UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO
ESCUELA DE POSGRADO

IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA APOYAR EL PROCESO DE ATENCIÓN AL PACIENTE EN INSTITUCIONES DE SALUD

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR
LUCERO GIOVANNA NIQUEN MEDIANERO

ASESOR
Mgtr. **GREGORIO MANUEL LEÓN TENORIO**
https://orcid.org/0000-0002-9650-4427

Chiclayo, 2019

ÍNDICE

RESUMEN....10
ABSTRACT....11
INTRODUCCIÓN....12
CAPÍTULO I MARCO TEÓRICO CONCEPTUAL....19
1.1 Antecedentes....20
1.2 Marco Teórico Conceptual....23
1.2.1 Proceso de atención al paciente....23
1.2.2 Procedimientos médicos....24
1.2.3 Historia Clínica....24
1.2.4 Sistema de Información en Salud....25
1.2.5 Consulta Externa....25
1.2.6 Área de Emergencia....25
1.2.7 Área de Hospitalización....26
1.2.8 Seguridad de la Información....26
1.2.9 Gobierno de TI....26
1.3.0 Sistema de gestión de seguridad de la información....27
1.3.1 Gestión de riesgos de TI....27
1.3.2 Confidencialidad de la Información....28
1.3.3 Disponibilidad de la Información....28
1.3.4 Integridad de la Información....28
1.3.5 Amenaza....29
1.3.6 Norma ISO/IEC 27001....29
1.3.7 Cobit 5 para seguridad de la información.....30
1.3.8 MAGERIT....30
1.3.9 Organismo Nacional de Gobierno Electrónico ONGEI....30
CAPÍTULO II MATERIALES Y MÉTODOS....31
2.1 Diseño de la Investigación....32
2.2 Población, Muestra y muestreo.....32
2.3 Criterios de selección....33
2.4 Técnicas e instrumentos de recolección de datos....33
2.5 Procedimientos....34
2.6 Plan de procesamientos y análisis de datos.....34
2.7 Consideraciones éticas....35
CAPÍTULO III RESULTADO Y DISCUSIÓN....36

3.1 Diagnóstico del Sector 37
3.2 Descripción de la Institución en estudio 40
3.3 Diagnóstico de la situación actual de las áreas de atención al paciente con respecto a la seguridad de la información en la institución en estudio. 41
3.4 Análisis comparativo de los estándares, marcos de trabajo y metodologías de seguridad de la información. 43
3.5 Modelo Propuesto de Gestión de Seguridad de la Información 47
3.6 Alcance del Modelo: 50
3.7 Fases del Modelo: 51
3.7.1 Fase 0: 51
3.7.2 Contexto Externo 51
3.7.3 Contexto Interno 53
3.7.4 Liderazgo y Compromiso de los Stakeholder 55
3.7.5 Definición de las Políticas y Objetivos de Seguridad de la Información en Salud 56
3.7.6 Objetivos del Modelo de Seguridad de la Información: 59
3.7.7 Instrumentos de Recolección de Información 59
3.7.8 Información de Salud a Proteger 60
3.7.9 Tipos de Amenazas y Vulnerabilidades 60
3.8 Roles y Responsabilidades 63
3.8.1 Identificar, Clasificación y Valorar activos 65
3.8.2 Dependencia de Activos: 72
3.8.3 Identificación y Valorización de Amenazas 76
3.8.4 Nivel de Estimación del Riesgo 78
3.8.5 Tratamiento del Riesgo 85
3.8.6 Identificar Controles 88
3.8.7 Seguridad de Recursos Humanos 89
3.8.8 Seguridad de Control de Accesos 90
3.8.9 Seguridad en las Operaciones 92
3.9 Seguridad en Comunicaciones y Proveedores 93
3.9.1 Seguridad Física y del Entorno 94
3.9.2 Evaluación de Indicadores 95
3.9.3 Cumplimiento de Requisitos Legales 99
3.9.4: Auditoria Interna 102
3.9.5 Revisión de Gestión 104
3.9.6 Formar y Concientizar Personal 104
3.9.7 Mejora Continua. 106

Aplicación del Modelo Propuesto: Caso de estudio “CuidaSalud” 110
CAPÍTULO IV: CONCLUSIONES 160
REFERENCIAS BIBLIOGRÁFICAS 161

ÍNDICE DE ANEXOS

Anexo 1: Consentimiento informado para participantes de investigación 164
Anexo 2: Formato de carta para participantes de la investigación 165
Anexo 3: Cuestionario para Jefes y encargados de las áreas de Soporte Informático de las instituciones de salud 166
Anexo 4: Gráficos de resultados de las encuestas realizadas a las áreas de TI 169
Anexo 5: Análisis del resultado de encuestas realizadas 174
Anexo 6: Matriz RACI de roles y responsabilidades 176
Anexo 7: Proyectos Propuestos 177
Anexo 8: Validación de Expertos 182
Anexo 9: Perfil de Expertos 194

ÍNDICE DE TABLAS

Tabla 1: Identificación de Roles y Responsabilidades 63
Tabla 2: Clasificación de Activos 65
Tabla 3: Procesos del Negocio 66
Tabla 4: Servicios Médicos 67
Tabla 5: Sistemas de Información Institucionales 68
Tabla 6: Identificación de Servicios de TI 68
Tabla 7: Dimensiones en Seguridad de la Información 69
Tabla 8: Contexto Externo de la Institución 110
Tabla 9: Contexto Interno de la Institución 111
Tabla 10: Compromiso de los StakeHolder 112
Tabla 11: Establecimiento de Políticas de Seguridad de la Información 113
Tabla 12: Información de salud a proteger 116
Tabla 13: Identificación de Roles y Responsabilidades 117
Tabla 14: Identificación de los activos 122
Tabla 15: Valoración de Activos 124
Tabla 16: Identificación de Amenazas y Vulnerabilidades 126
Tabla 17: Análisis de Riesgos 131
Tabla 18: Mapa de Calor 135
Tabla 19: Evaluación de Riesgos 136
Tabla 20: Tratamiento de Riesgos 143
Tabla 21: Identificación y descripción de recursos para los controles 149
Tabla 22: Comunicación de Controles 153
Tabla 23: Auditoría Interna 156
Tabla 24: Mejora Contínua 158
Tabla 25: Seguimiento de Proyectos 159

ÍNDICE DE FIGURAS

Figura 1: Mapeo de herramientas a utilizar por resultado esperado ----------20
Figura 2: Proceso de atención al paciente ----------24
Figura 3: Relación Amenaza - Vulnerabilidad ----------29
Figura 4: Contexto Interno de las Instituciones ----------39
Figura 5: Objetivos Estratégicos Institucionales ----------41
Figura 6: Situación de la Seguridad de la Información en el sector ----------42
Figura 7: Matriz de adaptación de Normas, Estándares y Metodologías para la construcción del Modelo ----------45
Figura 8: Análisis y Gestión de Riesgos ----------46
Figura 9: Modelo de Gestión de Seguridad de la Información a implementar ---------49
Figura 10: Lineamientos de Gobierno Digital-Presidencia de Consejo de Ministros --51
Figura 11: Dependencia de Activos ----------73

DEDICATORIA

A Dios por la vida.

A la memoria de mis adorados padres Esteban y Clara, símbolos de amor y constancia, quienes con mucho entusiasmo fueron testigos del inicio de éste reto en mi vida profesional.

A mi esposo Francisco por su comprensión y su constante apoyo en todo momento, y a mi hija María Julia por ser mi motivación más grande para concluir con éxito éste proyecto.

AGRADECIMIENTO

Al Mtro. Gonzalo Martín Valdivia Benites, por el aporte brindado en la revisión de mi investigación.

A mi profesora Mtro. María Ysabel Arangurí García, por sus enseñanzas y aportes en la presente investigación.

Al Mtro. Gregorio León Tenorio por la asesoría y experiencia profesional brindada.

RESUMEN

Las Tecnologías de Información han ocupado un lugar imprescindible en las organizaciones, proporcionando agilidad en los procesos de negocios, y con ello poder brindar un servicio de calidad a sus clientes. Es así, como las entidades prestadoras de salud en el Perú, han pasado a brindar la atención al paciente de una forma eficiente a través de los sistemas de información.

Esta investigación concentra su estudio en elaborar un Modelo de Gestión de Seguridad de la Información, basado en estándares, metodologías y marcos de trabajo adaptados a instituciones de salud, con la finalidad de apoyar los procesos de atención al paciente en sus diferentes áreas, partiendo de la evaluación hecha a cuatro entidades del rubro las cuales carecen de mecanismos para fortalecer un nivel de seguridad de su información apropiados, originando malestar en los pacientes que acuden a una institución de salud, así como el incumplimiento de la normatividad vigente.

El modelo planteado en la presente investigación se validó por juicio de expertos aplicando el coeficiente de Alfa de Cronbach para medir la fiabilidad, y el coeficiente de Kendall para medir la concordancia de los expertos.

Finalmente, el modelo se implementó en una institución de salud de la región Lambayeque, identificando 26 riesgos de los cuales el 23.08% fueron calificados de impacto crítico y 26.92% de alta magnitud, los cuales fueron alineados a controles mediante la propuesta de 4 proyectos y monitoreados adecuadamente, quedando demostrado que la Gestión de la Seguridad de la información logró mejorar los procesos de atención al paciente.

PALABRAS CLAVES: seguridad de la información, institución de salud, procesos de atención.

ABSTRACT

The Information Technology (IT) had occupied an indispensable place in the organisations, IT had given agility in the business process, and with that power to bring a service of quality for the clients. That is the way as the health care facilities in Peru have passed to bring the attention to the patient with a more efficient form using the information systems.

The present investigation focus its attention to develop an Information Security Management Model, this Model has been based on standards, methodologies and work framework that they have been adapted for health institutions, with the purpose of to support the patient attention process in the different areas, it is starting since the evaluation that was done to four health institutions without suitable mechanism to strengthen the security level of their information, this situation causes delay and discomfort in the patients who go to the health institution, and also a problem of failure to comply with existing laws.

The Model was validated through expert judgment applied the Cronbach´s Alpha coefficient to measure the level of reliability and the Kendall coefficient to measure the concordance between the experts.

Finally, the Model was implemented in a publicly owned health institution from Lambayeque region, 26 risks were identified, from these 23.08% were qualified as critical impact, and 26.92% were qualified as high magnitude, these were aligned with controls through the proposal of 4 projects and they were monitored properly, we demonstrated that the information security management to support the process of attention to patient.

Keywords: Information Security, health institution, process of attention.

INTRODUCCIÓN

Incorporar las tecnologías de la información y las comunicaciones a los servicios de salud ha significado ubicarnos en un alto nivel junto a los países desarrollados y, con ello, ofrecer una atención sanitaria de calidad. [1]

Estos sistemas, en sus diferentes plataformas incorporan magníficas funcionalidades que aportan efectividad y eficiencia al proceso de atención; sin embargo, no están exentas de sufrir ataques informáticos realizados por empleados, por este motivo, las instituciones buscan los mecanismos más adecuados para proteger su información de estas amenazas, tal como lo ha tenido en el ámbito internacional la empresa Sony, por el año 2014 y aunque hoy en día sigue trabajando ha tenido que tomarse un tiempo de recuperación después del ataque que sufrió, donde más de 47,000 personas se vieron afectadas por la violación de su seguridad: nombres, números de seguridad social, correos privados, direcciones de e-mail e información personal y de otra índole fueron filtradas. Una parte de los afectados fueron personas que hoy en día siguen formando parte de Sony como es el caso de algunas estrellas de Hollywood, aun así la compañía se recuperó con la retirada de su co-presidenta. [1]

Otro caso, fue American On Line (AOL) empresa de servicios de internet y medios con sede en New York cuando fue hackeada tres veces, la última fue en el 2014 y debido a lo sucedido la empresa publicó en un blog que estaban investigando un incidente en el que se vio comprometido el acceso no autorizado a sus redes y sistemas; debido a los ataques que ha sufrido la compañía decidió cambiar su imagen a una compañía de medios digitales y fue absorbida por Verizon. [1] En el año 2010, la compañía de seguros de salud Anthem envió 230,000 cartas a sus pacientes en California en donde avisaban de que se iban a develar datos de índole personal, miles de informaciones sobre sus pacientes fueron filtradas en Internet, incluido nombres de apellidos, fechas de nacimiento, números de identificación de la seguridad social y médico, correos

electrónicos y direcciones postales, detalles sobre trabajo e ingresos, el total de personas que se vieron afectadas por el ataque llega a pasar las 80 millones. [1]

Por otro lado, el portal de noticias Gestión informó en diciembre del 2018 que el Perú es un nicho para los hackers, uno de los últimos rincones donde aún no se han adoptado las nuevas tendencias de ciberseguridad y el riesgo es bastante alto debido a que la adopción del cloud security todavía no es un servicio ampliamente utilizado en el país. Entonces al no invertir en seguridad en nuestro país nos vuelve atractivos para el hacker, que ya conoce cómo atacar rápidamente sistemas de seguridad de tecnología tradicional. [3]

El cibercrimen también se aprovecha de las vulnerabilidades en nuestro país, una de las amenazas de este tipo es EternalBlue, que se utilizó para propagar Wannacry en el 2017, y dejó una decena de empresas peruanas perjudicadas y más de 200,000 sistemas afectados en 150 países. Eso fue lo que ocurrió en una consultora peruana y todo empezó por no actualizar el sistema operativo de las computadoras, en menos de 1 hora, 25 computadoras resultaron infectadas, no tuvieron un plan y todas las carpetas compartidas habían sido afectadas por ransomware lo que ocasionó la pérdida de la jornada laboral de 25 trabajadores. [2]

En el contexto nacional y de acuerdo a lo informado por el Portal Andina el 25.1% de ataques ransomware (secuestro de datos) en el 2017 fueron identificados en nuestro país, la cifra más alta de América Latina, según la empresa de seguridad Eset. [2]

El caso más conocido a nivel nacional fue el ciberataque a la Baviera del grupo Maersk de Dinamarca, esta empresa fue víctima de ransomware de la variante Petya. la compañía que restringió sus operaciones en el país, tuvo pérdidas financieras no reveladas en su reporte financiero.

Otra modalidad más común de robo de datos, es la ingeniería social a través del phishing para cometer fraude electrónico y estafas en línea. El cibercrimen apunta a los empleados, más que a las empresas para robar información financiera, diversificándose a través de redes sociales y correos electrónicos.

Así mismo, la Asociación de Bancos del Perú (Asbanc) informó el pasado 17 de agosto del 2018, según la cadena de información Andina, que entidades financieras nacionales sufrieron una serie de ataques cibernéticos que también

afectaron a compañías internacionales, dichas entidades tuvieron que suspender o limitar temporalmente ciertos servicios como parte de los procedimientos de respuesta ante incidentes de seguridad y que buscan proteger a sus usuarios [2].

En el ámbito local se ha revisado investigaciones realizadas con base en las conductas y comportamientos de los usuarios y a la concientización en la seguridad de la información, concluyendo que gestionar las conductas y comportamientos de los usuarios se puede obtener un impacto positivo en la concientización para el cumplimiento de las políticas de seguridad de la información siendo así como lo demuestra el caso de estudio de la Universidad Nacional Pedro Ruiz Gallo. [4]

Del mismo modo, Puyén [5] en su investigación aplica gestión de riesgos y Magerit para mejorar la Gestión de Seguridad de la Información en el Hospital Regional de Lambayeque afirmando que un uso adecuado de los modelos de gestión de riesgos, para la seguridad de la información, promueve una cultura de seguridad en toda la organización creando confianza entre sus clientes y mostrando su capacidad entre su competencia.

Por otro lado, Arenas [6] aborda la gestión de la seguridad de la información desde una óptica tecnológica-moderna en relación al tratamiento de información para la toma de decisiones, analiza la información entre la plataforma de gestión de seguridad de la información desarrollada y recopila información sensible dentro de un entorno de red junto con una guía de mejores prácticas reconocida mundialmente como COBIT. Este modelo de gestión de seguridad de la información para la toma de decisiones se desarrolla en el Área Telemática de una Universidad local, se describen las fases del desarrollo del modelo en base a los procesos habilitados y los resultados obtenidos permiten la evaluación fiable, consistente y repetible de un proceso en el ámbito de la gestión de la empresa de TI basada en la evidencia.

Nuestro país no es ajeno a los ciberataques estos son cada vez más sofisticados, frecuentes y peligrosos, constituyen pues una de las principales amenazas para la operatividad de las empresas peruanas.

El problema de la seguridad de la información en nuestro país va más allá de las herramientas puramente tecnológicas, es un problema de concientización y de inversión para proteger la información crítica del negocio lo que podría conllevar a gastos excesivos como sanciones y multas por incumplimiento de regulaciones.

Alrededor del 2003 en nuestro país, fue creada la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) como un órgano técnico especializado dependiente de la Presidencia de Consejo de Ministros y en su calidad de ente rector del Sistema Nacional de Informática, se encarga de liderar los proyectos, la normatividad y las diversas actividades que en materia de Gobierno Electrónico realiza el Estado. Entre sus actividades permanentes se encuentran: Normatividad informática, Seguridad de la Información, Desarrollo de proyectos emblemáticos en tecnologías de la información y la comunicación, además de brindar asesoría técnica e informática a las entidades públicas. [7]
Así también, a través de la oficina de Secretaría Digital se aprueban los Estándares de Interoperabilidad de la Plataforma de Interoperabilidad del Estado, con Resolución de Secretaría de Gobierno Digital No.002-2019-PCM/SEGDI, de Julio del 2019 en la que comprende los estándares necesarios para seguridad de información entre sistemas de información a través de la Plataforma de Interoperabilidad del Estado. [7]
Con el objetivo de proteger la infraestructura de información, los datos e información del Estado así como la Tecnología utilizada para su procesamiento, frente a amenazas internas o externas deliberadas o accidentales y con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información el Estado cuenta con un documento llamado: "Política Nacional de Ciberseguridad aprobado con Resolución de Secretaría de Gobierno Digital No.001-2018-PCM-/SEGDI del 04 de Enero del 2018, en donde señala 05 objetivos que se deben implementar para el cumplimiento de las políticas y lineamientos que se establezcan respecto a ciberseguridad. [7]
La necesidad de elaborar un modelo de gestión integral para la seguridad de la información en una institución de salud se hace cada vez más urgente por el incremento de su uso en las prestaciones de los servicios de salud; lo contrario

a esto, podría incrementar los riesgos de confidencialidad, integridad y disponibilidad de la información. Todas las instituciones de salud necesitan tener estrictos controles implementados para proteger la información de salud del paciente que se les ha confiado.

En nuestra localidad existen instituciones de salud, que brindan atención especializada de alto nivel de complejidad en todas las especialidades médicas, estos establecimientos cuentan con una gran población activa referida de los hospitales de menor nivel de atención, de la zona norte y nor oriental del país, por ello, surge la necesidad de proteger la información sensible del paciente en al momento de la atención, lo que permitirá dar un mejor servicio apoyados en los sistemas informáticos de gestión y evitar la fuga de información que podría ser usada de manera maliciosa por algún usuario, interno o externo al flujo de información minimizando los riesgos de seguridad de la información en TI.

La institución objeto de estudio en su Plan Estratégico orienta una gestión por procesos apoyados en una plataforma tecnológica moderna que impacta positivamente en el bienestar de su población.

En este contexto, dentro de la problemática actual en seguridad de la información en el sector salud se encontró que existe un desconocimiento de La Ley de Protección de Datos Personales (Ley N° 29733), por parte del personal que tiene como función el registro de los datos del paciente en las áreas de atención, existen vulnerabilidades en el entorno de la red de datos que puede ser extraída y utilizada por terceros, ausencia de políticas de seguridad de la información [8], falta de concientización en la confidencialidad de la información de los diagnósticos del paciente en el proceso de atención, ausencia de controles, las áreas claves de la institución donde se almacena o custodia la información del paciente deben reforzar la seguridad desde el proceso de ingreso hasta el alta del paciente, se ha evidenciado que la historia clínica se encuentra en muchos de los casos fragmentada por falta de disponibilidad de la misma, omisión de información en los datos de ayuda al diagnóstico, se debe mejorar la identificación de los datos personales de cada paciente mediante el sistema biométrico en todas las áreas principalmente en la consulta externa, emergencia y hospitalización, ausencia de seguridad de control de accesos a los sistemas de

información, personal con falta de entrenamiento y competencias respecto a seguridad de datos.

Bajo el análisis de esta problemática encontrada en el sector se formuló la siguiente interrogante: ¿De qué manera la implementación de un Modelo de Gestión de Seguridad de la Información apoyará el proceso de atención al paciente?, en respuesta a ésta interrogante se planteó la siguiente hipótesis: la implementación de un modelo de gestión de seguridad de la información basado en la armonización de metodologías, normas, marcos de trabajo apoyará el proceso de atención al paciente protegiéndola en su integridad, disponibilidad y confidencialidad.

Para demostrar la validez del modelo, fue necesario apoyarse en el cumplimiento de los siguientes objetivos específicos:

- Analizar las normas, estándares internacionales y metodologías que se adapten al modelo a implementar respecto a seguridad de la información, identificando herramientas válidas para el desarrollo de la investigación, determinando armonización de dichas metodologías de manera que mejor se adapten a la institución en estudio.

- Diseñar el modelo aplicando las metodologías y herramientas que permitan realizar análisis de riesgos e identificar amenazas que puedan afectar los activos de información.

- Implementar el modelo para el caso de estudio, aplicando mecanismos y controles que mitiguen los riesgos e identificar amenazas que puedan afectar los activos de información.

- Validar el modelo a través del juicio de tres expertos en la línea de investigación, método que sirve para obtener y verificar la fiabilidad entre las variables que la conforman, y la concordancia entre los expertos, dos criterios de calidad que debe reunir todo instrumento estadístico de medición tras ser sometido a la consulta y al juicio de expertos.

La investigación se justifica desde el aspecto legal porque permitirá dar cumplimiento a sus regulaciones y obligaciones legales, como la Ley 29733 Ley

de Protección de datos personales [10], Resolución Ministerial N°004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Requisitos 2da. ed. en todas las entidades integrantes del Sistema Nacional de Informática [11], RM.431-2015/MINSA 09-07-2015, Aprobar "Políticas de Seguridad de la Información del Ministerio de Salud-MINSA". [12]

En lo económico, habrá reducción de costos en la recuperación de bienes y servicios, así como evitará situaciones que podrían causar pérdidas inesperadas y no planificadas. En el aspecto tecnológico la institución procesará y protegerá los datos e información de sus pacientes con la seguridad adecuada de su entorno asignando roles específicos y responsabilidades.

Un sistema de seguridad de la información ayudó a lograr el cumplimiento de los objetivos de la institución mediante una serie de estrategias que incluyen la optimización de procesos, el enfoque centrado en la gestión y el pensamiento disciplinado. En el aspecto social se justifica a través de los planes de capacitación, aplicando programas de concientización en seguridad de la información de los datos del paciente incorporando de esta manera valor a la organización no olvidar que una institución que gestiona adecuadamente la seguridad de su información genera confianza a sus clientes.

La institución en estudio ha experimentado cambios evolutivos que reflejan; además, de las cuestiones propias de la administración pública, innovaciones pertinentes a la situación y tendencias de gestión asociadas a tiempos actuales: acelerado crecimiento de la tecnología, incremento de los servicios prestados, mayores exigencias en las regulaciones, reorganización institucional, políticas que apuntan al monitoreo de objetivos y medición de resultados, entre otros así como garantizar la confiabilidad de la información a través de la adopción de medidas oportunas.

CAPÍTULO I MARCO TEÓRICO CONCEPTUAL

1.1 Antecedentes

Con la finalidad de realizar el sustento técnico a la propuesta planteada, se han seleccionado los antecedentes relacionados al asunto en investigación:

Según Talavera [13], en su investigación elaboró un mapeo de las herramientas que utilizaron para identificar las metodologías que mejor se adapten a su objeto del estudio. Para ello utilizaron el ciclo de Deming y permitieron demostrar que la implementación de un diseño de Sistema de Gestión de Seguridad de la Información garantiza la protección de la información, los datos personales y activos con que cuenta.

Figura 1: Mapeo de herramientas a utilizar por resultado esperado

Resultado esperado	Herramienta a utilizar
RE1: Documentación exigida por la norma ISO 27001	**Norma ISO 27001** estándar internacional que especifica los requisitos a cumplir para establecer un SGSI.
RE2: Mapa de procesos del alcance	**Business Process Management (BPM 2.0)** metodología que agrupa varias herramientas cuya finalidad es el análisis y control de los procesos de negocio de una empresa.
RE3: Metodología de análisis de riesgos	**Norma ISO 31000** estándar internacional que sirve como referencia a la valuación y gestión de riesgos.
RE4: Metodología de valoración de activos	
RE5: Mapa de riesgos	
RE6: Declaración de aplicabilidad	**Norma ISO 27002** conjunto de objetivos de control y controles que pueden ser aplicados para el tratamiento del riesgo. **Norma ISO 27799** norma que aplica los conceptos contenidos en la norma 27002 al entorno de las instituciones de salud.

Fuente: Talavera, 2015 [13]

De esta manera asegurar el buen uso y protección de la información crítica que manejen, ya sea de clientes o información estratégica interna.

Talavera menciona, que existe una brecha importante en cuanto a seguridad de la información que debe ser resuelta cuanto antes involucrando a la dirección en las acciones del plan de seguridad de la

información el cual debe ser gestionado como un proyecto institucional y que cuente con el apoyo de las distintas direcciones y áreas del Instituto de Maternidad, urgen elaboración de planes de capacitación que concienticen al personal sobre la importancia de la información con la cual se realizan las labores institucionales, así como fomentar el cumplimiento de las políticas que garanticen la seguridad de la misma. Recomienda la definición del cargo del Oficial de Seguridad de la Información y que dependa de una dirección institucional para que cuente con el apoyo de la Dirección General de la Maternidad de Lima.

Recomienda también que se debe trabajar en conjunto, con el área de Control Interno apoyándose en el mismo durante el análisis de los riesgos de la institución dado que dicha área debería tener una visión holística de los riesgos que se presentan en la misma. Asi como la creación de un área de seguridad de la información que permita contar con personal especializado y dedicado al control y mantenimiento del Sistema de Gestión de Seguridad de la Iinformación a cargo de un Oficial de Seguridad de la Información.

Carazo [14], elabora un Plan de seguridad de la información a una empresa dedicada al sector de las tecnologías de la información, para ello realizan un análisis de riesgos inicial, de manera que identifican los activos críticos que podrían comprometer la continuidad del negocio en caso de incidente, posteriormente se analizan las amenazas que puedan afectar a la empresa y a partir de estos resultados se puedan diseñar los proyectos para acercar a niveles optimos la seguridad de los activos de la organización. En los resultados presentados concluyen que no existe una política de seguridad bien definida en general en ningun aspecto. Al no existir una política de seguridad formal y completa en la organización, tampoco existe una revisión sobre ella por lo que el dominio de la ISO/IEC 27002:2005 sería uno de los objetivos a mejorar, primeramente creando una política de seguridad adecuada para la organización y seguidamente estableciendo periodos de revisión de la misma.

Según De La Cruz [15], realiza una investigación que tiene como objetivo principal realizar la propuesta de políticas, basadas en buenas prácticas para la gestión de seguridad de la información en la Municipalidad Provincial de Paita, encontrando que dicha institución carece de políticas y controles eficientes por lo tanto queda demostrado que es necesario la elaboración de una propuesta el mismo que permitirá minimizar la pérdida de información. Asimismo recomienda la conformación de un Comité de Seguridad de la Información para que pueda iniciar sus funciones y distribuir responsabilidades en forma adecuada, las mismas que tienen por finalidad aprobar, implementar, divulgar y controlar la implementación de la propuesta de políticas basadas en buenas prácticas, para la gestión de seguridad de la información.

La reestructuración de su área de sistemas a la categoría de Gerencia de TI y sistemas de información, cuyas funciones deberían estar desagregadas a cada oficina para lograr una mejor coherencia funcional por constituirse en una pieza clave para el desarrollo organizacional en todas las áreas administrativas y más aún en la implementación de la propuesta de seguridad de la información. También plantea Planes de Capacitaciones en temas relacionados con la seguridad de la información para que todos los funcionarios adquieran competencias y destrezas en el uso adecuado de la misma, de igual forma incluir en el proceso de inducción, la socialización de las políticas de seguridad de la información.

Tarrillo [16], propone una metodología para un Sistema de Gestión de la Seguridad de la Información basado en la NTP 17799 en la Administración de la Municipalidad de Lambayeque, dicha metodología permitió determinar los objetivos, procesos, procedimientos para el establecimiento de políticas de seguridad, así como un conjunto de controles de seguridad que ayudan a gestionar los riesgos en la Seguridad de la Información que maneja al organismo objeto de estudio, mejorando de esta forma la gestión de los incidentes de seguridad que se detecten generando resultados en concordancia con los objetivos políticas requeridas para optimizar la plataforma tecnológica de la Municipalidad.

Rayme [17], deja demostrado a traves de una investigación realizada en tres universidades en la ciudad de Lima, las estrategias que se deben utilizar en la gestión de seguridad de la informacion como son: primero, la importancia de desarrollar políticas de seguridad de la informacion, segundo los programas de capacitación al personal donde los expertos consultados informaron el interes por asistir y tercero la protección a los recursos de información, así también el 38% de la población entrevistada manifestaron que sus equipos informáticos no poseen equipos de protección. Los resultados también demostraron que al implementarse estas estrategias el impacto en las aplicaciones de red e internet será eficaz y de acuerdo a los expertos consultados se obtendran beneficios tales como : una mejor protección de la información y una mejora de la calidad en el servicio a los alumnos y docentes. Además se minimizan los riesgos de la información en el caso de la UNMSM la infección de virus informáticos es de 56% mayor al de las otras universidades consultadas.

Villena [18], adopta algunas normas existentes en el mercado que establecen determinadas reglas o estándares que sirven de guía para gestionar la seguridad de la información de las cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú, como primer paso la clave consiste en obtener el apoyo y soporte de la alta gerencia, dandoles a conocer la importancia de la seguridad de la información en los procesos que manejan, luego se integran los lineamientos, políticas, normas. Estándares y procedimientos de seguridad soportados por el área de Tecnologías de Información de la Institución.

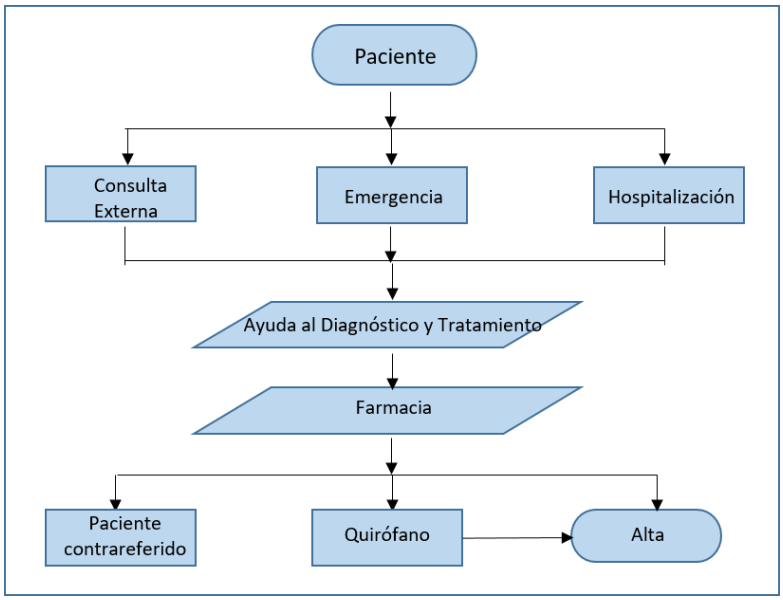
1.2 Marco Teórico Conceptual

En esta parte se hace referencia a los conceptos y términos relacionados a la investigación y que dan el sustento al modelo propuesto.

1.2.1 Proceso de atención al paciente

Variable de la investigación que habla de las actividades indispensable que se deben ejecutar para la realización y cumplimiento del proceso de atención al paciente que se brinda en los diferentes áreas hospitalarias clínicas, quirúrgicas y especializadas. El modelo fue aplicado a las áreas de mayor demanda como son: Consulta Externa, Emergencia y Hospitalización.

Figura 2: Proceso de atención al paciente



Fuente: Elaboración propia

1.2.2 Procedimientos médicos

Es importante para el desarrollo de la investigación, mencionar que los procedimientos médicos que se otorgan a un paciente dentro de una institución de salud, requieren de obtener datos que mantengan su integridad, puesto que apoyará al médico o personal de salud a realizar dicha acción con calidad y confianza, siendo así, dichos procedimientos médicos son todas aquellas acciones u operaciones que al ejecutarse otorgan bienestar y cuidados en la salud del paciente.

1.2.3 Historia Clínica

La historia clínica es un documento médico legal en el que se registra manualmente los datos relacionados a la atención al paciente, es llenada por los profesionales de la salud registrando de manera secuencial los detalles de la atención brindada. Es importante mencionar que para la investigación es un documento importante en el que se puede encontrar como dato sensible la información de salud de cada paciente la misma que debe guardar la confidencialidad e integridad, debe estar disponible para el momento de la atención, no se limita a contener una simple narración o exposición de hechos, sino que incluye juicios, documentaciones, procedimientos, informaciones así como consentimiento de la persona enferma, basados en el principio de autonomía, en su reconocimiento, aceptación del estado de salud o enfermedad que presenta y en su participación en las tomas de decisiones. [25]

1.2.4 Sistema de Información en Salud

Considerado así a todo sistema que almacena información importante sobre la terapéutica médica de la salud de uno o más pacientes, la cual se encuentra almacenada tanto en equipos como en áreas debidamente protegidas de cualquier incidente a cargo de personal autorizados según niveles de acceso a la misma.

Estas plataformas con diferentes infraestructuras de hardware y software se convierten en los principales activos del presente caso de estudio.

1.2.5 Consulta Externa

Acto médico realizado a un grupo de pacientes, de manera ambulatoria para tratar una dolencia mediante un diagnóstico encontrado, dicha acto está apoyado en la anamnesis y exploración física que se le realiza al paciente, así como en los resultados de exámenes auxiliares realizados.

1.2.6 Área de Emergencia

Según la Organización Mundial de la Salud (OMS), es la unidad orgánica encargada de realizar la atención especializada a los pacientes, que

requieren una atención de Emergencia en el más breve plazo para atender un problema de causa grave por parte del paciente que lo sufre. [20]

1.2.7 Área de Hospitalización

Consiste en el área física, en la que se le interna a un paciente para brindarle cuidados según las prescripciones del médico tratante, el control, seguimiento de su estado de salud y evolución del tratamiento apoyados en la información de ayuda al diagnóstico que se proporciona generalmente por los sistemas de información hospitalarios.

1.2.8 Seguridad de la Información

En la investigación, éste concepto permite aportar un conjunto de medidas preventivas y reactivas a las organizaciones así como sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

De acuerdo a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), la seguridad de la Informacion es el conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener las dimensiones de la misma. Cuando se habla de información se abarca todo tipo de información: impresa o escrita a mano, grabada con asistencia técnica, trasmitida por correo o electrónicamente, incluida en un sitio web, mostrada en videos corporativos ó mencionada durante las conversaciones.

1.2.9 Gobierno de TI

En la actualidad el gobierno de TI es una prioridad en las instituciones, ya que permite obtener el máximo valor de las Tecnologías de la Información, es importante mencionarlo asi como considerarlo en la investigación dado que a través de éste sistema se dirigen y controlan los recursos de TI que dan soporte a la organización como al monitoreo de dicho uso para alcanzar los objetivos de los planes estratégicos. Según Crue [19], el Gobierno de las TI es una responsabilidad del más alto nivel directivo y se

encuentra en lo más alto de una pirámide que estaría basado en las operaciones de TI y la gestión de TI, El éxito del Gobierno de las TI está ligado a la comprensión y apoyo que obtenga por parte del equipo de Dirección.

1.3.0 Sistema de gestión de seguridad de la información

Según la norma/estándar UNE ISO/IEC 27001:2007 el Sistema de Gestión de la Seguridad de la Información es la solución de mejora contínua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados), lógicos (virus informáticos, ataques de intrusión o denegación de servicios) de esta manera establecer las estrategias y controles adecuados que aseguren una permanente protección en salvaguarda de la información.

El Sistema de Seguridad de la Información se fundamenta en la norma UNE-ISO/IEC 27001:2014, que sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o de Deming, que consisten en Planificar –Hacer-Verificar- Actuar, más conocido con el acrónimo en inglés PDCA (Plan-Do-Check-Act). La seguridad de los activos de la institución en estudio se enfrentan a muchos riesgos e inseguridades procedentes de diferentes orígenes, por lo que éste sistema nos permite elaborar un plan para la correcta gestión de protección y seguridad de estos activos. [20]

1.3.1 Gestión de riesgos de TI

La Gestión de Riesgos en esta investigación tendrá un papel fundamental porque contribuirá a identificar los riesgos para luego evaluar las consecuencias y probabilidad de ocurrencia, así como permitirá establecer un orden de prioridad para el tratamiento de los riesgos y las acciones para reducir la ocurrencia.

También contribuirá a la participación de los interesados para la toma de decisiones de la gestión de riesgos, al monitoreo del tratamiento. Asimismo, como es un proceso contínuo y de constante desarrollo, debe estar integrado en la cultura de toda institución con políticas y programas dirigidos desde la alta dirección. [5]

1.3.2 Confidencialidad de la Información

Según la Secretaría de Gobierno Digital [7] la confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. Es importante en esta investigación demostrar que el modelo garantice la accesibilidad de la información a personal autorizado tal como lo menciona la ISO/IEC 27001 ya que es una de las piedras angulares de la seguridad de la información. La confidencialidad también está referida a un principio ético profesional. Por lo tanto, con la implementación del modelo la información debe ser accesible sólo a aquellos que se encuentran debidamente autorizados.

1.3.3 Disponibilidad de la Información

Según la Secretaría de Gobierno Digital [7], la disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Para el caso de estudio permitirá resolver problemas, dar respuestas en la institución y con ello proporcionará el apoyo al proceso de atención al paciente, ya que estará disponible en forma organizada para los usuarios autorizados cuando sea requerida.

1.3.4 Integridad de la Información

De acuerdo a la Secretaría de Gobierno Digital [7] es importante que la información no solo esté disponible sino que este íntegra en su conjunto de datos libres de modificaciones no autorizadas, la integridad es mantener

con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados, es decir completa, exacta y válida.

1.3.5 Amenaza

Toda posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial sobre los elementos de información).

Figura 3: Relación Amenaza - Vulnerabilidad

Amenazas	Vulnerabilidades
Robo	Almacén desprotegido y sin vigilancia
Error de entrada de datos por parte del personal	Complicados procedimientos de proceso de datos
Fraude, uso no autorizado de un sistema	No segregación de tareas
Robo de Información	Los datos no cifrados
Virus, gusanos, malware	Uso de software pirata
Acceso no autorizado a las personas que han abandonado la organización	No revisión de los derechos de acceso
Pérdida de información	Procedimientos de backup

Fuente: ONGEI [5, pag16]

1.3.6 Norma ISO/IEC 27001

La Organización Internacional de Estandarización estableció la norma ISO 27001, que se emplea para la certificación de los Sistemas de Gestión de Seguridad de la Información en las organizaciones empresariales [21]. Con el uso de esta norma, las instituciones pueden demostrar a sus clientes actuales y potenciales, así como a sus proveedores y accionistas, la integridad en el manejo de la seguridad de la información. También le

posibilita reforzar la seguridad de la información y disminuir los riesgos de fraude, pérdida o filtración de información.

1.3.7 Cobit 5 para seguridad de la información.

Marco de Gobierno de Tecnologías de Información que proporciona una serie de herramientas para que las empresas obtengan valor óptimo de las TI, manteniendo un balance entre los beneficios, riesgos y recursos. Estas herramientas encontradas en el AP13: Seguridad de la Información permitieron recopilar datos importantes en el contexto del rubro para llegar a la construcción del Modelo. [22]

1.3.8 MAGERIT

El Método de Análisis y Gestión de Riesgos de Tecnologías de Información (MAGERIT) desarrollado por el Consejo Superior de Administración Electrónica, y publicado por el Ministerio de Administraciones Públicas de España, comprende dos grandes procesos: El análisis de riesgos y la gestión de riesgos.

Si hablamos de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico. [23]

1.3.9 Organismo Nacional de Gobierno Electrónico ONGEI

La Oficina Nacional de Gobierno Electrónico e Informática ente rector del Sistema Nacional de Informática encargado de proponer la Estrategia Nacional de Gobierno Electrónico en todas las instituciones del Estado, así como de coordinar y supervisar su implementación. Permitirá dar el sustento normativo legal a la investigación ya que esta oficina coordina y supervisa la integración funcional de los sistemas informáticos del Estado y promueve el desarrollo de sistemas y aplicaciones de uso común en las entidades de la Administración Pública [24].

CAPÍTULO II MATERIALES Y MÉTODOS

2.1 Diseño de la Investigación

El diseño que presentó el estudio de investigación es experimental de pre y post evaluación con el proceso de atención al paciente en la especialidad de mayor demanda, teniendo en cuenta la siguiente fórmula:

E P1 M P2

Donde:

E: Grupo de colaboradores.
P1: Proceso de atención antes de la implementación del Modelo de Gestión de Seguridad de la Información
M: Modelo de Gestión de Seguridad de la Información
P2: Proceso de atención después de aplicar el Modelo de Gestión de Seguridad de la Información.

2.2 Población, Muestra y muestreo.

Población:

La población considerada para la investigación fueron todas las especialidades de consulta externa, así como el personal que otorga citas, el área de archivo de historias clínicas y personal del área de tecnologías de información.

Muestra:

Considerando que una de las principales actividades médicas más importantes es la consulta externa en un hospital, se tomó como muestra el personal que labora en la consulta externa de la especialidad de mayor demanda, el personal administrativo que otorga citas, así como el personal técnico que proporciona las historias clínicas para dicha especialidad y personal del área de tecnologías de información.

Del número de personas que se seleccionaron tanto para la entrevista como para la encuesta se obtuvo una apreciación real de la situación actual y problemática ya que cumplen un papel relevante en la atención al paciente.

Muestreo:

Para el estudio de investigación se ha considerado usar la técnica de muestreo por conveniencia dada la conveniente accesibilidad, disponibilidad y proximidad de los sujetos.

2.3 Criterios de selección

Después de haber revisado información respecto a las técnicas de muestreo se seleccionó la técnica de muestreo por conveniencia, mediante ésta técnica se pueden observar hábitos, opiniones y puntos de vista de manera más fácil, tomando en consideración los siguientes criterios:

- Método rápido para recolección de datos.
- Menos inversión en un corto periodo de tiempo.
- Muestra fácilmente recolectada.
- Menos inconvenientes para recopilar la información

2.4 Técnicas e instrumentos de recolección de datos

Con la finalidad de obtener los mejores resultados en el presente estudio de investigación se utilizó COBIT 5 para la seguridad de la información basado en una guía práctica que proporciona en su proceso APO13: Gestionar la seguridad, apoyo a los gestores de TI. Mediante ésta herramienta se garantiza el cumplimiento de normas y aumenta la eficiencia y eficacia ya que integra procesos y recursos de otros estándares y algunas normas ISO.

Los instrumentos construidos bajo ésta metodología fueron las entrevistas, encuestas, cuestionarios para la recolección de datos y plantillas.

2.5 Procedimientos

Para recolectar los datos del estudio se consideró seguir los siguientes mecanismos:

- Encuestas, se aplicaron encuestas al personal elegido, así como a los colaboradores de las áreas críticas.
- Entrevistas
- Consultas
- Reuniones
- Observación
- Revisión de documentación, los documentos revisados fueron:
  - Plan estratégico Institucional.
  - Visión, Misión, Objetivos Estratégicos y Organigrama.
  - La estructura de la organización, funciones y responsabilidades (MOF).
  - Normas y políticas institucionales.
  - Sistemas de seguridad informática (año 2005) y procesos de toma de decisiones.

2.6 Plan de procesamientos y análisis de datos.

El Plan de procesamiento de la información para el estudio propuesto basado en seguridad de la información se realizó con el siguiente criterio:

- Levantamiento de información (situación actual)
- Clasificación de la información.
- Registro de la información.
- Análisis de la información obtenida.
- Verificación de la información.
- Se tabuló la información para el recuento y ordenación de la información en tablas para ello fue necesario Office Excell v.2016, asimismo se consideró el software SPSS para análisis estadístico de la calificación de los expertos durante la validación del modelo aplicado al caso de estudio.

Con los datos obtenidos se analizarán la implementación de un Modelo de Gestión de Seguridad de la Información apoyados en las normas ISO 27001, ISO/IEC 25001, ISO/IEC 27799.

2.7 Consideraciones éticas

Para el presente estudio de investigación se utilizó un consentimiento informado, herramienta que fue llenada por los colaboradores involucradas en el muestreo con la finalidad de participar en la investigación de manera voluntaria y si desean o no formar parte de ella, también se les informó respecto a la metodología y procesos a utilizar, la duración estimada del estudio, los mecanismos para proteger la información que se obtendrá, la confidencialidad de la información, la misma que no fue usada para ningún otro propósito. (ver anexo 01)

Asimismo, se elaboró una carta dirigida al colaborador (ver anexo 2) en donde se manifestó el compromiso de guardar la confidencialidad y la total reserva respecto a la información obtenida de las entrevistas, encuestas y observación de los hechos la misma que será de sólo sustento dentro de la investigación.

CAPÍTULO III RESULTADO Y DISCUSIÓN

3.1 Diagnóstico del Sector

En el desarrollo de la presente investigación, se hizo un análisis a cuatro empresas públicas del sector salud de la región de Lambayeque de las cuales se obtuvo información respecto a la organización, razón social, valores, objetivos estratégicos, visión, misión, organigrama, así como la descripción de su área de TI de cada uno de ellos.

Para ello se realizaron visitas en sus instalaciones, principalmente donde se acceda a la información clínica de los pacientes (consultorios, archivos de historias clínicas, módulos de atención, áreas de atención). Respecto al uso de los sistemas de información se pudo evidenciar que los equipos informáticos de la institución se encuentran desprotegidos, expuestos ante la presencia de personas extrañas que pueda ingresar a las áreas, también se evidenció el acceso a los puertos USB, sin control, pudiendo afectar gravemente la información de los pacientes que están registrados en los sistemas de información de cada hospital.

Asimismo, se pudo evidenciar la inexistencia de Políticas de Seguridad de la Información mediante la ausencia de documentos. Los accesos físicos son vulnerables ante la presencia de cualquier personal externo al área y a la institución. Muy pocos trabajadores portan sus credenciales personales, por otro lado las contraseñas y los nombres de los usuarios para ingresar a los sistemas de información se encuentran escritos en las paredes cerca a los equipos de cómputo.

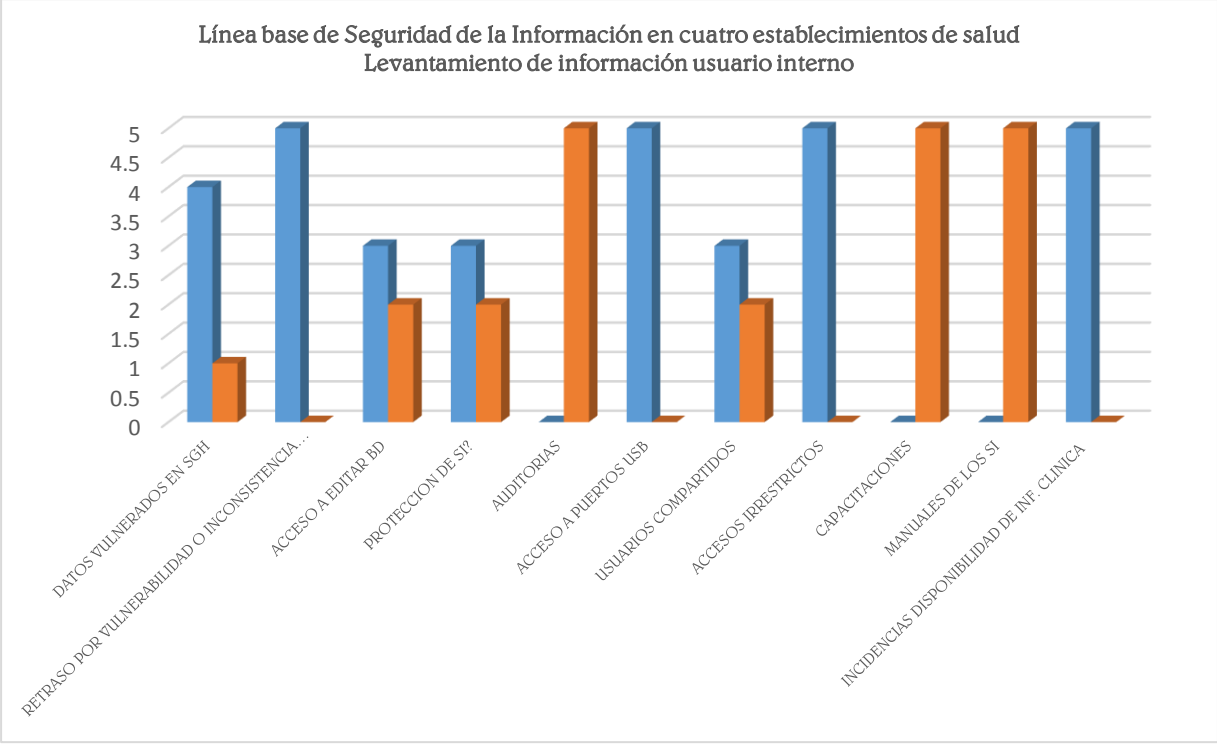
También se pudo observar que más de un trabajador conoce y maneja más de un usuario y contraseña a la vez, esto debido a que no hay conciencia del uso personal de la asignación de usuarios y contraseñas, se pudo obtener información respecto a los reportes que cada uno de ellos puede extraer de los sistemas hospitalarios (resultados de ayuda al diagnóstico, tratamientos farmacológicos por paciente, registros de nacimientos, registros de neonatos, etc.) inclusive la cantidad de material médico utilizado por paciente. Teniendo como principal riesgo la confidencialidad e integridad de la información clínica de todos los pacientes que se atiende en cada centro de salud.

Los procesos de los servicios hospitalarios se encuentran entonces en nuestro medio ante un cierto grado de inseguridad de la información, esto podría conllevar definitivamente a errores médicos al momento de la toma de decisión ante un tratamiento.

Se realizaron encuestas al usuario interno de cada establecimiento concluyendo que, el 62% de la población encuestada manifiesta que están

expuestos a la vulnerabilidad de datos y que esto ocasiona problemas a los profesionales de la salud en la atención al paciente, así como también existe inconsistencias de datos debido a la falta de personal para el ingreso de los mismos, errores involuntarios. No han tenido capacitaciones en los últimos 5 años con relación a temas relacionados a tecnologías de la información tampoco cuentan con manuales ni documentos de autoayuda.(ver figura 4)

Figura 4: Contexto Interno de las Instituciones



Fuente: Elaboración propia

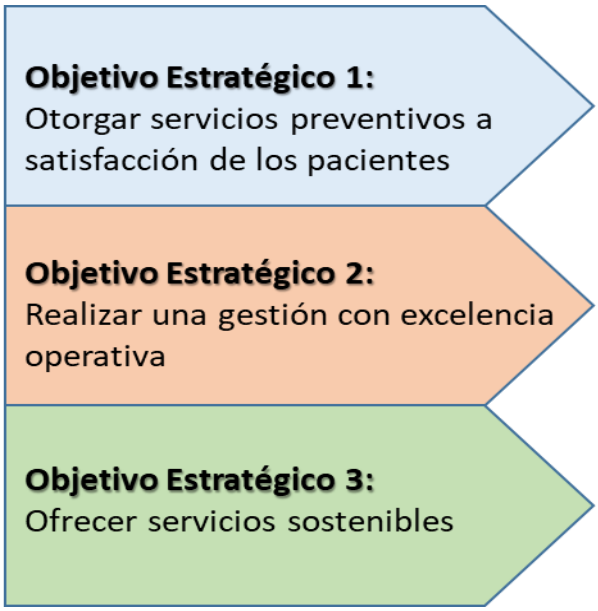
Estas deficiencias relacionadas a la seguridad de la información del paciente en un establecimiento de salud, conlleva también a un problema administrativo en la parte más importante de la gestión hospitalaria, como es el reporte de los indicadores hospitalarios, como acuerdos de gestión que se realizan anualmente en las redes hospitalarias a nivel nacional.

3.2 Descripción de la Institución en estudio

La Institución en estudio es el hospital de mayor nivel en la Región Norte del País, y atiende pacientes que son referidos de toda la zona norte. Tiene el apoyo de la alta dirección de su sede central, para la implementación en infraestructura de sus diferentes servicios, así como con modernos equipos y mobiliario. A la fecha cuenta con diversas especialidades médicas y quirúrgicas se encarga de realizar cirugías de alta complejidad. En el año 2016, se especializó en patologías cardiovasculares de alta complejidad realizando cirugías de corazón a pecho abierto cada año, contando a partir de ello con Sala de Cateterismo Cardíaco, equipos ecocardiógrafos y unidad de cuidados cardiovasculares, asimismo se realizan cateterismos cardiacos cada año, Tiene por finalidad dar cobertura a sus pacientes, a través del otorgamiento de prestaciones de salud, prevención, promoción, recuperación y rehabilitación, prestaciones económicas y prestaciones sociales.

Los Objetivos estratégicos de la institución en estudio son:

Figura 5: Objetivos Estratégicos Institucionales

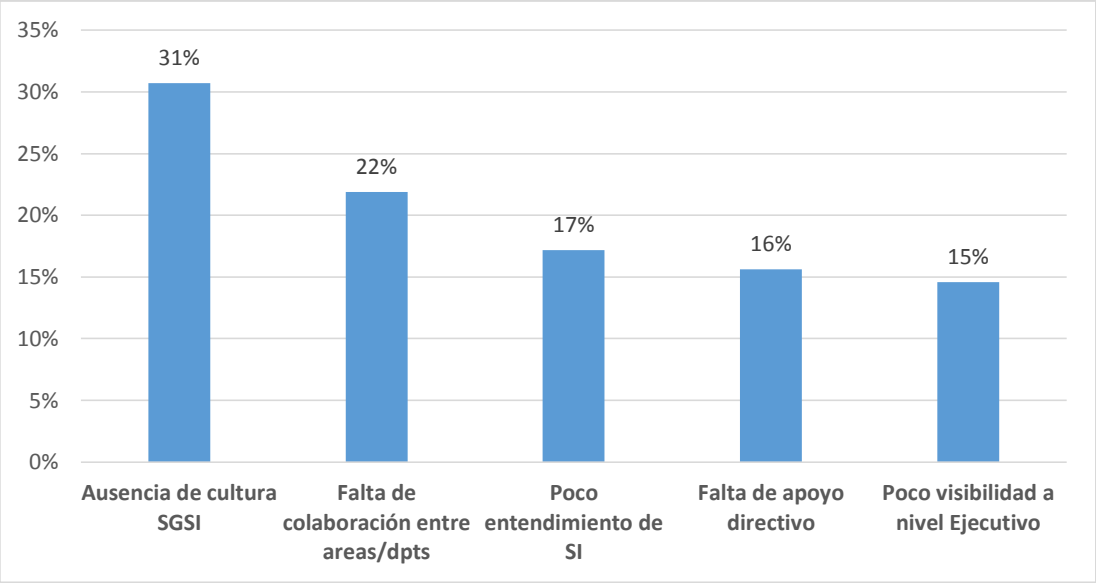


Fuente: Plan Operativo

3.3 Diagnóstico de la situación actual de las áreas de atención al paciente con respecto a la seguridad de la información en la institución en estudio.

Del estudio realizado a los establecimientos de salud, al personal asistencial que maneja información del paciente, así como al usuario interno se puede llegar al siguiente análisis: (ver Figura 06)

Figura 6: Situación de la Seguridad de la Información en el sector



Fuente: Elaboración propia

Análisis:

- Existe un 31% de ausencia de cultura en Seguridad de la Información
- El 22% manifiesta la falta de colaboración entre áreas y departamentos asistenciales para solucionar problemas relacionados a la información del paciente.
- El 17% tiene poco entendimiento del tema de seguridad de la información.
- Un 16% evidencia falta de apoyo y compromiso directivo para solucionar problemas en la atención al paciente.
- Existe poca visibilidad (15%) a nivel Ejecutivo de las normas y estándares que rigen la Seguridad de la Información, gestión de riesgos, activos críticos, etc.

- En dos de ellas tienen procesos básicos de gestión de seguridad Informática relacionados directamente con el equipamiento en sus centros soporte informáticos.

Por lo tanto, no existen controles que permiten detectar posibles incidentes de seguridad, tampoco se encuentran gestionados dentro de sus proyectos.

Inexistencia de planes de recuperación, comités de seguridad de la información, evaluaciones de riesgos, mejoras, procesos de detección, monitoreo continuo de seguridad.

El personal de TI reconoce que existe un problema y que hay que tratarlo, la implementación de controles depende de cada integrante del área y es principalmente reactiva.

3.4 Análisis comparativo de los estándares, marcos de trabajo y metodologías de seguridad de la información.

Para la construcción del Modelo de Gestión de la Seguridad de la Información se ha considerado aplicar el estándar internacional ISO 27001: 2014, para entender los requerimientos de seguridad de la información de las instituciones de salud y la necesidad de establecer políticas y objetivos para la seguridad de la información, la norma ISO 27002:2013 para implementar y operar controles, la norma ISO 27005:2011 proporciona pautas para la gestión de riesgos de seguridad de la información, así como la adopción de la ISO 27799:2008 da orientaciones a organizaciones de salud sobre la mejor manera de proteger la confidencialidad, integridad y disponibilidad de la información de los pacientes, cualquiera que sea su forma de información (grabaciones, imágenes, números y palabras), cualquiera que sea el medio a utilizar para guardarla (escritura en papel, almacenamiento electrónico) ya que la información tiene que estar protegida siempre adecuadamente.

El estándar internacional 27001:2014, adopta el modelo PDCA (Planear-Hacer-Chequear-Actuar), el cual se puede aplicar a todos los procesos de Sistema de Gestión de Seguridad de Información.

También se ha considerado MAGERIT como una metodología de análisis y gestión de riesgos y finalmente COBIT 5 que, como marco de trabajo, ha proporcionado en su proceso APO13: Gestionar la Seguridad, la meta 10 y 14 referente a Seguridad de la Información, infraestructura de procesamiento y aplicaciones, y Disponibilidad de información útil y relevante para la toma de decisiones.

En resumen, después del levantamiento de datos mediante encuestas, entrevistas, reuniones y procesos de observación se elaboró la siguiente matriz (ver Figura 6) en donde se adaptan los siguientes estándares, marcos de trabajo y metodologías cada uno con sus respectivos ítem:

- NTP/IEC 27001:2014. [26]
- NTP: ISO 27005:2008. [27]
- COBIT 5: APO13: Gestionar la seguridad [28]
- ISO 27799: 2008 Seguridad de la Información en Salud.
- ISO 27002:2013 Controles de seguridad de la información y recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables
- Magerit: Metodologías de Gestión de Riesgos

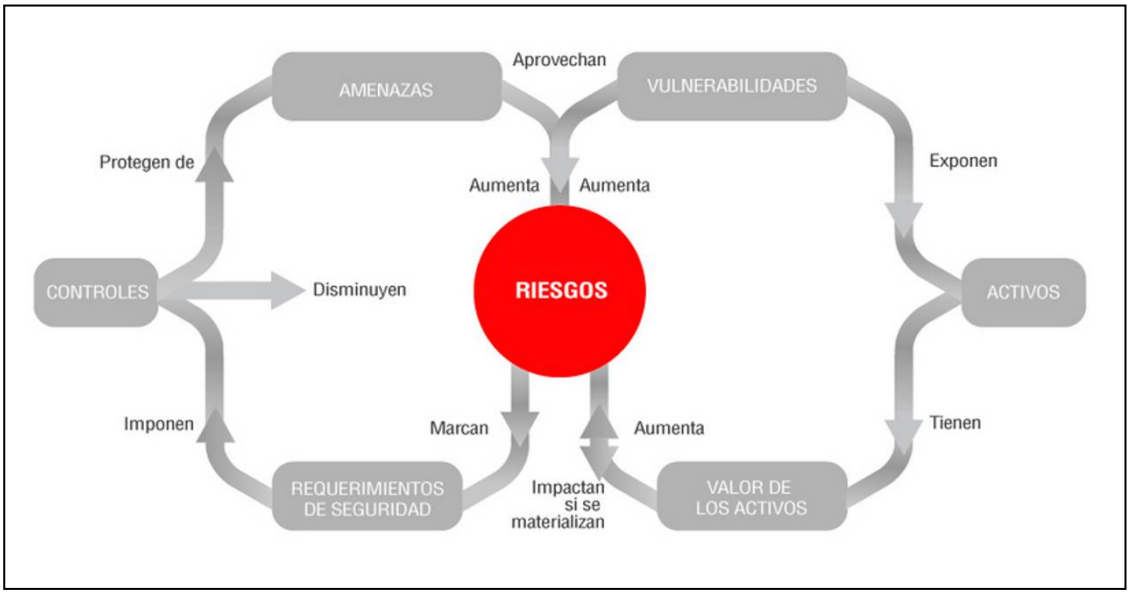
Figura 7: Matriz de adaptación de Normas, Estándares y Metodologías para la construcción del Modelo

ISO 27001:2014	ISO 27799:2008	ISO 27005:2011	ISO 27002:2013	MAGERIT
Alcance Referencias Normativas	Alcance			
	3.Terminos y definiciones de seguridad de la información en Salud		7. Seguridad de Recursos Humanos (06)	Dependencia de Activos
4.1 Contexto Interno 4.2 Contexto Externo			9. Seguridad de Control de Accesos (14)	Mapa de Calor
5. Compromiso y Liderazgo de los interesados			11. Seguridad física y ambiental (12)	Valoración del riesgo
5.2 Establecimiento de Políticas de Seguridad de la Información	5.1 Objetivos de Seguridad de la Información en Salud		12. Seguridad de las Operaciones (11)	Nivel de criticidad de los activos
5.3 Definición de Roles y Responsabilidades			13. Seguridad de las Comunicaciones (07)	Escala cualitativa de Probabilidad de Amenazas
	5.4 Información de Salud a proteger			Niveles de Impacto de amenazas
Tipos de Amenazas y Vulnerabilidades	5.5 Amenazas y Vulnerabilidades de seguridad de la Información en salud			Magnitud del Impacto
7.3 Formar y Concientizar personal	7.12 Conformidad de Requisitos Legales	8.2 Tratamiento del Riesgo		
9.2 Auditoría Interna		8.2.2 Identificación de Activos		
9.3 Revisión de Gestión		8.2.3 Amenazas 8.2.5 Vulnerabilidades		
10. Mejora Continua		8.3 Estimación del Riesgo		

Fuente: Elaboración propia

Se adaptó el proceso de análisis y gestión de riesgos que presenta Magerit para identificar los tipos de activos relevantes para la organización, valorar las dimensiones en caso se materialicen las amenazas, construir una escala para valorar los activos, identificar las posibles amenazas y determinar las salvaguardas frente a estas amenazas, las mismas que se presentan en el siguiente gráfico:

Figura 8: Análisis y Gestión de Riesgos



Fuente:Magerit [29]

Análisis:

Las instituciones de salud se preocupan hoy en día por la implementación de equipos biomédicos e incorporar con ello a los mejores especialistas ya que su principal preocupación es cuidar la salud de los pacientes, sin embargo, existen muchas amenazas que podrían acarrear problemas de imagen, presupuesto y cumplimientos legales.

Podemos comenzar aplicando la norma ISO 27001: 2014 basada en dos grandes pilares que la sostienen: investigar donde están los riesgos y luego tratarlos sistemáticamente, aplicando las medidas de seguridad que se van a implementar bajo la forma de políticas, procedimientos e implementación técnica.

La ISO 27001: 2014 Numeral 5 propone una lista de funciones que deben cumplirse por la Gerencia de la Institución para demostrar Liderazgo y compromiso con respecto al SGSI. Cláusula importante en el proyecto ya que tiene como objetivo asegurar que la Alta Dirección de la institución

ejerza una responsabilidad efectiva respecto al Modelo de Gestión de Seguridad de la Información.

Como parte de este liderazgo se debe comprender el contexto de la institución, así como se debe tener una visión clara de los objetivos estratégicos considerando los problemas internos y externos que puedan impactar en la planificación del SGSI, tener en cuenta los riesgos para después poder abordarlos, aplicar acciones y comprobar la efectividad de dichas acciones.

Durante las encuestas que se realizaron para conocer la institución de salud en estudio se consideraron los siguientes puntos claves para demostrar el compromiso de la Alta Dirección con el Sistema de Gestión de Seguridad de la Información:

1. Comunicación constante con la Alta Gerencia de la institución para que comprendan los riesgos y oportunidades que enfrentan respecto al Modelo a Implementar.
2. Alentar a las áreas la comunicación, esto ayudará a mejorar la reputación de la institución con sus clientes.
3. Comunicar a todos los colaboradores la importancia del Modelo a implementar, facilitar la participación de todos repartiendo y gestionando las responsabilidades.
4. Garantizar que las Políticas sean compatibles con la dirección estratégica y el contexto de la Institución.
5. Asignar recursos suficientes en todas las fases del Modelo de SGSI
6. Llevar a cabo revisiones periódicas del Modelo a implementar.

3.5 Modelo Propuesto de Gestión de Seguridad de la Información

En concordancia a la Resolución de Secretaría Gobierno Digital 002-2019-PCM/SEGDI 26-07-2019, se construyó el Modelo de Gestión de Seguridad de la Información (ver Figura 8), la misma que comprende los estándares necesarios para preservar la confidencialidad, integridad y disponibilidad de

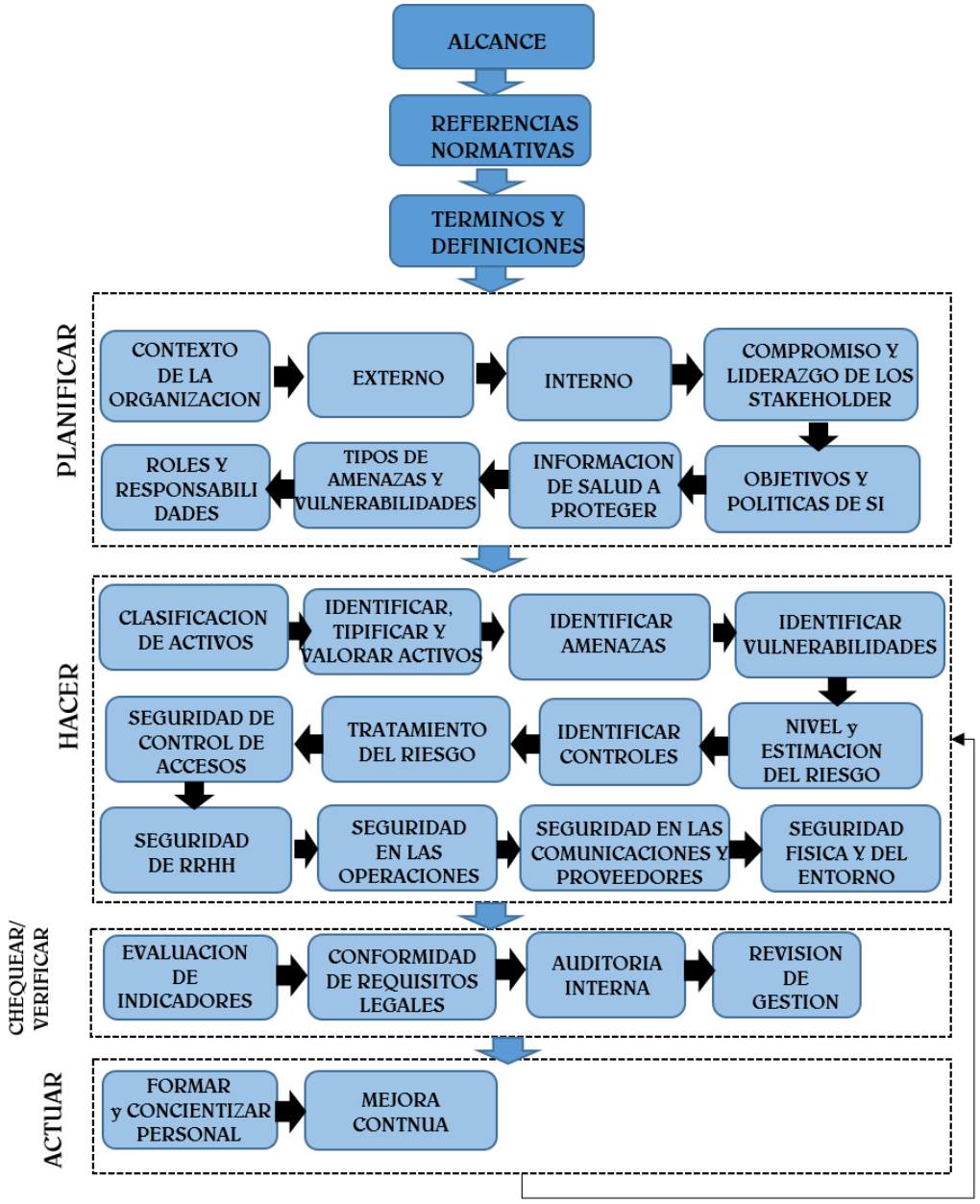
los datos e información que es intercambiada entre sistemas de información y que para nuestro caso permitió identificar los riesgos en los servicios de atención brindados y el resultado del análisis de riesgos con la finalidad de apoyar el proceso de atención al paciente en el caso de estudio.

Actualmente, el proceso de atención al paciente en sus diferentes actividades y servicios médicos está soportado por los sistemas de información institucional.
La funcionalidad básica de estos sistemas radica en la programación de consulta externa, generación de citas médicas, atención de Emergencia, Hospitalización, Centro Quirúrgico, Farmacia y almacenes, procesos de ayuda al diagnóstico, así como el procesamiento de las imágenes a cargo del servicio asistencial de Imagenología, dentro de éste marco se tiene como meta simplificar las tareas realizadas en las diferentes áreas de los servicios, así como brindar a la institución las herramientas e información necesarias para alcanzar sus objetivos institucionales trazados dentro de su plan de gestión.

Para la elaboración del Modelo de Gestión de la Seguridad de la Información se consideró aplicar el estándar internacional 27001: 2014 con la finalidad de aplicar los requerimientos de seguridad de la información para la institución y la necesidad de establecer una política y objetivos para la seguridad de la información, la norma ISO 27799:2008 se ocupa de las necesidades de gestión de seguridad de la información para el sector de la salud. Esta norma orienta a las organizaciones de salud a proteger la confidencialidad, integridad y disponibilidad de dicha información, adopta el modelo PDCA (Planear-Hacer-Chequear-Actuar), el cual se puede aplicar a todos los procesos de Sistema de Gestión de Seguridad de Información (ver figura 8).

En la figura 8 se muestra el Modelo de Gestión de Seguridad de la Información construido, indicando las actividades que lo conforman, el mismo que se implementó en el caso de estudio.

Figura 9: Modelo de Gestión de Seguridad de la Información a implementar



Fuente: Elaboración propia

3.6 Alcance del Modelo:

El presente modelo tiene por propósito generar una solución específica para una organización del sector de salud, tomando el proceso de atención al paciente en la Consulta Externa, en salvaguarda de la información clínica en los centros de salud ante cualquier amenaza, preservando su confidencialidad, integridad y disponibilidad.

La estructura del modelo se basó tanto en la ISO 27001:2014 (pag.3), como en la norma ISO/IEC 27799: 2008 (pag.1) la cual establece los requerimientos para una correcta implementación y gestión de un sistema de seguridad de la información en una institución de salud, en todos sus aspectos y en cualquiera sea la forma de la información (grabaciones, sonidos, videos e imágenes médicas), todos los medios que se utilizan para almacenarlo (impreso en papel o almacenamiento electrónico) y cualquier medio que se utilice para transmitirlo (a través de redes informáticas, por correo o en papel) siempre debe estar protegida adecuadamente. Esta norma en conjunto con la ISO 27002, agregan controles detallados para la gestión de seguridad de la información.

Están excluidos las siguientes áreas de seguridad en el modelo propuesto:

- Pruebas estadísticas para la anonimización eficaz de información personal de salud.
- Metodologías para seudónimos de información personal de salud (ISO /TS 25237, informática de la salud – seudonimización).
- Calidad de la red de servicio y métodos de medida de la disponibilidad de las redes utilizadas para la información de salud.
- Calidad de los datos.

El Modelo de Gestión de Seguridad de la Información para apoyar el proceso de atención al paciente propuesto se compone de las siguientes fases:

3.7 Fases del Modelo:

3.7.1 Fase 0:

Fase que se refiere a los términos de referencia del tema a abordar, así como conocer en el caso de estudio el soporte legal y normativo de la institución ya que se trata de una dependencia del Estado.

3.7.2 Contexto Externo

Se debe conocer el contexto interno y externo de la institución, y para ello se tomaron en consideración los Lineamientos de Gobierno Digital que dirigen, evalúan y supervisan a las instituciones estatales e internamente las directivas y normas de organización y funciones que permiten la atención integral de salud de su población como principal objetivo institucional.

Figura 10: Lineamientos de Gobierno Digital-Presidencia de Consejo de Ministros

Se construyeron las plantillas base para identificación del contexto externo

Plantilla para Contexto Externo de la Institución

Fase : Planificar – Contexto Externo de la Institución (plantilla)		
Nombre de la Institución: **Objetivo**: Identificar los aspectos externos que rigen e influyen en la institución. **Instrumentos**: Documentos normativos, entrevistas, visitas a superintendencias y otros organismos.		**Fecha de elaboración**: dd/mm/aa **Elaboración por**……. **Revisado por**…… …….
Nº	**Entorno**	**Aspectos identificados**
01	Reglamentario	Conjunto de exigencias legales como normas y lineamientos que rigen los procesos y procedimientos de atención
02	Político	Instituciones estatales y aspectos políticos que se relacionan con el cumplimiento de atención y seguridad de la información
03	Asociaciones y Colegios profesionales	Asociaciones que rigen los protocolos de manejo asistencial e Instituciones que rigen los aspectos de ética, derechos y deberes de los profesionales de salud.
04	Económico	Estados de gobierno que implantan las formas de financiamiento en las instituciones de salud (estatales, paraestatales y privadas)

Fuente: Elaboración propia

3.7.3 Contexto Interno

Cabe mencionar que en el contexto interno se revisó la siguiente fuente de información:

- Plan estratégico de la institución
- MOF de la institución (visión, misión, objetivos estratégicos)
- La estructura de la organización, funciones y responsabilidades.
- Normas y políticas adoptadas por la institución
- Organigrama actual.
- Sistemas de información.

Se ha considerado alinear las Políticas de Seguridad de la Información basado en normas internacionales propuestas en este estudio y los objetivos de seguridad de la información a los lineamentos estratégicos para el Gobierno Electrónico en el Perú aprobada mediante Decreto Supremo No.081-2013-PCM, el mismo que enfatiza la necesidad de velar por la integridad, seguridad y disponibilidad de los datos así como definir lineamientos en seguridad de la información para mitigar el riesgo de exposición sensible de los datos del paciente.

De manera que se integren los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización, tal como lo menciona en el capítulo III Art. 7 de sus funciones generales:"Formular y aprobar los estudios, investigaciones, documentos de gestión y reglamentos internos, así como otras normas que permitan ofrecer los servicios de manera ética, eficiente y competitiva".

Plantilla para elaborar el contexto interno de la Institución

Fase : Planificar – Contexto Interno de la Institución (Plantilla)		
Nombre de la Institución: **Objetivo**: Identificar los aspectos internos que rigen e influyen en la institución. **Instrumentos**: Se debe hacer uso de las fuentes de información de la institución (vía intranet).		**Fecha de elaboración**: dd/mm/aa **Elaboración por**: …… **Revisado por**:……
Nº	**Entorno**	**Aspectos Identificados**
01	Estructura funcional, cargos y responsabilidades	Todas las actividades, roles o tareas que la institución debe realizar, las cuales les permite alcanzar metas y objetivos estratégicos en el proceso de atención al paciente.
02	Objetivos y Estrategias	Propósito hacia donde la institución quiere llegar a través del servicio que ofrece a los pacientes.
03	Recursos y conocimientos	Capacidades, competencias, documentos, procedimientos e infraestructura tecnológica necesarios para el rendimiento de sus funciones en los procesos de atención al paciente.
04	Cultura de la Organización	Conocimientos, actitudes y experiencias conformado por el personal asistencial y administrativo que otorgan las prestaciones de salud.

Fuente: Elaboración propia

3.7.4 Liderazgo y Compromiso de los Stakeholder

Se construyó la plantilla para determinar el liderazgo y compromiso de los Stakeholder, de esta manera se pudo identificar el cumplimiento de las funciones de liderazgo de la Alta Gerencia.

Plantilla para identificar el compromiso y liderazgo de los Stakeholder

Fase – Planificar: Compromiso de liderazgo de los StakeHolder (plantilla)				
Nombre de la Institución: …….. **Objetivo**: Identificar **SI** los stakeholder cumplen con su compromiso y liderazgo, **NO** lo cumplen o lo realizan parcialmente.			**Fecha**: dd/mm/aa **Responsable**:…… …….. **Revisado por**:… ……	
Nº	**Funciones**	**SI**	**NO**	**PARCIAL**

Fuente: Elaboración propia

3.7.5 Definición de las Políticas y Objetivos de Seguridad de la Información en Salud

El establecimiento de Políticas de Seguridad de la Información es de vital importancia, dado que especifica los lineamientos generales de seguridad que deben ser cumplidos en la institución los cuales deben ir alineados a los objetivos del negocio.

Dado que se debe asegurar su cumplimiento, las Políticas de Seguridad de la Información debe ser aprobada por la Gerencia General que además tiene la obligación de comunicar la importancia que tiene la misma para alcanzar los objetivos trazados en la política.
Las políticas de Seguridad de la Información propuestas en el estudio se soportan en las siguientes bases:

- Los procesos de atención en servicios de salud se apoyan en los sistemas de información basados en sistemas de información los mismos que permiten procesar la información de los pacientes.
- Como institución de salud referencial dedicado al tratamiento de diagnósticos de alta complejidad y con un alto número de pacientes que se atienden en forma diaria urge la necesidad de proteger en todo su ámbito los datos personales y clínicos de los pacientes dentro y fuera de sus sistemas de información,
- La institución debe garantizar la confidencialidad de los datos personales y sensibles de sus pacientes en todo uso que a éstos se les pueda dar, siguiendo los lineamientos otorgados por la ley y el uso ético de los mismos [7]. Por este motivo se debe contar con el consentimiento informado del paciente en los casos de investigación previa comunicación del uso que se le dará a su información.
- Los usuarios internos deberán ser comunicados de la presente política de seguridad entendiendo la responsabilidad que tiene de manera individual en cuanto a la confidencialidad, integridad y disponibilidad de la información que maneja inherentes a sus funciones.

- De esta manera los colaboradores deben comprometerse con el cumplimiento de lo establecido, así como, con las políticas y procedimientos relacionados, tanto los vigentes como los que se publiquen posteriormente, comunicando de acuerdo al esquema de escalamiento definido aquellos casos en los que se encuentre un incidente.

  En el desarrollo del caso de estudio y de acuerdo a los controles utilizados se aplicaron las siguientes políticas:

  - Políticas de Seguridad en Recursos Humanos.
  - Políticas de Seguridad en Control de Accesos.
  - Políticas de Seguridad de las Operaciones.
  - Políticas de Seguridad de las Comunicaciones.
  - Políticas de Seguridad Física y del Entorno.

El formato elaborado para ésta actividad se puede apreciar en la siguiente plantilla:

Plantilla para establecer las Políticas de Gestión de Seguridad de la Información

Establecer Políticas de Gestión de Seguridad de la Información (plantilla)					
Nombre del documento……... Objetivo: Identificar las políticas de seguridad de acuerdo a las necesidades de la institución Método de recolección: Entrevistas, observación y revisión de documentos internos de la institución.				Fecha: dd/mm/aa Elaborado por……..... Revisado por…….	
Nº	**Políticas de Seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles**

Fuente: Elaboración Propia

3.7.6 Objetivos del Modelo de Seguridad de la Información:

- Ofrecer un servicio de calidad a los pacientes garantizando que se apliquen los controles necesarios para asegurar su información.
- Cumplir con los requerimientos legales en cuanto a la protección de la información del paciente.
- Establecer y monitorear el Modelo de GSI que identifique los riesgos a los que se expone la información de la institución y se pueda definir controles para los mismos.
- Concientizar al personal sobre la importancia de gestionar la seguridad de la información, así como su responsabilidad sobre el cumplimiento de lo dispuesto.
- Definición de roles y responsabilidades de los colaboradores, jefes de servicio, jefes de departamento, gerentes de línea y otros funcionarios, frente a la seguridad de la información.

Cabe mencionar que la ampliación de la documentación a recolectar generada a partir del modelo propuesto dependerá de las necesidades particulares de cada organización.

3.7.7 Instrumentos de Recolección de Información

Para el desarrollo del Modelo de Sistema de Gestión de Seguridad de la Información propuesto, se estableció que los mecanismos e instrumentos para la recolección de la información son los siguientes:

- Observación
- Entrevistas con funcionarios y usuarios internos que tienen como principal función la atención al paciente.
- Documentación interna de la entidad.
- Fuentes de información como normas, marcos de referencia, directivas, resoluciones existentes tanto en medio físico como electrónicos y publicados en la intranet de la institución.

En ésta etapa de Planificación se elaboraron los instrumentos de recolección de datos, así como se identificó la información de salud a proteger de los diferentes procesos de atención al paciente los mismo que se detallan en la siguiente tabla:

3.7.8 Información de Salud a Proteger

Plantilla para definir la información de salud a proteger

Definición de la Información de Salud a proteger		
No.	Datos a proteger	Contenido
1	Toda información que contenga datos clínicos del paciente en papel o electrónica, con formatos institucionales, relacionada a metas e indicadores hospitalarios, y/o de cumplimiento legal.	Detalle de la información, como por ejemplo datos personales del paciente, resultados de exámenes clínicos, indicaciones farmacológicas, orientaciones de prescripciones, información de terceros que brindan servicios de salud, etc.

Fuente: Elaboración propia

3.7.9 Tipos de Amenazas y Vulnerabilidades

Una amenaza es toda acción que aprovecha una vulnerabilidad y que significa un riesgo para la seguridad de la información y las vulnerabilidades, se consideran como una falencia que puede ser explotada, las cuales fueron identificadas por los colaboradores de las áreas de tecnologías de información para luego analizarlas, gestionarlas, tratarlas y establecer controles que permitan mitigarlas, transferirlas, evitarlas o aceptarlas.

En ésta etapa se describen el origen de las amenazas, las cuales podrían ser de origen natural, de origen industrial, errores y fallos no intencionales ó ataques intencionados.

Se listan las amenazas y las vulnerabilidades considerando el contexto de la institución, en las siguientes tablas:

Listado de Amenazas

N°	Amenazas
1	Desastre natural
2	Incendios
3	Daños por inundaciones
4	Avería de origen físico o lógico
5	Errores en los usuarios
6	Errores del adminstrador
7	Errores de configuración
8	Escapes de información
9	Alteración accidental de información
10	Destrucción de la información
11	Errores de mantenimiento / actualización de programas
12	Pérdida de equipos
13	Indisponibilidad del personal
14	Suplantación de identidad del usuario
15	Abuso de privilegios de acceso
16	Accesos no autorizados
17	Interceptación de información
18	Destrucción de información
19	Divulgación de información
20	Manipulación de equipos
21	Robo
22	Ataque a bases de datos bajo petición de rescate
23	Ataque a servidores bajo petición de rescate

Fuente: Elaboración propia

Listado de Vulnerabilidades

N°	Vulnerabilidades
1	Falta de Políticas para la Seguridad de la Información
2	No cuenta con responsables asignados para la SI
3	Escasa conciencia, educación y capacitación en seguridad de la información
4	No se informa inmediatamente los ceses, rotaciones o cambios de puestos de trabajo del personal.
5	No cuenta con inventario de activos actualizado
6	Existe un debil control para el acceso a redes y servicios asociados
7	No realizan la gestión de los roles de los usuarios con privilegios especiales
8	No realizan la validación y seguimiento sobre los privilegios de los usuarios en los roles asignados
9	No existe concientización del usuario para mantener la confidencialidad de sus contraseñas
10	Falta de control de acceso a los sistemas y aplicaciones mediante un procedimiento seguro de logeo
11	No se han definido perimetros de seguridad física para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.
12	No han establecido controles de ingreso en áreas restringidas
13	No han establecido procedimientos para la protección de los activos de amenazas externas y/o ambientales
14	No existe una diferencia entre los ambientes asignados para el área de desarrollo, pruebas y producción.
15	No existe control para la deteccion, prevención y recuperación ante afectaciones de malware.
16	No se realiza la planificación de controles de auditoria en los sistemas de información, con el fin de mantener la continuidad del negocio.
17	No existen procedimientos para mantener un registro sobre el control de cambios realizados en los sistemas
18	No se informa las debilidades sospechosas en la seguridad de la información en los sistemas o servicios tanto a los empleados como a proveedores que utilizan los sistemas y servicios de información de la institución
19	No se realizan auditorias internas y externas para supervisar y revisar las políticas de la seguridad de la información establecida.

Fuente: Elaboración propia.

En el caso de estudio se pudo observar que las atenciones en consulta externa, hospitalización y emergencia son los procesos más críticos identificándose a la historia clínica como el activo más importante en cada uno de ellos. Este documento de carácter Médico-Legal se ve expuesto a distintos riesgos.

3.8 Roles y Responsabilidades

Se definieron roles y responsabilidades de acuerdo a sus funciones, indicando nivel de implicancia. de esta manera se establecieron roles a cada uno como : Responsable (R), Aprobador (A), Consultado (C) e Informado (I), en donde el responsable es el encargado de hacer la tarea, aprobador es el que aprueba el trabajo realizado por el responsable, consultado son aquellas personas que son consultadas sobre el tema tener en cuenta que son ellos los expertos en la materia e Informado son aquellas personas a las que hay que mantener informadas sobre la evolución de la tarea, lo usual es cuando se haya terminado la tarea. Para ésta actividad se elaboró la siguiente plantilla.

Tabla 1: Identificación de Roles y Responsabilidades

Fase Planificar: Identificación de roles y responsabilidades (plantilla)		
Elaborado por: **Registrado por**: **Objetivo**: Identificar los roles y las responsabilidades		**Fecha**: dd/mm/aa
Descripción: Para la recolección de información se debe hacer uso del Manual de Organización y Funciones de la institución		
Rol	**Responsabilidad**	**Nivel de implicancia**
Identificar el rol o cargo del personal involucrado en la atencion al paciente	Identificar las funciones asociadas a cada rol del personal involucrado en la atención al paciente	Indicar el nivel de implicancia del personal mediante la siguiente calificación: **(A)** Responsable de aprobarlo. **(R)**Responsable de hacerlo. **(C)**Consultado. **(I)**Informado.

Términos y condiciones de empleo

Los términos y condiciones de empleo deberán estar comunicados por la Oficina de Recursos Humanos mediante correo electrónico institucional y el personal nuevo a laborar deberá apersonarse a la oficina de TI para su registro, generación de su acceso y contraseñas, así como para el cumplimiento de sus funciones respecto al uso de los sistemas de información dentro de la institución.

El término del contrato de trabajo con la institución implica el cumplimiento de los procesos de entrega de activos de información y remoción de privilegios sobre la plataforma tecnológica de la entidad.

Como resultado de la implementación de la plantilla de roles y responsabilidades se obtuvo la matriz RACI (ver anexo 6).

3.8.1 Identificar, Clasificación y Valorar activos

En esta fase se identificaron los activos que sostienen la operatividad de los servicios que la institución brinda a su población de pacientes, asi también se identificaron los procesos del negocio, los servicios médicos que brindan, los sistemas de información y los servicios de TI que dan el soporte tecnológico para la atención al paciente.

La clasificación de activos se realizó considerando todos aquellos recursos que para la institución en estudio tienen valor y que necesiten ser protegidos de potenciales riesgos.

Se clasificaron los activos por categorías según su naturaleza y de la siguiente manera:

- Datos, Software, Hardware, Redes, Tecnología, Personal, Instalaciones, Equipamiento auxiliar.

La clasificación de activos para la institución en estudio se realizó de la siguiente manera:

Tabla 2: Clasificación de Activos

COD_ACTIVO	DETALLE
D_activo	Todos aquellos datos (en cualquier formato) que se genera, gestionan, procesan, transmiten.
HW_activo	Elementos físicos de Hardware que soportan la ejecuciónn de las aplicaciones informáticas y los sistemas de información
SW_activo	Programas o aplicativos que gestionan, analizan y transforman los datos, permitiendo la explotación de la información para la prestación de los servicios.
EB_activo	Equipos biomédicos que procesan información y que permite a la institución prestar sus servicios al paciente y que es transmitida a través de redes.
SI_activo	Sistemas de Información que dan soporte al procesamiento de la información del paciente.
Media_activo	Soportes de información: dispositivos físicos.
I_activo	Áreas o instalaciones donde se ubican los equipos de computo, comunicaciones y de atención al paciente.
P_activo	Usuario (personal) que labora en la institución y que tiene acceso a los sistemas de información.
Red_activo	Red de datos que permite intercambia información (intranet, internet, etc).
SF_activo	Seguridad física de las instalaciones de la institución

Los Procesos del Negocio, conformado por actividades administrativas que relacionadas entre sí, dan el soporte de gestión necesarios y correspondiente para apoyar los procesos de atención al paciente (ver tabla 3).

Tabla 3: Procesos del Negocio

N°	Procesos del Negocio	Código
1	Proceso Logística y Adquisiciones	[P_Log]
2	Proceso de Finanzas	[P_Fin]
3	Proceso de Administración	[P_Adm]
4	Proceso de Gestión Calidad	[P_GC]
5	Proceso de Recaudación	[P_SyR]
6	Proceso de Capacitación e Investigación	[P_CapInv]
7	Proceso de Admisión y Registros Médicos	[P_AyRM]
8	Proceso de Recursos Humanos	[P_RH]
9	Proceso de Ingeniería	[P_IH]
10	Proceso de Control Interno	[P_CI]
11	Proceso de Planificación Operativa	[P_OPO]
12	Proceso de Cobranzas Coactivas	[P_CCoact]
13	Proceso de Costos	[P_Costos]

Fuente: Manual de Normas y Procedimientos

Los Servicios Médicos, conformados por grupos de actividades relacionados entre sí, y que producen servicios de atención al paciente, los cuales se identificaron mediante la siguiente tabla:

Tabla 4: Servicios Médicos

No.	Servicio Médico	Código
1	**Servicio de Consulta externa**	**[SA_Cext]**
2	Servicio de Emergencia	[SA_Eme]
3	Servicio de Hospitalización	[SA_Hos]
4	Servicio de Especialidades Médicas	[SA_EM]
5	Servicio de Ayuda al diagnóstico	[SA_AdyT]
6	Servicio de Cuidados Críticos	[SA_UCI]
7	Servicio de MO	[SA_TMO]
8	Servicio de Nefrología y TR	[SA_UTR]
9	Servicio de Radioterapia	[SA_RadT]
10	Servicio de Quimioterapia	[SA_QT]
11	Servicio de Especialidades Quirurgicas	[SA_EQx]
12	Servicio de Centro Quirúrgico	[SA_CQx]
13	Servicio de Especialidades Pediátricas	[SA_EPd]
14	Servicio de Hemodialisis	[SA_Hemo]
15	Servicio de Rehabilitación	[SA_Reha]
16	Servicio de Programas Especiales	[SA_PEsp]
17	Servicio de Endoscopia	[SA_Endos]

Fuente: Manual de Organización y Funciones

Los Sistemas de Información, conformados por un conjunto de programas de cómputo, que permiten una gestión integrada de factores que inciden en la institución de salud y dan soporte a los servicios médicos y administrativos, se identificaron en la siguiente tabla:

Tabla 5: Sistemas de Información Institucionales

No.	Sistemas de Información	Código
1	Sistema de Gestión de Servicios de salud	[SI_SISS]
2	Sistema de Imagenología (Picture Archiving and Communications System) Sistema de almacenamiento y Comunicación de imágenes	[SI_Pac]
3	Sistema de Gestión Hospitalaria	[SI_SGH]
4	Sistema de Referencias	[SI_Ref]
5	Sistema de Administración	[SI_SID]
6	Sistema de Acreditación	[SI_Acredita]
7	Sistema de Anatomía Patológica	[SI_AP]
8	Sistema de Patrimonio	[S_Patri]
10	Sistema de Logística	[S_Logis]

Fuente: Oficina de Soporte Informático

Los servicios de Tecnologías de la Información que permiten dar solución a las necesidades de los usuarios, para el presente modelo se identificaron de la siguiente manera:

Tabla 6: Identificación de Servicios de TI

No.	Servicios	Código
1	Servicio de correo electrónico	[S_email]
2	Servicio de Citas en Linea	[S_CenLin]
3	Servicio de Acreditación	[S_Acreditación]
4	Servicio de Tramite de Subsidio por Lactancia	[S_TramLact]
5	Servicio de Consulta de Referencias y Contrareferencias	[S_CRyC]
6	Servicio de Telefonía	[S_Central]
7	Servicio de Telemedicina	[S_Telmed]

Fuente: Elaboración propia

La valoración se realizó en base a los criterios definidos para cada dimensión: Confidencialidad, Integridad, Disponibilidad, asignándole el valor de acuerdo al grado de importancia, para este proceso se utilizó la Escala de Likert, midiendo el grado de conformidad con respecto a cada criterio. (ver tabla 7).

Tabla 7: Dimensiones en Seguridad de la Información

Valor en escala Likert	Dimensiones en Seguridad de la Información		
	Confidencialidad	Integridad	Disponibilidad
1	La publicación o filtración de la información no presenta un riesgo para la organización. Se puede considerar como información de dominio público.	Si la información presentada en el activo no es correcta o tiene un porcentaje de error del 25% no presenta un riesgo para la organización dado que no afecta de manera crítica las actividades de la misma.	En caso se requiera el activo de Información debe poder ser accesible un 25% de las ocasiones en que se haga necesario, sin embargo su No disponibilidad por distintos factores no se considera un riesgo.
2	El activo de información debería ser sólo de uso interno a la organización, sin embargo, su filtración no supone un riesgo o un daño para la misma.	Se requiere que el activo tenga un porcentaje de error como máximo del 50%, dado que un porcentaje mayor podría perjudicar a la organización.	El activo de información debe ser accesible el 50% de las veces en que se requiera, caso contrario podría perjudicar de manera leve a la organización.
3	El activo de información contiene información de índole privada, debiendo establecer controles para el acceso al mismo. Su filtración supone un riesgo moderado para la organización.	El activo de información debe contener información correcta en un 75%, caso contrario se podría generar un daño moderado a la organización o incluso iniciar acciones legales contra la misma.	Se requiere que sea accesible el 75% de las ocasiones en que se necesite, de lo contrario se perjudica moderadamente los procesos de negocio asociados al mismo pudiendo conllevar a consecuencias legales.
4	La información contenida por el activo es altamente sensible y debe ser protegida contra cualquier posible filtración, caso contrario los dueños de la información Contenida pueden ser afectados y la organización ser demandada o multada.	La información no debe contener errores, de otro modo se afecta seriamente los procesos de negocio asociados, siendo susceptible la organización a ser demandada o multada.	La información contenida en el activo de información no puede ser inaccesible dada su criticidad. Su no disponibilidad se traduce en una paralización de las actividades asociadas ocasionando pérdidas serias o acciones legales en contra de la organización.

Fuente: Elaboración Propia

Para la valoración de activos se tuvo en cuenta las siguientes dimensiones:

- **Disponibilidad (D):** es el acceso y utilización de la información por parte de los individuos, entidades o procesos autorizados sólo y en el momento de ser solicitado por una persona autorizada. [30]
- **Confidencialidad (C)**: Información disponible exclusivamente a personas autorizadas. [30]
- **Integridad (I)** : Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas. Contra la integridad la información puede parecer manipulada, corrupta o incompleta. [30]

La suma de las tres dimensiones determinará el nivel de criticidad del activo valorado según el siguiente anexo:

Nivel de Criticidad del activo valorado

Valor	Nivel
1 - 3	Muy bajo
4 - 6	Bajo
7 - 9	Alto
10 - 12	Muy alto

Fuente: Elaboración propia

Luego, se debe valorar los activos mediante la siguiente tabla y de acuerdo a su prioridad.

Plantilla para valoración de activos

Fase Hacer: Valoración de Activos (plantilla)							
Registrado por: **Aprobado por**:						Fecha: dd / mm / aa	
Objetivo: Identificar el nivel de criticidad de cada activo **Descripción**: Para el desarrollo de ésta actividad se extraen los activos de la plantilla de identicación de activo							
N°.	Cod. Activo	Activo	Criterio			Total	Nivel
			(D)	(I)	(C)		
01							
02							
….							

Fuente: Elaboración propia.

Se aplicó el nivel de criticidad de los activos y se obtuvieron las calificaciones para cada criterio de seguridad de la siguiente manera:

Valoración = Disponibilidad+Integridad+Confidencialidad, obteniendo de ésta manera los niveles de: Muy bajo (MB), Bajo(B), Alto(A), Muy Alto(MA).

3.8.2 Dependencia de Activos:

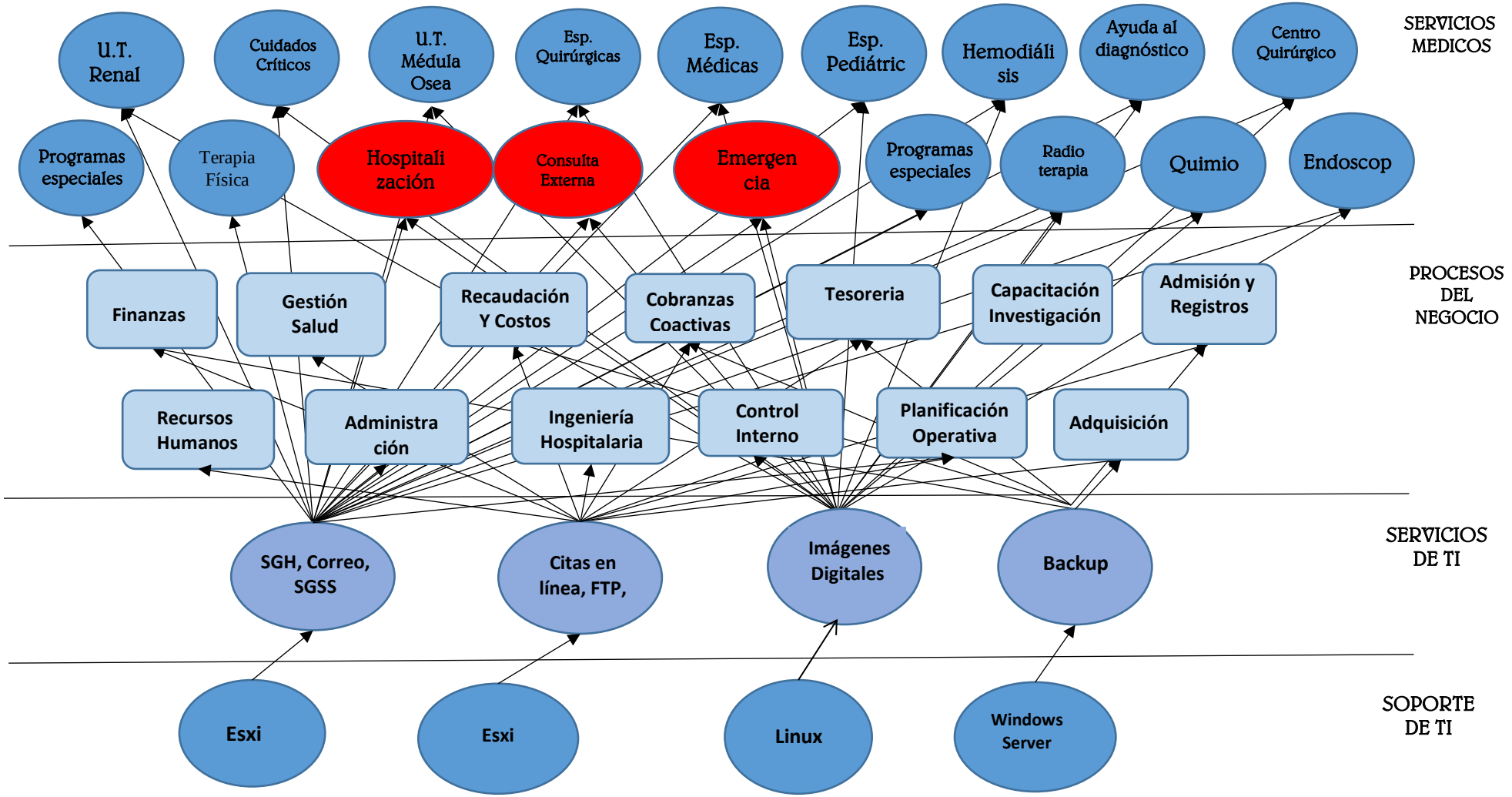
En ésta fase se elaboró la dependencia de activos y su interacción con los servicios de TI, servicios médicos y procesos del negocio, así como el soporte tecnológico de la institución. También se pudo apreciar el grado de importancia y el valor de proteger los activos de TI, que soportan las categorías identificadas, teniendo en cuenta los criterios de disponibilidad, integridad y confidencialidad de seguridad de la información.

Es importante mencionar, el alto grado de dependencia de los sistemas de información hospitalaria para otorgar la atención al paciente en cualquiera de las actividades asistenciales, de los cuales depende lo siguiente:

- Llevar un control de todos los servicios otorgados a los pacientes.
- Obtener indicadores hospitalarios mensualmente en cumplimiento de normas y directivas institucionales.
- Obtener datos epidemiológicos, para la toma de decisiones.
- Obtener costos de la atención en los casos de atenciones particulares.
- Mantener un expediente clínico electrónico disponible e íntegro.
- Obtener datos del tratamiento del paciente en otros centros asistenciales de la misma entidad.
- Acceso seguro, inmediato y eficiente respecto a la terapéutica médica del paciente.
- Información precisa sobre los procesos de acreditación.

Como resultado se obtuvo la siguiente figura:

Figura 11: Dependencia de Activos



Fuente: Elaboración propia

Para identificar la relación de dependencia de los activos se tuvo en cuenta lo siguiente:

1. Identificación de los activos: Se deben identificar todos lo recursos que se utilizan para que la institución funcione y consiga el cumplimiento de sus objetivos estratégicos propuestos por la alta dirección, y que están asociados a los procesos del negocio, servicios médicos y sistemas de información, de la institución de salud, realizado a través de un inventario por la oficina de TI (ver siguiente plantilla).

FASE : Hacer Identificación de Activos (plantilla)	
Nombre de la Institución……. Elaborado por……Aprobado por: …….	Servicio…….. . Fecha: dd/mm/aa
Objetivo: Identificar los activos presentes en las diferentes áreas de trabajo asistencial y de procesamiento de la información del paciente.	
Descripción: Para recoger la información se puede hacer uso de la observación directa.	

Nº	Categoría de los Activo	Activo	Código_activo	Descrip.	Responsable
01	Hardware	Son los elementos físicos de hardware que soportan la ejecución de las aplicaciones informáticas y el procesamiento o la transmisión de la información.	[HW_activo]	Men-cionar la función del activo	Personal responsable a cargo del activo
02	Software	Son los programas o aplicativos que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios	[SW_activo]		
03	Sistemas de Información	Son las funcionalidades que satisfacen una o varias necesidades de los usuarios. (sistemas institucionales)	[SI_activo]		
04	Datos	Los datos que contienen información de los pacientes almacenada en equipos.	[Datos]		
05	Soportes de información	Se consideran los dispositivos físicos que permiten almacenar información de forma permanente o, al menos durante largos periodos de tiempo. (DD, USB)	[Media_activo]		
06	Instalaciones	Son los lugares donde se hospedan los sistemas de información y comunicaciones.	[L_activo]		
07	Seguridad física	Seguridad física de las instalaciones de la institución	[SF_activo]		
08	Personal	Son las personas que laboran en la organización relacionadas con los sistemas de información.	[P_activo]		
09	Redes	Dispositivos de conectividad (routers, switches, concentradores, etc)	[Red_activo]		
10	Equipos auxiliares	Equipamientos auxiliares que complementan el material informático (equipos en sesión de uso)	[EA_activo]		

Fuente: Elaboración propia

2. Construir las líneas de dependencia: Se establecieron las líneas de dependencia entre las categorías identificadas, resaltando los servicios médicos de mayor demanda en la institución en estudio como son la Consulta Externa, Emergencia y Hospitalización, determinándolos como críticos y el impacto que podría representar en cualquiera de ellos al materializarse una amenaza.

3.8.3 Identificación y Valorización de Amenazas

Después de identificar, tipificar y valorar los activos de la institución, ésta etapa permitió identificar sobre ellos, las amenazas y vulnerabilidades asociadas. Se identificaron las posibles amenazas que pueden aprovechar las vulnerabilidades existentes las mismas que se registraron usando la siguiente plantilla.

Plantilla para Identificación de Amenazas y Vulnerabilidades

Identificación de Amenazas y Vulnerabilidades (plantilla)					
Registrado por:_____					**VoBo:** **Fecha:** **dd/mm/aa:**
Objetivo: Identificar las amenazas y vulnerabilidades de cada activo identificado.					
Descripción: Para el desarrollo de esta actividad se ubica el activo identificado en la lista de amenazas y vulnerabilidades.					
No	**Cod. Activo**	**Activo**	**Amenazas**	**Vulnerabilidades**	**Medidas Recomendadas**

Fuente:Elaboración propia.

Las amenazas se pueden agrupar de la siguiente manera:

- Amenazas Cibernéticas (AC)
- Amenazas Humanas (AH)
- Amenazas de Interoperabilidad (AI)
- Infraestructura Crítica (IC).

Se identificaron las amenazas para cada activo de información así como las medidas recomendadas.

3.8.4 Nivel de Estimación del Riesgo

En ésta etapa se estima el nivel de riesgos proveniente de las amenazas asociadas a los activos de la información ya identificados.

Valoración de la probabilidad del riesgo

Para realizar ésta actividad y después de haber identificado las amenazas que pudieran causar daño a un activo de información, debemos valorar la probabilidad de ocurrencia de dicha amenaza en razon a las vulnerabilidades que se tengan: Magerit proporcionó los niveles de probabilidad que se utilizaron para estimar la probabilidad de ocurrencia de las amenazas, los niveles son los siguientes:

Escala Cualitativa de Probabilidad de Amenazas

Escala	Probabilidad	Descripción
5	**MA**: Prácticamente seguro	El evento puede ocurrir más de una vez al año
4	**A**: Probable	El evento puede ocurrir una vez al año
3	**M**: Posible	El evento puede ocurrir al menos una vez cada 2 años
2	**B**: Poco probable	El evento puede ocurrir una vez cada 5 años
1	**MB**: Muy raro	El evento no se ha presentado en los últimos 5 años

Fuente: Magerit 3.0

Valoración del impacto del riesgo:

Asimismo, se estimó el nivel de impacto que pueda alcanzar una amenaza, al aprovechar las vulnerabilidades asociadas a un activo de información. Magerit proporcionó el nivel de las escalas o niveles de impacto que se utilizaron para estimar la probabilidad de ocurrencia de una amenaza, los cuales se pueden apreciar en el siguiente cuadro.

La asignación de la escala estuvo a cargo del responsable del área de Soporte Informático.

Niveles de impacto de amenazas

Escala	Impacto	Descripcion
5	**MA**: Muy alto	El evento puede ocurrir más de una vez al año
4	**A**: Alto	El evento puede ocurrir una vez al año
3	**M**: Medio	El evento puede ocurrir al menos una vez cada 2 años
2	**B**: Bajo	El evento puede ocurrir una vez cada 5 años
1	**MB**: Muy bajo	El evento no se ha presentado en los últimos 5 años

Fuente: Magerit 3.0

Valoración de la magnitud del riesgo

Para determinar la magnitud del riesgo se tiene que:

Riesgo = Probabilidad x Impacto

Se utilizó la siguiente escala del 1 al 25

Magnitud del impacto

Valor	Magnitud
1 – 5	Baja
6 – 10	Media
11 – 15	Alta
16 – 25	Crítica

Fuente: Magerit 3.0

Utilizando la siguiente plantilla se elaboró el análisis del riesgo:

Plantilla para realizar el Análisis del Riesgo

Fase Hacer: Análisis del Riesgo (plantilla)								
Nombre de la Institución……. **Elaborado por**…… **Aprobado por**…… **Objetivo**: Determinar el análisis del riesgo **Descripción**: Para el desarrollo de esta actividad se hace uso del resultado de la plantilla de identificación de amenazas y vulnerabilidades.							Fecha de registro: dd/mm/aa	
Nº	**Activo**	**Amenaza**	**Vulnerabilidad**	**P**	**I**	**Valor (PxI)**	**Código de riesgo**	**Magnitud**
Conclusión: se realiza en análisis o comentario final de lo percibido después de almacenar la información en esta tabla.								

Fuente: Elaboración propia

Para estimar el nivel del riesgo se utilizó la siguiente matriz de riesgos:

Mapa de Calor

PROBABILIDAD de OCURRENCIA							
	Seguro	5	5	10	15	20	25
	Probable	4	4	8	12	16	20
	Posible	3	3	6	9	12	15
	Poco Probable	2	2	4	6	8	10
	Muy Raro	1	1	2	3	4	5
			1	2	3	4	5
			Muy bajo	Bajo	Medio	Alto	Muy alto
			IMPACTO				

Fuente: elaboración propia.

Se utilizaron los siguientes valores para identificar la tolerancia al riesgo [32](pag.123).

Identificación de Tolerancia al riesgo

Valor del riesgo	Tolerancia al riesgo	Descripcion
1 – 6	Aceptable	El riesgo es aceptable tal y como existe
7 – 13	Tolerable	El riesgo es tratado basado en la mitigación
14 - 25	No tolerable	El riesgo es inaceptable por pérdidas extremadamente mayores.

Fuente: Elaboración propia.

Y finalmente en la siguiente plantilla, se realiza la evaluación del riesgo, de manera que se determine si el riesgo es aceptable, tolerable, moderado o no tolerable.

Plantilla para Evaluación del Riesgo

<table>
<tr><th colspan="8">Fase – Hacer: Evaluación del riesgo (plantilla)</th></tr>
<tr><td colspan="6">Nombre de la Institución……
Elaborado por……..
Aprobado por……
Objetivo: Determinar la evaluación del riesgo
Descripción: Para el desarrollo de ésta actividad se hace uso del resultado de la plantilla del análisis del riesgo</td><td colspan="2">Fecha: dd/mm/aa</td></tr>
<tr><th>Cod. Riesgo</th><th>Magnitud</th><th>Activo</th><th>Amenaza</th><th>Vulnerabilidad</th><th>Valor (PxI)</th><th>Tolerancia</th><th>Observación</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="8">Conclusiones: se realiza el comentario y análisis de lo percibido.</td></tr>
</table>

Fuente: Elaboración propia.

3.8.5 Tratamiento del Riesgo

Luego de realizar la evaluacion de los riesgos en la institución se aplicó un proceso de tratamiento de riesgos de la seguridad de la información. Dentro de las estrategias de llevar el tratamiento del riesgo estan:

Eliminación: Consiste en eliminar la amenaza eliminando la causa que puede provocarla. Prevenir la materialización del riesgo retirando una actividad o un conjunto de actividades planificadas o existentes.

Transferencia: Subcontratar un servicio que pueda manejar de manera más eficaz el riesgo en particular.

Mitigar: Busca disminuir el impacto y la probabilidad del riesgo se aplica implementación de controles. Para llevar a cabo la mitigación de riesgos es necesario: seleccionar, implantar y verificar los controles y establecer indicadores. La selección de los controles se podrá realizar utilizando como referencia la norma ISO/IEC 27002:2013.

Aceptación del riesgo:Los daños ocasionados por la materialización del riesgo no son significativos y no es necesario implementar controles adicionales.

Para el tratamiento de los riesgos se debe: "1)Aplicar los controles apropiados; 2)aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo de la organización; 3) evitar los riesgos; y 4) transferir los riesgos comerciales asociados a otras entidades; por ejemplo: aseguradoras, proveedores." [31]

Para el tratamiento del riesgo se elaboró la siguiente plantilla:

Fase – Hacer: Tratamiento del riesgo (plantilla)					
Nombre de la Institución:…… **Elaborado por:**…….. **fecha: dd/mm/aa** **Aprobado por**: **Objetivo**: Establecer la evaluación del riesgo. **Descripción**: Para el desarrollo de ésta acción se hace uso de las amenazas identificadas en el análisis del riesgo y se proponen los controles.					
Cod. Riesgo	**Magnitud**	**Tolerancia**	**Amenaza**	**Estrategia**	**Controles**
Conclusiones: Se realiza el comentario final de lo percibido después de llenada la plantilla.					

Fuente: Elaboración propia

El objetivo del tratamiento del riesgo es definir la estrategia a aplicar, los controles, actividades y los recursos que se necesitan para implementar el modelo de SGI, para tal actividad se elaboró la plantilla de identificación de recursos.

Plantilla para identificación y descripción de recursos para el modelo de GSI

Identificación y descripción de recursos para el modelo de GSI (plantilla)							
Registrado por:…… **Objetivo**: Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados **Descripción**: Para el desarrollo de esta actividad se debe elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							**Fecha**: dd/mm/aa
Cod.del riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**

Fuente: Elaboración propia

3.8.6 Identificar Controles

Los controles fueron seleccionados e implementados de acuerdo a los requerimientos identificados por la valoración del riesgo y los procesos de tratamiento del riesgo.

Según la ISO/IEC 27001, "Un control es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable" [32], para ello se necesita conocer a las personas responsables que intervienen en la comunicación de los controles a implementarse en la siguiente plantilla

Plantilla para Comunicar Controles

Comunicación de Controles (plantilla)					
Registrado por:……. **Objetivo**: Informar a la gerencia y al personal de la organización los controles a implementar				**Fecha:** **dd/mm/aa**	
Descripción: Para el desarrollo de esta actividad se deben seleccionar medios de comunicación para cada control.					
Controles	**Actividades**	**Riesgos asociados**	**A quien comunicar**	**Quien debe comunicar**	**Tipo de comunicación**
Lista de controles a implementar	Actividades para lograr la implementación de los controles.	Riesgos a tratar.	Área o persona a quien comunicar el control a implementar	Responsable de comunicar el control a implementar	Documento escrito, email.

Fuente: Elaboración propia

3.8.7 Seguridad de Recursos Humanos

Este grupo cubre nueve controles (ISO 27799:2008) y también se encuentran considerados:

Antes del empleo: Responsabilidades y roles, verificaciones curriculares, términos y condiciones de empleo.

Durante el empleo: Administración de responsabilidades, preparación, educación y entrenamiento en seguridad de la información, medidas disciplinarias.

Finalización o cambio de empleo: Finalización de responsabilidades, devolución de recursos, revocación de derechos.

La Seguridad de los Recursos Humanos es un gran ausente en las instituciones del sector, se trata pues, de realizar un serio trabajo entre RRHH y los responsables de Seguridad de la Información de la institución en estudio. Se debe partir por la redacción de la documentación necesaria para la contratación de personal y la revocación de sus contratos (por renuncia, cambio o despido). En la cual debe quedar bien claro las acciones a seguir para los diferentes perfiles de la Organización, basados en la responsabilidad de manejo de información que tenga en el puesto. Es así que, tanto la contratación como cese de un puesto, es una actividad conjunta de éstas dos áreas, y cada paso deberá ser coordinado para que no pueda pasar por alto ningún detalle, ya que son justamente estas pequeñas omisiones de las que luego resulta el haber quedado con alta dependencia técnica de personas cuyo perfil es peligroso, o que al tiempo de haberse ido mantiene accesos o permisos que no se debieran, tal como se ha evidenciado.

Controles a implementar para Seguridad de Recursos Humanos

7	Seguridad de Recursos Humanos (RRHH)
7.1	**Antes de asumir el empleo**
7.1.1	Selección
7.1.2	Terminos y condiciones del empleo
7.2	**Durante la ejecución del empleo**
7.2.1	Responsabilidades de la dirección
7.2.2	Concientización, educación y formación en la seguridad de la información.
7.2.3	Proceso disciplinario
7.3	**Terminación o cambio de empleo**
7.3.1	Terminación o cambio de responsabilidades de empleo.

Fuente: Adaptación de la norma ISO/IEC 27002:2013.

3.8.8 Seguridad de Control de Accesos

La fase de Seguridad de Control de accesos, regula que el usuario autenticado acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro, es decir que tiene dos tareas derivadas:

- Encauzar al usuario debidamente.
- Verificar el desvío de cualquier acceso, fuera de lo correcto.

El control de acceso es una de las actividades más importantes de la arquitectura de seguridad de un sistema y los agrupa en 04 subgrupos que se pueden apreciar a continuación:

Seguridad de Control de Accesos

9.	Control de acceso
9.1	**Requisito del negocio para el control de acceso**
9.1.1	Política de control de acceso
9.1.2	Acceso a redes y a servicios en red.
9.2	**Gestión del acceso de usuarios**
9.2.1	Registro y cancelación del registro de usuarios
9.2.2	Suministro de acceso de usuarios
9.2.3	Gestión de derechos de acceso privilegiado
9.2.4	Gestión de información de autenticación secreta de usuarios
9.2.5	Revisión de los derechos de acceso de usuarios
9.2.6	Retiro o ajuste de los derechos de acceso
9.3	**Responsabilidades de los usuarios**
9.3.1	Uso de información de autenticación secreta.
9.4	**Control de acceso a sistemas y aplicaciones**
9.4.1	Restricción de acceso a la información
9.4.2	Procedimiento de ingreso seguro
9.4.3	Sistema de gestión de contraseñas
9.4.4	Uso de programas utilitarios privilegiados
9.4.5	Control de acceso a códigos fuente de programas

Fuente: Adaptación de la norma ISO/IEC 27002:2013.

3.8.9 Seguridad en las Operaciones

Son los controles relacionados con la gestión de la producción en tecnologías de la información: gestión de cambios, gestión de la capacidad, malware, respaldo, espejos, instalación, vulnerabilidades, etc.

Seguridad de Control de las Operaciones

12	Seguridad de las operaciones
12.1	**Procedimientos operacionales y responsabilidades**
12.1.1	Procedimientos de operación documentados
12.1.2	Gestión de cambios
12.1.3	Gestión de capacidad
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación
12.2	**Protección contra códigos maliciosos**
12.2.1	Controles contra códigos maliciosos
12.3	Copias de respaldo
12.3.1	Respaldo de la información
12.4	Registro y Seguimiento
12.4.1	Registro de eventos
12.4.2	Protección de la información de registro
12.4.3	Registro del administrador y del operador
12.4.4	Sincronización de relojes

Fuente: Adaptación de la norma ISO/IEC 27002:2013.

3.9 Seguridad en Comunicaciones y Proveedores

Controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc., y controles acerca de que incluir en los contratos y como hacer el seguimiento a los proveedores.

Seguridad de las Comunicaciones

13	Seguridad de las comunicaciones
13.1	Gestión de la seguridad de las redes
13.1.1	Controles de redes
13.1.2	Seguridad de los servicios de red
13.1.3	Separación en las redes
13.2	Transferencia de Información
13.2.1	Políticas y procedimientos de transferencia de información
13.2.2	Acuerdos sobre transferencia de información
13.2.3	Mensajería electrónica
13.2.4	Acuerdos de confidencialidad o de no divulgación

Fuente: Adaptación de la norma ISO/IEC 27002:2013.

3.9.1 Seguridad Física y del Entorno

Para esta actividad se han considerado doce controles y se encuentra dividido en:

Áreas de Seguridad: Seguridad física y perimetral, control físico de entradas, seguridad de locales edificios y recursos, protección contra amenazas externas y del entorno, el trabajo en áreas de seguridad, accesos públicos.

Equipamiento: Ubicación y protección de los equipos, servicio de suministros, seguridad de cableado, mantenimiento de equipos, retiro de activos, disposición segura o reutilización de equipos, política de escritorio limpio y pantalla limpia.

Controles para la Seguridad Física y del Entorno

11.	Seguridad Física y del Entorno
11.1	**Áreas Seguras**
11.1.1	Perímetro de seguridad física
11.1.2	Cotroles físicos de entrada
11.1.3	Seguridad de oficinas, recintos e instalaciones
11.1.4	Protección contra amenazas externas y ambientales
11.1.5	Trabajo en áreas seguras
11.2	**Equipamiento**
11.2.1	Ubicación y protección de los equipos
11.2.2	Servicios de suministros
11.2.3	Seguridad de cableado
11.2.4	Mantenimiento de equipos
11.2.5	Retiro de activos
11.2.6	Disposición segura o reutilización de equipos
11.2.7	Política de escritorio limpio y pantalla limpia

Fuente: Adaptación de la norma ISO/IEC 27002:2013.

3.9.2 Evaluación de Indicadores

Con la finalidad de contrastar la hipótesis se evaluaron los siguientes indicadores:

- **Armonización de las metodologías, estándares y normas de Seguridad de la Información**.

Para tal acción se revisó las normativas vigentes del Estado especialmente del Organismo Nacional de Gobierno Electrónico (ONGEI) y Secretaría de

Gobierno Digital como entes rectores responsables de formular, proponer políticas, planes, normas, lineamientos y estrategias en materia de Informática y Gobierno Electrónico, dentro del item 11 Art. 48 de sus funciones dice: "Aprobar las normas y estándares para promover el desarrollo e implementación de la seguridad de la información, infraestructura de datos especiales, datos abiertos, interoperabilidad, portales del Estado, entre otros de las entidades públicas del Estado". [11]

Por otro lado se identificaron las leyes, estándares, metodologías y marcos de trabajo relacionados con la seguridad de la información en salud.

Se compararon cada uno de ellos, se analizaron detallando las actividades similares entre sí seleccionandolos de acuerdo a las necesidades de la institución.

Se realizó una estructura definiéndola como el Modelo a seguir en la implementación de la seguridad de la información, especificando los ítems de los estándares, metodologías y marcos de trabajo.

- Validez del Modelo de Seguridad de la Información

En la validez se tiene como objetivo apoyar el proceso de atención al paciente en una institucion de salud mediante la implementación de un Modelo de Gestión de Seguridad de la Información y para demostrar se validó mediante el uso de dos instrumentos:

1°. Se sometió a la evaluación de tres expertos con el fin de medir el nivel de confiabilidad del modelo. Se procesaron los resultados del juicio de expertos aplicando Alfa de Crombach, obteniendo un nivel de confiabilidad del 66% como lo demuestra el siguiente cálculo:

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,722	,668	8

Fuente: Programa estadístico SPSS

Valores para estimar el nivel de confiabilidad

VALOR	CONCLUSION
0,53 a menos	Confiabilidad nula
0,54 a 0,59	Confiabildiad baja
0,60 a 0,65	Confiable
0,66 a 0,71	Muy Confiable
0,72 a 0,99	Excelente confiabilidad
1,0	Confiabilidad perfecta

En base a los resultados obtenidos, en la tabla anterior se puede considerar que el coeficiente de confiabildiad obtenido es muy confiable.

2° Como segundo instrumento se sometió a la prueba de concordancia de Kendall, para la validación de contenidos, el cual arrojó el siguiente resultado:

Para medir la validez de contenido, se utilizó la prueba de concordancia de Kendall el cual nos permite conocer el grado de concordancia entre los tres expertos (K=3) en el número de elementos estudiados N=19,
Sabiendo que:
Ho: No existe concordancia entre las opiniones de los evaluadores (W=0)
H1: Existe concordancia entre las opiniones de los evaluadores (W>0).
Siendo el resultado: W=0.198, es decir W es mayor que cero, se rechaza la hipótesis nula y se concluye que existe concordancia entre las opiniones de los evaluadores, en las dimensiones de: Suficiencia, Claridad, Coherencia y Relevancia.

Prueba W de Kendall

Pruebas NPar

Prueba W de Kendall

Rangos

	Rango promedio
TOTAL E1	1,68
TOTAL E2	2,18
TOTAL E3	2,13

Estadísticos de prueba

N	19
W de Kendall[a]	,198
Chi-cuadrado	7,517
gl	2
Sig. asintótica	,023

a. Coeficiente de concordancia de Kendall

- Número de Proyectos propuestos respecto a seguridad de la Información

De acuerdo a la estimación del nivel de los riesgos y en función a los niveles de probabilidad e impacto de materialización de amenazas, se proponen proyectos y planes que permitan accionar mecanismos de protección ante amenazas, las actividades que se consideran en ésta etapa son relevantes para el desarrollo del modelo propuesto, - sin embargo se deja a priori agregar alguna otra propuesta según la madurez de la organización en la que se aplique -, cabe mencionar que los proyectos propuestos están dirigidos a mitigar las amenazas.

Proyecto N° 1:

Plan de Capacitacion en Seguridad de la Información.

Dominios cubiertos: Seguridad de recursos humanos, conformidad de requisitos, mejora continua.

Proyecto N° 2:

Implementación de Políticas de Seguridad de la Información

Dominios cubiertos: Seguridad ligada a los recursos humanos, control de accesos, seguridad física y del ambiente, seguridad de las operaciones, seguridad de las comunicaciones y cumplimiento.

Proyecto N° 3:

Implementación de un Sistema de Gestión de Eventos en Seguridad de la Información.

Dominios afectados: Gestión de activos, control de accesos, seguridad de las operaciones, seguridad de las comunicaciones, conformidad de requisitos

Proyecto N° 4:

Implementación de un Modelo para la gestión de una Mesa de Ayuda a los Servicios de TI, basados en tecnologías ITIL para una institución de Salud.

Dominios cubiertos: Servicio de Soporte al usuario atendido de forma inmediata e individualizada de cualquier tipo de incidente y que cause una interrupción o reducción en la calidad de atención de un servicio médico.

3.9.3 Cumplimiento de Requisitos Legales

En ésta actividad, respaldada por la ISO 27799:2008 en su item 7.12.2, en el caso de estudio se considera lo siguiente:

- **Protección de datos y privacidad de la información personal**,

De acuerdo a las orientaciones dadas por la norma se debe "gestionar el consentimiento de información de los sujetos de atención", para los casos de estudios e investigaciones y, para tal situación se elaboró la plantilla de consentimiento informado del paciente en la que el mismo paciente otorga la autorización necesaria para que sus datos personales sean tomados e involucrados en un caso de estudio, y para tal actividad se elaboró el siguiente modelo de consentimiento informado:

Consentimiento informado del paciente

CONSENTIMIENTO INFORMADO PARA LA REALIZACIÓN DE PRUEBAS GENÉTICAS DIAGNÓSTICA

(Modelo sugerido por la Comisión de Ética de la AEGH –Asociación Española de Genetica Humana)

Solicitamos su consentimiento para

1. Realizar pruebas genéticas de laboratorio en muestras biológicas…….cuya finalidad es diagnósticar si esta afectado o es portador de…….
2. Dichas pruebas será realizadas en el Servicio de……..del hospital…….
3. Unicamente el personal asistencial, debidamente autorizado por el hospital…….podrá acceder a los datos personales y facilitarle el asesoramiento genético.
4. El facultativo que le solicita estas pruebas adquiere el compromiso de suministrarle información acerca del objeto de los análisis y usted puede decidir si desea o no que se le comunique.
5. La información obtenida puede ser relevante también por sus familiares y en este caso le explicaremos el porque de la conveniencia de que la conozcan. Es decisión personal informarles algo que nosotros le recomendamos con el fin de que, si ellos lo desean, puedan acudir a una consulta especializada en genética donde le informarán sobre su riesgo personal y sus opciones de salud en el futuro.
6. En las pruebas, podría ser que se encontrase información no directamente relacionada con el objeto de los análisis y usted puede decidir si desea o no que se le comunique.
7. Una vez finalizada los análisis, los datos obtenidos y las muestras excedentes se guardarán en el hospital …….por el interés que puedan tener para satisfacer futuras necesidades asistenciales de usted y sus familiares.

Por favor firme este consentimiento informado en sentido afirmativo:

Yo……..

Declaro que he sido informado que …….

Podría estar afectado(a) a ser portadora de una alteración genética y que el diagnóstico se basa en los resultados de las pruebas genéticas de laboratorio.

Doy consentimiento para realizar dichas pruebas genéticas en el servicio……del Hospital…….……..y en caso sea necesario en otros laboratorios designados por el mismo para ayudar al procesoo diagnóstico.
Fecha: Ciudad, ……..de…… del …….

Firma……
Nombre de paciente……
DNI…….

Firma……..
Profesional autorizado que solicita el consentimiento…….
DNI……..
Hospital……

Fuente: Revista Elsevier, Vol.24 Num.2 Anexo 01, 2013. [33]

Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico

Siguiendo las indicaciones de la ISO 27799:2008 en su item 7.12.3, se presta atención al cumplimiento de los fines de interoperabilidad técnica,como los sistemas de información en salud, respaldados por los principales documentos legales relacionados a las políticas públicas del uso de las tecnologías de la información y la comunicación (TIC) en salud [34].

3.9.4: Auditoria Interna

La Auditoría permite que se optimicen procesos, en la medida que se implementen planes de mejora, acciones preventivas y correctivas, al mismo tiempo, como un mecanismo de control que garantice la seguridad de la información.

La Auditoría Interna que se empleará en la institución está apoyada en el item 9.2 de la norma ISO 27001:2014 la misma que permitirá revisar si el modelo aplicado cumple sus objetivos de seguridad de la información, es entonces la auditoría interna una de las herramientas más interesantes ya que nos permite identificar insufiencias en el sistema y detectar potenciales situaciones de riesgo.

En cumplimiento al modelo planteado se deja propuesto lo siguiente:

- Plan de Auditoría Interna el cual está dirigido al área de tecnologías de información para la verificación de la seguridad de la información en el manejo y administración de los sistemas de información en las áreas de atención al paciente, involucrando como actores principales de éste Plan a los jefes de Servicios Médicos Asistenciales, Jefes de Departamentos Clínicos y Quirúrgicos y Gerentes de Línea lo que permitirá revisar el estado de la gestión de la información sensible que se necesita para la eficiente atención al paciente.
- Para tal efecto se elaboró la plantilla para establecer el Plan de Auditoría Interna del Modelo de Gestión de Seguridad de la Información, la cual podría ser realizada por una empresa externa. En dicha plantilla se

definen las acciones que se van a realizar, los involucrados, las tareas a llevarse a cabo, las fichas de inicio y cierre asi como los resultados obtenidos.

Plantilla para Establecer un Plan de Auditoría

Formato: Auditoria Interna (plantilla)								
Realizado por : Revisado por:								Fecha:
Objetivo: Establecer un Plan de Auditoria								
N°	Acción	Involucrados	Recursos	Tarea	Inicio	Fin	Resultados	Sugerencias

Fuente: Elaboración propia

3.9.5 Revisión de Gestión

Esta actividad es un requisito de la norma dentro del capítulo 9 en el punto "9.3 Revisión de Gestión", que recae en la Gerencia General de la Institución, la revisión del Sistema de Gestión de Seguridad de la Información es un punto clave ya que permite mantener vivo a un sistema de gestión y permite que se cumpla su verdadera función dentro de las buenas prácticas en seguridad de la información de la cual la alta Gerencia tiene una activa participación.

Con ésta actividad se garantizan dos puntos importantes:

- Garantizar que el Modelo de Seguridad de la Información y sus objetivos continuen siendo los adecuados y efectivos.
- Revisar la validez de los problemas identificados y los riesgos de la organización.

Para ello se cuenta fundamentalmente con los resultados de las auditorías internas que nos proporcionarían la siguiente información:

- Análisis de los eventos monitorizados.
- No conformidades o incidencias en la seguridad de la información.
- Análisis de las causas de las no conformidades
- Medidas preventivas para mitigar los riesgos.

3.9.6 Formar y Concientizar Personal

Para que la implementación del modelo sea efectiva, es necesario concientizar y formar a todas las personas implicadas. La formación y capacitación de cada usuario deberá ser acorde con las funciones que desempeñe dentro de la institución y su rol en la Seguridad de la Información. Todos los usuarios internos deben ser concientizados en la importancia de su labor para salvaguardar la información y cómo

desarrollar su trabajo aplicando las normas y procedimientos de seguridad de la información definidos.

Esta actividad quedó incluida en el Plan de Capacitación Institucional por lo tanto los gastos ocasionados serán presupuestados dentro de dicho plan.

En cuanto a formación, para dar cumplimiento al estándar, no solo es necesario dar cursos. Hace falta contar con un "Plan de formación". La formación en seguridad de la información, no puede ser una actividad aperiódica y determinada en un momento dado, tiene que ser tratada como cualquier otra actividad de la organización, es decir se debe plantear:

- Meta a la que se desea llegar.
- Determinación de los diferentes perfiles de conocimiento.
- Forma de acceder al conocimiento.
- Objetivos de la formación.
- Metodología a seguir.
- Planificación y asignación de recursos.
- Confección del plan de formación.
- Implementación del plan,
- Medición de resultados.
- Mejoras.

3.9.7 Mejora Continua.

Para el desarrollo de ésta actividad se elaboró la plantilla de Mejora Contínua, en la cual se tomarán en cuenta los controles que no han sido cumplidos tanto en el Modelo del Sistema de Seguridad de la Información como en los proyectos ejecutados y propuestos.

Se deja propuesta la plantilla para el seguimiento de los proyectos del Modelo de Gestión de Seguridad de la Información, y que a continuación se muestra.

Plantilla de Mejora Contínua

Mejora Contínua (plantilla)					
Registrado por:…… **Objetivo**: Establecer un plan de mejora contínua **Descripción**: Para el desarrollo de ésta actividad se debe tener en cuenta los controles que no han sido cumplidos					Fecha: dd/mm/aa
N°	**Plan de acción**	**Riesgos involucrados**	**Controles**	**Fecha Inicio**	**Fecha fin**
1					
2					
3					
…..					

Fuente: Elaboración propia

Plantilla para seguimiento de los Proyectos

Seguimiento de Proyectos														
Nombre del Proyecto: Responsable: Área o servicio de aplicación: Fecha:														
Objetivo: Permitir determinar el progreso de las actividades realizadas en los proyectos y tomar medidas necesarias para resolver problemas e incidentes, haciendo los ajustes necesarios en los objetivos y actividades.														
Etapa 1	Fecha Inicio	Fecha Fin	Cumplimiento de etapas del Proyecto											Recomendaciones
			Etapa 1			**Etapa 2**			**Etapa 3**			**Etapa 4**		
Actividades:			**NC**	**C**	**CP**	**NC**	**C**	**CP**	**NC**	**C**	**CP**	**NC**	**C**	**CP**	
1.Act.1														
2.Act.2														
3.Act.3														
4.Act.4														
NC: No ha cumplido en la fecha establecida C: Ha cumplido en la fecha establecida CP: Cumple parcialmente en la fecha establecida														
Conclusiones: Análisis del seguimiento de las etapas evaluadas.														

Fuente: Elaboración Propia

TABLAS

Aplicación del Modelo Propuesto: Caso de estudio "CuidaSalud"

Tabla 8: Contexto Externo de la Institución

Fase : Planificar – Contexto Externo de la Institución		
Nombre de la Institución: CuidaSalud **Objetivo**: Identificar los aspectos externos que rigen e influyen en la institución. **Instrumentos**: Documentos normativos, entrevistas, revisiones en las superintendencias y otras instituciones del rubro.		**Fecha de elaboración**: 15/03/2019 **Elaboración por**: Analista de TI **Revisado por:** Jefe de TI
N°	**Entorno**	**Aspectos identificados**
01	Reglamentario	-Ley 26842-1997 Ley General de Salud. -Ley 29733 Ley de Protección de Datos Personales. -D.S.050-2018-PCM: Aprueban la definición de seguridad Digital en el ámbito nacional -R.M.004-2016-PCM: Uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014. -R.M.431-2015-MINSA: Aprobar documento técnico "Políticas de Seguridad de la Información del Ministerio de Salud".
02	Político	- SUSALUD. - Defensoría del Pueblo - Fiscalía de Prevención del Delito - Indecopi.
03	Asociaciones y Colegios profesionales	-Colegio Médico del Perú – Consejo Regional VIII-Chiclayo. -Colegio de Enfermeros del Perú-Consejo Regional IX-Lambayeque -Colegio de Ingenieros del Perú-Consejo departamental Lambayeque.
04	Económico	- Empresas Publicas. - Fonafe. - Empresas Privadas.

Fuente: Caso se estudio

Tabla 9: Contexto Interno de la Institución

Fase : Planificar – Contexto Interno de la Institución		
Nombre de la Institución: CuidaSalud **Objetivo**: Identificar los aspectos internos que rigen e influyen en la institución. **Instrumentos**: Portal Intranet Institucional, MOF. ROF, Planeamiento Estratégico.		**Fecha de elaboración**: 25/03/2019 **Elaboración por**: Analista de TI **Revisado por**: Jefe de TI
Nº	**Entorno**	**Aspectos Identificados**
01	Proyectos enfocados a la mejora en la atención de servicios de salud.	-Aprobar la nueva Política Anticorrupción de la institución en estudio. -Implementar el código de ética institucional y ser comunicado a todo el personal de la institución. -Implementar el plan de Integridad y lucha contra la corrupción 2019-2021.
02	Objetivos Estratégicos	-**OE1**: Brindar servicios preventivos y recuperativos a satisfacción de nuestros asegurados. -**OE2**: Desarrollar una gestión con excelencia operativa. -**OE3**: Brindar servicios sostenibles financieramente. -**OE4**: Promover una gestión con ética y transparencia.
03	Visión y Misión	**Visión**: Ser una institución líder en salud en América Latina, superando las expectativas de sus pacientes en la protección de su salud y siendo reconocida por su buen trato, con una gestión moderna y a la vanguardia de la innovación. **Misión**: Somos una entidad pública que tiene como fin la protección de la población brindando prestaciones de salud, económicas y sociales con calidad, integridad, eficiencia y buen gobierno corporativo.
04	Recursos y conocimientos	-Directiva, Normas de seguridad física y del entorno de la institución -Directiva, Normas para una adecuada racionalización y administración de los servicios de INTERNET en la institución. -D.2005 Normas para dotar del correo electrónico oficial a los profesionales de la salud en los hospitales de la institución. -R. 2005. Políticas de seguridad informática de la institución.
05	Cultura de la Organización	-Medidas destinadas a mejorar la calidad del servicio y declara de interés público al mantenimiento de la infraestructura y el equipamiento en los establecimientos de salud a nivel nacional. -Medidas para cautelar el cumplimiento de normas a la seguridad en salud y la obligación de informar del trabajador. -Optimizar el intercambio prestacional en salud en el sector público.

Fuente: Caso se estudio

Tabla 10: Compromiso de los StakeHolder

Fase – Planificar: Compromiso de liderazgo de los StakeHolder				
Nombre de la Institución: CuidaSalud Objetivo: Identificar SI los stakeholder cumplen con su compromiso y liderazgo, NO lo cumplen o lo realizan parcialmente.			Fecha: 26/03/2019 Resp.:.Analista de TI Revisado por: Jefe de TI	
Nº	Funciones	SI	NO	PARCIAL
01	Asegura que la política y los objetivos de seguridad de la información sean establecidos y compatibles con la dirección estratégica de la institución.			X
02	Asegura la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la institución.	X		
03	Asegura que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.		X	
04	Comunicar la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información.	X		
05	Asegurar que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s).		X	
06	Dirigir y apoyar a las personas para que contribuyan con la efectividad del sistema de gestión de seguridad de la información.	X		
07	Promover la mejora continua.			X
08	Apoyar otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.	X		
Conclusiones: La gerencia no cumple con todas las funciones de liderazgo necesarias por la ISO 27001:2014. Para cumplir completamente con la fase de liderazgo, se debe culminar con las funciones referidas en los puntos 1,3,5,7.				

Fuente: Caso se estudio

Tabla 11: Establecimiento de Políticas de Seguridad de la Información

Fase – Planificar: Establecer Políticas del modelo de Gestión en Seguridad de la Información					
Nombre del documento: Registro de Establecimiento de Políticas **Objetivo**: Identificar las políticas de seguridad de acuerdo a las necesidades de la institución y de acuerdo a los Lineamientos del MINSA (RM-431-2015-MINSA) **Método de recolección**: Entrevistas, observación y revisión de documentos internos de la institución.				**Fecha**: 28/03/2019 **Elaborado por**: Analista de TI **Revisado por**: Jefe de TI.	
Nº	**Políticas de Seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles**
01	Políticas de Seguridad de la Información	Establecer controles para la gestión de seguridad de la información dentro de la institución.	Identificar las áreas donde se aplicaron las políticas y las personas involucradas en el cumplimiento de la misma.	Establecer los principios para la implementación de la GSI	Controles de SI según la lista de controles de la ISO 27002
02	Políticas de seguridad de los recursos humanos	Esta política ayuda en la asignación y cumplimiento de las responsabilidades del personal antes, durante y en terminación o cambio de empleo.			
03	Políticas de gestión de activos	Gestionar y administrar los activos de la organización durante sus procesos o funciones			
04	Políticas de control de accesos	Es la autorización que se otorga a las personas para acceder a las instalaciones o sistemas que contienen información			

<table>
<tr><th colspan="6">Fase – Planificar: Establecer Políticas del modelo de Gestión en Seguridad de la Información</th></tr>
<tr><td colspan="4">Nombre del documento: Registro de Establecimiento de Políticas
Objetivo: Identificar las políticas de seguridad de acuerdo a las necesidades de la institución
Método de recolección: Entrevistas, observación y revisión de documentos internos de la institución.</td><td colspan="2">Fecha: 28/03/2019
Elaborado por: Analista de TI.
Revisado por: Jefe de TI.</td></tr>
<tr><th>Nº</th><th>Políticas de Seguridad</th><th>Definición</th><th>Alcance</th><th>Objetivo</th><th>Controles</th></tr>
<tr><td>05</td><td>Políticas de Seguridad física y del entorno.</td><td>En esta política se debe detallar:
-Áreas seguras.
-Equipamiento.
-Controles de acceso físico para empleados, proveedores.</td><td rowspan="3">Identificar las áreas donde se aplicaron las políticas y las personas involucradas en el cumplimiento de la misma.</td><td rowspan="3">Establecer los principios para la implementación de la GSI</td><td rowspan="3">Controles de SI según la lista de controles de la ISO 27002</td></tr>
<tr><td>06</td><td>Políticas de seguridad de las operaciones: respaldo y restauración de información</td><td>Detallar las medidas convenientes para asegurar que la información del paciente esté protegida contra pérdida, alteración o divulgación de manera accidental o malintencionada, ya sea por fallas de los equipos y/o redes.</td></tr>
<tr><td>07</td><td>Políticas de seguridad de las comunicaciones</td><td>Se encarga de prevenir que algún usuario y/o entidad no autorizada, pueda acceder a la transferencia de información.</td></tr>
</table>

Fuente: Caso se estudio

Fase – Planificar: Establecer Políticas del modelo de Gestión en Seguridad de la Información					
Nombre del documento: Registro de Establecimiento de Políticas **Objetivo**: Identificar las políticas de seguridad de acuerdo a las necesidades de la institución **Método de recolección**: Entrevistas, observación y revisión de documentos internos de la institución.				**Fecha**: 28/03/2019 **Elaborado por**: Analista de TI. **Revisado por**: Jefe de TI.	
Nº	**Políticas de Seguridad**	**Definición**	**Alcance**	**Objetivo**	**Controles**
08	Políticas de cumplimiento	Definir tareas y responsabilidades de modo que se cumpla toda obligación legal aplicable a la seguridad de la información.	Identificar las áreas donde se aplicaron las políticas y las personas involucradas en el cumplimiento de la misma.	Establecer los principios para la implementación de la GSI	Controles de SI según la lista de controles de la ISO 27002
09	Políticas de privacidad	Se debe dar a conocer las condiciones que rigen el tratamiento y protección de datos personales que son enviados a través de los sistemas de información de un establecimiento a otro.			

Fuente: Caso se estudio

Tabla 12: Información de salud a proteger

No.	Datos a proteger	Contenido
1	Documentos con datos del paciente.	Historia clínica, imágenes, PDF´s, con datos de fichas de pacientes, que se intercambian entre instituciones publicas y privadas de salud .
2	Información con resultados de tests.	Laboratorio Clínico, Banco de Sangre, Anatomía Patologica, que se intercambian entre unidades de la institución.
3	Información con indicaciones farmacológicas.	Formulas magistrales, Recetas con medicamentos de alto costo y controlados.
4	Documentación interna que se procesa a terceros.	Proveedores, almacenes y Convenios de tratamientos oncológicos.
5	Información relacionada con temas de innovación.	Investigaciones, Terapias alternativos, Procedimientos especiales.
6	Información relacionada con metas y cumplimientos legales.	Indicadores hospitalarios, estadísticas, indicadores epidemiológicos.
7	Información de seguros y acreditaciones.	Empresas y organizaciones que aportan al estado un seguro de salud..

Fuente: Caso se estudio

Tabla 13: Identificación de Roles y Responsabilidades

Fase Planificar: Identificación de roles y responsabilidades		
Elaborado por: Analista de TI **Registrado por**:Jefe de TI **Objetivo**: Identificar los roles y las responsabilidades		**Fecha**: 01/04/2019
Descripción: Para la recolección de información se hizo uso del Manual de Organización y Funciones de la institución		
Rol	**Responsabilidad**	**Nivel de implicancia**
Digitadores	• Módulo de datos del paciente. • Asignación de citas • Modulo de ayuda al diagnóstico • Módulo de Farmacia • Módulo de hospitalizacion. • Egresos, mopri, Módulo de centro quirurgico, • Módulo de reportes • Módulo de emergencia • Modulo de referencias de pacientes.	Responsable (R)
Programadores	• Mantenimiento de los sistemas de información. • Mantenimiento de Base de Datos.	Responsable (R)
Soporte Técnico	• Mant.de equipos de computo • Instalación de redes	Responsable (R)
Ingenieros de Sistemas	• Módulo de datos del paciente • Validación de datos personales • Citas • Módulo de ayuda al diagnóstico y tratamiento • Módulo de Farmacia • Módulo de hospitalización • Datos operacionales • Módulo de centro quirurgico • Módulo de reportes • Módulo de emergencia • Módulo de referencias • Instalación de redes • Mant. de equipos informaticos • Adm de sistemas de información	Consultado (C) Aprobado (A) Responsable (R)
Jefe de TI	• Módulo de datos del paciente • Validación de datos personales	Consultado (C)

Fase Planificar: Identificación de roles y responsabilidades		
Elaborado por: Analista de TI **Registrado por**:Jefe de TI **Objetivo**: Identificar los roles y las responsabilidades		**Fecha**: 01/04/2019
Descripción: Para la recolección de información se hizo uso del Manual de Organización y Funciones de la institución		
Rol	**Responsabilidad**	**Nivel de implicancia**
	•Citas •Módulo de ayuda al diagnóstico y tratamiento •Módulo de Farmacia •Módulo de hospitalización •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia •Módulo de referencias •Mant. de equipos informaticos •Instalación de redes	Informado (I)
Tecnico Asistencial	•Módulo de datos del paciente •Módulo de Farmacia •Módulo de hospitalización •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia	Responsable (R)
Médico Residente	•Módulo de datos del paciente •Módulo de ayuda al diagnóstico y tratamiento •Módulo de hospitalización •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia	Responsable (R)
Médico Asistente	•Módulos de datos del paciente •Módulo de ayuda al diagnóstico y tratamiento •Módulo de hospitalización •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia	Consultado (C)

Fase Planificar: Identificación de roles y responsabilidades		
Elaborado por: Analista de TI **Registrado por**:Jefe de TI **Objetivo**: Identificar los roles y las responsabilidades		**Fecha**: 01/04/2019
Descripción: Para la recolección de información se hizo uso del Manual de Organización y Funciones de la institución		
Rol	**Responsabilidad**	**Nivel de implicancia**
	•Módulo de referencias	Informado (I)
Jefe de SSAA	•Módulo de datos del paciente •Asignación de citas •Módulo de ayuda al diagnóstico •Módulo de Farmacia •Módulo de hospitalizacion •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia •Mantenimiento de equipos	Informado (I) Consultado (C) Informado (I)
Estadista	•Validación de datos personales •Asignación de citas •Módulo de ayuda al diagnóstico •Módulo de Farmacia •Módulo de hospitalizacion •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia •Módulo de referencias	Aprobado (AI) Informado (I) Aprobado (A)
Epidemiólogo	•Validación de datos personales •Asignación de citas •Módulo de ayuda al diagnóstico •Módulo de hospitalizacion •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia	Aprobado (A)
COPOES	•Datos operacionales	Responsable (R)
PADOMI	•Datos operacionales	Responsable (R)
Jefe Departamento	•Módulo de datos del paciente •Asignación de citas	Informado (I)

Fase Planificar: Identificación de roles y responsabilidades		
Elaborado por: Analista de TI **Registrado por**:Jefe de TI **Objetivo**: Identificar los roles y las responsabilidades		**Fecha**: 01/04/2019
Descripción: Para la recolección de información se hizo uso del Manual de Organización y Funciones de la institución		
Rol	**Responsabilidad**	**Nivel de implicancia**
	•Módulo de ayuda al diagnóstico •Módulo de Farmacia •Módulo de hospitalizacion •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia •Módulo de referencias •Mant. de equipos informaticos	
Gerente de Seguros	•Módulo de datos del paciente •Validación de datos personales	Informado (I)
Gerente Hospital	•Módulo de datos del paciente •Asignación de citas •Módulo de ayuda al diagnóstico •Módulo de Farmacia •Módulo de hospitalizacion •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia •Módulo de referencias •Mant. de equipos informaticos	Informado (I)
Gerente C.P.	•Módulos de datos del paciente •Asignación de citas •Administracion de SI	Informado (I)
Gerente de Red	•Módulo de datos del paciente •Asignación de citas •Módulo de Farmacia •Módulo de hospitalizacion •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Modulo de referencias	Informado (I)
Jefe de OCI-ODIII	•Módulo de datos del paciente •Validación de datos personales	Informado (I)

Fase Planificar: Identificación de roles y responsabilidades		
Elaborado por: Analista de TI **Registrado por**:Jefe de TI **Objetivo**: Identificar los roles y las responsabilidades		**Fecha**: 01/04/2019
Descripción: Para la recolección de información se hizo uso del Manual de Organización y Funciones de la institución		
Rol	**Responsabilidad**	**Nivel de implicancia**
	•Asignación de citas •Módulo de ayuda al diagnóstico •Módulo de farmacia •Módulo de hospitalización •Datos operacionales •Módulo de centro quirurgico •Módulo de reportes •Módulo de emergencia •Adm de sistemas de información •Módulo de referencias •Mant. de equipos informáticos	

Fuente: Caso se estudio

Tabla 14: Identificación de los activos

FASE Hacer: Identificación de los Activos					
Nombre de la Institución: CuidaSalud **Elaborado por**: Analista de Sistemas Aprob: Jefe de TI				**Servicio**: Consulta Externa **Fecha**: 02/04/2019	
Objetivo: Identificar los activos presentes en las diferentes áreas de trabajo asistencial y de procesamiento de la información del paciente					
Descripción: Para recoger la información se puede hacer uso de la observación directa.					
Nº	**Tipo de Activo**	**Activo**	**Código**	**Descripción**	**Responsable**
01	Hardware	Equipos de computo	[HW_pc]	Equipo de cómputo utilizado por el personal técnico asistencial en consultorio	Centro asistencial
02	Hardware	Impresora	[HW_print]	Impresora utilizada por personal técnico en consultorio	Centro asistencial
03	Hardware	Escáner	[HW_scan]	Escáner utilizado por personal técnico para obtener copias.	Centro asistencial
04	Software	Sistema SISS	[SI_SGSS]	Sistema de información contiene información del paciente.	Área de TI
05	Software	Sistema AP	[SI_AnaPat]	Sistema de información que contiene datos de procesamientos histológicos del paciente	Área de TI
06	Software	Sistema SGH	[SI_SGH]	Sistema información que contiene diagnósticos de los pacientes	Área de TI
07	Software	Sistema PAC	[SI_PAC]	Sistema que almacena información de las imágenes de los pacientes.	Área de TI
08	Software	Antivirus y actualizaciones	[SW_antiv]	Antivirus e instalaciones en los sistemas de información	Área de TI
09	Software	Cliente de correo electrónico	[SW_email]	Software para correo electrónico	Área de TI
10	Datos	Historia clínica	[D_hc]	Información en papel contiene datos diagnóstico del paciente	Centro asistencial
11	Datos	Contraseñas	[D_passw]	Contraseñas para que el personal asistencial acceda a los sistemas de información	Área de TI

Nº	Tipo de Activo	Activo	Código	Descripción	Responsable
12	Datos	Nombre de usuarios	[D_user]	Datos personales de cada usuario que accede a los sistemas de información	Área de TI
13	Servicios	Servicios externos	[S_activo]	Información que se entrega a terceros para obtener un servicio al paciente	Centro asistencial
14	Soportes de información	Discos Duros	[Media_dd]	Dispositivo físico para almacenar información antigua del paciente	Área de TI
15	Soportes de información	USB	[Media_usb]	Dispositivos físicos para almacenar información	Área de TI
16	Soportes de información	Lap Top	[Media_lap]	Equipo de cómputo utilizado por la gerencia.	Centro asistencial
17	Instalaciones	Ambiente físico de consultorios	[I_AF]	Áreas donde se accede a la información del paciente	Centro asistencial
18	Equipo Biomédico	Impresora de placas radiográficas con lector, grabador y DD	[EB_printpl]	Dispositivo que permite imprimir imágenes de resultados de placas con lector, grabador y memoria.	Centro asistencial
19	Equipo Biomédico	Equipos automatizados de hemogramas	[EB_activo]	Dispositivo que procesa hemogramas, graba y con interfaz accede al sistema SGSS	Centro asistencial
20	Equipo Biomédico	Equipo de imágenes con memoria, grabadora de CD, y disco duro.	[EB_tac]	Equipo biomédico que realiza tomografías, graba y reproduce mediante uso de CD´s.	Centro asistencial
21	Seguridad física	Sistema de Videovigilancia dentro de las instalaciones de la institución.	[SF_camvd]	Equipo de gestión de video para el control de accesos de personal a áreas restringidas, con grabadora y disco duro.	Centro asistencial
22	Servidor Backup	Equipo Dell Power Edge R730	[HW_back]	Dispositivo que permite guardar copias de respaldo de la información del paciente	Área de TI
23	Servidor PAC	Equipo Dell Power Edge R730	[HW_pac]	Equipo de cómputo que contiene la información de imágenes del paciente a nivel nacional	Área de TI
24	Servidor Correo, SGH	Equipo HP Proliant ML350 Gen9	[HW_email]	Equipo que permite brindar el servicio de correo electrónico dentro de la institución	Área de TI
25	Personal	Usuarios internos	[P_ui]	Personal que labora en la institución y atiende al paciente	Centro asistencial

Tabla 15: Valoración de Activos

Fase Hacer: Valoración de Activos							
Registrado por: Analista de TI **Aprobado por**: Jefe de TI						Fecha: 05 / 04 / 2019	
Objetivo: Identificar el nivel de criticidad de cada activo **Descripción**: Para el desarrollo de esta actividad se extraen los activos de la plantilla de identicación de activo							
N°.	Activo	Cod. Activo	Criterio			Total	Nivel
			(D)	(I)	(C)		
01	Equipo de computo	[HW_pc]	4	4	4	12	Muy alto
02	Impresora	[HW_print]	3	4	2	9	Alto
03	Escáner	[HW_scan]	1	2	2	5	Bajo
04	Sistema SGSS	[SI_SISS]	4	4	4	12	Muy alto
05	Sistema AP	[SI_AP]	4	4	4	12	Muy alto
06	Sistema SGH	[SI_SGH]	4	4	4	12	Muy alto
07	Sistema PACS	[SI_PAC]	4	4	4	12	Muy alto
08	Antivirus y actualizaciones	[SW_antiv]	4	4	4	12	Muy alto
09	Correo electrónico	[SW_email]	3	4	4	11	Muy alto
10	Historia clínica	[D_hc]	4	4	4	12	Muy alto
11	Contraseñas	[D_passw]	4	4	4	12	Muy alto
12	Nombre de usuarios	[D_user]	4	4	4	12	Muy alto
13	Proveedor servicios externos	[D_diagn]	3	3	3	9	Alto

Fuente: Caso se estudio

Fase Hacer: Valoración de Activos	
Registrado por: Analista de TI **Aprobado por**: Jefe de TI	Fecha: 05 / 04 / 2019
Objetivo: Identificar el nivel de criticidad de cada activo **Descripción**: Para el desarrollo de esta actividad se extraen los activos de la plantilla de identicación de activo	

N°.	Activo	Cod. Activo	Criterio			Total	Nivel
			(D)	(I)	(C)		
14	Discos Duros	[Media_DD]	1	4	4	9	Alto
15	USB	[Media_usb]	1	4	4	9	Alto
16	Lap Top	[Media_Lap]	1	4	4	9	Alto
17	Ambiente físico de consultorios y de TI	[I_CM]	4	4	4	12	Muy alto
18	Impresora de placas radiográficas	[EB_Rayos]	4	4	4	12	Muy alto
19	Equipos biomédicos de hemogramas	[EB_Hemo]	1	4	4	9	Alto
20	Equipo de imágenes con grabadora de CD y DD	[EB_Imag]	3	4	4	11	Muy alto
21	Sistema de Video vigilancia.	[SF_camvd]	3	2	2	7	Alto
22	Servidor Backup	[HW_back]	4	4	4	12	Muy alto
23	Servidor pac	[HW_pac]	3	3	4	10	Muy alto
24	Servidor correo electrónico	[HW_email]	3	3	3	9	Alto
25	Personal interno	[P_ui]	4	4	4	12	Muy alto

Fuente: Caso se estudio

Tabla 16: Identificación de Amenazas y Vulnerabilidades

Identificación de Amenazas y Vulnerabilidades					
Registrado por: Analista de Sistemas.					VoBo Fecha: 06/04/2019
Objetivo: Identificar las amenazas y vulnerabilidades de cada activo identificado.					
Descripción: Para el desarrollo de esta actividad se ubica el activo identificado en la lista de amenazas y vulnerabilidades.					
N	**Activo**	**Cod. Activo**	**Amenazas**	**Vulnerabilidades**	**Medidas Recomendadas**
1	Equipos de computo	[HW_pc]	Daño físico a los routers, switches y cableado expuestos a temperaturas, altas que interrumpa el servicio.	Recursos de red expuestos a riesgos físicos	Políticas de seguridad física y del entorno de red.
2	Impresora	[HW_print]	Mal funcionamiento	Procedimientos inadecuado de mantenimiento.	Planes de mantenimientos, supervisión y comunicación
3	Escaner	[HW_scan]	Deterioro	Inadecuada programación de mantenimiento	Planes de mantenimientos, supervisión y comunicación
4	Sistema SGSS.	[SI_SISS]	Sustracción de información confidencial	Privilegios excesivos y abuso de privilegios	Políticas de control de accesos y Proyecto de Gestión de Incidencias
5	Sistema AnaPat	[SI_AP]	Sustracción de información confidencial	Privilegios excesivos y abuso de privilegios	Políticas de control de accesos y Proyecto de Gestión de Incidencias

Identificación de Amenazas y Vulnerabilidades					
N	Activo	Cod. Activo	Amenazas	Vulnerabilidades	Medidas Recomendadas
6	Sistema SGH	[SI_SGH]	Sustracción de información confidencial	Privilegios excesivos y abuso de privilegios	Políticas de control de accesos y Proyecto de Gestión de Incidencias
7	Sistema Pac´s	[SI_PAC]	Sustracción de información confidencial	Privilegios excesivos y abuso de privilegios	Políticas de control de accesos y Proyecto de Gestión de Incidencias
8	Antivirus y actualizaciones	[SW_antiv]	Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada	Aplicación desactualizada o parchada incorrectamente.	Adquisición de licencias
9	Correo electrónico	[SW_email]	Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento	Falta de políticas para el correcto uso del correo electrónico de la institucion	Plan de Capacitación en seguridad de información
10	Historia clínica	[D_hc]	Acceso a los documentos por parte de personas ajenas a la institución o por usuarios inadecuados	Falta de control de acceso al lugar donde se guarda el documento.	Políticas de perímetro de seguridad física
11	Contraseñas	[D_passw]	Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas.	Contraseñas de usuarios sencillas	Políticas para gestión de contraseñas

Identificación de Amenazas y Vulnerabilidades					
N	Activo	Cod. Activo	Amenazas	Vulnerabilidades	Medidas Recomendadas
12	Nombre de usuarios	[D_user]	Acceso a los sistemas por usuarios inadecuados que no deberían consultar dichos accesos	Nombres de usuarios que exceden los requerimientos del cargo.	Gestión de control de accesos y buenas políticas de contratación
13	Servicios externos	[D_diagn]	Ingeniería social.	Personal con desconocimiento de normas de seguridad de información	Seguridad fisica y del entorno
14	Discos Duros	[Media_DD]	Hurto o deterioro interno del dispositivo	Almacenamiento inadecuado y sin protección	Seguridad de oficinas, recintos e instalaciones
15	USB	[Media_usb]	Hurto o deterioro interno del dispositivo	Almacenamiento inadecuado y sin protección	Seguridad de oficinas, recintos e instalaciones
16	Lap Top	[Media_Lap]	Hurto o deterioro interno del equipo	Almacenamiento inadecuado y sin protección	Seguridad de oficinas, recintos e instalaciones
17	Ambientes físicos de consultorios	[L_CM]	Accesos de personas ajepnas al área para manipular impresoras o escaner y que podrían sustraer información.	Áreas físicas sin controles de accesos.	Seguridad física de oficinas e instalaciones y Políticas para protección de equipos.

Identificación de Amenazas y Vulnerabilidades					
N	Activo	Cod. Activo	Amenazas	Vulnerabilidades	Medidas Recomendadas
18	Impresora de placas radiograficas	[EB_Rayos]	Acceso a la información del paciente a través de la pantalla por parte de personas ajeno a la empresa o por usuarios no autorizados	Incorrecta identificación de usuarios y contraseñas para acceder a los datos de los equipos biomedicos	Mejores prácticas de seguridad de la información a través de políticas. Políticas de seguridad de información en contratos con proveedores de equipos biométicos
19	Equipos biomedicos de hemogramas	[EB_Hemo]	Acceso a la información del paciente a través de la pantalla por parte de personas ajenas a la empresa o por usuarios inadecuados	Incorrecta identificación de usuarios y contraseñas para acceder a los datos de los equipos biomedicos	Mejores prácticas de seguridad de la información a través de políticas. Políticas de seguridad de información en contratos con proveedores de equipos biométicos
20	Equipo de imágenes con grabadora de CD y DD	[EB_Imag]	Acceso a la información del paciente a través de la pantalla por parte de personas ajenas a la empresa o por usuarios inadecuados	Incorrecta identificación de usuarios y contraseñas para acceder a los datos de los equipos biomedicos	Mejores prácticas de seguridad de la información a través de políticas. Políticas de seguridad de información en contratos con proveedores de equipos biométicos
21	Sistema de videovigilancia	[SF_camvd]	Hackeo e Interrupción del sistema por extraños	Contraseñas debiles y falta de cultura de cambio de contraseñas.	Recurrir a herramientas y soluciones de software que creen contraseñas seguras

Identificación de Amenazas y Vulnerabilidades					
N	Activo	Cod. Activo	Amenazas	Vulnerabilidades	Medidas Recomendadas
22	Servidor Backup	[HW_back]	Inadecuada infraestructura donde se almacenan o guardan los dispositivos de backups	Posible deterioro de dispositivos de backups	Seguridad de oficinas, recintos e instalaciones
23	Servidor Pacs	[HW_pac]	Inadecuada infraestructura donde se almacenan o guardan los dispositivos.	Posible deterioro de dispositivos.	Seguridad de oficinas, recintos e instalaciones
24	Servidor correo electrónico	[HW_email]	Acceso no autorizado a información del servidor, utilización de recursos por parte de personas no autorizadas para enviar correos a terceros .	Falta de control adecuado y monitoreo periodicamente a los accesos otorgados al personal.	Seguridad de oficinas, recintos e instalaciones
25	Personal interno	[P_ui]	Falta de acciones ante incidencias de disponibilidad e integridad de la información del paciente	Ausencia de Gestión de incidencias.	Políticas para procedimientos operacionales y gestión de incidencias

Fuente: Caso se estudio

Tabla 17: Análisis de Riesgos

Fase Hacer: Análisis de Riesgos								
Nombre de la Institución: CuidaSalud **Elaborado por**: Analista de TI **Aprobado por**: Jefe de TI **Objetivo**: Determinar el análisis del riesgo **Descripción**: Para el desarrollo de esta actividad se hace uso del resultado de la plantilla de identificación de amenazas y vulnerabilidades.							Fecha de registro: 10/04/2019	
Nº	**Activo**	**Amenaza**	**Vulnerabilidad**	**P**	**I**	**Valor (PxI)**	**Código de riesgo**	**Magnitud**
01	Equipos de computo	Daño físico a los routers, switches y cableado expuestos a temperaturas, altas que interrumpa el servicio.	Recursos de red expuestos a riesgos físicos	2	4	8	R01	**Media**
02	Impresora	Mal funcionamiento	Procedimientos inadecuado de mantenimiento	4	2	8	R02	**Media**
03	Escáner	Deterioro	Inadecuada programación de mantenimiento	2	2	4	R03	**Baja**
04	Sistema SISS	Sustracción de Información confidencial	Falta de registros, eventos y actividades criticas realizadas por los usuarios internos	4	4	16	R04	**Crítica**
05	Sistema AP	Sustracción de Información confidencial	Falta de registros, eventos y actividades criticas realizadas por los usuarios internos	4	4	16	R05	**Crítica**
06	Sistema SGH	Sustracción de Información confidencial	Falta de registros, eventos y actividades criticas realizadas por los usuarios internos	2	3	6	R06	**Media**

Análisis de Riesgos								
Nº	Activo	Amenaza	Vulnerabilidad	P	I	Valor (PxI)	Código de riesgo	Magnitud
07	Sistema Pac	Sustracción de información confidencial	Falta de registros, eventos y actividades criticas realizadas por los usuarios internos	2	3	6	R07	Media
08	Antivirus y actualizaciones	Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada	Aplicación desactualizada o parchada incorrectamente.	2	3	6	R08	Media
09	Correo electrónico	Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento	Falta de políticas para el correcto uso del correo electrónico de la institucion	3	3	9	R09	Media
10	Historia clínica	Acceso a los documentos por parte de personas ajenas a la institución o por usuarios inadecuados	Falta de control de acceso al lugar donde se guarda el documento.	4	3	12	R10	Alta
11	Documentos de respaldo	Divulgación de información confidencial	Accesos inadecuados a los archivos físicos	2	3	6	R11	Media
12	Contraseñas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas.	Contraseñas de usuarios sencillas	4	5	20	R12	Crítica
13	Nombre de usuarios	Acceso a los sistemas por parte de usuarios inadecuados que no deberían tener dicho acceso.	Exceso de privilegios para usuarios no indicados.	4	3	12	R13	Alta

Análisis de Riesgos								
Nº	Activo	Amenaza	Vulnerabilidad	P	I	Valor (PxI)	Código de riesgo	Magnitud
14	Servicios externos	Ingeniería social	Personal con desconocimiento d normas de seguridad de información	4	4	16	R14	Crítica
15	Discos Duros	Sustracción o deterioro interno del dispositivo	Almacenamiento inadecuado y sin protección	3	4	12	R15	Alta
16	USB	Sustracción o deterioro interno del dispositivo	Almacenamiento inadecuado y sin protección	3	4	12	R16	Alta
17	Lap Top	Sustracción o deterioro interno del equipo	Almacenamiento inadecuado y sin protección	2	4	8	R17	Media
18	Ambientes físicos de consultorios	Accesos de personas ajenas al área para manipular impresoras o escaner y que podrían sustraer información	Áreas físicas sin controles de accesos.	4	4	16	R18	Crítica
19	Impresora de placas radiograficas	Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados	Falta de correcta identificación de usuarios y contraseñas para acceder a las pantallas y equipos biomedicos	3	3	9	R19	Media
20	Equipos biomedicos de hemogramas	Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados	Falta de correcta identificación de usuarios y contraseñas para acceder a las pantallas y equipos biomedicos	3	3	9	R20	Media
21	Equipo de imágenes con grabadora de CD y DD	Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados	Falta de correcta identificación de usuarios y contraseñas para acceder a las pantallas y equipos biomedicos.	3	4	12	R21	Alta

Análisis de Riesgos								
Nº	Activo	Amenaza	Vulnerabilidad	P	I	Valor (PxI)	Código de riesgo	Magnitud
22	Sistema de videovigilancia	Hackeo e Interrupción del sistema por extraños	Contraseñas debiles y falta de cultura de cambio de contraseñas.	3	4	12	R22	Alta
23	Servidor Backup	Inadecuada infraestructura donde se almacenan o guardan los dispositivos de backups	Posible deterioro de dispositivos de backups	3	3	9	R23	Media
24	Servidor Pac	Inadecuada infraestructura donde se almacenan o guardan los dispositivos.	Posible deterioro de dispositivos.	3	3	9	R24	Media
25	Servidor correo electrónico	Acceso no autorizado a información del servidor, utilización de recursos por parte de personas no autorizadas para enviar correos a terceros .	Falta de control adecuado y monitoreo periodicamente a los accesos otorgados al personal.	3	3	9	R25	Media
26	Personal interno	Falta de acciones ante incidencias de disponibilidad e integridad de la información del paciente	Ausencia de Gestión de incidencias.	4	4	16	R26	Crítica

Fuente: Caso se estudio

Tabla 18: Mapa de Calor

PROBABILIDAD							
	Casi seguro	5					
	Probable	4		R02,	R10, R13,	**R04,R05 R14, R18, R26**	**R12,**
	Posible	3			R09, R19, R23, R24	R15, R16, R20, R21, R22.	
	Improbable	2		R03	R06, R07, R08, R11	R01, R17 R25	
	Raro	1					
			1	2	3	4	5
			Insignificante	Menor	Moderado	Mayor	Catastrófico
			IMPACTO				

Análisis:

Del mapa de calor elaborado se observa que el 23.08% (06) de los riesgos son de impacto crítico, el 26.92% (07) de riesgos corresponden a una alta magnitud, el 46.15% (12) corresponden a una magnitud media y el 3.85% es de magnitud baja.

Tabla 19: Evaluación de Riesgos

Fase – Hacer: Evaluación de Riesgos							
Nombre de la Institución: CuidaSalud **Elaborado por**: Analista de Sistemas **Aprobado por**: Jefe de TI **Objetivo**: Determinar la evaluación del riesgo **Descripción**: Para el desarrollo de esta actividad se hace uso del resultado del análisis de riesgos						**Fecha**: 13 / 04 / 2019	
Cód. Riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PxI)**	**Tolerancia**	**Observación**
R01	Media	Equipos de computo	Daño físico a los routers, switches y cableado expuestos a temperaturas, altas que interrumpa el servicio.	Recursos de red expuestos a riesgos físicos	8	Tolerable	
R02	Media	Impresoras	Mal funcionamiento	Procedimientos inadecuado de mantenimiento	8	Tolerable	
R03	Baja	Escáner	Deterioro	Inadecuada programación de mantenimiento	4	Aceptable	
R04	Crítica	Sistema SISS	Sustracción de Información confidencial	Falta de registros, eventos y actividades criticas realizadas por los usuarios internos	16	No tolerable	
R05	Crítica	Sistema AP	Sustracción de Información confidencial	Falta de registros, eventos y actividades criticas realizadas por los usuarios internos	16	No tolerable	

Fuente: Caso se estudio

Fase – Hacer: Evaluación de Riesgos							
Nombre de la Institución: CuidaSalud **Elaborado por**: Analista de Sistemas **Aprobado por**: Jefe de TI **Objetivo**: Determinar la evaluación de Riesgos **Descripción**: Para el desarrollo de esta actividad se hace uso del resultado del análisis de Riesgos						**Fecha**: 13 / 04 / 2019	
Cód. Riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PxI)**	**Tolerancia**	**Observación**
R06	Media	Sistema SGH	Sustracción de Información confidencial	Falta de registros, eventos y actividades criticas realizadas por los usuarios internos	6	Aceptable	
R07	Media	Sistema Pac	Sustracción de información confidencial	Falta de registros, eventos y actividades criticas realizadas por los usuarios internos	6	Aceptable	
R08	Media	Antivirus y actualizaciones	Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada	Aplicación desactualizada o parchada incorrectamente.	6	Aceptable	
R09	Media	Correo electrónico	Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento	Falta de políticas para el correcto uso del correo electrónico de la institucion	9	Tolerable	

Fuente: Caso se estudio

Fase – Hacer: Evaluación de Riesgos							
Nombre de la Institución: CuidaSalud **Elaborado por**: Analista de Sistemas **Aprobado por**: Jefe de TI **Objetivo**: Determinar la Evaluación de Riesgos **Descripción**: Para el desarrollo de esta actividad se hace uso del resultado del Análisis de Riesgos						**Fecha**: 13 / 04 / 2019	
Cód. Riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PxI)**	**Tolerancia**	**Observación**
R10	Alta	Historia Clínica	Acceso al área por parte de personas ajenas o por usuarios inadecuados	Falta de control de acceso al lugar donde se guarda el documento.	12	Tolerable	
R11	Media	Documentos de respaldo	Divulgación de información confidencial	Accesos inadecuados a los archivos físicos	6	Aceptable	
R12	Crítica	Contraseñas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas.	Contraseñas de usuarios sencillas	20	No tolerable	
R13	Alta	Nombre de usuarios	Acceso a los sistemas por parte de usuarios inadecuados que no deberían tener dicho acceso	Exceso de privilegios para usuarios no indicados.	12	Tolerable	

Fuente: Caso se estudio

Fase – Hacer: Evaluación de Riesgos							
Nombre de la Institución: CuidaSalud **Elaborado por**: Analista de Sistemas **Aprobado por**: Jefe de TI **Objetivo**: Determinar la Evaluación de Riesgo **Descripción**: Para el desarrollo de esta actividad se hace uso del resultado del Análisis de Riesgos						**Fecha**: 13 / 04 / 2019	
Cód. Riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PxI)**	**Tolerancia**	**Observación**
R14	**Crítica**	Servicios externos	Ingeniería social	Personal con desconocimiento de normas de seguridad de información	**16**	No tolerable	
R15	**Alta**	Discos Duros	Hurto o deterioro interno del dispositivo	Almacenamiento inadecuado y sin protección	**12**	Tolerable	
R16	**Alta**	USB	Hurto o deterioro interno del dispositivo	Almacenamiento inadecuado y sin protección	**12**	Tolerable	
R17	**Media**	Lap Top	Hurto o deterioro interno del equipo	Almacenamiento inadecuado y sin protección	**8**	Tolerable	

Fuente: Caso se estudio

Fase – Hacer: Evaluación de Riesgos							
Nombre de la Institución: CuidaSalud **Elaborado por**: Analista de Sistemas **Aprobado por**: Jefe de TI **Objetivo**: Determinar la Evaluación de Riesgos **Descripción**: Para el desarrollo de esta actividad se hace uso del resultado del Análisis de Riesgos						**Fecha**: 13 / 04 / 2019	
Cód. Riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PxI)**	**Tolerancia**	**Observación**
R18	Crítica	Ambientes físicos de consultorios	Accesos de personas ajenas al área para manipular impresoras o escaner y que podrían sustraer información	Áreas físicas sin controles de accesos.	16	No tolerable	
R19	Media	Impresora de placas radiograficas	Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados	Falta de correcta identificación de usuarios y contraseñas para acceder a las pantallas y equipos biomedicos	9	Tolerable	
R20	Media	Equipos biomedicos de hemogramas	Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados	Falta de correcta identificación de usuarios y contraseñas para acceder a las pantallas y equipos biomedicos	9	Tolerable	

Fuente: Caso se estudio

Fase – Hacer: Evaluación de Riesgos							
Nombre de la Institución: CuidaSalud **Elaborado por**: Analista de Sistemas **Aprobado por**: Jefe de TI **Objetivo**: Determinar la Evaluación de Riesgos **Descripción**: Para el desarrollo de esta actividad se hace uso del resultado del Análisis de Riesgos						**Fecha**: 13 / 04 / 2019	
Cód. Riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PxI)**	**Tolerancia**	**Observación**
R21	**Alta**	Equipo de imágenes con grabadora de CD y disco duro	Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados	Falta de correcta identificación de usuarios y contraseñas para acceder a las pantallas y equipos biomedicos	**12**	Tolerable	
R22	**Alta**	Sistema de videovigilancia	Hackeo e Interrupción del sistema por extraños	Contraseñas debiles y falta de cultura de cambio de contraseñas.	**12**	Tolerable	
R23	**Media**	Servidor Backup	Posible deterioro o pérdida de dispositivos de backups	Inadecuada infraestructura física donde se almacenan los dispositivos.	**9**	Tolerable	
R24	**Media**	Servidor Pac	Posible deterioro ó pérdida de dispositivos y estaciones de trabajo de diagnóstico.	Inadecuada infraestructura donde se almacenan los dispositivos.	**9**	Tolerable	

Fuente: Caso se estudio

Fase – Hacer: Evaluación de Riesgos							
Nombre de la Institución: CuidaSalud **Elaborado por**: Analista de Sistemas **Aprobado por**: Jefe de TI **Objetivo**: Determinar la Evaluación de Riesgos **Descripción**: Para el desarrollo de esta actividad se hace uso del resultado del Análisis de Riesgos						**Fecha**: 13 / 04 / 2019	
Cód. Riesgo	**Magnitud**	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor (PxI)**	**Tolerancia**	**Observación**
R25	**Media**	Servidor correo electrónico	Acceso no autorizado a información del servidor, utilización de recursos por parte de personas no autorizadas para enviar correos a terceros .	Falta de control adecuado y monitoreo periodicamente a los accesos otorgados al personal.	**9**	Tolerable	
R26	**Crítica**	Personal interno	Falta de acciones ante incidencias de disponibilidad e integridad de la información del paciente	Ausencia de Gestión de incidencias.	**16**	No tolerable	

Fuente: Caso se estudio

Tabla 20: Tratamiento de Riesgos

Fase – Hacer: Tratamiento de Riesgos						
Nombre de la Institución: CuidaSalud **Elaborado por:** Analista de TI. **Fecha:** 22 / 04 / 2019 **Aprobado por**: Jefe de TI **Objetivo**: Organizar cada amenaza con los controles adecuados para tratar los riesgos identificados **Descripción**: Se hizo uso de las amenazas identificadas en el análisis de riesgos y se proponen los controles.						
Cód. Riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R01	Media	Aceptable	Equipos de computo	Daño físico a los routers, switches y cableado expuestos a temperaturas, altas que interrumpa el servicio.	Mitigar	Recursos de red con protección y seguridad física.
R02	Media	Tolerable	Impresora	Mal funcionamiento	Mitigar	Programación adecuada de mantenimiento
R03	Baja	Aceptable	Escaner	Deterioro	Mitigar	Programación adecuada de mantenimiento
R04	Crítica	No tolerable	Sistema SISS	Sustracción de Información	Mitigar	Políticas de seguridad de usuarios, permisos, autenticación, registro de eventos, RRHH.
R05	Crítica	No tolerable	Sistema AP	Sustracción de Información	Mitigar	Políticas de seguridad de usuarios, permisos, autenticación, registro de eventos, RRHH.
R06	Media	Aceptable	Sistema SGH	Sustracción de Información	Mitigar	Políticas de seguridad de usuarios, permisos, autenticación, registro de eventos, RRHH.
R07	Media	Tolerable	Sistema Pac	Sustracción de Información	Mitigar	Políticas de seguridad de usuarios, permisos, autenticación, registro de eventos, RRHH.

Fuente: Caso se estudio

Fase – Hacer: Tratamiento de Riesgos						
Nombre de la Institución: CuidaSalud **Elaborado por:** Analista de TI. **Fecha: 22 / 04 / 2019** **Aprobado por**: Jefe de TI **Objetivo**: Organizar cada amenaza con los controles adecuados para tratar los riesgos identificados **Descripción**: Se hizo uso de las amenazas identificadas en el análisis de riesgos y se proponen los controles.						
Cód. Riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R08	Media	Aceptable	Antivirus y actualizaciones	Ataque por parte de Hackers a las vulnerabilidades de la aplicación desactualizada	Transferir	Estándares de mejores prácticas de seguridad, actualización de software, controles y filtros.
R09	Media	Tolerable	Correo electrónico	Uso inadecuado del correo electrónico por parte de los usuarios debido a desconocimiento	Mitigar	Estándares de encriptación para los mensajes de correo electrónico, estándares de mejores prácticas de seguridad
R10	Alta	Tolerable	Historia Clínica	Acceso al área por parte de personas ajenas o por usuarios inadecuados	Mitigar	Delimitar el acceso a personal no autorizado y/o sólo con credenciales autorizados.
R11	Media	Aceptable	Documentos de respaldo	Divulgación de información confidencial	Aceptable	Implementación de Políticas de seguridad de información y derechos de protección de datos personales.

Fase – Hacer: Tratamiento de Riesgos						
Nombre de la Institución: CuidaSalud **Elaborado por:** Analista de TI. **Fecha:** 22 / 04 / 2019 **Aprobado por**: Jefe de TI **Objetivo**: Organizar cada amenaza con los controles adecuados para tratar los riesgos identificados **Descripción**: Se hizo uso de las amenazas identificadas en el análisis de riesgos y se proponen los controles.						
Cód. Riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R12	Crítica	No tolerable	Contraseñas	Fácil descifrado de las contraseñas de los usuarios por parte de personas inadecuadas.	Mitigar	Establecer políticas para contraseñas seguras y capacitaciones para concientizar sobre el tema.
R13	Alta	Tolerable	Nombre de usuario	Acceso a los sistemas por parte de usuarios inadecuados que no deberían tener dicho acceso	Mitigar	Implementar registros de control de usuarios (altas y bajas) y de acuerdo a roles y funciones asignar derechos de accesos.
R14	Crítica	No tolerable	Servicios externos	Ingeniería social	Mitigar	Delimitar el acceso a las oficinas a personal externo (proveedores) o no autorizado.
R15	Alta	Tolerable	Discos Duros	Sustracción o deterioro interno del dispositivo	Mitigar	Asignar áreas seguras y con temperaturas adecuadas a los dispositivos informáticos para evitar el deterioro o pérdida
R16	Alta	Tolerable	USB	Sustracción o deterioro interno del dispositivo	Mitigar	Asignar áreas seguras y con temperaturas adecuadas a los dispositivos informáticos para evitar el deterioro o pérdida

Fase – Hacer: Tratamiento de Riesgos						
Nombre de la Institución: CuidaSalud **Elaborado por:** Analista de TI. **Fecha: 22 / 04 / 2019** **Aprobado por**: Jefe de TI **Objetivo**: Organizar cada amenaza con los controles adecuados para tratar los riesgos identificados **Descripción**: Se hizo uso de las amenazas identificadas en el análisis de riesgos y se proponen los controles.						
Cód. Riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R17	Media	Tolerable	Lapa Top	Hurto o deterioro interno del equipo	Mitigar	Asignar áreas seguras y con temperaturas adecuadas a los dispositivos informáticos para evitar el deterioro o pérdida
R18	Crítica	No tolerable	Ambientes físicos de atención	Accesos de personas ajenas al área para manipular impresoras o escaner y que podrían sustraer información	Mitigar.	Controles físicos de entrada, aplicar seguridad en las instalaciones.
R19	Media	Tolerable	Impresoras de placas radiográficas	Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados	Transferir	Referenciar políticas de seguridad lógica de la información que se almacena en los equipos biomédicos
R20	Media	Tolerable	Equipos biomédicos de hemogramas	Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados	Transferir	Referenciar políticas de seguridad lógica de la información que se almacena en los equipos biomédicos

Fase – Hacer: Tratamiento de Riesgos						
Nombre de la Institución: Cuida Salud **Elaborado por:** Analista de TI. **Fecha:** 22 / 04 / 2019 **Aprobado por**: Jefe de TI **Objetivo**: Organizar cada amenaza con los controles adecuados para tratar los riesgos identificados **Descripción**: Se hizo uso de las amenazas identificadas en el análisis de riesgos y se proponen los controles.						
Cód. Riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R21	Alta	Tolerable	Equipo de imágenes con grabadora de CD y disco duro	Fácil acceso a las pantallas por parte de personas ajenas a la empresa o por usuarios inadecuados	Transferir	Referenciar políticas de seguridad lógica de la información que se almacena en los equipos biomédicos
R22	Alta	Tolerable	Sistema de Video vigilancia	Hackeo e Interrupción del sistema por extraños	Transferir.	Convocar a concurso a empresas certificada en seguridad de la información y seguridad física que garantice un servicio seguro.
R23	Media	Tolerable	Servidor Backus	Inadecuada infraestructura física donde se almacenan o guardan los dispositivos de backups	Mitigar	Comprobar la vida útil de los soportes que se utilizan para realizar las copias, Plan de mantenimiento de hardware y software de los soportes de mantenimiento y asegurar las condiciones de climatización del lugar donde se almacena para su adecuada conservación.

Fase – Hacer: Tratamiento de Riesgos						
Nombre de la Institución: Cuida Salud **Elaborado por:** Analista de TI. **Fecha: 22 / 04 / 2019** **Aprobado por**: Jefe de TI **Objetivo**: Organizar cada amenaza con los controles adecuados para tratar los riesgos identificados **Descripción**: Se hizo uso de las amenazas identificadas en el análisis de riesgos y se proponen los controles.						
Cód. Riesgo	**Magnitud**	**Tolerancia**	**Activo**	**Amenaza**	**Estrategia**	**Controles**
R24	Media	Tolerable	Servidor Pac	Inadecuada infraestructura física	Transferir	Los servidores deben tener un sistema de seguridad física con estándares apropiados como: control de accesos mediante sistema electrónico, control de presencia e intrusión, control de apertura de puertas, sistema de circuito cerrado de TV y servicio de vigilancia física permanente. (24x7)
R25	Media	Tolerable	Servidor de correo electrónico	Acceso no autorizado a información del servidor, utilización de recursos por parte de personas no autorizadas para enviar correos a terceros .	Transferir	Solicitar a proveedor del servicio servidores con altos niveles de control de seguridad.
R26	Crítica	No Tolerable	Personal Interno	Falta de acciones ante incidencias de disponibilidad e integridad de la información del paciente	Mitigar	Reportar incidencias encontradas en la disponibilidad e integridad de la información del paciente y establecer procedimientos de gestión.

Tabla 21: Identificación y descripción de recursos para los controles

Identificación y descripción de recursos para los controles							
Registrado por: Jefe de TI **Objetivo**: Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados **Descripción**: Para el desarrollo de esta actividad se debe elegir los riesgos pconsiderados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							**Fecha**: 06 / 05 / 2019
Cod.del riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
R04	Crítica	Sistema SISS	Sustracción de información	Mitigar	Concientización de uso de contraseñas seguras y generar cambios de contraseña en periodos cortos.	Programar en forma periódica capacitaciones	Plan de Capacitación con experto en S.I.
R05	Crítica	Sistema AP	Sustracción de información	Mitigar	Concientización de uso de contraseñas seguras y generar cambios de contraseña en periodos cortos.	Programar en forma periódica capacitaciones	Plan de Capacitación con experto en S.I.
R10	Alta	Historia Clínica	Acceso al área por parte de personas ajenas o por usuarios inadecuados	Mitigar	Sólo se deberá permitir el acceso con credenciales al personal autorizado	Aplicar normas y asignar roles	Políticas de acceso a áreas restringidas

Identificación y descripción de recursos para los controles							
Registrado por: Jefe de TI **Objetivo**: Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados **Descripción**: Para el desarrollo de esta actividad se debe elegir los riesgos considerados como altos y críticos que se obtienen de la plantilla del tratamiento del riesgo.							**Fecha**: 06 / 05 / 2019
Cod.del riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
R12	Crítica	Contraseñas	Fácil descifrado de las contraseñas de los usuarios	Mitigar	Establecer políticas para contraseñas seguras, capacitar, concientizar e incluir las sanciones de incumplimiento en el PAS	Implementar políticas, programar capacitaciones y comunicar el PAS	Politicas de control de contraseñas, registro de eventos
R13	Alta	Nombre de usuario	Acceso a los sistemas por parte de usuarios inadecuados	Mitigar	Implementar registros de control de usuarios (altas y bajas) y de acuerdo a roles y funciones asignar derechos de accesos.	Implementar políticas para la gestión de contraseñas e identificación de usuarios no autorizados	Políticas de control de usuarios, asignación de permisos
R14	Crítica	Servicios Externos	Ingeniería social.	Mitigar	Concientización contínua del personal responsable de la información del paciente	Capacitación contínua al personal	Planes de capacitación y monitoreo

Identificación y descripción de recursos para los controles							
Registrado por: Jefe de TI **Objetivo**: Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados **Descripción**: Para el desarrollo de esta actividad se debe elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							**Fecha**: 06 / 05 / 2019
Cod.del riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
R18	Crítica	Ambientes físicos de atención	Acceso y manejo de las equipos de computo por parte de usuarios inadecuados.	Mitigar	Monitoreo con cámaras de vigilancia (24/7)	Instalar nuevos puntos de videos vigilancia en áreas restringidas, capacitar y aplicar sanciones	Sistema de videovigilancia
R22	Alta	Sistema de Videovigilancia	Hackeo e Interrupción del sistema por extraños	Transferir.	Contratar empresa certificada en seguridad de la información y seguridad física	Convocar a concurso empresas del rubro	Financiamiento

Identificación y descripción de recursos para los controles							
Registrado por: Jefe de TI **Objetivo**: Determinar las actividades y los recursos necesarios para el cumplimiento de los controles seleccionados **Descripción**: Para el desarrollo de esta actividad se debe elegir los riesgos considerados como altos y críticos que obtienen de la plantilla del tratamiento del riesgo.							**Fecha**: 06 / 05 / 2019
Cod.del riesgo	**Magnitud**	**Activo**	**Amenaza**	**Estrategia**	**Controles**	**Actividades**	**Recursos**
R26	Crítica	Personal Interno	Falta de acciones ante incidencias de disponibilidad e integridad de la información del paciente	Mitigar	Reportar incidencias encontradas en la disponibilidad e integridad de la información del paciente y establecer procedimientos de gestión.	Supervisar el procesamiento y manejo de la información en materia de seguridad de la información	Organizaciones profesionales y proveedores de seguridad de la información, conferencias, seminarios online, boletines, etc.

Tabla 22: Comunicación de Controles

Comunicación de Controles					
Registrado por: Jefe de TI **Objetivo**: Informar a la gerencia y al personal de la institución los controles a implementar				**Fecha:** **13 / 05 / 2019**	
Descripción: Para el desarrollo de esta actividad se deben seleccionar medios de comunicación para cada control.					
Controles	**Actividades**	**Riesgos asociados**	**A quien comunicar**	**Quien debe comunicar**	**Tipo de comunicación**
Concientización de uso de contraseñas seguras y generar cambios de contraseña en periodos cortos.	Programar en forma periódica capacitaciones	R04, R05,	Gerente General Hospital	Jefe de TI	**Escrita**
Establecer Políticas para contraseñas seguras y capacitaciones sobre el tema	Programar en forma periódica capacitaciones y hacer auditorias de control	R12	Gerente General Hospital	Jefe de TI	**Escrita**
Admitir acceso con credenciales a personal autorizado	Definir y asignar roles en base a normas	R10,	RRHH	Jefe de TI	**Escrita**

Comunicación de Controles					
Registrado por: Jefe de TI **Objetivo**: Informar a la gerencia y al personal de la institución los controles a implementar				**Fecha:** **13 / 05 / 2019**	
Descripción: Para el desarrollo de esta actividad se deben seleccionar medios de comunicación para cada control.					
Controles	**Actividades**	**Riesgos asociados**	**A quien comunicar**	**Quien debe comunicar**	**Tipo de comunicación**
Implementar registros de control de usuarios (altas y bajas) y de acuerdo a roles y funciones asignar derechos de accesos.	Procedimiento de registro y validación de usuarios	**R13,**	Gerente General Hospital	Jefe de TI	Escrita y por correo electrónico
Ingeniería social.	Educación al usuario sobre técnicas de ingeniería social	R14	Gerente General Hospital y Oficina de Capacitación	Jefe de TI	Escrita y por correo electrónico
Monitoreo con cámaras de vigilancia (24/7) en áreas críticas	Instalar nuevos puntos de videos vigilancia en áreas restringidas, aplicar normas	R18, R10	Administración y Oficina de Ingenieria hospitalaria	Jefe de TI	Escrita

Comunicación de Controles					
Registrado por: Jefe de TI **Objetivo**: Informar a la gerencia y al personal de la institución los controles a implementar				**Fecha:** 13 / 05 / 2019	
Descripción: Para el desarrollo de esta actividad se deben seleccionar medios de comunicación para cada control.					
Controles	**Actividades**	**Riesgos asociados**	**A quien comunicar**	**Quien debe comunicar**	**Tipo de comunicación**
Contratar empresa certificada en seguridad de la información y seguridad física	Convocar a concurso empresas del rubro	R22	Administración y Oficina de Ingeniería	Jefe de TI	Escrita
Reportar incidencias encontradas en la disponibilidad e integridad de la información del paciente y establecer procedimientos de gestión.	Supervisar el procesamiento y manejo de la información en materia de seguridad de la información	**R26**	Gerencia General	Jefe de TI, Jefe de Capacitación	Escrita

Tabla 23: Auditoría Interna

Auditoria Interna								
Realizado por : Empresa externa. **Aprobado por**: Gerente General de la Institución.								**Fecha**: 02-09-2019
Objetivo: Establecer un Plan de Auditoria								
N	**Acción**	**Involucrados**	**Recursos**	**Tarea**	**Inicio**	**Fin**	**Resultados**	**Sugerencias**
01	Reunión de Inicio	**Responsable**: Auditor interno -Gerente General -Jefe de TI -Administrador -Usuario Interno	-Sala de reunión de Gerencia General -Laptop con accesos a sistemas de información institucionales	1. Plan de Auditoría 2. Ejecutar la reunión				
02	Auditoria al Gerente General	**Responsable**: Auditor interno -Gerente General	Sala de reunión Gerencia General -Laptop con accesos a sistemas de información instit.	1.Ejecutar la auditoria 2.Solicitar evidencia complementaria				
03	Auditoría al Jefe de TI	**Responsable**: Auditor interno. -Jefe de TI	Oficina de TI Solicitar reportes de incidencias y gestión de contraseñas	1.Ejecutar auditoría 2.Solicitar evidencia de los controles de TI				

Auditoria Interna								
Realizado por : Empresa externa. **Aprobado por**: Gerente General de la Institución.								**Fecha**: 02-09-2019
Objetivo: Establecer un Plan de Auditoria								
N	**Acción**	**Involucrados**	**Recursos**	**Tarea**	**Inicio**	**Fin**	**Resultados**	**Sugerencias**
04	Auditoría al Administrador	**Responsable**: Auditor interno -Administrador	-Sala de reuniones de Administración - Evidencia de acciones realizadas	1. Ejecutar la reunión 2. Verificación de cumplimiento de actividades.				
05	Auditoría al usuario Interno	**Responsable**: Auditor interno -Usuario Interno	Jefatura de áreas de atención al paciente -Verificación de equipos de computo y equipoa biomédicos	1.Ejecutar reunión 2.Check list del cumplimiepnto de Políticas implementadas				

Tabla 24: Mejora Contínua

Mejora Contínua					
Registrado por: Experto en Seguridad de la Información **Objetivo**: Establecer un plan de mejora contínua **Descripción**: Para el desarrollo de esta actividad se debe tener en cuenta los proyectos propuestos, monitorearlos y tomar acciones para mejorar el proyecto					Fecha: 16/09/2019
N°	**Plan de acción**	**Riesgos involucrados**	**Controles**	**Fecha Inicio**	**Fecha fin**
1	Plan de Políticas de Seguridad de la Información	R04, R05, R12, R19, R20, R21	Definición de un conjunto de políticas para la seguridad de la infotmación, aprobada por la Gerencia General, publicada con documento resolutivo y comunicada a todos los empleados, las mismas que deberán ser revisadas a intervalos planificados en caso ocurrieran cambios significativos y con ello asegurar la eficacia contínua		
2	Plan de Capacitación	R10, R13, R14, R18	Programar planes de capacitación con expertos en Seguridad de la Información, y especialistas en ciberseguridad, así como en legislación laboral y ética profesional a través de los convenios marcos de las universidades locales con que cuenta la institución.		
3	Proyecto de Gestión de eventos e incidencias	R08, R13, R24, R26	Implementar un Sistema de Gestión de Incidencias de manera que se puedan monitorizar los eventos ocurridos y restaurar cuanto antes la operatividad del servicio.		
4	Proyecto: Implementación de un Help Desk	R04, R05, R26	Implementar este recurso de información y asistencia para resolver problemas con los equipos de computo y dispositivos		

Tabla 25: Seguimiento de Proyectos

Seguimiento de Proyectos														
Responsable: Área o servicio de aplicación: Fecha:														
Objetivo: Permitir determinar el progreso de las actividades realizadas en los proyectos y tomar medidas necesarias para resolver problemas e incidentes, haciendo los ajustes necesarios en los objetivos y actividades.														
Etapa 1	Fecha Inicio	Fecha Fin	Cumplimiento de etapas del Proyecto											Recomendaciones
			Etapa 1			**Etapa 2**			**Etapa 3**			**Etapa 4**		
Actividades:			**NC**	**C**	**CP**	**NC**	**C**	**CP**	**NC**	**C**	**CP**	**NC**	**C**	**CP**	
1.Act.1														
2.Act.2														
3.Act.3														
4.Act.4														
NC: No ha cumplido en la fecha establecida C: Ha cumplido en la fecha establecida CP: Cumple parcialmente en la fecha establecida														
Conclusiones: Análisis del seguimiento de las etapas evaluadas.														

CAPÍTULO IV: CONCLUSIONES

1. Del análisis realizado al caso de estudio se evidenció que la institución de salud no cuenta con normas, políticas o alguna estrategia para gestionar la seguridad de la información, la implemenración del Modelo de Gestión de Seguridad de la Información basado en normas y estándares internacionales permitieron cumplir los 7 lineamientos de las Políticas de Seguridad de la Información establecida en la normativa vigente oficial (Resolución 002-2019-PCM/SEGDI), la misma que esta considerada en el Plan Estratégico al año 2020, relacionada a Seguridad de la Información.

2. La revisión analítica de las normas y marcos de trabajo basados en estándares internacionales han permitido construir un Modelo de Gestión de Seguridad de la Infomación que ha logrado implementar controles para apoyar los procesos de atención al paciente en el caso de estudio.

3. Mediante el juicio de 3 profesionales expertos, se pudo concluir que el Modelo de Gestión de Seguridad de la Información implementado cuenta con una concordancia de Kendall de .198, lo que demuestra que existe proporción entre los expertos y un resultado de .668 en el estadístico del Alfa de Cronbach de elementos estandarizados, concluyendo que es un modelo muy confiable, lo que permite que sea aplicado a cualquier institución de salud.

4. Implementación de 04 proyectos en cumplimiento de los requisitos legales del Estado, relacionados a la transformación digital, interoperabilidad y seguridad de los sistemas de información, como parte de la estrategia en salud electrónica.

REFERENCIAS BIBLIOGRÁFICAS

[1] O. O. D. Security, «Openn Data Security,» 29 Noviembre 2016. [En línea]. Available: https://opendatasecurity.io/es/5-companias-que-mas-han-sufrido-por-los-ataques-informaticos/. [Último acceso: 28 06 2019].

[2] P. Andina, «Andina,» 26 08 2018. [En línea]. Available: https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html.

[3] «Gestión,» 06 12 2018. [En línea]. Available: https://gestion.pe/economia/mercado-ciberseguridad-peru-crecera-us-220-millones-2021-nndc-252046.

[4] F. d. A. Alarcon Cubas, «Repositorio de la Universidad Nacional Pedro Ruiz Gallo,» 2018. [En línea]. Available: http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/3476/BC-TES-TMP-2283.pdf?sequence=1&isAllowed=y.

[5] V. R. Puyen Santos, «Repositorio de la Universidad Nacional Pedro Ruiz Gallo,» 2019. [En línea]. Available: http://repositorio.unprg.edu.pe/handle/UNPRG/3331.

[6] C. A. Arenas Villanueva y D. l. S. M. Diana, «Repositorio Universidad Nacional Pedro Ruiz Gallo,» 2019. [En línea]. Available: http://repositorio.unprg.edu.pe/handle/UNPRG/3830.

[7] S. d. G. Digital, «Secretaría de Gobierno Digital,» Julio 2019. [En línea]. Available: https://www.peru.gob.pe/normas/docs/Estandares_Interoperabilidad_PIDE_SEGDI.pdf.

[8] M. d. Trabajo, «Plan Estrategico Insitucional 2017-2021,» Lima, 2017.

[9] L. A. G. Alarcón, «Revista Scielo Analytics,» Octubre 2017. [En línea]. Available: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-61802017000300042. [Último acceso: 01 Agosto 2019].

[10] C. d. l. República, «Ley 29733 Ley de Protección de datos personales,» El Peruano, Lima, 2011.

[11] S. d. G. Digital, «Política Nacional de Ciberseguridad,» Lima, 2016.

[12] M. d. Salud, «Políticas de Seguridad de la Información del Ministerio de Salud-MINSA,» 09 Julio 2015. [En línea]. Available: http://www.minsa.gob.pe/transparencia/dge_normas.asp. [Último acceso: 10 06 2019].

[13] V. R. Talavera Aguilar, «Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013,» Pontificia Universidad Católica del Perú, Lima, 2015.

[14] C. T. Omar, «Elaboración de un Plan de Seguridad de la Información,» UOC, España, 2013.

[15] D. l. C. V. R. Eduardo, «Propuesta de Políticas basadas en buenas prácticas para la gestión de seguridad de la información en la Municipalidad Provincial de Paita,» Universidad Católica Los Ángeles de Chimbote, Chimbote, 2016.

[16] E. A. Tarrillo Clavo, «Metodología para un sistema de gestion de seguridad de la información basado en la NTP 17799 en la Administración de la Municipalidad distrital de Lambayeque,» Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Setiembre 2013-Febrero 2014.

[17] R. S. R. Alejandro, «Gestión de seguridad de la información y los servicios críticos de las universidades: un estudio de tres casos en Lima Metropolitana,» Universidad Nacional Mayor de San Marcos, Lima, 2007.

[18] M. A. Villena Aguilar, «Sistema de Gestión de Seguridad de Información para una institucion financiera,» Pontificia Universidad Católica del Perú Facultad de Ciencia e Ingeniería, Lima, 2006.

[19] C. d. R. d. l. U. Españolas, «Gobierno de las Tecnologías de la Información en Universidades.,» España, 2016.

[20] IsoTools, «La norma ISO 27001: Aspectos claves de su diseño e implantacion,» [En línea]. Available: www.isotools.org.

[21] Esan, «¿Que es y para que sirve la Norma ISO 27001?,» 03 Mayo 2016. [En línea]. Available: https://www.esan.edu.pe/apuntes-empresariales/2016/05/que-es-y-para-que-sirve-la-norma-iso-27001/. [Último acceso: 02 07 2019].

[22] P. I. J. Angel, «COBIT 5 - ISACA,» 03 Mayo 2012. [En línea]. Available: https://www.isaca.org/chapters7/Monterrey/Events/Documents/20120305%20CobiT%205.pdf.

[23] S. B. M. y. otros, «Un proceso práctico de Análisis de Riesgos de Activos de Información,» *Comtel: IV Congreso Internacional de Computación y Telecomuicaciones,* p. 7, 2012.

[24] P. d. C. d. Ministros, «Taller de Implementación de la norma ISO 27001,» Oficina Nacional de Gobierno Electrónico , Lima, 2018.

[25] A. A. M. y. otros, «La historia clínica: un documento básico para el personal médico,» *Medisan - Scielo,* vol. 14, nº 7, 2010.

[26] N. T. P. N.-I. 27001:2014, «UTP,» 2014. [En línea]. Available: https://canvas.utp.edu.pe/courses/8870/files/42244.

[27] R. N. d. I. y. E. d. Ecuador, «Gestión del Riesgo de las TI NTC 27005,» [En línea]. Available: https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI9.pdf.

[28] L. A. Romulo, COBIT 5: Un marco de Negocio para el Gobierno y la Gestión de la Empresa, Lima: EEUU, 2012.

[29] Security&IT, «Análisis y Gestión del Riesgo - Magerit,» 2019. [En línea]. Available: https://www.secureit.es/procesos-y-gobierno-it/analisis-y-gestion-de-riesgos/.

[30] G. C. d. C. Baldecchi Q. Rodrigo, «Implementación efectiva de un SGSI ISO 27001 - ISACA,» 04 sep. 2014. [En línea]. Available: https://m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposici%C3%B3n%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf. [Último acceso: 24 Junio 2019].

[31] I. 27001:2005, «Estándar Internacional ISO/IEC 27001:2005,» Primera Edición, 2005 .

[32] A. Corletti Estrada, «ISO 27001: Los Controles,» Noviembre 2006. [En línea]. Available: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf. [Último acceso: 25 06 2019].

[33] T. P. y. otros, «Revista Elsevier España,» Elsevier, Abril-Junio 2013. [En línea]. Available: https://www.elsevier.es/es-revista-diagnostico-prenatal-327-articulo-el-documento-consentimiento-informado-realizacion-S217341271200056X. [Último acceso: 30 06 2019].

[34] W. H. Curioso, «eSalud en Perú: Implementación de Políticas para el fortalecimiento de sistemas de información en salud,» *Pan American Journal of Public Health,* vol. 35, nº 5/6, p. 438, 2014.

[36] Y. Valle, «El Alineamiento estratégico y su repercusión en los resultados empresariales,» 10 Agosto 2015. [En línea]. Available: https://www.esan.edu.pe/conexion/actualidad/2015/08/10/el-alineamiento-estrategico-y-su-repercusion-en-los-resultados-empresariales/. [Último acceso: 10 06 2019].

ANEXOS

Anexo 1: Consentimiento informado para participantes de investigación

Consentimiento informado para participantes de investigación

Yo, _____

Acepto participar voluntariamente en esta investigación, conducida por la investigadora. He sido informado (a) de que la meta de este estudio es la elaboración de un Modelo de Gestión de Seguridad de la Información para apoyar el proceso de atención al paciente en una institución de salud.

Me han indicado también que tendré que responder cuestionarios y preguntas en una entrevista, lo cual tomará el tiempo necesario.

Reconozco que la información que yo provea en el curso de esta investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de este estudio sin mi consentimiento. He sido informado de que puedo hacer preguntas sobre el proyecto en cualquier momento y que puedo retirarme del mismo cuando así lo decida, sin que esto acarree perjuicio alguno para mi persona. De tener preguntas sobre mi participación en este estudio, puedo contactar a la autora al teléfono…….

Entiendo que una copia de esta ficha de consentimiento me será entregada.

---------- ----------

Nombre del Participante Firma del Participante

Fecha: (en letras de imprenta)

Fuente: http://blog.pucp.edu.pe/blog/eticapsico/2008/05/24/ejemplo-de-

Anexo 2: Formato de carta para participantes de la investigación

Formato: Carta dirigida al Participante

Sr.(a):

La presente investigación es conducida por ……..., alumna de la escuela de post grado de:…….. La meta de este estudio es elaborar un Modelo de Gestión de Seguridad de la Información en el proceso de atención al paciente en instituciones de salud.

Si usted accede a participar en este estudio, se le pedirá responder preguntas en una entrevista (o completar una encuesta, o lo que fuera según el caso). Esto tomará el tiempo estrictamente necesario. Se tomará nota de las conversaciones durante las sesiones de entrevista.

La participación es este estudio es estrictamente voluntaria. La información que se recoja será confidencial y no se usará para ningún otro propósito fuera de los de esta investigación. Sus respuestas al cuestionario y a la entrevista serán codificadas usando un número de identificación, por lo tanto, serán anónimas.

Si tiene alguna duda sobre este proyecto, puede hacer preguntas en cualquier momento durante su participación en él. Igualmente, puede retirarse del proyecto en cualquier momento sin que eso lo perjudique en ninguna forma. Si alguna de las preguntas durante la entrevista le parecen incómodas, tiene usted el derecho de hacérselo saber al investigador o de no responderlas.

Desde ya le agradecemos su participación.

La Autora

Anexo 3: Cuestionario para Jefes y encargados de las áreas de Soporte Informático de las instituciones de salud

Objetivo: Situación actual respecto al manejo de seguridad de la información dentro de un centro de salud.
Dirigido a: Jefe del área de Soporte Informático de la institución.

1. ¿Tiene conocimiento sobre la normatividad vigente respecto a Lineamientos de Política de Seguridad de la Información de su institución?

   SI: _____ NO: _____
2. ¿Han implementado su plan de seguridad de información acordes con las disponibilidades técnicas actuales de su institución?
   SI: _____ NO: _____

3. ¿El área de Soporte Informático ha adoptado las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales en su banco de datos?
   SI: _____ NO: _____

4. ¿El área de Soporte Informático ha considerado dentro de sus proyectos establecer un modelo integral para el desarrollo de los planes de seguridad de la información?
   SI: _____ NO: _____

5. ¿La Alta dirección de su institución ha manifestado su apoyo y compromiso en establecer las líneas de actuación en relación al establecimiento de Políticas de Seguridad en toda la organización?
   SI: _____ NO: _____

6. ¿Con que frecuencia el área de soporte informático ha registrado incidentes relativos a la accesibilidad de los sistemas por parte de usuarios no autorizados?
   Nunca ( ) Raramente ( ) Ocasionalmente ( ) Frecuentemente ( ) Muy Frecuente ( )

7. ¿Con que frecuencia el área de soporte informático ha recibido incidentes respecto a la integridad de la información de los pacientes?
   Nunca ( ) Raramente ( ) Ocasionalmente ( ) Frecuentemente ( ) Muy Frecuente ( )

8. ¿Con que frecuencia el área de soporte informático ha evidenciado incidentes en materia de confidencialidad, poniendo en riesgo la información sensible del paciente?
   Nunca ( ) Raramente ( ) Ocasionalmente ( ) Frecuentemente ( ) Muy Frecuente ( )

9. Usted, como usuario interno de su organización ¿tiene conocimiento del incumplimiento de las medidas de seguridad de la información y su

responsabilidad administrativa, civil o penal del mal uso que se haga de los sistemas de información?

SI: _____ NO: _____

10. ¿Identifica los requerimientos de seguridad de la información relacionados con TI que enfrenta su institución?
    SI: _____ NO: _____
11. ¿En su institución existen controles para mitigar los riesgos que se presenten en materia de integridad, disponibilidad y confidencialidad de la información de su institución?
    SI: _____ NO: _____
    ¿Cuáles son esos controles?.....
12. ¿Existe un sistema de gestión de accesos para los sistemas de información?
    SI: _____ NO: _____
13. ¿Están definidas las facultades y atributos de los usuarios que utilizan los sistemas de información de su institución?
    SI: _____ NO: _____
14. ¿Existen controles que permitan verificar el cumplimiento de la normatividad vigente respecto a seguridad de la información por parte de los usuarios en su institución?
    SI: _____ NO: _____
15. ¿Están formalmente establecidos los niveles de autorización de acceso y ejecución de las funciones de procesamiento de las aplicaciones que garanticen reducir el riesgo de error y fraudes en el área de soporte informático?
    SI: _____ NO: _____
16. ¿Existen adecuados sistemas de control y autenticación para evitar accesos no autorizados de terceros y ataques externos a la información crítica?
    SI: _____ NO: _____
17. ¿Existen controles adecuados para detectar la instalación de software no autorizado?
    SI: _____ NO: _____
18. ¿Existen controles para proteger la información contenida en documentos, medios de almacenamiento, u otros dispositivos en los servicios críticos de su institución?
    SI: _____ NO: _____
19. ¿Cuentan con áreas protegidas para el procesamiento de información y evitar daños a los equipos de TI en donde se almacena y distribuye la información de su institución?
    SI: _____ NO: _____
20. ¿La transferencia de información en su institución son seguros? ¿Podría mencionar cómo?
    SI: _____ NO: _____

--

21. Su institución cuenta con un sistema de registro sobre las consultas realizadas por los usuarios
    SI: _____ NO: _____

22. ¿Cuenta con vigilancia privada en las instalaciones donde se almacenan las historias clínicas?
    SI: _____ NO: _____

23. ¿Su institución cuenta con un comité de seguridad de información?
    SI: _____ NO: _____

24. ¿Tienen identificados los activos de información críticos dentro de su organización?
    SI: _____ NO: _____

25. ¿El área de soporte informático donde labora cuenta con planes de continuidad del negocio y recuperación en caso de incidentes en los sistemas de información?
    SI: _____ NO:_____

Fuente: Cobit 5: APO13: Gestión de Seguridad.

Anexo 4: Gráficos de resultados de las encuestas realizadas a las áreas de TI

Gráfico No1

Gráfico No2

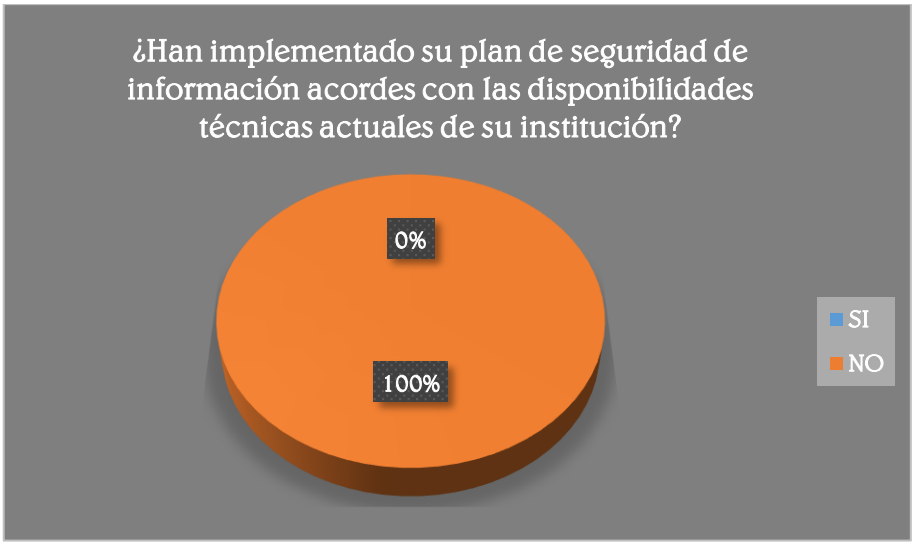


Gráfico No.3

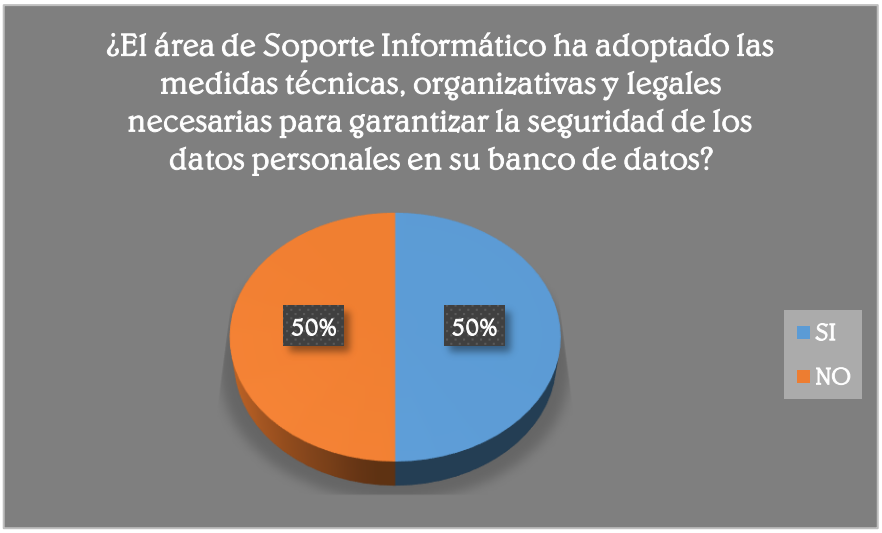


Gráfico No4

Gráfico No5

Gráfico No6

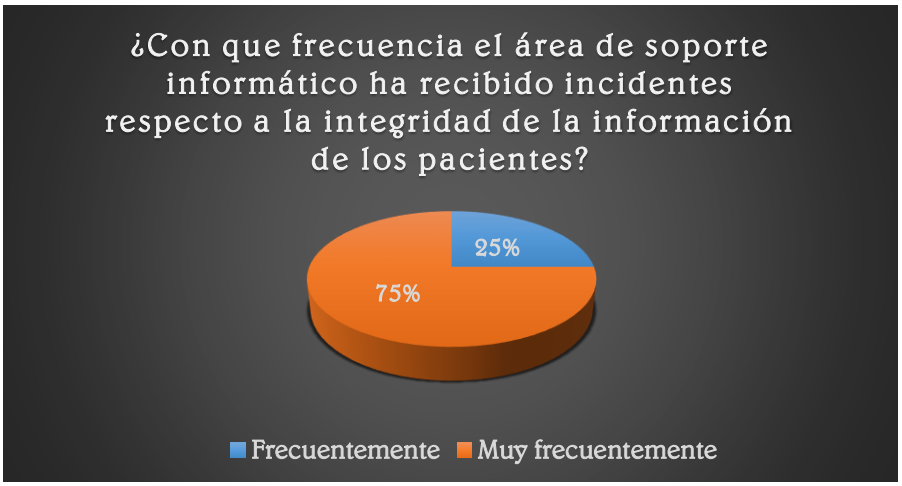


Gráfico No7

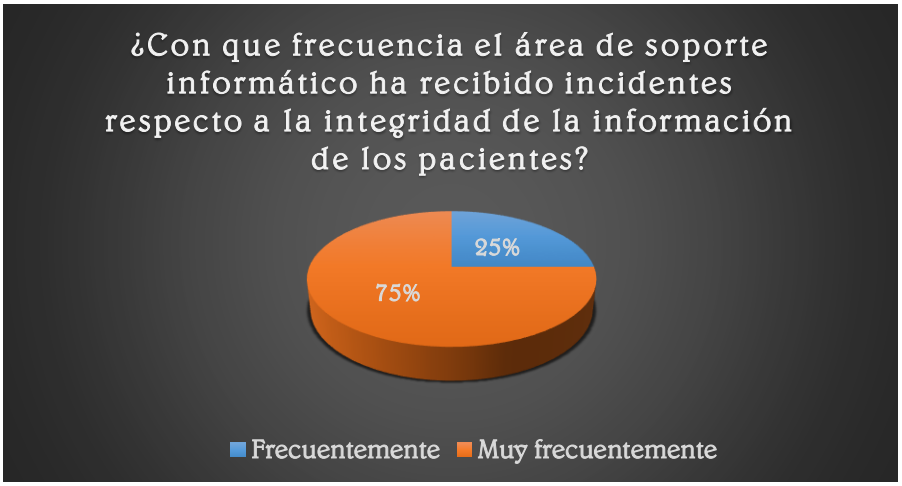


Gráfico No8

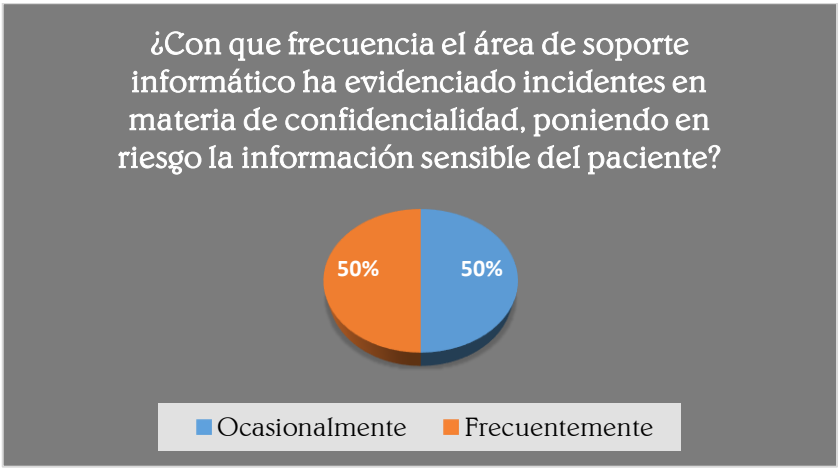


Gráfico No9

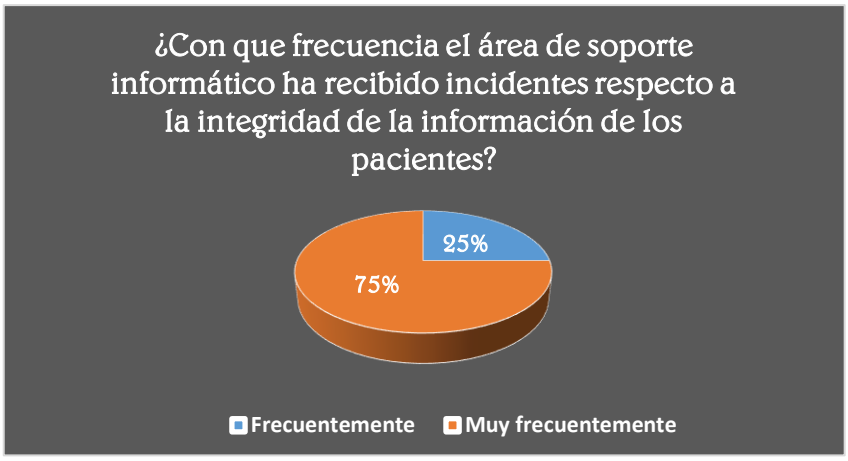


Gráfico No10

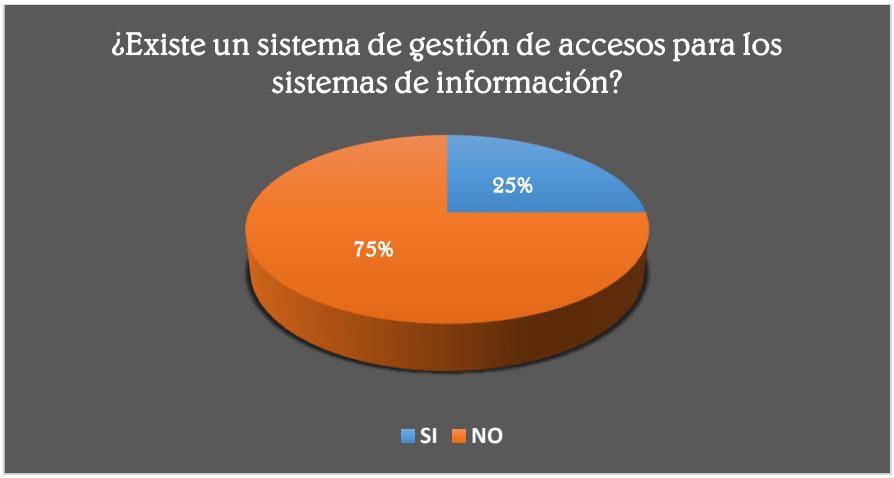


Gráfico No11

Gráfico No12

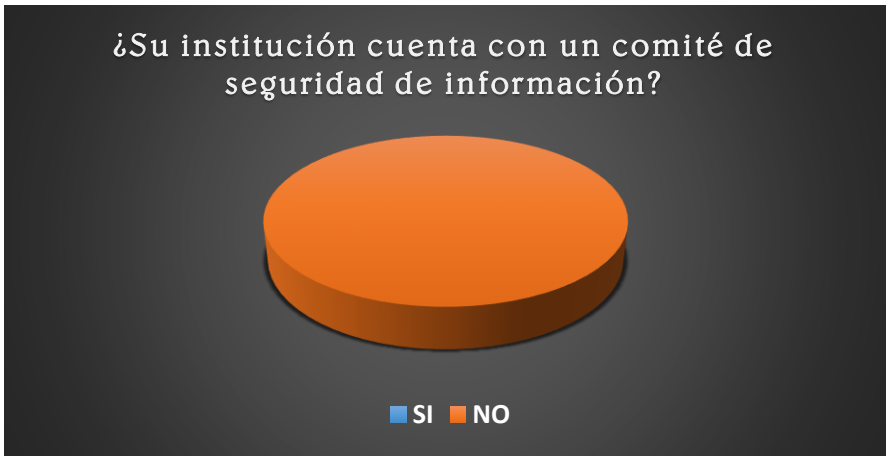


Gráfico No13

Grafico No14

Anexo 5: Análisis del resultado de encuestas realizadas

(Instituciones del sector)

De acuerdo a lo hallado a través de las encuestas realizadas a las instituciones de salud del Estado, a las reuniones de trabajo, a las evidencias y observaciones hechas se puede concluir en lo siguiente:

- El 75% de las áreas de soporte informático dependen estructuralmente de las Gerencias Centrales de Tecnologías de la Información y Comunicaciones, ubicadas físicamente en sus sedes centrales en la ciudad de Lima, lo que trae retraso en la implementación de directivas y normas vigentes por la cantidad de autorizaciones dentro de su estructura jerárquica.
- El 75% de las oficinas de soporte informático tienen conocimiento de los lineamientos de Políticas de seguridad de la información, sin contar con alguna herramienta que pueda ser implementada.
- Todas las instituciones de salud visitadas y encuestadas no han implementado un plan de seguridad de la información acordes con las disponibilidades técnicas actuales.
- El 50% de ellas, han adoptado medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales dentro de su infraestructura física como área.
- El 75% de directivos y actuales gerentes no han manifestado el apoyo y compromiso en establecer líneas de actuación en relación a Políticas de Seguridad en toda la organización.
- El 50% de las áreas de soporte informático ha registrado ocasionalmente incidentes relativos a la accesibilidad de los sistemas de información por parte de usuarios internos no autorizados, y la otra mitad nunca.

- El 75% de las áreas de TI ha recibido muy frecuentemente incidentes respecto a la integridad de la información del paciente y el 25% frecuentemente por parte del cliente externo.
- El 50% del personal de informática ha evidenciado incidentes en materia de confiabilidad, poniendo en riesgo la información sensible del paciente por parte del personal de la institución.
- El 75% del personal de informática sí identifica los requerimientos de seguridad de la información que enfrenta su institución.
- El 75% de las áreas no cuenta con un sistema de gestión de accesos para los sistemas de información.
- El 75% de las áreas de informática no cuenta con controles adecuados para detectar la instalación de software no autorizado.
- Ninguna institución cuenta con comités de seguridad de la información y tampoco tienen identificados los activos críticos de información dentro de sus organizaciones.

En resumen, y según los resultados obtenidos se puede evidenciar que ninguna institución de salud cuenta con una gestión en seguridad de la información implementada poniendo en riesgo los activos que respaldan los procesos de atención a los pacientes, sin embargo, cabe mencionar que los empleados de las diferentes oficinas de soporte informático conocen los lineamientos y políticas de seguridad de la información, pero no cuentan con los recursos para la implementación adecuada.

Anexo 6: Matriz RACI de roles y responsabilidades

	Digitadores	programadores	soporte técnico	Ing. de Sistemas	Jefe de TI	Técnicos asist.	Med. Residentes	Med. Asistentes	Jefes de SSAA	Estadista	Epidemiólogo	COPOES	PADOMI	Jefes de dpto.	Gerente Seguros	Gerente Hospital	Gerente de C.P.	Gerente de Red	Jefe OCI-ODIII
Módulo de datos del paciente	**R**			**C**	**C**	**R**	**R**	**C**	**I**					**I**	**I**	**I**	**I**	**I**	**I**
Validación de datos personales				**C**	**C**					**A**	**A**				**I**				**I**
Asignación de citas	**R**				**C**				**I**	**A**	**A**			**I**		**I**	**I**	**I**	**I**
Módulo de ayuda al diagnóstico y tto.	**R**			**C**	**C**		**R**	**C**	**C**	**I**	**A**			**I**		**I**			**I**
Módulo de farmacia	**R**			**C**	**C**	**R**			**I**	**I**				**I**		**I**		**I**	**I**
Módulo de hospitalización	**R**			**C**	**C**	**R**	**R**	**C**	**I**	**A**	**A**			**I**		**I**		**I**	**I**
Datos operacionales: egresos	**R**			**C**	**C**	**R**	**R**	**C**	**I**	**A**	**A**	**R**	**R**	**I**		**I**		**I**	**I**
Datos operacionales: MOPRI	**R**			**C**	**C**	**R**	**R**	**C**	**I**	**A**	**A**			**I**		**I**		**I**	**I**
Módulo de Centro Quirúrgico	**R**			**C**	**C**	**R**	**R**	**C**	**I**	**A**	**A**			**I**		**I**		**I**	**I**
Módulo de Reportes	**R**			**C**	**C**	**R**	**R**	**C**	**I**	**A**	**A**			**I**		**I**		**I**	**I**
Módulo de Emergencia	**R**			**C**	**C**	**R**	**R**	**C**	**I**	**A**	**A**					**I**			**I**
Administración de Sistemas de Información		**R**		**R**	**C**												**I**		**I**
Módulo de Referencias	**R**			**C**	**C**		**R**	**I**		**A**	**R**	**I**	**I**	**I**		**I**		**I**	**I**
Mantenimiento de equipos informáticos			**R**	**A**	**I**				**I**					**I**		**I**			**I**
Mantenimiento de tablas y BD																			
Instalación de redes.		**R**	**R**	**C**	**I**														

Fuente: Elaboración propia

Anexo 7: Proyectos Propuestos

Proyecto 1: "Plan de Capacitación"	
Acción:	Programar talleres, cursos, especializaciones y programas de educación continua respecto a seguridad de la información
Descripción:	El plan de capacitación es un programa que busca sensibilizar, capacitar y comunicar el concepto de seguridad de la información y explicar de manera apropiada las reglas de comportamiento para el uso de los sistemas y la información de salud del paciente en la institución, la misma que debe ser cumplida por parte de todos los usuarios del sistema
Riesgo a tratar:	R04, R05, R14.
Estrategia de riesgo:	Mitigar
Categoría de riesgo:	Crítico
Objetivo:	Asegurar que cada integrante de la institución cumpla con los roles y responsabilidades de seguridad y privacidad de la información dentro de la institución
Responsable:	Oficina de Capacitación, Docencia e Investigación
Recursos requeridos:	Auditorio, Computadora, USB, personal de la oficina de TI
Procesos de negocios afectado:	Consulta Externa, Emergencia, Hospitalización, Acreditación.
Tiempo de ejecución:	72 horas
Monitoreo:	Elaboración de una plataforma que permita manejar cronogramas, cargar los soportes de asistencia y que a su vez permita generar reportes de alto nivel para mostrar progresos y otros tipos de datos a nivel gerencial.
Variables a controlar:	Incumplimiento de roles y funciones en seguridad de la información por parte de los usuarios entrenados.
Indicadores:	Uso de métricas que permitan saber si el plan está funcionando, por ejemplo: % Porcentaje de usuarios capacitados apropiadamente, % porcentaje de ataques de ingeniería social exitosos se ha reducido, % porcentaje de usuarios que hayan recibido material de sensibilización)
Acciones para mejorar el proyecto	Evaluar resultados e implementar programas de inducción, capacitación y concientización en seguridad de la información que se incluya en el plan a nivel nacional .
Financiamiento:	Contraprestación por Convenio Marco con Universidades de la Región

Proyecto 2: "IMPLEMENTACION DE POLÍTICAS DE SEGURIDAD DE LA INFORMACION"	
Acción:	Las Políticas de Seguridad de la Información propuestos deberán ser revisados aprobados y difundidos por la Gerencia General y agregados en las funciones de los colaboradores así como requeridos en los perfiles de cargos CAP, PAP
Dominios cubiertos:	Seguridad de RRHH, Control de accesos, Seguridad física y del Entorno, Seguridad de las operaciones, Seguridad de las comunicaciones, Seguridad de Control de las Comunicaciones,
Riesgo a tratar:	R10, R12, R13, R14, R18
Estrategia de riesgo:	Mitigar
Categoría de riesgo:	Crítica. Alta
Objetivo:	Implantar el conjunto de políticas de seguridad de la información propuestos, que dirija el comportamiento de la institución como conjunto, para el cumplimiento del Modelo de Gestión de la Seguridad de la Información
Responsable:	Gerencia General, Oficina de TI
Recursos requeridos:	Correo Electrónico, Documento resolutivo, documentos normativos institucionales (MOF).
Procesos de negocios afectado:	Todos los procesos asistenciales y administrativos de la institución
Tiempo de ejecución:	03 a 6 meses
Anexos:	Formatos conteniendo las Políticas de seguridad de la información
Monitoreo:	Se hará seguimiento a los riesgos y con ello informes regulares de la situación de la seguridad de la información, se adoptarán medidas relevantes cuando existan cambios que impliquen un nivel de riesgo no aceptable.
Variables a controlar:	Incumplimiento de Políticas en Seguridad de la Información que forman parte del manual de funciones de cada trabajador.
Indicadores:	Número de incidentes en seguridad de la información, Número de fraudes detectados. Número de pacientes no atendidos por falta de disponibilidad de su información médica.

Proyecto 2: **"IMPLEMENTACION DE POLÍTICAS DE SEGURIDAD DE LA INFORMACION"**	
Acciones para mejorar el proyecto:	Ante la identificación de nuevos riesgos se revisará con los encargados e interesados la implementación de nuevas Políticas de seguridad de la Información que mitiguen los nuevos riesgos.
Pautas específicas:	- La institución identificará acciones o procedimientos realizados de manera incorrecta con el fin de generar un proceso de capacitación para mejora de procedimientos. - La oficina de Capacitación solicitará la convocatoria para licitar contratos de capacitación en seguridad de la información con expertos las cuales estarán dirigidas a los funcionarios de la clínica. - Los funcionarios deben asistir a la capacitación y es obligación cumplir con la totalidad de las horas establecidas para tal fin - La empresa externa o personal externo que realice la capacitación debe certificar a los funcionarios sobre el cumplimiento y aprobación de la misma.
Presupuesto:	Recursos Humanos: Horas de Trabajo por parte de personal asignado del área de TI de la organización. Convocatoria: Analista en Seguridad de la Información Requisitos: - Conocimientos de la Gestión de Riesgos - Conocimientos en Gestión de la Continuidad de Negocios - Conocimientos en Implementación de un SGSI. - Experiencia Implementación de controles de Seguridad de la Información - Experiencia como analista en SI: 02 años mínima. No.Especialistas * Costoxhora * días (mes) 02 * 27.50 * 8 * 26 = S/. 11,440. mensual

Proyecto 3: " IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE EVENTOS E INCIDENCIAS EN SEGURIDAD DE LA INFORMACION "	
Acción:	Recopila eventos relacionados con la seguridad de dispositivos de usuario final, servidores, equipos de red e incluso equipos de seguridad especializados como firewall, antivirus, o sistemas de prevención de intrusiones.
Riesgo a tratar:	R08, R13, R24, R26
Estrategia de riesgo:	Mitigar
Categoría de riesgo:	Crítico
Objetivo:	Este sistema permitirá un análisis casi en tiempo real que permite al personal de seguridad tomar medidas defensivas más rápidamente ante un evento de seguridad en los sistemas institucionales, y con ello se estaría efectuando con los requisitos de cumplimiento legal de la institución
Responsable: **Recursos requeridos:**	Gerente de TIC y Jefe de TI Computadora, Programador, Analista de TI.
Procesos de negocios afectado:	Todos los procesos de atención al paciente y servicios médicos asistenciales de la institución de salud.
Tiempo de ejecución:	03 meses
Monitoreo:	Detectar tempranamente eventos y alertas que pudieran ocasionar demoras en la atención al paciente.
Variables a controlar:	Detección los ciberataques no detectados, analizar y descubrir nuevas vulnerabilidades.
Indicadores:	#´s de eventos ocurridos que detienen o alteran el funcionamiento de los sistemas vs. #'s de eventos identificados después de la implementación del proyecto
Acciones para mejorar el proyecto	Evaluar los informes generados del sistema en tiempos y eventos, para que sean analizados por el personal de seguridad de TI y poder anteponerse a posibles fallos, ataques o errores en los sistemas
Financiamiento:	Contratación de un especialista en Gestión de Procesos de TI Especialista * Costo por hora * Número de horas * #días. 1*29.00*8h. * 26d = S/. 6,032.00.

Proyecto 4: " IMPLEMENTAR UN MODELO PARA LA GESTION DE UNA MESA DE AYUDA A LOS SERVICIOS DE TI, BASADOS EN TECNOLOGIAS ITIL PARA UNA INSTITUCION DE SALUD"	
Acción:	Garantizar el cumplimiento de los niveles de servicio de TI que se brindan a las diferentes áreas usuarias asistenciales de las aplicaciones informáticas y la infraestructura de TI que tiene una institución de salud
Riesgo a tratar:	R04, R05, R26.
Estrategia de riesgo:	Mitigar
Categoría de riesgo:	Crítica
Objetivo:	Desarrollar un modelo de mesa de ayuda a los servicios de TI, tomando como referencia el framework de ITIL que garantice el cumplimiento en niveles aceptables de los servicios de TI en las diferentes áreas usuarias asistenciales.
Responsable:	Gerente de Tecnologías de la Información, Jefe de la oficina de Tecnologías de la Información.
Recursos requeridos:	Programador, Computadora, Impresora.
Procesos de negocios afectado:	Todos los servicios asistenciales en donde se brinda atención al usuario.
Tiempo de ejecución:	02 meses
Monitoreo:	Para mantener el nivel del servicio, la oficina de TI debe evaluar periódicamente si los recursos disponibles son los adecuados y realizar encuestas de satisfacción cada cierto tiempo para conocer la opinión del usuario.
Variables a controlar:	- Implementar una aplicación en la web para mesa de ayuda - Mejorar la gestión de requerimientos
Indicadores:	Tasa de cumplimiento de SLA, Costo por ticket, Tasa de resolución en la primera llamada, N° de horas operativas perdidas.
Acciones para mejorar el proyecto	Evaluar el tiempo de solución de requerimientos de los usuarios y minimizar éste tiempo de atención de manera que se aumenten los requerimientos atendidos.
Financiamiento:	Contratación de un especialista en Soporte y Help Desk Especialista * Costo por hora * Número de horas * #días. 1*31.50*8h. * 26d = S/. 6,552.

Anexo 8: Validación de Expertos

CONSTANCIA DE VALIDACION

La constancia de validación es un formato que constituye la prueba de que el revisor ha realizado la validación de la metodología, asimismo da a conocer el resultado final de la validación.

Formato de Constancia de Validación

Nombres y apellidos del Experto: GILBERTO CARRIÓN BORJA

Formación Académica: DOCTOR EN CIENCIAS DE LA COMPUTACION Y SISTEMAS

Áreas de experiencia profesional: INFRAESTRUCTURA TECNOLOGICA, SEGURIDAD INFORMÁTICA

Cargo actual: CATEDRÁTICO

Institución: UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Por medio de la presente hago constar que, a través del instrumento correspondiente, se revisó con fines de validación el Modelo de Gestión de Seguridad de la Información para mejorar el proceso de atención al paciente en una institución de salud, habiendo determinado que dicha metodología es válida y aplica como tal para su fin correspondiente.

Chiclayo, 20 de Julio del 2019

Firma

VALIDACION POR JUICIO DE EXPERTO

Fases del Modelo a Implementar	Actividades a calificarse	Dimensiones				
		Coherencia	Relevancia	Claridad	Suficiencia	Observaciones
Planificar	Conocer el contexto interno y externo para identificar factores, situaciones relacionados a la institución.	4	4	3	4	
	Identificar el liderazgo de los stakeholder en mejorar y establecer políticas para la seguridad de la información en la institución en relación a los requisitos de carácter obligatorio.	4	4	3	4	
	Establecer políticas y objetivos de seguridad de la Información apropiadas para la Institución.	3	4	3	4	
	Identificar la información de salud a proteger.	4	4	3	4	
	Identificar y codificar los tipos de amenazas y vulnerabilidades que afectan a la institución.	4	4	4	3	
	Establecer los mecanismos e instrumentos de recolección de datos.	3	3	3	3	
	Definir los roles y responsabilidades de acuerdo a funciones e indicando el nivel de implicancia.	4	4	4	4	

Fases del Modelo a Implementar	Actividades a calificarse	Dimensiones				
		Coherencia	Relevancia	Claridad	Suficiencia	Observaciones
Hacer	Identificar y valorar activos que dan soporte a los procesos de atención y cuantificar su valor en términos de confidencialidad, integridad y disponibilidad	4	4	4	4	
	Identificar amenazas asociadas a los procesos de atención, probabilidad de ocurrencia y vulnerabilidades ante dichas amenazas, lo que permitirá estimar e impacto dentro de la institución.	4	4	4	4	
	Establecer el nivel de estimación del riesgo en la cual se asignó valores a la probabilidad y las consecuencias de un riesgo.	4	4	4	4	
	Realizar tratamiento del riesgo, aplicando las estrategias de transferencia, mitigación, aceptación, eliminar.	4	4	4	4	
	Identificar controles existentes o planificar nuevos que permitan brinda los tres pilares de la información y comunicarlos.	4	4	4	4	

Fases del Modelo a Implementar	Actividades a calificarse	Dimensiones				
		Coherencia	Relevancia	Claridad	Suficiencia	Observaciones
	Implementar la seguridad de RRHH, en los controles de accesos, en las operaciones, comunicaciones y proveedores.	3	4	4	4	
Verificar	Se evalúan dos indicadores, la armonización de las metodologías, normas, estándares y la validez del modelo de SI mediante la evaluación de tres expertos.	4	4	4	4	
	Auditoría interna de la organización revisando la documentación mínima requerida por las normas y los registros de controles.	4	4	4	4	
	Gestionar los incidentes: comunicar eventos y debilidades en la SI.	3	4	4	4	
Actuar	Formar y concientizar a todo el personal involucrado	4	4	4	4	
	Aplicar proceso de mejora continua para monitorear, evaluar y gestionar los incidentes en la seguridad de la información.	4	4	4	4	
	Implementación de proyectos de mejora con el respectivo seguimiento y medición de sus resultados.	4	4	4	4	

CONSTANCIA DE VALIDACION

Nombres y apellidos del experto: Jessie Leila Bravo Jaico

Formación Académica: Dra. en Ciencias de la Computación y Sistemas

Áreas de experiencia profesional: Gestión y Seguridad de Sistemas de Inf.

Cargo actual: Catedrática

Institución: UNPRG - USAT

Por medio de la presente hago constar que, a través del instrumento correspondiente, se revisó con fines de validación el Modelo de Gestión de Seguridad de la Información para poyar el proceso de atención al paciente en una institución de salud, habiendo determinado que dicha metodología es válida y aplica como tal para su fin correspondiente.

Chiclayo, 31 de Julio del 2019.

Firma

JESSIE LEICA BRAVO JAICO
ING. COMP. Y SIST.
R. CIP. 71194

VALIDACION POR JUICIO DE EXPERTO

Fases del Modelo a Implementar	Actividades a calificarse	Dimensiones				
		Coherencia	Relevancia	Claridad	Suficiencia	Observaciones
Planificar	Conocer el contexto interno y externo para identificar factores, situaciones relacionados a la institución.	4	4	4	4	
	Identificar el liderazgo de los stakeholder en mejorar y establecer políticas para la seguridad de la información en la institución en relación a los requisitos de carácter obligatorio.	4	4	3	4	
	Establecer políticas y objetivos de seguridad de la Información apropiadas para la Institución.	4	4	4	4	
	Identificar la información de salud a proteger.	4	3	4	4	
	Identificar y codificar los tipos de amenazas y vulnerabilidades que afectan a la institución.	4	4	4	4	
	Establecer los mecanismos e instrumentos de recolección de datos.	4	4	4	4	
	Definir los roles y responsabilidades de acuerdo a funciones e indicando el nivel de implicancia.	4	4	4	4	

JESSIE LEILA BRAVO JAICO
ING. COMP. Y SIST.
C. IP. 71104

Fases del Modelo a Implementar	Actividades a calificarse	Dimensiones				
		Coherencia	Relevancia	Claridad	Suficiencia	Observaciones
Hacer	Identificar y valorar activos que dan soporte a los procesos de atención y cuantificar su valor en términos de confidencialidad, integridad y disponibilidad	4	4	4	4	
	Identificar amenazas asociadas a los procesos de atención. probabilidad de ocurrencia y vulnerabilidades ante dichas amenazas. lo que permitirá estimar e impacto dentro de la institución.	4	4	4	4	
	Establecer el nivel de estimación del riesgo en la cual se asignó valores a la probabilidad y las consecuencias de un riesgo.	4	4	4	4	
	Realizar tratamiento del riesgo, aplicando las estrategias de transferencia, mitigación, aceptación, eliminar.	4	4	4	4	
	Identificar controles existentes o planificar nuevos que permitan brinda los tres pilares de la información y comunicarlos.	4	4	4	4	

JESSIE LEILA BRAVO JAICO
ING. COMP. Y SIST.

Fases del Modelo a Implementar	Actividades a calificarse	Dimensiones				
		Coherencia	Relevancia	Claridad	Suficiencia	Observaciones
	Implementar la seguridad de RRHH, en los controles de accesos, en las operaciones, comunicaciones y proveedores.	4	4	4	4	
Verificar	Se evalúan dos indicadores, la armonización de las metodologías, normas, estándares, etc y la validez del modelo de SI mediante la evaluación de tres expertos.	4	4	4	4	
	Auditoría interna de la organización revisando la documentación mínima requerida por las normas y los registros de controles.	4	4	4	4	
	Gestionar los incidentes: comunicar eventos y debilidades en la SI.	4	4	4	4	
Actuar	Formar y concientizar a todo el personal involucrado	4	4	4	4	
	Aplicar proceso de mejora continua para monitorear, evaluar y gestionar los incidentes en la seguridad de la información.	4	4	4	4	
	Implementación de proyectos de mejora con el respectivo seguimiento y medición de sus resultados.	4	4	4	4	

JESSIE LEILA BRAVO JAICO
ING. COMP. Y SIST.

Constancia de Validación

Nombres y apellidos del Experto: **AMPUERO PASCO GILBERTO MARTÍN**

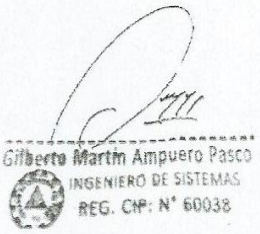
Formación Académica: **POST GRADO INGENIERO DE SISTEMAS CON MAESTRIA EN CIENCIAS**

Áreas de experiencia profesional: **SEGURIDAD DE LA INFORMACION - DESARROLLO DE SOFTWARE**

Cargo actual: **GERENTE GENERAL – DOCENTE NOMBRADO**

Institución: **GARZASOFT - UNPRG**

Por medio de la presente hago constar que, a través del instrumento correspondiente, se revisó con fines de validación el Modelo de Gestión de Seguridad de la Información para apoyar el proceso de atención al paciente en una institución de salud, habiendo determinado que dicha metodología es válida y aplica como tal para su fin correspondiente.



VALIDACION POR JUICIO DE EXPERTO

Fases del Modelo a Implementar	Actividades a calificarse	Dimensiones				
		Coherencia	Relevancia	Claridad	Suficiencia	Observaciones
Planificar	Conocer el contexto interno y externo para identificar factores, situaciones relacionados a la institución.	4	3	4	4	
	Identificar el liderazgo de los stakeholder en mejorar y establecer políticas para la seguridad de la información en la institución en relación a los requisitos de carácter obligatorio.	4	4	4	4	
	Establecer políticas y objetivos de seguridad de la Información apropiadas para la Institución.	3	4	4	4	
	Identificar la información de salud a proteger.	4	4	4	4	

Gilberto Martin Ampuero Pasco
INGENIERO DE SISTEMAS
REG. CIP: N° 60038

Fases del Modelo a Implementar	Actividades a calificarse	Dimensiones				
		Coherencia	Relevancia	Claridad	Suficiencia	Observaciones
Planificar	Identificar y codificar los tipos de amenazas y vulnerabilidades que afectan a la institución.	4	4	4	4	
	Establecer los mecanismos e instrumentos de recolección de datos.	4	4	4	4	
	Definir los roles y responsabilidades de acuerdo a funciones e indicando el nivel de implicancia.	4	4	4	4	
Hacer	Identificar y valorar activos que dan soporte a los procesos de atención y cuantificar su valor en términos de confidencialidad, integridad y disponibilidad	4	4	4	4	
	Identificar amenazas asociadas a los procesos de atención, probabilidad de ocurrencia y vulnerabilidades ante dichas amenazas, lo que permitirá estimar e impacto dentro de la institución.	4	4	4	4	

Gilberto Martín Ampuero Pasco
INGENIERO DE SISTEMAS
REG. CIP. N° 60038

Fases del Modelo a Implementar	Actividades a calificarse	Dimensiones				Observaciones
		Coherencia	Relevancia	Claridad	Suficiencia	
Verificar	Se evalúan dos indicadores, la armonización de las metodologías, normas, estándares y la validez del modelo de SI mediante la evaluación de tres expertos.	4	4	4	4	
	Auditoría interna de la organización revisando la documentación mínima requerida por las normas y los registros de controles.	4	4	4	4	
	Gestionar los incidentes: comunicar eventos y debilidades en la SI.	4	4	4	4	
Actuar	Formar y concientizar a todo el personal involucrado	4	4	4	4	
	Aplicar proceso de mejora continua para monitorear, evaluar y gestionar los incidentes en la seguridad de la información.	4	4	4	4	
	Implementación de proyectos de mejora con el respectivo seguimiento y medición de sus resultados.	4	4	4	4	

Gilberto Martín Ampuero Pasco
INGENIERO DE SISTEMAS
REG. CIP: N° 60038

Anexo 9: Perfil de Expertos

La información detallada a continuación ha sido obtenida del Directorio Concytec: https://dina.concytec.gob.pe/appDirectorioCTI/

PERFIL DE EXPERTO	
	Gilberto Carrión Barco Doctor en Ciencias de la Computación y Sistemas. Maestro en Ingeniería de Sistemas, Magister en Docencia Universitaria. Ingeniero en Computación e Informática y Licenciado en Administración Pública, con Colegiatura N° 90931 por el Colegio de Ingenieros del Perú, habilitado. Con más de 12 años de experiencia en docencia universitaria en UNPRG, USS, UTP, USMP, USAT e Investigador en la línea Tecnologías de la Información, Gobierno Electrónico y Gestión por Procesos y Gestión por Resultados. Amplia experiencia como Jurado y Asesor de Investigaciones tanto en pregrado como en postgrado. Comprometido con el trabajo en equipo, proactivo y con vocación de servicio.

Datos académicos

Grado	Título	Centro de Estudios
LICENCIADO / TÍTULO	INGENIERO EN COMPUTACION E INFORMATICA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
BACHILLER	BACHILLER EN COMPUTACION E INFORMATICA	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
BACHILLER	BACHILLER EN ADMINISTRACIÓN PÚBLICA	UNIVERSIDAD SEÑOR DE SIPÁN
MAGISTER	MAESTRO EN INGENIERIA DE SISTEMAS, ESPECIALIDAD: CON	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

	MENCION EN GERENCIA DE TECNOLOGIAS DE LA INFORMACION Y GESTION DEL SOFTWARE	
MAGISTER	MAGISTER EN DOCENCIA UNIVERSITARIA	UNIVERSIDAD PRIVADA CÉSAR VALLEJO
DOCTORADO	DOCTOR EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD SEÑOR DE SIPÁN

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DOCENTE ORDINARIO TIEMPO COMPLETO CATEGORÍA AUXILIAR	2008-08-01	A la actualidad
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECTOR DE ESCUELA	2013-12-01	2016-01-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE AREA ADMINISTRATIVA RED TELEMÁTICA	2010-07-01	2011-11-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DE LABORATORIO	2010-04-01	2010-09-01
INSTITUTO DE EDUCACION SUPERIOR TECNOLOGICO PRIVADO ABACO	GERENTE DE ALTA TECNOLOGÍA E INNOVACIÓN TECNOLÓGICA	2004-03-01	2006-01-01

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD TECNOLOGICA DEL PERU S.A.C. O UTP S.A.C.	Ordinario-Auxiliar	Mayo 2014	A la actualidad
UNIVERSIDAD DE SAN MARTIN DE PORRES	Ordinario-Auxiliar	Agosto 2010	Noviembre 2016
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Auxiliar	Agosto 2008	A la actualidad
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Ordinario-Auxiliar	Agosto 2006	Diciembre 2009
UNIVERSIDAD SENOR DE SIPAN SAC	Ordinario-Asociado	Abril 2006	A la actualidad

Experiencia como asesor de tesis

Universidad	Tesis	Tesistas	Fecha aceptación
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Magister	Rosa América Cobeñas Sánchez	Noviembre 2016
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Guevara Chumán, Javier Gustavo	Agosto 2015
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Rivas Estrada, Carol Meliza; Estrada Masgo, Danny Christian	Junio 2014

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Arévalo Díaz Janira; Sánchez Pérez Cinthya del Milagro	Febrero 2015
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ramírez Arrunátegui Pamela Susanne; Rojas Muñoz Jonatan Jorge	Abril 2015
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Apolaya Segura Carlos Eduardo; Vílchez Castillo Sylvia Susana	Junio 2018
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Palacios Ormeño, Julio César	Noviembre 2013
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Arrieta Gómez, Víctor Manuel; Camacho Aguirre, Martin Horacio	Julio 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Villegas Carrasco, Carlos Alonso; Negreiros Chinchihuara, Wilfredo Martin	Octubre 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Sacravilca Narciso, Dante Gonzalo; López Alarcón, Absalón	Junio 2014
UNIVERSIDAD SENOR DE SIPAN SAC	Licenciado / Título	Balcázar De Los Santos, César Augusto; Correa Villegas, Ricardo	Octubre 2013

PERFIL DE EXPERTO	
	Jessie Leila Bravo Jaico Ing. de Computación y Sistemas. Primera Promoción de la Universidad Privada Antenor Orrego de Trujillo. Doctora en Ciencias de Computación y Sistemas en la USS. Magister en Informática y Multimedia en la Universidad de Los Lagos - Chile. Magister en Administración de empresas con mención en Gerencia Empresarial de la Universidad Nacional Pedro Ruiz Gallo. Especialización en Redes Informáticas, Gestión de proyectos, Auditoría y consultoría de sistemas. Asesora y Consultora de TI en empresas de la región.

Datos Académicos

Grado	Título	Centro de Estudios
MAGISTER	MAGÍSTER EN INFORMÁTICA Y MULTIMEDIA	UNIVERSIDAD SAN PEDRO
LICENCIADO / TÍTULO	INGENIERO DE COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO
BACHILLER	BACHILLER EN INGENIERIA DE COMPUTACION Y SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO
MAGISTER	MAESTRA EN ADMINISTRACION CON MENCION EN GERENCIA EMPRESARIAL	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
DOCTORADO	DOCTORA EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS	UNIVERSIDAD SEÑOR DE SIPÁN

Experiencia laboral

Institución	Cargo	Fecha Inicio	Fecha Fin
SERVIMEDICOS S.A.C.	CONSULTORA TI	2006-06-01	2008-09-01
INSTITUTO DE ALTA CALIDAD DE ATENCION A LA SALUD EN LIQUIDACION	CONSULTORA TI	2005-04-01	2007-07-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DEL LABORATORIO DE CÓMPUTO	2003-09-01	2006-12-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	JEFE DEL LABORATORIO DE CÓMPUTO	2001-05-01	2003-09-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DESARROLLO SISTEMAS	1996-06-01	2000-12-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	DIRECCIÓN DE ESCUELA	1997-09-01	1999-12-01
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	MIEMBRO COMITÉ DIRECTIVO	1996-12-01	1999-12-01
CIS - CATSOFT S.R.LTDA.	ANALISTA-DISEÑADORA	1996-09-01	1997-12-01
CUERPO MÉDICO HOSPITAL NACIONAL ALMANZOR AGUINAGA ASENJO	PROGRAMADORA	1993-01-01	1993-03-01

Experiencia laboral como docente

Institución	Tipo Docente	Fecha Inicio	Fecha Fin
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Principal	Junio 2010	A la actualidad
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Contratado	Agosto 2002	A la actualidad
UNIVERSIDAD JUAN XXIII-VALLE JEQUETEPEQUE	Contratado	Agosto 1999	Diciembre 2000
UNIVERSIDAD SAN PEDRO	Contratado	Setiembre 1998	Diciembre 1999
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Auxiliar	Mayo 1998	Diciembre 2001
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Contratado	Octubre 1994	Abril 1998

Experiencia como asesor de tesis

Universidad	Tesis	Tesista(s)	Fecha Aceptación
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	CÉSAR WENCESLAO DE LA CRUZ GUERRERO y JUAN CARLOS VASQUEZ MONTENEGRO	Abril 2008
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	Santa María Becerra, Franck Jhonathan	Junio 2012

UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	BURGA BASTO, JORGE HUMBERTO JESÚS y LEY CUÉN RODAS, CHRISTIAN ALEXIS	Abril 2011
UNIVERSIDAD CATOLICA SANTO TORIBIO DE MOGROVEJO	Licenciado / Título	RICHARD TUSET TRINIDAD y DANIEL ALEJANDRO YI RAMOS	Abril 2011
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	César Augusto López Nicolini	Junio 2014
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Fernández Vílchez Richar Marvin	Enero 2012
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	ALARCÓN CUSMAN JOSÉ CARLOS y CHERO IZQUIERDO JULIO FRANCISCO	Mayo 2014
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Roxana Paola Bazán becerra	Febrero 2001
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	María del Rosario Becerra Aguilar	Setiembre 2002
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Guisella Lontop Vilchez/Franklin Terán/Melvy terán	Junio 2003
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Milagros Vanessa Peña Seclén/Mónica Lecca Vinces	Abril 2004

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ronald Javier Medina Campaña	Abril 2006
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	CHANAME BALDERA, OSCAR ENRIQUE	Abril 2006
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Chirinos Fernández Maykol	Julio 2007
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Ronald Leiva Peña	Febrero 2016
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	GONZALO MARTIN ROMERO ABANTO y ROBERTH CÓRDOVA OBLITAS	Noviembre 2017
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Olano Díaz, Juan Daniel; Sánchez Aguilar, Segundo Román	Marzo 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Pérez Artemio, Calderón; Vásquez Hoyos, Álvaro	Julio 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Cubas Penas, Clara Patricia	Abril 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Magister	Niño Morante, Nilton Rogger	Mayo 2018
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	Arenas Morales, Victor Jaime / Brios Guevara, Lessly Yein	Marzo 2019

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	LARREA DUPIS CARLO ANTONIO / HERNÁNDEZ CAMPOS ROBERT DANILO	Marzo 2019

PERFIL DE EXPERTO	
	Ampuero Pasco Gilberto Martín Ingeniero de Sistemas. Catedrático en Universidad Nacional Pedro Ruiz Gallo. Tutor de post grado en Universidad Nacional Pedro Ruiz Gallo. Administrador de la Red Telemática en Universidad Nacional Pedro Ruiz Gallo. Gerente General de Garzasoft E.I.R.L.

Datos Personales

Apellidos :	AMPUERO PASCO
Nombres:	GILBERTO MARTIN
Género:	MASCULINO
País de Nacimiento :	PERÚ

Experiencia Laboral

Institución	Cargo	Sector	Fecha Inicio	Fecha Fin
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	**DOCENTE**	**Público**	**1998-04-01**	A la actualidad
GARZASOFT E.I.R.L.	GERENTE	Privado	2018-02-01	A la actualidad
GARZATEC SOCIEDAD ANONIMA CERRADA	GERENTE DE DESARROLLO	Privado	2014-02-01	A la actualidad

Experiencia Laboral como Docente

Institución	Tipo Docente	Tipo Institución	Fecha Inicio	Fecha Fin
UNIVERSIDAD PARTICULAR DE CHICLAYO	Contratado	Universidad	Agosto 2013	A la actualidad
UNIVERSIDAD DE LAMBAYEQUE SAC	Contratado	Universidad	Mayo 2012	A la actualidad
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Ordinario-Asociado	Universidad	Abril 1997	A la actualidad

Experiencia como Asesor de Tesis

Universidad	Tesis	Tesista(s)	Repositorio	Fecha Aceptación de Tesis
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Licenciado / Título	David James Moreno Chapoñan		Agosto 2017

Datos Académicos

Grado	Título	Centro de Estudios	País de Estudios	Fuente
LICENCIADO / TÍTULO	MAESTRO EN CIENCIAS	UNIVERSIDAD NACIONAL PEDRO RUÍZ GALLO	PERÚ	SUNEDU
MAGISTER	MAESTRO EN CIENCIAS, ESPECIALIDAD: CON MENCION EN INFORMATICA Y SISTEMAS	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	PERÚ	SUNEDU

Idiomas

#	Idioma	Lectura	Conversación	Escritura	Lengua Materna
1	PORTUGUES	BÁSICO	BÁSICO	BÁSICO	NO
2	INGLES	AVANZADO	INTERMEDIO	AVANZADO	NO
3	ESPAÑOL O CASTELLANO	AVANZADO	AVANZADO	AVANZADO	SI

Proyectos de Investigación

Título	Fecha de Inicio	Fecha Fin	Inv. Principal	Área OCDE
Implementación de un sistema de almacén utilizando el paradigma Cloud Computing y el concepto de negocio Software como Servicio SaaS	Junio 2013	Junio 2014	GILBERTO MARTIN AMPUERO PASCO	Ingeniería y Tecnología
Desarrollo de aplicaciones Java EE para acceso a base de datos PostgreSQL	Diciembre 2015	Diciembre 2016	GILBERTO MARTIN AMPUERO PASCO	Ingeniería y Tecnología
Aplicación móvil para cumplimiento de indicaciones médicas e ingesta de medicinas	Marzo 2017	Marzo 2018	GILBERTO MARTIN AMPUERO PASCO	Ingeniería y Tecnología