTRE 1 – 2018

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN EN SEGURIDAD DE LA
INFORMACIÓN PARA EL HOSPITAL AGUA DE DIOS

ANDRÉS CÁRDENAS HERNÁNDEZ

DANIEL HERNÁN CASTAÑEDA MONTES

Trabajo de grado para obtener el título de Especialista en Gerencia de Proyectos

Asesor: DIANA PATRICIA GARCÍA OCAMPO



FACULTAD DE CIENCIAS SOCIALES Y EMPRESARIALES

ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS

BOGOTÁ D.C. SEMESTRE 1 – 2018

DEDICATORIA

A mi esposa Jaqueline, por su motivación y apoyo constante. Por creer en mí, incluso cuando ni yo mismo creía.

A mis hijos, Sofia y Juan, por su paciencia en mis largas horas de ausencia. Por enseñarse el sentido de la vida.

ANDRES

A mi vida entera Alejandra, Santiago, Matías y Valentina, quienes me han tomado de la mano para apoyarme en la alegría y en la tristeza, en el logro y en la derrota, que sin importar lo difícil del camino siguen dándolo todo por esta fascinación que se llama familia.

DANIEL

AGRADECIMIENTOS

A mi familia, por darme su apoyo incondicional, por creer en mis capacidades y ayudarme siempre a pesar de los obstáculos.

A la Universidad Piloto de Colombia, por permitirme ser parte de este programa y abrirme las puertas para el desarrollo de nuevas habilidades y progresar profesionalmente.

A cada una de las personas que han aportado una palabra de aliento en el extraordinario camino del emprendimiento, a cada una de las personas que incentivan el aprendizaje, y cada una de las personas que facilitan las herramientas para que los demás alcancemos nuestros sueños.

CONTENIDO

ÍNDICE DE FIGURAS	12
ÍNDICE DE TABLAS.....	14
ÍNDICE DE ANEXOS	16
RESUMEN	18
ABSTRACT	19
INTRODUCCIÓN	20
OBJETIVOS.....	21
1 ANTECEDENTES	22
1.1 DESCRIPCIÓN DE LA ORGANIZACIÓN	23
1.1.1 <i>descripción general.</i>	23
1.1.2 <i>Direccionamiento estratégico.</i>	26
2 MARCO METODOLÓGICO	33
2.1 TIPOS Y MÉTODOS DE INVESTIGACIÓN.....	33
2.1.1 <i>fases Metodológicas.</i>	33
2.2 HERRAMIENTAS PARA LA RECOLECCIÓN DE INFORMACIÓN	34

2.3	FUENTES DE INFORMACIÓN.....	34
2.4	SUPUESTOS Y RESTRICCIONES PARA EL DESARROLLO DEL TRABAJO DE GRADO	35
2.4.1	<i>supuestos</i>	35
2.4.2	<i>restricciones</i>	35
3	ESTUDIOS Y EVALUACIONES.....	36
3.1	ESTUDIO TÉCNICO	36
3.1.1	<i>diseño conceptual de la solución</i>	36
3.1.2	<i>análisis y descripción del proceso</i>	37
3.1.3	<i>definición del tamaño y localización del proyecto</i>	39
3.1.4	<i>requerimientos para el desarrollo del proyecto</i>	40
3.1.5	<i>mapa de procesos de la entidad con el proyecto implementado</i>	42
3.2	ESTUDIO DE MERCADO	43
3.2.1	<i>población</i>	43
3.2.2	<i>dimensionamiento de la demanda</i>	43
3.2.3	<i>dimensionamiento de la oferta</i>	44
3.2.4	<i>precios</i>	45
3.2.5	<i>punto de equilibrio oferta-demanda</i>	45
3.2.6	<i>técnicas de predicción</i>	46

3.3	ESTUDIO ECONÓMICO-FINANCIERO.....	47
3.3.1	<i>estimación de costos de inversión del proyecto.</i>	<i>47</i>
3.3.2	<i>definición de costos de operación y mantenimiento del proyecto.....</i>	<i>48</i>
3.3.3	<i>flujo de caja del proyecto caso.</i>	<i>49</i>
3.3.4	<i>determinación del costo de capital, fuentes de financiación y uso de fondos. 50</i>	
3.3.5	<i>evaluación financiera del proyecto.</i>	<i>51</i>
3.4	ESTUDIO SOCIAL Y AMBIENTAL	52
3.4.1	<i>descripción y categorización de impactos ambientales.</i>	<i>52</i>
3.4.2	<i>definición de flujo de entradas y salidas.</i>	<i>52</i>
3.4.3	<i>estrategias de mitigación de impacto ambiental.</i>	<i>53</i>
4	EVALUACIÓN Y FORMULACIÓN.....	57
4.1	PLANTEAMIENTO DEL PROBLEMA.....	57
4.1.1	<i>Análisis de involucrados.</i>	<i>58</i>
4.1.2	<i>árbol de problemas.....</i>	<i>59</i>
4.1.3	<i>árbol de objetivos.</i>	<i>60</i>
4.2	ALTERNATIVAS DE SOLUCIÓN	62
4.2.1	<i>identificación de acciones y alternativas.....</i>	<i>62</i>

4.2.2	<i>descripción de alternativa seleccionada.</i>	62
4.2.3	<i>justificación del proyecto.</i>	63
5	INICIO DEL PROYECTO	64
5.1	CASO DE NEGOCIO.	64
5.2	GESTIÓN DE LA INTEGRACIÓN	64
5.2.1	<i>acta de constitución (Project Charter).</i>	64
5.2.2	<i>actas de cierre del proyecto o fase.</i>	64
6	PLANES DE GESTIÓN	65
6.1	PLAN DE GESTIÓN DEL ALCANCE	65
6.1.1	<i>línea base del alcance.</i>	65
6.1.2	<i>matriz de trazabilidad de requisitos.</i>	67
6.1.3	<i>diccionario de la EDT.</i>	67
6.2	PLAN DE GESTIÓN DEL CRONOGRAMA	68
6.2.1	<i>listado de actividades con estimación de duraciones esperadas.</i>	68
6.2.2	<i>línea base de tiempo.</i>	68
6.2.3	<i>diagrama de red.</i>	68
6.2.4	<i>diagrama de Gantt.</i>	68
6.2.5	<i>nivelación de recursos y uso de recursos.</i>	70

6.3	PAN DE GESTIÓN DEL COSTO	72
6.3.1	<i>línea base de costos.....</i>	72
6.3.2	<i>presupuesto por actividades.....</i>	74
6.3.3	<i>estructura de desagregación de recursos ReBS y estructura de desagregación de costos CBS.....</i>	74
6.3.4	<i>indicadores de medición de desempeño.</i>	77
6.3.5	<i>aplicación técnica del valor ganado con curvas S de avance.....</i>	77
6.4	PLAN DE GESTIÓN DE LA CALIDAD	79
6.4.1	<i>especificaciones técnicas de requerimientos.....</i>	79
6.4.2	<i>herramientas de control de la calidad.....</i>	79
6.4.3	<i>formato Inspecciones.....</i>	83
6.4.4	<i>formato auditorias.....</i>	84
6.4.5	<i>listas de verificación del entregables.....</i>	84
6.5	PLAN DE GESTIÓN DE RECURSOS HUMANOS	85
6.5.1	<i>definición de roles, responsabilidades y competencias del equipo.....</i>	85
6.5.2	<i>matriz de asignación de responsabilidades.....</i>	89
6.5.3	<i>calendario de recursos.</i>	89
6.5.4	<i>plan de capacitación y desarrollo del equipo.....</i>	90

6.5.5	<i>esquema de contratación y liberación de personal.....</i>	92
6.5.6	<i>definición de indicadores de medición de desempeño del equipo y esquema de incentivos y recompensas.....</i>	93
6.6	PLAN DE GESTIÓN DE LAS COMUNICACIONES	95
6.6.1	<i>sistema de información de comunicaciones.</i>	95
6.6.2	<i>matriz de comunicaciones.</i>	99
6.7	PLAN DE GESTIÓN DEL RIESGO	101
6.7.1	<i>identificación de riesgos y determinación del umbral.</i>	102
6.7.2	<i>Risk Breakdown Structure (RBS).</i>	106
6.7.3	<i>análisis de riesgos.</i>	108
6.7.4	<i>matriz de riesgos.</i>	110
6.7.5	<i>plan de respuesta a los riesgos.</i>	110
6.8	PLAN DE GESTIÓN DE ADQUISICIONES	112
6.8.1	<i>definición y criterios de valoración de proveedores.</i>	112
6.8.2	<i>selección y tipificación de contratos.</i>	115
6.8.3	<i>criterios de contratación, ejecución y control de compras y contratos.</i>	116
6.8.4	<i>cronograma de compras con la asignación de responsable.....</i>	118
6.9	PLAN DE GESTIÓN DE LOS INTERESADOS.....	120

6.9.1	<i>identificación y categorización de interesados.....</i>	120
6.9.2	<i>matriz de interesados.</i>	121
6.9.3	<i>matriz dependencia influencia.</i>	122
6.9.4	<i>matriz de temas y respuestas.....</i>	124
6.9.5	<i>formato para la resolución de conflictos y gestión de expectativas.</i>	125
7	CONCLUSIONES.....	126
8	REFERENCIAS BIBLIOGRAFICAS	127
	ANEXOS.....	1

ÍNDICE DE FIGURAS

Figura 1. Mapa de ubicación de Agua de Dios. Fuente: iMaps	24
Figura 2. Climograma de Agua de Dios. Fuente: climate-data.org.....	25
Figura 3. Diagrama de temperatura del municipio. Fuente: climate-data.org.....	25
Figura 4. Datos históricos del tiempo en Agua de Dios.....	26
Figura 5. Organigrama de la entidad.....	31
Figura 6. Mapa estratégico de la organización.....	31
Figura 7. Cadena de valor de la organización.....	32
Figura 8. Fases iniciales para la implementación de un SGSI.	33
Figura 9. Proceso de implementación del SGSI.....	37
Figura 10. Mapa de ubicación de unidades funcionales del sanatorio en Agua de Dios.	40
Figura 11. Mapa de procesos de la entidad con el proyecto implementado.....	43
Figura 12. Promotoras de Salud EPS, vinculadas al hospital.	44
Figura 13. Diagrama de inversiones de capital.	50
Figura 14. Árbol de problemas. Fuente: Elaboración propia	60
Figura 15. Árbol de objetivos. Fuente: Elaboración propia.....	61
Figura 16. Estructura de desglose de trabajo.....	66

Figura 17. Desagregación de la matriz de trazabilidad de requisitos.	67
Figura 18. Cronograma de hitos. Fuente: Edición propia	68
Figura 19. Diagrama de Gantt.	70
Figura 20. Uso de recursos.	71
Figura 21. ReBS.	75
Figura 22. CBS.	76
Figura 23. Variables en project.	77
Figura 24. Curva S.	78
Figura 25. Diagrama de Pareto.	81
Figura 26. Estructura de desglose de riesgos.	107
Figura 27. Cronograma de adquisiciones.	119
Figura 28. Matriz de poder/interés.	124

ÍNDICE DE TABLAS

Tabla 1. Beneficios cuantificados	45
Tabla 2. Flujo de caja del proyecto	49
Tabla 3. Cálculo del valor actual neto	51
Tabla 4. Definición de entradas y salidas ambientales.....	52
Tabla 5. Recursos de trabajo, material y costo para el proyecto.....	70
Tabla 6. Presupuesto estimado de los paquetes de trabajo.....	72
Tabla 7. Presupuesto estimado de las cuentas control	73
Tabla 8. Presupuesto de costos	74
Tabla 9. Principales causas de ataques informáticos	80
Tabla 10. Escala de valoración de controles	82
Tabla 11. Formato de inspección a equipos informáticos	83
Tabla 12. Horarios de trabajo para el personal	90
Tabla 13. Capacitación del personal involucrado	91
Tabla 14. Capacitaciones propuestas	92
Tabla 15. Criterios de liberación del personal	93
Tabla 16. Matriz de comunicaciones SGSI	99
Tabla 17. Calendario de riesgos	101

Tabla 18. Registro de riesgos	102
Tabla 19. Probabilidad de los riesgos	104
Tabla 20. Impacto de los riesgos	104
Tabla 21. Matriz de probabilidad / Impacto	105
Tabla 22. Matriz de respuesta al riesgo	106
Tabla 23. Matriz de clasificación y evaluación de riesgos	108
Tabla 24. Matriz de evaluación cuantitativa de riesgos	109
Tabla 25. Matriz de interesados	121
Tabla 26. Matriz de influencia / interés	122
Tabla 27. Matriz de temas y respuestas.....	124

ÍNDICE DE ANEXOS

Anexo A. Análisis PESTLE.....	1
Anexo B. Matriz P5.....	5
Anexo C. Matriz de requisitos legales	13
Anexo D. Caso de negocio.....	18
Anexo E. Acta de constitución del proyecto	21
Anexo F. Acta de cierre SGSI	24
Anexo G. Enunciado del alcance	27
Anexo H. Matriz de trazabilidad de requisitos administrativos	35
Anexo I. Matriz de trazabilidad de requisitos técnicos.....	37
Anexo J. Diccionario de la EDT.....	41
Anexo K. Listado de actividades SGSI – Análisis PERT	44
Anexo L. Cronograma en MS Project.....	47
Anexo M. Diagrama de red SGSI.....	50
Anexo N. Presupuesto por actividades	54
Anexo O. Indicadores de medición de desempeño.....	59
Anexo P. Especificaciones técnicas de requerimientos	61
Anexo Q. Auditoria SGSI.....	64

Anexo R. Lista de verificación de entregables	73
Anexo S. Matriz RACI	74
Anexo T. Matriz de gestión de riesgos del proyecto.....	77
Anexo U. Plan de respuesta a los riesgos.....	78
Anexo V. Matriz de revaluacion de riesgos	80
Anexo W. Formato de resolución de conflictos y gestión de expectativas	82

RESUMEN

El presente trabajo pretende establecer los lineamientos para asegurar una adecuada gestión para el proyecto de implementación de un Sistema de Gestión en Seguridad de la Información (SGSI), para el Sanatorio de Agua de Dios (ESE). Basado en las buenas prácticas para la dirección de proyectos propuestas por el Project Management Institute (PMI). El capítulo 1 presenta una visión general de la entidad donde se pretende implementar el proyecto. Los capítulos 2, 3 y 4 presentan información sobre el marco metodológico para realizar el proyecto y los estudios previos para iniciar el desarrollo de este. Los capítulos 5 y 6 hacen referencia a la información necesaria para dar inicio al proyecto y los planes de gestión para el desarrollo de este.

Palabras clave:

Seguridad de la información, confidencialidad, integridad, disponibilidad

ABSTRACT

The present work aims to establish the guidelines to ensure an adequate solution for the Information Security Management System (ISMS), for the Sanatorio de Agua de Dios (ESE). Based on the good practices for project management proposed by the Project Management Institute (PMI). Chapter 1 presents an overview of the entity where the project is to be implemented. Chapters 2, 3 and 4 present information on the methodological framework to carry out the project and the previous studies to start its development. Chapters 5 and 6 refer to the information necessary for the start of the project and the management plans for its development.

Keywords:

Information security, confidentiality, integrity, availability

INTRODUCCIÓN

En el actual entorno empresarial globalizado y competitivo en el que se desenvuelven las organizaciones, cada vez se hace más dependiente de sus sistemas de información y la administración de estos, pues se hace evidente que tienen una enorme influencia en la toma de dediciones estratégicas para aumentar su nivel de competitividad. El problema de la seguridad de la información se caracteriza por la complejidad y la interdependencia. La gestión de la seguridad contiene un número importante de factores y elementos que se interrelacionan entre sí. Las Micro, Pequeñas y Medianas Empresas (MIPYMES), suelen tener una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridades olvidadas. De ahí la gran importancia de implementar un Sistema de Gestión en Seguridad de la Información (SGSI), al interior de las organizaciones en nuestro país.

La implementación del SGSI en las organizaciones está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Mediante la implementación de SGSI por parte de las entidades del estado, se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

OBJETIVOS

Objetivo general.

Implementar un Sistema de Gestión en Seguridad de la Información (SGSI), para el Sanatorio de Agua de Dios, empresa social del estado (ESE), basado en la norma técnica ISO 27001

Objetivos específicos

Realizar el diagnóstico de la entidad, con el fin de determinar el nivel de madurez que presenta el hospital con respecto al modelo de seguridad y privacidad de la información.

Determinar los riesgos, vulnerabilidades y amenazas con respecto a la información que se maneja al interior de la institución.

Realizar los planes de gestión necesarios para disminuir al nivel más bajo posible la brecha en seguridad de la información que presenta la entidad.

Utilizar herramientas tecnológicas que permitan gestionar procesos que apoyen la seguridad de la información.

Aplicar los controles de la norma ISO 27001 que permitan administrar el funcionamiento del sistema de gestión.

1 Antecedentes

Los proyectos en materia de seguridad de la información se han venido desarrollando en diferentes empresas de todos los sectores durante los últimos años, por ser una necesidad del entorno. La normativa vigente para esta implementación es la norma técnica Colombiana ISO 27000, junto con los lineamientos que el ministerio de las TIC ofrece en esta materia.

Se entiende por seguridad de la información al conjunto de procedimientos, herramientas y medidas preventivas y reactivas de las organizaciones y los sistemas tecnológicos que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema o en una organización.

En la actualidad son bastante frecuentes los ataques a la información confidencial de las empresas en general. Cada día, cibercriminales intentan tener acceso a datos privados de los sistemas informáticos. El acceso no autorizado a una red informática o a los equipos que en ella se encuentran pueden ocasionar grandes problemas en la mayoría de los casos.

Una de las posibles consecuencias de una intrusión es la pérdida de datos. Es un hecho frecuente y ocasiona muchos inconvenientes, sobre todo si no se cuenta con copias de seguridad actualizadas, y, aun así, no siempre es posible recuperar la totalidad de los datos. Otro de los problemas más dañinos es el hurto de información sensible y confidencial. La divulgación de la información que posee una empresa puede ocasionar demandas millonarias en su contra.

Con un escenario de constante avance tecnológico en áreas como la informática, es fundamental conocer las necesidades empresariales para garantizar la seguridad en los sistemas de información.

1.1 Descripción de la organización

1.1.1 descripción general.

Sanatorio de Agua de Dios Empresa Social del Estado, es una institución prestadora de servicios de salud de baja complejidad a pacientes Hansen y demás población, ejecuta actividades de docencia, investigación y capacitación en enfermedades de salud pública.

El Sanatorio de Agua de Dios E.S.E., desde sus inicios históricos que datan de 1870 cuando fue creado como institución para atender los entonces llamados "Enfermos de Elefancia", ha recibido diferentes denominaciones de "nombre", pero con la certeza ser una misma empresa Adscrita al Hoy denominado Ministerio de Salud para todos los fines de tipo Administrativo, Legal, Financiero y Misional.

Agua de Dios es un municipio de Cundinamarca, ubicado en la Provincia del Alto Magdalena, a 114 km de Bogotá. Limita por el oeste con Girardot, por el norte con Tocaima, y por el sur con Ricaurte y Nilo.

El topónimo de Agua de Dios tiene su origen en las aguas termales ubicadas en el lugar conocido como "Los Chorros". Se dice que los primeros en descubrir esas termales, exclamaron: «¡Esto es agua de Dios!» (FCM, 2017).

La figura 1 presenta la ubicación del municipio de Agua de Dios en el departamento de Cundinamarca.



Figura 1. Mapa de ubicación de Agua de Dios. Fuente: iMaps

El municipio cuenta con una población de 11515 habitantes. Su economía se basa principalmente en la ganadería, agricultura y explotaciones forestales. (Agua de Dios, 2017)

1.1.1.1 Datos climáticos del municipio

Agua de Dios tiene un clima tropical. Hay lluvias significativas en la mayoría de los meses del año. La corta estación seca tiene poco efecto sobre el clima general. Este clima es considerado Am según la clasificación climática de Köppen-Geiger. La temperatura aquí es en promedio 26.9 ° C. La precipitación es de 1337 mm al año.

En la figura 2, se presenta un gráfico de precipitación para todos los meses del año. El mes más seco es julio, con 50 mm. Con un promedio de 193 mm, la mayor precipitación cae en octubre. En la figura 3 se presentan los promedios de temperatura durante el año. La figura 4 muestra los datos históricos de temperaturas durante el año para el municipio.

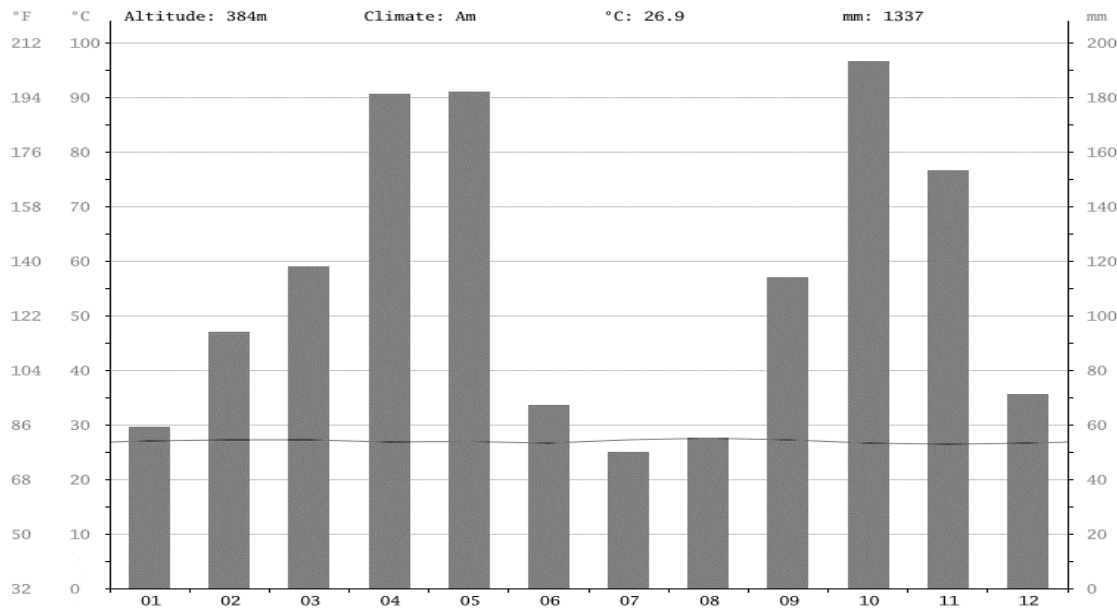


Figura 2. Climograma de Agua de Dios. Fuente: climate-data.org

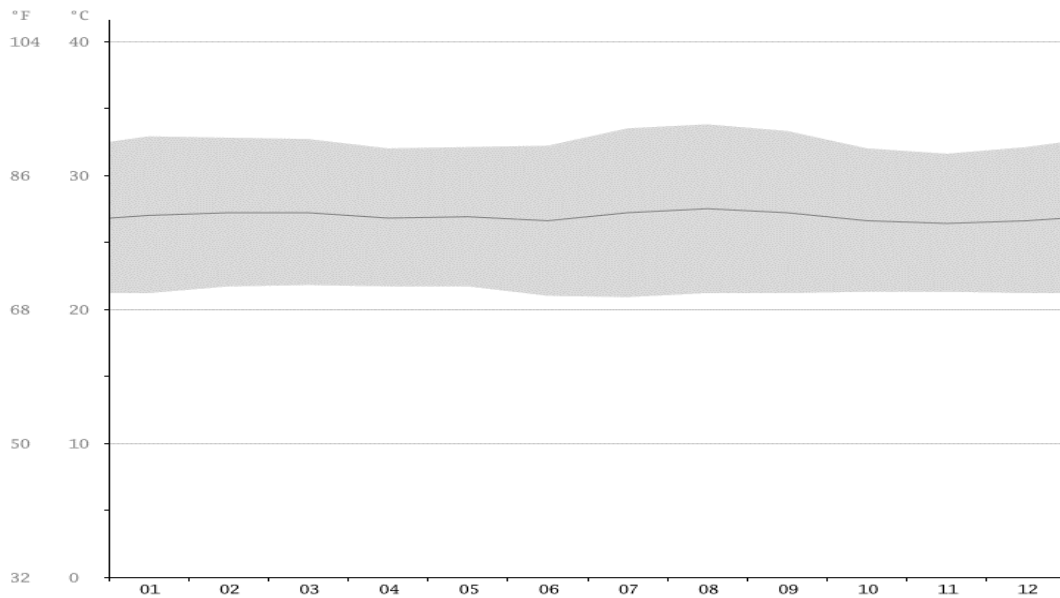


Figura 3. Diagrama de temperatura del municipio. Fuente: climate-data.org

El mes más caluroso del año con un promedio de 27.5 °C de agosto. noviembre tiene la temperatura promedio más baja del año. Es 26.4 ° C.

	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Temperatura media (°C)	27	27.2	27.2	26.8	26.9	26.6	27.2	27.5	27.2	26.6	26.4	26.6
Temperatura mín. (°C)	21.2	21.7	21.8	21.7	21.7	21	20.9	21.2	21.2	21.3	21.3	21.2
Temperatura máx. (°C)	32.9	32.8	32.7	32	32.1	32.2	33.5	33.8	33.3	32	31.6	32.1
Temperatura media (°F)	80.6	81.0	81.0	80.2	80.4	79.9	81.0	81.5	81.0	79.9	79.5	79.9
Temperatura mín. (°F)	70.2	71.1	71.2	71.1	71.1	69.8	69.6	70.2	70.2	70.3	70.3	70.2
Temperatura máx. (°F)	91.2	91.0	90.9	89.6	89.8	90.0	92.3	92.8	91.9	89.6	88.9	89.8
Precipitación (mm)	59	94	118	181	182	67	50	55	114	193	153	71

Figura 4. Datos históricos del tiempo en Agua de Dios.

Fuente: climate-data.org

La diferencia en la precipitación entre el mes más seco y el mes más lluvioso es de 143 mm. Durante el año, las temperaturas medias varían en 1.1 ° C.

1.1.2 Direccionamiento estratégico.

El DECRETO 1288 DE 1994 (junio 22), transforma el Sanatorio de Agua de Dios en E.S.E., con el siguiente objetivo:

"ARTICULO 3o. OBJETO. El Sanatorio de Agua de Dios, Empresa Social del Estado, tiene por objeto prestar con el carácter de servicio público a cargo del Estado, el servicio de salud a los enfermos de Hansen en todo el territorio nacional. En desarrollo de este objeto prestará atención médica, asistencia social y de rehabilitación y desarrollará programas de promoción y de prevención en salud."

1.1.2.1 Objetivos estratégicos de la organización.

Entre los objetivos estratégicos de la organización se cuentan los siguientes:

- a) Garantizar el enfoque, implementación, medición y mejoramiento continuo del Sistema Obligatorio de Garantía de Calidad de la Atención en Salud y sus cuatro componentes, buscando la fidelización del paciente y su familia.
- b) Generar una cultura de humanización a través de la implementación, medición y mejoramiento de la política y programa de humanización.
- c) Fortalecimiento de la cultura de seguridad del paciente a través de la implementación, medición y mejoramiento de la política y programa de seguridad del paciente.
- d) Gestionar los recursos económicos para readecuar la infraestructura del Hospital Herrera, para brindar a nuestros usuarios un ambiente cálido, humanizado y seguro.
- e) Fortalecer la sostenibilidad económica y el crecimiento financiero del Sanatorio de Agua de Dios, mediante la eficiencia en el gasto y la generación de ingresos propios.
- f) Brindar capacitación y asistencia técnica en programas de salud pública a los entes territoriales, con un enfoque de investigación y educación en las enfermedades de Hansen y tuberculosis.

El Sanatorio de agua de Dios, Empresa Social del Estado cumple con las siguientes funciones:

- a) Prestar atención médica a los enfermos de Hansen y a sus convivientes.
- b) Asistir a los inválidos y enfermos de Hansen albergados en las instituciones oficiales dependientes del sanatorio.
- c) Llevar a cabo programas de rehabilitación física y social para los enfermos de Hansen.

- d) Administrar las instituciones oficiales dedicadas al internamiento o albergue de enfermos de Hansen, que se encuentran bajo su dependencia.
- e) Administrar los subsidios destinados a los enfermos de Hansen de su jurisdicción, de conformidad con las normas vigentes.
- f) Desarrollar programas de promoción y prevención en salud.

1.1.2.2 políticas institucionales.

Política de seguridad. El compromiso del Sanatorio de Agua de Dios Empresa Social del Estado es prestar servicios de salud con seguridad y enfoque de gestión del riesgo, promoviendo el mejoramiento continuo de la calidad de la atención y minimizando todo tipo de riesgo que pueda afectar el bienestar de nuestros usuarios internos y externos.

Política de humanización. El Sanatorio de Agua de Dios es una Empresa Social del Estado sensible a la necesidad del usuario, con un modelo de atención institucional que desde su direccionamiento estratégico está comprometida en fortalecer valores y actitudes que respondan a los requerimientos y dimensiones de los usuarios y sus familias.

Política de gestión de tecnología. El Sanatorio de Agua de Dios está comprometido con una adecuada gestión de la tecnología y de los dispositivos médicos, desde la compra, renovación, reposición y su uso, apoyándose en un talento humano idóneo y eficiente, disminuyendo el riesgo para el usuario, su familia y el medio ambiente, gestionando su adecuada disposición final.

Política de Responsabilidad Social Empresarial. El Sanatorio de Agua de Dios Empresa Social del Estado desarrolla en el día a día actividades que fortalecen y mejoran continuamente los procesos de humanización de la atención en salud, la seguridad del paciente, la gestión de la tecnología, el enfoque y gestión del riesgo,

buscando constantemente la satisfacción del usuario y la transformación cultural de la Institución.

1.1.2.3 misión, visión y valores.

Misión. El Sanatorio de Agua de Dios Empresa Social del Estado, del orden nacional, institución prestadora de servicios de salud de baja complejidad a pacientes Hansen y demás población, tiene como misión ejecutar actividades de docencia, investigación y capacitación en enfermedades de salud pública, con un talento humano que brinda seguridad, humanización, calidad y calidez en el proceso de atención al paciente y su familia.

Visión. En el 2018 el Sanatorio de Agua de Dios Empresa Social del Estado será reconocido a nivel nacional como ente referenciador y facilitador del conocimiento científico de la enfermedad de Hansen y su compromiso con el mejoramiento continuo de las políticas de humanización y seguridad del paciente en la prestación de servicios de salud, transformando la cultura organizacional, garantizando su responsabilidad social empresarial y su auto sostenibilidad financiera.

1.1.2.3.1 Valores

Pro actividad: Hospital de Agua de Dios Empresa Social del Estado Tiene la capacidad de cumplir a cabalidad con las actividades asignadas y superar las expectativas de las acciones esperadas.

Educación: Siempre un saludo de bienvenida y una despedida, las hacemos con respeto, calidez y sinceridad. Expresiones tales como: buenos días, buenas tardes, a sus órdenes, muchas gracias, para servirle, con gusto, causan en el paciente una grata impresión.

Ética social: Responsabilidad del individuo con los demás y consigo mismo en las actividades que realiza en nombre del Hospital de Agua de Dios ESE y en su vida cotidiana.

1.1.2.4 estructura organizacional.

En la figura 5 se muestra el organigrama actual de la entidad (Sanatorio de Agua de Dios).

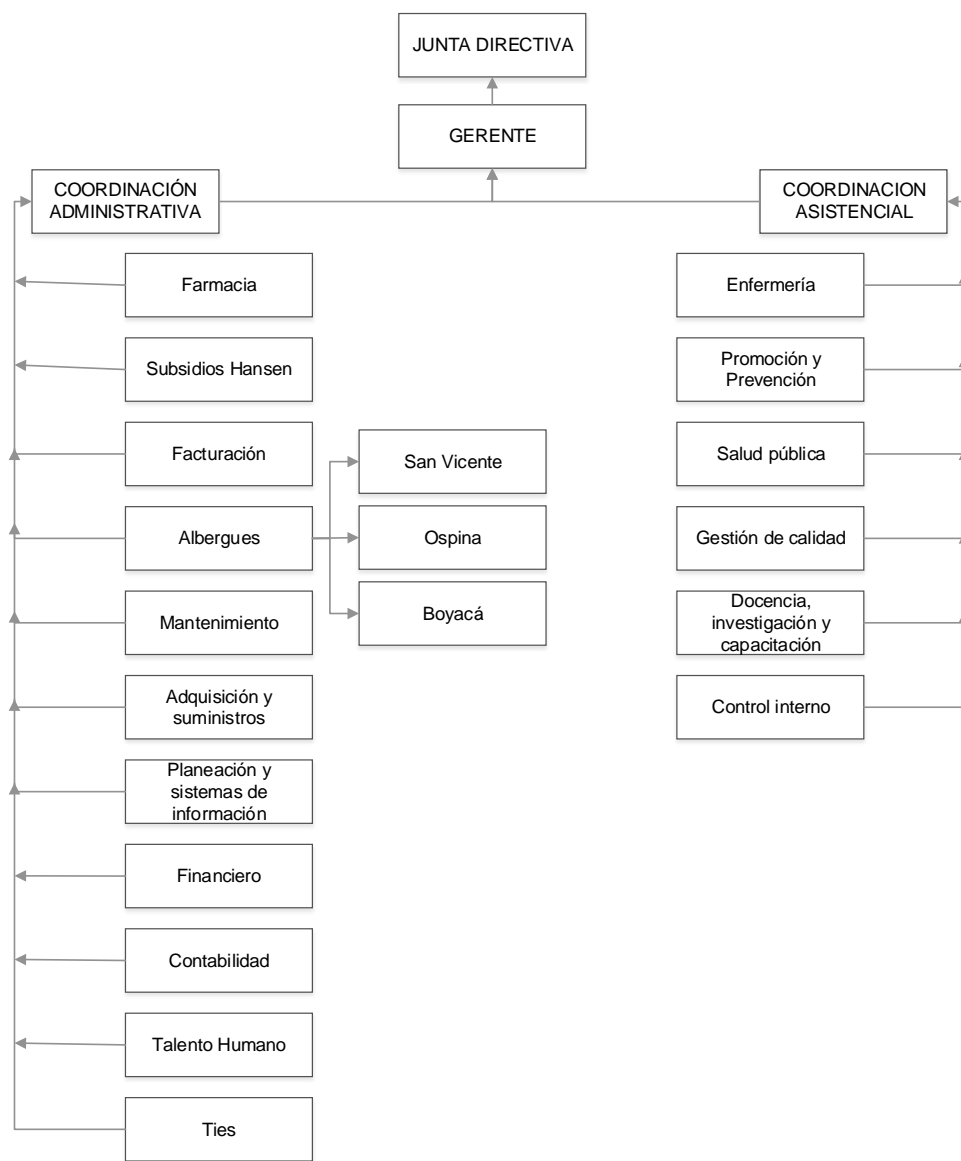


Figura 5. Organigrama de la entidad.

Fuente: www.sanatorioaguadedios.gov.co

1.1.2.5 mapa estratégico.

En la siguiente figura se presenta el mapa estratégico de la organización Sanatorio Agua de Dios ESE.



Figura 6. Mapa estratégico de la organización.

Fuente: Elaboración propia con base en datos del sanatorio de Agua de Dios

1.1.2.6 cadena de valor de la organización.

En la siguiente figura se presenta la cadena de valor de la organización Sanatorio de Agua de Dios ESE.



Figura 7. Cadena de valor de la organización.

Fuente: Elaboración propia con base en datos del sanatorio de Agua de Dios

2 Marco metodológico

2.1 Tipos y métodos de investigación

El presente trabajo corresponde al análisis y desarrollo de una propuesta para la implementación de un sistema de gestión de seguridad de la información para el Hospital de Agua de Dios E.S.E, de acuerdo con el alcance definido, las necesidades de la entidad y tomando como base para ello el modelo de referencia de seguridad de la norma ISO/IEC 27001:2013. También, durante el desarrollo del proyecto se utilizará el método de investigación de campo, que permite el análisis sistemático del problema en la realidad, con el fin de describirlo, interpretarlo, entender su naturaleza y explicar sus causas y efectos. En este tipo de investigación, la información de interés es recogida de forma directa de la fuente, mediante encuestas, cuestionario, entrevista o reuniones.

2.1.1 fases Metodológicas.

Teniendo en cuenta los requerimientos establecidos en la norma ISO/IEC 27001:2013 para el diseño del Sistema de Gestión de Seguridad de la Información, se establecieron las fases para el desarrollo del proyecto que se ilustran en la figura 8.

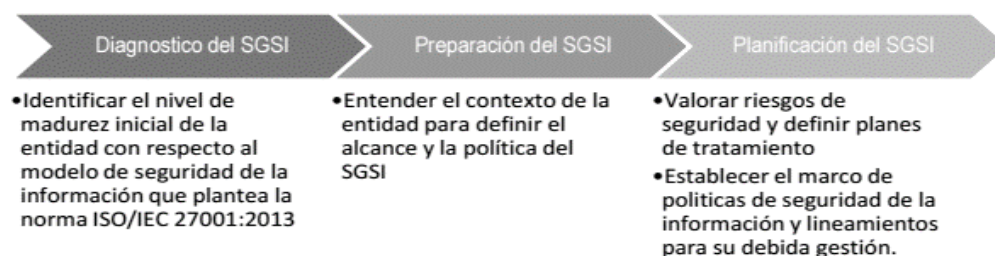


Figura 8. Fases iniciales para la implementación de un SGSI.

Fuente: Norma Técnica Colombiana NTC ISO/IEC 27001:2013

2.2 Herramientas para la recolección de información

Para el desarrollo del presente proyecto, se utilizaron los siguientes mecanismos e instrumentos para la recolección de información:

- a) Inspecciones.
- b) Observaciones.
- c) Entrevistas con funcionarios y sobre todo con el personal de la Dirección de Tecnología de la Entidad.
- d) Documentación existente en el sistema de gestión calidad de la entidad.

Un ejemplo de encuesta aplicada presenta los resultados que evidencian las vulnerabilidades en la red informática al interior de la institución, en la sección 6.4.2.2, utilizada para el análisis de Pareto. Entrevistas con los funcionarios para establecer la población, dimensionamiento de la oferta y la demanda, aplicados en la sección 3.2. Observaciones y encuestas para la estimación de los beneficios del producto y su vida útil.

2.3 Fuentes de información

Evaluación con base en la experiencia del autor. El uso de diferentes fuentes de información, como son la Norma Técnica Colombiana NTC-ISO/IEC 27001, información histórica de las dependencias del sanatorio y bases de datos públicas del municipio de Agua de Dios. También se utiliza la información que pone a disposición el ministerio de las tecnologías de la información y las telecomunicaciones (MINTIC), relacionada con los lineamientos para la implementación del sistema de seguridad y privacidad de la información en entidades del estado.

2.4 Supuestos y restricciones para el desarrollo del trabajo de grado

2.4.1 supuestos

La solución no pretende certificar a la entidad en la norma ISO 27001. No se buscará, por tanto, una auditoría externa para la certificación en ISO 27001. Las auditorías se realizarán internamente y serán exclusivas del equipo de dirección como parte del proceso de mejora continua, mientras el proyecto se encuentre en ejecución.

Se cuenta con el respaldo de la dirección general de la entidad, para la gestión del presupuesto necesario para la ejecución del proyecto. Los equipos y dispositivos son compatibles con las necesidades del proyecto.

Se cuenta con un recurso humano en capacitación constante, sin embargo, se necesita voluntad de la dirección para las capacitaciones necesarias en el marco de la seguridad de la información.

2.4.2 restricciones

No se contratará personal de planta para la ejecución del proyecto. Requerimientos adicionales de personal, equipos, insumos y otros deben estar debidamente soportados por la gerencia del proyecto y avalados por la gerencia de la entidad.

3 Estudios y evaluaciones

3.1 Estudio técnico

3.1.1 diseño conceptual de la solución.

Con el proposito de focalizar la implementación del SGSI, se ha seleccionado el sanatorio de agua de Dios empresa social del estado como organización objetivo, ya que en esta entidad sus diferentes procesos deben cumplir eficientemente sus funciones dentro de la normativa establecida en el modelo de seguridad y privacidad, acorde con las buenas prácticas de seguridad definidas en la norma técnica internacional ISO/IEC 27001.

Por tanto, la implementación del SGSI está determinado por decisión estratégica de la organización y por la necesidad de cumplir los requisitos legales de seguridad y calidad en los procesos de la organización, buscando el mejoramiento continuo de procesos y minimización de riesgos que pueda afectar el bienestar de los usuarios internos y externos de la organización.

La solución es desarrollada con base en la implementación de la política general de seguridad de la información y requisitos de seguridad vigentes.

Lo anteriormente descrito en busca de instituir y delimitar un marco legal basado en la confianza y desarrollo del compendio de deberes con el estado y los ciudadanos, y enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la organización, garantizando el buen uso y la privacidad de los datos. Además se busca la disminución del impacto generado sobre los activos de la organización por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición mínima.

3.1.2 análisis y descripción del proceso.

Es necesario realizar el análisis de los procesos involucrados en la implementación SGSI y la descripción de cada uno de ellos, y las recomendaciones necesarias de los procedimientos de seguridad de la información como lineamiento o modelo de seguridad y privacidad de la Información para la organización. Estos procedimientos constituyen una base sólida para que la organización pueda generar y establecer documentos propios ajustados a sus características particulares e inherentes de su servicio, sus activos de información, sus procesos y los servicios de información que pueda prestar.

Con el objetivo propuesto de hacer una correcta y completa implementación de seguridad de la Información en la organización, se trabajará en su desarrollo con base a los diferentes numerales de control de seguridad de la información, que están definidos en la norma ISO/IEC 27001, para definir los procedimientos de seguridad necesarios y realizar de manera directa el desarrollo del proceso, mediante procedimientos presentados en la figura 9, que encierran de manera global el (SGSI).

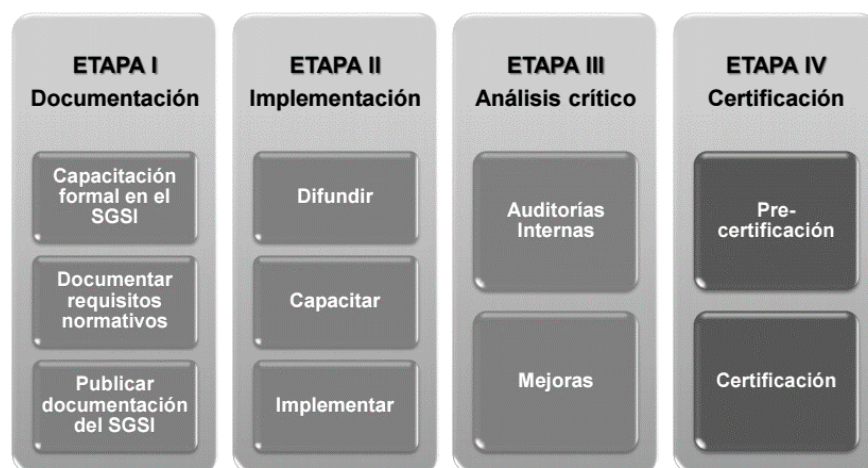


Figura 9. Proceso de implementación del SGSI.

Fuente: <https://www.isaca.org/>

3.1.2.1 documentación.

Proceso de seguridad del recurso humano: Este ítem está relacionado con el personal que labora en la organización Sanatorio Agua de Dios ESE.

- a) *Procedimiento de capacitación y sensibilización del personal*
- b) *Procedimiento de ingreso y desvinculación del personal*

Proceso de gestión de activos: Este ítem está relacionado con la identificación y clasificación de activos de acuerdo con su criticidad y nivel de confidencialidad.

- a) *Procedimiento de identificación y clasificación de activos*

Proceso de control de acceso: Este ítem está relacionado con el acceso a la información y a las instalaciones de procesamiento de la información.

- a) *Procedimiento para ingreso seguro a los sistemas de información*
- b) *Procedimiento de gestión de usuarios y contraseñas*

Seguridad física y del entorno: Este ítem está relacionado con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información.

- a) *Procedimiento de control de acceso físico*
- b) *Procedimiento de protección de activos*
- c) *Procedimiento de retiro de activos*
- d) *Procedimiento de mantenimiento de equipos*

Seguridad de las comunicaciones: Este ítem busca el aseguramiento y la protección de la información a través de los diferentes servicios de comunicaciones de la organización.

- a) *Procedimiento de aseguramiento de servicios en la red*
- b) *Procedimiento de transferencia de información*

Relaciones con los proveedores: Este dominio está relacionado con la protección de los activos de la organización a los cuales los proveedores o terceros tienen acceso.

- a) *Procedimiento para el tratamiento de la seguridad en los acuerdos con los proveedores*
- b) *Procedimiento adquisición, desarrollo y mantenimiento de software*
- c) *Procedimiento de control software*
- d) *Procedimiento de gestión de incidentes de seguridad de la información*
- e) *Procedimiento de gestión de la continuidad de negocio*

3.1.3 definición del tamaño y localización del proyecto.

Ubicado en el municipio de Agua de Dios, el Sanatorio de Agua de Dios Empresa Social del Estado, es una institución prestadora de servicios de salud de baja complejidad a pacientes Hansen y demás población, ejecuta actividades de docencia, investigación y capacitación en enfermedades de salud pública. (Sanatorio, 2017)

El sanatorio se distribuido en unidades funcionales como son:

- a) Hospital Herrera Restrepo, principal prestador de servicios de salud del municipio.
- b) Edificio Carrasquilla, donde se ubica la unidad administrativa.
- c) Albergues Boyacá, San Vicente, Ospina, vivienda permanente para los pacientes Hansen.

Estos albergues mencionados son la residencia permanente de pacientes enfermos de Hansen, provenientes de todos los lugares del territorio nacional, que llegan en busca de tratamiento y refugio. Están distribuidos en los 16 barrios que componen el municipio.

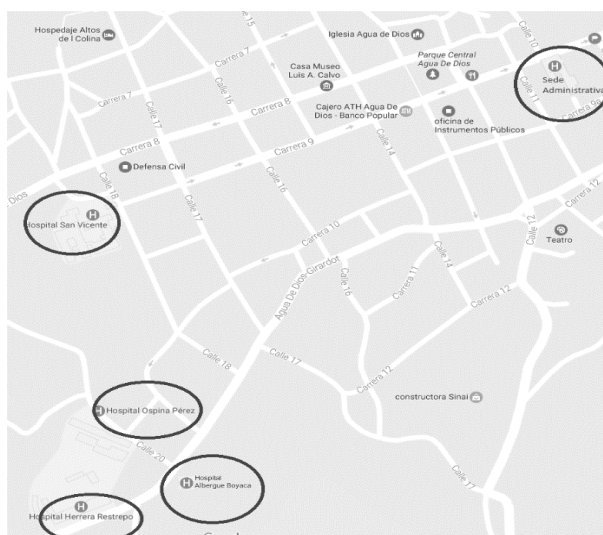


Figura 10. Mapa de ubicación de unidades funcionales del sanatorio en Agua de Dios.

Fuente: Google Maps

La unidad funcional edificio Carrasquilla, sede administrativa de la entidad en la cual se encuentra instalado el Data Center, servidores de red y distribución de internet para todas las unidades funcionales, las cuales están conectadas mediante enlaces inalámbricos de radio frecuencia.

3.1.4 requerimientos para el desarrollo del proyecto.

3.1.4.1 requerimiento de equipos.

Cada día se hace más necesario diseñar y mejorar un plan para mantener la seguridad de nuestros datos y equipos a salvo de intrusiones e infecciones de virus y

troyanos que puedan afectar al buen desarrollo de las actividades cotidianas de nuestra organización.

Para poder hacer frente a estas amenazas, lo ideal es proteger nuestra red de datos y nuestros equipos, con sistemas robustos, que se mantengan actualizados de forma constante.

Los equipos básicos identificados para la implementación de este proyecto son: firewall, NAS, consola de antivirus, servidor de base de datos, equipo de control de acceso remoto, Circuito cerrado de televisión (CCTV), Sistema de alimentación de energía ininterrumpido (UPS).

3.1.4.2 requerimiento de personal.

El equipo técnico de trabajo se debe conformar teniendo en cuenta los perfiles específicos necesarios para el desarrollo de cada una de las fases del proyecto de esta naturaleza. Estos perfiles se describen de manera detallada en la sección 6.5.1.1, del plan de gestión de los recursos humanos.

3.1.4.3 Infraestructura.

Data Center debidamente acondicionados para alojar los servicios informáticos y servidores requeridos por el proyecto. Ambiente de coexistencia y pruebas. Conexiones físicas. Datos de prueba en ambiente adecuado para operar de manera simultánea e ininterrumpida durante la ejecución de mejora continua. Bodega de desechos electrónicos y condiciones de almacenaje adecuadas. Circuito cerrado de TV y cámaras de seguridad en los principales centros de datos.

3.1.5 mapa de procesos de la entidad con el proyecto implementado.

En la siguiente figura se presenta el mapa de procesos de la entidad con el proyecto implementado.

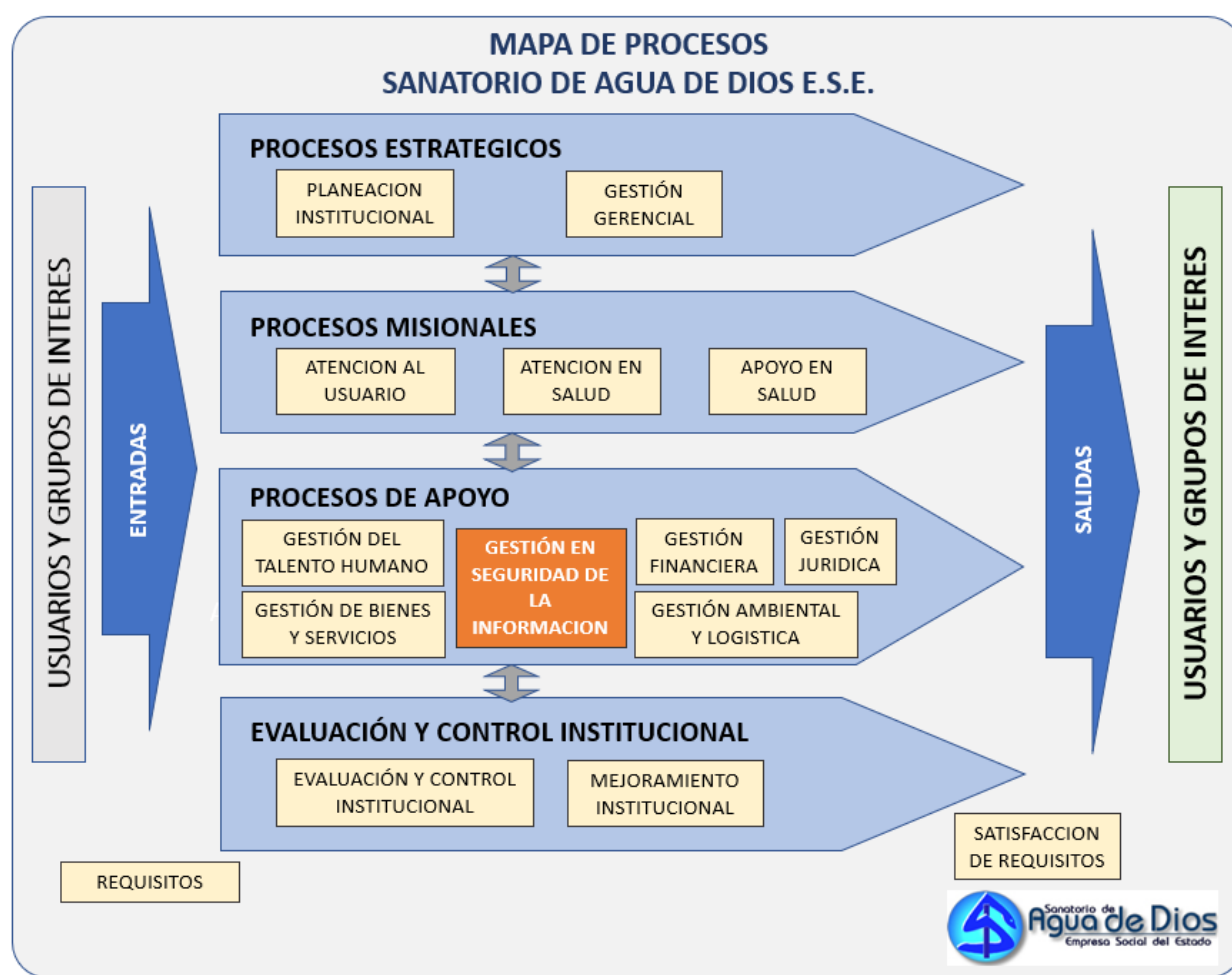


Figura 11. Mapa de procesos de la entidad con el proyecto implementado.

Fuente: Elaboración propia

3.2 Estudio de mercado

3.2.1 población.

La población objetivo de este proyecto es la comunidad en general del municipio de Agua de Dios, la cual tiene como IPS el sanatorio de Agua de Dios.

Existe además población de otros sectores del país que ven en los albergues un estilo de vida, ellos son los denominados pacientes Hansen, para los cuales el gobierno nacional, por intermedio del sanatorio presta ayudas económicas y tratamientos para esta enfermedad.

Según estimaciones de la alcaldía del municipio, se estima que unas 15.000 personas son beneficiarios directos e indirectos del sanatorio, y, por ende, de la puesta en marcha y ejecución de este proyecto.

3.2.2 dimensionamiento de la demanda.

Además de la población que tiene como sede principal la IPS Hospital Herrera del sanatorio de Agua de Dios, varias de las EPS están vinculadas al hospital para la atención de sus afiliados, Entre las de más usuarios se cuentan: Famisanar EPS, Ecoopsos EPS, EPS Convida, entre otras. La figura 12 presenta las EPS vinculadas al hospital.

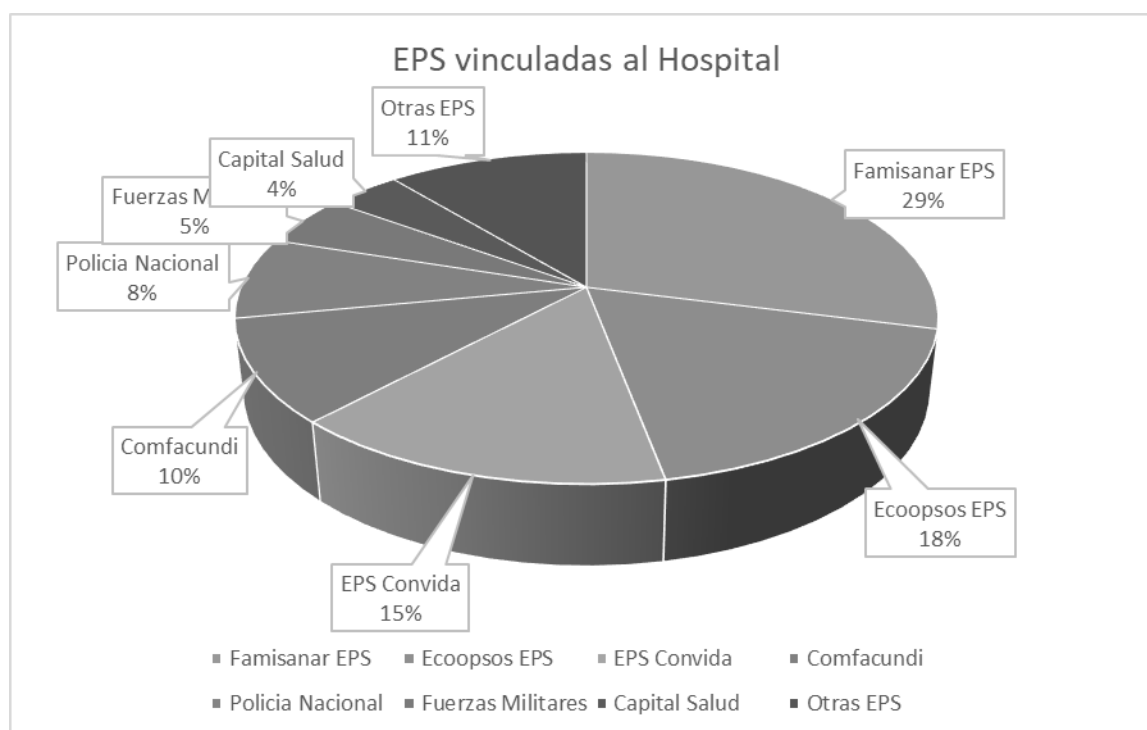


Figura 12. Promotoras de Salud EPS, vinculadas al hospital.

Fuente: Elaboración propia

3.2.3 dimensionamiento de la oferta.

Existen alrededor de 9.000 pacientes que serían los beneficiarios directos de la implementación de un sistema de seguridad de la información para salvaguardar información privada, más de 100 convenios con distintas EPS, universidades, proveedores y contratistas del sanatorio, así como 174 funcionarios de planta y más de 50 contratistas, que sentirán la seguridad de que su información personal esté asegurada.

3.2.4 precios.

Este proyecto, al ser interno del hospital, no tiene precio de venta. El análisis se basa en la cuantificación de los beneficios esperados. La tabla 1 presenta los beneficios cuantificados del proyecto.

Tabla 1. Beneficios cuantificados

BENEFICIO	VALOR (ANUAL)
	\$
Reduce los riesgos de seguridad de la información	30.000.000
Reduce la probabilidad y el impacto de los incidentes de seguridad	\$
	39.000.000
	\$
Posibilidad de obtener un certificado internacional	15.000.000
	\$
Ventaja de posicionamiento de la entidad en el sector	30.000.000
	\$
Focaliza el gasto en seguridad de la información	20.000.000
	\$
TOTAL	134.000.000

Fuente: Elaboración propia

3.2.5 punto de equilibrio oferta-demanda.

Basados en las estimaciones de la propuesta inicial (presupuesto asignado), el proyecto se pretende desarrollar en 1 año, a partir del cual se esperan beneficios económicos que irán contribuyendo a que se logre el punto de equilibrio.

Costo de implementación (CI) = \$ 300'000.000

Beneficios anuales cuantificados (BC) = \$ 134'000.000

Punto de equilibrio = $CI / BC = 2,24$ años

Se espera que el punto de equilibrio se encuentre alrededor de 2,3 años después de que el proyecto este implementado.

3.2.6 técnicas de predicción.

Debido a la dificultad de encontrar datos históricos de proyectos similares, puesto que la inversión para este sistema de gestión es elevada y abarca todos los aspectos tanto técnicos como operativos de la seguridad de la información, la técnica cualitativa que mejor se acomodó a nuestro estudio fue el método Delphi.

En el universo de expertos, se tuvieron en cuenta los siguientes perfiles:

- a) Experto en redes informáticas.
- b) Experto en ciberseguridad
- c) Experto en seguridad física y del entorno.
- d) Personal de planta de la institución que, por su conocimiento del entorno del proyecto y las características de este, pudo aportar ideas para la generación de soluciones.

3.3 Estudio económico-financiero

3.3.1 estimación de costos de inversión del proyecto.

El proyecto de implementación de un sistema de gestión de seguridad de la información consiste en garantizar la disponibilidad, integridad y confidencialidad de los sistemas de información en una entidad pública prestadora de servicios de salud.

Inicialmente se estima un presupuesto de 300 millones de pesos para el desarrollo del proyecto. Los cuales se deberán distribuir de la siguiente manera:

3.3.1.1 *inversión en equipos.*

Firewall o cortafuegos Ng Firewall F180 3 Year Basic Remote Access (Precio actual \$ 6'492.340).

Servidor NAS Noontec-terramaster F4-220 Servidor Nas De 4 Bahías Intel Du (Precio actual \$ 5'389.900).

Consola de antivirus (Precio actual \$ 2'250.000).

3.3.1.2 *inversión en personal.*

Personal que se contratara para el proyecto con sus costos asociados.

- a) 1 gerente de proyecto (Ingeniero con certificación PMP) (Salario base: \$ 3'500.000)
- b) 1 ingeniero de Sistemas (Experiencia en redes, sin especialización) (Salario base: \$ 2'700.000)
- c) 1 ingenieros de Sistemas (sin experiencia) (Salario base: \$ 1'700.000)
- d) 1 técnico en sistemas (Sin experiencia) (Salario base: \$ 1'200.000)
- e) 1 ingeniero experto en redes (Asesor externo) (Salario base: \$ 2'900.000)

- f) 1 ingeniero (Asesor externo en gerencia de proyectos) (Salario base: \$ 2'500.000)

3.3.1.3 inversión en software.

Antivirus Eset EndPoint 2017 Licencia para 250 pc (Precio actual \$ 2'250.000),

Software de acceso remoto TeamViewer V12 (Precio actual \$ 3'756.800)

Licencias SQL Server Ms (Precio actual \$ 4'606.800)

3.3.1.4 inversión en infraestructura.

Energía de respaldo ininterrumpida para los datacenter, cámaras de vigilancia en sitios críticos, lectores de acceso biométrico para todas las sedes. (Precio actual \$ 16'000.000)

3.3.2 definición de costos de operación y mantenimiento del proyecto.

La gestión de la Seguridad de la Información tiene unos costos asociados, que normalmente van vinculados a las siguientes actividades:

- a) Inventarios: una vez realizada la identificación, definición, descripción y valoración de los activos, se requiere una actualización constante de los mismos, de acuerdo con la dinámica de la organización y las políticas establecidas para la valoración de activos.
- b) Hacer seguimiento a la mejora continua del sistema que el propio estándar requiere.
- c) Analizar los riesgos e identificar nuevos riesgos que se pueden presentar.
- d) Controlar y actualizar el plan de continuidad del negocio.
- e) Integrar diversos controles de seguridad y control de riesgos.

- f) Mantenimiento del sistema en el largo plazo, reemplazo de equipos obsoletos y mantenimiento de estos.

Todos estos costos los asumirá la entidad una vez que el proyecto esté en su fase de mejora continua, mediante la contratación de un encargado de seguridad de la información o asignación de un responsable en el personal de planta, el cual apoyará y supervisará las tareas de mantenimiento del SGSI, con un costo aproximado de \$ 16'650.000 anual.

3.3.3 flujo de caja del proyecto caso.

La tabla 2 presenta el flujo de caja estimado del proyecto SGSI

Tabla 2. Flujo de caja del proyecto

Flujo de Caja SGSI				
Item		Valor	N° Pagos	
Firewall	\$	6.492.340	1	única vez
Servidor NAS	\$	5.389.900	1	única vez
ESET Antivirus 250 pc	\$	2.825.000	1	única vez
Teamviewer	\$	3.756.800	1	única vez
SQL server MS	\$	4.606.800	1	única vez
Infraestructura	\$	16.000.000	3	3 pagos
Personal Contratado	\$	14.900.000	12	12 meses
Stock de equipos	\$	22.000.000	1	única vez
Equipo de oficina	\$	2.500.000	1	única vez
Reservas	\$	25.629.160	1	única vez
Costo total	\$	300.000.000		
i(EA) - CDT a 360 días		6,53%	Tomado en base a los datos de Superfinanciera 20/05/2017	

Se toma la tasa actual de un CDT a 360 días debido a que los recursos provienen del estado para una entidad publica como lo es el Sanatorio Agua de Dios ESE.

Fuente: Elaboración propia

3.3.4 determinación del costo de capital, fuentes de financiación y uso de fondos.

La siguiente grafica muestra en flujo de inversiones del proyecto durante los 12 meses que vida útil del proyecto, entre los que se encuentran: 12 pagos de nómina (Nom), 1 pago de Firewall (FW), 1 pago de servidor de almacenamiento (NAS), 1 pago de consola de antivirus (Eset), 1 pago de software de acceso remoto (TV), 1 pago de servidor de base de datos (SQL), 3 pagos de infraestructura (INF), 1 pago de stok de equipos (Stk), 1 pago de equipo de oficina (E.of).

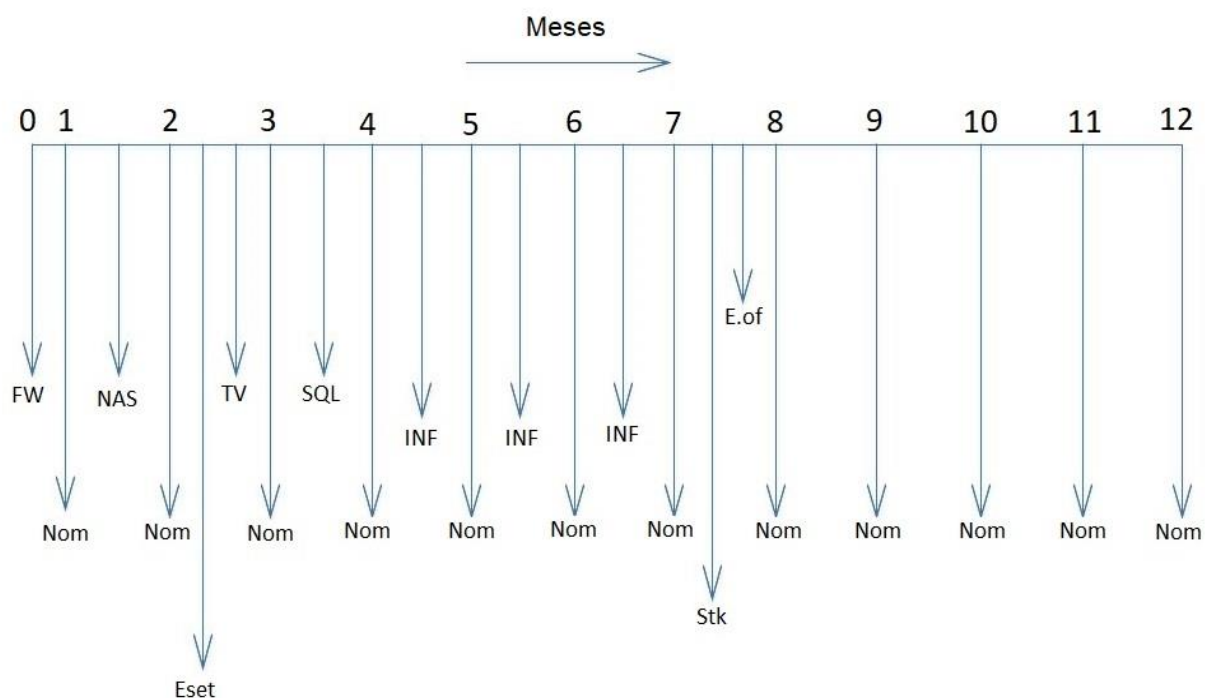


Figura 13. Diagrama de inversiones de capital.

Fuente: Elaboración propia

La fuente de financiación del proyecto se contempla en el presupuesto asignado de acuerdo con el plan estratégico de inversiones de la organización.

3.3.5 evaluación financiera del proyecto.

De acuerdo con las estimaciones realizadas en el flujo de caja, sección 3.3.3, y teniendo en cuenta los beneficios cuantificados desarrollados en la sección 3.2.4, se realiza un el cálculo de la VAN del proyecto. El análisis de los beneficios se presenta en valor presente y la tasa de interés se fija en 6,53% EA. La tabla 3 presenta el cálculo del valor neto actual de acuerdo con las estimaciones realizadas.

Tabla 3. Cálculo del valor actual neto

Mes	CASH FLOWS		
	Inversiones	Beneficios	VAN
0	-\$ 6.492.340	-\$	6.492.340
1	-\$ 20.289.900	-\$	20.180.087
2	-\$ 17.725.000	-\$	17.533.656
3	-\$ 18.656.800	-\$	18.355.513
4	-\$ 19.506.800	-\$	19.087.916
5	-\$ 30.900.000	-\$	30.072.815
6	-\$ 30.900.000	-\$	29.910.055
7	-\$ 30.900.000	-\$	29.748.175
8	-\$ 36.900.000	-\$	35.332.253
9	-\$ 14.900.000	-\$	14.189.737
10	-\$ 14.900.000	-\$	14.112.939
11	-\$ 17.400.000	-\$	16.391.684
12	-\$ 40.529.160	\$ 134.000.000	\$ 96.026.113
24		\$ 134.000.000	\$ 134.000.000
26		\$ 22.333.333	\$ 22.333.333
VAN Proyecto			\$ 952.276

Fuente: Elaboración

A partir del mes 12, se comienzan a recibir los beneficios descritos, por lo cual se obtiene que para el mes 26 el valor actual neto es positivo ($VAN > 0$), por lo cual en este mes se garantiza un retorno de la inversión.

3.4 Estudio social y ambiental

3.4.1 descripción y categorización de impactos ambientales.

3.4.1.1 análisis PESTLE.

Consiste en el análisis de los factores políticos, económicos, sociales, tecnológicos, legales y ecológicos del proyecto. (Ver anexo A)

3.4.2 definición de flujo de entradas y salidas.

En la tabla 4, se presenta las entradas y salidas ambientales para el proyecto.

Tabla 4. Definición de entradas y salidas ambientales

Entradas	Etapas	Salidas
Diagnóstico del SGSI		
Energía eléctrica	Computadores, impresoras, aire acondicionado, ups	Calor
Papel		Papel usado
Tinta		Cartuchos
Lapiceros		Plástico
Planificación del SGSI		
Energía eléctrica	Computadores, impresoras, aire acondicionado, ups, plotter, vehiculó	Calor
Papel		Papel usado
Tinta		Documentación
Lapiceros		Cartuchos
Combustible		Plástico
		Emisiones
Implementación		
Energía eléctrica	Computadores, impresoras, aire acondicionado, ups,	Calor
Papel		Papel usado
Tinta		Cartuchos

Entradas	Etapas	Salidas
Lapiceros	plotter, video	Plástico
Transporte	proyector, vehículo	Emisiones, polución
Combustible		
Cables y conectores		Residuos reciclables
Equipos de comunicación		Residuos electrónicos
Evaluación		
Energía eléctrica		Calor
Papel	Computadores,	Papel usado
Tinta	impresoras, aire	Cartuchos
Lapiceros	condicionado, ups,	Plástico
Transporte	plotter, video	
Combustible	proyector, vehículo	Emisiones, polución
Cierre		
Energía eléctrica		Calor
Papel		Papel usado
Tinta	Computadores,	Cartuchos
Lapiceros	impresoras, aire	Plástico
Transporte	condicionado, ups,	
Combustible		Emisiones, polución

Fuente: Elaboración propia

3.4.3 estrategias de mitigación de impacto ambiental.

3.4.3.1 análisis de impactos.

En el análisis de impactos se tienen en cuenta los impactos asociados al uso de materias primas e insumos y los impactos asociados al producto que deriva del proyecto.

3.4.3.1.1 Impactos asociados al uso de materias primas e insumos

a) Impactos ambientales.

En el proyecto de implementación de un sistema de gestión en seguridad de la información se utilizan una gran variedad de equipos tecnológicos como son: computadores de escritorio y laptops, teléfonos celulares, teléfonos de mesa, tabletas, antenas de radio frecuencia, switches y routers, video beam, equipos de sonido, aires acondicionados, ventiladores, que serán la base de nuestras operaciones de oficina y campo. Dichos dispositivos una vez que terminan con su vida útil o los desechamos por su obsolescencia, se convierten en contaminación tecnológica. La mayoría de estos dispositivos ha sido fabricada con materiales como silicio y plomo, con los cuales, si no se realiza una disposición final adecuada pueden comprometer seriamente nuestro entorno, generando contaminación y graves consecuencias ambientales.

El transporte de estos dispositivos tecnológicos, generalmente desde países donde la mano de obra es barata, también genera impacto ambiental, pues en el transporte de estos se utilizan grandes cantidades de combustible que emiten gases contaminantes a la atmosfera.

b) Impactos sociales.

Los impactos sociales en la producción tecnológica se evidencian en mayor medida en los países emergentes, en los cuales la mano de obra es abundante y barata, por lo cual las grandes corporaciones instalan allí sus fábricas y aprovechan tanto los recursos naturales de estos lugares como las necesidades laborales y económicas de la sociedad.

c) Impactos económicos.

También existen impactos económicos en la generación de tecnología en países de bajos recursos económicos, las jornadas laborales son extenuantes y nunca se

compensa de la mejor manera estos trabajos, generando riqueza únicamente a las compañías que la producen y que no se ve retribuido en la sociedad ni en el país en donde se origina esta tecnología.

3.4.3.1.2 Impactos asociados al uso del producto que deriva del proyecto

Los impactos ambientales derivados del producto a desarrollar en nuestro proyecto son principalmente los asociados a los residuos electrónicos y emisiones de gases a la atmosfera.

Se contemplan los residuos tecnológicos puesto que el proyecto requiere grandes inversiones en nuevo hardware y software, para realizar actualización de equipos, muchos de los cuales ya se encuentran obsoletos o simplemente no cumplen con las especificaciones requeridas para pertenecer a los inventarios del proyecto.

Para estos se debe disponer de una clara política de reciclaje y disposición final de los residuos, puesto que estos desechos son una importante fuente de contaminación.

En el caso específico de los impactos sociales en la implementación de un sistema de gestión en seguridad de la información para el hospital de Agua de Dios, se pueden tener en cuenta los siguientes:

- d) Limitaciones y acceso restringido a páginas de internet por parte de los usuarios.
- e) Administración segura de contraseñas para todos los usuarios de la red.
- f) Limitación de uso de espacios y acceso no autorizados.
- g) Uso adecuado de roles en los usuarios del sistema.
- h) Divulgación de instructivos, manuales y políticas en seguridad de la información.

Todas estas actividades requieren divulgación, capacitación y sensibilización por parte de los usuarios, los cuales en muchas ocasiones se resisten al cambio por considerarlo engorroso, sin conocer los beneficios reales que genera una buena gestión en cuanto a la seguridad de la información en un entorno de trabajo.

3.4.3.1.3 Disposición final de los productos y equipos

Colombia es hoy referente en América Latina por el uso responsable y el aprovechamiento de los residuos electrónicos. Cerca del 90% de los residuos tecnológicos son aprovechables. (RELAC, 2011)

Las acciones empleadas por el Ministerio son la recolección y transporte hasta Bogotá para demanufacturar y convertirlos en materiales limpios para otras empresas en el Centro de Aprovechamiento de Residuos Electrónicos (Cenare), de Computadores para Educar. Allí, los equipos obsoletos o en desuso son sometidos a un proceso de demanufactura que consiste en la separación, limpieza y clasificación de las partes de los computadores.

Basados en estas directrices, en este proyecto se pretende realizar los contactos correspondientes con el MINTIC, para la disposición final de los residuos electrónicos.

3.4.3.2 matriz de sostenibilidad ambiental P5.

El Estándar P5 es una herramienta que brinda soporte para la alineación de programas y proyectos con la estrategia organizacional para la sostenibilidad y se centra en los impactos de los procesos y entregables de los proyectos en el Medio Ambiente, en la Sociedad. La matriz de sostenibilidad ambiental P5 se muestra cómo anexo (Ver anexo B).

3.4.3.3 matriz de requisitos legales y normatividad aplicable al proyecto.

La matriz de requisitos legales es el documento que contiene toda la información sobre la normatividad que una empresa debe cumplir legalmente. Están moderadas por diferentes mecanismos que buscan que una empresa evidencie el cumplimiento de la normatividad concerniente a la seguridad y salud en el trabajo.

La matriz de requisitos legales se incluye como anexo (Ver anexo C)

4 Evaluación y formulación

4.1 Planteamiento del problema

El proyecto de implementación de un sistema de gestión de seguridad de la información consiste en garantizar la disponibilidad, integridad y confidencialidad de los sistemas de información en una entidad pública prestadora de servicios de salud.

La implementación de la seguridad de la información es crítica hoy en día, y está presente en muchas situaciones cotidianas. Las técnicas empleadas para proteger la información como los controles de acceso mediante usuario y contraseña no son suficientes en la actualidad para protegernos de ataques y delincuentes informáticos.

La gran cantidad de bases de datos ubicadas en sistemas de computación públicos y privados que contienen información sensible de los usuarios (bancaria, judicial, de seguros, de salud, educación, etc.) conforman un riesgo potencial de invasión a la privacidad.

En el ámbito médico, las bases de datos y protección de la privacidad, integridad y disponibilidad de la información, como las historias clínicas computarizadas, movimientos financieros e inventarios se ven amenazados y son atacados frecuentemente por delincuentes informáticos.

Para proteger la información y asegurarnos que esta no sea leída o adultera el sistema debe emplear diversas técnicas descritas en la norma ISO 27000 sobre seguridad de la información.

Es conocido que las pérdidas económicas y de reputación de la empresa son gigantescas cuando se presentan fallas en la seguridad de la información. El hurto y adulteración de bases de datos es frecuente en nuestros tiempos, por lo cual los costos asociados a la implementación en seguridad de la información son sustancialmente bajos, comparados con el impacto negativo que tendría un evento adverso en la información almacenada.

Para el caso concreto del Hospital de Agua de Dios, se observa que, aunque se tiene conocimiento de la importancia del proyecto en seguridad de la información, su formulación no ha sido la adecuada, por lo cual no se reflejan avances en el mismo desde hace más de dos años. No existe quien dirija los esfuerzos del grupo de profesionales en TIC para lograr materializar la idea de proyecto.

4.1.1 Análisis de involucrados.

Una vez analizado el entorno y la organización donde se desarrollará el proyecto, se logran identificar 8 grupos de involucrados descritos a continuación.

- a) *Alta gerencia.* Su compromiso abarca todas las etapas del proyecto, desde su inicio hasta su cierre. Encargada de la gestión de los recursos. Interés alto.
- b) *Ministerio TIC.* Establece los lineamientos mediante los cuales se rige el desarrollo del proyecto. Interés moderado.
- c) *Personal del área de Tecnología.* Encargado de ejecutar cada una de las fases del proyecto, siguiendo los lineamientos de la dirección y del ministerio. Interés alto.

- d) *Líderes de proceso*. Son los encargados de velar que las directrices impartidas en el marco del proyecto sean acatadas, respetadas y aceptadas por todos los funcionarios de la entidad. Interés moderado.
- e) *Funcionarios*. Deberán regirse por las políticas, procedimientos y herramientas desarrolladas en el marco del proyecto. Interés bajo.
- f) *Usuarios*. Los usuarios para este proyecto son los clientes y pacientes de la IPS Sanatorio agua de dios ESE. Se verán beneficiados directamente por la implementación de este proyecto. Interés moderado.
- g) *Contratistas*. Beneficiarios directos, algunos de ellos encargados de ejecutar ciertos procesos de apoyo e implementación dentro del proyecto Interés moderado.
- h) *Proveedores*. Beneficiarios directos interés bajo.

4.1.2 árbol de problemas.

El árbol de problemas se muestra según la figura 14.

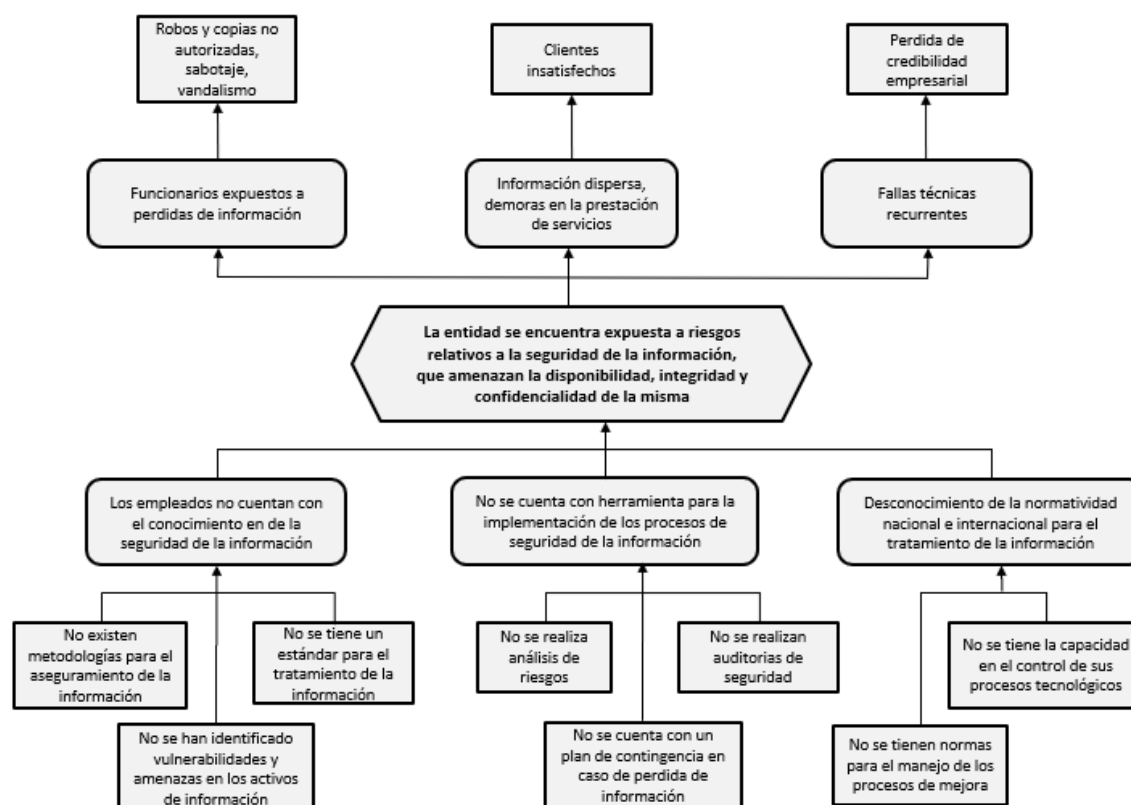


Figura 14. Árbol de problemas. Fuente: Elaboración propia

4.1.3 árbol de objetivos.

El árbol de objetivos se muestra según la figura 15.

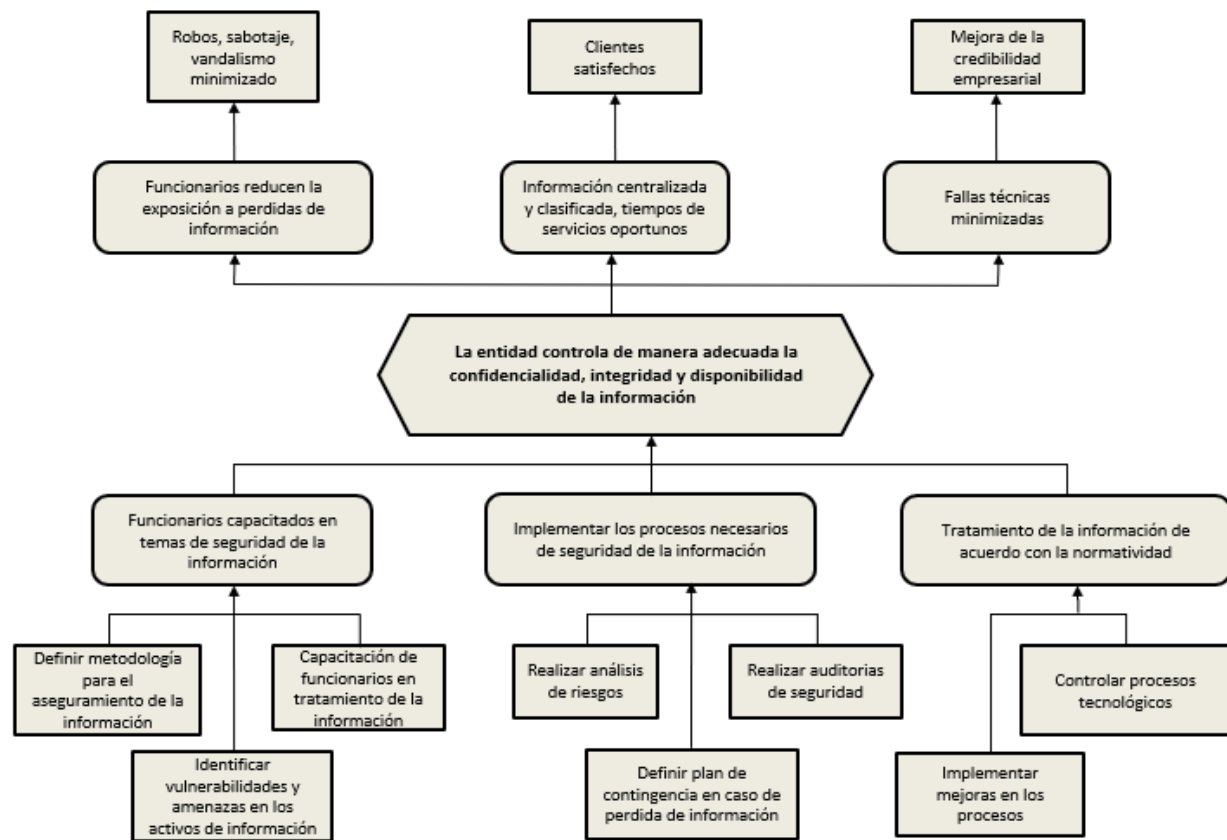


Figura 15. Árbol de objetivos. Fuente: Elaboración propia

4.2 Alternativas de solución

4.2.1 identificación de acciones y alternativas.

A partir de las raíces del árbol de problemas, se proponen las siguientes acciones tendientes a reducir el problema, es decir, lograr el objetivo propuesto.

Implementar una metodología para el manejo de la información, mediante implementación de normas y estándares internacionales, cumpliendo así con la normatividad de MINTIC. Con base en esto se sugiere seguir el estándar ISO 27000 para el tratamiento de la información.

Para la identificación de amenazas se requiere: conformación de un comité que realice la identificación, o el uso de software específico de análisis de amenazas. Realizar el análisis de riesgos mediante la contratación de asesor externo, o realizar el análisis de riesgos mediante el comité de seguridad de la información. Se realiza un plan de contingencia con el uso de servidores de respaldo de información mediante almacenamiento de respaldo en la nube, o mediante servidores físicos instalados en el data center. Realización de un cronograma de auditorías externas o realizar auditorías internas del SGSI.

4.2.2 descripción de alternativa seleccionada.

Teniendo en cuenta el costo que representa la certificación en ISO 27000, no se tendrá en cuenta esta opción en la ejecución del proyecto. No obstante, el producto cumplirá todos los requisitos administrativos y técnicos para una futura certificación, si así lo requiere la entidad.

Se selecciona alternativa de almacenamiento físico tradicional dada la infraestructura y aprovechamiento de locaciones. El almacenaje en la nube se toma

como una opción a futuro, adecuando la infraestructura para una vez finalizado el proyecto.

Dado que la implementación del sistema debe conformar un comité de seguridad de la información, este se encargará de la identificación de amenazas y riesgos, descartando por costos la opción de software especializado y equipos de expertos externos.

Se define la realización de auditorías internas periódicas durante el desarrollo del proyecto. Las auditorías externas estarán para disposición de la entidad una vez finalizado el proyecto.

4.2.3 justificación del proyecto.

La Entidad SANATORIO DE AGUA DE DIOS E.S.E. como entidad prestadora de servicios de salud, consciente de la necesidad de mantener la seguridad y privacidad de la información que maneja, se ve en la obligación de implementar un sistema de gestión de seguridad de la información. El problema de la seguridad de la información se caracteriza por la complejidad y la interdependencia. La gestión de la seguridad contiene un número importante de factores y elementos que se interrelacionan entre sí. Las Micro, pequeñas y medianas empresas por lo general tienen una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridad olvidadas. De ahí la gran importancia de implementar es este proyecto al interior de la Institución.

5 Inicio del proyecto

5.1 Caso de negocio

El caso de negocio es un documento que representa la base estructural del proyecto. Este documento se presenta como anexo (Ver Anexo D)

5.2 Gestión de la integración

5.2.1 acta de constitución (Project Charter).

El acta de constitución del proyecto (Project Charter) es el documento emitido por el patrocinador, que autoriza la existencia del proyecto. El acta de constitución del proyecto SGSI se presenta como anexo (Ver Anexo E).

5.2.2 actas de cierre del proyecto o fase.

El acta de cierre de proyecto incluye la información de los entregables, responsables y criterios de aceptación (Ver Anexo F. Acta de cierre SGSI).

6 Planes de gestión

6.1 Plan de gestión del alcance

6.1.1 línea base del alcance.

La línea base del alcance está compuesta por el enunciado del alcance del proyecto y la estructura de desagregación de trabajo (EDT).

6.1.1.1 enunciado del alcance.

El enunciado del alcance es un documento que proporciona las bases para las futuras tomas de decisiones tales como cambios en el alcance del proyecto. Su propósito es asegurar que todos los interesados tengan un conocimiento común del alcance del proyecto. En este documento se incluyen los objetivos, la descripción de los entregables, el resultado o producto final, los supuestos y restricciones que pueden causar un impacto en el desarrollo del cronograma del proyecto y la justificación del proyecto y define los criterios de aceptación establecidos por el usuario del producto. El enunciado del alcance del proyecto SGSI se presenta como anexo (Ver Anexo G).

6.1.1.2 estructura de desglose de trabajo (EDT).

La figura 16 presenta la estructura de desglose de trabajo (EDT) para el proyecto.

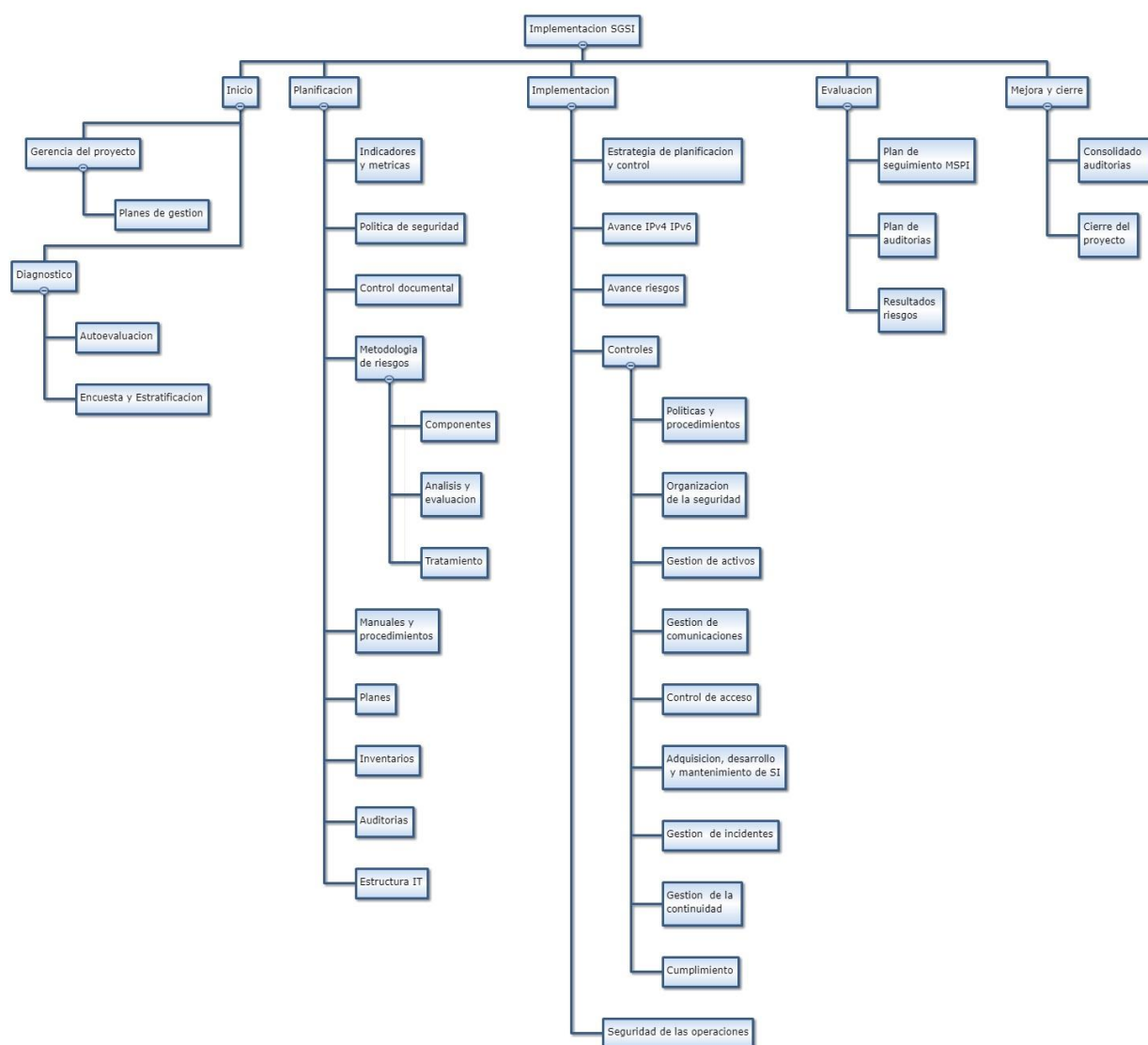


Figura 16. Estructura de desglose de trabajo.

Fuente: Elaboración propia

6.1.2 matriz de trazabilidad de requisitos.

De acuerdo a la definición establecida por el PMI, “la matriz de trazabilidad de requisitos es un cuadro que vincula los requisitos del proyecto desde su origen hasta los entregables que lo satisfacen” (PMI, 2013).

Basado en los lineamientos y controles de la norma NTC-ISO-EIC 27001 en su anexo 5, se presenta la matriz de trazabilidad de requisitos para el proyecto de implementación del SGSI en la entidad.

Para una mejor identificación de los requisitos, se realiza una desagregación de los requisitos. El anexo H indica la matriz de trazabilidad de requisitos administrativos del proyecto. El anexo I indica la matriz de trazabilidad de requisitos técnicos del proyecto.



Figura 17. Desagregación de la matriz de trazabilidad de requisitos.

Fuente: Edición propia

6.1.3 diccionario de la EDT.

El diccionario de la EDT del proyecto nos proporciona información detallada sobre los entregables, actividades y programación de cada uno de los componentes del proyecto SGSI. (Ver anexo J).

6.2 Plan de gestión del cronograma

6.2.1 listado de actividades con estimación de duraciones esperadas.

Listado de actividades del proyecto con la estimación de duraciones esperadas se muestra en el anexo (Ver anexo K).

6.2.2 línea base de tiempo.

6.2.2.1 cronograma en Project.

El anexo L presenta el cronograma de actividades realizado en MS Project.

6.2.2.2 cronograma de hitos.

La figura 18 presenta el cronograma de hitos del proyecto SGSI.



Figura 18. Cronograma de hitos. Fuente: Edición propia

6.2.3 diagrama de red.

El diagrama de red se encuentra como anexo (Ver anexo M. Diagrama de red SGSI)

6.2.4 diagrama de Gantt.

La figura 19 representa el diagrama de Gantt del proyecto, en donde se puede visualizar la ruta crítica.

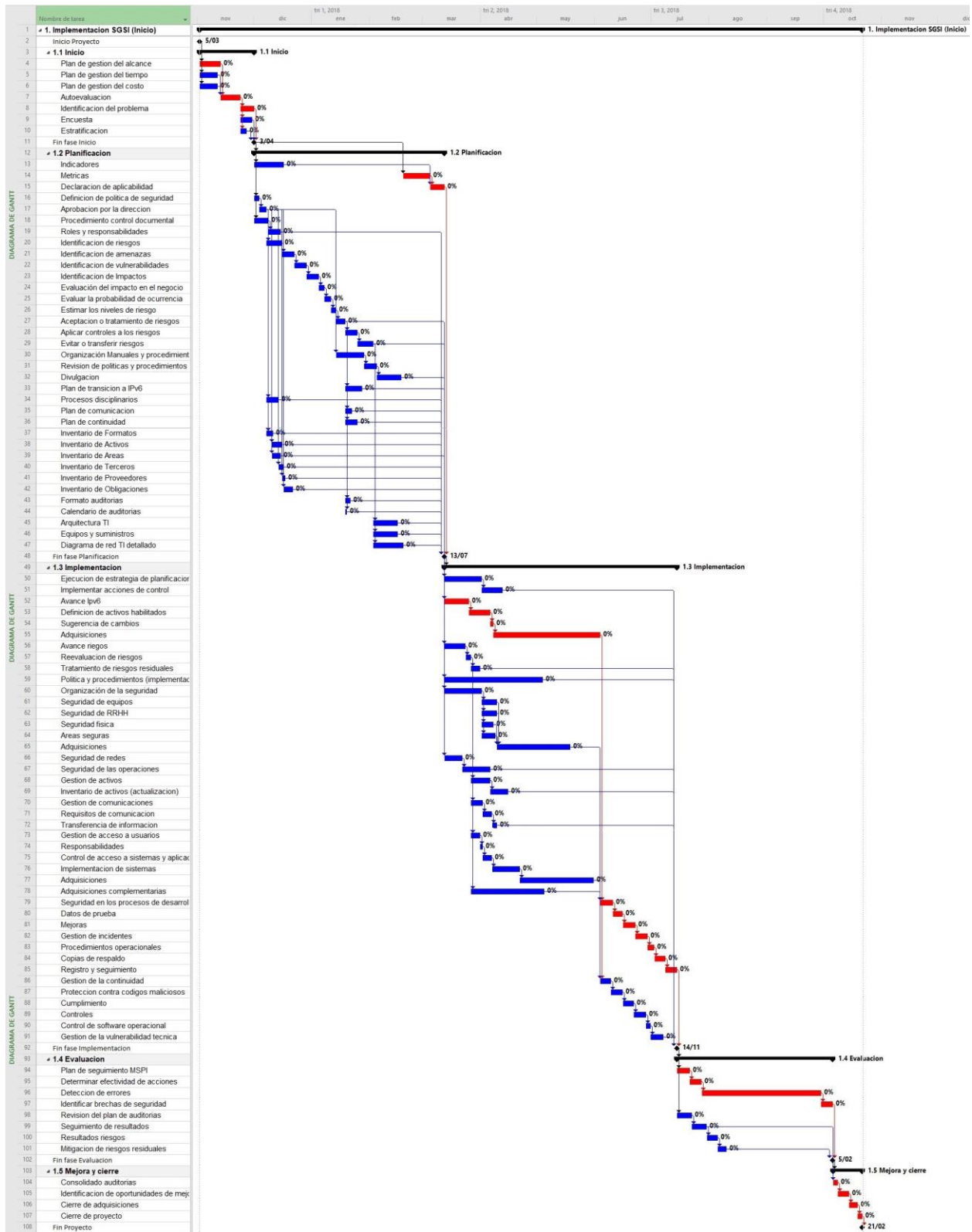


Figura 19. Diagrama de Gantt.

Fuente: Edición propia

6.2.5 nivelación de recursos y uso de recursos.

6.2.5.1 nivelación de recursos.

La tabla 5 presenta los recursos definidos para el proyecto. Algunas sobreasignaciones presentadas en personal y equipo se solucionaron aumentando el tiempo de la actividad o reprogramando ciertas actividades hasta que el recurso estuviera disponible.

Tabla 5. Recursos de trabajo, material y costo para el proyecto

Nombre del recurso	Tipo	Iniciales	Grupo	Capacidad máxima	Tasa estándar
Gerente de proyecto	Trabajo	GP	Personal	100%	\$35.000/hora
Ingeniero Líder	Trabajo	IL	Personal	100%	\$25.000/hora
Ingeniero Asistente	Trabajo	IA	Personal	100%	\$20.000/hora
Técnico	Trabajo	TEC	Personal	100%	\$15.000/hora
Asesor TI	Trabajo	ATI	Personal	100%	\$35.000/hora
Asesor GP	Trabajo	AGP	Personal	100%	\$25.000/hora
Computador Desktop	Trabajo	COMP	Equipo	100%	\$3.000/hora
Computador Laptop	Trabajo	CLP	Equipo	100%	\$3.500/hora
Impresora	Trabajo	I	Equipo	100%	\$500/hora
Celular 1	Trabajo	C1	Equipo	100%	\$500/hora
Celular 2	Trabajo	C2	Equipo	100%	\$500/hora
Video Proyector	Trabajo	VP	Equipo	100%	\$3.500/hora
Vehículo	Trabajo	Veh	Equipo	100%	\$25.000/hora
Firewall	Material	FW	Equipo		\$6.492.000
NAS	Material	NAS	Equipo		\$5.389.000
Antivirus	Material	AV	Equipo		\$2.250.000
TeamViewer	Material	TV	Equipo		\$3.756.000
SQL Server	Material	SQ	Equipo		\$4.606.000
Energía de respaldo	Material	UPS	Equipo		\$8.000.000
Cámaras de Vigilancia	Material	CCTV	Equipo		\$6.000.000

Nombre del recurso	Tipo	Iniciales	Grupo	Capacidad máxima	Tasa estándar
Lector biométrico	Material	LB	Equipo		\$2.000.000
Aire acondicionado	Material	AA	Equipo		\$800.000
Servidor de aplicaciones	Material	Sapp	Equipo		\$5.000.000
Servidor de base de datos	Material	Sdb	Equipo		\$5.000.000
Servidor datos de prueba	Material	Sdp	Equipo		\$5.000.000
Computadores nuevos	Material	C	Equipo		\$25.000.000
Transporte	Costo	Tp			NA
Implementación de UPS	Costo	UPS			NA
Implementación Firewall	Costo	Imp Fw			NA
Implementación NAS	Costo	IN			NA
Implementación Antivirus	Costo	IAV			NA
Implementación servidores	Costo	IS			NA

Fuente. Elaboración propia

6.2.5.2 uso de recursos.

La figura 20 representa el uso de recursos definidos para el proyecto

	i	Nombre del recurso	Trabajo	Detalles	tri 4, 2017		tri 1, 2018		tri 2, 2018		tri 3, 2018		tri 4, 2018	
					oct	nov	ene	feb	mar	abr	may	jun	ago	sep
USO DE RECURSOS		▷ Sin asignar	0 horas	Trabajo										
	1	▷ Gerente de proyecto	502 horas	Trabajo	20h	8h	34h	30h	54h	40h	70h	38h	53,43h	50,57h
	2	▷ Ingeniero Lider	726 horas	Trabajo	78h	67,8h	90,2h	72,67h	99,33h	68h	10h	66h	56,5h	37,5h
	3	▷ Ingeniero Asistente	792 horas	Trabajo	10h	99,75h	92,25h	96h	100h	62h	10h	80h	42,5h	34,03h
	4	▷ Tecnico	511 horas	Trabajo	22h	78,8h	20,2h	78h	36h	90h	10h	24h	32h	31,9h
	5	▷ Asesor TI	456 horas	Trabajo	20h	8h	108h	72h	42h	56h	8h	48h	52,5h	41,5h
	6	▷ Asesor GP	364 horas	Trabajo	30h	2h	62h		46h	48h	8h	36h	54,25h	29,75h
	7	▷ Firewall	1 Unidad	Trabajo (U)					1					
	8	▷ NAS	1 Unidad	Trabajo (U)					1					
	9	▷ Antivirus	1 Unidad	Trabajo (U)							1			
	10	▷ TeamViewer	1 Unidad	Trabajo (U)					1					
	11	▷ SQL Server	1 Unidad	Trabajo (U)					1					
	12	▷ Energia de respaldo	1 Unidad	Trabajo (U)				0,63	0,38					
	13	▷ Camaras de Vigilancia	1 Unidad	Trabajo (U)					1					
	14	▷ Lector biometrico	2 Unidad	Trabajo (U)					0,83	0,56	0,49	0,12		
	15	▷ Aire acondicionado	4 Unidad	Trabajo (U)					0,08	2,53	1,25	0,14		
	16	▷ Computador Desktop	760 horas	Trabajo	13,7h	103,3h	92,68h	42,35h	80,97h	63,53h	4,52h	113,18h	94,25h	29,62h
	17	▷ Computador Laptop	745 horas	Trabajo	26,45h	110,55h	101h	76,05h	49,63h	83,25h	8,95h	29,95h	80,62h	34,57h
	18	▷ Impresora	29 horas	Trabajo	5h			24h						
	19	▷ Celular 1	766 horas	Trabajo	11,4h	77,6h	89,85h	49,18h	86,97h	63,53h	4,52h	113,18h	94,25h	29,62h
	20	▷ Celular 2	615 horas	Trabajo	20,9h	70,1h	97h	30h	39,68h	83,25h	8,95h	29,95h	80,62h	34,57h
	21	▷ Video Proyector	108 horas	Trabajo		2h	8h	24h	14,18h	26,52h	1,32h			
	22	▷ Vehiculo	196 horas	Trabajo	1,9h	12,1h		1,22h	108,8h	14,23h	1,77h			
	23	▷ Transporte		Trabajo										
	24	▷ Implementacion energia de		Trabajo										
	25	▷ Implementacion Firewall		Trabajo										
	26	▷ Implementacion NAS		Trabajo										
	27	▷ Implementacion Antivirus		Trabajo										
	28	▷ Implementacion servidores		Trabajo										
	29	▷ Servidor de aplicaciones	1	Trabajo			1							
	30	▷ Servidor de base de datos	2	Trabajo			2							
	31	▷ Servidor datos de prueba	1	Trabajo			1							
	32	▷ Computadores nuevos	1	Trabajo					0,56	0,44				

Figura 20. Uso de recursos.

Fuente. Elaboración propia

6.3 Pan de gestión del costo

6.3.1 línea base de costos.

A continuación, se presentan los costos estimados de los paquetes de trabajo, cuentas control y reservas de contingencia y gestión. La tabla 6 presenta los costos de los paquetes de trabajo. La tabla 7 presenta el presupuesto de costos estimado para las cuentas de control. La tabla 8 presenta el presupuesto de costos del proyecto sumando todas las cuentas de control.

Tabla 6. Presupuesto estimado de los paquetes de trabajo

ID-PT	PAQUETE DE TRABAJO	COSTO
I-0	INI (A-B-C)	\$ 1.868.000
D-1	DIAG (D-E)	\$ 2.571.500
D-2	DIAG (F-G)	\$ 1.016.000
P-1	PLAN (H-I-J)	\$ 2.074.000
P-2	PLAN (K-L)	\$ 374.000
P-3	PLAN (M-N)	\$ 1.490.000
P-4	PLAN (O-P-Q-R)	\$ 2.904.000
P-5	PLAN (S-T-U)	\$ 3.520.000
P-6	PLAN (V-W-X)	\$ 2.590.000
P-7	PLAN (Y-Z-AA)	\$ 4.371.000
P-8	PLAN (AB-AC-AD-AE)	\$ 23.358.000
P-9	PLAN (AF-AG-AH-AI-AJ-AK)	\$ 1.295.000
P-10	PLAN (AL-AM)	\$ 553.000
P-11	PLAN (AN-AO-AP)	\$ 32.114.000
I-1	IMP (AQ-AR)	\$ 1.074.000
I-2	IMP (AS-AT-AU-AV)	\$ 4.572.000
I-3	IMP (AW-AX-AY)	\$ 2.254.000
I-4	IMP (AZ)	\$ 2.945.000

ID-PT	PAQUETE DE TRABAJO	COSTO
I-5	IMP (BA-BB-BC-BD-BE-BF-BG-BH)	\$ 58.512.000
I-6	IMP (BI-BJ)	\$ 319.000
I-7	IMP (BK-BL-BM)	\$ 6.671.000
I-8	IMP (BN-BO-BP-BQ-BR)	\$ 13.418.000
I-9	IMP (BS-BT-BU-BV)	\$ 5.858.000
I-10	IMP (BW-BX-BY-BZ)	\$ 4.654.000
I-11	IMP (CA-CB)	\$ 3.254.000
I-12	IMP (CC-CD-CE-CF)	\$ 2.625.000
E-1	EVAL (CG-CH-CI-CJ)	\$ 7.590.000
E-2	EVAL (CK-CL)	\$ 3.094.000
E-3	EVAL (CM-CN)	\$ 3.402.000
M-1	CO-CP	\$ 5.812.000
C-1	CQ-CR	\$ 4.556.000
TOTAL		\$ 210.708.500

Fuente. Elaboración propia

Tabla 7. Presupuesto estimado de las cuentas control

ID-CT	CUENTA CONTROL	COSTO
CT-1	Cuenta control inicio	\$ 5.455.500
CT-2	Cuenta control planificación	\$ 74.643.000
CT-3	Cuenta control implementación	\$ 106.156.000
CT-4	Cuenta control evaluación	\$ 14.086.000
CT-5	Cuenta control mejora y cierre	\$ 10.368.000
TOTAL		\$ 210.708.500

Fuente. Elaboración propia

La siguiente tabla muestra el presupuesto de costos, teniendo en cuenta la reserva para contingencias calculada en el plan de gestión de riesgos, sección 6.7.3.2, según tabla 24.

Tabla 8. Presupuesto de costos

ID	ITEM	COSTO
SGSI	PROYECTO	\$ 210.708.500
R-CTG	RESERVA PARA CONTINGENCIAS	\$ 69.800.000
LINEA BASE DE COSTOS		\$ 280.508.500
	RESERVA DE GESTION	\$ 28.050.850
TOTAL		\$ 308.559.350

Fuente. Elaboración propia

6.3.2 presupuesto por actividades.

El presupuesto estimado para las actividades de las fases de inicio, planificación, implementación, evaluación, mejora y cierre del proyecto SGSI, se presentan como anexo (Ver Anexo N).

6.3.3 estructura de desagregación de recursos ReBS y estructura de desagregación de costos CBS.

La figura 21 muestra la estructura de desagregación de recursos del proyecto.

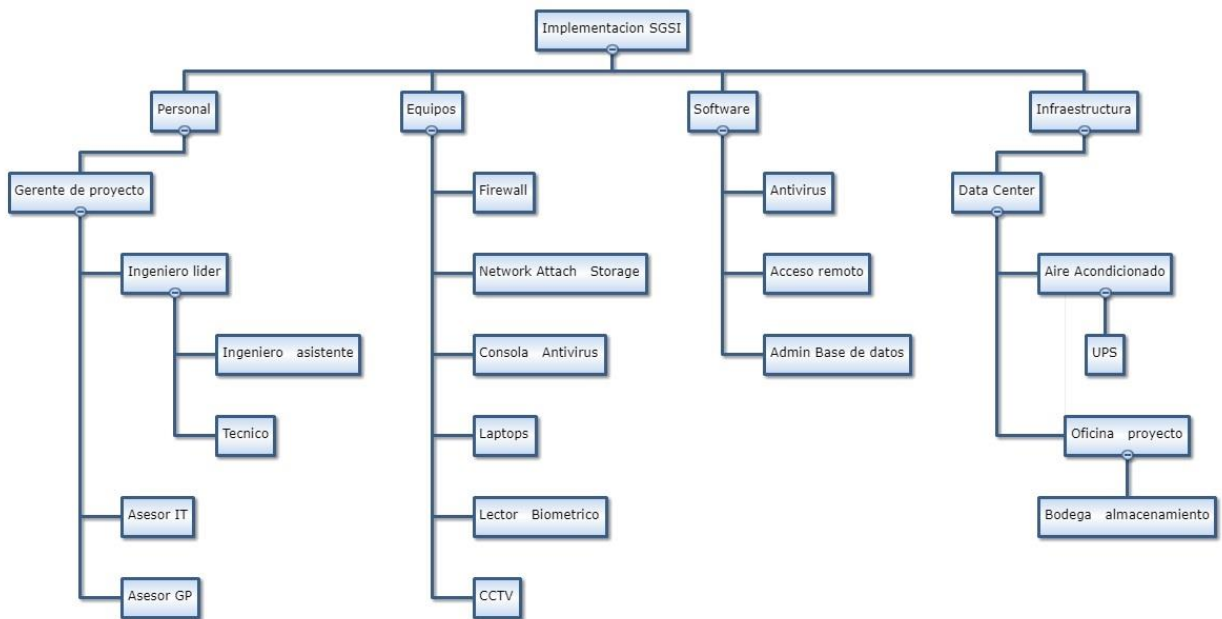


Figura 21. ReBS.

Fuente: Edición propia

La figura 22 muestra la estructura de desagregación de costos del proyecto.

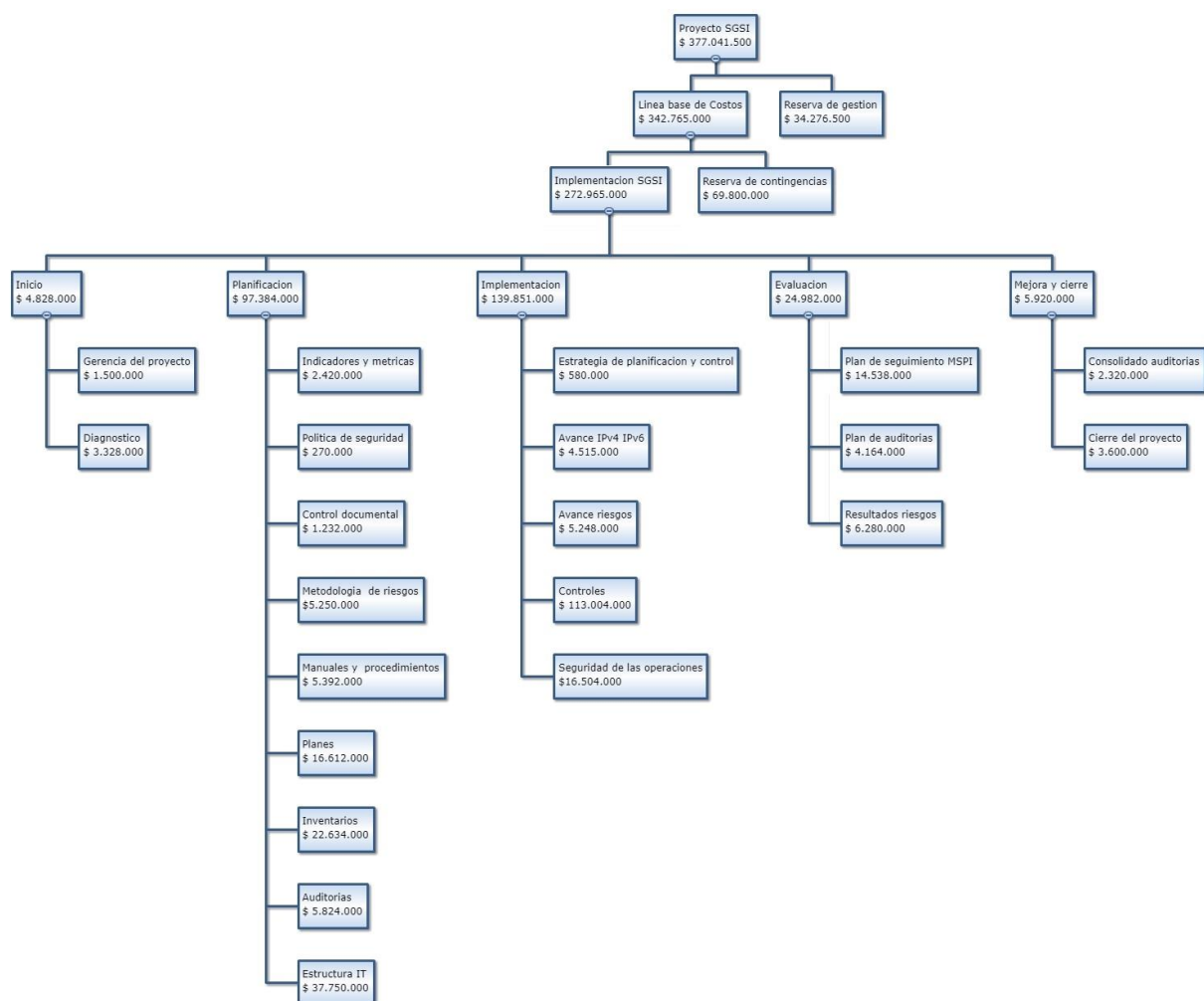


Figura 22. CBS.

Fuente: Edición propia

6.3.4 indicadores de medición de desempeño.

La explicación detallada de los indicadores de medición de desempeño utilizados se presenta en el anexo (Ver Anexo O). La figura 23 presenta los indicadores de medición del desempeño realizados en MS Project.

	Nombre de tarea	Valor planeado: PV	Valor acumulados: EV	AC (Costo actual)	SV	CV	SPI	CPI	BAC	EAC	ETC	VAC	TCPI
1	1. Implementacion S	\$21.772.752	\$20.390.066	\$20.989.191	-\$1.382.687	-\$599.125	0,94	0,97	\$218.123.502	\$224.533.827		\$0	1
2	Inicio Proyecto	\$0	\$0	\$0	\$0	\$0	0	0	\$0	\$0	\$0	\$0	0
3	1.1 Inicio	\$6.554.502	\$6.554.502	\$6.554.502	\$0	\$0	1	1	\$5.455.502	\$5.455.502	\$0	\$0	1
11	Fin fase Inicio	\$0	\$0	\$0	\$0	\$0	0	0	\$0	\$0	\$0	\$0	0
12	1.2 Planificacion	\$15.218.250	\$13.835.563	\$14.434.688	-\$1.382.687	-\$599.125	0,91	0,96	\$74.643.000	\$77.875.555	\$0	-\$3.232.555	1,01
48	Fin fase Planificaci	\$0	\$0	\$0	\$0	\$0	0	0	\$0	\$0	\$0	\$0	0
49	1.3 Implementacion	\$0	\$0	\$0	\$0	\$0	0	0	\$106.696.000	\$106.696.000	\$0	\$0	1
92	Fin fase Implemen	\$0	\$0	\$0	\$0	\$0	0	0	\$0	\$0	\$0	\$0	0
93	1.4 Evaluacion	\$0	\$0	\$0	\$0	\$0	0	0	\$14.086.000	\$14.086.000	\$0	\$0	1
102	Fin fase Evaluacion	\$0	\$0	\$0	\$0	\$0	0	0	\$0	\$0	\$0	\$0	0
103	1.5 Mejora y cierre	\$0	\$0	\$0	\$0	\$0	0	0	\$10.368.000	\$10.368.000	\$0	\$0	1
108	Fin Proyecto	\$0	\$0	\$0	\$0	\$0	0	0	\$0	\$0	\$0	\$0	0

Figura 23. Variables en Project.

Fuente: Edición propia

6.3.5 aplicación técnica del valor ganado con curvas S de avance.

Se realiza un análisis de valor ganado al día 25 de enero de 2018 mediante la generación de la curva S de avance, la cual se muestra en la figura 24.

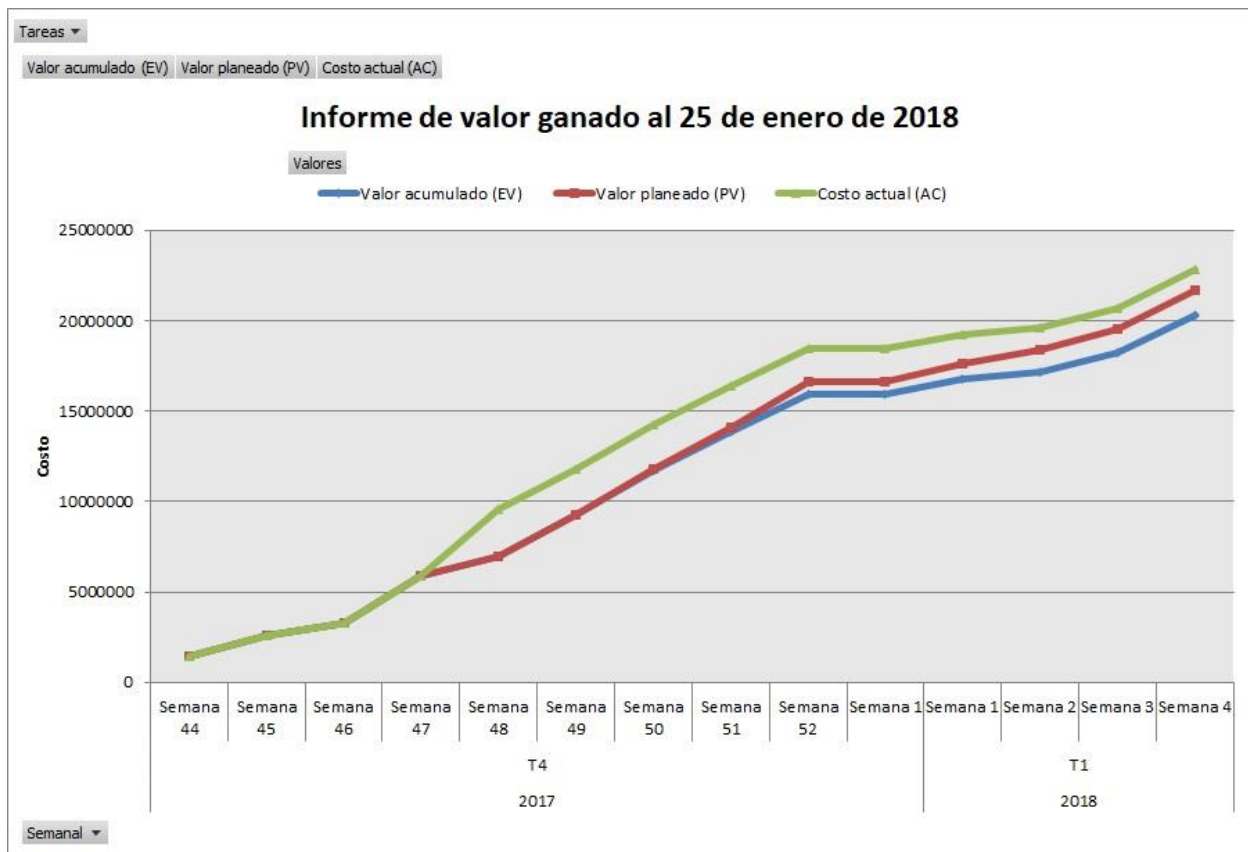


Figura 24. Curva S.

Fuente: Edición propia

Realizado el análisis de la gráfica obtenida, observamos que el proyecto a la fecha se encuentra retrasado ligeramente en lo respectivo al cronograma, para lo cual se requiere un esfuerzo adicional del personal involucrado para realizar actividades pendientes que mejoren este indicador, $SPI = 0,97$. También se puede apreciar que el proyecto se encuentra a la fecha con un sobrecosto respecto a lo presupuestado, debido a inversiones que ya se han realizado sin la respectiva ejecución de las tareas correspondientes, $CPI = 0,94$.

6.4 Plan de gestión de la calidad

6.4.1 especificaciones técnicas de requerimientos.

Las especificaciones técnicas de requerimientos se presentan en anexo (Ver Anexo P).

6.4.2 herramientas de control de la calidad.

Entre las herramientas de control que se emplearan para el proyecto se cuentan el análisis PERT y diagrama de Pareto.

6.4.2.1 *diagrama de PERT.*

Mediante este diagrama realizaremos una representación visual de las tareas y actividades que facilita una visión global. Esta perspectiva simplifica y agiliza la gestión de la calidad. Esta técnica o herramienta nos permite descubrir todas las formas posibles de lograr ejecutar una tarea en términos de máxima eficiencia para su gestión de calidad.

El uso del método PERT expone gráficamente todos los pasos que se deben tomar, mostrando las fechas de inicio y fin de cada uno, para poder lograr el objetivo final. Su aplicación nos ayuda a maximizar la eficacia y aumentar el rendimiento, en la implementación de nuestro proyecto.

Listado de actividades del proyecto con la estimación de duraciones esperadas (análisis PERT), se muestra en el anexo (Ver anexo K).

6.4.2.2 *diagrama de Pareto.*

La mayoría de las causas de los ataques informáticos son por la falta de conocimiento y de precaución de los usuarios de la red. Sin embargo, de acuerdo con

las mediciones realizadas en distintos ámbitos, se relacionan las causas en la tabla 9 como los principales factores que indican la vulnerabilidad de redes informáticas. La figura 25 presenta estos datos usando la técnica de diagramación de Pareto.

Tabla 9. Principales causas de ataques informáticos

Causa	FRECUENCIA	%	% ACUMULADO
Antivirus obsoleto	95	37%	37%
ausencia de políticas de seguridad	64	25%	62%
Red sin clave de acceso	51	20%	82%
antivirus inexistente	24	9%	91%
Sistema operativo obsoleto	12	5%	96%
Servidores sin protección	6	2%	98%
deficiente administración de la red	4	2%	100%
TOTAL	256	100%	

Fuente: Elaboración propia

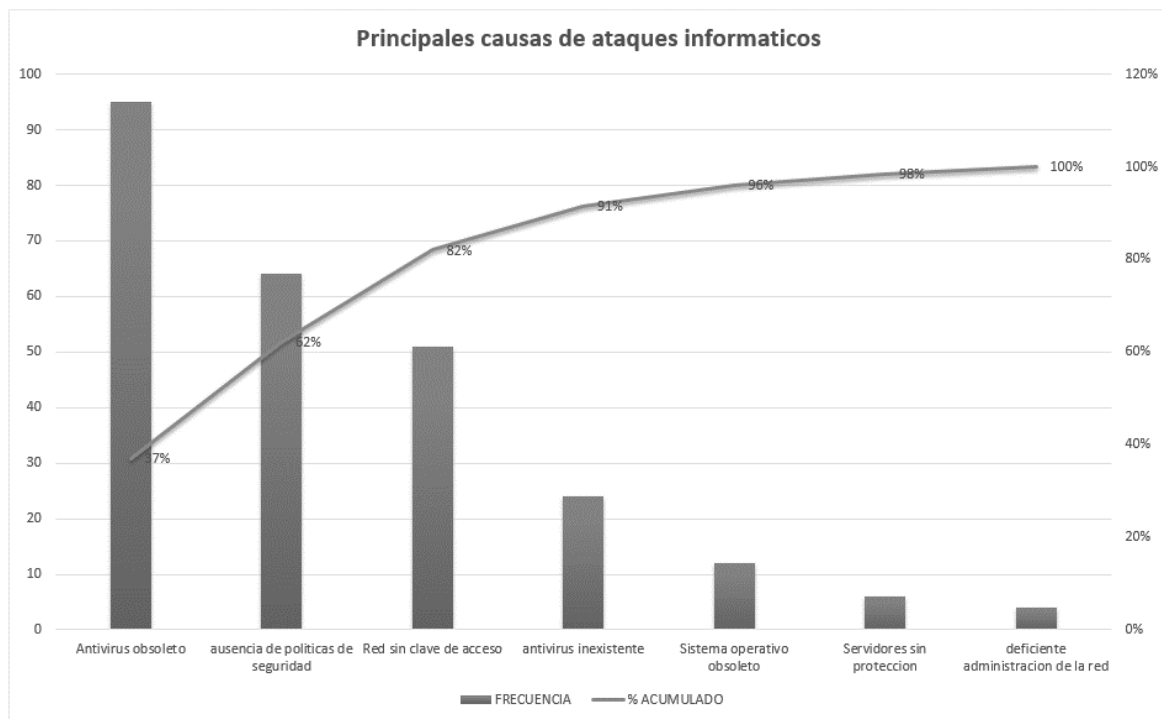


Figura 25. Diagrama de Pareto.

Fuente: Edición propia

6.4.2.3 plan de auditorías.

La ISO/IEC 27001:2013 establece la necesidad de llevar a cabo auditorías internas con el objeto de verificar que el Sistema de Gestión de Seguridad de la Información cumple con los requisitos propios de la organización y con los requisitos de la norma indicada.

6.4.2.4 escala de valoración de controles.

De acuerdo con el anexo A de la norma ISO 27001, se utiliza la siguiente tabla para determinar el estado de cumplimiento de la entidad en cuanto a seguridad de la información.

Esta valoración se debe hacer en periodos mensuales, determinando así el avance de acuerdo con el cronograma establecido y las fechas para cada fase.

Tabla 10. Escala de valoración de controles

Descripción	Calificación	Criterio
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.

Descripción	Calificación	Criterio
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: MINTIC

6.4.3 formato Inspecciones.

A continuación, se presenta el formato de inspección a equipos de cómputo.

Tabla 11. Formato de inspección a equipos informáticos

Equipo	PC	Marca	Lenovo Ideacentre	N° Serie	YQY81C
Ubicación	Administración		Responsable	Ricardo Jordan	
Ítem	Vulnerabilidad			Verificación	
1	Antivirus obsoleto			x	

Equipo	PC	Marca	Lenovo Ideacentre	N° Serie	YQY81C
Ubicación	Administración		Responsable	Ricardo Jordan	
Ítem	Vulnerabilidad			Verificación	
2	Ausencia o desconocimiento de políticas de seguridad			x	
3	Equipo sin clave de acceso				
4	Usuario sin clave de acceso			x	
5	Equipo fuera del dominio empresarial			x	
6	Antivirus inexistente				
7	Sistema operativo obsoleto			x	
8	Equipo infectado (virus)			x	
9	Equipo sin seguridad adecuada				
10	Mal manejo de equipos y programas			x	
11	Acceso remoto no autorizado				
12	Programas no autorizados instalados			x	
13	Archivos sin copia de seguridad			x	
14	Desconocimiento del usuario en cuanto a seguridad de la información			x	
	Total de amenazas encontradas			10	

Fuente: Elaboración propia

6.4.4 formato auditorias.

El formato de auditoria que se utilizara en el proyecto se encuentra en el cómo anexo (Ver anexo Q. Auditoria SGSI)

6.4.5 listas de verificación del entregables.

El anexo R presenta la lista de verificación de los entregables a auditar.

6.5 Plan de gestión de recursos humanos

El plan de gestión de recursos humanos pretende identificar y determinar los roles de cada uno de los integrantes en el proyecto de implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) para el Sanatorio de Agua de Dios ESE, así como las habilidades, responsabilidades y las relaciones de comunicación. Además de determinar las necesidades de capacitación, las acciones para fomentar el trabajo en equipo, los planes de reconocimiento y motivación de los integrantes y los aspectos relacionados con el cumplimiento de objetivos, incluyendo los procesos que organizan, gestionan y conducen al logro de cada una de las actividades propuestas en la EDT y el plan de trabajo.

6.5.1 definición de roles, responsabilidades y competencias del equipo.

El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección.

En la organización se deberá constituir el comité de seguridad que estará integrado por los directivos e ingenieros de nuevas tecnologías, el responsable de Sistemas de Información, el Responsable de Seguridad, el Interventor, entre otros actores principales.

Se considerará como máximo responsable a nivel político del SGSI al jefe de calidad y los ingenieros involucrados con Nuevas Tecnologías de la información. Se llevarán a cabo las siguientes tareas:

- a) Proporcionar una seguridad suficiente sobre la información de acuerdo con el contexto y situación de la organización.
- b) Asegurar el desarrollo, documentación e implementación de un sistema de gestión de seguridad de la información para todos los sistemas, redes e información en el ámbito del alcance definido.
- c) Verificar la alineación del sistema de gestión de la seguridad de la información con los objetivos estratégicos de la organización.
- d) Conceder autoridad al resto de responsables en materia de tratamiento de la información para asegurar un correcto desempeño de sus funciones.
- e) Designar un responsable de los Sistemas de Información.
- f) Verificar la correcta formación del personal asignado a tareas de seguridad de la información.
- g) Verificar que el responsable de los Sistemas de Información reporta periódicamente y de forma planificada la efectividad del SGSI.

El responsable de los Sistemas de Información deberá llevar a cabo las siguientes tareas:

- a) Designar un Responsable de Seguridad
- b) Desarrollar y mantener un SGSI para todos los sistemas, redes e información en el ámbito del alcance definido.
- c) Desarrollar y mantener políticas, procedimientos y controles técnicos para cumplir con las especificaciones normativas.
- d) Asegurar el cumplimiento de los requerimientos establecidos en materia de seguridad de la información.
- e) Informar de forma periódica y planificada de la efectividad de la efectividad del SGSI, así como de los efectos de las medidas correctoras que eventualmente se hubieran adoptado.

El Responsable de Seguridad será responsable de las siguientes tareas:

- a) Ejecutar todas las tareas relacionadas con la seguridad de la información
- b) Realizar periódicamente evaluaciones del riesgo.
- c) Asegurar la correcta formación en materia de seguridad de todo el personal de la organización.
- d) Entrenar y supervisar al personal que tenga responsabilidades relevantes en materia de seguridad.
- e) Probar y evaluar periódicamente la efectividad de las políticas y procedimientos de seguridad.
- f) Desarrollar e implementar procedimientos para detectar, informar y responder a incidentes de seguridad.
- g) Apoyar al responsable de Sistemas de Información en sus informes a la dirección.

Los usuarios son responsables cada uno de ellos en su ámbito de observar y aplicar toda la normativa que en materia de seguridad de la información publique la organización, así como de reportar a sus superiores jerárquicos cualquier incidencia que en dicha materia detecten. Los responsables de cada proceso, a su vez, pondrán en conocimiento del responsable de seguridad la información que por esta vía les llegue.

El Comité de Seguridad de la Información es el encargado de la revisión y ajustes a la política de seguridad de la información, sus funciones están descritas en la resolución No. 20.16.627 de octubre 14 de 2017, este comité es responsable de realizar la sensibilización y la adopción la interior de la entidad.

El coordinador del Comité de Seguridad de Información está a cargo del Coordinador Tics quien será el responsable de la realización de los comités de seguimiento de implementación de la Política de Seguridad de información.

El responsable del Activo de Información estará encargado de la clasificación, mantenimiento y actualización de los activos de información y deberán registrar en la

herramienta que se disponga para el levantamiento de esta información. Así mismo definir los perfiles y roles que deben tener cada usuario para acceder a la información, y será el responsable de la integridad, confidencialidad y disposición del Activo que este a su cargo y su salvaguarda.

El Coordinador del Grupo de Talento Humano deberá notificar a todo el personal que se incorpore a la institución en cualquier tipo de vinculación sobre las obligaciones del cumplimiento de la Política de Seguridad de la Información, así mismo de la elaboración de los compromisos de confidencialidad según el perfil y funciones de cada Servidor Público.

El Coordinador Tics deberá seguir las directrices de esta política y cumplir con los requerimientos que en temas de seguridad informática se incorporen para la garantizar el cumplimiento de la operación, administración, comunicación, mantenimiento, gestión de los sistemas de información y recursos tecnológicos de la entidad.

El Asesor Jurídico velará por el cumplimiento de la presente política en relación con la elaboración de los contratos u órdenes, representación judicial, tramite de conciliaciones, contestación de tutelas y derechos de petición de la entidad. Así mismo asesorara en materia jurídica en los temas de seguridad de información.

El Asesor de Control Interno será responsable de la realización de auditorías en los diferentes procesos que conforman el mapa de procesos institucional sobre la aplicación y medidas que se tienen para el manejo de seguridad de información.

6.5.1.1 requisitos de personal.

El equipo técnico de trabajo recomendado por el ministerio de tecnologías de información y comunicaciones (MINTIC), para desarrollar el proyecto implementación de un SGSI, debe contener los siguientes perfiles: Gerente del Proyecto, Ingeniero de Seguridad, Ingeniero de Redes, Ingeniero de Comunicaciones, Ingeniero de

Aplicaciones. Un equipo conformado por estas funciones puede abordar proyectos de este tipo de diferentes procesos de negocio o alcances organizacionales, para desarrollar las actividades que conforman las diferentes fases de cada proceso planteado para la cada Entidad.

Personal con el que se desarrollara el proyecto en la Entidad

- a) 1 gerente de proyecto (Ingeniero con certificación PMP) (Salario base: \$ 3'500.000)
- b) 1 ingeniero de Sistemas (Experiencia en redes, sin especialización) (Salario base: \$ 2'700.000)
- c) 1 ingenieros de Sistemas (sin experiencia) (Salario base: \$ 1'700.000)
- d) 1 técnico en sistemas (Sin experiencia) (Salario base: \$ 1'200.000)
- e) 1 ingeniero experto en redes (Asesor externo) (Salario base: \$ 2'900.000)
- f) 1 ingeniero (Asesor externo en gerencia de proyectos) (Salario base: \$ 2'500.000)

6.5.2 matriz de asignación de responsabilidades.

La matriz de asignación de responsabilidades se presenta como anexo (Ver Anexo S)

6.5.3 calendario de recursos.

Para el proyecto se contempla la ejecución de las actividades en días laborales de lunes a viernes. Eventualmente se requiere la presencia de personal los días sábados o domingos, para lo cual se programarán de acuerdo con la disponibilidad.

6.5.3.1 horarios.

A continuación, se relacionan los horarios laborales para cada día de la semana.

Tabla 12. Horarios de trabajo para el personal

Dia	Horario	
Lunes	7:00 -m - 1:00 pm	2:00 pm - 5:00 pm
Martes	7:00 -m - 1:00 pm	2:00 pm - 5:00 pm
Miércoles	7:00 -m - 1:00 pm	2:00 pm - 5:00 pm
Jueves	7:00 -m - 1:00 pm	2:00 pm - 5:00 pm
Viernes	7:00 -m - 1:00 pm	2:00 pm - 4:00 pm

Fuente: Elaboración propia

6.5.4 plan de capacitación y desarrollo del equipo.

Se debe garantizar la estabilidad del empleo y adicionalmente proyectar un horizonte de trabajo que permita el desarrollo profesional e integral de cada involucrado. Se implementarán mecanismos de contratación de personal que faciliten la idoneidad de adaptación puesto-individuo y trabajo en equipo. Implementación de sistema de compensaciones y retribuciones acorde con los resultados obtenidos y a las metas formuladas para los diferentes equipos de trabajo. Se facilitará la formación continua y el desarrollo de la profesión. Se Disminuirán las barreras organizativas y el número de niveles en los estatus empresariales. Se estimulará el trabajo en equipo con base a la descentralización de funciones. Se verificará la calidad y transparencia en los sistemas de información necesarios para cada nivel organizativo. Mejora las competencias e interacciones de los miembros del equipo y ayuda a mejorar el rendimiento del proyecto

Desarrollar los siguientes objetivos:

- a) Mejorar las habilidades de los miembros del equipo a fin de aumentar su capacidad de completar las actividades del proyecto

- b) Mejorar los sentimientos de confianza y cohesión entre los miembros del equipo a fin de incrementar la productividad a través de un mayor trabajo en equipo.

Tabla 13. Capacitación del personal involucrado

CAPACITACION			
Formación y desarrollo profesional			
ÁMBITO	HERRAMIENTAS		
Planifica acciones formativas	Ejecución	de	acciones formativas
Diseña y contrata recursos formativos	E-learning		
Planes de desarrollo de personal	Planes de carrera profesional		
	Modelos de dirección por objetivos		
	Evaluación del desempeño profesional		

Fuente: Elaboración propia

Ya que algunas de las habilidades personales son singulares en cada individuo y la combinación de capital humano e inversión en capacitación permitirá desarrollar dichas habilidades en pro de mejorar aspectos que vinculados a la motivación del empleado permitirán alcanzar con éxito los objetivos del proyecto.

No es suficiente hacer una sola sesión de capacitación y concientización, ya que se incorporan nuevo personal a la organización, los que ya estaban se les debe realizar re inducción y sensibilizaciones además de capacitaciones en temas específicos del SGSI. Es por esto por lo que la capacitación debe ser un proceso permanente a lo largo del tiempo de ejecución del proyecto y de su tiempo de operatividad.

Por tanto, conocer el estándar internacional sobre la Seguridad de la Información proporcionará, entonces, la orientación adecuada a los involucrados que deseen implementar, gestionar, mejorar y/o auditar un sistema de gestión de Seguridad de la Información dentro de la organización.

Tabla 14. Capacitaciones propuestas

Capacitaciones propuestas para el personal involucrado en la Implementación y Auditoría del Sistemas de Gestión de Seguridad de la Información (SGSI) en el sanatorio de Agua de Dios.

Fundamentos e Implementación, Introducción a la Gestión	Auditoría Interna y de un Sistema de	Riesgos, Controles e
Norma ISO/IEC 27001 - Sistema	Mantenimiento de un Gestión de	Indicadores de Gestión
de Gestión de Seguridad de la Información (SGSI).	de un Sistema de Gestión de Seguridad de la Información (SGSI).	de un Sistema de Gestión de Seguridad de la Información (SGSI).
Basado en la Norma ISO/IEC 27001	Basado en la Norma ISO/IEC 27001	Basado en la Norma ISO/IEC 27001
42 horas	42 horas	42 horas

Fuente: Elaboración propia

6.5.5 esquema de contratación y liberación de personal.

6.5.5.1 estrategias para adquirir el equipo de trabajo.

- Planes de adquisición de personal y buenos procedimientos de contratación son importantes, como también los incentivos para la contratación y la retención del personal.
- Generar expectativas de estabilidad y ascenso en el empleo.

- c) Utilizar mecanismos de contratación de personal que faciliten la idoneidad de adaptación puesto-individuo.
- d) Sistema de compensaciones y retribuciones contingente a los resultados obtenidos y a las metas formuladas o a los objetivos específicos propuestos.
- e) Ofrecer posibilidades de formación continua y desarrollo profesional.
- f) Disminuir las barreras organizativas y el número de niveles en los estatus empresariales.

6.5.5.2 criterios de liberación.

A continuación, se relacionan los criterios de liberación para el personal.

Tabla 15. Criterios de liberación del personal

Gestión de salida de los recursos humanos	
ÁMBITO	HERRAMIENTAS
Renuncias voluntarias y despidos	Entrevistas
Jubilaciones y prejubilaciones	Políticas de jubilación anticipada
	Sistemas de recolocación laboral

Fuente: Elaboración propia

6.5.6 definición de indicadores de medición de desempeño del equipo y esquema de incentivos y recompensas.

Se promoverá el trabajo en equipo por medio de actividades que vinculen a los integrantes de cada proceso, se utilizará el método de recompensa para los equipos o

individuos que se destaquen en el logro de objetivos específicos, las recompensas podrán ser bonificaciones o tiempo no laborable.

Se programarán holguras de tiempo para que los miembros del equipo se ayuden mutuamente para alcanzar los objetivos del proyecto y desarrollar los recursos humanos.

Después de evaluar el rendimiento del equipo y la información relacionada, el gerente del proyecto debe decidir: si debe solicitar cambios para el proyecto, si recomienda acciones correctivas o preventivas, si se necesitan actualizaciones al plan de gestión del proyecto o a los activos de los procesos de la organización.

Las evaluaciones de desempeño se realizarán trimestralmente y estarán a cargo del líder de proceso de recursos humanos.

6.6 Plan de gestión de las comunicaciones

6.6.1 sistema de información de comunicaciones.

6.6.1.1 comunicaciones para la alta gerencia.

Para la alta gerencia se debe utilizar una comunicación formal mediante correo electrónico. Se debe comunicar semanalmente los avances del proyecto. Eventos inesperados o adversos deben ser comunicados de manera inmediata mediante correo electrónico que la institución habilitara para estos casos.

Cualquier cambio en la planeación debe ser comunicado a la alta gerencia y evaluar el impacto que se origina de dicho cambio en el desempeño del proyecto.

6.6.1.2 comunicaciones para el Ministerio TIC.

Debido a que el proyecto se desarrolla para una entidad del estado del orden nacional, se debe contar con una comunicación directa y fluida con el ministerio de las tecnologías de información y las comunicaciones (MINTIC). Sesiones de videoconferencia se programarán cada 2 meses para evaluar el desempeño de la entidad y el avance de acuerdo con el cronograma, así como para resolver dudas legales sobre el proyecto.

Correos electrónicos del ministerio están habilitados para las asesorías a las entidades del estado que así lo requieren.

6.6.1.3 comunicaciones para el personal de tecnología.

Como parte fundamental en la implementación del proyecto, el personal de tecnología deberá estar familiarizado con los avances de cada actividad, tanto para soporte técnico como para gestión del servicio.

Se programan reuniones diarias de máximo 15 minutos, en las cuales se comunica a todo el equipo las tareas a realizar en la jornada laboral.

Reuniones semanales, exposiciones, en las cuales se evaluará el avance del proyecto y las actividades desarrolladas por cada integrante del equipo, problemas presentados y soluciones aportadas o pendientes de solución. Se requiere que se documente el avance semanalmente y los reportes se deben recibir mediante correo electrónico al gerente de proyecto, quien consolida la información y generara un estado general de avance del proyecto.

6.6.1.4 comunicaciones para los líderes de proceso.

Cada líder de proceso debe estar enterado de las actividades que se realizaran y que involucren su proceso. Es por esto por lo que se debe informar mediante oficio a los líderes de proceso, en el momento en que las actividades a desarrollar involucren de manera directa o indirecta su proceso. La comunicación deberá realizarse con mínimo 3 días hábiles anteriores a la fecha de inicio de actividades para dicho proceso.

Reunión mensual de seguimiento con los líderes de proceso para socializar avances, riesgos y restricciones del proyecto.

6.6.1.5 comunicación para los funcionarios.

Todos los funcionarios de la entidad deberán estar enterados de las actividades que se están realizando y la forma en que estas actividades influirán en su trabajo diario.

Definir muy bien la estrategia a utilizar en este grupo de interesados puede determinar un avance significativo en la ejecución del proyecto.

Folletos informativos generados mensualmente sobre las actividades y la cultura de seguridad de la información.

Se tiene habilitada una intranet, con acceso a todos los empleados de la entidad, donde encontraran manuales, tips, registros y demás información necesaria para mantener satisfechos. Todos los funcionarios deberán contar con acceso restringido a los archivos de la organización.

Mensajes directos a los funcionarios de interés para cada actividad deberán ser comunicados por el personal de tecnología designado para ello.

6.6.1.6 comunicaciones para los usuarios.

En este grupo de interesados debe permanecer neutral para el proyecto, por lo cual se debe monitorear.

Videos informativos en las salas de espera del hospital, con material enfocado a la seguridad de la información y su impacto en los usuarios de la IPS. Estos deben ser renovados o actualizados por lo menos una vez cada mes.

Folletos relativos a la cultura de la seguridad de la información deberán estar disponibles en las ventanillas de citas y atención al usuario en todo momento.

6.6.1.7 comunicaciones para sensibilización.

Se colocarán a disposición diferentes técnicas para la propagación de mensajes de sensibilización, la selección de cada método debe ser acorde al presupuesto, recursos y tecnología a disposición del proyecto:

- a) Posters con mensajes o checklist sobre que debe y que no debe hacerse.
- b) Videos institucionales a través de videowalls o pantallas.
- c) Screensavers con mensajes de sensibilización.
- d) Cuadernos, relojes o elementos de oficina con mensajes alusivos.
- e) Boletines vía email.
- f) Eventos relacionados con seguridad, concursos etc.

- g) Sesiones con instructores (si se planean charlas que contengan varios temas de sensibilización a la vez).

Por lo general, los mensajes de sensibilización son de mucha brevedad y simplicidad, lo que facilita en gran medida la recepción del mensaje que se está transmitiendo. El uso de imágenes o videos pueden reforzar el tema a tratar.

6.6.1.8 tecnologías de comunicación.

Es importante generar distintos soportes de comunicación para que sea más eficaz. Pueden ser orales, escritos, audiovisuales, digitales y demás. Las Nuevas Tecnologías de la Información y Comunicación (NTIC) abren múltiples posibilidades e integran distintas modalidades generando soportes multimedia e hipermedia para gestionar las comunicaciones.

- a) *Oficio*: Debe tener como mínimo el membrete, asunto de la referencia, oficina a la cual va dirigida. deben ser breves y legibles. Se van a utilizar para difundir la información importante como son, resultados, cambios en la organización y otros. Tiene la ventaja de ser rápida su llegada y el impacto que provoca el remitente, por esto, no se realizará de forma múltiple con un destinatario común sino personalizada generando mayor respeto.
- b) *Cartelera*: Se colocarán en un lugar de tránsito seguro del personal del proyecto. Puede contener información general, normativas institucionales e informaciones que intercambia el personal.
- c) *Manuales*: Son guías de procedimientos que reúnen la información técnica, organizativa, histórica. Ayudan a organizar y coordinar las actividades. Además, ayudará a evitar discursos no necesariamente verbales; evitando contradicciones.

- d) *Folletos*: Estos deberán diseñarse de una forma sencilla y práctica. Con claridad en la información que se quiere divulgar y agradables a la vista, usando imágenes para contextualizar.
- e) *Reuniones*: Las reuniones son un espacio de comunicación para: informar, capacitar, reflexionar y tomar decisiones. Lo importante es contar con espacio acorde y convocar a los participantes con la debida anticipación.
- f) *Comités*: son reuniones programadas mensualmente por la gerencia para tratar distintos asuntos de interés general de la institución. En ellos se generará un espacio para socialización del proyecto a todos los interesados.
- g) *Medios electrónicos*: Se utilizarán con el fin de intercambiar información con personal que no tiene la posibilidad de reunirse frecuentemente con los demás miembros del grupo de. Entre estos medios tenemos:
- h) *E-mail*: sus ventajas son: rapidez, interactividad, multidifusión, facilidad de fijación del destinatario.
- i) *Intranet*: se utilizará la red interna de la institución para envío de mensajes rápidos e instantáneos.

En la página web institucional se puede debe contar con un área restringida sólo para los integrantes de la institución e implementar los foros.

6.6.2 matriz de comunicaciones.

En la siguiente tabla se presentan los aspectos a comunicar para cada interesado en el proyecto.

Tabla 16. Matriz de comunicaciones SGSI

ASPECTOS A COMUNICAR	DIRIGIDO A	FRECUENCIA	RESPONSABLE	RECURSOS
Avances del proyecto	Alta gerencia	Semanal	Gerente proyecto	Correo electrónico

ASPECTOS A COMUNICAR	DIRIGIDO A	FRECUENCIA	RESPONSABLE	RECURSOS
Eventos inesperados o adversos	Alta gerencia	Inmediato	Gerente proyecto / Personal de tecnología	Correo electrónico / comunicación directa
Sesiones de video conferencia	MinTIC	Bimensual	Gerente proyecto	Video conferencia / Skype
Dudas y aclaraciones tecnológicas	MinTIC	Continua	Gerente proyecto	Correo electrónico
Avance de actividades	Personal de tecnología	Diario, 15 min	Gerente proyecto / Personal de tecnología	Reuniones
Avance semanal	Personal de tecnología	Semanal	Gerente proyecto / Personal de tecnología	Reuniones, presentación de diapositivas
Inicio de actividad	Líderes de proceso	3 días antes de iniciar actividad	Gerente proyecto	Oficio / correo electrónico
Seguimiento del proyecto	Líderes de proceso	Mensual	Gerente proyecto	Reuniones
Actividades en ejecución	Funcionarios	15 días	Personal de tecnología	Folletos, Mensajes Intranet, Fondos de pantalla
Socialización SGSI	Usuarios	Mensual	Personal de tecnología	Videos digiturno / folletos / página web
Políticas y procedimientos en Seguridad de la información	Usuarios y funcionarios en el alcance del proyecto	Continua	Gerente proyecto / Personal de tecnología	Página web, Intranet, Folletos, Videos digiturno, fondos de pantalla, Protector de pantalla, Reuniones

Fuente: Elaboración propia

6.7 Plan de gestión del riesgo

El proceso de identificación de riesgos se debe realizar al inicio del proyecto y deberá contener el máximo posible de riesgos identificando sus posibles causas y consecuencias. Los análisis cualitativo y cuantitativo de riesgos se deberán realizar una vez se cuente con el listado, lo más completo posible de los riesgos identificados (registro de riesgos), así como la definición de los planes de respuesta a los riesgos.

Las reuniones deberán ser periódicas mensuales, el último jueves de cada mes, donde se identificarán los riesgos y se iniciara con la lista de riesgos identificados.

Tabla 17. Calendario de riesgos

ACTIVIDAD	MOMENTO DE EJECUCIÓN	FRECUENCIA
Planificación de la Gestión de riesgos	Al inicio del proyecto	Una vez
Determinar roles y responsabilidades	Al inicio del proyecto	Una vez
Identificación de Riesgos	Al inicio del proyecto y en cada reunión para Re planificación por parte del equipo de Proyecto	Quincenal
Realizar el análisis cualitativo y cuantitativo de riesgos	Al inicio del proyecto y cada vez que se identifiquen nuevos riesgos	A solicitud
Realizar el plan de respuesta a los riesgos	Al inicio del proyecto	Una vez
Implementar los planes de respuesta	Posterior a la realización del plan de respuesta a los riesgos	A solicitud

ACTIVIDAD	MOMENTO DE EJECUCIÓN	FRECUENCIA
hacer seguimiento a los riesgos	Posterior a implementar el plan de respuesta	Quincenal
Identificar nuevos riesgos	Durante todo el ciclo de vida del proyecto	Quincenal
Solicitudes de cambio	Durante todo el ciclo de vida del proyecto	A solicitud
Realizar auditorías de riesgo	Durante todo el ciclo de vida del proyecto	Mensual
Gestión de la reserva de riesgos	Durante todo el ciclo de vida del proyecto	Mensual

Fuente: Elaboración propia

6.7.1 identificación de riesgos y determinación del umbral.

A continuación, se establece una lista detallada de los riesgos asociados al proyecto SGSI, identificando sus posibles causas y consecuencias.

Tabla 18. Registro de riesgos

ITEM	CAUSA	RIESGO IDENTIFICADO	CONSECUENCIA
1	Presupuesto limitado	Falta de personal autorizado para realizar las actividades	Retrasos en las actividades
2	Escases de proveedores	No disponibilidad del servicio de mantenimiento a equipos	Fallas en equipos críticos
3	Falla en servidores	Interrupción en la continuidad del negocio	Imagen negativa de la empresa
4	Asignación inadecuada de permisos	Imposibilidad para la prestación de algunos servicios	Clientes insatisfechos

ITEM	CAUSA	RIESGO IDENTIFICADO	CONSECUENCIA
5	Accesos no controlados a las bases de datos	Afectación de la integridad de los datos	Errores en los procesos
6	Falta de espacio de almacenamiento	No disponibilidad de información de respaldo	Perdida de información
7	Inestabilidad de los sistemas	Funcionamiento inadecuado de aplicaciones de software	Errores en los procesos
8	Planes de mantenimiento inexistentes	No disponibilidad del servidor o equipos de computo	No prestación de servicios
9	Fluctuaciones en la red eléctrica	Falta de suministro de energía	Demoras en los servicios
10	Calor excesivo	Falla de enlaces de comunicación	Sedes sin acceso a la red

Fuente: Elaboración propia

6.7.1.1 definiciones de probabilidad e impacto de los riesgos.

El análisis del riesgo busca establecer la probabilidad de ocurrencia de este y sus consecuencias, este último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados: Probabilidad e Impacto.

6.7.1.1.1 Definiciones de probabilidad

La probabilidad se medirá de acuerdo con los parámetros de la siguiente tabla

Tabla 19. Probabilidad de los riesgos

NIVEL	DEFINICIÓN PROBABILIDAD	DESCRIPCION	FRECUENCIA
0,1	Muy baja	El evento puede ocurrir solo en circunstancias excepcionales	No se ha producido en los últimos 5 años
0,3	Baja	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
0,5	Moderada	El evento podría ocurrir en cualquier momento	al menos una vez en los últimos dos años
0,7	Alta	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez e el intimo año
0,9	Muy alta	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas de una vez al año

Fuente: Elaboración propia

6.7.1.1.2 Definiciones de impacto

El impacto se medirá de acuerdo con los parámetros de la siguiente tabla

Tabla 20. Impacto de los riesgos

NIVEL	DEFINICIÓN IMPACTO	DESCRIPCION
-------	-----------------------	-------------

NIVEL	DEFINICIÓN IMPACTO	DESCRIPCION
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llega a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Fuente: Elaboración propia

6.7.1.2 matriz de probabilidad e impacto.

La tabla a continuación establece los niveles de prioridad de los riesgos de acuerdo con la matriz de probabilidad / impacto

Tabla 21. Matriz de probabilidad / Impacto

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Muy baja (0,1)	Bajo	Bajo	Medio	Alto	Alto
Baja (0,3)	Bajo	Bajo	Medio	Alto	Extremo
Moderada (0,5)	Bajo	Medio	Alto	Extremo	Extremo
Alta (0,7)	Medio	Alto	Alto	Extremo	Extremo
Muy alta (0,9)	Alto	Alto	Extremo	Extremo	Extremo

Fuente: Elaboración propia

6.7.1.3 tolerancia de los interesados y determinación del umbral de riesgo.

Se determina para todos los interesados que la respuesta para todos los riesgos ubicados en la zona de riesgo BAJO, el plan de respuesta puede ser aceptar. Para los riesgos en zona de riesgo extrema la estrategia permitida solo puede ser EVITAR.

La siguiente tabla muestra la respuesta al riesgo según las tolerancias establecidas.

Tabla 22. Matriz de respuesta al riesgo

Tipo de riesgo	Zona de riesgo	Respuesta
Bajo	BAJA	Aceptar
Medio	MEDIA	Mitigar
Alto	ALTA	Mitigar - Transferir
Extremo	EXTREMA	Evitar

Fuente: Elaboración propia

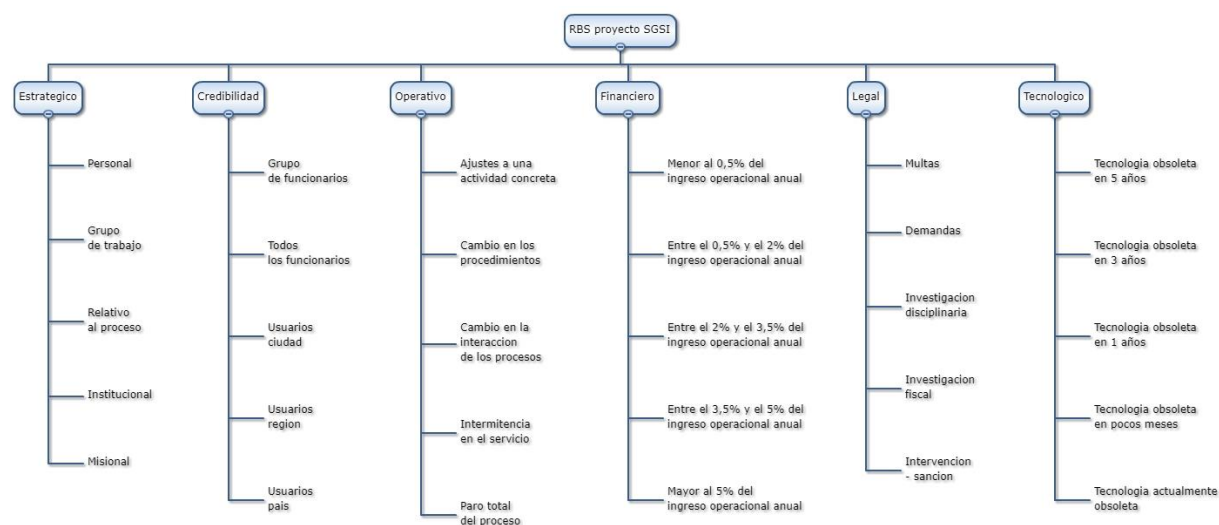
6.7.2 Risk Breakdown Structure (RBS).

Para la clasificación del riesgo se utilizan las siguientes categorías que representan los temas en que suelen impactar la ocurrencia de los riesgos.

- a) *Riesgo estratégico.* Se asocia con la forma en que se administra la entidad. Se enfoca a asuntos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas y el concepto de la entidad por parte de la alta gerencia.
- b) *Riesgo de credibilidad.* Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- c) *Riesgos operativos.* comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

- d) *Riesgos financieros*. Se relacionan con el manejo de los recursos de la entidad que incluyen, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
- e) *Riesgos legales*. Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
- f) *Riesgos tecnológicos*. Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras en el cumplimiento de la misión.

La figura 26 muestra la estructura de desglose de riesgos (RBS)



www.wbsol.com

Figura 26. Estructura de desglose de riesgos.

Fuente: Edición propia

6.7.3 análisis de riesgos.

6.7.3.1 análisis cualitativo de riesgos.

A cada riesgo identificado se define su probabilidad de ocurrencia y el impacto generado si llegara a presentarse, de acuerdo con la categoría de riesgo previamente establecida.

La tabla a continuación representa la matriz de clasificación de los riesgos priorizados según su nivel de riesgo.

Tabla 23. Matriz de clasificación y evaluación de riesgos

ITEM	RIESGO IDENTIFICADO	CATEGORIA	PROBABILIDAD	IMPACTO	TIPO DE RIESGO
1	No disponibilidad del servicio de mantenimiento a equipos	OPERATIVO	0,7	4	EXTREMO
2	No disponibilidad del servidor o equipos de computo	TECNOLOGICO	0,7	4	EXTREMO
3	Afectación de la integridad de los datos	CREDIBILIDAD	0,5	4	EXTREMO
4	Falta de suministro de energía	OPERATIVO	0,3	5	EXTREMO
5	Funcionamiento inadecuado de aplicaciones de software	TECNOLOGICO	0,9	2	ALTO
6	Falta de personal autorizado para realizar las	FINANCIERO	0,5	3	ALTO

ITEM	RIESGO IDENTIFICADO	CATEGORIA	PROBABILIDAD	IMPACTO	TIPO DE RIESGO
	actividades				
7	Interrupción en la continuidad del negocio	LEGAL	0,1	5	ALTO
8	No disponibilidad de información de respaldo	TECNOLOGICO	0,3	3	MEDIO
9	Falla de enlaces de comunicación	OPERATIVO	0,1	3	MEDIO
10	Imposibilidad para la prestación de algunos servicios	LEGAL	0,3	2	BAJO

Fuente: Elaboración propia

6.7.3.2 análisis cuantitativo de riesgos.

Para cada riesgo identificado se define su valor monetario o impacto en los costos del proyecto, así como el valor monetario esperado teniendo en cuenta su probabilidad de ocurrencia.

La tabla a continuación representa la matriz de evaluación cuantitativa de los riesgos y el cálculo del valor monetario esperado.

Tabla 24. Matriz de evaluación cuantitativa de riesgos

ITEM	RIESGO IDENTIFICADO	PROBABILIDAD	VALOR RIESGO	VME
1	No disponibilidad del servicio de mantenimiento a equipos	0,7	\$ 20.000.000	\$ 14.000.000
2	No disponibilidad del servidor o equipos de	0,7	\$ 7.000.000	\$ 4.900.000

ITEM	RIESGO IDENTIFICADO	PROBABILIDAD	VALOR RIESGO	VME
	computo			
3	Afectación de la integridad de los datos	0,5	\$ 25.000.000	\$ 12.500.000
4	Falta de suministro de energía	0,3	\$ 3.000.000	\$ 900.000
5	Funcionamiento inadecuado de aplicaciones de software	0,9	\$ 12.000.000	\$ 10.800.000
6	Falta de personal autorizado para realizar las actividades	0,5	\$ 30.000.000	\$ 15.000.000
7	Interrupción en la continuidad del negocio	0,1	\$ 10.000.000	\$ 1.000.000
8	No disponibilidad de información de respaldo	0,3	\$ 28.000.000	\$ 8.400.000
9	Falla de enlaces de comunicación	0,1	\$ 2.000.000	\$ 200.000
10	Imposibilidad para la prestación de algunos servicios	0,3	\$ 7.000.000	\$ 2.100.000
				\$
RESERVA DE CONTINGENCIA				69.800.000

Fuente: Elaboración propia

6.7.4 matriz de riesgos.

En el anexo se muestra el formato utilizado para realizar la gestión del riesgo en el proyecto. (Ver anexo T)

6.7.5 plan de respuesta a los riesgos.

Este proceso desarrolla las opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto. Para diseñar el plan de respuesta a los riesgos presentes en la implementación del SGSI, se analizarán los riesgos asociados en las anteriores tablas enmarcadas dentro del análisis cualitativo de riesgos y el análisis cuantitativo de riesgos. Estos riesgos corresponden a las categorías de riesgos bajos, medios, altos y extremos clasificados en el análisis cualitativo.

En el anexo, se presenta el plan para los riesgos, indicándose, la estrategia, plan de acción, activador y el responsable de cada riesgo. Se deben calcular las reservas de tiempo y costos mediante el presupuesto del proyecto, teniendo en cuenta el porcentaje de impacto de cada riesgo (Ver Anexo U).

Una vez implementado el plan de respuesta para cada riesgo identificado, se procede a realizar la revaluación de los riesgos y determinar su nueva probabilidad de ocurrencia.

La matriz de revaluación de riesgos es presentada en el anexo (Ver Anexo V).

6.8 Plan de gestión de adquisiciones

6.8.1 definición y criterios de valoración de proveedores.

La selección del contratista se hará mediante licitación pública. Los términos y condiciones serán publicados en la página web del hospital.

La propuesta de los proveedores se presentará: escrita, foliada, en sobre cerrado y sellado. El proponente sufragará todos los costos tanto directos como indirectos relacionados con la preparación y presentación de su propuesta. El Hospital no será responsable en ningún caso de dichos costos cualquiera que sea el resultado que se derive de este proceso de contratación.

6.8.1.1 documentos necesarios para la escogencia de la oferta o contenido de la propuesta.

La propuesta deberá contener la siguiente información:

6.8.1.1.1 Contenido jurídico

- a) Formulario de inscripción como proveedor del Hospital
- b) Certificado de existencia y representación legal
- c) Certificado de antecedentes disciplinarios y fiscales
- d) Garantía de seriedad de la oferta

6.8.1.1.2 Contenido financiero

Los índices financieros fijados por la entidad para habilitar propuestas son:

- a) *Endeudamiento total:* Pasivo total / Activo total x 100 igual o menos a 60%
- b) *Liquidez:* Activo corriente / Pasivo corriente igual o superior a 1,5

- c) *Capital de trabajo*: Activo corriente – pasivo corriente igual o superior al presupuesto oficial

6.8.1.1.3 Contenido técnico

El oferente deberá acreditar la experiencia específica requerida mediante certificados de experiencia en contratos similares a los descritos en la propuesta, cuya sumatoria del valor deberá ser igual o superior a 200 SMMLV.

6.8.1.1.4 Personal mínimo requerido

El oferente deberá acreditar el personal mínimo exigido para el desarrollo del proyecto, anexando la documentación de idoneidad necesaria, de acuerdo con la naturaleza del contrato

6.8.1.1.5 Propuesta económica

- a) El oferente deberá incluir en el valor de la propuesta la totalidad de los costos directos e indirectos que genere el contrato.
- b) Los precios consignados en la propuesta se mantendrán vigentes durante el término de la ejecución del contrato, y no habrá lugar a reajustes.
- c) El proponente debe diligenciar el formato de análisis de AIU.

6.8.1.2 factores de escogencia o evaluación de las propuestas.

El Hospital de Agua de Dios, durante los dos días hábiles siguientes al cierre del proceso, por medio del comité de apoyo contractual, hará los estudios del caso y el análisis comparativo de las propuestas, teniendo en cuenta para ello los criterios de selección objetiva establecidos en los términos de referencia.

6.8.1.2.1 Requisitos habilitantes

La ausencia de requisitos o falta de documentos referentes a la futura contratación o al proponente, necesarios para la comparación de propuestas servirá de título suficiente para la inadmisión jurídica y/o no cumplimiento técnico y financiero de los ofrecimientos hechos, según lo establecido en los presentes parámetros de contratación.

El procedimiento y los criterios de evaluación serán los establecidos en los términos de referencia. La evaluación de las propuestas se basará en la documentación, información y anexos correspondientes.

- a) Evaluación jurídica: en la evaluación jurídica se determina si el oferente cumple o no con los requisitos legales establecidos. Su resultado será Admitida o No Admitida. La propuesta que sea admitida será sometida a evaluación financiera.
- b) Evaluación financiera: Se verifica el cumplimiento de los indicadores financieros descritos en el numeral 4.2.1.2 del presente documento.

Puntajes: Para efectos de selección objetiva se tendrá en cuenta, sobre un máximo de 100 puntos, los siguientes criterios y puntajes:

6.8.1.2.2 Evaluación técnica

Se otorga un máximo de 60 puntos a quien acredite experiencia adicional, distribuidos así:

Experiencia en contratación: 30 puntos. Dos (2) puntos por cada 10 SMLMV que excedan los 200 SMLMV exigidos como requisito mínimo en el contenido técnico.

Valor agregado de calidad: 30 puntos otorgados al proponente que ofrezca un profesional con experiencia en el control de calidad de proyectos similares.

6.8.1.2.3 Evaluación económica

Serán objeto de evaluación económica solamente las propuestas que hayan sido habilitadas en los aspectos jurídicos, financieros, técnicos mínimos y de experiencia.

Para efectos de la calificación económica se considerarán únicamente las propuestas hábiles, es decir aquellas que:

- a) Cumplan la totalidad de los requisitos de orden jurídico, financiero y de experiencia.
- b) El valor total de la propuesta no supere el presupuesto oficial.

6.8.2 selección y tipificación de contratos.

Para la selección de contratos se tiene en cuenta la normatividad aplicable y el tipo de proyecto a ejecutar y los activos de los procesos de la organización. Preferiblemente se usarán dos tipos de contratos:

- a) *Contrato de Precio Fijo Cerrado (PFC)*. El precio de los bienes se fija al comienzo y no está sujeto a cambios, salvo que se modifique el alcance del trabajo. Cualquier aumento de costos por causa de un desempeño desfavorable es responsabilidad del vendedor, quien está obligado a completar el trabajo. El comprador debe especificar con precisión el producto o servicio a adquirir, y cualquier cambio en las especificaciones de la adquisición puede ocasionar aumento de los costos para el comprador.
- b) *Contrato por tiempo y materiales (M&T)*. Tipo de contrato abierto y sujeto a posibles aumentos en los costos para el comprador. El valor total del contrato y la cantidad total de elementos a entregar puede que no estén definidos por el comprador en el momento de la adjudicación del contrato.

6.8.3 criterios de contratación, ejecución y control de compras y contratos.

6.8.3.1 selección del contratista.

Dentro de los plazos propuestos, la entidad efectuará las comparaciones de los diferentes ofrecimientos recibidos, aplicando los criterios y las calificaciones que se enuncian en el aparte respectivo del presente documento; la evaluación contemplará los aspectos jurídico, técnico y económico. Elaborado el concepto técnico será puesto en consideración del ordenador del gasto, quien dentro de los dos (2) días siguientes al vencimiento del plazo establecido para la evaluación de las propuestas decidirá sobre la selección del contratista. Cuando sólo se presente una propuesta y ésta pueda ser considerada como favorable para el Sanatorio de conformidad con los criterios de selección objetiva, así lo recomendará a la Gerencia un comité conformado por quienes realizaron las respectivas evaluaciones. La Gerencia, si así lo considera, ordenará con este oferente la contratación; en caso contrario, se considerará desierta la invitación.

6.8.3.2 legislación aplicable.

El Hospital de Agua de Dios es una Empresa Social del Estado y como tal, en materia de contratación, se le aplican las normas de derecho privado y su propio reglamento de conformidad con lo dispuesto en el numeral 6 del artículo 195 de la ley 100 de 1993, razón por la cual los procesos de selección se efectuarán mediante Invitación pública.

6.8.3.3 condiciones del contrato.

En el evento de ser adjudicado el contrato el proponente, además de las establecidas en otros apartes de estos parámetros de contratación y los que el contrato mismo implica, se comprometerá a:

- a) Cumplir con el objeto contractual de conformidad con lo ofrecido, y en las especificaciones y condiciones previstas en los pliegos de condiciones y según lo pactado en el contrato.
- b) Cumplir con las condiciones técnicas, jurídicas, económicas, financieras y comerciales presentadas en la propuesta.
- c) Acatar las instrucciones que durante el desarrollo del contrato le imparte el Sanatorio Agua de Dios ESE a través de las funciones que ejerzan el control de la ejecución.
- d) Atender en debida forma las instrucciones, sugerencias, recomendaciones y solicitudes que le efectúe la Institución y adoptar las medidas inmediatas para la corrección de las fallas
- e) Las demás obligaciones que se deriven de los pliegos de condiciones y de la naturaleza del objeto del contrato a celebrar.
- f) Asumir por su cuenta y riesgo todos los costos que conlleve la total ejecución del objeto contractual.
- g) El contratista deberá tener afiliado a su personal a los sistemas de seguridad social.
- h) En general se obliga a cumplir con todas las de la esencia que se deriven del cumplimiento del presente contrato.

6.8.3.4 garantías exigidas.

El contratista deberá suscribir póliza de garantía con Compañía de Seguros debidamente autorizada para operar en Colombia, que ampare los siguientes riesgos:

- a) Cumplimiento del Contrato: Para garantizar los perjuicios que se deriven del incumplimiento de las obligaciones contractuales, incluidas las multas y la cláusula penal por una suma equivalente al diez por ciento (10%) del valor total del contrato, con una vigencia igual a la del plazo de ejecución y cuatro (4) meses más.

- b) Pago de Salarios y Prestaciones Sociales e Indemnizaciones: Para garantizar los eventos en que el Contratista sea requerido por el pago de obligaciones laborales en relación con la ejecución de las obligaciones derivadas del contrato por una suma equivalente al cinco por ciento (5%) del valor total del contrato, con una vigencia igual a la del plazo total del contrato y tres (3) años más contados a partir de la fecha de terminación de este.
- c) De calidad y correcto funcionamiento de los bienes: Se exigirá para precaver las eventualidades en que uno o varios de los bienes contratados, no reúnan las especificaciones o calidades exigidas en la contratación o que no sean aptos para los fines que fueron contratados. Su cuantía no será inferior al diez por ciento (10%) del contrato y su vigencia será mínimo de doce (12) meses contados a partir del recibo o aceptación final.
- d) Anticipo: Se exigirá para precaver las eventualidades en que no se haga uso adecuado del valor concedido como anticipo. Su cuantía no será inferior al cien por ciento (100%) del valor del anticipo y su vigencia será hasta el recibo o aceptación final del contrato
- e) Estabilidad de Obra: Se exigirá para precaver las eventualidades en que se presente falla estructural que afecte la estabilidad de la obra eléctrica realizada. Su cuantía no será inferior al veinte por ciento (20%) del valor del contrato y su vigencia será hasta cinco (5) años contados a partir del recibo o aceptación final.

Las pólizas deberán ser entregadas dentro de los cinco (5) días hábiles siguientes a la suscripción del contrato.

6.8.4 cronograma de compras con la asignación de responsable.

En la figura 27 se presenta el cronograma de adquisiciones para el proyecto SGSI.

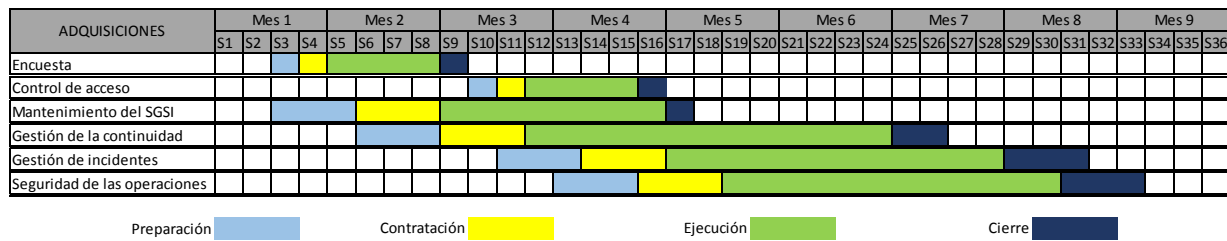


Figura 27. Cronograma de adquisiciones.

Fuente: Edición propia

6.8.4.1 asignación de responsables.

Para asignación del responsable de las adquisiciones se realizará sesión del comité de apoyo contractual de la entidad, el cual evaluará las propuestas y asignará el responsable de la contratación.

El gerente de proyecto hará parte integral del comité de apoyo contractual.

6.9 Plan de gestión de los interesados

6.9.1 identificación y categorización de interesados.

Una vez analizado el entorno y la organización donde se desarrollará el proyecto, se logran identificar 9 grupos de involucrados descritos a continuación.

- a) *Alta gerencia*. Su compromiso abarca todas las etapas del proyecto, desde su inicio hasta su cierre. Encargada de la gestión de los recursos. Poder alto, Interés alto.
- b) *MINTIC*. El ministerio de las tecnologías de la información y las comunicaciones establece los lineamientos mediante los cuales se rige el desarrollo del proyecto. Poder alto, interés alto.
- c) *MINSALUD*. El ministerio de salud recibe reportes permanentes de la base de datos de pacientes e historias clínicas de la entidad, por lo cual es un interesado moderado en el desarrollo del proyecto. Poder bajo, interés alto.
- d) *Personal del área de Tecnología*. Encargado de ejecutar cada una de las fases del proyecto, siguiendo los lineamientos de la dirección y del ministerio. Poder alto, interés alto.
- e) *Líderes de proceso*. Son los encargados de velar que las directrices impartidas en el marco del proyecto sean acatadas, respetadas y aceptadas por todos los funcionarios de la entidad. Poder bajo, interés alto.
- f) *Funcionarios*. Deberán regirse por las políticas, procedimientos y herramientas desarrolladas en el marco del proyecto. Poder bajo, interés bajo.
- g) *Usuarios*. Los usuarios para este proyecto son los clientes y pacientes de la IPS Sanatorio agua de dios ESE. Se verán beneficiados directamente por la implementación de este proyecto. Poder bajo, interés bajo.
- h) *Contratistas*. Beneficiarios directos, algunos de ellos encargados de ejecutar ciertos procesos de apoyo e implementación dentro del proyecto. Poder bajo, interés bajo.

- i) *Proveedores*. Beneficiarios directos. Se encuentran indiferentes ante la implementación del proyecto, no sienten un beneficio real en sus actividades. Poder bajo, interés bajo.

6.9.2 matriz de interesados.

En la tabla 25 se presenta la clasificación de interesados del proyecto, se muestran sus preocupaciones y expectativas.

Tabla 25. Matriz de interesados

Interesado	Preocupaciones	Expectativas
Alta gerencia	Que la información generada al interior de la entidad esté protegida	Que se realicen todas las acciones e inversiones necesarias para salvaguardar la información
MINTIC	Que las entidades del estado cuenten con un sistema de protección de la información	La entidad debe ejecutar una estrategia para cumplir con la legislación en cuanto a seguridad de la información, de acuerdo con los plazos establecidos
MINSALUD	Adulteración de información	Que los datos se encuentren protegidos contra amenazas
Personal de Tecnología	Asignación de trabajo excesiva, falta de motivación para realizar	Generar oportunidades de crecimiento laboral,

Interesado	Preocupaciones	Expectativas
	actividades	capacitaciones, etc
Líderes de proceso	Interrupción o demora en los procesos	Agilidad en los procesos
Funcionarios	Actividades realizadas que influyen en su trabajo diario, sobre carga de trabajo	La dinámica de trabajo de la entidad mejora
Usuarios	Interrupción de los servicios, demoras en la atención	Datos confidenciales
Contratistas	Gestión de la contratación dispendiosa	Datos seguros, confidencialidad
Proveedores	Neutral	Neutral

Fuente: Elaboración propia.

6.9.3 matriz dependencia influencia.

La tabla 26 muestra los interesados del proyecto con su respectiva influencia, interés y su impacto en el proyecto.

Tabla 26. Matriz de influencia / interés

Interesado	Influencia	Tipo de influencia	Interés	Impacto en el proyecto
Alta gerencia	Alta	Positiva	Alto	Líder
MINTIC	Alta	Positiva	Alto	Apoyo
MINSALUD	Baja	Neutral	Bajo	Apoyo

Interesado	Influencia	Tipo de influencia	Interés	Impacto en el proyecto
Personal de Tecnología	Alta	Positiva	Bajo	Apoyo
Líderes de proceso	Alta	Positiva	Alto	Apoyo
Funcionarios	Baja	Neutral	Bajo	Apoyo
Usuarios	Baja	Neutral	Bajo	Apoyo
Contratistas	Baja	Neutral	Bajo	Apoyo
Proveedores	Baja	Neutral	Bajo	Apoyo

Fuente: Elaboración propia.

La figura 28 muestra las estrategias a considerar de acuerdo con la matriz de poder-interés.

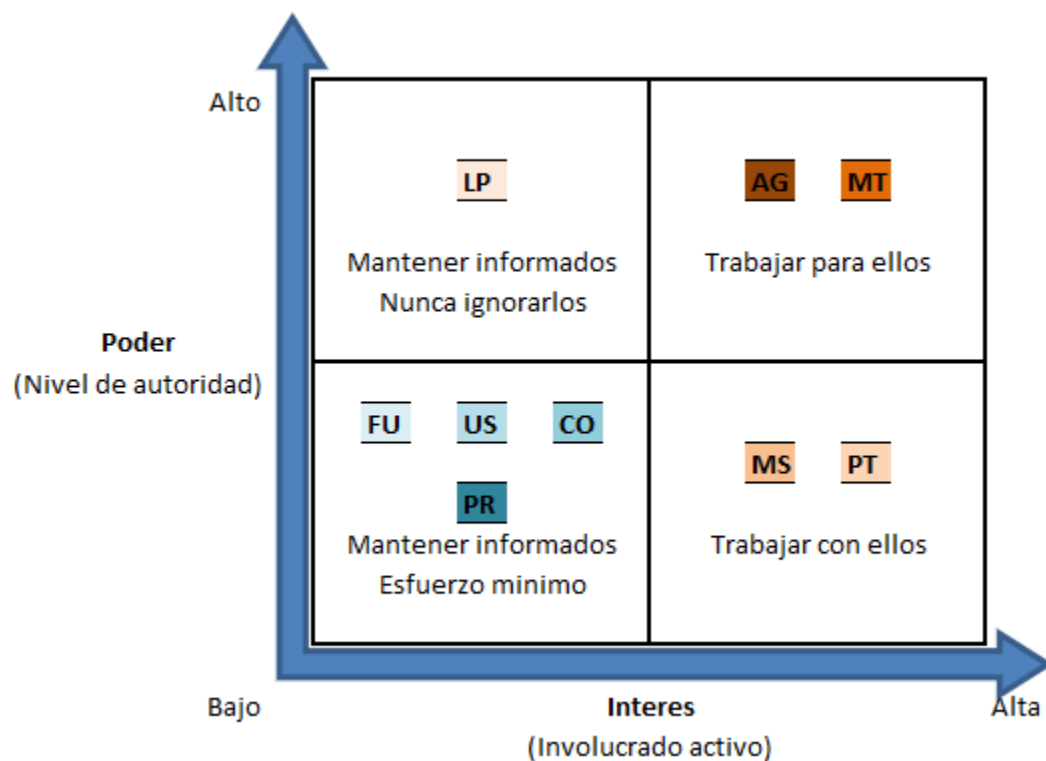


Figura 28. Matriz de poder/interés.

Fuente: Edición propia

6.9.4 matriz de temas y respuestas.

En la tabla 27 se presentan los temas a tratar con los interesados, así como las estrategias a desarrollar con cada uno.

Tabla 27. Matriz de temas y respuestas

Interesado	Temas	Respuesta / Estrategia
Alta gerencia	Comunicar avance, eventos inesperados o adversos, cambios en el plan	Gestionar de cerca, informar requerimientos de los demás interesados, gestión del presupuesto
MINTIC	Comunicar el desempeño de la entidad, avance, cuestiones legales	Gestionar de cerca, solicitar capacitaciones, guías, metodologías y dudas legales
MINSALUD	Comunicar avance	Mantener Informado
Personal de Tecnología	Comunicar avance de cada actividad, actividades a realizar	Mantener Informado
Líderes de proceso	Actividades a realizar que involucren su proceso	Mantener satisfecho
Funcionarios	Actividades realizadas que influyen en su trabajo diario	Monitorear
Usuarios	Comunicar los beneficios que se recibirán con el desarrollo	Monitorear

Interesado	Temas	Respuesta / Estrategia
	del proyecto	
Contratistas	Comunicar los beneficios que se recibirán con el desarrollo del proyecto	Monitorear
Proveedores	Comunicar los beneficios que se recibirán con el desarrollo del proyecto	Monitorear

Fuente: Elaboración propia.

6.9.5 formato para la resolución de conflictos y gestión de expectativas.

El anexo presenta el formato para resolución de conflictos y gestión de expectativas (Ver Anexo W).

7 CONCLUSIONES

Se implementa el sistema de gestión en seguridad de la información para el Sanatorio de Agua de Dios, actualmente en etapa de planificación.

Se define la metodología para la gestión del proyecto en su totalidad, hasta la fase de cierre.

Con la aplicación de la metodología propuesta se puede lograr un alto nivel de calidad en un proceso de implementación en seguridad de la información, sin embargo, no existe una garantía de seguridad absoluta puesto que siempre van a existir amenazas que vulneren las medidas de control adoptadas referentes a confidencialidad, integridad y disponibilidad de la información.

Después de realizado el proyecto, junto con el nivel de madurez alcanzado, se determina que, cumpliendo la norma a un nivel Gestionado, es posible optar por la certificación.

8 REFERENCIAS BIBLIOGRAFICAS

- DAFP. (2011). *Guía para la administración de riesgo*. Departamento administrativo de la función pública (4ta Edición). Bogotá DC.
- Halli, W. (2001). Procurement online. PM Network, 15(3), 40–45. Recuperado de <https://www.pmi.org/learning/library/procurement-online-planning-3514>
- Homer, J. L. (1998). A project procurement vision statement. PM Network, 12(3), 51–55. Recuperado de <https://www.pmi.org/learning/library/project-procurement-vision-statement-3297>
- Icontec. (2006). *Norma Técnica Colombiana NTC-ISO/IEC 27001*. Sistemas de gestión de seguridad de la información.
- Lledó, Pablo. (2013). *Administración de proyectos, El ABC para un director de proyectos exitoso* (3ra Edición). Victoria, BC, Canadá
- MINTIC. (2016). *Controles de seguridad y privacidad de la información*. Recuperado de <http://www.MINTIC.gov.co/gestionti/615/w3-article-5482.html>
- MINTIC. (2016). *Guía para la Implementación de Seguridad de la Información en una MIPYME*. Recuperado de <http://www.MINTIC.gov.co/gestionti/615/w3-article-5482.html>
- MINTIC. (2016). *Modelo de seguridad y privacidad de la información*. Recuperado de <http://www.MINTIC.gov.co/gestionti/615/w3-article-5482.html>
- MINTIC. (2016). *Roles y responsabilidades en seguridad de la información*. Recuperado de <http://www.mintic.gov.co/gestionti/615/w3-article-5482.html>

- PMI, (2013). *Guía de los fundamentos para la dirección de proyectos* (5th Edición) Project Management Institute.
- PMI, (2014). *Implementing organizational project management, a practice guide*, Project Management Institute.
- PMI, (2011). *Practice standard for Earned value management* (2da edition). Project Management Institute.
- PMI, (2007). *Practice standard for Project configuration management*, Project Management Institute.
- PMI, (2011). *Practice standard for Project estimating*, Project Management Institute.
- PMI, (2013). *Practice standard for Project risk management*, Project Management Institute.
- PMI, (2011). *Practice standard for Scheduling* (2da edition). Project Management Institute.
- PMI, (2006). *Practice standard for work breakdown structures* (2da edition). Project Management Institute.
- Zuberi, S. H. (1986). Contract/procurement management. *Project Management Journal*, 17(3), 89–95. Recuperado de <https://www.pmi.org/learning/library/contract-procurement-management-1782>
- Ortegón, E., Pacheco, J., Prieto, A. (2005) *Metodología del marco lógico para la planeación, el seguimiento y la evaluación de proyectos y programas*. Cepal, Naciones Unidas.

ANEXOS

Anexo A. Análisis PESTLE

Componente	Factor	Descripción del factor en el entorno del proyecto	Fase de análisis	¿Describa cómo incide en el proyecto?	¿Cómo potenciaría los efectos positivos y disminuiría los negativos?
Político	Políticas que regulan el sector	El proyecto está determinado por las políticas que dicta en la materia el gobierno nacional, a través del Ministerio de tecnologías de información MinTIC.	P	Los lineamientos que imparte el MinTIC son la base para la realización del proyecto. Se deben seguir los planteamientos según el caso de estudio como entidad prestadora de servicios de salud de baja complejidad	Se debe mantener informado a los delegados del ministerio en cuanto a los avances, retrasos e inconvenientes que se presenten en el desarrollo del proyecto.
	Compromiso de la dirección	La dirección tiene un papel fundamental en este proyecto debido a que los recursos se van asignando de acuerdo con las necesidades cambiantes del proyecto	IMP	Todas la adquisiciones, contrataciones y mejoras se deben realizar justificadas con un estudio de factibilidad que involucra los aspectos económicos de la entidad	Se realiza un análisis detallado de las inversiones a realizar de acuerdo con la política empresarial y el estudio de factibilidad, tanto en su etapa de planificación como ejecución. Es importante que el análisis involucre todas las adquisiciones y contrataciones necesarias para llevar a buen término el proyecto.
Económico	Servicios públicos	Proveedores de servicios de comunicaciones en la zona de influencia del proyecto	P	Un servicio de baja capacidad en un entorno de alta demanda de tráfico en la red puede llegar a desmejorar el servicio en la red actual	Plantear la posibilidad de aumentar los estándares actuales del servicio. Servicios de comunicaciones adicionales serían ideales para mantener en

Componente	Factor	Descripción del factor en el entorno del proyecto	Fase de análisis	¿Describa cómo incide en el proyecto?	¿Cómo potenciaría los efectos positivos y disminuiría los negativos?
					operación los servicios del sanatorio.
		Servicios de recolección de basuras	IMP	No se cuenta con políticas locales de reciclaje de elementos tecnológicos	Se debe realizar una política interna de disposición de los desechos electrónicos para su posterior reubicación en los sitios adecuados de acuerdo con la naturaleza de los mismos
	Recursos limitados	No se tiene un monto específico para la realización del proyecto	P	Es un factor que se debe tener en cuenta con especial atención, dado que todas las adquisiciones se deben justificar desde la fase de inicio y planificación.	Realizar un análisis detallado de todas las inversiones a realizar durante todas las etapas del proyecto, garantizando que se cuentan con los recursos suficientes o el compromiso de la dirección y descartando las que no son viables para buscar alternativas más económicas o justificarlas de manera más adecuada.
Social	Demográfico	Cantidad de usuarios con necesidades de acceso a la información	P	Usuarios de la red de datos con equipos obsoletos	Se debe realizar el inventario de equipos tecnológicos garantizando que todos los usuarios estén dentro de los estándares de seguridad informática, reemplazar los equipos que no cumplan con las características mínimas seguridad.

Componente	Factor	Descripción del factor en el entorno del proyecto	Fase de análisis	¿Describa cómo incide en el proyecto?	¿Cómo potenciaría los efectos positivos y disminuiría los negativos?
	Seguridad de las instalaciones	Exposición de equipos y tecnologías adicionales ante amenazas comunitarias (Robos, saqueos)	IMP	Controles de acceso a las instalaciones no se encuentran reglamentados	Se debe estructurar una política de seguridad de control de acceso a las instalaciones. Monitoreo constante de las cámaras de seguridad con las que cuenta la entidad.
Tecnológico	Tecnología disponible	El inventario tecnológico de la entidad está en un 30% obsoleto	P	Equipos obsoletos representan un riesgo alto para la seguridad de la información, dado que es un factor de vulnerabilidad en la seguridad y privacidad de la información	Con la actualización y verificación del inventario tecnológico de la entidad se pretende realizar las modificaciones, actualizaciones y sustituciones necesarias para mitigar el riesgo que representan estos equipos.
	Redes de conexión	Las redes inalámbricas comunican la sede principal con los albergues	P	Las redes inalámbricas que comunican los albergues presentan constantes fallas, que no permiten en óptimo funcionamiento de la red a los usuarios de estos albergues	Realizar la evaluación de los equipos con los cuales se cuenta para garantizar un adecuado funcionamiento de la red, proponiendo en los casos necesarios las adquisiciones correspondientes para asegurar el servicio y minimizar los fallos.
Legal	Legislación que afecta el proyecto	Norma ISO 27000 sobre seguridad de la información	IMP	La norma ISO 27000 es el estándar internacional para la gestión de la seguridad de la información, en la cual se basa el ministerio de las TIC para diseñar estrategias que ayuden a las entidades del estado a	Se realiza un análisis de los elementos que abarca la norma y los que se definen en el alcance del proyecto, el cual debe ser lo más claro posible con sus limitaciones, ya que el proyecto no pretende certificar a la entidad en

Componente	Factor	Descripción del factor en el entorno del proyecto	Fase de análisis	¿Describa cómo incide en el proyecto?	¿Cómo potenciaría los efectos positivos y disminuiría los negativos?
				salvaguardar su información.	la norma.
Ecológico	Amenazas naturales	Sismos, incendios, inundaciones, temperatura extrema	P	Destrucción de equipos tecnológicos, hardware, instalaciones y daños estructurales, cableados y estaciones de trabajo.	Contar con planes de emergencia para minimizar el impacto en la continuidad del negocio. Contar con sistemas de respaldo en casos de emergencia.
	Contaminación	Contaminación de los suelos por los desechos tecnológicos, contaminación visual por la implementación de torres de comunicación y antenas de radio enlaces	P	Los desechos tecnológicos son una amenaza para el medio ambiente. El proyecto tiene el potencial de generar gran cantidad de residuos de este tipo	Implementar procesos y políticas de reciclaje para los empleados y contratistas del Hospital. Se debe realizar revisiones periódicas a estos procesos para garantizar la disposición final de los residuos.

Fase de análisis: P = Planificación, IMP = Implementación

Fuente: Elaboración propia

Anexo B. Matriz P5

Categorías de sostenibilidad	Sub Categorías	Elementos
Sostenibilidad económica	Retorno de la inversión	Retorno de la Inversión (ROI) ganancia financiera directa a obtenerse producto de la inversión en un portafolio, programa o proyecto. Esta subcategoría cubre la ganancia financiera y el valor presente neto de un proyecto individual.
		Beneficios financieros directos Valor presente neto
	Agilidad del negocio	P5 ve la agilidad del negocio como la capacidad de una organización para adaptarse con facilidad (desde una perspectiva financiera) en respuesta a los cambios en la cartera, programa o proyecto para cumplir con los resultados del proyecto desde una perspectiva de sostenibilidad. Esta sub-categoría se centra en dos elementos, flexibilidad / opcionalidad en el proyecto y el aumento de la flexibilidad del negocio.
		Flexibilidad/Opción en el proyecto Flexibilidad creciente del negocio
	Estimulación económica	P5 ve estimulación económica como la estimulación financiera que se produce como resultado del proyecto. Las dos medidas son de Impacto Económico
		Impacto económico local

Categorías de sostenibilidad	Sub Categorías	Elementos	
		Local y beneficios indirectos.	
		Beneficios indirectos	Los beneficios financieros a la economía que se realicen como consecuencia del portafolio, programa o proyecto que no están definidas en el plan de negocios, pero se materializó como resultado de la inversión
Sostenibilidad ambiental	Transporte	Esta subcategoría cubre los procesos de proyectos y productos impactos que se relacionan con el transporte y se centra en cuatro áreas: Contratación Local, Comunicación Digital, Viajar y Transporte.	
		Mientras que cada elemento de esta categoría se clasifica en la línea de fondo del medio ambiente, cada uno tiene impactos sociales y económicos importantes que deben tenerse en cuenta cuando teniendo en cuenta el impacto global	
		Proveedores locales	La política de una organización y procedimiento para la adquisición de bienes y servicios a partir de fuentes locales para reducir el impacto ambiental (también sirve para disminuir negativo social y económico impactos.)
		Comunicación digital	Políticas y procedimientos para utilizar la tecnología para la comunicación de una organización para reducir el consumo de recursos no renovables
		Viajes	La política de una organización que limite los viajes innecesarios y asegura que los usos de recursos para los viajes tienen el menor impacto sobre el medio ambiente como sea posible
		Transporte	La política de una organización en el transporte de mercancías o materiales que garantiza los aspectos logísticos y el embalaje son lo más ecológica posible

Categorías de sostenibilidad	Sub Categorías	Elementos	
Energía	Esta subcategoría cubre los procesos del proyecto y los impactos de los productos, se centra en tres áreas principales: la energía utilizada, Emisiones/Co2 y cambio a energía limpias.	Energía usada	El tipo y la cantidad de energía que se consume en todo el ciclo de vida del proyecto y la cantidad de energía que el resultado del proyecto consumirá durante su vida útil
		Emisiones /CO2 por la energía usada	La cantidad de las emisiones de carbono que se emite durante el ciclo de vida del proyecto y la impacto en la calidad del aire durante el ciclo de vida del producto del proyecto
		Retorno de energía limpia	El tipo y la cantidad de energía renovable que se genera por el proyecto o productos del proyecto que puede ser devuelto y reasignado
Residuos	Esta subcategoría cubre los procesos del proyecto y los impactos de productos, ya que pertenecen a los residuos durante la extracción de las materias primas, el procesamiento de las materias primas en intermedia y de los productos finales y el consumo de los productos finales y se centra en cinco primarias	Reciclaje	La política de la organización y la práctica en relación con el suministro y el uso de productos y material reciclado, y la adherencia del proyecto a tener prácticas de reciclaje
		Disposición final	La política de la organización para la disposición de los recursos y los activos, y del impacto de los productos del proyecto al finalizar su ciclo de vida en la sociedad y el medio ambiente

Categorías de sostenibilidad	Sub Categorías	Elementos	
	áreas: Reciclaje, reutilización, energía incorporada y los residuos.	Reusabilidad	La política de la organización de reutilizar los materiales en la creación de nuevos productos y la reutilización del producto al final de su vida
		Energía incorporada	La cantidad de energía procedente de fuentes renovables que se incorpora en el proyecto de producto y el consumo de energías renovables durante el ciclo de vida del proyecto.
		Residuos	La política y las prácticas de la organización con respecto a la eliminación de residuos, el tratamiento de residuos durante el ciclo de vida del proyecto, y el tipo y cantidad de residuos generados por los productos del proyecto
	Agua	Calidad del agua	El impacto en la calidad del agua que el proyecto y otros productos del proyecto tendrán en los hábitats y las especies afectadas
		Consumo del agua	La cantidad de agua que será consumida por el proyecto o producto y del proyecto durante su ciclo de vida

Categorías de sostenibilidad	Sub Categorías	Elementos	
Sostenibilidad social	Practicas labores y trabajo decente	Esta subcategoría cubre las políticas de gobierno de proyectos que se relacionan con las prácticas de trabajo, en las normas de organización y operaciones, procedimientos de contratación de la organización y dotación de personal, el trato de los empleados y su bienestar.	<p>Empleo</p> <p>Las prácticas de empleo y el abastecimiento de los individuos que componen el proyecto organización, que van desde el comité directivo del proyecto hasta los miembros del equipo del proyecto miembros, se pueden medir por</p> <ul style="list-style-type: none"> • Tipo de empleo (a tiempo completo o por contrato) • Género • Edad
			<p>Relaciones laborales</p> <p>Enfoque de una organización y su relación con los proyectos propietarios / patrocinadores / partes interesadas en lo que respecta para interferir con mutuas derechos legítimos y humanos: políticas para abordar los problemas, los riesgos y el rendimiento; y procedimientos para la mediación justa</p>
			<p>Educación y capacitación</p> <p>Enfoque de una organización para la gestión de habilidades y de formación que apoya la capacidad del personal para llevar a cabo las actividades del proyecto, maximizando el valor para el proyecto y una contribución positiva a sus carreras</p>

Categorías de sostenibilidad	Sub Categorías	Elementos	
		Aprendizaje organizacional	Enfoque de una organización para la gestión del conocimiento que mejora su capacidad colectiva para aceptar y hacer uso de los nuevos conocimientos en beneficio del avance de la organización y de mitigar el riesgo
		Diversidad e igualdad de oportunidades	Políticas de una organización con respecto a la no discriminación de personal y de recursos de los proyectos basados el grupo de edad, sexo, grupo minoritario y otros indicadores de diversidad.
	Derechos humanos	No discriminación	Política de la organización en materia de no discriminación por motivos de raza, color, origen nacional o étnico, edad, religión, discapacidad, sexo, orientación sexual, identidad y expresión de género, condición de veterano o cualquier otra característica protegida por la ley aplicable
		Libre asociación	Políticas y procesos organizacionales que garantizan los derechos del personal a afiliarse o retirarse de los grupos de su elección y de los grupos a emprender acciones colectivas para defender los intereses de sus miembros

Categorías de sostenibilidad	Sub Categorías	Elementos
Sociedad y consumidores	Esta subcategoría cubre los impactos de una cartera, programa o proyecto en la sociedad en la que el producto del proyecto tendrá un impacto en los usuarios finales o los clientes que hagan uso de ella	Trabajo forzoso y obligatorio
		Políticas y medidas de organización que salvaguarden contra el trabajo forzoso u obligatorio, ya sea directamente o a través de los canales de proveedores
		Apoyo de la comunidad
		El nivel de apoyo de la comunidad hacia el proyecto tendrá un impacto en forma directa e indirecta desde una perspectiva nacional y global-local, regional
		Salud y seguridad del consumidor
		La adhesión a las medidas que aseguren que el proyecto no pone en peligro o genera efectos adversos para el usuario final
Sociedad y consumidores	Esta subcategoría cubre los impactos de una cartera, programa o proyecto en la sociedad en la que el producto del proyecto tendrá un impacto en los usuarios finales o los clientes que hagan uso de ella	Etiquetas de productos y servicios
		El etiquetado de la información de productos y servicios del proyecto, para asegurar la precisión del contenido, el uso seguro, eliminación y cualquier factor que pueda tener impactos ambientales o sociales
		Mercadeo y publicidad
Sociedad y consumidores	Esta subcategoría cubre los impactos de una cartera, programa o proyecto en la sociedad en la que el producto del proyecto tendrá un impacto en los usuarios finales o los clientes que hagan uso de ella	La notificación de los incidentes y relacionados con el cumplimiento normativo, los derechos humanos, las leyes o políticas públicas
		Privacidad del consumidor
Sociedad y consumidores	Esta subcategoría cubre los impactos de una cartera, programa o proyecto en la sociedad en la que el producto del proyecto tendrá un impacto en los usuarios finales o los clientes que hagan uso de ella	Las políticas y procedimientos de la organización relacionadas con el tratamiento de la información de los clientes, quejas, cuestiones de reglamentación o la pérdida de información de los clientes

Categorías de sostenibilidad	Sub Categorías	Elementos
Comportamiento ético	Esta subcategoría cubre los procesos de proyectos y productos impactos, relacionados con el comportamiento ético y se centra en tres áreas: Inversiones y Adquisiciones, soborno, corrupción y anti-Competencia.	Prácticas de inversión y abastecimiento de Los procesos de la organización para seleccionar las inversiones y las prácticas para proveer el proyecto de los recursos.
		Comportamiento anti ético La política, acciones de una organización y reportes sobre el comportamiento anticompetitivo, incluyendo cualquier acción legal o quejas de los organismos reguladores

Fuente: Elaboración propia

Anexo C. Matriz de requisitos legales

JERARQUÍA DE LA NORMA	NÚMERO/ FECHA	TITULO	ARTICULO	APLICACIÓN ESPECIFICA	VERIFICACIÓN	PLAN DE ACCIÓN
DECRETO	0948 de 1995	Medio Ambiente-Emisiones atmosféricas	Art. 37	Prohibida la descarga al aire, por parte de cualquier fuente móvil, en concentraciones superiores a las previstas en las normas de emisión, de contaminantes tales como monóxido de carbono (CO), hidrocarburos (HC), óxidos de nitrógeno (NOX), partículas.	Todos los vehículos que se usaran en el proyecto deben contar con revisión técnico-mecánica y de gases vigente.	Se realizan inspecciones diarias mediante lista de chequeo a los vehículos a utilizar en el día
DECRETO	2811 de 1974	Medio Ambiente	Art. 35	Se prohíbe descargar, sin autorización, los residuos, basuras y desperdicios y, en general, de desechos que deterioren los suelos o causen daño o molestia a individuos o núcleos humanos.	Todos los contratistas de la entidad deben proporcionar información sobre la disposición final de residuos.	No aplica
DECRETO	838 de 2005	Disposición final de residuos sólidos	Art.5	Disposición Final de Residuos Sólidos	Todos los contratistas de la entidad deben proporcionar información sobre la disposición final de residuos.	No aplica

JERARQUÍA DE LA NORMA	NÚMERO/ FECHA	TITULO	ARTICULO	APLICACIÓN ESPECIFICA	VERIFICACIÓN	PLAN DE ACCIÓN
Ley	697 de 2001	Programa uso eficiente y ahorro en el consumo de energía.	Art.1	Mediante la cual se fomenta el uso racional y eficiente de la energía, se promueve la utilización de energías alternativas y se dictan otras disposiciones.	Inspecciones de rutina y verificación de que los equipos electrónicos no usados permanezcan apagados	Capacitaciones y sensibilización al personal mediante correo electrónico y charlas
DECRETO	2501 de 2007	Programa uso eficiente y ahorro en el consumo de energía.	Art. 3	Propiciar el uso racional de energía	Inspecciones de rutina y verificación de que los equipos electrónicos no usados permanezcan apagados	Capacitaciones y sensibilización al personal mediante correo electrónico y charlas
Uso racional de energía eléctrica.	Decreto 3450 de 2008	Ministerio de Medio Ambiente	Art 1	Todos los usuarios del servicio de energía deben sustituir todas las fuentes de baja eficacia lumínica	Listado actualizado de ambientes con fuentes lumínicas que requieren sustitución	Departamento de mantenimiento gestionara la adquisición de lamparas ahorradoras para todos los ambientes de la institución

JERARQUÍA DE LA NORMA	NÚMERO/ FECHA	TITULO	ARTICULO	APLICACIÓN ESPECIFICA	VERIFICACIÓN	PLAN DE ACCIÓN
RESOLUCIÓN	180173 14 de febrero	residuos peligrosos luminarias	Art 1	Establecer los requisitos mínimos de eficacia, vida útil y demás especificaciones técnicas de las fuentes de iluminación que se deben utilizar, desacuerdo con el desarrollo tecnológico y las condiciones de mercado de estos productos.	Listado actualizado de ambientes con fuentes lumínicas que requieren sustitución	Departamento de mantenimiento gestionara la adquisición de lamparas ahorradoras para todos los ambientes de la institución
LEY	1672 de 3013	Gestión integral de RAEE	Art 1	Por la cual se establecen los lineamientos para la adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos (raee), y se dictan otras disposiciones"	Los residuos electrónicos son almacenados de acuerdo con la política institucional de manejo de residuos electrónicos	Socialización y sensibilización de la política de gestión de residuos electrónicos
RESOLUCIÓN	372	Por la cual se establecen los elementos que deben contener los Planes de Gestión de Devolución	Art 4, 5, 10	Por la cual se establecen los elementos que deben contener los Planes de Gestión de Devolución de Productos Post consumo de Baterías Usadas Plomo Acido, y se adoptan otras disposiciones. Aplicable al proveedor de transporte. Art 4, los distribuidores y comercializadores de baterías plomo acido deben informar sobre los puntos y mecanismos de	Baterías en desuso almacenadas en los espacios acondicionados para tal fin	No Aplica

JERARQUÍA DE LA NORMA	NÚMERO/ FECHA	TITULO	ARTICULO	APLICACIÓN ESPECIFICA	VERIFICACIÓN	PLAN DE ACCIÓN
		de Productos Post consumo de Baterías Usadas Plomo Acido, y se adoptan otras disposicione s.		recolección de estos residuos. Art 5, Son obligaciones de los consumidores a) Seguir las instrucciones de manejo seguro suministradas por el fabricante o importador del producto hasta finalizar su vida útil; y b) Entregar los residuos o desechos peligrosos post consumo al mecanismo de devolución o retorno que el fabricante o importador establezca. Art 10, Está prohibido quemar las baterías plomo acido, drenar el líquido que contiene, disponerla en relleno sanitario o a cielo abierto		
Proyecto de ley	91 de 2009	mediante la cual se regula la política pública de residuos eléctricos y electrónicos (RAEE) en Colombia.	Art 1	Establecer los lineamientos para la elaboración de una política pública que regule la gestión y el manejo integral de los Residuos de Aparatos Eléctricos y Electrónicos RAEE generados en el territorio nacional. Así como establecer las responsabilidades extendidas del importador, productor, comercializador y generador de los Residuos de Aparatos eléctricos y electrónicos RAEE.	La vida útil de los equipos deberá garantizar su operabilidad durante todo el proyecto	Adquisiciones realizadas deberán cumplir con estándares de calidad y vida útil adecuada para el proyecto

JERARQUÍA DE LA NORMA	NÚMERO/ FECHA	TITULO	ARTICULO	APLICACIÓN ESPECIFICA	VERIFICACIÓN	PLAN DE ACCIÓN
Norma interna (voluntaria)	Res 1354 de 2017	Política institucional de consumo eficiente de energía	Art 1	Mediante la cual se establecen los lineamientos para la reducción y uso eficiente de energía en el Hospital de Agua de Dios ESE.	Costos mensuales de energía son reducidos en un 20%	Socialización y sensibilización de la política de uso eficiente de energía eléctrica
Norma interna (voluntaria)	Res 1343 de 2017	Política institucional para la gestión de residuos de aparatos eléctricos y electrónicos (RAEE)	Art 1	Mediante la cual se establecen los lineamientos para la recolección y disposición final de residuos de aparatos eléctricos y electrónicos en el Hospital de Agua de Dios ESE.	Los residuos electrónicos son almacenados de acuerdo con la política institucional de manejo de residuos electrónicos	Socialización y sensibilización de la política de gestión de residuos electrónicos
Norma interna (voluntaria)	Res 1322 de 2017	Política de cero papeles	Art 1	Mediante la cual se establecen los lineamientos para la impresión y fotocopiado de documentos internos en la institución.	Disminución de papel impreso circulante en la institución	Socialización y sensibilización de la política de cero papel

Fuente: Elaboración propia

Anexo D. Caso de negocio

Caso de Negocio	
Proyecto	Implementación SGSI para el Hospital de Agua de Dios E.S.E.

DESCRIPCIÓN DEL PRODUCTO DEL PROYECTO
El producto a desarrollar consiste en generar la documentación administrativa e instalación de los recursos técnicos para la puesta en marcha del modelo de seguridad y privacidad de la información para el sanatorio de Agua de dios, además de implementar todos los sistemas necesarios en el tratamiento de la información dentro de la organización.

ALINEAMIENTO DEL PROYECTO			
OBJETIVOS ESTRATÉGICOS DE LA ORGANIZACIÓN			
Implementar un sistema de seguridad y privacidad de la información para la entidad con el fin de salvaguardar la información que se maneja al interior de la institución.			
Reducir a su nivel más bajo posible la brecha en seguridad de la información de acuerdo con la norma NTC ISO 27001			
ANÁLISIS COSTO - BENEFICIO			
(Descripción de la acción que origina el costo)		(Beneficios que tendrá la organización una vez que el producto del proyecto esté operativo o sea entregado)	

Total	\$	Total	\$

OBJETIVOS DEL PROYECTO			
Concepto	Objetivos	Métrica	Indicador de Éxito
Alcance	<p>Establecer una metodología mediante la cual se puede gestionar la seguridad de la información de forma clara y concisa</p> <p>Permitir a la organización continuar operando con normalidad en caso de producirse problemas importantes.</p>	La entidad debe manejar un SGSI en fase de mejora continua	Requisito de cumplimiento superior al 72% de los requisitos de la norma.
Tiempo	Cumplir con los plazos establecidos para la ejecución de las actividades.	Se establece un periodo de 12 meses para la ejecución del proyecto	Ciclo de vida del proyecto entre 10 y 14 meses.
Costo	Cumplir con el presupuesto establecido para el proyecto.	Se establece un presupuesto inicial de COP \$ 300'000.000	Costo total de la implementación inferior a COP \$ 310'000.000

Calidad	Reducir el riesgo de que se produzcan pérdidas de información en la organización.	Riesgo de pérdida de información controlado	Cero pérdidas de información durante la fase de mejora continua del SGSI
Satisfacción del Clientes	Garantizar frente a clientes y socios estratégicos que la entidad demuestra compromiso en salvaguardar la información que es depositada en la misma.	Imagen institucional mejorada.	Aprobación de MINTIC para operar bajo los estándares establecidos para entidades públicas del sector salud.

NECESIDADES DEL NEGOCIO

La implementación de la seguridad de la información es crítica hoy en día, y está presente en muchas situaciones cotidianas. Las técnicas empleadas para proteger la información de cómo los controles de acceso mediante usuario y contraseña no son suficientes en la actualidad para protegernos de ataques informáticos y delincuentes informáticos.

La gran cantidad de bases de datos ubicadas en sistemas de computación públicos y privados que contienen información relativa a las personas (bancaria, judicial, de seguros, de salud, educación, etc.) conforman un riesgo potencial de invasión a la privacidad.

En el ámbito médico, las bases de datos y protección de la privacidad, integridad y

disponibilidad de la información, como las historias clínicas computarizadas, movimientos financieros e inventarios se ven amenazados y son atacados frecuentemente por delincuentes informáticos.

Para proteger la información y asegurarnos que esta no sea leída o adultera el sistema debe emplear diversas técnicas descritas en la norma ISO 27000 sobre seguridad de la información.

Es conocido que las pérdidas económicas y de reputación de la empresa son gigantescas cuando se presentan fallas en la seguridad de la información. El hurto y adulteración de bases de datos es frecuente en nuestros tiempos, por lo cual los costos asociados a la implementación en seguridad de la información son sustancialmente bajos, comparados con el impacto negativo que tendría un evento adverso en la información almacenada.

FINALIDAD DEL PROYECTO

El proyecto de implementación de un sistema de gestión de seguridad de la información consiste en garantizar la disponibilidad, integridad y confidencialidad de los sistemas de información en una entidad pública prestadora de servicios de salud, como lo es el Sanatorio de Agua de Dios.

FACTORES CRÍTICOS DEL ÉXITO DEL PROYECTO

El Hospital de Agua de Dios ESE. Consciente de la necesidad de salvaguardar su información, garantizando su integridad, privacidad y disponibilidad, requiere la ejecución de un proyecto para satisfacer esta necesidad, y así reducir a su nivel más bajo posible la brecha en seguridad de la información de acuerdo con la norma NTC ISO 27001.

ACTA DE CONSTITUCIÓN DEL PROYECTO

Fecha: 28-Octubre-2017	Nombre del Proyecto: Implementación de un Sistema de gestión en seguridad de la información (SGSI) para el Sanatorio de Agua de Dios ESE.
<p>Justificación:</p> <p>La Entidad SANATORIO DE AGUA DE DIOS E.S.E. como entidad prestadora de servicios de salud, consciente de la necesidad de mantener la seguridad y privacidad de la información que maneja, ha tomado la determinación de implementar un sistema de gestión de seguridad de la información. El problema de la seguridad de la información se caracteriza por la complejidad y la interdependencia. La gestión de la seguridad contiene un número importante de factores y elementos que se interrelacionan entre sí. Las micro, pequeñas y medianas empresas por lo general tienen una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridad olvidadas. De ahí la gran importancia de implementar es este proyecto al interior de la Institución.</p>	
<p>Objetivos estratégicos</p> <p>Implementar un sistema de seguridad y privacidad de la información para la entidad con el fin de salvaguardar la información que se maneja al interior de la institución</p>	<p>Criterios de éxito</p> <p>Reducir a su nivel más bajo posible la brecha en seguridad de la información de acuerdo con la norma NTC ISO 27001</p>
<p>Breve descripción del proyecto</p> <p>El producto a desarrollar consiste en generar toda la documentación administrativa y la instalación de los recursos técnicos para la puesta en marcha del modelo de seguridad y privacidad de la información para el sanatorio de Agua de dios, además de implementar todos los sistemas necesarios en el tratamiento de la información dentro de la organización, siguiendo los lineamientos que para ello dicta el ministerio de las tecnologías de la información y las comunicaciones (MINTIC), basándose en la norma técnica colombiana NTC ISO 27001.</p>	

El proyecto consta de 4 fases las cuales se discriminan a continuación:

Fase de diagnóstico: Autoevaluación de la entidad para determinar estado actual en cuanto a seguridad de la información.

Fase de planificación: Generación de los planes requeridos para la ejecución del proyecto.

Fase de ejecución: Puesta en marcha de los planes que se realizaron en la fase de planificación.

Fase de mejora: Mejora continua y controles al sistema de gestión de la seguridad de la información.

Principales interesados

Entre los principales interesados se cuentan:

Entidades del Gobierno (MINTIC, MINSALUD)

Alta gerencia

Paciente y usuarios

Coordinadores de área

Líderes de proceso

Empleados, contratistas y proveedores.

Requisitos generales y restricciones

Implementación de controles y generación de documentos, políticas, procedimientos, manuales, que sirvan como base para establecer el SGSI.

Instalación y configuración de los equipos, dispositivos e infraestructura necesarios para dar soporte a las políticas, procedimientos y planes de gestión establecidos en el SGSI.

La implementación no pretende certificar a la entidad en la norma ISO 27001

Riesgos principales

Perdida de información, secuestro de información, parada de planta, problemas legales con usuarios, pacientes, contratistas y proveedores.	
Cronograma de hitos principales	
Inicio del proyecto. 30-10-2017	
Terminación fase de inicio 28-11-2017	
Terminación fase de planificación 12-03-2018	
Terminación fase de implementación 13-07-2018	
Terminación fase de evaluación 29-10-2018	
Terminación proyecto 14-11-2018	
Presupuesto global preliminar	
Presupuesto para la ejecución del proyecto se tendrá en cuenta de acuerdo con los estudios generados en el marco del proyecto, partiendo de una base de \$ 300'000.000	
Director del Proyecto	Nivel de autoridad
Nestor Martinez M.	<input checked="" type="checkbox"/> Acceder a la información del cliente y negociar cambios <input checked="" type="checkbox"/> Programar reuniones del proyecto con los gerentes funcionales <input checked="" type="checkbox"/> Aprobar el presupuesto del proyecto y sus modificaciones <input checked="" type="checkbox"/> Negociar con los gerentes funcionales los miembros del equipo
Patrocinador	Firma del patrocinador
Hector Medina	

Información del Proyecto

Empresa / Organización	
Proyecto	
Fecha de preparación	
Cliente	
Patrocinador principal	
Gerente de Proyecto	

Patrocinador / Patrocinadores

Nombre	Cargo	Departamento / División

Razón de cierre

--

Por medio de la presente, se da cierre formal al proyecto, por las razones especificadas en la siguiente ficha:

Marcar con una "X" la razón de cierre:

Entrega de todos los productos de conformidad con los requerimientos del cliente.	
Entrega parcial de productos y cancelación de otros de conformidad con los requerimientos del cliente.	

Cancelación de todos los productos asociados con el proyecto.	
---	--

Aceptación de los productos o entregables

A continuación, se establece cuales entregables de proyecto han sido aceptados:

Entregable	Aceptación (Si o No)	Observaciones

Para cada entregable aceptado, se da por entendido que:

- El entregable ha cumplido los criterios de aceptación establecidos en la documentación de requerimientos y definición de alcance.
- Se ha verificado que los entregables cumplen los requerimientos.
- Se ha validado el cumplimiento de los requerimientos funcionales y de calidad definidos.
- Se ha realizado la transferencia de conocimientos y control al área operativa.
- Se ha concluido el entrenamiento que se definió necesario.
- Se ha entregado la documentación al área operativa.

Se autoriza al Gerente de Proyecto a continuar con el cierre formal del proyecto o fase, lo cual deberá incluir:

- Evaluación post-proyecto o fase.
- Documentación de lecciones aprendidas.
- Liberación del equipo de trabajo para su reasignación.

- Cierre de todos los procesos de procura y contratación con terceros.
- Archivo de la documentación del proyecto.

Una vez concluido el proceso de cierre, el Patrocinador (Sponsor) del proyecto deberá ser notificado para que el Gerente de Proyectos sea liberado y reasignado.

Aprobaciones

Patrocinador	Fecha	Firma

Anexo G. Enunciado del alcance

ENUNCIADO DEL ALCANCE

IMPLEMENTACION SGSI

Fecha:	Nombre del Proyecto:		Versión
28-Octubre-2017	Implementación SGSI para el Hospital de Agua de Dios E.S.E.		1.1
Director del Proyecto	Miembros del equipo . Nestor Martinez . Hector Medina . Angelino Guerrero . Antonio Valdez	Otros Interesados . Pacientes IPS . Contratistas IPS . Funcionarios IPS . Gobierno Nacional . Comunidad de Agua de Dios	
Nestor Martinez			
Patrocinador			
Hector Medina			
Cliente			
Hospital de Agua de Dios E.S.E.			
Descripción del Producto			
<p>El producto a desarrollar consiste en generar toda la documentación administrativa y la instalación de los recursos técnicos para la puesta en marcha del modelo de seguridad y privacidad de la información para el sanatorio de Agua de dios, además de implementar todos los sistemas necesarios en el tratamiento de la información dentro de la organización.</p> <p>Dentro de los sistemas necesarios para el tratamiento y disposición de la información y que garanticen la integridad, disponibilidad y confidencialidad de la</p>			

información se definen los siguientes:

Instalación de cámaras de seguridad, (CCTV)

Instalación de infraestructura para la operación de datacenter

Instalación de sistema de alimentación ininterrumpida

Utilización

La información, junto a los procesos y los sistemas que hacen uso de ella, son activos demasiado importantes para la empresa. La **confidencialidad, integridad y disponibilidad** de dicha información puede ser esencial para mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la empresa necesarios para conseguir los objetivos de la empresa y asegurarse de que haya beneficios económicos.

El cumplimiento de la legislación, la adaptación dinámica y de forma puntual de todas las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar que se obtiene el máximo beneficio son algunos de los aspectos fundamentales en los que un **SGSI** es una herramienta de gran utilidad y de importante ayuda para la gestión de las empresas.

El modelo de gestión de la seguridad tiene que contemplar unos procedimientos adecuados y planificar e implementar controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de estos.

La documentación mínima que se debe tener en cuenta a la hora de implementar un **SGSI**:

Política y objetivos de seguridad.

El alcance del **SGSI**.

Los procedimientos y los controles que apoyan al **SGSI**.

Plan de tratamiento de riesgos.

Procedimientos de planificación, manejo y control de los procesos de **seguridad de la información** y de medición de la eficacia de los controles.

Declaración de aplicabilidad.

Procedimiento de gestión de toda la documentación del **SGSI**.

Requerimientos	Solicitado por	Importancia (A, M, B)
Pruebas de efectividad	Gerencia	A
Elaboración de políticas y procedimientos	G.E.L.	A
Distribución de roles y responsabilidades	G. Proyecto	A
Gestión y clasificación de activos	G.E.L.	A
Gestión documental	Gerencia	M
Gestión de riesgos	G. Proyecto	A
Controles e indicadores de gestión de la seguridad de la información	G. Proyecto	A
Plan de continuidad del negocio y análisis de impacto	Gerencia	A
Seguridad en la nube	Gerencia	B
Plan de comunicación, sensibilización y capacitación	G.E.L.	M
Auditoria	G.E.L.	A
Evaluación de desempeño	G. Proyecto	M

Transición de IPv4 a IPv6	Oficina TIC	A
<p>Plazo de entrega del producto final: 1 año</p> <p>Se espera que la finalización del proyecto sea en Noviembre de 2018</p> <p>Costo total del proyecto:</p> <p>Costo del proyecto se calcula de acuerdo con los análisis a realizar en la fase de inicio, según la situación actual de la entidad, inicialmente estimado en \$ 300'000.000</p> <p>Beneficios:</p> <p>Establecer una metodología de Gestión de la Seguridad estructurada y clara.</p> <p>Reducción del riesgo de que se produzcan pérdidas de información en la organización.</p> <p>El personal puede acceder a la información autorizada de una manera confiable.</p> <p>Se genera una cultura de revisión periódica mediante la realización de auditorías externas, que permitan identificar los incidentes que pudiera haber en el Sistema de Gestión de Seguridad de la Información, fomentando de este modo la mejora continua en el sistema.</p> <p>Mejora la imagen de la institución al garantizar frente a clientes y socios estratégicos que la entidad demuestra compromiso en salvaguardar la información que es depositada en la misma.</p> <p>Permite a la organización continuar operando con normalidad en caso de producirse</p>		

problemas importantes.

Hace que la entidad cumpla con la legislación vigente en materia de información personal y propiedad intelectual.

Entregables

Finales	Parciales	Fecha	Persona que Aprueba
Diagnostico	Autoevaluación	30-07-2017	G.P.
	Encuesta	30-07-2017	G.P.
	Estratificación	30-07-2017	G.P.
Políticas y procedimientos	Manual de políticas de seguridad de la información	30-09-2017	G.P.
	Procedimientos de seguridad de la información	30-09-2017	G.P.
Planes	Plan de transición a IPv6	30-04-2018	G.P.
	Plan de continuidad del negocio	30-04-2018	G.P.
	Plan de auditorias	30-04-2018	G.P.
	Plan de gestión de riesgos	30-04-2018	G.P.
Inventarios	Inventario de activos de información	30-04-2018	G.P.

	Inventario de áreas	30-04-2018	G.P.
	Interesados	30-04-2018	G.P.
	Proveedores	30-04-2018	G.P.
Avances	Avance Plan IPv6	30-07-2018	G.P.
	Avance Plan de auditorias	30-07-2018	G.P.
	Avance plan de gestión de riesgos	30-07-2018	G.P.
	Avance plan de continuidad	30-07-2018	G.P.
<p>Criterios de aceptación</p> <p>Debe ser una demostración clara de que el proyecto cumple a cabalidad con los objetivos de acuerdo con la fase entregada.</p> <p>El porcentaje de cumplimiento debe llegar a un 80% en cada fase del entregable.</p> <p>Todos los entregables deben ser aprobados por la oficina de planeación y sistemas de información</p>			
<p>Exclusiones:</p> <p>No se pretende certificar a la entidad en la norma ISO 27001</p>			

<p>Restricciones</p> <p>No se contratará personal de planta para la ejecución del proyecto</p> <p>Requerimientos adicionales de personal, equipos, insumos y otros deben estar debidamente soportados por la gerencia del proyecto y avalados por la gerencia de la entidad.</p> <p>Prioridades 1º Costo / 2º Alcance / 3º Tiempo</p>	
<p>Supuestos</p> <p>Se contempla la contratación de expertos externos para la implementación de equipos tecnológicos necesarios para la seguridad de la información.</p>	
Director del Proyecto	Nestor Martinez (Supervisor E.S.E.)
Otros interesados	<p>Hector Medina (Gerente administrativo E.S.E.)</p> <p>Andrés Cárdenas (Asesor de proyecto)</p>

Fuente: Edición propia basado en formato original de Pablo Lledó, tomado de www.pablolledo.com

Anexo H. Matriz de trazabilidad de requisitos administrativos

ID	CARGO	ITEM	DESCRIPCIÓN	ENTREGABLE	VERSION
1	Responsable de SI	Documento de la política de seguridad y privacidad de la Información	Definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados.	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	1,1
2	Responsable de SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	1,1
3	Responsable de SI	Responsabilidades de la dirección	La dirección debe exigir 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.	SEGURIDAD DE LOS RECURSOS HUMANOS	1,1
4	Responsable de SI	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	SEGURIDAD DE LOS RECURSOS HUMANOS	1,1
5	Responsable de SI	Inventario de activos	Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	GESTIÓN DE ACTIVOS	1,1

ID	CARGO	ITEM	DESCRIPCIÓN	ENTREGABLE	VERSION
6	Responsable de SI	Devolución de activos	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.	GESTIÓN DE ACTIVOS	1,1
7	Responsable de SI	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	GESTIÓN DE ACTIVOS	1,1
8	Responsable de la Continuidad	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa,	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	1,1
9	Responsable de SI	Protección de registros.	Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales	CUMPLIMIENTO	1,1
10	Control interno	Cumplimiento con las políticas y normas de seguridad.	Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.	CONTROL INTERNO	1,1
11	Responsable de compras y adquisiciones	Seguridad de la información en las relaciones con los proveedores	Asegurar la protección de los activos de la entidad que sean accesibles para los proveedores	RELACIONES CON LOS PROVEEDORES	1,1

Fuente: Edición propia basado en controles de la norma ISO 27002

Anexo I. Matriz de trazabilidad de requisitos técnicos

ID	CARGO	ITEM	DESCRIPCIÓN	ENTREGABLE	VERSION
1	Responsable de SI	REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	Se debe limitar el acceso a información y a instalaciones de procesamiento de información.	CONTROL DE ACCESO	1,1
2	Responsable de TICs	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	CONTROL DE ACCESO	1,1
3	Responsable de SI	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	GESTIÓN DE ACCESO DE USUARIOS	1,1
4	Responsable de SI	Restricción de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	1,1
5	Responsable de la seguridad física	ÁREAS SEGURAS	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	SEGURIDAD FÍSICA Y DEL ENTORNO	1,1
6	Líderes de los procesos	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	SEGURIDAD FÍSICA Y DEL ENTORNO	1,1

ID	CARGO	ITEM	DESCRIPCIÓN	ENTREGABLE	VERSION
7	Responsable de SI	Trabajo en áreas seguras	Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	SEGURIDAD FÍSICA Y DEL ENTORNO	1,1
8	Responsable de SI	EQUIPOS	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	SEGURIDAD FÍSICA Y DEL ENTORNO	1,1
9	Responsable de TICs	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SEGURIDAD FÍSICA Y DEL ENTORNO	1,1
10	Responsable de TICs	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SEGURIDAD FÍSICA Y DEL ENTORNO	1,1
11	Responsable de TICs	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	SEGURIDAD DE LAS OPERACIONES	1,1
12	Responsable de SI	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	SEGURIDAD DE LAS OPERACIONES	1,1
13	Responsable de TICs	COPIAS DE RESPALDO	Proteger contra la pérdida de datos.	SEGURIDAD DE LAS OPERACIONES	1,1
14	Responsable de TICs	CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.	GESTIÓN DE LA VULNERABILIDAD TÉCNICA	1,1

ID	CARGO	ITEM	DESCRIPCIÓN	ENTREGABLE	VERSION
15	Responsable de TICs	GESTIÓN DE LA SEGURIDAD DE LAS REDES	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	SEGURIDAD DE LAS COMUNICACIONES	1,1
16	Responsable de TICs	TRANSFERENCIA DE INFORMACIÓN	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	SEGURIDAD DE LAS COMUNICACIONES	1,1
17	Responsable de TICs	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SEGURIDAD DE LAS COMUNICACIONES	1,1
18	Responsable de SI	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1,1
19	Responsable de SI	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE	Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1,1
20	Responsable de TICs	Procedimientos de control de cambios en sistemas	El cambio a los sistemas dentro del ciclo de vida de desarrollo se debe controlar mediante el uso de procedimientos formales de control de cambios.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1,1

ID	CARGO	ITEM	DESCRIPCIÓN	ENTREGABLE	VERSION
21	Responsable de SI	DATOS DE PRUEBA	Asegurar la protección de los datos usados para pruebas.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1,1
22	Responsable de SI	Protección de datos de prueba	Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	1,1
23	Responsable de SI	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	1,1

Fuente: Edición propia basado en controles de la norma ISO 27002

Anexo J. Diccionario de la EDT

1. Implementación SGSI	Descripción: Implementación de un sistema de gestión de seguridad de la información para el Sanatorio de Agua de Dios ESE. Criterios de aceptación: Sistema implementado de acuerdo con la norma NTC/ISO 27001
1.1 Inicio	Descripción: Actividades de inicio del proyecto Duración: 1 mes
1.1.1 Gerencia de proyecto	Descripción: Documentación requerida para el inicio de las actividades
1.1.1.1 Planes de gestión	Plan de gestión de alcance, tiempo y costo
1.1.2 Diagnostico	Descripción: Identificación del problema Criterios de aceptación: Identificación de amenazas, establecimiento de la línea base del estado de la entidad
1.1.2.1 Autoevaluación	Descripción: Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección Criterios de aceptación: Documento generado
1.1.2.2 Encuesta y estratificación	Descripción: Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección Criterios de aceptación: Documento generado
1.2 Planificación	Descripción: definición del alcance, generación de planes y análisis de riesgos Duración: 3 meses Criterios de aceptación: Cumplimiento de la normativa aplicable de acuerdo con las tareas
1.2.1 Indicadores y métricas	Descripción: Indicadores y métricas de seguridad de la información definidos. Criterios de aceptación:
1.2.2 Política de seguridad	Descripción: Declaración de aplicabilidad del MSPI Criterios de aceptación: Documento generado
1.2.3 Control documental	Descripción: Listado de procedimientos de control documental del MSPI Criterios de aceptación: Listado generado
1.2.4 Metodología de riesgos	Descripción: Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información Criterios de aceptación: Organigrama de roles
1.2.4.1 Componentes	Descripción: Generación de manuales y procedimientos del SGSI Criterios de aceptación: Manuales y procedimientos avalados por la dirección
1.2.4.2 Análisis y evaluación	Descripción: Riesgos identificados y valorados de acuerdo con la metodología Criterios de aceptación: Documento generado

1.2.4.3 Tratamiento de riesgos	Descripción: Elaboración del plan de tratamiento de riesgos de acuerdo la metodología de gestión de riesgos
	Criterios de aceptación: Plan elaborado
1.2.5 Manuales y procedimientos	
1.2.6 Planes	Descripción: Elaboración de los planes contemplados en el SGSI - Plan de transición a IPV6, Plan de comunicación, Plan de continuidad
	Criterios de aceptación: Se elaboran la totalidad de los planes
1.2.7 Inventarios	Descripción: Realizar los inventarios requeridos
	Criterios de aceptación: listado de inventarios
1.2.8 Auditorias	Descripción: Elaboración del diagrama de red de la entidad
	Criterios de aceptación: Documento generado
1.2.9 Estructura TI	Descripción: Implementación y puesta en marcha del modelo de seguridad y privacidad de la información
1.3 Implementación	Descripción: Implementación y puesta en marcha del modelo de seguridad y privacidad de la información
	Duración: 6 meses
	Criterios de aceptación: Implementación de acuerdo con el plan realizado
1.3.1 Estrategia de planificación y control	Descripción: Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
	Criterios de aceptación: Documento aprobado
1.3.2 Avance IPv4 IPv6	Descripción: Avance en la implementación de la estrategia de transición de IPv4 a Ipv6
	Criterios de aceptación: Adecuada medición del avance del plan
1.3.3 Avance riesgos	Descripción: Avance en la ejecución del plan de tratamiento de riesgos
	Criterios de aceptación: Adecuada medición del avance del plan
1.3.4 Controles	Descripción: Realización de todos los controles contemplados en el MSPI
	Criterios de aceptación: Implementación de todos los controles
1.3.4.1 Políticas y procedimientos	Descripción: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
1.3.4.2 Organización de la seguridad	Descripción: Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización
1.3.4.3 Gestión de activos	Descripción: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
1.3.4.4 Gestión de comunicaciones	Descripción: Asegurar la operación correcta y segura de los servicios de procesamiento de información
1.3.4.5 Control de acceso	Descripción: Controlar el acceso a la información.
1.3.4.6 Adquisición, desarrollo y mantenimiento de SI	Descripción: garantizar que la seguridad es parte integral de los sistemas de información.
1.3.4.7 Gestión de incidentes	Descripción: Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

1.3.4.8 Gestión de la continuidad	Descripción: Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.
1.3.4.9 Cumplimiento	Descripción: Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.
1.3.5 Seguridad de las operaciones	Descripción: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
1.4 Evaluación	Descripción: Tercera fase del ciclo de vida Duración: 3 meses Criterios de aceptación: se cumplen con los requisitos exigidos en la norma
1.4.1 Plan de seguimiento MSPI	Descripción: Elaboración y seguimiento del plan
1.4.2 Plan de auditorias	Descripción: Elaboración y seguimiento del plan
1.4.3 Resultados riesgos	Descripción: Elaboración y seguimiento del plan
1.5 Mejora y cierre	Descripción: Elaboración y seguimiento del plan Duración: 2 meses
1.5.1 Consolidado auditorias	Descripción: Elaboración y seguimiento del plan
1.5.2 Cierre del proyecto	Descripción: Realizar el cierre

Fuente: Elaboración propia

Anexo K. Listado de actividades SGSI – Análisis PERT

Cod	Actividad	Predecesora	Duración Optimista	Duración Esperada	Duración Pesimista	PERT
1.1 Inicio						
A	Plan de gestión del alcance	A0	6	10	14	10,00
B	Plan de gestión del tiempo	A0	6	8	12	8,33
C	Plan de gestión del costo	A0	6	8	12	8,33
D	Autoevaluación	A,B,C	4	5	7	5,17
E	Identificación del problema	A,B,C	4	5	10	5,67
F	Encuesta	A,B,C	3	5	8	5,17
G	Estratificación	F	2	3	5	3,17
1.2 Planificación						
H	Indicadores	G	5	7	10	7,17
I	Métricas	G	5	7	10	7,17
J	Declaración de aplicabilidad	H,I	4	6	10	6,33
K	Definición de política de seguridad	G	2	3	5	3,17
L	Aprobación por la dirección	K	1	2	5	2,33
M	Procedimiento control documental	G	3	4	8	4,50
N	Roles y responsabilidades	M	3	4	7	4,33
O	Identificación de riesgos	L	4	6	10	6,33
P	Identificación de amenazas	O	3	5	7	5,00
Q	Identificación de vulnerabilidades	P	3	5	7	5,00
R	Identificación de Impactos	Q	3	5	7	5,00
S	Evaluación del impacto en el negocio	R	1	2	3	2,00
T	Evaluar la probabilidad de ocurrencia	S	1	2	3	2,00
U	Estimar los niveles de riesgo	T	1	2	3	2,00
V	Aceptación o tratamiento de riesgos	U	2	3	5	3,17
W	Aplicar controles a los riesgos	V	2	3	5	3,17
X	Evitar o transferir riesgos	W	6	7	10	7,33
Y	Organización Manuales y procedimientos	L	3	4	7	4,33
Z	Revisión de políticas y procedimientos	Y	3	5	8	5,17
AA	Divulgación	Z	5	7	10	7,17
AB	Plan de transición a IPv6	V	3	5	8	5,17
AC	Procesos disciplinarios	L	2	4	7	4,17
AD	Plan de comunicación	V	1	3	4	2,83

Cod	Actividad	Predecesora	Duración Optimista	Duración Esperada	Duración Pesimista	PERT
AE	Plan de continuidad	V	2	4	6	4,00
AF	Inventario de Formatos	L	3	4	5	4,00
AG	Inventario de Activos	L	3	4	5	4,00
AH	Inventario de Áreas	L	1	3	5	3,00
AI	Inventario de Terceros	L	1	3	5	3,00
AJ	Inventario de Proveedores	L	1	2	3	2,00
AK	Inventario de Obligaciones	L	1	3	6	3,17
AL	Formato auditorias	V	2	3	5	3,17
AM	Calendario de auditorias	V	1	1	2	1,17
AN	Arquitectura TI	X	5	7	10	7,17
AO	Equipos y suministros	X	5	8	12	8,17
AP	Diagrama de red TI detallado	X	10	12	22	13,33
1.3 Implementación						
AQ	Ejecución de estrategia de planificación y control	V	6	8	12	8,33
AR	Implementar acciones de control	AQ	6	8	10	8,00
AS	Avance Ipv6	AB	8	10	15	10,50
AT	Definición de activos habilitados	AS	2	5	6	4,67
AU	Sugerencia de cambios	AT	1	2	3	2,00
AV	Adquisiciones	AU	30	40	50	40,00
AW	Avance riegos	X	5	8	12	8,17
AX	Reevaluación de riesgos	AW	2	3	7	3,50
AY	Tratamiento de riesgos residuales	AX	2	3	5	3,17
AZ	Política y procedimientos (implementación)	AA	20	25	30	25,00
BA	Organización de la seguridad	X	10	15	20	15,00
BB	Seguridad de equipos	BA	5	7	10	7,17
BC	Seguridad de RRHH	BA	5	7	10	7,17
BD	Seguridad física	BA	3	5	8	5,17
BE	Áreas seguras	BA	4	6	10	6,33
BF	Adquisiciones	BB,BC,BD,BE	20	30	40	30,00
BG	Seguridad de redes	AH	5	6	10	6,50
BH	Seguridad de las operaciones	BG	10	12	15	12,17
BI	Gestión de activos	AX	5	7	10	7,17
BJ	Inventario de activos (actualización)	BI	4	8	12	8,00
BK	Gestión de comunicaciones	AX	2	5	8	5,00
BL	Requisitos de comunicación	BK	1	3	5	3,00
BM	Transferencia de información	BL	1	3	4	2,83






































Cod	Actividad	Predecesora	Duración Optimista	Duración Esperada	Duración Pesimista	PERT
BN	Gestión de acceso a usuarios	AX	2	3	5	3,17
BO	Responsabilidades	BN	1	2	3	2,00
BP	Control de acceso a sistemas y aplicaciones	BO	2	3	5	3,17
BQ	Implementación de sistemas	BP	3	4	7	4,33
BR	Adquisiciones	BQ	20	30	40	30,00
BS	Adquisiciones complementarias	AX	20	30	40	30,00
BT	Seguridad en los procesos de desarrollo y soporte	BS	2	5	8	5,00
BU	Datos de prueba	BT	3	4	7	4,33
BV	Mejoras	BU	2	5	8	5,00
BW	Gestión de incidentes	BV	2	5	8	5,00
BX	Procedimientos operacionales	BW	3	4	7	4,33
BY	Copias de respaldo	BX	3	4	8	4,50
BZ	Registro y seguimiento	BY	3	5	9	5,33
CA	Gestión de la continuidad	BS	3	4	5	4,00
CB	Protección contra códigos maliciosos	CA	2	5	8	5,00
CC	Cumplimiento	CB	3	4	7	4,33
CD	Controles	CC	4	5	8	5,33
CE	Control de software operacional	CD	2	3	5	3,17
CF	Gestión de la vulnerabilidad técnica	CE	3	5	8	5,17
1.4 Evaluación						
CG	Plan de seguimiento MSPI	CF	3	5	8	5,17
CH	Determinar efectividad de acciones	CG	2	5	7	4,83
CI	Detección de errores	CH	3	6	9	6,00
CJ	Identificar brechas de seguridad	CI	3	5	8	5,17
CK	Revisión del plan de auditorias	CF	5	6	8	6,17
CL	Seguimiento de resultados	CK	5	7	9	7,00
CM	Resultados riesgos	CL	2	4	5	3,83
CN	Mitigación de riesgos residuales	CM	2	3	5	3,17
1.5 Mejora y cierre						
CO	Consolidado auditorias	CL	2	3	5	3,17
CP	Identificación de oportunidades de mejora	CO	2	4	6	4,00
CQ	Cierre de adquisiciones	CP	1	3	5	3,00
CR	Cierre de proyecto	CQ	2	3	5	3,17

Fuente: Elaboración propia












































Anexo L. Cronograma en MS Project

		Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1			1. Implementacion SGSI (Inicio)	279 días	lun 30/10/17	mié 14/11/18	
2			Inicio Proyecto	0 días	lun 30/10/17	lun 30/10/17	
3			1.1 Inicio	23 días	lun 30/10/17	mar 28/11/17	
4			Plan de gestion del alcance	10 días	lun 30/10/17	vie 10/11/17	2
5			Plan de gestion del tiempo	8 días	lun 30/10/17	mié 8/11/17	2
6			Plan de gestion del costo	8 días	lun 30/10/17	mié 8/11/17	2
7			Autoevaluacion	7 días	vie 10/11/17	lun 20/11/17	4;5;6
8			Identificacion del problema	6 días	lun 20/11/17	mar 28/11/17	7
9			Encuesta	5 días	lun 20/11/17	lun 27/11/17	7
10			Estratificacion	4 días	lun 20/11/17	vie 24/11/17	7
11			Fin fase Inicio	0 días	mar 28/11/17	mar 28/11/17	8;10;9
12			1.2 Planificacion	81 días	mar 28/11/17	lun 12/03/18	11
13			Indicadores	13 días	jue 7/12/17	lun 25/12/17	11
14			Metricas	12 días	vie 15/12/17	lun 1/01/18	11
15			Declaracion de aplicabilidad	6 días	vie 26/01/18	lun 5/02/18	13;14
16			Definicion de politica de seguridad	3 días	mar 28/11/17	jue 30/11/17	11
17			Aprobacion por la direccion	2 días	jue 30/11/17	lun 4/12/17	16
18			Procedimiento control documental	6 días	lun 11/12/17	lun 18/12/17	11
19			Roles y responsabilidades	5 días	mar 26/12/17	lun 1/01/18	18
20			Identificacion de riesgos	7 días	jue 7/12/17	vie 15/12/17	17
21			Identificacion de amenazas	5 días	vie 15/12/17	vie 22/12/17	20
22			Identificacion de vulnerabilidades	5 días	mié 10/01/18	mié 17/01/18	21
23			Identificacion de Impactos	5 días	mié 17/01/18	mié 24/01/18	22
24			Evaluación del impacto en el negocio	3 días	mié 24/01/18	lun 29/01/18	23
25			Evaluar la probabilidad de ocurrencia	2 días	lun 29/01/18	mar 30/01/18	24
26			Estimar los niveles de riesgo	3 días	mar 30/01/18	vie 2/02/18	25
27			Aceptacion o tratamiento de riesgos	3 días	vie 2/02/18	mié 7/02/18	26
28			Aplicar controles a los riesgos	5 días	jue 8/02/18	mié 14/02/18	27
29			Evitar o transferir riesgos	7 días	mié 14/02/18	vie 23/02/18	28
30			Organización Manuales y procedimientos	12 días	jue 7/12/17	vie 22/12/17	17
31			Revisión de políticas y procedimientos	5 días	vie 22/12/17	jue 28/12/17	30
32			Divulgacion	10 días	jue 28/12/17	mié 10/01/18	31
33			Plan de transicion a IPv6	8 días	mié 7/02/18	vie 16/02/18	27
34			Procesos disciplinarios	5 días	lun 4/12/17	lun 11/12/17	17
35			Plan de comunicacion	4 días	mié 7/02/18	lun 12/02/18	27
36			Plan de continuidad	5 días	mié 7/02/18	mar 13/02/18	27

IMPLEMENTACION SGSI

		Modo de	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
37			Inventario de Formatos	4 días	lun 4/12/17	vie 8/12/17	17
38			Inventario de Activos	4 días	lun 4/12/17	vie 8/12/17	17
39			Inventario de Areas	3 días	lun 4/12/17	jue 7/12/17	17
40			Inventario de Terceros	3 días	lun 4/12/17	jue 7/12/17	17
41			Inventario de Proveedores	2 días	lun 4/12/17	mié 6/12/17	17
42			Inventario de Obligaciones	3 días	lun 4/12/17	jue 7/12/17	17
43			Formato auditorias	3 días	mié 7/02/18	lun 12/02/18	27
44			Calendario de auditorias	1 día	mié 7/02/18	jue 8/02/18	27
45			Arquitectura TI	10 días	vie 23/02/18	jue 8/03/18	29
46			Equipos y suministros	10 días	vie 23/02/18	jue 8/03/18	29
47			Diagrama de red TI detallado	13 días	vie 23/02/18	lun 12/03/18	29
48			Fin fase Planificacion	0 días	lun 12/03/18	lun 12/03/18	15;19;34;37;38;
49			1.3 Implementacion	97 días	mar 13/03/18	vie 13/07/18	48
50			Ejecucion de estrategia de planificacion	15 días	mar 13/03/18	vie 30/03/18	27
51			Implementar acciones de control	8 días	vie 30/03/18	mar 10/04/18	50
52			Avance Ipv6	10 días	mar 13/03/18	lun 26/03/18	33
53			Definicion de activos habilitados	8 días	lun 26/03/18	mié 4/04/18	52
54			Sugerencia de cambios	2 días	mié 4/04/18	vie 6/04/18	53
55			Adquisiciones	45 días	vie 6/04/18	lun 4/06/18	54
56			Avance riegos	8 días	mar 13/03/18	jue 22/03/18	29
57			Reevaluacion de riesgos	3 días	jue 22/03/18	lun 26/03/18	56
58			Tratamiento de riesgos residuales	3 días	mar 27/03/18	jue 29/03/18	57
59			Politica y procedimientos (implementacion)	40 días	mar 13/03/18	mié 2/05/18	32
60			Organización de la seguridad	15 días	mar 13/03/18	vie 30/03/18	29
61			Seguridad de equipos	7 días	vie 30/03/18	lun 9/04/18	60
62			Seguridad de RRHH	7 días	vie 30/03/18	lun 9/04/18	60
63			Seguridad fisica	5 días	vie 30/03/18	vie 6/04/18	60
64			Areas seguras	6 días	vie 30/03/18	lun 9/04/18	60
65			Adquisiciones	30 días	mar 10/04/18	jue 17/05/18	61;62;63;64
66			Seguridad de redes	6 días	mar 13/03/18	mar 20/03/18	39
67			Seguridad de las operaciones	12 días	mar 20/03/18	mié 4/04/18	66
68			Gestion de activos	7 días	mar 27/03/18	mié 4/04/18	57
69			Inventario de activos (actualizacion)	8 días	mié 4/04/18	vie 13/04/18	68
70			Gestion de comunicaciones	5 días	mar 27/03/18	lun 2/04/18	57
71			Requisitos de comunicacion	3 días	lun 2/04/18	jue 5/04/18	70
72			Transferencia de informacion	3 días	jue 5/04/18	lun 9/04/18	71

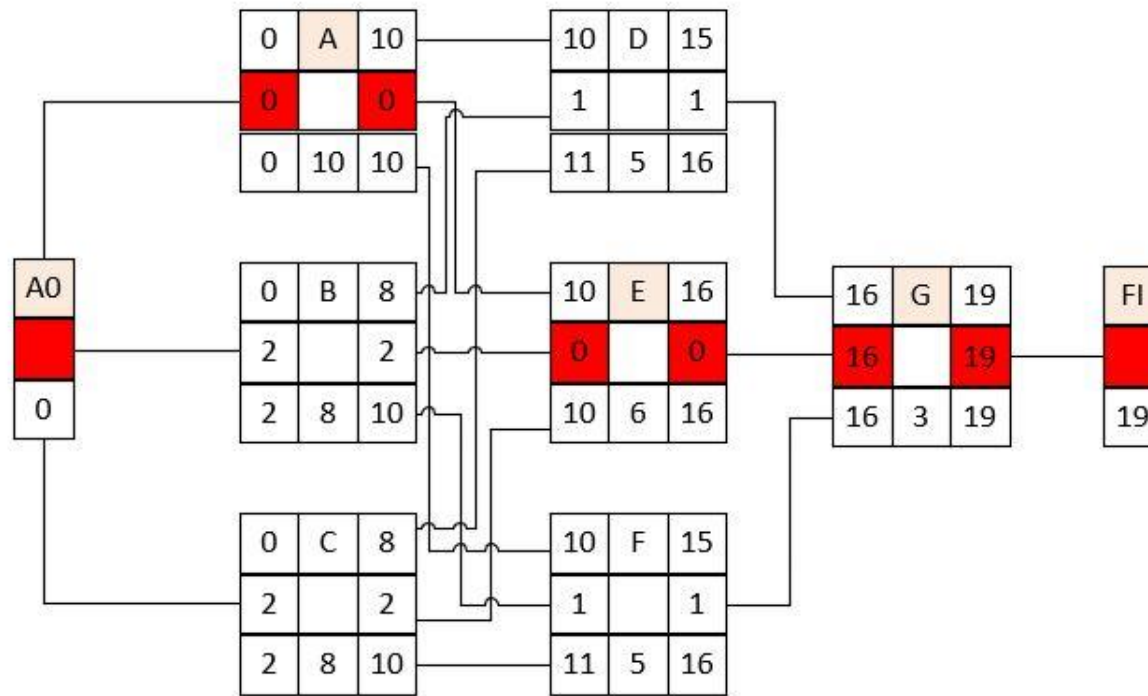
IMPLEMENTACION SGSI

		Modo de 	Nombre de tarea 	Duración 	Comienzo 	Fin 	Predecesoras 
73			Gestion de acceso a usuarios	3 días	mar 27/03/18	jue 29/03/18	57
74			Responsabilidades	2 días	jue 29/03/18	lun 2/04/18	73
75			Control de acceso a sistemas y aplicac	3 días	lun 2/04/18	jue 5/04/18	74
76			Implementacion de sistemas	12 días	jue 5/04/18	vie 20/04/18	75
77			Adquisiciones	30 días	vie 20/04/18	mar 29/05/18	76
78			Adquisiciones complementarias	30 días	mar 27/03/18	jue 3/05/18	57
79			Seguridad en los procesos de desarrol	5 días	lun 4/06/18	vie 8/06/18	78;55;65;77
80			Datos de prueba	4 días	vie 8/06/18	jue 14/06/18	79
81			Mejoras	5 días	jue 14/06/18	mié 20/06/18	80
82			Gestion de incidentes	5 días	mié 20/06/18	mié 27/06/18	81
83			Procedimientos operacionales	4 días	mié 27/06/18	lun 2/07/18	82
84			Copias de respaldo	4 días	mar 3/07/18	vie 6/07/18	83
85			Registro y seguimiento	5 días	vie 6/07/18	vie 13/07/18	84
86			Gestion de la continuidad	4 días	lun 4/06/18	jue 7/06/18	78;55;65;77
87			Proteccion contra codigos maliciosos	5 días	jue 7/06/18	jue 14/06/18	86
88			Cumplimiento	4 días	jue 14/06/18	mar 19/06/18	87
89			Controles	5 días	mar 19/06/18	mar 26/06/18	88
90			Control de software operacional	3 días	mar 26/06/18	vie 29/06/18	89
91			Gestion de la vulnerabilidad tecnica	5 días	vie 29/06/18	jue 5/07/18	90
92			Fin fase Implementacion	0 días	vie 13/07/18	vie 13/07/18	51;58;59;67;69;
93			1.4 Evaluacion	65 días	vie 13/07/18	lun 29/10/18	92
94			Plan de seguimiento MSPI	5 días	lun 23/07/18	jue 2/08/18	92
95			Determinar efectividad de acciones	5 días	mar 14/08/18	lun 20/08/18	94
96			Deteccion de errores	50 días	mar 21/08/18	mar 23/10/18	95
97			Identificar brechas de seguridad	5 días	mar 23/10/18	lun 29/10/18	96
98			Revision del plan de auditorias	6 días	vie 13/07/18	vie 20/07/18	92
99			Seguimiento de resultados	7 días	vie 20/07/18	lun 30/07/18	98
100			Resultados riesgos	4 días	mar 31/07/18	vie 3/08/18	99
101			Mitigacion de riesgos residuales	3 días	jue 9/08/18	lun 13/08/18	100
102			Fin fase Evaluacion	0 días	lun 29/10/18	lun 29/10/18	101;97
103			1.5 Mejora y cierre	13 días	mar 30/10/18	mié 14/11/18	102
104			Consolidado auditorias	3 días	mar 30/10/18	jue 1/11/18	99
105			Identificacion de oportunidades de mej	4 días	jue 1/11/18	mié 7/11/18	104
106			Cierre de adquisiciones	3 días	mié 7/11/18	lun 12/11/18	105
107			Cierre de proyecto	3 días	lun 12/11/18	mié 14/11/18	106
108			Fin Proyecto	0 días	mié 14/11/18	mié 14/11/18	107

Fuente. Elaboración propia

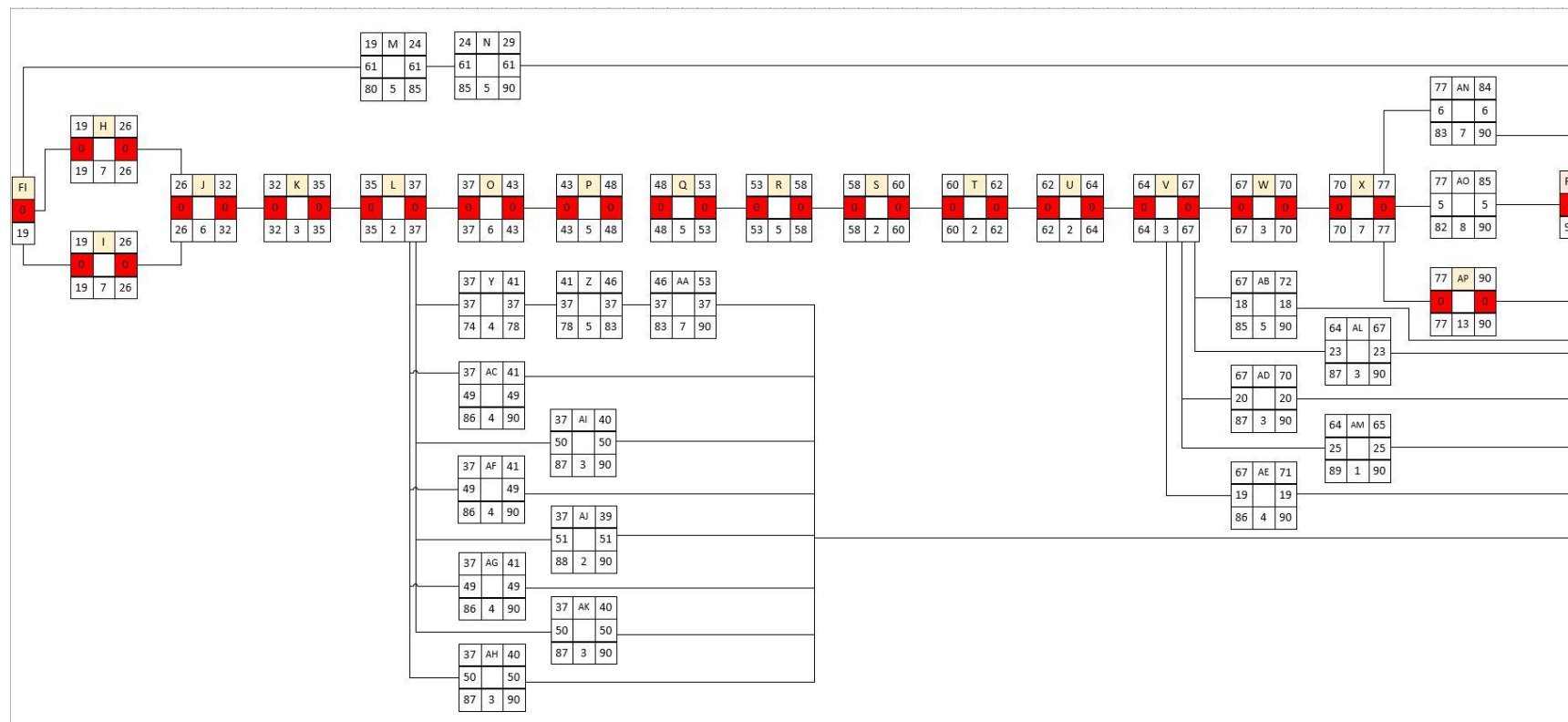
Anexo M. Diagrama de red SGSI

Fase de inicio



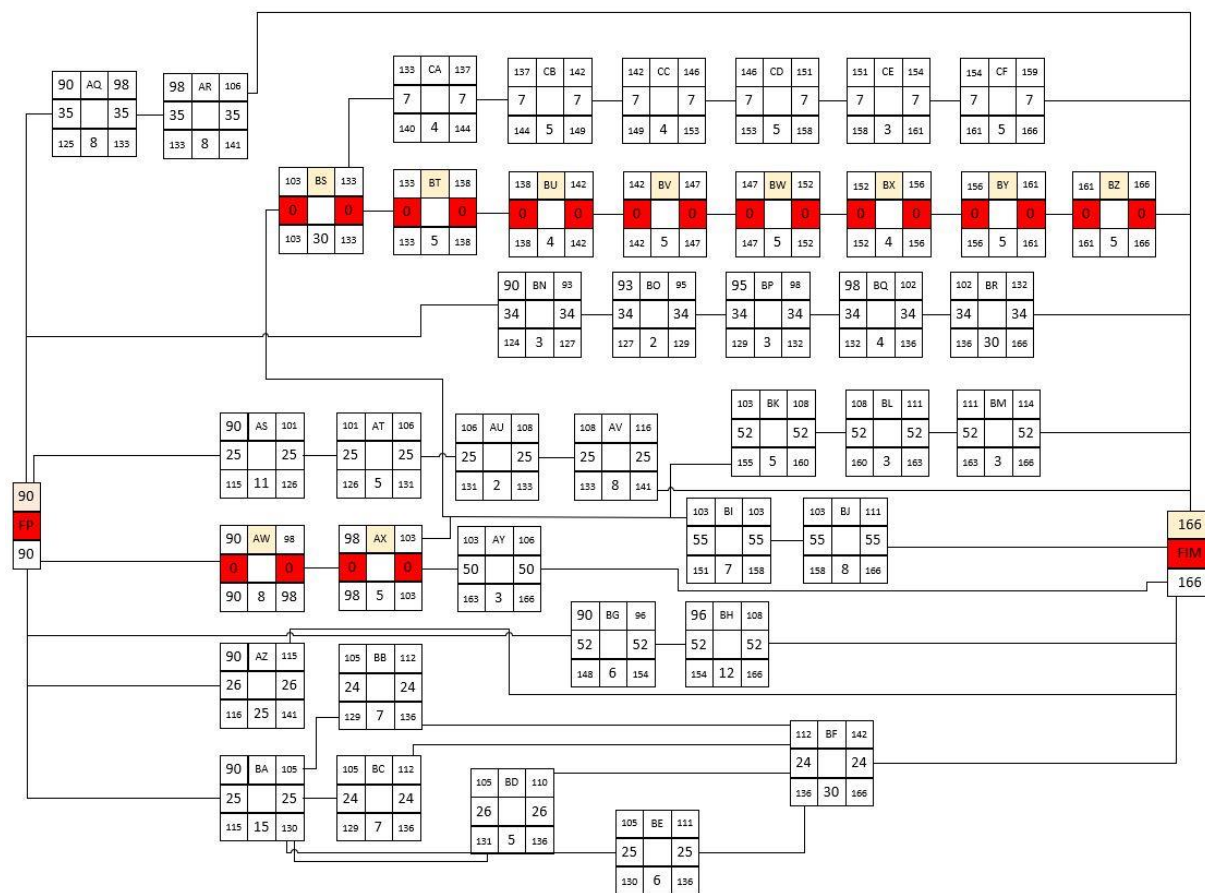
Fuente. Elaboración propia

Fase de planificación



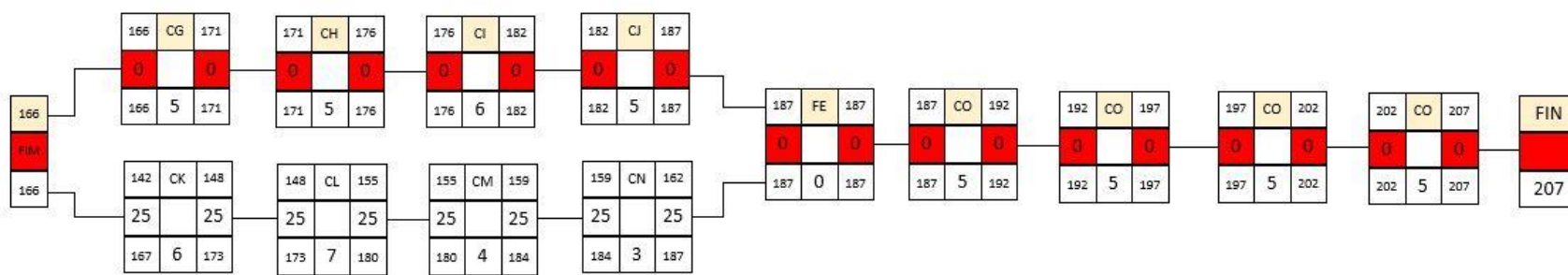
Fuente. Elaboración propia

Fase de implementación



Fuente. Elaboración propia

Fase de evaluación y cierre



Fuente. Elaboración propia

Anexo N. Presupuesto por actividades

Presupuesto estimado para las actividades de la fase de inicio.

ID	ACTIVIDAD	COSTO
A	Plan de gestión del alcance	\$ 591.000
B	Plan de gestión del tiempo	\$ 645.000
C	Plan de gestión del costo	\$ 632.000
D	Autoevaluación	\$ 864.500
E	Identificación del problema	\$ 1.707.000
F	Encuesta	\$ 766.000
G	Estratificación	\$ 250.000
TOTAL		\$ 5.455.500

Fuente. Elaboración propia

Presupuesto estimado para las actividades de la fase de planificación.

ID	ACTIVIDAD	COSTO
H	Indicadores	\$ 700.000
I	Métricas	\$ 1.000.000
J	Declaración de aplicabilidad	\$ 374.000
K	Definición de política de seguridad	\$ 232.000
L	Aprobación por la dirección	\$ 142.000
M	Procedimiento control documental	\$ 890.000
N	Roles y responsabilidades	\$ 600.000
O	Identificación de riesgos	\$ 596.000
P	Identificación de amenazas	\$ 498.000
Q	Identificación de vulnerabilidades	\$ 780.000

ID	ACTIVIDAD	COSTO
R	Identificación de Impactos	\$ 1.030.000
S	Evaluación del impacto en el negocio	\$ 1.420.000
T	Evaluar la probabilidad de ocurrencia	\$ 1.400.000
U	Estimar los niveles de riesgo	\$ 700.000
V	Aceptación o tratamiento de riesgos	\$ 928.000
W	Aplicar controles a los riesgos	\$ 392.000
X	Evitar o transferir riesgos	\$ 1.270.000
Y	Organización Manuales y procedimientos	\$ 1.493.000
Z	Revisión de políticas y procedimientos	\$ 1.564.000
AA	Divulgación	\$ 1.314.000
AB	Plan de transición a IPv6	\$ 7.268.000
AC	Procesos disciplinarios	\$ 224.000
AD	Plan de comunicación	\$ 508.000
AE	Plan de continuidad	\$ 15.358.000
AF	Inventario de Formatos	\$ 150.000
AG	Inventario de Activos	\$ 235.000
AH	Inventario de Áreas	\$ 224.000
AI	Inventario de Terceros	\$ 198.000
AJ	Inventario de Proveedores	\$ 184.000
AK	Inventario de Obligaciones	\$ 304.000
AL	Formato auditorias	\$ 324.000
AM	Calendario de auditorias	\$ 229.000
AN	Arquitectura TI	\$ 1.864.000
AO	Equipos y suministros	\$ 27.784.000
AP	Diagrama de red TI detallado	\$ 2.466.000
TOTAL		\$ 74.643.000

Fuente. Elaboración propia

Presupuesto estimado para las actividades de la fase de implementación.

ID	ACTIVIDAD	COSTO
AQ	Ejecución de estrategia de planificación y control	\$ 734.000
AR	Implementar acciones de control	\$ 340.000
AS	Avance Ipv6	\$ 668.000
AT	Definición de activos habilitados	\$ 388.000
AU	Sugerencia de cambios	\$ 158.000
AV	Adquisiciones	\$ 3.358.000
AW	Avance riegos	\$ 598.000
AX	Reevaluación de riesgos	\$ 1.062.000
AY	Tratamiento de riesgos residuales	\$ 594.000
AZ	Política y procedimientos (implementación)	\$ 2.945.000
BA	Organización de la seguridad	\$ 4.018.000
BB	Seguridad de equipos	\$ 1.250.000
BC	Seguridad de RRHH	\$ 942.000
BD	Seguridad física	\$ 532.000
BE	Áreas seguras	\$ 7.154.000
BF	Adquisiciones	\$ 26.756.000
BG	Seguridad de redes	\$ 7.622.000
BH	Seguridad de las operaciones	\$ 10.238.000
BI	Gestión de activos	\$ 167.000
BJ	Inventario de activos (actualización)	\$ 152.000
BK	Gestión de comunicaciones	\$ 418.000
BL	Requisitos de comunicación	\$ 456.000
BM	Transferencia de información	\$ 5.797.000
BN	Gestión de acceso a usuarios	\$ 2.388.000
BO	Responsabilidades	\$ 64.000
BP	Control de acceso a sistemas y aplicaciones	\$ 4.056.000
BQ	Implementación de sistemas	\$ 4.888.000
BR	Adquisiciones	\$ 2.022.000

ID	ACTIVIDAD	COSTO
BS	Adquisiciones complementarias	\$ 2.858.000
BT	Seguridad en los procesos de desarrollo y soporte	\$ 1.112.000
BU	Datos de prueba	\$ 1.392.000
BV	Mejoras	\$ 496.000
BW	Gestión de incidentes	\$ 972.000
BX	Procedimientos operacionales	\$ 2.070.000
BY	Copias de respaldo	\$ 1.332.000
BZ	Registro y seguimiento	\$ 280.000
CA	Gestión de la continuidad	\$ 1.192.000
CB	Protección contra códigos maliciosos	\$ 2.062.000
CC	Cumplimiento	\$ 312.000
CD	Controles	\$ 344.000
CE	Control de software operacional	\$ 761.000
CF	Gestión de la vulnerabilidad técnica	\$ 1.208.000
TOTAL		\$ 106.156.000

Fuente. Elaboración propia

Presupuesto estimado para las actividades de la fase de evaluación.

ID	ACTIVIDAD	COSTO
CG	Plan de seguimiento MSPI	\$ 1.920.000
CH	Determinar efectividad de acciones	\$ 1.502.000
CI	Detección de errores	\$ 3.328.000
CJ	Identificar brechas de seguridad	\$ 840.000
CK	Revisión del plan de auditorias	\$ 1.048.000
CL	Seguimiento de resultados	\$ 2.046.000
CM	Resultados riesgos	\$ 1.686.000
CN	Mitigación de riesgos residuales	\$ 1.716.000
TOTAL		\$ 14.086.000

Fuente. Elaboración propia

Presupuesto estimado para las actividades de la fase de mejora y cierre

ID	ACTIVIDAD	COSTO
CO	Consolidado auditorias	\$ 2.100.000
CP	Identificación de oportunidades de mejora	\$ 3.712.000
CQ	Cierre de adquisiciones	\$ 2.820.000
CR	Cierre de proyecto	\$ 1.736.000
TOTAL		\$ 10.368.000

Fuente. Elaboración propia

Anexo O. Indicadores de medición de desempeño.

Indicador	Formula	Descripción
PV	NA	Valor Planeado. Es el costo estimado a lo largo del proyecto. Cuando se grafica este costo en un gráfico, se observa la Curva S.
AC	NA	Costo Real. Es el costo acumulado a la fecha. Este costo se determina sumando los usos de recursos a la fecha (materiales, mano de obra, equipos y vehículos, alquileres de oficina, etc.).
EV	$BAC * \%avance$	Valor Ganado. Es la expresión del avance del proyecto, a costos del presupuesto
CV	$EV - AC$	Cost Variance. Es una medida de la diferencia entre el Valor Ganado y el Costo Real. Si el CV es igual a 0, los entregables están costándonos lo que esperábamos que cuesten. Si el CV es menor a 0, los entregables están costándonos más de lo que esperábamos. Si el CV es mayor a 0, los entregables están costando menos que lo que pensábamos.
SV	$EV - PV$	Schedule Variance. Es una medida que expresa la diferencia entre el Valor Ganado y el Valor Planeado. Si el SV es = 0, el ritmo del proyecto es el ritmo previsto en el presupuesto. Si el SV es mayor a 0, el ritmo del proyecto es más rápido que lo presupuestado. Si el SV es menor a 0, el ritmo del proyecto es más lento que lo presupuestado.
CPI	EV / AC	Cost Performance Index. Es un índice que expresa la "eficiencia" en los costos reales del proyecto, comparando el Valor Ganado (costo presupuestado para el trabajo realizado), versus el Costo Real. Si el Valor Ganado es igual al Costo Real, diríamos que el trabajo ha costado lo previsto, y el CPI sería igual a 1. Si el Valor Ganado fuese menor al Costo Real, querría decir que el trabajo realizado (Valor Ganado) ha costado más que lo previsto, en cuyo caso el CPI sería menor a 1. Un CPI menor a 1 indica un desempeño peor al previsto, UnCPI mayor a 1 indica un desempeño mejor al previsto.

Indicador	Formula	Descripción
SPI	EV / PV	<p>Schedule Performance Index. Es un índice que compara el EV (Valor Ganado), es decir lo avanzado, contra el PV (Valor Planeado) lo que se tenía pensado avanzar a un momento dado.</p> <p>Si el SPI es igual a 1, quiere decir que el entregable se está avanzando al ritmo previsto durante el presupuesto.</p> <p>Si el SPI es mayor a 1, quiere decir que el entregable se está avanzando a un ritmo mayor al previsto en el presupuesto.</p> <p>Si el SPI es menor a 1, quiere decir que se está avanzando a un ritmo peor que el previsto</p>
BAC	NA	BAC - Budget at Completion. Es el presupuesto original del proyecto (o del entregable a analizar). Se define sumando los costos de cada una de las actividades.
EAC	$\frac{BAC / CPI}{AC + ETC}$ $\frac{AC+BAC-EV}{AC + (BAC-EV)/CPI}$	Estimate at Completion. Es el estimado del costo total del proyecto, a medida que avanza el tiempo. Se calcula, sumando el costo acumulado del proyecto (a la fecha), con el Estimate to Complete
ETC	EAC - AC	ETC - Estimate to Complete. Este estimado generalmente se calcula usando el desempeño acumulado, es decir usando el CPI para corregir el monto del saldo del trabajo por realizar. Hay cuatro formas de definir el ETC:
VAC	BAC - EAC	Variance at completion. Cuanto más o menos del presupuesto estaremos al final del proyecto
TCPI	$TCPI = \frac{(BAC - EV)}{(BAC - AC)}$	Índice de desempeño del trabajo por completar. > 1 mayor esfuerzo. < 1 menor esfuerzo
Entregas	Numero de entregas oportunas / Total de entregas	Identifica el nivel de efectividad del grupo del proyecto en la entrega de productos que afecta la recepción oportuna de entregables y el cronograma del proyecto
Satisfacción del cliente	Número de reclamaciones / número de usuarios	Permite medir la satisfacción del cliente y demuestra la calidad del producto y/o servicio. Impacta en el presupuesto
Cobertura	N.º de equipos habilitados / número de equipos inventariados	Consiste en medir el número de terminales inventariados y actualizados, que están habilitados para el SGSI

Fuente: Elaboración propia

Anexo P. Especificaciones técnicas de requerimientos

INDICADOR	DESCRIPCIÓN	FÓRMULA	IMPACTO	ESTÁNDAR DE CUMPLIMIENTO	ACCIÓN DE MEJORA
Entregas	Consiste en calcular el nivel de efectividad en las fechas de entregas de los entregables en SGSI	Numero de entregas oportunas X 100 Total de entregas	Identifica el nivel de efectividad del grupo de proyecto en la entrega de productos que afecta la recepción oportuna de entregables y que afecta el cronograma del proyecto	90%	1. Mejorar los tiempos de entrega. 2. Se debe diseñar un plan de acción para evitar entregas no oportunas.
TIEMPO	Medición entre lo programado y lo ejecutado.	<u>Ejecutado</u> Programado	Evaluar la ejecución de lo planeado porque nos impactaría en el cumplimiento del cronograma.	10%	1. Definir un plan de acción para mejorar los tiempos en la ejecución de las actividades.

INDICADOR	DESCRIPCIÓN	FÓRMULA	IMPACTO	ESTÁNDAR DE CUMPLIMIENTO	ACCIÓN DE MEJORA
FINANCIERO	Hacer una medición de lo presupuestado y lo real invertido.	$\frac{\text{Inversión}}{\text{Presupuesto}}$	Se debe verificar lo invertido en comparación con el presupuesto que se tiene, puede afectar el proyecto en el cumplimiento del alcance.	5%	1. Implementar un plan de acción para cumplir con los costos presupuestados en las actividades.
SATISFACCIÓN DEL CLIENTE	Consiste en medir el número de reclamaciones efectuadas por el cliente durante la fase de operación en el periodo de garantía.	$\frac{\text{Número de reclamaciones}}{\text{Número de usuarios}}$ = 5 200	Permite medir la satisfacción del cliente y demuestra la calidad del producto y/o servicio, impacta en el presupuesto	4%	1. Tomar un plan de acción que permita disminuir las reclamaciones de los usuarios.

INDICADOR	DESCRIPCIÓN	FÓRMULA	IMPACTO	ESTÁNDAR DE CUMPLIMIENTO	ACCIÓN DE MEJORA
	Se sugiere realizarlo mensualmente.				
Cobertura	Consiste en medir el número de terminales inventariados y actualizados, que están habilitados para el SGSI	$\frac{\text{N° Equipos habilitados}}{\text{N° de equipos inventariados}}$	Identifica el nivel de cobertura del SGSI en todos los terminales de la entidad	90%	1. Seguir el cronograma y el alcance del proyecto para garantizar cubrimiento a todas las terminales de la entidad

Fuente. Elaboración propia

Anexo Q. Auditoria SGSI

ITEM	CONCEPTO	RESULTADO
	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
	Solicite la política de seguridad de la información de la entidad y evalúe:	
	a) Si se definen los objetivos, alcance de la política	
	b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad	
	c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección	
	Revise si la política:	
1	a) Define que es seguridad de la información	
	b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos;	
	c) Los procesos para manejar las desviaciones y las excepciones.	
	Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas.	
	Verifique cada cuanto o bajo qué circunstancias se revisan y actualizan, verifique la última fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual.	
	RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN	

ITEM	CONCEPTO	RESULTADO
	<p>verifique si 1) los roles y responsabilidades frente a la ciberseguridad han sido establecidos 2) los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas 3) Los a) proveedores, b) clientes, c) socios, d) funcionarios, e) usuarios privilegiados, f) directores y gerentes (mandos senior), g) personal de seguridad física, h) personal de seguridad de la información entienden sus roles y responsabilidades, i) Están claros los roles y responsabilidades para la detección de incidentes</p> <p>Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección.</p> <p>Revise la estructura del SGSI:</p>	
2	<p>1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes.</p> <p>2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?</p> <p>3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección)</p> <p>4) Están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales?</p> <p>5) Están definidos y documentados los niveles de autorización?</p> <p>6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo, campañas de sensibilización en seguridad de la información)</p>	

ITEM	CONCEPTO	RESULTADO
3	<p>Indague como evitan que una persona pueda acceder, modificar o usar activos sin autorización ni detección. La mejor práctica dicta que el inicio de un evento deber estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación.</p> <p>Tenga en cuenta que para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, en estos casos se deben considerar controles compensatorios como revisión periódica de, los rastros de auditoría y la supervisión de cargos superiores.</p>	
4	Pregunte sobre las membrecías en grupos o foros de interés especial en seguridad de la información en los que se encuentran inscritos las personas responsables de la SI.	
SEGURIDAD DE LOS RECURSOS HUMANOS		
	Revise el proceso de selección de los funcionarios y contratistas, verifique que se lleva a cabo una revisión de:	
	a) Referencias satisfactorias	
	b) Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales;	
	c) Confirmación de las calificaciones académicas y profesionales declaradas;	
	d) Una verificación más detallada, como la de la información crediticia o de antecedentes penales.	
5	<p>e) sea confiable para desempeñar el rol, especialmente si es crítico para la organización.</p> <p>f) Cuando un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, por ejemplo, información financiera o información muy confidencial, la organización debería también considerar verificaciones adicionales más detalladas (por ejemplo, estudio de seguridad, polígrafo, visita domiciliaria)</p> <p>g) También se debería asegurar un proceso de selección para contratistas. En estos casos, el acuerdo entre la organización y el contratista debería especificar las responsabilidades por la realización de la selección, y los procedimientos de notificación que es necesario seguir si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud.</p>	

ITEM	CONCEPTO	RESULTADO
6	<p>los contratistas deben estar coordinados y alineados con los roles y responsabilidades de seguridad de la información.</p> <p>Indague y solicite evidencia del como la dirección se asegura de que los empleados y contratistas:</p> <p>a) Estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales.</p> <p>b) Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad.</p> <p>c) Logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización y estén motivados para cumplir con las políticas.</p> <p>d) Tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular.</p> <p>e) Cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información (“denuncias internas”).</p>	
7	<p>Entreviste a los líderes de los procesos y pregúnteles que saben sobre la seguridad de la información, cuáles son sus responsabilidades y como aplican la seguridad de la información en su diario trabajo.</p> <p>Pregunte como se asegura que los funcionarios, Directores, Gerentes y contratistas tomen conciencia en seguridad de la información, alineado con las responsabilidades, políticas y procedimientos existentes en la Entidad.</p> <p>Solicite el documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección. Verifique que se han tenido en cuenta buenas prácticas como:</p> <p>a) Desarrollar campañas, elaborar folletos y boletines.</p> <p>b) Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, están aprobados y documentados, por la alta Dirección</p> <p>c) Verifique que nuevos empleados y contratistas son objeto de sensibilización en SI.</p> <p>d) Indague cada cuanto o con qué criterios se actualizan los programas de toma de conciencia.</p>	

ITEM	CONCEPTO	RESULTADO
	<p>e) Verifique que en las evidencias se puede establecer los asistentes al programa y el tema impartido.</p> <p>f) Incluir en los temas de toma de conciencia los procedimientos básicos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios).</p> <p>g) De acuerdo a NIST verifique que los funcionarios con roles privilegiados entienden sus responsabilidades y roles.</p>	
8	Pregunte cual es el proceso disciplinario que se sigue cuando se verifica que ha ocurrido una violación a la seguridad de la información, quien y como se determina la sanción al infractor	
9	Revisar los acuerdos de confidencialidad, verificando que deben acordar que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo.	
GESTIÓN DE ACTIVOS		
	<p>Solicite el inventario de activos de información, revisado y aprobado por la alta Dirección y revise:</p> <p>1) Ultima vez que se actualizó</p> <p>2) Que señale bajo algún criterio la importancia del activo</p> <p>3) Que señale el propietario del activo</p>	
10	<p>Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de activos y cada cuanto se realiza esta revisión.</p> <p>De acuerdo con NIST se deben considerar como activos el personal, dispositivos, sistemas e instalaciones físicas que permiten a la entidad cumplir con su misión y objetivos, dada su importancia y riesgos estratégicos.</p>	

ITEM	CONCEPTO	RESULTADO
11	<p>Solicite el procedimiento para asegurar la asignación oportuna de la propiedad de los activos. Tenga en cuenta que la propiedad se debería asignar cuando los activos se crean o cuando son entregados a la Entidad. De acuerdo con las mejores prácticas el propietario de los activos (individuo o entidad, que es responsable por el activo) tiene las siguientes responsabilidades:</p> <p>a) asegurarse de que los activos están inventariados;</p> <p>b) asegurarse de que los activos están clasificados y protegidos apropiadamente;</p> <p>c) definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables;</p> <p>d) asegurarse del manejo apropiado del activo cuando es eliminado o destruido.</p>	
12	<p>Solicite el procedimiento mediante el cual se clasifican los activos de información y evalúe:</p> <p>1) Que las convenciones y criterios de clasificación sean claros y estén documentados</p> <p>2) Que se defina cada cuanto debe revisarse la clasificación de un activo</p> <p>3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad. Solicite muestras de inventarios de activos de información clasificados y evalúe que se aplican las políticas y procedimientos de clasificación definidos. Evalúe si los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.</p>	
13	<p>Solicite el procedimiento para el etiquetado de la información y evalúe:</p> <p>1) Aplica a activos en formatos físicos y electrónicos (etiquetas físicas, metadatos)</p> <p>2) Que refleje el esquema de clasificación establecido</p> <p>3) Que las etiquetas se puedan reconocer fácilmente</p>	

ITEM	CONCEPTO	RESULTADO
	4) Que los empleados y contratistas conocen el procedimiento de etiquetado	
	Revise en una muestra de activos el correcto etiquetado	
14	<p>Solicite las directrices, guías, lineamientos y procedimientos para la gestión de medios removibles, que consideren:</p> <p>a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable;</p> <p>b) cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría;</p> <p>d) si la confidencialidad o integridad de los datos se consideran importantes, se deben usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles;</p> <p>f) se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos;</p> <p>h) sólo se deben habilitar unidades de medios removibles si hay una razón de valida asociada a los procesos la Entidad para hacerlo;</p> <p>i) En donde hay necesidad de usar medios removibles, se debería hacer seguimiento a la transferencia de información a estos medios (Por ejemplo, DLP)</p>	
15	<p>Solicite los procedimientos existentes para garantizar que los medios a desechar o donar, no contienen información confidencial que pueda ser consultada y copiada por personas no autorizadas.</p> <p>Verifique si se ha realizado esta actividad y si existen registros de esta.</p>	
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		

ITEM	CONCEPTO	RESULTADO
	<p>Verifique si la entidad cuenta con</p> <p>a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias.</p> <p>b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.</p>	
16	<p>c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección.</p> <p>Revise si los controles de seguridad de la información que se han implementado continúan operando durante un evento contingente. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se la Entidad debe establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.</p>	
	<p>Indague y solicite evidencias de la realización de pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información;</p>	
17	<p>Tenga en cuenta que la verificación de los controles de continuidad de la seguridad de la información es diferente de las pruebas y verificación generales de seguridad de la información. Si es posible, es preferible integrar la verificación de los controles de continuidad de negocio de seguridad de la información con las pruebas de recuperación de desastres y de continuidad de negocio de la organización.</p>	
	<p>Verifique si la Entidad cuenta con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo.</p>	
18	<p>Indague como se han definido las necesidades de los procesos para seleccionar que elementos deben ser redundantes.</p>	

ITEM	CONCEPTO	RESULTADO
	Solicite si aplica las pruebas aplicadas para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.	
CUMPLIMIENTO		
19	Solicite la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Normograma). Indague si existe un responsable de identificarlos y se definen los responsables para su cumplimiento.	
20	Revise si la Entidad cuenta con tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.	
21	1) Verifique si los gerentes aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad. 2) Verifique la revisión periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas. 3) Verifique si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información	
22	Verifique si se realizan evaluaciones de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas. Solicite evidencia de las últimas pruebas realizadas, sus resultados y seguimiento para asegurar que las brechas de seguridad fueron solucionadas.	

Fuente: Edición propia basado en controles de la norma ISO 27002

Anexo R. Lista de verificación de entregables

Entregables a auditar			
Finales	Parciales	Fecha	Persona que Aprueba
Diagnostico	Autoevaluación		
	Encuesta		
	Estratificación		
Políticas y procedimientos	Manual de políticas de seguridad de la información		
	Procedimientos de seguridad de la información		
Planes	Plan de transición a IPv6		
	Plan de continuidad del negocio		
	Plan de auditorías		
	Plan de gestión de riesgos		
Inventarios	Inventario de activos de información		
	Inventario de áreas		
	Interesados		
	Proveedores		
Avances	Avance Plan IPv6		
	Avance Plan de auditorías		
	Avance plan de gestión de riesgos		
	Avance plan de continuidad		
Criterios de aceptación			
Debe ser una demostración clara de que el proyecto cumple a cabalidad con los objetivos de acuerdo con la fase entregada.			
El porcentaje de cumplimiento debe llegar a un 80% en cada fase del entregable.			
Todos los entregables deben ser aprobados por la oficina de planeación y sistemas de información			

Fuente. Elaboración propia

Anexo S. Matriz RACI

Actividad	Personal					
	Gerente de Proyecto	Ingeniero Líder	Ingeniero Asistente	Técnico	Asesor TI	Asesor GP
1.1 Diagnostico						
Autoevaluación	A	R	R	I	C	C
Encuesta	A	I	R	R	C	C
Estratificación	A	C	R	I	C	C
1.2 Planificación						
Indicadores y métricas	A	R	R	C	I	C
Declaración de aplicabilidad	A	R	R	I	C	C
Procedimiento control documental	A	C	R	R	I	C
Roles y responsabilidades	A	C	C	R	I	I
Manuales y procedimientos	A	C	R	R	I	I
Objetivo, alcance, limites MSPI	A	C	R	I	C	C
Identificación de riesgos	A	R	C	I	C	C
Plan de tratamiento de riesgos	A	R	C	I	C	C
Planes	R	C	C	I	C	C

Actividad	Personal					
	Gerente de Proyecto	Ingeniero Líder	Ingeniero Asistente	Técnico	Asesor TI	Asesor GP
Plan de transición IPv4 IPv6	I	A	C	I	R	C
Plan de comunicación	R	A	R	I	C	C
Plan de continuidad	A	R	C	I	C	C
Inventarios	A	C	C	R	I	I
Arquitectura de red	I	A	C	C	R	C
1.3 Implementación						
Estrategia de planificación y control	A	R	C	I	C	C
Avance IPv4 IPv6	I	A	C	I	R	C
Avance riesgos	I	A	R	I	C	C
Indicadores de gestión	C	A	C	R	C	C
Políticas y procedimientos	A	R	C	C	C	C
Organización de la seguridad	I	A	R	C	C	C
Gestión de activos	A	R	C	C	C	C
Seguridad de RH	A	C	R	I	C	C
Seguridad física	A	C	C	R	I	I
Gestión de comunicaciones	A	R	C	I	C	I

Actividad	Personal					
	Gerente de Proyecto	Ingeniero Líder	Ingeniero Asistente	Técnico	Asesor TI	Asesor GP
Control de acceso a sistemas	I	A	R	I	R	I
Adquisición, desarrollo y mantenimiento de SI	R	C	C	I	A	C
Gestión de incidentes	A	R	C	I	C	C
Gestión de la continuidad	C	A	R	I	C	C
Cumplimiento	A		R	C	I	C
Controles	I	R	C	I	A	I
Criptografía	I	A	R	I	C	I
Seguridad de las operaciones	R	C	C	I	A	C
1.4 Evaluación						
Plan de seguimiento MSPI	R	A	C	I	C	C
Plan de auditorías	R	A	C	I	C	C
Resultados riesgos	R	A	C	I	C	C
1.5 Mejora						
Consolidado auditorías	R	A	C	I	C	C

Fuente. Elaboración propia

Anexo T. Matriz de gestión de riesgos del proyecto

GESTION DEL RIESGO

Nombre del proyecto: Implementacion SGSI
 Director del proyecto:

IDENTIFICACION DE RIESGOS						ANALISIS CUALITATIVO			ANALISIS CUANTITATIVO			PLAN DE RESPUESTA					
ITEM	CAUSA	RIESGO IDENTIFICADO	CONSECUENCIA	CATEGORIA	RESPONSABLE	PROBABILIDAD	IMPACTO	TIPO DE RIESGO	VALOR RIESGO	VME	ESTRATEGIA	PLAN DE RESPUESTA	PROBABILIDAD FINAL	IMPACTO FINAL	NUEVO TIPO DE RIESGO	INVERSION DE LA ESTRATEGIA	NUEVO VME
1	Presupuesto limitado	Falta de personal autorizado para realizar las actividades	Retrasos en las actividades	OPERATIVO	Coordinador TIC	0,7	4	EXTREMO	\$ 20.000.000	\$ 14.000.000	Evitar - Transferir	Disponer de un servicio externo de mantenimiento equipos.	0,1	2	BAJO	\$ 1.000.000	\$ 2.000.000
2	Escases de proveedores	No disponibilidad del servicio de mantenimiento a equipos	Fallas en equipos criticos	TECNOLOGICO	Gerente del proyecto	0,7	4	EXTREMO	\$ 7.000.000	\$ 4.900.000	Evitar	Contar con recursos de sostenimiento.	0,3	2	BAJO	\$ 4.000.000	\$ 2.100.000
3	Falla en servidores	Interrupcion en la continuidad del negocio	Imagen negativa de la empresa	CREDIBILIDAD	Coordinador TIC	0,5	4	EXTREMO	\$ 25.000.000	\$ 12.500.000	Evitar	Implementación de Firewall y consola de antivirus	0,3	1	BAJO	\$ -	\$ 7.500.000
4	Asignacion inadecuada de permisos	Imposibilidad para la prestación de algunos servicios	Cientes Insatisfechos	OPERATIVO	Jefe de mantenimiento de activos	0,3	5	EXTREMO	\$ 3.000.000	\$ 900.000	Evitar	Instalar sistema de UPS	0,1	1	BAJO	\$ -	\$ 300.000
5	Accesos no controlados a las bases de datos	Afectacion de la integridad de los datos	Errores en los procesos	TECNOLOGICO	Coordinador TIC	0,9	2	ALTO	\$ 12.000.000	\$ 10.800.000	Mitigar	Contratar equipo de soporte de software.	0,3	1	BAJO	\$ -	\$ 3.600.000
6	Falta de espacio de almacenamiento	No disponibilidad de informacion de respaldo	Perdida de informacion	FINANCIERO	Equipo de trabajo	0,5	3	ALTO	\$ 30.000.000	\$ 15.000.000	Transferir	Contratar y autorizar al personal que realizará las actividades	0,1	1	BAJO	\$ -	\$ 3.000.000
7	Inestabilidad de los sistemas	Funcionamiento inadecuado de aplicaciones de software	Errores en los procesos	LEGAL	Gerente del proyecto	0,1	5	ALTO	\$ 10.000.000	\$ 1.000.000	Mitigar	Contar con recursos de sostenimiento.	0,1	5	ALTO	\$ -	\$ 1.000.000
8	Planes de mantenimiento inexistentes	No disponibilidad del servidor o equipos de computo	No prestacion de servicios	TECNOLOGICO	Equipo de trabajo	0,3	3	MEDIO	\$ 28.000.000	\$ 8.400.000	Mitigar	Utilización de sistemas NAS y Cloud	0,1	1	BAJO	\$ -	\$ 2.800.000
9	Fluctuaciones en la red electrica	Falta de suministro de energia	Demoras en los servicios	OPERATIVO	Gerente del proyecto.	0,1	3	MEDIO	\$ 2.000.000	\$ 200.000	Mitigar	Contratar soporte técnico de nuevas tecnologías.	0,1	1	BAJO	\$ 1.500.000	\$ 200.000
10	Calor excesivo	Falla de enlaces de comunicación	Sedes sin acceso a la red	LEGAL	Gerente del proyecto.	0,3	2	BAJO	\$ 7.000.000	\$ 2.100.000	Aceptar	Capacitar al personal en el uso de las nuevas tecnologías.	0,1	1	BAJO	\$ 300.000	\$ 700.000

Fuente. Elaboración propia

Anexo U. Plan de respuesta a los riesgos

RIESGO	ESTRATEGIA	PLAN DE RESPUESTA	ACTIVADOR	RESPONSABLE
No disponibilidad del servicio de mantenimiento a equipos	Evitar - Transferir	Disponer de un servicio externo equipo de mantenimiento	Informes de gestión operacional.	Coordinador TIC
Indisponibilidad del servidor o equipos de computo	Evitar	Contar con recursos de sostenimiento	Informes de la dirección de proyecto.	Gerente del proyecto
Afectación de la integridad de los datos	Evitar	Implementación de Firewall y consola de antivirus	Informes de gestión operacional.	Coordinador TIC
Falta de suministro de energía	Evitar	Instalar sistema de UPS	Informes de gestión operacional.	Jefe de mantenimiento de activos
Funcionamiento inadecuado de aplicaciones de software	Mitigar	Contratar equipo de soporte de software.	Informes de gestión operacional.	Coordinador TIC
Falta de personal autorizado para realizar las actividades	Transferir	Contratar y autorizar al personal que realizará las actividades	Informes de la dirección de proyecto.	Equipo de trabajo
Interrupción en la continuidad del negocio	Mitigar	Contar con recursos de sostenimiento.	Informes de la dirección de proyecto.	Gerente del proyecto
No disponibilidad de información de respaldo	Mitigar	Utilización de sistemas NAS y Cloud	Informes de la dirección de proyecto.	Equipo de trabajo

RIESGO	ESTRATEGIA	PLAN DE RESPUESTA	ACTIVADOR	RESPONSABLE
Falla de enlaces de comunicación	Mitigar	Contratar soporte técnico de nuevas tecnologías.	Informes de la dirección de proyecto.	Gerente del proyecto.
Diseño inadecuado para la prestación de algunos servicios	Aceptar	Capacitar al personal en el uso de las nuevas tecnologías.	Informes de la dirección de proyecto.	Coordinador TIC

Fuente. Elaboración propia

Anexo V. Matriz de revaluacion de riesgos

ITEM	RIESGO	ESTRATEGIA	PLAN DE RESPUESTA	PROBABILIDAD FINAL	IMPACTO FINAL	NUEVO TIPO DE RIESGO
1	No disponibilidad del servicio de mantenimiento a equipos	Evitar - Transferir	Disponer de un servicio externo de mantenimiento equipos.	0,1	2	BAJO
2	Indisponibilidad del servidor o equipos de computo	Evitar	Contar con recursos de sostenimiento.	0,3	2	BAJO
3	Afectación de la integridad de los datos	Evitar	Implementación de Firewall y consola de antivirus	0,3	1	BAJO
4	Falta de suministro de energía	Evitar	Instalar sistema de UPS	0,1	1	BAJO
5	Funcionamiento inadecuado de aplicaciones de software	Mitigar	Contratar equipo de soporte de software.	0,3	1	BAJO
6	Falta de personal autorizado para realizar las actividades	Transferir	Contratar y autorizar al personal que realizará las actividades	0,1	1	BAJO
7	Interrupción en la continuidad del negocio	Mitigar	Contar con recursos de sostenimiento.	0,1	5	ALTO

ITEM	RIESGO	ESTRATEGIA	PLAN DE RESPUESTA	PROBABILIDAD FINAL	IMPACTO FINAL	NEVOTIPO DE RIESGO
8	No disponibilidad de información de respaldo	Mitigar	Utilización de sistemas NAS y Cloud	0,1	1	BAJO
9	Falla de enlaces de comunicación	Mitigar	Contratar soporte técnico de nuevas tecnologías.	0,1	1	BAJO
10	Diseño inadecuado para la prestación de algunos servicios	Aceptar	Capacitar al personal en el uso de nuevas tecnologías.	0,1	1	BAJO

Fuente. Elaboración propia

Anexo W. Formato de resolución de conflictos y gestión de expectativas

COMITÉ DE RESOLUCION DE CONFLICTOS		
Proyecto: _____	Fecha: _____	Consec: _____
INTERESADOS EN CONFLICTO:		
NOMBRE	DEPENDENCIA	GRUPO DE INTERESADO
SITUACION DE CONFLICTO:		
ESTRATEGIAS DE SOLUCION		
_____	_____	
Director de proyecto	Interesado	
_____	_____	
Interesado	Interesado	

Fuente. Elaboración propia