UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN E INFORMÁTICA

TESIS

TÍTULO

"Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015"

AUTOR:

Ronald Leiva Peña

ASESOR:

MSc. Ing. Jessie Bravo Jaico

Lambayeque, Marzo del 2016

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001 E ISO/IEC 27002 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN EL PROCESO DE SUMINISTROS DE MEDICAMENTOS DE LA RED DE SALUD DE LAMBAYEQUE 2015"

MIEMBROS DEL JURADO:

Ing. Luis Alberto Reyes Lescano

Presidente

Ing. Gisella Maquen Niño

Secretario

Ing. Alejandro Chayán Coloma

Vocal

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NORMAS ISO/IEC 27001 E ISO/IEC 27002 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN EL PROCESO DE SUMINISTROS DE MEDICAMENTOS DE LA RED DE SALUD DE LAMBAYEQUE 2015"

MSc. Ing. Jessie Bravo Jaico

Asesor

Ronald Leiva Peña

Bachiller

Dedicatoria

A ti mamá, que eres mi ejemplo a seguir, aunque ya no estás físicamente conmigo siento que me das las fuerzas para seguir luchando día a día, fuiste la mejor madre del mundo.

A mi hermana que, aunque está lejos es la persona que me da fuerzas para seguir adelante siempre, al igual que mi padre que sé que en el fondo siempre me apoya.

A mi tía Teresa que es como una madre para mí siempre está aconsejándome para dar lo mejor de mí en mi vida profesional, la quiero un montón.

A toda mi demás familia que de alguna u otra manera quieren que avance como persona y profesional, muchas gracias

A Yesenia que es una persona maravillosa, quien ha sido mi motivación para terminar con este proyecto.

Agradecimiento

A Dios porque siempre está conmigo para guiarme por el camino del bien a lo largo de mi vida y mi carrera profesional, de ésta manera lograr las metas y los objetivos.

A la Ing. Jessie Bravo Jaico por su valioso apoyo y asesoría para en el desarrollo de la presente investigación.

A mis profesores que estuvieron a lo largo de mi carrera e impartieron los conocimientos que sirven de base para seguir desarrollándome como profesional.

A la Red de Servicios de Salud de Lambayeque y sus trabajadores por permitir desarrollar la presente investigación en la Institución.

Finalmente agradezco a mis amigos del Programa Nacional Cuna Más de la UT Lima 04, que me apoyaron para emprender este gran reto.

RESUMEN

El presente proyecto de investigación se centra en el diseño de un sistema de gestión de seguridad de la información, basándose en la norma ISO IEC 27001 y 27002, además del uso de la conocida metodología PDCA, para mejorar el proceso de suministro de medicamentos en la Red de Servicios de Salud de Lambayeque, ayudando así a que los sistemas de información usados estén más seguros.

Para lograr un buen diseño y plantear la situación problemática se usó la técnica de recolección de datos de la encuesta, además de fichas de observación, con la finalidad de que se logre extraer cuales eran las causas del porque era necesario un sistema de gestión de información en la Institución.

Los resultados determinaron que: trabajar con una metodología y seguir paso a paso las recomendaciones que nos brinda una norma ISO permitieron identificar dentro de los procesos de negocio, cuales son las dificultades por las que atraviesa la seguridad de los sistemas y de los activos en general que se encuentran dentro de la institución, que al no contar con buenos controles pueden terminar ocasionando un gran riesgo en la continuidad de cualquier entidad.

En la primera parte se empezó identificando los procesos de negocio involucrados en el desarrollo del proyecto; se definió el alcance que tendría el SGSI en la institución; se identificaron y analizaron todos los activos dentro del alcance del SGSI; luego se definió una metodología para la evaluación de riesgos.

Al final del proyecto se elaboró un plan de tratamiento de riesgos y aplicando como parte de la documentación de la ISO dio como resultado la elaboración de políticas, procedimientos y controles que la institución puede implementar para una certificación.

Palabras Claves:

SGSI, ISO, PDCA, Seguridad de la información, ISO IEC 27001 e ISO IEC 27002

ABSTRACT

This research project focuses on the design of a management system of information security based on ISO 27001 and 27002, and the use of known methodology PDCA to improve the process of drug supply in the network Health Services Lambayeque, thus helping information systems used safer.

To achieve a good design and raise the problematic situation the technique of collecting data from the survey was used, in addition to observation sheets, with the aim of achieving an extract which you were the causes of why a system of information management needed in the institution.

The results determined that: work with a methodology and follow step by step the recommendations gives us an ISO possible to identify within the business processes, which are the difficulties being experienced security systems and assets in general They found within the institution, that by not having good controls can end caused a great risk in the continuity of any entity.

In the first part it began by identifying the business processes involved in the development of the project; the scope that would ISMS defined in the institution; they were identified and analyzed all assets within the scope of the ISMS; then a methodology for risk assessment was defined.

At the end of the project, a risk treatment plan was developed and implemented as part of the ISO documentation resulted in the development of policies, procedures and controls that the institution can implement for certification.

KEY WORD:

SGSI, ISO, PDCA, Security of the information, ISO 27001 and ISO IEC 27002

INDICE GENERAL

Dedicatoria **2**

Agradecimiento **3**

RESUMEN **4**

ABSTRACT **5**

Introducción: **11**

CAPÍTULO I: DATOS GENERALES DE LA ORGANIZACIÓN ***13***

1.1.- Descripción de la Organización **14**

1.2.- Misión, Visión y Objetivos de la Organización **14**

1.2.1.- Misión 14

1.2.2.- Visión 14

1.2.3.- Objetivos 15

1.3.- Estructura Orgánica **16**

CAPÍTULO II: ***18***

PROBLEMÁTICA DE LA INVESTIGACIÓN ***18***

2.1.- Realidad problemática **19**

2.1.1.- Planteamiento del Problema 19

2.2.- Formulación del Problema **21**

2.3.- Justificación e Importancia de la Investigación **21**

2.3.1.- Justificación Económica 21

2.3.2.- Justificación Tecnológica 21

2.3.3.- Justificación social 22

2.3.4.- Justificación científica 22

2.3.5.- Importancia 22

2.4.- Objetivos de la Investigación **23**

2.4.1.- Objetivo General 23

2.4.2.- Objetivos Específicos: 23

2.5.- Limitaciones de la Investigación **23**

2.5.1- Geográfica 23

2.5.2.- Administrativa 23

2.5.3.- Tecnológica 23

2.5.4.- Científica 24

2.5.5.- Personal 24

2.5.6.- Económicas 24

CAPÍTULO III: ***25***

MARCO METODOLÓGICO ***25***

3.1.- Tipo de Investigación **26**

3.2.- Hipótesis **26**

3.3.-Variables **26**

3.3.1. Variable Independiente 26
3.3.2. Variable Dependiente 26

3.4.- Selección de la metodología 27
3.4.1.- Ciclo Deming (2005) Mejora Continua. 27

CAPÍTULO IV: 34

MARCO TEÓRICO 34

4.1.- Antecedentes 35
4.1.1.- Antecedentes en el contexto internacional 35
4.1.2.- Antecedentes en el contexto nacional 36
4.1.3.- Antecedentes en el contexto local 38

4.2.- Base teórica 39
4.2.1.- Sistema de Gestión de Seguridad de Información (SGSI) 39
4.2.2.- ISO/IEC 27001 47
4.2.3.- ISO/IEC 27002 52
4.2.4.- ISO/IEC 27003:2010 61
4.2.5.- ISO/IEC 27005:2011 63
4.2.6.- COBIT 5 64

4.3.-Conceptos y Definiciones 71

CAPÍTULO V: 75

DESARROLLO DE LA PROPUESTA 75

5.1. Inicio del Proyecto 76
5.1.1. Compromiso de la Dirección 76
5.1.2. Objetivos de negocio de la Institución 77
5.1.3. Sistemas de Gestión existentes 77
5.1.4. Planificación 77

5.2. Establecer el SGSI 77
5.2.1. Alcance del SGSI 77
5.2.2. Política de Seguridad 78

5.3. Diseño del SGSI 80
5.3.1. Análisis de la Organización 80
5.3.2.- Identificación y evaluación de riesgos 102
5.3.3.-Plan Tratamiento de riesgos 110
5.3.4.- Controles para el tratamiento de riesgos. 118
5.3.5.- Mapeo de los Controles con COBIT 5. 131
5.3.6.- Declaración de Aplicabilidad 144

5.4.- Implementar y Utilizar el SGSI 148
5.4.1.- Gestión de la seguridad de la información 148
5.4.1.1.- Comité de seguridad 148
5.4.2.- Política de control de acceso 150
5.4.2.- Procedimientos operativos para la gestión de TI 154
5.4.3.- Procedimiento para gestión de incidentes 175
5.4.4.- Procedimientos de la continuidad del negocio 182

CAPITULO VI: Costos y Beneficios 196

CAPITULO VII: Conclusiones 201

CAPITULO VIII: Recomendaciones.....203

CAPÍTULO IX: Referencias Bibliográficas.....205

ANEXOS.....208

INDICE DE TABLAS

TABLA N° 01. INVENTARIO DE ACTIVOS 90
TABLA Nº 02. CRITERIOS DE VALORIZACIÓN DE ACTIVOS 91
TABLA N° 03. VALORES SEGÚN NIVEL DE CRITICIDAD 92
TABLA N° 04. VALORIZACIÓN DE LOS ACTIVOS DE LA INFORMACIÓN 99
TABLA N° 05. ACTIVOS CON CRITICIDAD ALTA 102
TABLA N° 06. MATRIZ DE CALOR 103
TABLA N° 07. DESCRIPCIÓN DE LOS NIVELES DE LA PROBABILIDAD DE AFECTACIÓN 103
TABLA Nº 08. DESCRIPCIÓN DE LOS NIVELES DE IMPACTO EN EL NEGOCIO 104
TABLA N° 09. MATRIZ DE RIESGOS 110
TABLA N° 10. PLAN DE TRATAMIENTO DE RIESGOS 110
TABLA N° 11. ACTIVIDADES DEL PLAN DE TRATAMIENTO RIESGOS 111
TABLA N° 12. LISTA DE RIESGOS NO ACEPTABLES 118
TABLA N° 13. POLÍTICAS DE SEGURIDAD 124
TABLA N° 14. CONTROLES PARA EL TRATAMIENTO DE RIESGOS 131
TABLA N° 15. OBJETIVOS ORGANIZACIONALES DE LA INSTITUCIÓN SEGÚN COBIT 5 132
TABLA N° 16. OBJETIVOS DE TI DE LA INSTITUCIÓN SEGÚN LOS OBJETIVOS ORGANIZACIONALES. 135
TABLA N° 17. PROCESOS HABILITADORES DE COBIT 5 SEGÚN LOS OBJETIVOS DE TI DE LA INSTITUCIÓN 138
TABLA N° 18. MAPEO DE PROCESOS HABILITADORES 143
TABLA N° 19. DECLARACIÓN DE APLICABILIDAD 147
TABLA Nº 20. INTEGRANTES DEL COMITÉ DE SEGURIDAD 148
TABLA Nº 21. MATRIZ DE RESPONSABILIDADES 150
TABLA Nº 22. TIPO DE INCIDENTE 177
TABLA Nº 23. NIVEL DE CRITICIDAD 178
TABLA Nº 24. RESPONSABLES DE LA GESTIÓN DE INCIDENTES 179
TABLA Nº 25. INDICADORES 182
TABLA Nº 26. COMITÉ DE GESTIÓN DE CONTINUIDAD 186
TABLA Nº 27. ACTIVIDADES DE ESTRATEGIA DE RECUPERACIÓN LAN –SWITCH 193
TABLA Nº 28. TIPO DE PRUEBAS 194
TABLA Nº 29. COSTO DE SOFTWARE 197
TABLA Nº 30. COSTO DE PERSONAL 197
TABLA Nº 31. COSTO DE SERVICIOS 197
TABLA Nº 32. COSTO DE MATERIALES 198
TABLA Nº 33. COSTO DE HARDWARE 198
TABLA Nº 34. RESUMEN DE COSTOS 199
TABLA Nº 35. FLUJO DE EFECTIVO 199
TABLA Nº 36. PERIODO DE RECUPERACIÓN DE LA INVERSIÓN 200

INDICE DE FIGURAS

FIGURA N° 01: ESTRUCTURA ORGÁNICA DE LA INSTITUCIÓN 16
FIGURA N° 02: CICLO DEMING 27
FIGURA Nº 03: FASE DE EJECUCIÓN 50
FIGURA Nº 04: FASE DE SEGUIMIENTO 51
FIGURA Nº 05: FASE DE MEJORA 51
FIGURA Nº 06: LOS 5 PRINCIPIOS DEL MARCO COBIT 5 65
FIGURA Nº 07: LOS SIETE PRINCIPIOS DEL MARCO COBIT 5 66
FIGURA Nº 08: LA CASCADA DE OBJETIVOS DE COBIT 5 67
FIGURA Nº 09: PERSPECTIVAS DEL CUADRO DE MANDO INTEGRAL 70
FIGURA Nº 10: INICIO DEL PROYECTO 76
FIGURA Nº 11: ALCANCE DEL SGSI 78
FIGURA Nº 12: DISEÑO DEL SGSI 80
FIGURA Nº 13: IMPLEMENTAR EL SGSI 148

Introducción:

En los últimos 20 años, con el desarrollo de la tecnología, la información se ha convertido en uno de los activos más importantes dentro de las empresas, pudiendo estar presente en múltiples formatos: papel, almacenada electrónicamente, ilustrada en películas, hablada en conversaciones o transmitida por alguna tecnología de comunicaciones, entre otros. (Ampuero Chang, 2011).
En la Red de Servicios de Salud de Lambayeque es muy importante la protección de los activos de la información para el buen curso de los procesos de negocio, además porque se ha tenido dificultades como la falta de un mecanismo de backup en caso de pérdida de información para recuperarla, seguridad en los equipos, entre otros; ante esto se puso en marcha el diseño de un sistema de gestión de seguridad de la información teniendo en cuenta la norma ISO/IEC 27001 y 27002.

Los objetivos a desarrollar se han definido de la siguiente manera: Identificar los procesos de negocios de la entidad involucrados en la gestión de seguridad informática; valorar los activos de información asociados al proceso de suministro de medicamentos en la Red de Salud de Lambayeque; evaluar los riesgos a los que están expuestos los activos de mayor valor para la Red de Salud de Lambayeque; seleccionar los controles que permitan gestionar y tratar los riesgos identificados en base a la Norma ISO/IEC 27002; finalmente elaborar la documentación exigida por la Norma ISO/IEC 27001 adoptada para el diseño del SGSI en la Red de Salud de Lambayeque.

Al desarrollar el SGSI permitirá en lo económico reducir costos en cuanto a la gestión de seguridad de la información. En la parte tecnológica ayudará a permitir una buena gestión de los recursos informáticos. Socialmente dentro de la institución permitió que se familiaricen con los conceptos de seguridad respecto a las actividades diarias de los trabajadores. En lo científico nos da una forma de incrementar el conocimiento y el profesionalismo por medio de la investigación.

La estructura del proyecto está dividida en capítulos quedando de la siguiente forma:

En el capítulo 1 se realizó la investigación acerca de la institución, estructura orgánica, misión, visión y sus objetivos.

Para el capítulo 2 se definió la situación problemática de la Red de Salud de Lambayeque, justificar en diferentes situaciones el desarrollo del proyecto, plantear los objetivos y también tomar en cuenta sobre que limitaciones se trabaja en el proyecto.

Luego en el capítulo 3 se hizo realce sobre la metodología PDCA para el trabajo del SGSI dado que es muy recomendable para sus diferentes procesos.

En el capítulo 4 se plasma toda la teoría de investigación realizada como base para la realización del proyecto de investigación tales como las normas ISO, COBIT 5.0.

En el capítulo 5 para el desarrollo del proyecto se estructura en 4 partes. En la primera parte se analizó el compromiso de la gerencia con el proyecto, los objetivos de la institución sobre los cuales se trabajó. En la segunda parte vemos el alcance que tendrá el SGSI que delimitó qué áreas iba abarcar.

Seguido en la tercera parte se trabajó con el diseño del SGSI, empezando por la definición de los procesos de negocio, identificar los activos de información y valorizarlos; luego vemos como avanzamos hacia una identificación de los riesgos más resaltantes para luego desarrollar una metodología de evaluación de riesgos y un plan de evaluación en base a una serie de actividades para hacer cumplir el SGSI. Seguido de eso se tendrá las políticas que adoptarán la institución y los controles para la mitigación de los riesgos que no pueden ser aceptados ya que causarían un daño en la continuidad del negocio. Se concluye con el mapeo a los controles usando el marco de referencia COBIT 5.0 y culminar con la declaración de aplicabilidad donde se muestra el detalle del producto del SGSI. Para la cuarta parte se definió todas las políticas para el control de acceso, los procedimientos operativos por cada control aplicado en la institución, procedimientos para la gestión de incidentes y los que sirven para manejar la continuidad del negocio.

CAPÍTULO I: DATOS GENERALES DE LA ORGANIZACIÓN

1.1.- Descripción de la Organización

Nombre	: “Red de Servicios de Salud de Lambayeque”
Dirección	: Av. Libertad 513 – Lambayeque
Gerente	: Mgtr. Anita del Rosario Zevallos Cotrina
Teléfono	: 074 - 283898
Rubro al que se dedica	: Sector Salud – Servicios

1.2.- Misión, Visión y Objetivos de la Organización

La misión y visión de la Red de Salud de Lambayeque fue extraído del Plan Operativo Institucional 2015 de la Red de Salud de Lambayeque. (Red de Salud de Lambayeque, Manual de Organizacion y Funciones 2015, 2015)

1.2.1.- Misión

Somos una Red de Establecimientos de Salud en la Provincia de Lambayeque que brindamos Servicios de Salud preventivo-promocional y recuperativa al individuo, familia y comunidad en el primer nivel de atención con equidad, eficiencia y calidad, mediante una organización de Micro redes de Salud con recursos humanos capacitados y competentes con participación activa de la comunidad organizada, que promueve servicios de salud que ofertan la máxima calidad técnica e interpersonal a sus usuarios, que busca contribuir a elevar el nivel de salud de la población; desarrollar armónicamente los sistemas de salud, centrados en las personas; fortalecer el control de los factores que puedan afectar la salud y reforzar la gestión de la red nacional de atención. Todo ello para acoger oportunamente las necesidades de las personas, familias y comunidades, con la obligación de rendir cuentas a la ciudadanía y promover la participación de las mismas en el ejercicio de sus derechos y sus deberes.

1.2.2.- Visión

Ser al 2016 una Red de Servicios de Salud del primer nivel de atención en el ámbito de la Región Lambayeque, con autonomía administrativa, que asegure el acceso a una atención en salud oportuna, acogedora, equitativa, integral y de calidad, con lo cual se sentirán más seguras y protegidas., dotado de personal comprometido y competente, que promueve la

participación social activa permitiendo el desarrollo de la población de la provincia de Lambayeque, logrando que las personas, familias y comunidades tendrán una vida más saludable, participarán activamente en la construcción de estilos de vida que favorezca su desarrollo..

1.2.3.- Objetivos

- OE1. Reducir la mortalidad materna y Neonatal, con enfoque de interculturalidad en la población más vulnerable.
- OE2. Reducir la morbilidad por IRAS en niños menores de 5 años.
- OE3. Disminuir la Tasa de incidencia de TBC.
- OE4. Disminuir la Morbimortalidad por Cáncer.
- OE5. Reducir la Desnutrición crónica infantil y otros desordenes nutricionales.
- OE6. Prevención de ITS-VIH/SIDA.
- OE7.Disminuir la Tasa de Incidencia de enfermedades no transmisibles/enfermedades hipertensivas, diabetes, salud ocular, salud mental y salud bucal.
- OE8.Reducir la Tasa de incidencia de las EDAS.
- OE9.Disminuir la Tasa de incidencia por Dengue, malaria, peste, leshmaniasis y rabia.
- OE10.Reducir la vulnerabilidad ante peligros naturales frente a emergencias y desastres.
- OE11.Incrementar el acceso a los servicios de salud (cobertura SIS, Débil Sistema de Referencia y Contra referencia).

1.3.- Estructura Orgánica

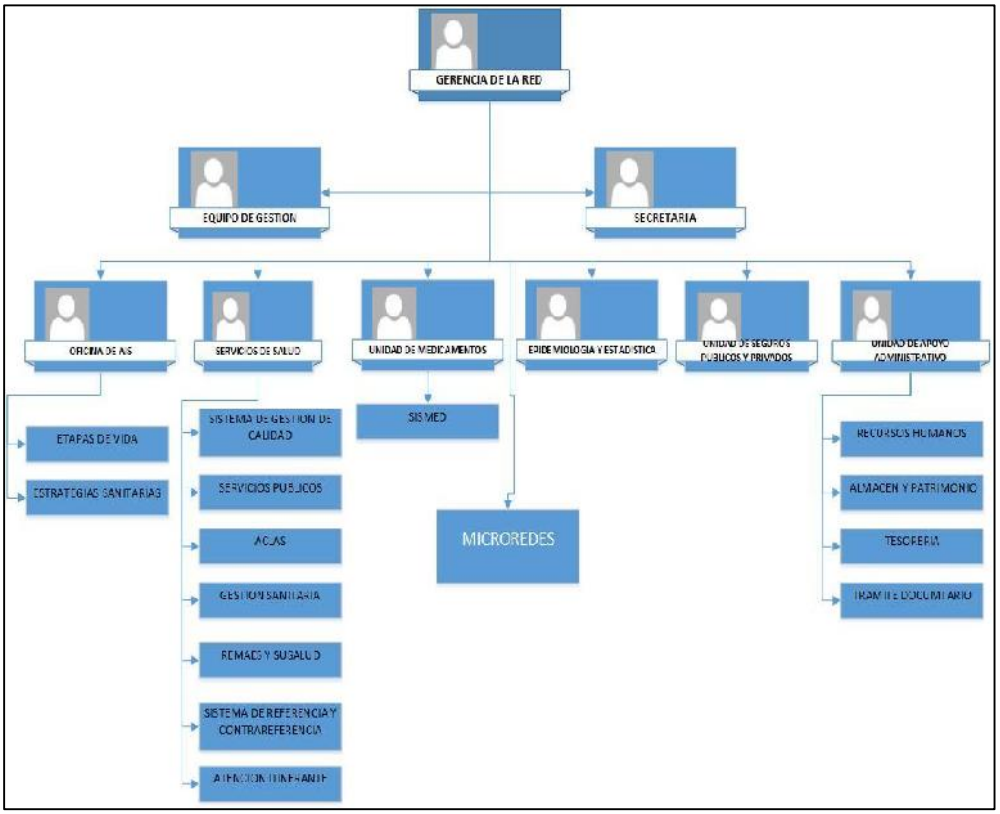


Figura N° 01: Estructura Orgánica de la Institución

Fuente: (Red de Salud de Lambayeque, Manual de Organizacion y Funciones 2015, 2015)

1.4.- Infraestructura Tecnológica

En la Red de Salud de Lambayeque según el alcance del SGSI se identificó la siguiente infraestructura, que se detalla a continuación:

1.4.1.- Hardware

a) Equipos de Red

- 1 Switch Tplink 24 puertos
- 1 Router nucom R5000 UN V2
- Cableado UTP categoría 5

b) Equipos de cómputo

- 1 Impresora multifuncional Epson L555
- 1 Impresora multifuncional Konica Minolta bizhub 282
- 2 Impresora hp LaserJet p1102w
- 14 pcs HP Compaq Elite8300

1.4.2.- Software

Los sistemas y aplicaciones que se tienen son los siguientes:

a) Sistema Operativo

- Windows 7 de 64 bits
- Windows 7 de 32 bits

b) Aplicaciones en las pcs

Se detalla las siguientes aplicaciones y sistemas usadas por los trabajadores:

- Microsoft Office 2007
- Adobe Reader 2013
- Antivirus Nod 32 Antivirus 8.0304.1
- Antivirus Avast
- Team Viewer versión 9.0
- SISMED (Sistema Integrado de Suministro de medicamentos e Insumos Médicos Quirúrgicos)
- SPSS
- HIS
- SIEN (Sistema De Información Del Estado Nutricional)

CAPÍTULO II: PROBLEMÁTICA DE LA INVESTIGACIÓN

2.1.- Realidad problemática

2.1.1.- Planteamiento del Problema

La Red de Salud de Lambayeque ubicada en av. Libertad 530 Lambayeque, es un órgano desconcentrado que depende jerárquicamente de la Dirección Regional de Salud de Lambayeque. Tiene como objetivo principal el abastecimiento oportuno de productos farmacéuticos, dispositivos médicos y productos sanitarios de las estrategias sanitarias a los 88 Establecimientos de Salud que se encuentran bajo su cargo; para eso realiza la recepción de la información de los casos presentados y atenciones de las diferentes estrategias en formatos de requerimientos y el registro de los datos en los Sistemas de Información.

Actualmente la Red de Salud de Lambayeque está organizada en las siguientes áreas que son: Oficina de Atención Integral de Salud, Servicios de Salud, Unidad de Medicamentos, Epidemiología y Estadística, Unidad de Apoyo administrativo, Unidad de Seguros Públicos y privados.

Para la presente investigación se tomó como alcance el área de informática, el área de SISMED, oficinas de estrategias sanitarias, así como el área de almacén que conforman el proceso de gestionar el suministro de medicamentos por ser un proceso crítico. Este proceso empieza con la digitación de los requerimientos de medicamentos en los 88 establecimientos de salud correspondientes a la red de salud de Lambayeque. Luego los responsables de farmacia traen sus guías de remisión y sus informes de requerimientos para ser revisados por el área del SISMED para su control de calidad, luego según cada estrategia sanitaria también se coordina para el abastecimiento de medicamentos. Finalmente, si hay la disponibilidad en el momento llevan de almacén los medicamentos que requieran llevar según su hoja de disponibilidad y su respectivo informe. En total son 14 personas involucradas en este proceso, 1 encargado de almacén, 1 encargado el SISMED, 1 encargado de informática y 11 coordinadores de estrategias sanitarias.

El 62% usa un sistema de información mientras que el 38 % lo realiza de forma manual dentro del proceso de gestionar el suministro de medicamentos dentro de la red de salud de Lambayeque.

Actualmente se ha determinado la siguiente problemática en base a una encuesta realizada a los mismos trabajadores y al responsable de

informática: Se pudo determinar que el 100% considera que no se siente seguro en el ambiente donde se encuentra los equipos informáticos; el 8% aun no usa la forma debida de apagar los equipos; el 92% observa que no existe un extintor cerca de los equipos; solo el 15% observa que existe una señalización de emergencia donde existe equipos informáticos; el 62 % nunca ha participado en un simulacro frente a un desastre natural o humano donde hay equipos informáticos; el 77 % ingiere bebidas o come cuando realiza un trabajo en la computadora, realizando una mala práctica de seguridad de su información. El 54% tiene que manipular algún componente de su computador para que este funcione ocasionando un retraso en sus labores. El 92 % saca información en algún dispositivo de almacenamiento por lo que se debe tener en cuenta que la información no vaya ser divulgada por precaución. El 23 % aún no sabe cómo utilizar un antivirus cuando es necesario. El antivirus no funciona correctamente según el 31 %. El principal medio de hacer llegar la información es el correo electrónico, el 31 % de los trabajadores indican que alguna vez le fallo el enviar o recibir un correo. Se determinó que el 85 % no usa un usuario y contraseña para ingresar a su computadora; El 62 % no siempre son las únicas personas que utilizan sus equipos, sino que lo comparten. El total de trabajadores desconoce sobre seguridad de la información, ya que nunca ha tenido una capacitación. El 100% indica que por lo menos una vez le han revisado la pc ante una falla en la pc. El 54% indico que alguna vez había perdido su información. La instalación del cableado estructurado y conexiones eléctricas no tienen una correcta instalación según los mismos trabajadores en un 54%, el 46 % de los equipos informáticos y componentes no están codificados. En cuanto a los acuerdos de no divulgación de la información que se trabaja en la red, solo el 15% sabe que existe ocasionando muy poca responsabilidad sobre ésta información.

Según el responsable de informática existe políticas de seguridad que solo abarcan la generación de backups, solo les sugiere a los trabajadores que guarden su información en su USB o quemarlo en un Cd; no hay todavía un control para la protección si hubiera una interrupción como corte de luz dentro de las instalaciones.

Todavía no se ha implementado ningún servidor en la red de salud, ya que solo se trabaja con correos electrónicos en caso quiera enviar o recibir algún

tipo de información, ya sea de las micro redes que envían su información a la red y de la red a la Gerencia Regional de Salud.

En cuanto a las licencias del Microsoft Office ninguna tiene licencia y el 25% de computadoras no cuentan con licencia para Windows 7.

Ante ésta problemática se ha propuesto diseñar un Sistema de Gestión de Seguridad de Información para proteger los activos de información en el proceso de suministro de medicamentos, permitiendo así una buena toma de decisiones en la Red de Salud de Lambayeque.

2.2.- Formulación del Problema

¿Cómo permitirá proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque, el diseño de un Sistema de Gestión de Seguridad de la información SGSI basado en la Norma ISO/IEC 27001 e ISO/IEC 27002?

2.3.- Justificación e Importancia de la Investigación

2.3.1.- Justificación Económica

Porque el desarrollo del Proyecto va a permitir que la persona encargada de la gestión de la información respecto al SISMED mejore de manera eficiente y eficaz la aplicación de la seguridad y el flujo adecuado de la información, reduciendo costos ante cualquier incidente.

2.3.2.- Justificación Tecnológica

Hoy en día las instituciones y o empresas hacen uso de información en todos sus procesos para lo cual implementan ciertos procedimientos. El uso de un Sistema de Gestión de Seguridad de la Información en todo tipo de empresa traerá consigo muchos beneficios como: análisis de riesgos, identificación de amenazas, vulnerabilidades e impactos en las actividades de la empresa, la mejora continua en gestión de la seguridad, mejora de la imagen de la organización, garantía de continuidad y disponibilidad del negocio.

La Red de Salud de la Lambayeque es un órgano desconcentrado de la Dirección Regional de Salud de Lambayeque que tiene como principal fin abastecer de una manera oportuna productos farmacéuticos, dispositivos

médicos y productos sanitarios a los diferentes establecimientos de salud a los cuales tiene a cargo; para esto utilizan una gran cantidad de información en sus procesos , usando desde formatos en físico hasta el uso de sistemas de información, donde se observó la falta o poca seguridad para los activos de la información, primordiales para el proceso de suministro de medicamentos. De esta manera se ha planteado diseñar un Sistema de Gestión de Seguridad de Información que permita la buena gestión de los recursos informáticos asegurando su confidencialidad, integridad, disponibilidad.

2.3.3.- Justificación social

Se mejoraría de esta forma la comunicación y el clima tecnológico entre los trabajadores dentro de la Red de Salud de Lambayeque, haciendo participe a todos en el buen funcionamiento del Sistema de Gestión de Seguridad de la información y además permitiendo que la información deje de ser una actividad poco organizada y poco apoyada por los trabajadores para ser un conjunto de actividades metódicas y controladas.

2.3.4.- Justificación científica

En la actualidad se puede diseñar diferentes sistemas de gestión, que van de la mano con las nuevas tecnologías, metodologías, etc. Trabajar e investigar con estos recursos permite a las personas incrementar los conocimientos que día a día vamos aprendiendo y gracias a ello somos mejores profesionales.

2.3.5.- Importancia

El diseño de un SGSI será de vital importancia para mejorar la protección y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de la información en la Red de Salud de Lambayeque, reduciendo así los riesgos de pérdida de información si en algún momento se diera algún tipo de amenaza.

2.4.- Objetivos de la Investigación

2.4.1.- Objetivo General

Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) basado en las normas internacionales ISO/IEC 27001 e ISO/IEC 27002, para proteger los activos de la información en el proceso de suministro de medicamentos en la Red de Salud de Lambayeque.

2.4.2.- Objetivos Específicos:

- Identificar los procesos de negocios de la entidad involucrados en la gestión de seguridad informática.
- Valorar los activos de información según la Norma ISO/IEC 27005 asociados al proceso de suministro de medicamentos en la red de salud de Lambayeque.
- Evaluar los riesgos a los que están expuestos los activos con criticidad alta en la red de Salud de Lambayeque, apoyándose de la Norma ISO/IEC 27005.
- Seleccionar los controles que permitan gestionar y tratar los riesgos identificados en base a la Norma ISO/IEC 27002
- Elaborar la documentación exigida por la Norma ISO/IEC 27001 adoptada para el diseño del SGSI en la red de Salud de Lambayeque.

2.5.- Limitaciones de la Investigación

2.5.1- Geográfica

El Proyecto se desarrollará en los ambientes de la Red de Salud de Lambayeque ubicado en av. libertad 530 Lambayeque, donde se va diseñar un Sistema de Gestión de Seguridad de la Información.

2.5.2.- Administrativa

Las áreas donde se va a realizar la investigación no cuentan con autonomía propia para llevar a cabo el desarrollo de la investigación ya que son áreas que dependen de la gerencia para cualquier autorización.

2.5.3.- Tecnológica

La Red de Salud de Lambayeque no cuenta con recursos de Tecnología de información en sus instalaciones, por tal motivo ésta investigación ha tomado mucho énfasis en las áreas que son fundamentales para el correcto

procesamiento de la información y así cumplir con el objetivo de la Institución.

2.5.4.- Científica

Se hizo un análisis durante la investigación del tema a desarrollar, encontrando que no existe información en libros, pero si se encontró artículos y otros recursos web que ayudaron a desarrollar la Tesis.

2.5.5.- Personal

Las personas que trabajan en la Institución la mayoría no están familiarizadas con las normas de seguridad respecto a la información, a través de ésta investigación se les ayuda a tener mayor conocimiento sobre tema seguridad y que lo apliquen en sus actividades diarias.

2.5.6.- Económicas

Realizar un Sistema de Gestión de Seguridad de la Información es económico y por lo tanto la aplicación de este presente proyecto permitirá en el futuro ahorrar en lo económico y agilizar los procesos.

CAPÍTULO III:

MARCO METODOLÓGICO

3.1.- Tipo de Investigación

Investigación tecnológica Formal

3.2.- Hipótesis

El diseño de un Sistema de Gestión de Seguridad de la Información basado en las normas ISO/IEC 27001 e ISO/IEC 27002, permite proteger los activos de la información en el proceso de Suministro de Medicamentos de la Red de Salud de Lambayeque.

3.3.-Variables

3.3.1. Variable Independiente

Sistema de Gestión de Seguridad de la Información

a) Definición conceptual:

Es parte del sistema de gestión general, basada en un enfoque de riesgo comercial para establecer, implementar, operar, monitorear, revisar y mejorar la seguridad de la información. (Padilla Ramos, 2013)

b) Definición operacional:

Es el diseño de un conjunto de procesos que permite asegurar la integridad, confidencialidad, accesibilidad, disponibilidad de los activos de la información y la mitigación de riesgos en el proceso de suministros de medicamentos en la Red de Salud de Lambayeque.

3.3.2. Variable Dependiente

Protección de los activos de información

a) Definición conceptual

Es la protección de todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

Seria critico que a una entidad que maneja alta información confidencial, los intrusos pudieran acceder a ella afectando así la confidencialidad, la disponibilidad y la integridad de dicha información por eso algunas de tantas

entidades adoptan un plan de seguridad para los activos de información y así no tener la desgracia de que los datos se fuguen, se modifiquen o se pierdan. (Caita Castro, 2015)

b) Definición operacional:

Implicar reglamentar con una serie de normas los controles que se debe usar para proteger la información que se encuentra tanto en equipos informáticos como en sistema de información o documentos que se maneja en la Red de Salud de Lambayeque.

3.4.- Selección de la metodología

Para el desarrollo del Sistema de Gestión de Seguridad de la Información se empleó la metodología PDCA o Ciclo Deming cuyas siglas significan: Plan, Do Check, Act, que en español es Planear, Hacer, Verificar y Actuar.

Esta metodología es la que más se ajusta como una estrategia de mejora continua en los procesos de cualquier organización y también para la documentación que se usa para estos procesos; además este modelo se alinea con la ISO 27001 para la implementación de un buen sistema de gestión de seguridad de la información.

3.4.1.- Ciclo Deming (2005) Mejora Continua. (Agustín & Javier, 2015)

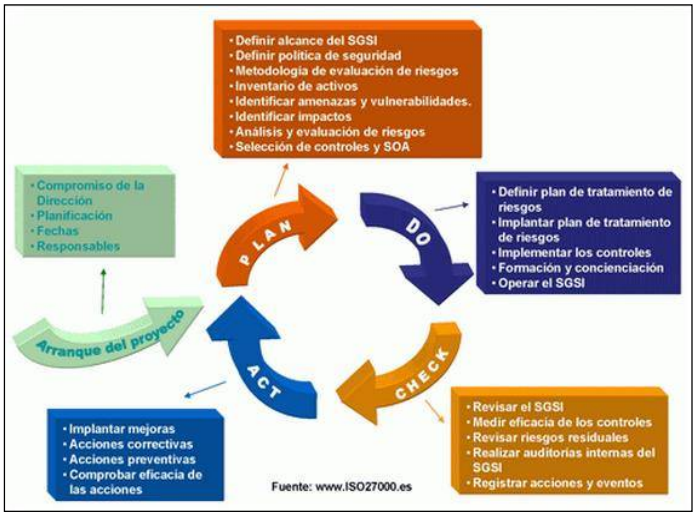


Figura N° 02: Ciclo Deming

Fuente: (Agustín & Javier, 2015)

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001:2005, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

3.4.1.1.- Plan =Establecer con planificación

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Es importante que defina los límites del SGSI ya que no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado). Es importante disponer de un mapa de procesos de negocio, definir claramente los interfaces con el exterior del alcance, determinar las terceras partes (proveedores, clientes, etc.) que tienen influencia sobre la seguridad de la información del alcance, crear mapas de alto nivel de redes y sistemas, definir las ubicaciones físicas, disponer de organigramas organizativos, definir claramente los requisitos legales y contractuales relacionados con seguridad de la información, etc.

La política del SGSI es normalmente un documento muy general, una especie de "declaración de intenciones" de la Dirección pero que:

- Incluya el marco general y los objetivos de seguridad de la información de la organización;
- tenga en cuenta los requisitos de negocio además de considerar los requerimientos legales o contractuales relativos a la seguridad de la información;
- Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
- Establezca los criterios con los que se va a evaluar el riesgo;
- Esté aprobada por la dirección.

- **Definir el Enfoque de evaluación de Riesgos**

Mediante una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio. El riesgo nunca es totalmente eliminable ni sería rentable hacerlo, por lo que es necesario definir una estrategia de aceptación de riesgo estableciendo criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de la metodología es que los resultados obtenidos sean comparables y repetibles para evitar grados de subjetividad que falseen la

valoración de los riesgos. Existen numerosas metodologías estandarizadas para la evaluación de riesgos y la organización puede optar por una de ellas, aplicar una combinación de varias o crear la suya propia. ISO 27001:2005 no impone ninguna para que cada organización pueda aplicar la que estime más oportuno y funcional según el esfuerzo de análisis y recursos que pueda aplicar. Como documento de apoyo ISO 27005 sí profundiza en directrices sobre la materia.

- **Identificar los riesgos:**

  - ✓ Identificar todos aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
  - ✓ Identificar las amenazas relevantes asociadas a los activos identificados;
  - ✓ Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
  - ✓ Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

- **Analizar y evaluar los riesgos:**

  - ✓ Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
  - ✓ Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
  - ✓ Estimar los niveles de riesgo;
  - ✓ Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

- **Tratamiento de riesgos:**

  Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

  - ✓ Aplicar controles adecuados (mitigación);
  - ✓ Aceptar el riesgo (de forma consciente), siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
  - ✓ Evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
  - ✓ Transferir el riesgo total o parcialmente a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.

- **Seleccionar los objetivos de control y los controles:**

  Para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.

- **Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.**

  Hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación final en cada revisión y/o acciones de tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

- **Definir una declaración de aplicabilidad también llamada SOA**
  - ✓ Los objetivos de control y controles seleccionados y los motivos para su elección;
  - ✓ Los objetivos de control y controles que actualmente ya están implantados;
  - ✓ Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

3.4.1.2.- Do = Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

3.4.1.3.- Check = Monitorizar y Revisar

- **La organización deberá:**
  - ✓ Ejecutar procedimientos de monitorización y revisión para:
    - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
    - Identificar brechas e incidentes de seguridad;
    - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
    - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
    - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- ✓ Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

- ✓ Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

- ✓ Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior - requerimientos legales, obligaciones contractuales, etc.

- ✓ Realizar periódicamente auditorías internas del SGSI en intervalos planificados para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001:2005, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.

- ✓ Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y las posibles mejoras en el proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

- ✓ Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión

- ✓ Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

3.4.1.4- Act=Mantener y Mejorar

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas para prevenir potenciales no conformidades antes de que se produzcan y solucionar no conformidades detectadas y materializadas. En relación a la cláusula 8 de ISO 27001:2005 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

CAPÍTULO IV:
MARCO TEÓRICO

4.1.- Antecedentes

4.1.1.- Antecedentes en el contexto internacional

Título: Sistema de Gestión de Seguridad de la información (SGSI) para el área de contabilidad de la E.S.E. Hospital local de rio de Oro Cesar"
Universidad: Universidad Francisco de Paula Santander Ocaña
Nacionalidad: Ecuador
Autores:

- Aura Lucia Casadiegos Santana.
- Marcela Quintero Jiménez.
- Mileidy Toro Rueda.

Conclusión:
Tomando como marcos de referencia, normas o buenas prácticas, se identificaron COBIT 4.1, NTC-ISO/IEC 27001 y NTC-ISO/IEC 27002, mostrando un comparativo entre las mismas y de acuerdo a la necesidad encontrada en el Área de Contabilidad que justifique establecer un Sistema de Gestión de Seguridad de la Información, se tomó como base la norma NTC-ISO/IEC 27001 que ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información y la NTC-ISO/IEC 27002 puesto que permite buenas prácticas para salvaguardar la información.

La importancia de la implementación del sistema de gestión de seguridad de la información en el Área contable se ve reflejada al realizar el diseño según la norma ISO/IEC 27001:2005 aplicando todos sus controles en cada uno de sus procesos contables y realizando todos los seguimientos acordes a lo establecido en dicha norma.

Título: “Diseño del Sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda”

Universidad: Universidad Tecnológica de Pereira

Nacionalidad: Colombia

Autores:

- Juan David Aguirre Cardona.
- Catalina Aristizabal Betancourt.

Conclusión:

Cabe resaltar que, partiendo de esta premisa, es importante contar con un Sistema de Gestión de Seguridad de la Información para poder asegurar, a un nivel aceptable, la información, de la organización empresarial La Ofrenda S.A, la cual es colombiana, dado que se trata de una organización dedicada a satisfacer integralmente las necesidades de la población en servicios funerarios, parques cementerios y cremación; es una organización, poder cumplir con las regulaciones de la ISO 27002.

En este documento se consideraron los procesos que tiene el grupo empresarial La Ofrenda S.A, pero es importante considerar siempre que el SGSI debe estar enfocado en las necesidades del negocio. Es decir, si la organización considera un 80 proceso en particular como crítico, se deben implementar controles necesarios para asegurar el mismo.

4.1.2.- Antecedentes en el contexto nacional

Título: “Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo”

Universidad: Pontificia Universidad Católica Del Perú

Nacionalidad: Lima -Perú

Autor:

- Luis Carlos Aliaga Flores.

Conclusión:

Un Sistema de Gestión de Seguridad de Información (SGSI) establecido en una institución educativa se muestra como la solución para que el flujo de información que se da entre los procesos críticos y los activos involucrados dentro de dichos procesos, logren el nivel de seguridad adecuado para garantizar el cumplimiento de los objetivos de TI y, en consecuencia, los objetivos organizacionales.

Título: "Diseño de un sistema de gestión de seguridad de información para una compañía de seguros"

Universidad: Pontificia Universidad Católica Del Perú

Nacionalidad: Lima -Perú

Autor:

- Ampuero Chang, Carlos Enrique.

Conclusión:

Cumplir con la normativa impuesta por la SBS (la circular G140) para todas las compañías de seguros que operen en territorio peruano.

Brindar un nivel aceptable de seguridad con relación a la información que maneja la empresa, evitando incidentes que puedan afectar en la operativa diaria de la misma.

Contar con un modelo que se amolde al paso del tiempo y se pueda actualizar siempre, debido a las revisiones periódicas a las que se ve sujeto el SGSI.

Título: "Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos"

Universidad: Universidad San Martin de Porres.

Nacionalidad: Lima Perú

Autores:

- Barrantes Porras, Carlos Eduardo.
- Hugo Herrera, Javier Roberto.

Conclusión:

El implementar una política de seguridad y que los colaboradores la conozcan e interiorizan, es de gran utilidad cuando se quiere implementar cualquier sistema de gestión en una organización, ya que les da una visión clara de cómo sus labores cotidianas aportan para el mantenimiento y mejora de un sistema de gestión empresarial.

Diseñando e implementando una buena metodología para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables gran porcentaje de riesgos que afecten a los activos de información.

4.1.3.- Antecedentes en el contexto local

Título: "Elaboración y Aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) Para La Realidad Tecnológica de la Usat"

Universidad: Universidad Católica Santo Toribio de Mogrovejo-Chiclayo

Nacionalidad: Perú

Autores:

- César Wenceslao de la Cruz Guerrero.
- Juan Carlos Vásquez Montenegro.

Conclusión:

El objetivo es elaborar y aplicar un Sistema de Gestión de la Seguridad de la Información en la Universidad Católica Santo Toribio de Mogrovejo delimitando nuestro alcance a las áreas involucradas con las Tics (Desarrollo de Sistemas y Taller de computo), con lo cual pretendemos garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados; de manera que se busca proteger la información de un amplio rango de amenazas.

Título: “Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo”.

Universidad: Universidad Católica Santo Toribio de Mogrovejo

Nacionalidad: Chiclayo -Perú

Autor:

- Julio César Alcántara Flores.

Conclusión:

Con la Guía de Implementación, se logró incrementar el nivel de seguridad en las aplicaciones informáticas de la institución policial, y esto se vio reflejado en el incremento de políticas de seguridad que fueron puestas en marcha que beneficiaron a la institución y ayudaron a incrementar el nivel de seguridad en la misma.
El uso de la guía de implementación, se logró mejorar el proceso para detectar las anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla prevenir su mal uso y divulgación no adecuada que perjudiquen a la institución.

4.2.- Base teórica

4.2.1.- Sistema de Gestión de Seguridad de Información (SGSI) (Agustín & Javier, 2015)

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

4.2.1.1.- Fundamentos

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, es de un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

4.2.1.2.- Uso

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

4.2.1.3.- Beneficios

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.

- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

4.2.1.4.- Aspectos clave

a) Fundamentales:

- Compromiso y apoyo de la Dirección de la organización que debe:
  - ✓ Establecer una política de seguridad de la información.
  - ✓ Asegurarse de que se establecen objetivos y planes del SGSI.
  - ✓ Establecer roles y responsabilidades de seguridad de la información.
  - ✓ Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
  - ✓ Asignar suficientes recursos al SGSI en todas sus fases.
  - ✓ Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
  - ✓ Asegurar que se realizan auditorías internas.
  - ✓ Realizar revisiones del SGSI, como se detalla más adelante.
- Definición clara de un alcance apropiado.
- Concienciación y formación del personal en base a:
  - ✓ Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.
  - ✓ Satisfacer dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado.
  - ✓ Evaluar la eficacia de las acciones realizadas.

- ✓ Mantener registros de estudios, formación, habilidades, experiencia y cualificación.
- ✓ Además, la dirección debe asegurar que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

- Evaluación de riesgos adecuada a la organización.
- Compromiso de mejora continua por la dirección con evidencias de:

  Al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

  - ✓ Resultados de auditorías y revisiones del SGSI.
  - ✓ Observaciones de todas las partes interesadas.
  - ✓ Consideración de técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
  - ✓ Información sobre el estado de acciones preventivas y correctivas.
  - ✓ Identificación de vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
  - ✓ Resultados de las mediciones de eficacia.
  - ✓ Revisión de estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
  - ✓ Valoración de cualquier cambio que pueda afectar al SGSI.
  - ✓ Recomendaciones de mejora.
  - ✓ Toma de decisiones y acciones positivas.
  - ✓ Mejora de la eficacia del SGSI.
  - ✓ Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.

- ✓ Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- ✓ Necesidades de recursos.
- ✓ Mejora de la forma de medir la efectividad de los controles.

- Establecimiento de políticas y normas.
- Organización y comunicación.
- Gestión adecuada de la continuidad de negocio, de los incidentes de seguridad, del cumplimiento legal y de la externalización.
- Integración del SGSI en la organización.

b) Factores de Éxitos

- La concienciación del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités a distintos niveles (operativos, de dirección, etc.) con gestión continua de no conformidades, incidentes de seguridad, acciones de mejora, tratamiento de riesgos...
- Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.

c) Riesgos

- Exceso de tiempos de implantación: con los consecuentes costes descontrolados, desmotivación, alejamiento de los objetivos iniciales, etc.
- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.
- Delegación de todas las responsabilidades en departamentos técnicos.
- No asumir que la seguridad de la información es inherente a los procesos de negocio.
- Planes de formación y concienciación inadecuados.
- Calendario de revisiones que no se puedan cumplir.
- Definición poco clara del alcance.
- Exceso de medidas técnicas en detrimento de la formación, concienciación y medidas de tipo organizativo.
- Falta de comunicación de los progresos al personal de la organización.

d) Consejos Básicos

- Mantener la sencillez y restringirse a un alcance manejable y reducido: un centro de trabajo, un proceso de negocio clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases.
- Comprender en detalle el proceso de implantación: iniciarlo en base a cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación; adquirir experiencia de otras implantaciones, asistir a cursos de formación o contar con asesoramiento de consultores externos especializados.
- Gestionar el proyecto fijando los diferentes hitos con sus objetivos y resultados.
- La autoridad y compromiso decidido de la Dirección de la empresa -incluso si al inicio el alcance se restringe a un alcance reducido- evitarán

un muro de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales de la norma.

- La certificación como objetivo: aunque se puede alcanzar la conformidad con la norma sin certificarse, la certificación por un tercero asegura un mejor enfoque, un objetivo más claro y tangible y, por lo tanto, mejores opciones de alcanzar el éxito. Eso sí, la certificación es la "guinda del pastel", no es bueno que sea la meta en sí misma. El objetivo principal es la gestión de la seguridad de la información alineada con el negocio.
- No reinventar la rueda: apoyarse lo más posible en estándares, métodos y guías ya establecidos, así como en la experiencia de otras organizaciones.
- Servirse de lo ya implementado: otros sistemas de gestión (como ISO 9001 para la calidad o ISO 14001 para medio ambiente) ya implantados en la organización son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo y creando sinergias; es conveniente pedir ayuda e implicar a responsables y auditores internos de otros sistemas de gestión.
- Reservar la dedicación necesaria diaria o semanal: el personal involucrado en el proyecto debe ser capaz de trabajar con continuidad en el proyecto.
- Registrar evidencias: deben recogerse evidencias al menos tres meses antes del intento de certificación para demostrar que el SGSI funciona adecuadamente. No precipitarse en conseguir la certificación.
- Mantenimiento y mejora continua: tener en consideración que el mantenimiento y la mejora del SGSI a lo largo de los años posteriores requerirán también esfuerzo y recursos.

4.2.2.- ISO/IEC 27001 (Wikipedia, ISO/IEC 27001 Wikipedia, La Enciclopedia Libre, 2015)

Es un estándar para la seguridad de la información (Information technology - Security techniques–Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electro technical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como “Ciclo de Deming”: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

4.2.2.1.- ISO 27001:2013

Existen varios cambios con respecto a la versión 2005 en esta versión 2013. Entre ellos destacan:

- Desaparece la sección "enfoque a procesos" dando mayor flexibilidad para la elección de metodologías de trabajo para el análisis de riesgos y mejoras.
- Cambia su estructura conforme al anexo SL común al resto de estándares de la ISO.
- Pasa de 102 requisitos a 130.
- Considerables cambios en los controles establecidos en el Anexo A, incrementando el número de dominios a 14 y disminuyendo el número de controles a 114.
- Inclusión de un nuevo dominio sobre "Relaciones con el Proveedor" por las crecientes relaciones entre empresa y proveedor en la nube.
- Se parte del análisis de riesgos para determinar los controles necesarios y compararlos con el Anexo A, en lugar de identificar primero los activos, las amenazas y sus vulnerabilidades.

4.2.2.2.- Beneficios que aporta la norma a la Organización

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

4.2.2.3- Implantación

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información elegido. En general, es recomendable la ayuda de consultores externos.

Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos (p.ej., en España la conocida LOPD y sus normas de desarrollo, siendo el más importante el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos) o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente Ingenieros o Ingenieros Técnicos en Informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información (que hayan realizado un curso de implantador de SGSI).

4.2.2.4.- Certificación

La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

Antes de la publicación del estándar ISO 27001, las organizaciones interesadas eran certificadas según el estándar británico BS 7799-2.

Desde finales de 2005, las organizaciones ya pueden obtener la certificación ISO/IEC 27001 en su primera certificación con éxito o mediante su re certificación trienal, puesto que la certificación BS 7799-2 ha quedado reemplazada.

La norma muestra las correspondencias del Sistema de Gestión de la Seguridad de la Información (SGSI) con el Sistema de Gestión de la Calidad según ISO 9001:2000 y con el Sistema de Gestión Medio Ambiental según ISO 14001:2004 (ver ISO 14000), hasta el punto de poder llegar a certificar una organización en varias normas y con base en un sistema de gestión común.

4.2.2.5.- Fases del modelo PDCA (Gobierno de España, 2015)

- **Planificación (Plan) [establecer el SGSI]**

Establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejorar la seguridad de la información de la organización para ofrecer resultados de acuerdo con las políticas y objetivos generales de la organización.

- ✓ Identificar lo que se quiere mejorar.
- ✓ Recopilar datos del proceso que se quiere mejorar.
- ✓ Analizar los datos recogidos.
- ✓ Establecer los objetivos de mejora.
- ✓ Detallar los resultados esperados.
- ✓ Definir los procesos necesarios conseguir los objetivos.

- **Ejecución (Do) [implementar y gestionar el SGSI]**

Implementar y gestionar el SGSI de acuerdo a su política, controles, procesos y procedimientos. En la medida de lo posible debería hacerse en un entorno de prueba para poder verificar sus resultados antes de implantarlo en el sistema real.

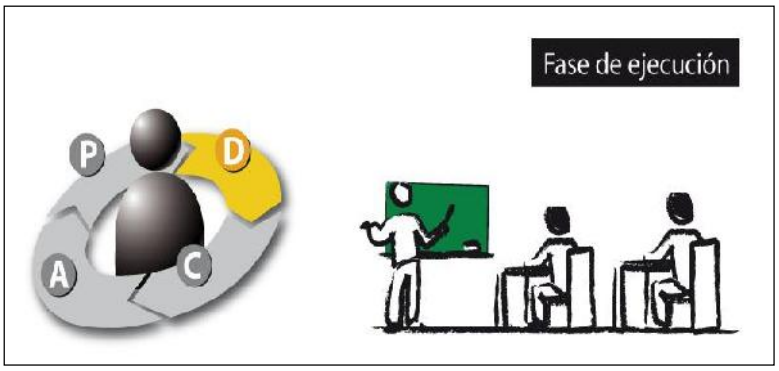


Figura Nº 03: Fase de Ejecución

Fuente: (Gobierno de España, 2015)

- **Seguimiento (Check) [monitorizar y revisar el SGSI]**

Verificar, Medir y revisar las prestaciones de los procesos del SGSI. Comprobar que las medidas adoptadas han surtido efecto, para ello se debe volver a recopilar datos y monitorizar el comportamiento del sistema.

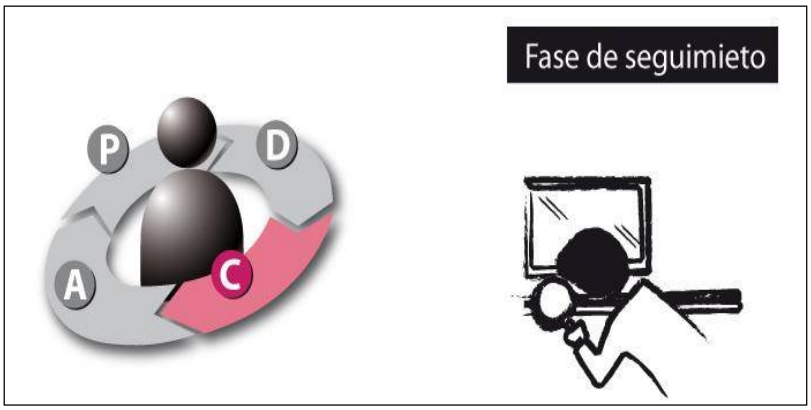


Figura Nº 04: Fase de Seguimiento

Fuente: (Gobierno de España, 2015)

- **Mejora (Act) [mantener y mejorar el SGSI]**

Adoptar acciones correctivas y preventivas basadas en auditorías y revisiones internas con el objetivo de mejorar el SGSI. Hace referencia a la actitud que se debe tomar después de los tres primeros pasos y dependerá de lo que haya ocurrido. En caso de haber ocurrido algún mal funcionamiento, se deberá repetir el ciclo de nuevo. Si el funcionamiento ha sido correcto, se instalarán las modificaciones en el sistema de manera definitiva.

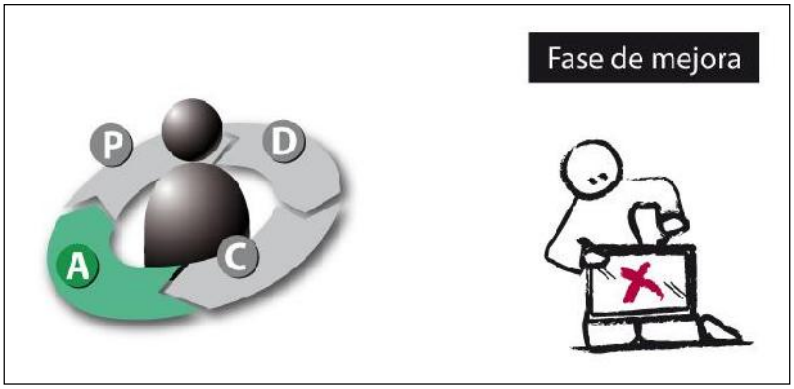


Figura Nº 05: Fase de Mejora

Fuente: (Gobierno de España, 2015)

4.2.3.- ISO/IEC 27002 (ISO, ISO/IEC 27002:2013(en), 2015)

Esta Norma Internacional está diseñado para que las organizaciones utilizan como referencia para la selección de los controles en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO / IEC 27001 o como un documento de orientación para las organizaciones que efectúan controles de seguridad de la información generalmente aceptadas. Esta norma también es para uso en el desarrollo de directrices de gestión de seguridad de la información y la industria- específicas de la organización, teniendo en cuenta su entorno de riesgo seguridad de la información específica.

Organizaciones de todos los tipos y tamaños (incluyendo sector público y privado, comercial y sin fines de lucro) recoger, procesar, almacenar y transmitir información en muchas formas, incluyendo (conversaciones y presentaciones por ejemplo electrónicos, físicos y verbales).

El valor de la información va más allá de los escritos palabras, números e imágenes: conocimientos, conceptos, ideas y marcas son ejemplos de formas intangibles de información. En un mundo interconectado, los procesos de información y afines, sistemas, redes y personal que participan en su funcionamiento, manejo y protección son activos que, al igual que otros activos comerciales importantes, son valiosos para el negocio de una organización y, en consecuencia, merecen o que requieren protección contra diversos riesgos.

Los activos están sujetos a las amenazas deliberadas o accidentales, mientras que los relacionados con los procesos, los sistemas, las redes y las personas tienen vulnerabilidades inherentes. Los cambios en los procesos de negocio y sistemas u otros cambios externos (por ejemplo, nuevas leyes y reglamentos) pueden crear nuevos riesgos de seguridad de la información. Por lo tanto, dada la multiplicidad de formas en que las amenazas podrían aprovecharse de las vulnerabilidades para dañar a la organización, los riesgos de seguridad de la información están siempre presentes. Seguridad de la información eficaz reduce estos riesgos mediante la protección de la organización contra las amenazas y vulnerabilidades, y luego reduce los impactos de sus activos.

Seguridad de la información se logra mediante la implementación de un conjunto adecuado de controles, incluidas las políticas, procesos, procedimientos, estructuras organizativas y de software y funciones de hardware. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y de negocios de la organización. Un SGSI como el que se especifica en la norma ISO / IEC 27001 tiene una visión holística y coordinada de los riesgos de seguridad de la información de la organización con el fin de poner en práctica un conjunto completo de controles de seguridad de la información en el marco general de un sistema de gestión coherente.

Muchos sistemas de información no han sido diseñados para ser seguro en el sentido de la norma ISO / IEC 2700 y este estándar. La seguridad de que se puede lograr a través de medios técnicos es limitada y debe ser apoyada por la administración y los procedimientos apropiados. La identificación que controla debe estar en su lugar requiere una cuidadosa planificación y atención al detalle. Un éxito SGSI requiere el apoyo de todos los empleados en la organización. También se puede requerir la participación de los accionistas, proveedores u otras partes externas. Asesoramiento especializado de las partes externas también puede ser necesario.

En un sentido más general, seguridad de la información eficaz también asegura la administración y otras partes interesadas de que los activos de la organización son razonablemente seguros y protegidos contra daños, actuando, así como un habilitador de negocios.

4.2.3.1.- Alcance

Esta Norma Internacional proporciona directrices para las normas de seguridad de información de la organización y las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta el medio ambiente riesgo seguridad de la información de la organización

Esta Norma Internacional está diseñado para ser utilizado por las organizaciones que tengan la intención de:

- controles seleccionados dentro del proceso de implantación de un Sistema de Gestión de Seguridad de la Información basado en ISO / IEC 27001;
- aplicar controles de seguridad de la información generalmente aceptadas;
- desarrollar sus propias directrices de gestión de seguridad de la información.

4.2.3.2.- Estructura

Está organizado en base a los 14 dominios, 35 objetivos de control y 114 controles de ISO/IEC 27002:2013.

Dominios Contemplados:

- Políticas de Seguridad
- Aspectos Organizativos de la Seguridad de la información
- Seguridad ligada a los recursos humanos
- Gestión de activos
- Control de accesos
- Cifrado
- Seguridad Física y Ambiental
- Seguridad en la Operativa
- Seguridad en las Telecomunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Relaciones con Suministradores
- Gestión de incidentes en la Seguridad de la información
- Aspectos de la Seguridad de la Información en la gestión de la continuidad del negocio
- Cumplimiento

Controles:

A. Políticas de Seguridad

5.1 Directrices de la Dirección en seguridad de la información

Actividades de control del riesgo:

5.1.1 Políticas para la seguridad de la información

5.1.2 Revisión de las políticas para la seguridad de la información

B. Aspectos Organizativos de la Seguridad de la información

6.1 Organización Interna

Actividades de control del riesgo:

6.1.1 Asignación de responsabilidades para la SI

6.1.2 Segregación de tareas

6.1.3 Contacto con las autoridades

6.1.4 Contacto con grupos de interés especial

6.1.5 Seguridad de la información en la gestión de proyectos

6.2. Dispositivos para movilidad y teletrabajo

Actividades de control del riesgo

6.2.1 Política de uso de dispositivos para movilidad

6.2.2 Teletrabajo

C. Seguridad ligada a los recursos humanos

7.1 Antes de la contratación

Actividades de control del riesgo:

7.1.1 Investigación de antecedentes

7.1.2 Términos y condiciones de contratación

7.2. Durante la contratación

Actividades de control del riego:

7.2.1 Responsabilidades de gestión

7.2.2 Concienciación, educación y capacitación en SI

7.2.3 Proceso disciplinario

7.3. Cese o cambio de puesto de trabajo

Actividades de control del riego:

7.3.1. Cese o cambio de puesto de trabajo

D. Gestión de activos

8.1. Responsabilidad sobre los activos

Actividades de control del riesgo:

8.1.1 Inventario de activos

8.1.2 Propiedad de los activos

8.1.3 Uso aceptable de los activos

8.1.4 Devolución de activos

8.2. Clasificación de la información

Actividades de control del riego:

8.2.1 Directrices de clasificación

8.2.2 Etiquetado y manipulado de la información

8.2.3 Manipulación de activos

8.3. Manejo de los soportes de almacenamiento

Actividades de control del riego:

8.3.1 Gestión de soportes extraíbles

8.3.2 Eliminación de soportes

8.3.3 Soportes físicos en tránsito

E. Control de accesos

9.1. Requisitos de negocio para el control de accesos

Actividades de control del riesgo:

9.1.1 Política de control de accesos

9.1.2 Control de acceso a las redes y servicios asociados

9.2. Gestión de acceso de usuario

Actividades de control del riesgo:

9.2.1 Gestión de altas/bajas en el registro de usuarios

9.2.2 Gestión de los derechos de acceso asignados a usuarios

9.2.3 Gestión de los derechos de acceso con privilegios especiales

9.2.4 Gestión de información confidencial de autenticación de usuarios

9.2.5 Revisión de los derechos de acceso de los usuarios

9.2.6 Retirada o adaptación de los derechos de acceso

9.3. Responsabilidades del usuario

Actividades de control del riesgo:

9.3.1 Uso de información confidencial para la autenticación

9.4. Control de acceso a sistemas y aplicaciones

Actividades de control del riesgo:

9.4.1 Restricción del acceso a la información

9.4.2 Procedimientos seguros de inicio de sesión

9.4.3 Gestión de contraseñas de usuario

9.4.4 Uso de herramientas de administración de sistemas

9.4.5 Control de acceso al código fuente de los programas

F. Cifrado

10.1. Controles criptográficos

Actividades de control del riesgo:

10.1.1 Política de uso de los controles criptográficos

10.1.2 Gestión de claves

G. Seguridad Física y Ambiental

11.1. Áreas seguras

Actividades de control del riesgo:

11.1.1 Perímetro de seguridad física

11.1.2 Controles físicos de entrada

11.1.3 Seguridad de oficinas, despachos y recursos

11.1.4 Protección contra las amenazas externas y ambientales

11.1.5 El trabajo en áreas seguras

11.1.6 Áreas de acceso público, carga y descarga

11.2. Seguridad de los equipos

Actividades de control del riesgo

11.2.1 Emplazamiento y protección de equipos

11.2.2 Instalaciones de suministro

11.2.3 Seguridad del cableado

11.2.4 Mantenimiento de los equipos

11.2.5 Salida de activos fuera de las dependencias de la empresa

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones

11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento

11.2.8 Equipo informático de usuario desatendido

11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla

H. Seguridad en la Operativa

12.1. Responsabilidades y procedimientos de operación

Actividades de control del riesgo:

12.1.1 Documentación de procedimientos de operación

12.1.2 Gestión de cambios

12.1.3 Gestión de capacidades

12.1.4 Separación de entornos de desarrollo, prueba y producción

12.2. Protección contra código malicioso

Actividades de control del riesgo:

12.2.1 Controles contra el código malicioso

12.3. Copias de seguridad

Actividades de control del riesgo:

12.3.1 Copias de seguridad de la información

12.4. Registro de actividad y supervisión

Actividades de control del riesgo:

12.4.1 Registro y gestión de eventos de actividad

12.4.2 Protección de los registros de información

12.4.3 Registros de actividad del administrador y operador del sistema

12.4.4 Sincronización de relojes

12.5 Control del software en explotación

Actividades de control del riesgo:

12.5.1 Instalación del software en sistemas en producción

12.6. Gestión de la vulnerabilidad técnica

Actividades de control del riesgo:

12.6.1 Gestión de las vulnerabilidades técnicas

12.6.2 Restricciones en la instalación de software

12.7. Consideraciones de las auditorías de los sistemas de información

Actividades de control del riesgo

12.7.1 Controles de auditoría de los sistemas de información

I. Seguridad en las Telecomunicaciones

13.1. Gestión de la seguridad en las redes

Actividades de control del riesgo

13.1.1 Controles de red

13.1.2 Mecanismos de seguridad asociados a servicios en red

13.1.3 Segregación de redes

13.2. Intercambio de información con partes externas

Actividades de control del riesgo

13.2.1 Políticas y procedimientos de intercambio de información

13.2.2 Acuerdos de intercambio

13.2.3 Mensajería electrónica

13.2.4 Acuerdos de confidencialidad y secreto

J. Adquisición, desarrollo y mantenimiento de los sistemas de información

14.1. Requisitos de seguridad de los sistemas de información

Actividades de control del riesgo

14.1.1 Análisis y especificación de los requisitos de seguridad

14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes pública

14.1.3 Protección de las transacciones por redes telemáticas

14.2. Seguridad en los procesos de desarrollo y soporte

Actividades de control del riesgo

14.2.1 Política de desarrollo seguro de software

14.2.2 Procedimientos de control de cambios en los sistemas

14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

14.2.4 Restricciones a los cambios en los paquetes de software

14.2.5 Uso de principios de ingeniería en protección de sistemas

14.2.6 Seguridad en entornos de desarrollo

14.2.7 Externalización del desarrollo de software

14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas

14.2.9 Pruebas de aceptación

14.3. Datos de prueba

Actividades de control del riesgo

14.3.1 Protección de los datos utilizados en prueba

K. Relaciones con Suministradores

15.1. Seguridad de la información en las relaciones con suministradores

Actividades de control del riesgo:

15.1.1 Política de seguridad de la información para suministradores

15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones

15.2. Gestión de la prestación del servicio por suministradores

Actividades de control del riesgo

15.2.1 Supervisión y revisión de los servicios prestados por terceros

15.2.2 Gestión de cambios en los servicios prestados por terceros

L. Gestión de incidentes en la Seguridad de la información

16.1. Gestión de incidentes de seguridad de la información y mejoras

Actividades de control del riesgo

16.1.1 Responsabilidades y procedimientos

16.1.2 Notificación de los eventos de seguridad de la información

16.1.3 Notificación de puntos débiles de la seguridad

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones

16.1.5 Respuesta a los incidentes de seguridad

16.1.6 Aprendizaje de los incidentes de seguridad de la información

16.1.7 Recopilación de evidencias

M. Aspectos de la Seguridad de la Información en la gestión de la continuidad del negocio

17.1. Continuidad de la seguridad de la información

Actividades de control del riesgo:

17.1.1 Planificación de la continuidad de la seguridad de la información

17.1.2 Implantación de la continuidad de la seguridad de la información

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

17.2. Redundancias

Actividades De Control Del Riesgo

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información

N. Cumplimiento

18.1. Cumplimiento de los requisitos legales y contractuales

Actividades de control del riesgo

18.1.1 Identificación de la legislación aplicable

18.1.2 Derechos de propiedad intelectual (DPI)

18.1.3 Protección de los registros de la organización

18.1.4 Protección de datos y privacidad de la información personal

18.1.5 Regulación de los controles criptográficos

18.2. Revisiones de la seguridad de la información

Actividades de control del riesgo

18.2.1 Revisión independiente de la seguridad de la información

18.2.2 Cumplimiento de las políticas y normas de seguridad:

18.2.3 Comprobación del cumplimiento

4.2.4.- ISO/IEC 27003:2010 (ISO, ISO/IEC 27003:2010(en), 2015)

El propósito de esta Norma Internacional es proporcionar orientación práctica en el desarrollo del plan de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de una organización, de acuerdo con la norma ISO / IEC 27001: 2005. La aplicación real de un SGSI es generalmente ejecutada como proyecto.

El proceso descrito en esta norma internacional ha sido diseñado para proporcionar apoyo a la implementación de la norma ISO / IEC 27001: 2005; (partes relevantes de las cláusulas 4, 5, y 7 inclusive) y el documento:

- la preparación de comenzar un plan de implementación de SGSI en una organización, la definición de la estructura organizativa para el proyecto, y la obtención de la aprobación de la gestión,
- las actividades críticas para el proyecto SGSI y,
- ejemplo para alcanzar los requisitos de la norma ISO / IEC 27001: 2005.

Mediante el uso de esta norma la organización será capaz de desarrollar un proceso de gestión de seguridad de la información, dando a las partes interesadas la seguridad de que los riesgos para los activos de información mantienen ininterrumpidamente dentro de los límites de seguridad de información aceptables según la definición de la organización.

Esta Norma Internacional no cubre las actividades operacionales y otras actividades SGSI, pero cubre los conceptos sobre cómo diseñar las actividades que se traducirá después comienzan las operaciones de SGSI. Los resultados de concepto en el plan de implementación del proyecto SGSI finales. La ejecución real de la parte específica de la organización de un proyecto de SGSI está fuera del alcance de esta Norma Internacional.

La ejecución del proyecto de SGSI debe llevarse a cabo utilizando metodologías de gestión de proyectos estándar.

4.2.4.1.- Alcance

Esta Norma Internacional se centra en los aspectos críticos necesarios para el éxito del diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con la norma ISO / IEC 27001: 2005. En él se describe el proceso de especificación y diseño SGSI desde su inicio hasta la producción de los planes de ejecución. En él se describe el proceso de obtener la aprobación de la gerencia para implementar un SGSI, define un proyecto de implantación de un SGSI, y proporciona orientación sobre cómo planificar el proyecto SGSI, dando lugar a un proyecto final SGSI plan de implementación.

Esta Norma Internacional está destinada a ser utilizado por las organizaciones ejecutoras un SGSI. Es aplicable a todos los tipos de organización (por ejemplo, las empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) de todos los tamaños. Complejidad y riesgos de cada organización son únicos, y sus requisitos específicos impulsarán la implantación del SGSI. Las organizaciones más pequeñas se encuentran que las actividades señaladas en esta norma son aplicables a ellos y se pueden simplificar. A gran escala o de organizaciones complejas podrían encontrar que es necesario un sistema de organización o gestión de capas para gestionar las actividades en esta norma internacional efectiva. Sin embargo, en ambos casos, las actividades pertinentes pueden planificarse mediante la aplicación de esta norma internacional.

Esta Norma Internacional proporciona recomendaciones y explicaciones; no especifica los requisitos. Esta Norma Internacional está destinado a ser utilizado en conjunción con la norma ISO / IEC 27001: 2005 y la ISO / IEC 27002: 2005, pero no tiene la intención de modificar y / o reducir los requisitos especificados en la norma ISO / IEC 27001: 2005 o las recomendaciones de ISO / IEC 27002: 2005. Reivindicación de la conformidad con esta Norma Internacional no es apropiada.

4.2.5.- ISO/IEC 27005:2011 (ISO, ISO/IEC 27005:2011(en), 2015)

Esta Norma Internacional proporciona directrices para la gestión de riesgos de seguridad de información en una organización, apoyando en particular las exigencias de una gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO / IEC 27001. Sin embargo, esta Norma Internacional no proporciona ningún método específico para la información de gestión de riesgos de seguridad. Corresponde a la organización para definir su enfoque de gestión de riesgos, en función, por ejemplo, sobre el alcance del SGSI, el contexto de la gestión de riesgos, o sector de la industria. Una serie de metodologías existentes se puede utilizar bajo el marco descrito en esta norma internacional para implementar los requisitos de un SGSI.

Esta Norma Internacional es relevante para los gerentes y el personal de que se trate con la gestión de riesgos de seguridad de información dentro de una

organización y, en su caso, las partes externas de apoyo a este tipo de actividades.

4.2.5.1.- Alcance

Esta Norma Internacional proporciona directrices para la gestión de riesgos de seguridad de la información.

Esta norma es compatible con los conceptos generales especificados en la norma ISO / IEC 27001 y está diseñado para ayudar a la ejecución satisfactoria de seguridad de la información basado en un enfoque de gestión de riesgos.

El conocimiento de los conceptos, modelos, procesos y terminologías que se describen en la norma ISO / IEC 27001 y la ISO / IEC 27002 es importante para una comprensión completa de esta Norma Internacional.

Esta Norma Internacional es aplicable a todo tipo de organizaciones (por ejemplo, las empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro), que tienen la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización.

4.2.6.- **COBIT 5** (INSTITUTE, 2012)

COBIT 5 provee un marco de referencia para asistir a las empresas y organizaciones a que alcancen sus objetivos de negocio y entregar valor a través de un gobierno eficiente y una buena gestión de sus tecnologías de información. Con esto las empresas se aseguran de que están entregando valor y obteniendo confianza de la información y sus sistemas, afrontando los retos a los que se enfrentan en la actualidad.

COBIT 5 tiene una perspectiva de negocio, no solo de TI. Este es el principal cambio frente a sus anteriores ediciones. Este framework puede ser usado por cualquier usuario de cualquier área de la empresa. Asimismo, puede ser tomado como referencia por cualquier stakeholder que tenga la organización.

COBIT 5 está basado en cinco principios clave:

Principio 1: Satisfacer las necesidades de los Stakeholders

Las empresas existen para crear valor a sus Stakeholders. Esto se logra manteniendo un balance entre los objetivos de negocio, la optimización de los riesgos que puedan existir y el uso de recursos dentro de la organización. COBIT 5 provee todos los procesos requeridos y otros habilitadores para dar

soporte a la creación de valor a través del uso de las tecnologías de información.

Principio 2: Cubrir la organización de principio a fin

COBIT 5 cubre todas las funciones y procesos dentro de la empresa. No solo se enfoca en la parte de TI, sino que trata a la información y a la tecnología como activos que necesitan ser tratados como otro cualquier activo dentro de la empresa.

Principio 3: Aplicar un único marco de trabajo integrado

Hay varios estándares relacionados a las tecnologías de información y sus buenas prácticas. COBIT 5 se alinea con estos estándares y frameworks en un alto nivel y puede ser utilizado como un marco contenedor de todos estos.

Principio 4: Aproximación holística

COBIT 5 define un conjunto de habilitadores para dar soporte a la implementación de un gobierno y una gestión comprensiva de TI. Estos habilitadores son definidos como cualquier cosa que pueda ayudar a alcanzar los objetivos de negocio de la organización.

Principio 5: Separar "Gestión" de "Gobierno"

COBIT 5 hace una clara distinción entre gobierno y gestión. Estas dos disciplinas tienen diferentes tipos de actividades, requieren distintas estructuras organizacionales y sirven para diferentes propósitos

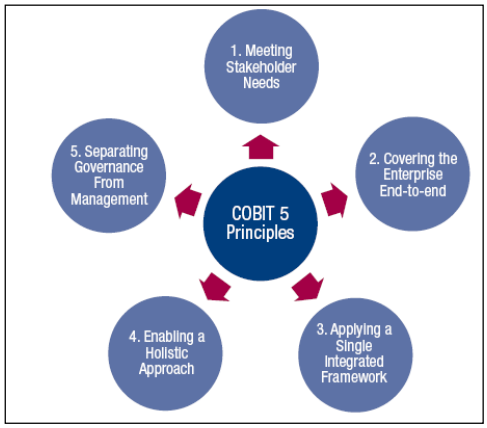


Figura Nº 06: Los 5 principios del marco COBIT 5

Fuente: (INSTITUTE, 2012)

Asimismo, COBIT 5 nos define siete categorías de habilitadores:

1.- Principios, políticas y marcos de trabajo son el medio para trasladar el comportamiento deseado a una guía práctica para la conducir la gestión del día-a-día.

2.- Procesos constituyen un conjunto organizado de prácticas y actividades para producir los outputs respectivos para alcanzar las metas de TI

3.-Estructura organizacional son las entidades que toman las decisiones críticas en la organización

4.- Cultura, ética y comportamiento de los individuos y de la empresa son muy frecuentemente sobrestimados como un factor de éxito de los objetivos de gobierno y gestión establecidos.

5.-La Información está en todos los ámbitos de la organización. Es requerida para mantener a la organización andando y bien gestionada. Asimismo, en un nivel operacional, la información es pieza clave.

6.-Servicios, infraestructura y aplicaciones dan soporte a los procesos y servicios de TI

7.-Personas, habilidades y competencias están conectadas a las personas. Son requeridas para tomar decisiones correctas y tomar acciones correctivas adecuadas.

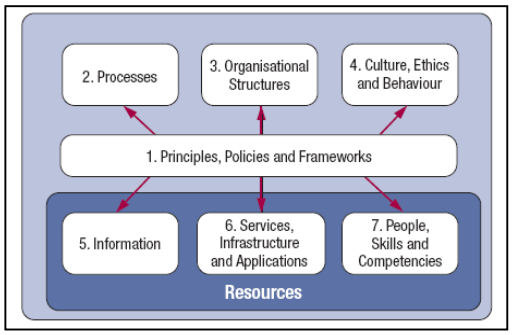


Figura Nº 07: Los siete principios del marco COBIT 5

Fuente: (INSTITUTE, 2012)

Finalmente, COBIT 5 nos introduce una cascada de objetivos la cual permite definir las prioridades para la implementación, mejora y aseguramiento del gobierno de TI basada en los objetivos de negocio de la organización y el posible riesgo al que este expuesta. Principalmente, la cascada de objetivos:

- Define los objetivos más relevantes y tangibles en varios niveles de responsabilidad.

- Permite extraer la información más relevante del conocimiento base de COBIT 5 para su inclusión en proyectos específicos.

- Identifica y comunica claramente como los habilitadores son importantes para alcanzar los objetivos organizacionales.

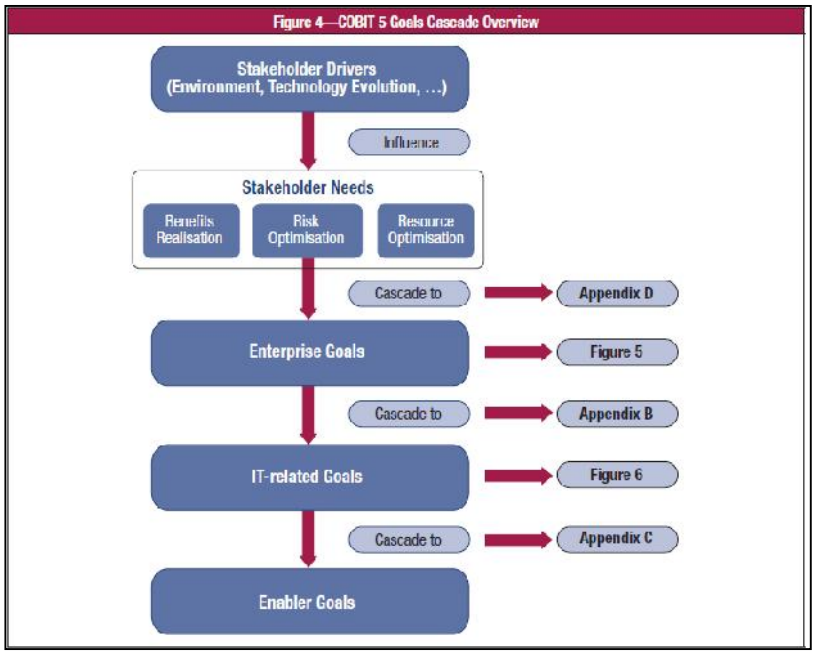


Figura Nº 08: La cascada de objetivos de COBIT 5

Fuente: (INSTITUTE, 2012)

4.2.7.- Cuadro de Mando integral

(Sinnexus, 2016)

El Cuadro de Mando Integral (CMI), también conocido como Balanced Scorecard (BSC) o dashboard, es una herramienta de control empresarial que permite establecer y monitorizar los objetivos de una empresa y de sus diferentes áreas o unidades.

También se puede considerar como una aplicación que ayuda a una compañía a expresar los objetivos e iniciativas necesarias para cumplir con su estrategia, mostrando de forma continuada cuándo la empresa y los empleados alcanzan los resultados definidos en su plan estratégico.

4.2.7.1.- Tipos de cuadro de mando

El Cuadro de Mando Operativo (CMO), es una herramienta de control enfocada al seguimiento de variables operativas, es decir, variables pertenecientes a áreas o departamentos específicos de la empresa. La periodicidad de los CMO puede ser diaria, semanal o mensual, y está centrada en indicadores que generalmente representan procesos, por lo que su implantación y puesta en marcha es más sencilla y rápida. Un CMO debería estar siempre ligado a un DSS (Sistema de Soporte a Decisiones) para indagar en profundidad sobre los datos.

El Cuadro de Mando Integral (CMI), por el contrario, representa la ejecución de la estrategia de una compañía desde el punto de vista de la Dirección General (lo que hace que ésta deba estar plenamente involucrada en todas sus fases, desde la definición a la implantación). Existen diferentes tipos de cuadros de mando integral, si bien los más utilizados son los que se basan en la metodología de Kaplan & Norton. Las principales características de esta metodología son que utilizan tanto indicadores financieros como no financieros, y que los objetivos estratégicos se organizan en cuatro áreas o perspectivas: financiera, cliente, interna y aprendizaje/crecimiento.

- **La perspectiva financiera** incorpora la visión de los accionistas y mide la creación de valor de la empresa. Responde a la pregunta: ¿Qué indicadores tienen que ir bien para que los esfuerzos de la empresa

realmente se transformen en valor? Esta perspectiva valora uno de los objetivos más relevantes de organizaciones con ánimo de lucro, que es, precisamente, crear valor para la sociedad.

- La **perspectiva del cliente** refleja el posicionamiento de la empresa en el mercado o, más concretamente, en los segmentos de mercado donde quiere competir. Por ejemplo, si una empresa sigue una estrategia de costes es muy posible que la clave de su éxito dependa de una cuota de mercado alta y unos precios más bajos que la competencia. Dos indicadores que reflejan este posicionamiento son la cuota de mercado y un índice que compare los precios de la empresa con los de la competencia.

- La **perspectiva interna** recoge indicadores de procesos internos que son críticos para el posicionamiento en el mercado y para llevar la estrategia a buen puerto. En el caso de la empresa que compite en coste, posiblemente los indicadores de productividad, calidad e innovación de procesos sean importantes. El éxito en estas dimensiones no sólo afecta a la perspectiva interna, sino también a la financiera, por el impacto que tienen sobre las rúbricas de gasto.

- La **perspectiva de aprendizaje y crecimiento** es la última que se plantea en este modelo de CMI. Para cualquier estrategia, los recursos materiales y las personas son la clave del éxito. Pero sin un modelo de negocio apropiado, muchas veces es difícil apreciar la importancia de invertir, y en épocas de crisis lo primero que se recorta es precisamente la fuente primaria de creación de valor: se recortan inversiones en la mejora y el desarrollo de los recursos.

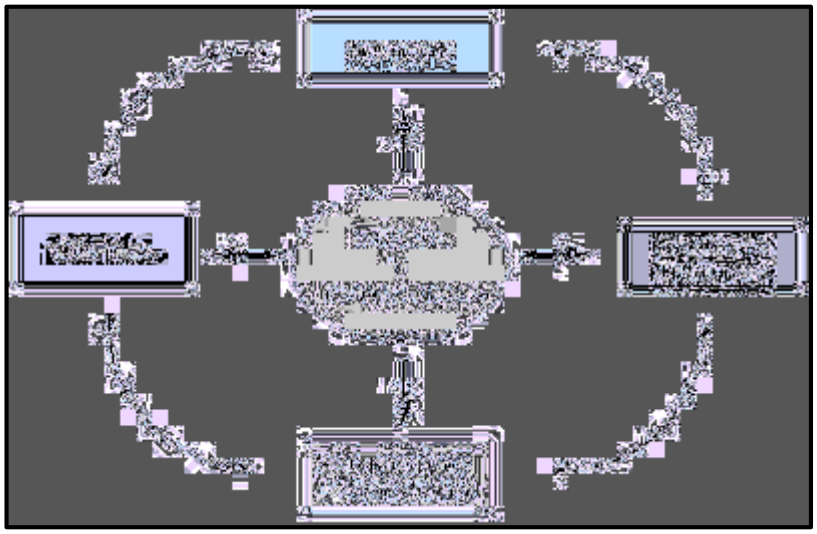


Figura Nº 09: Perspectivas del Cuadro de mando integral

Fuente: (Sinnexus, 2016)

Una vez que se tienen claros los objetivos de cada perspectiva, es necesario definir los indicadores que se utilizan para realizar su seguimiento. Para ello, debemos tener en cuenta varios criterios: el primero es que el número de indicadores no supere los siete por perspectiva, y si son menos, mejor. La razón es que demasiados indicadores difuminan el mensaje que comunica el CMI y, como resultado, los esfuerzos se dispersan intentando perseguir demasiados objetivos al mismo tiempo. Puede ser recomendable durante el diseño empezar con una lista más extensa de indicadores. Pero es necesario un proceso de síntesis para disponer de toda la fuerza de esta herramienta.

No obstante, la aportación que ha convertido al CMI en una de las herramientas más significativas de los últimos años es que se cimenta en un modelo de negocio. El éxito de su implantación radica en que el equipo de dirección se involucre y dedique tiempo al desarrollo de su propio modelo de negocio.

4.2.7.2.- Beneficios de la implantación de un Cuadro de Mando Integral

- La fuerza de explicitar un modelo de negocio y traducirlo en indicadores facilita el consenso en toda la empresa, no sólo de la dirección, sino también de cómo alcanzarlo.

- Clarifica cómo las acciones del día a día afectan no sólo al corto plazo, sino también al largo plazo.
- Una vez el CMI está en marcha, se puede utilizar para comunicar los planes de la empresa, aunar los esfuerzos en una sola dirección y evitar la dispersión. En este caso, el CMI actúa como un sistema de control por excepción.
- Permita detectar de forma automática desviaciones en el plan estratégico u operativo, e incluso indagar en los datos operativos de la compañía hasta descubrir la causa original que dio lugar a esas desviaciones.

4.2.7.3.- Riesgos de la implantación de un Cuadro de Mando Integral

- Un modelo poco elaborado y sin la colaboración de la dirección es papel mojado, y el esfuerzo será en vano.
- Si los indicadores no se escogen con cuidado, el CMI pierde una buena parte de sus virtudes, porque no comunica el mensaje que se quiere transmitir.
- Cuando la estrategia de la empresa está todavía en evolución, es contraproducente que el CMI se utilice como un sistema de control clásico y por excepción, en lugar de usarlo como una herramienta de aprendizaje.
- Existe el riesgo de que lo mejor sea enemigo de lo bueno, de que el CMI sea perfecto, pero desfasado e inútil.

4.3.-Conceptos y Definiciones

4.3.1.- Aceptación del riesgo (Aliaga Flores, 2013)
Decisión de aceptar el riesgo.

4.3.2.- Activo (Aliaga Flores, 2013)
Cualquier elemento o información, tenga o no valor contable para la organización.

4.3.3.- Activo de información (Fernández & Piattini, 2003)
Los activos son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, necesarios para que la organización funcione y alcance los objetivos que propone su dirección.

4.3.4.- Amenaza (Aliaga Flores, 2013)

Una causa potencial de un incidente no-deseado, el cual puede resultar dañando a un sistema.

4.3.5.- Análisis de riesgo (Aliaga Flores, 2013)

Uso sistemático de la información para identificar fuentes y para estimar el riesgo. Identifica los activos a proteger o evaluar.

4.3.6.-Confidencialidad (Fernández & Piattini, 2003)

La propiedad que información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

4.3.7.- Control (Aliaga Flores, 2013)

Medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

4.3.8.- Declaración de aplicabilidad (Excellence, 2015)

La declaración de aplicabilidad es uno de los tantos documentos que tienen que ser redactados por exigencia de la norma ISO27001.

Se trata de una declaración de aplicabilidad documentada que detalla los objetivos de control aplicables al Sistema de Gestión de Seguridad de la Información (SGSI). Estos objetivos se basan en el rendimiento de los medios de valoración y tratamiento de los riesgos, responsabilidades contractuales y requisitos legales o del negocio de la empresa para la seguridad de la información.

4.3.9.-Disponibilidad (Aliaga Flores, 2013)

La propiedad tiene que estar disponible y utilizable cuando lo requiera una entidad autorizada.

4.3.10.- Entregable (Wikipedia, Entregable, 2015)

El término entregable es utilizado en la gestión de proyectos para describir un objeto, tangible o intangible, como resultado del proyecto, destinado a un cliente, ya sea interno o externo a la organización. Un entregable puede ser

un reporte, un documento, un paquete de trabajo, una actualización de servidor o cualquier otro bloque de construcción resultado del proyecto en su totalidad.

4.3.11.- Evaluación del riesgo (Aliaga Flores, 2013)
Proceso de comparar el nivel de riesgo estimado durante el proceso de análisis de riesgo con un criterio dado para determinar la importancia del riesgo.

4.3.12.- Gestión del riesgo (Aliaga Flores, 2013)
Actividades coordinadas para dirigir y controlar una organización con relación al riesgo. Normalmente incluye la evaluación, tratamiento, aceptación y comunicación del riesgo. Estas actividades se enfocan a manejar la incertidumbre relativa de las amenazas detectadas.

4.3.13.- Gobierno de TI (Aliaga Flores, 2013)
El gobierno de TI es parte integral del gobierno corporativo heredando todas sus características generales. Es una estructura de relaciones y proceso que brinda dirección a la empresa con el fin de alcanzar los objetivos de negocio con una adecuada implementación de los procesos de TI en su interior, generando valor a través de TI, logrando gestionar adecuadamente los riesgos de TI.

4.3.14.- Información (Aliaga Flores, 2013)
Es un activo esencial para el negocio de una organización. Puede existir de muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación.

4.3.15.- Integridad (Aliaga Flores, 2013)
La propiedad de guardar la exactitud e integridad de los activos.

4.3.16.- Política (Aliaga Flores, 2013)
Intención y dirección general expresada formalmente por la gerencia.

4.3.17.- Proyecto de SGSI (Aliaga Flores, 2013)
Actividades estructuradas llevadas a cabo por la organización con el fin de implementar un SGSI.

4.3.18.- Riesgo residual (Aliaga Flores, 2013)

El riesgo remanente después del tratamiento del riesgo.

4.3.19.- Riesgo (Aliaga Flores, 2013)

Es la combinación de la probabilidad de un evento y su ocurrencia.

4.3.20.- Seguridad de Información (Fernández & Piattini, 2003)

Es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. Se logra implementando un adecuado conjunto de controles incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

4.3.21.- Tratamiento del riesgo (Aliaga Flores, 2013)

Proceso de tratamiento de la selección e implementación de controles para modificar el riesgo.

4.3.22.- Vulnerabilidad (Aliaga Flores, 2013)

La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

CAPÍTULO V: DESARROLLO DE LA PROPUESTA

5.1. Inicio del Proyecto

Al comenzar el desarrollo de un proyecto es importante el compromiso de la dirección y determinar sobre qué objetivos se está partiendo. En la figura Nº10 se ilustra el contenido de este tema:

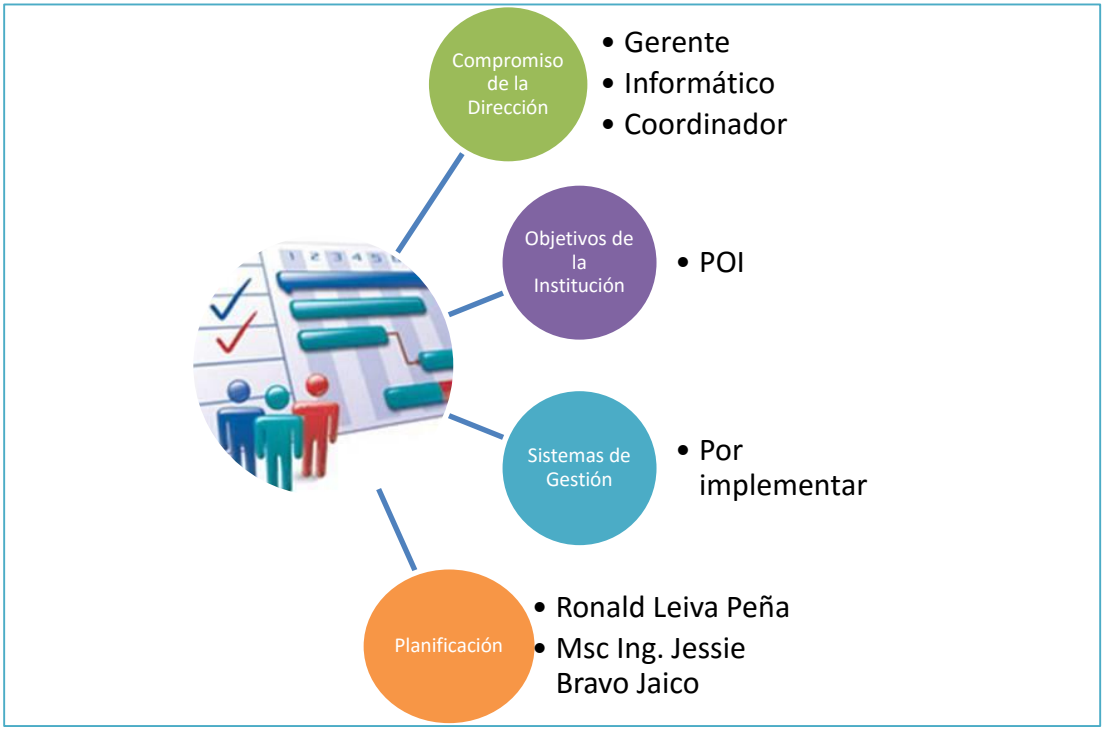


Figura Nº 10: Inicio del Proyecto

Fuente: Elaboración propia

5.1.1. Compromiso de la Dirección

Para el desarrollo del presente Proyecto del diseño de un Sistema de Gestión de Seguridad de la Información en la Red de Servicios de Salud de Lambayeque se presentó el proyecto a la gerente de la Red para su evaluación y aprobación. Posteriormente se obtuvo la aprobación y el respaldo tanto del Responsable de Informática del Sistema SISMED que es utilizado en uno de sus procesos principales, además del Coordinador del SISMED a cargo, ya que el desarrollo de un SGSI implica que todos los trabajadores estén involucrados con la cultura de seguridad de la información.

5.1.2. Objetivos de negocio de la Institución

- OE1. Reducir la mortalidad materna y Neonatal, con enfoque de interculturalidad en la población más vulnerable.
- OE 2. Reducir la morbilidad por IRAS en niños menores de 5 años.
- OE 3. Disminuir la Tasa de incidencia de TBC.
- OE 4. Disminuir la Morbimortalidad por Cáncer.
- OE5.Reducir la Desnutrición crónica infantil y otros desordenes nutricionales.
- OE6. Prevención de ITS-VIH/SIDA.
- OE7.Disminuir la Tasa de Incidencia de enfermedades no transmisibles/enfermedades hipertensivas, diabetes, salud ocular, salud mental y salud bucal.
- OE 8. Reducir la Tasa de incidencia de las EDAS.
- OE 9. Disminuir la Tasa de incidencia por Dengue, malaria, peste, leshmaniasis y rabia.
- OE10.Reducir la vulnerabilidad ante peligros naturales frente a emergencias y desastres.
- OE11 Incrementar el acceso a los servicios de salud (cobertura SIS, Débil Sistema de Referencia y Contra referencia).

5.1.3. Sistemas de Gestión existentes

Actualmente no tiene implementado ningún sistema de gestión.

5.1.4. Planificación

Responsables:

- Msc. Ing. Jessie Bravo Jaico.
- Bach. Ronald Leiva Peña.

5.2. Establecer el SGSI

5.2.1. Alcance del SGSI

El Sistema de Gestión de Seguridad de Información de la Red de Salud de Lambayeque abarcara las áreas de Informática, SISMED, Almacén y de las Estrategias Sanitarias, dirigido a los Jefes de dichas áreas y sus coordinadores.

Según los procesos y servicios el SGSI se limitará al proceso de suministro de medicamentos de la Red de Salud de Lambayeque definido en el título del proyecto.

En la siguiente figura Nº 11 se observa las áreas que corresponden al alcance del sistema de gestión de seguridad de la información:

Figura Nº 11: Alcance del SGSI

Fuente: Elaboración propia

5.2.2. Política de Seguridad

5.2.2.1. Generalidades

La información es un recurso muy importante como activo de información para la Red de Salud de Lambayeque, por lo tanto, debe ser protegido adecuadamente.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de seguridad de la información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas., con el fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la misma. Es importante que los principios de la Política de Seguridad sean parte de la cultura de la Red de Salud de Lambayeque. Para esto, se debe asegurar un compromiso

manifiesto con la gerencia dela Red de Salud de Lambayeque para la difusión, consolidación y cumplimiento de la presente Política.

5.2.2.2. Objetivo principal

Fijar las directrices generales que orientan la seguridad de la información en la Red de Salud de Lambayeque, reflejando el compromiso, apoyo, interés, fomento y desarrollo de una cultura de seguridad de la información en la Institución.

5.2.2.3. Objetivo secundario

- Proteger los recursos de información y tecnología de la Red de Salud de Lambayeque utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
- Mantener la Política de Seguridad de la Red de Salud de Lambayeque actualizada, a efectos de asegurar su vigencia y nivel de eficacia a lo largo de su aplicación.

5.3. Diseño del SGSI

Para el diseño del SGSI se desarrolló en 6 etapas, que describen desde que procesos se ha trabajado hasta finalmente concluir en un documento llamado declaración de aplicabilidad, las cuales ilustran en la siguiente figura:

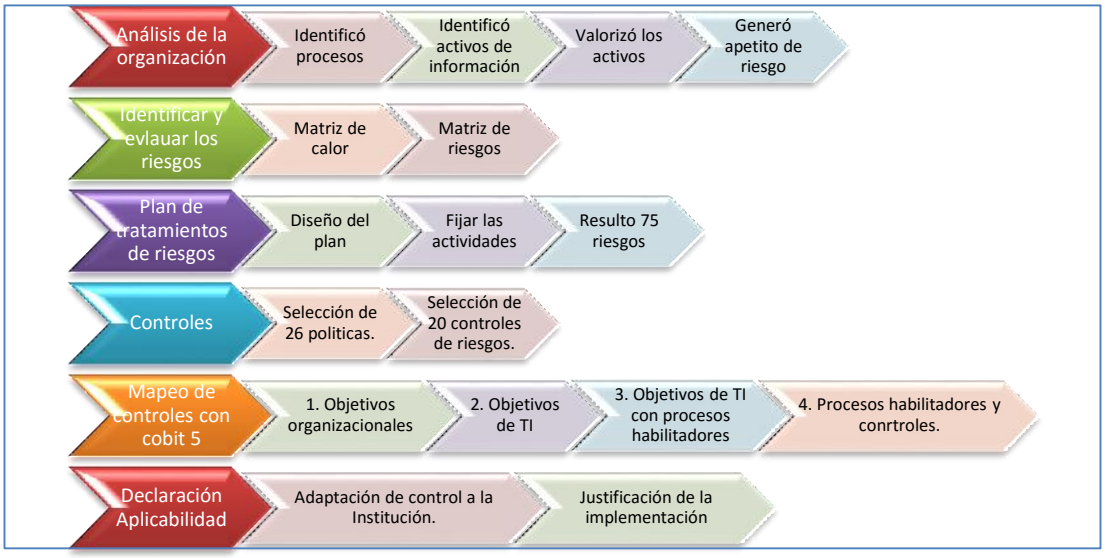


Figura Nº 12: Diseño del SGSI

Fuente: Elaboración propia

5.3.1. Análisis de la Organización

5.3.1.1. Identificación de los procesos de la Institución

Se desarrollará el proceso principal de la Institución, para lo cual se modelará siguiendo la notación BPMN 2.0 (Business Process Modeling Notation) la cual es una notación gráfica estandarizada que permite observar de manera detallada todo el flujo de trabajo que siguen dichos procesos.

A. Proceso de Suministro de Medicamentos:

El proceso de suministro de medicamentos se divide a su vez en:

- **Gestionar compra**

  - ✓ **Objetivo:**

    Registrar entrada de medicamentos al Almacén especializado.

- ✓ **Descripción:**

1.- Coordinador del área de medicamentos envía un informe de requerimientos al Almacenero General.

2.- Almacenero General de medicamentos recibe el informe y lo evalúa.

3.- Almacenero General consulta si hay stock de medicamentos en el almacén.

4.- El Almacenero General envía un informe de los medicamentos al Jefe del área de medicamentos en Lima.

5.- El jefe principal recibe el informe del Almacenero General.

6.- Jefe del área de medicamentos de Lima somete a licitación a los proveedores.

7.- Si el Proveedor cumple con los requisitos establecidos en la licitación se le envía el pedido.

8.- Los proveedores revisan el pedido solicitado por el Jefe del área de medicamentos en Lima.

9.-Proveedores envían cotizaciones al Jefe del área de medicamentos de Lima.

10.- Jefe del área de medicamentos de Lima revisa las cotizaciones enviadas por los proveedores.

11.- El Jefe del área de medicamentos de Lima selecciona al proveedor y lo Registra.

12.- El Jefe del área de medicamentos de Lima confirma pedido al Proveedor.

13.- El proveedor Elabora una orden de compra.

14.- El proveedor envía al Jefe del área de Logística los productos solicitados en Armadas.

15.- EL jefe del área de Logística recibe la mercadería del proveedor.

16.- El jefe del área de Logística envía reporte de los medicamentos comprados.

17.-El almacenero general registra la información de la compra.

- ✓ **Responsable del Proceso.**

  Almacenero General

- ✓ **Definiciones**

  No aplica

- ✓ **Diagrama del Proceso**

  Ver anexo 1.1

- **Distribución de Medicamentos.**

  - ✓ **Objetivo:**

  Distribución de medicamentos e insumos a través de los responsables de farmacia.

  - ✓ **Descripción del proceso:**

  1.- El responsable de Farmacia solicita a responsable de Sub Almacén medicamentos a llevar.

  2.- Responsable de Farmacia, cuenta y verifica las cantidades recibidas; si es conforme:

  2.1.- Responsable de Sub Almacén selecciona material de embalaje y coloca productos en cajas según tipo de envase. Firma guía de remisión.

  2.2.- Sino es conforme: Toma las acciones necesarias para los cambios de productos o devolución, repone diferencia o repone dañados y comunica al Químico Farmacéutico.

  3.- Responsable de Farmacia firma su guía de Remisión.

  4.- Responsable de Sub Almacén entrega cargo de la guía de remisión a Coordinador del SISMED, emite su reporte y actualiza en el TCV (Tarjeta de Control visible).

5.- Coordinador del SISMED verifica la conformidad de la Guía de Remisión.

6.- Responsable de Sub Almacén archiva la Guía de Remisión.

7.- Fin

✓ **Responsable del Proceso.**

- Responsable de Farmacia
- Responsable de Sub Almacén
- Coordinador del SISMED

✓ **Definiciones**

TCV.- Llamado tarjeta de control visible, donde se ingresa los medicamentos e insumos que salieron de almacén, las salidas, el stock, fecha de entrega, número de la guía de remisión, y por supuesto el nombre del insumo o medicamento.

SISMED.- Sistema Integrado de Suministros de Medicamentos e Insumos Médicos – Quirúrgicos, Sistema que busca incrementar el acceso a medicamentos a la población.

✓ **Diagrama del Proceso**

Ver anexo 1.2

- **Gestionar control de calidad de medicamentos.**

✓ **Objetivo:**

Realizar el control de calidad el ingreso y salidas de medicamentos de cada Puesto de Salud.

✓ **Descripción del Proceso:**

1.- EL representante de farmacia de cada Puesto de Salud entrega un informe de los ingresos y salidas de medicamentos en un formato ICI, anexando el formato IME y el porcentaje de disponibilidad al Coordinador del área de medicamentos.

2.- El Coordinador recibe el informe y evalúa si los datos son correctos, conforme a sus guías de remisión de cada puesto de salud.

3.- El Coordinador realiza el control de calidad de la información verificando en el sistema SISMED si esta todo conforme.

4.- El Coordinador verifica la Disponibilidad de medicamentos del puesto de salud en el Sistema SISMED

4.1.- Adicionalmente el representante de cada Puesto de Salud pasa por cada una de la Estrategias Sanitarias para que sea revisado su informe y proyectar cuanto de medicamentos necesitaría por estrategia para los próximos 3 meses, según su consumo promedio mensual.

5.- El Coordinador recepciona informes, firma cargos al responsable de farmacia.

- ✓ **Responsable del Proceso.**

Coordinador de SISMED.

- ✓ **Definiciones**

ICI.-Informe de consumo integrado, presentado por los responsables de farmacia de los establecimientos de salud hacia el coordinador de Sismed cada mes, donde se detalla ingresos, egresos de medicamentos.
IME.-Informe de movimiento económico, presentado por los responsables de farmacia de los establecimientos de salud hacia el coordinador del Sismed cada mes.
Porcentaje de Disponibilidad. - Documento que contiene información sobre stock de medicamentos e insumos de los últimos 3 meses, además del consumo promedio mensual por cada uno.

- ✓ **Diagrama del Proceso**

Ver anexo 1.3

5.3.1.2. Identificación de los Activos de Información

En este punto se identificarán los activos que están envueltos en cada proceso descrito anteriormente. Según el estándar ISO 27005, se pueden identificar dos tipos de activos: los primarios y los de soporte. Los primarios, según este estándar, son los procesos e información más sensibles para la organización. Los activos de soporte, son los activos que dan el debido soporte a estos activos primarios. (Aliaga Flores, 2013)

Dentro de estas dos agrupaciones, se definieron siete distintos tipos específicos de activos:

1) **Dato:** Es toda aquella información que se genera, envía, recibe y gestionan dentro de la organización. Dentro de este tipo, podemos encontrar distintos documentos que la Red de Salud de Lambayeque gestiona dentro de sus procesos.

2) **Aplicación:** Todo aquel software que se utilice como soporte en los procesos.

3) **Personal:** Son todos los actores que se ven involucrados en el acceso y el manejo de una u otra manera a los activos de información de la organización.

4) **Servicio:** Son los servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.

5) **Tecnología:** Es todo el hardware donde se maneje la información y las comunicaciones.

6) **Instalación:** Es cualquier lugar donde se alojan los activos de información. Este lugar o ambiente puede estar ubicado dentro de la organización tanto como fuera de la misma.

7) **Equipamiento auxiliar:** Son los activos que no se hallan definidos en ninguno de los anteriores tipos.

Los activos identificados en la Red de Salud de Lambayeque, según el alcance del SGSI se puede observar en la Tabla N° 01 a continuación:

Id	Activo	Tangible	Tipo de activo
1	Computadora de escritorio.	SI	Tecnología
2	Licencia de Microsoft Windows 7.	NO	Aplicación
3	Licencia de Microsoft Office 2013.	NO	Aplicación
4	Página web del MINSA.	NO	Aplicación
5	Antivirus.	NO	Aplicación
6	Email (para el envío electrónico de información).	NO	Aplicación
7	Teléfono.	SI	Tecnología
8	Impresora.	SI	Tecnología
9	Fotocopiadora.	SI	Tecnología
10	Scanner.	SI	Tecnología
11	Cableado Ethernet.	SI	Tecnología
12	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas).	NO	Aplicación
13	Firewall de Windows.	NO	Aplicación
14	SISMED.	NO	Aplicación
15	Archivadores para los documentos.	SI	Equipamiento Auxiliar
16	Archivos del SISMED.	SI	Instalación
17	Llaves de ingreso.	SI	Equipamiento Auxiliar
18	Stakeholder interno: Gerente de la Red de Salud de Lambayeque.	SI	Personal
19	Stakeholder externo: Gerencia Regional de Salud.	SI	Personal
20	Stakeholder externo: Almacén Especializado de la Geresa	SI	Personal
21	Coordinadora de TBC, etapa vida adulto, etapa vida niño.	SI	Personal
22	Coordinador de metaxénicas, salud ambiental, zoonosis, salud ocupacional y metales pesados..	SI	Personal

23	Coordinadora de Salud mental, discapacidad, adulto mayor.	SI	Personal
24	Coordinadora de ESSRR y referencia y contra referencia.	SI	Personal
25	Coordinadora de ESANS.	SI	Personal
26	Coordinador de Niño e Inmunizaciones.	SI	Personal
27	Coordinadora de Promoción de la Salud y atención itinerante.	SI	Personal
28	Coordinadora de E.S daños no transmisibles/HTA-Diabetes y Programa de Prevención y control de cáncer, salud ocular y prevención de la ceguera.	SI	Personal
29	Coordinadora de VIH/Sida, etapa vida adolescente	SI	Personal
30	Coordinadora Epidemiología, Salud Familiar Comunitaria.	SI	Personal
31	Coordinador de SISMED	SI	Personal
32	Coordinador Salud Bucal y Salud Escolar	SI	Personal
33	Responsable Logística, almacén de medicamentos.	SI	Personal
34	Responsable CSI, Portal Institucional, Informático del SISMED	SI	Personal
35	Formato de Consumo Integrado(ICI)	SI	Dato
36	Guías de Remisión de abastecimiento	SI	Dato
37	Movimiento Biológico o de vacunas	SI	Dato
38	Formato de Movimiento Económico(IME)	SI	Dato
39	Voucher de vacunas(depósito del banco)	SI	Dato
40	Formato de Requerimientos	SI	Dato
41	Informe de porcentaje de disponibilidad	SI	Dato
42	Consulta de envío de información	SI	Dato
43	Consulta de stocks	SI	Dato
44	Consumo promedio mensual y óptimo	SI	Dato
45	Control de Calidad de la información	SI	Dato

46	Medicamentos sin fecha de vencimiento	SI	Dato
47	Medicamentos vencidos en el mes	SI	Dato
48	Medicamentos vencidos por fecha de vencimiento	SI	Dato
49	Plan Operativo Institucional	SI	Dato
50	Informe de monitoreo, supervisión, evaluación y control del Programa Articulado Nutricional	SI	Dato
51	Informe de número de niños con vacunas completos	SI	Dato
52	Informe de número de niños con cred completo	SI	Dato
53	Informe de número de niños con suplemento de hierro Población total de niños programados	SI	Dato
54	Informe de número de casos de infecciones respiratorias agudas(IRAS)	SI	Dato
55	Informe de número de casos de enfermedad diarreica aguda(EDA)	SI	Dato
56	Informe de número de casos de Infecciones respiratorias agudas (IRAS) complicadas.	SI	Dato
57	Informe de número de casos de enfermedad diarreica aguda (EDA) complicada.	SI	Dato
58	Informe de número de atenciones de otras enfermedades prevalentes.	SI	Dato
59	Informe de número de gestantes con suplemento de hierro y ácido fólico.	SI	Dato
60	Informe de número de atención de niños con diagnóstico de parasitosis intestinal.	SI	Dato
61	Informe de número de adolescentes atendidos que acceden a servicios de salud para prevención del embarazo	SI	Dato
62	Informe de número de gestantes con atención prenatal reenfocada.	SI	Dato
63	Informe de número de parejas protegidas que acceden a métodos de Planificación Familiar	SI	Dato

64	Informe de número de sintomáticos respiratorios con despistaje de tuberculosis.	SI	Dato
65	Informe de número de casos de contacto de TBC	SI	Dato
66	Informe de número de casos de diagnóstico de TBC	SI	Dato
67	Informe de número monitoreo, supervisión y control de VIH/SIDA	SI	Dato
68	Informe de número de personas atendidas con infecciones de transmisión sexual	SI	Dato
69	Informe de monitoreo, supervisión, evaluación y control Metaxénicas y Zoonosis	SI	Dato
70	Informe de número de personas con diagnóstico y tratamiento de casos de enfermedades zoonóticas.	SI	Dato
71	Informes de monitoreo, supervisión, evaluación control de enfermedades no transmisibles.	SI	Dato
72	Informe de número de personas con tamizaje y diagnóstico de cataratas.	SI	Dato
73	Informe de número de personas con valoración clínica y laboratorio de enfermedades crónicas no transmisibles	SI	Dato
74	Informe de número de personas tratadas y controladas con Hipertensión Arterial	SI	Dato
75	Informe de número de personas tratadas con diabetes	SI	Dato
76	Informe de número de personas con atención estomatológica preventiva básica	SI	Dato
77	Informe de monitoreo, supervisión, evaluación y control de prevención y control de cáncer	SI	Dato
78	Informe de número de personas con evaluación médica preventiva en cáncer de colon y recto, hígado, leucemia, linfoma, piel y otros.	SI	Dato
79	Informe de monitoreo, supervisión, evaluación y control del programa en salud mental.	SI	Dato

80	Informe de número de niña y/o niño de 8 a 11 años identificado con déficit en sus habilidades sociales.	SI	Dato
81	Informe de número de personas tamizadas con trastornos mentales y problemas psicosociales ejecutados.	SI	Dato
82	Informe de número de personas tratadas con problemas psicosociales.	SI	Dato
83	Informe de número de personas tratadas ambulatoriamente con trastornos afectivos	SI	Dato
84	Informe de número de personas tratadas ambulatoriamente debido al consumo de alcohol.	SI	Dato
85	Informe de número de personas tratadas ambulatoriamente debido al consumo de drogas.	SI	Dato
86	Informe de número de tratamiento ambulatorio de personas con síndrome o trastorno psicótico.	SI	Dato
87	Informe de número de prevención familiar de conductas de riesgo en adolescentes, familias fuertes amor y límites.	SI	Dato
88	Informe de número de personas atendidas en sesiones de entrenamiento en habilidades sociales para adolescentes, jóvenes y adultos.	SI	Dato
89	Informes de número de personas atendidas en sesiones de entrenamiento en habilidades sociales para niños, niñas.	SI	Dato
90	Informe de número de familias con conocimiento de prácticas saludables para prevenir los trastornos mentales y psicosociales.	SI	Dato

Tabla N° 01. Inventario de Activos

Fuente: Elaboración propia

5.3.1.3. Valorización de los activos de información

El siguiente paso a la identificación de los activos que se encuentren comprendidos dentro de los procesos "core" de la Red de Salud de Lambayeque es valorizarlos, y así determinar el valor que cada activo tiene para la organización y el impacto que tendría dentro de la misma si llegara a fallar en algún momento.

Para realizar dicha valorización, se determinó una escala cualitativa ya que no es posible valorar económicamente todos los activos que intervienen dentro de estos procesos.

En la siguiente tabla se muestra cuáles son los criterios que se usaron para realizar la correcta valorización de estos activos, en conjunto con los valores que se tendrán en cuenta para clasificarlos y su respectivo significado dentro del contexto actual:

Criterio	Valor	Descripción
Disponibilidad	0	No Aplica / No es relevante.
	1	Debe estar disponible al menos el 10% del tiempo.
	2	Debe estar disponible al menos el 50% del tiempo.
	3	Debe estar disponible siempre.
Integridad	0	No Aplica / No es relevante.
	1	No son relevantes los errores que tenga o la información faltante.
	2	Tiene que estar correcto y completo al menos en un 50%.
	3	Tiene que estar correcto y completo en un 100%.
Confidencialidad	0	No Aplica / No es relevante.
	1	Daños muy bajos, el incidente no trascendería del área afectada.
	2	Seria relevantes, el incidente implicaría a otras áreas.
	3	Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas.

Tabla Nº 02. Criterios de valorización de activos

Fuente: (Aliaga Flores, 2013)

Para hallar el valor final del activo, se realizará una suma de los valores de los distintos criterios. Esta suma se ubicará en el rango de valores de 0 a 9, para lo cual cada valor representará a un nivel de criticidad. Mientras más alto sea el número final que resulto de la suma, más alta será su criticidad. Para este proyecto, se definieron cuatro niveles de criticidad del activo: no aplica, bajo, medio y alto.

A continuación, la siguiente tabla detalla todos los valores que se puede obtener, asociados a un nivel de criticidad específico:

Valor	Nivel de Criticidad
0	No Aplica
1	Baja
2	Baja
3	Baja
4	Medio
5	Medio
6	Medio
7	Alta
8	Alta
9	Alta

Tabla N° 03. Valores según nivel de criticidad

Fuente: Elaboración Propia

Apetito de Riesgo:

Se definió que los activos cuya criticidad sea “Alta” son los que entrarán dentro de la identificación y análisis de riesgos de los activos de información del siguiente capítulo. Los activos con criticidad “Media” y “Baja” no se toman como activos críticos para la Red de Salud de Lambayeque, por lo tanto no entrarán dentro de dicho análisis.

Luego de haber definido el contexto de la valorización, se procederá a mostrar el total de los activos identificados con el valor respectivo que cada activo tiene dentro de la institución:

ID	ACTIVO	Criterios de valorización			Valor Total	Criticidad
		Integridad	Disponibilidad	Confidencialidad		
1	Computadora de escritorio	3	3	3	9	ALTA
2	Licencia de Microsoft Windows 7	3	3	1	7	ALTA
3	Licencia de Microsoft Office 2013	3	3	1	7	ALTA
4	Página web del MINSA	2	3	2	7	ALTA
5	Antivirus	3	3	2	8	ALTA
6	Email (para el envío electrónico de información)	2	3	2	7	ALTA
7	Teléfono	3	3	0	6	MEDIO
8	Impresora	3	2	0	5	MEDIO
9	Fotocopiadora	3	2	0	5	MEDIO
10	Scanner	3	2	0	5	MEDIO
11	Cableado Ethernet	3	3	2	8	ALTA
12	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	3	2	3	8	ALTA
13	Firewall de Windows	2	3	1	6	MEDIO
14	SISMED	3	3	3	9	ALTA
15	Archivadores para los documentos	2	1	2	5	MEDIO
16	Archivos del SISMED	2	2	2	6	MEDIO
17	Llaves de ingreso	3	3	3	9	ALTA
18	Stakeholder interno: Gerente de la Red de Salud de Lambayeque	3	2	0	5	MEDIO
19	Stakeholder externo: Gerencia Regional de Salud	3	2	0	5	MEDIO
20	Stakeholder externo: Almacén Especializado de la Geresa.	3	2	0	5	MEDIO
21	Coordinadora de TBC, etapa vida adulto, etapa vida niño.	3	2	0	5	MEDIO

22	Coordinador de metaxénicas, salud ambiental, zoonosis, salud ocupacional y metales pesados.	3	2	0	5	MEDIO
23	Coordinadora de Salud mental, discapacidad, adulto mayor.	3	2	0	5	MEDIO
24	Coordinadora de ESSRR y referencia y contra referencia.	3	2	0	5	MEDIO
25	Coordinadora de ESANS	3	2	0	5	MEDIO
26	Coordinador de Niño e Inmunizaciones	3	2	0	5	MEDIO
27	Coordinadora de Promoción de la Salud y atención itinerante.	3	2	0	5	MEDIO
28	Coordinadora de E.S daños no transmisibles/HTA-Diabetes y Programa de Prevención y control de cáncer, salud ocular y prevención de la ceguera.	3	2	0	5	MEDIO
29	Coordinadora de VIH/Sida, etapa vida adolescente	3	2	0	5	MEDIO
30	Coordinadora Epidemiología, Salud Familiar Comunitaria.	3	2	0	5	MEDIO
31	Coordinador de SISMED	3	2	0	5	MEDIO
32	Coordinador Salud Bucal y Salud Escolar	3	2	0	5	MEDIO
33	Responsable Logística, almacén de medicamentos.	3	2	0	5	MEDIO
34	Responsable CSI, Portal Institucional, Informático del SISMED	3	2	0	5	MEDIO
35	Formato de Consumo Integrado(ICI)	3	2	2	7	ALTA
36	Guías de Remisión de abastecimiento	3	2	2	7	ALTA

37	Movimiento Biológico o de vacunas	3	2	2	7	ALTA
38	Formato de Movimiento Económico(IME)	3	2	2	7	ALTA
39	voucher de vacunas(depósito del banco)	3	2	2	7	ALTA
40	Formato de Requerimientos	3	3	2	8	ALTA
41	Informe de porcentaje de disponibilidad	3	2	2	7	ALTA
42	Consulta de envío de información	2	3	3	8	ALTA
43	Consulta de stocks	2	3	3	8	ALTA
44	Consumo promedio mensual y óptimo	2	3	3	8	ALTA
45	Control de Calidad de la información	2	3	3	8	ALTA
46	Medicamentos sin fecha de vencimiento	2	3	3	8	ALTA
47	Medicamentos vencidos en el mes	2	3	3	8	ALTA
48	Medicamentos vencidos por fecha de vencimiento	2	3	3	8	ALTA
49	Plan Operativo Institucional	3	3	1	7	ALTA
50	Informe de monitoreo, supervisión, evaluación y control del Programa Articulado Nutricional	2	1	2	5	MEDIO
51	Informe de número de niños con vacunas completos	3	3	1	7	ALTA
52	Informe de número de niños con cred completo	3	3	1	7	ALTA
53	Informe de número de niños con suplemento de hierro Población total de niños programados	3	3	1	7	ALTA
54	Informe de número de casos de infecciones respiratorias	3	3	1	7	ALTA

	agudas(IRAS)					
55	Informe de número de casos de enfermedad diarreica. aguda(EDA)	3	3	1	7	ALTA
56	Informe de número de casos de Infecciones respiratorias agudas (IRAS) complicadas.	3	3	1	7	ALTA
57	Informe de número de casos de enfermedad diarreica aguda (EDA) complicada.	3	3	1	7	ALTA
58	Informe de número de atenciones de otras enfermedades prevalentes.	2	3	1	6	MEDIO
59	Informe de número de gestantes con suplemento de hierro y ácido fólico.	3	3	1	7	ALTA
60	Informe de número de atención de niños con diagnóstico de parasitosis intestinal.	3	2	1	6	MEDIO
61	Informe de número de adolescentes atendidos que acceden a servicios de salud para prevención del embarazo	3	3	1	7	ALTA
62	Informe de número de gestantes con atención prenatal reenfocada.	2	3	1	6	MEDIO
63	Informe de número de parejas protegidas que acceden a métodos de Planificación Familiar	3	3	1	7	ALTA
64	Informe de número de sintomáticos respiratorios con despistaje de tuberculosis.	3	3	1	7	ALTA
65	Informe de número de casos de contacto de TBC	2	3	1	6	MEDIO

66	Informe de número de casos de diagnóstico de TBC	2	3	1	6	MEDIO
67	Informe de número monitoreo, supervisión y control de VIH/SIDA	3	3	1	7	ALTA
68	Informe de número de personas atendidas con infecciones de transmisión sexual	3	3	1	7	ALTA
69	Informe de monitoreo, supervisión, evaluación y control Metaxénicas y Zoonosis	3	3	1	7	ALTA
70	Informe de número de personas con diagnóstico y tratamiento de casos de enfermedades zoonóticas.	3	3	1	7	ALTA
71	Informes de monitoreo, supervisión, evaluación control de enfermedades no transmisibles.	3	3	1	7	ALTA
72	Informe de número de personas con tamizaje y diagnóstico de cataratas.	2	3	1	6	MEDIO
73	Informe de número de personas con valoración clínica y laboratorio de enfermedades crónicas no transmisibles	2	3	1	6	MEDIO
74	Informe de número de personas tratadas y controladas con Hipertensión Arterial	3	3	1	7	ALTA
75	Informe de número de personas tratadas con diabetes	3	3	1	7	ALTA
76	Informe de número de personas con atención estomatológica preventiva básica	3	3	1	7	ALTA

77	Informe de monitoreo, supervisión, evaluación y control de prevención y control de cáncer	3	3	1	7	ALTA
78	Informe de número de personas con evaluación médica preventiva en cáncer de colon y recto, hígado, leucemia, linfoma, piel y otros.	2	3	3	8	ALTA
79	Informe de monitoreo, supervisión, evaluación y control del programa en salud mental	2	3	1	6	MEDIO
80	Informe de número de niña y/o niño de 8 a 11 años identificado con déficit en sus habilidades sociales.	2	3	1	6	MEDIO
81	Informe de número de personas tamizadas con trastornos mentales y problemas psicosociales ejecutados.	2	3	1	6	MEDIO
82	Informe de número de personas tratadas con problemas psicosociales.	2	3	1	6	MEDIO
83	Informe de número de personas tratadas ambulatoriamente con trastornos afectivos	2	3	1	6	MEDIO
84	Informe de número de personas tratadas ambulatoriamente debido al consumo de alcohol.	2	3	1	6	MEDIO
85	Informe de número de personas tratadas ambulatoriamente debido al consumo de drogas.	2	3	1	6	MEDIO

86	Informe de número de tratamiento ambulatorio de personas con síndrome o trastorno psicótico.	2	3	1	6	MEDIO
87	Informe de número de prevención familiar de conductas de riesgo en adolescentes, familias fuertes amor y límites.	2	3	1	6	MEDIO
88	Informe de número de personas atendidas en sesiones de entrenamiento en habilidades sociales para adolescentes, jóvenes y adultos.	2	3	1	6	MEDIO
89	Informes de número de personas atendidas en sesiones de entrenamiento en habilidades sociales para niños, niñas.	2	3	1	6	MEDIO
90	Informe de número de familias con conocimiento de prácticas saludables para prevenir los trastornos mentales y psicosociales.	2	3	1	6	MEDIO

Tabla N° 04. Valorización de los activos de la información

Fuente: Elaboración Propia

Después de realzar la valorización de los activos se obtuvo una lista de **47 activos** cuya criticidad resultó con valor **alto**, se muestran a continuación:

Id	Activo
1	Computadora de escritorio
2	Licencia de Microsoft Windows 7
3	Licencia de Microsoft Office 2013
4	Página web del MINSA
5	Antivirus
6	Email (para el envío electrónico de información)
7	Cableado Ethernet
8	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)
9	SISMED
10	Llaves de ingreso
11	Documento de Consumo Promedio Mensual Acumulado
12	Formato de Consumo Integrado(ICI)
13	Guías de Remisión de abastecimiento
14	Movimiento Biológico o de vacunas
15	Formato de Movimiento Económico(IME)
16	Voucher de vacunas (depósito del banco)
17	Formato de Requerimientos
18	Informe de porcentaje de disponibilidad
19	Consulta de envío de información
20	Consulta de stocks
21	Consumo promedio mensual y óptimo
22	Control de Calidad de la información

23	Medicamentos sin fecha de vencimiento
24	Medicamentos vencidos en el mes
25	Medicamentos vencidos por fecha de vencimiento
26	Plan Operativo Institucional
27	Informe de número de niños con vacunas completos
28	Informe de número de niños con cred completo
29	Informe de número de niños con suplemento de hierro Población total de niños programados
30	Informe de número de casos de infecciones respiratorias agudas(IRAS)
31	Informe de número de casos de enfermedad diarreica aguda(EDA)
32	Informe de número de casos de Infecciones respiratorias agudas (IRAS) complicadas.
33	Informe de número de casos de enfermedad diarreica aguda (EDA) complicada.
34	Informe de número de gestantes con suplemento de hierro y ácido fólico.
35	Informe de número de adolescentes atendidos que acceden a servicios de salud para prevención del embarazo
36	Informe de número de parejas protegidas que acceden a métodos de Planificación Familiar
37	Informe de número de sintomáticos respiratorios con despistaje de tuberculosis.
38	Informe de número monitoreo, supervisión y control de VIH/SIDA
39	Informe de número de personas atendidas con infecciones de transmisión sexual

40	Informe de monitoreo, supervisión, evaluación y control Metaxénicas y Zoonosis
41	Informe de número de personas con diagnóstico y tratamiento de casos de enfermedades zoonóticas.
42	Informes de monitoreo, supervisión, evaluación control de enfermedades no trasmisibles.
43	Informe de número de personas tratadas y controladas con Hipertensión Arterial
44	Informe de número de personas tratadas con diabetes
45	Informe de número de personas con atención estomatológica preventiva básica
46	Informe de monitoreo, supervisión, evaluación y control de prevención y control de cáncer
47	Informe de número de personas con evaluación médica preventiva en cáncer de colon y recto, hígado, leucemia, linfoma, piel y otros.

Tabla N° 05. Activos con criticidad alta

Fuente: elaboración propia

5.3.2.- Identificación y evaluación de riesgos

5.3.2.1. Mapa de Riesgos

Previamente al desarrollo del mapa de riesgos se procedió a realizar una valorización detallada de riesgos, los cuales involucran hallar las vulnerabilidades y amenazas que puedan afectar a los activos que se ubican dentro del apetito de riesgo previamente definido.

Para la realización de dicha valorización, el estándar ISO 27005 propone varios ejemplos de métodos con los cuales se puede llevar a cabo la valorización de riesgos de manera adecuada. Finalmente, se optó por la realización de una matriz de calor, la cual tiene como criterios la probabilidad que cierta amenaza explote cierta vulnerabilidad y el impacto al negocio estimado que la ocurrencia

del riesgo pueda ocasionar al negocio. A continuación se presenta la matriz de calor con los criterios que se han definido.

Impacto en el Negocio	Probabilidad de Afectación				
	Muy Baja	**Baja**	**Media**	**Alta**	**Muy Alta**
Muy Alto	Relevante	Relevante	Alto	Crítico	Crítico
Alto	Relevante	Relevante	Alto	Alto	Crítico
Medio	Moderado	Moderado	Relevante	Alto	Crítico
Bajo	Bajo	Bajo	Bajo	Moderado	Relevante
Muy Bajo	Bajo	Bajo	Bajo	Bajo	Moderado

Tabla N° 06. Matriz de Calor

Fuente: Elaboración propia

El significado respecto a los criterios de probabilidad de afectación se describe en la siguiente tabla Nº 07:

Probabilidad de Afectación	Interpretación
Muy Alta	Es casi seguro que la amenaza afectará la vulnerabilidad.
Alta	Es probable que la amenaza afectará la vulnerabilidad.
Media	Es posible que la amenaza afectará la vulnerabilidad.
Baja	Es improbable que la amenaza afectará la vulnerabilidad.
Muy Baja	Es impensable que la amenaza afectará la vulnerabilidad.

Tabla N° 07. Descripción de los niveles de la Probabilidad de Afectación

Fuente: Elaboración propia

El significado respecto a los criterios de impacto en el negocio se describe en la siguiente tabla Nº 08:

Impacto en el Negocio	Interpretación
Muy Alto	Afecta por más de una semana las operaciones de la Red de Salud.
Alto	Afecta hasta en 72 horas las operaciones de la Red de Salud.
Medio	Afecta hasta en 24 horas las operaciones de la Red de Salud.
Bajo	Afecta hasta en 6 horas las operaciones del la Red de Salud.
Muy Bajo	Tiene un efecto nulo o muy pequeño en las operaciones de la Red de Salud.

Tabla Nº 08. Descripción de los niveles de Impacto en el negocio

Fuente: Elaboración propia

Luego de evaluar y definir la probabilidad y el impacto en el negocio que pueda ocasionar la materialización de los riesgos identificados obtenemos el nivel de dichos riesgos. Como se observa en el mapa de calor, se pudieron obtener cinco valores de riesgo: bajo, moderado, relevante, alto y crítico. En el siguiente capítulo, se establecerá un criterio de aceptación del riesgo, el cual servirá para realizar un plan de tratamiento de riesgo: si el riesgo es aceptable o si requiere algún tratamiento para reducir, evitar o transferir dicho riesgo.

A continuación, se presenta la matriz completa de riesgos de los activos críticos (criticidad alta) que se entraron en el análisis, según el apetito de riesgo establecido anteriormente.

MATRIZ DE RIESGO						
ID DE RIESGO	ACTIVO	VULNERABILIDAD	AMENAZA	Posibilidad de que la amenaza explote la vulnerabilidad	Impacto estimado en la Institución	Nivel de Riesgo
R1	Computadora de escritorio	Falta de cierre de sesión al momento de salir del área de trabajo	Manipulación de información	Alto	Alto	Alto
R2	Computadora de escritorio	Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	Medio	Muy Alto	Alto
R3	Computadora de escritorio	Susceptibilidad a variaciones en el voltaje	Perdida de suministro de energía	Alto	Muy Alto	Crítico
R4	Computadora de escritorio	Sensibilidad de golpes o caídas	Destrucción de equipos o medios de comunicación	Bajo	Muy Alto	Relevante
R5	Computadora de escritorio	Falta de backups de información	Robo de información o del mismo equipo	Muy Alto	Muy Alto	Crítico
R6	Computadora de escritorio	Mala seguridad de contraseñas	Divulgación de la información	Alto	Muy Alto	Crítico
R7	Licencia de Microsoft Windows 7	Falta de mecanismos de autenticación e identificación de usuarios	Abuso o forzado de derechos	Bajo	Muy Alto	Relevante
R8	Licencia de Microsoft Windows 7	Mala gestión de contraseñas	Abuso o forzado de derechos	Bajo	Muy Alto	Relevante
R9	Licencia de Microsoft Windows 7	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Muy Alto	Alto
R10	Licencia de Microsoft Office 2013	Falta de mecanismos de autenticación e identificación de usuarios	Abuso o forzado de derechos	Bajo	Alto	Relevante
R11	Licencia de Microsoft Office 2013	Mala gestión de contraseñas	Abuso o forzado de derechos	Bajo	Alto	Relevante
R12	Licencia de Microsoft Office 2013	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Alto	Alto
R13	Página web del Minsa	Falta de pruebas del software	Abuso de derechos	Medio	Medio	Relevante
R14	Página web del Minsa	Defectos en el funcionamiento del software	Abuso de derechos	Alto	Medio	Alto
R15	Página web del Minsa	Interfaz de usuario complicada	Error en el uso del software	Alto	Medio	Alto
R16	Página web del Minsa	Falta de documentación	Error en el uso del software	Medio	Medio	Relevante
R17	Página web del Minsa	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Medio	Alto

R18	Antivirus	Interfaz de usuario complicada	Error en el uso del software	Alto	Medio	Alto
R19	Antivirus	Configuración incorrecta de parámetros	Error en el uso del software	Medio	Medio	Relevante
R20	Antivirus	Funciones del antivirus obsoletas	licencia caducada	Alto	Bajo	Moderado
R21	Email (para el envío electrónico de información)	Defectos en el funcionamiento del software	Abuso de derechos	Alto	Alto	Alto
R22	Email (para el envío electrónico de información)	Falta de un log de pistas de auditoria	Abuso de derechos	Medio	Alto	Alto
R23	Email (para el envío electrónico de información)	Fechas incorrectas	Error en el accionar	Muy Bajo	Alto	Bajo
R24	Email (para el envío electrónico de información)	Falta de mecanismos de autenticación e identificación de usuarios	Abuso de derechos	Medio	Alto	Alto
R25	Email (para el envío electrónico de información)	Falta de backups de información	Manipulación de información	Medio	Alto	Alto
R26	Cableado Ethernet	Trafico de información desprotegido	Escuchar información ilegalmente	Medio	Alto	Alto
R27	Cableado Ethernet	Cableado desprotegido	Falla en los equipos de Red	Alto	Alto	Alto
R28	Cableado Ethernet	Arquitectura de red insegura	Espionaje remoto	Bajo	Alto	Relevante
R29	Cableado Ethernet	Gestión inadecuada de la red	Saturación de los sistemas de información	Alto	Alto	Alto
R30	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Falta de controles en el traspaso de información	Robo de documentos o de equipos tecnológicos	Alto	Alto	Alto
R31	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Falta de privilegios en los permisos	Manipulación de información	Muy Alto	Alto	Crítico
R32	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Mala seguridad de contraseñas	Manipulación de información	Alto	Alto	Alto
R33	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Gestión inadecuada de la red	Saturación de los sistemas de información	Alto	Alto	Alto
R34	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Conexiones de red desprotegidas	Uso no autorizado de los equipos de red	Medio	Alto	Alto
R35	SISMED	Interfaz de usuario complicada	Error en el uso del software	Alto	Muy Alto	Crítico

R36	SISMED	Falta de documentación	Error en el uso del software	Medio	Muy Alto	Alto
R37	SISMED	Fechas incorrectas	Error en el accionar	Muy Bajo	Muy Alto	Relevante
R38	SISMED	Falta de backups de información	Manipulación de información con software	Medio	Muy Alto	Alto
R39	SISMED	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Muy Alto	Crítico
R40	Llaves de ingreso	Uso inadecuado o sin cuidado de accesos a instalaciones o habitaciones	Destrucción o robo de equipos o medios de comunicación	Alto	Muy Alto	Crítico
R41	Documento de Consumo Promedio Mensual Acumulado	Falta de mecanismos de backup	Robo o manipulación del activo	Media	Alto	Alto
R42	Formato de Informe de Consumo Integrado(ICI)	Falta de mecanismos de backup	Robo o pérdida de documentos	Muy Alto	Medio	Crítico
R43	Formato de Informe de Consumo Integrado(ICI)	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R44	Formato de Informe de Consumo Integrado(ICI)	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R45	Guías de Remisión de abastecimiento	Falta de mecanismos de backup	Robo o pérdida de documentos	Muy Alto	Medio	Crítico
R46	Guías de Remisión de abastecimiento	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R47	Guías de Remisión de abastecimiento	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R48	Movimiento Biológico o de vacunas	Falta de mecanismos de backup	Robo o pérdida de documentos	Muy Alto	Medio	Crítico
R49	Movimiento Biológico o de vacunas	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R50	Movimiento Biológico o de vacunas	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R51	Formato de Informe de Movimiento Económico(IME)	Falta de mecanismos de backup	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R52	Formato de Informe de Movimiento Económico(IME)	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R53	Formato de Informe de Movimiento Económico(IME)	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R54	Voucher de vacunas(deposito del banco)	Falta de mecanismos de backup	Robo o manipulación del activo	Media	Alto	Alto

R55	Voucher de vacunas(deposito del banco)	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Media	Alto	Alto
R56	Voucher de vacunas(deposito del banco)	Pocos o nulos controles de acceso	Robo o manipulación del activo	Media	Alto	Alto
R57	Formato de Requerimientos	Falta de mecanismos de backup	Robo o manipulación del activo	Media	Alto	Alto
R58	Formato de Requerimientos	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Media	Alto	Alto
R59	Formato de Requerimientos	Pocos o nulos controles de acceso	Robo o manipulación del activo	Media	Alto	Alto
R60	Informe de porcentaje de disponibilidad	Falta de mecanismos de backup	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R61	Informe de porcentaje de disponibilidad	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R62	Informe de porcentaje de disponibilidad	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R63	Consulta de envío de información	Consulta errónea en el sistema	Error en el uso del software	Alto	Medio	Alto
R64	Consulta de stocks	Consulta errónea en el sistema	Error en el uso del software	Medio	Medio	Relevante
R65	Consumo promedio mensual y óptimo	Consulta errónea en el sistema	Error en el uso del software	Medio	Medio	Relevante
R66	Control de Calidad de la información	Consulta errónea en el sistema	Error en el uso del software	Alto	Medio	Alto
R67	Medicamentos sin fecha de vencimiento	Consulta errónea en el sistema	Error en el uso del software	Alto	Medio	Alto
R68	Medicamentos vencidos en el mes	Consulta errónea en el sistema	Error en el uso del software	Alto	Medio	Alto
R69	Medicamentos vencidos por fecha de vencimiento	Consulta errónea en el sistema	Error en el uso del software	Medio	Medio	Relevante
R70	Plan Operativo Institucional	Pocos o nulos controles de acceso	Robo o pérdida de documentos	Medio	Medio	Relevante
R71	Informe de número de niños con vacunas completos	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R72	Informe de número de niños con CRED completo	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto

R73	Informe de número de niños con suplemento de hierro Población total de niños programados	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R74	Informe de número de casos de infecciones respiratorias agudas(IRAS)	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R75	Informe de número de casos de enfermedad diarreica aguda(EDA)	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R76	Informe de número de casos de Infecciones respiratorias agudas (IRAS) complicadas.	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R77	Informe de número de casos de enfermedad diarreica aguda (EDA) complicada.	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R78	Informe de número de gestantes con suplemento de hierro y ácido fólico.	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R79	Informe de número de adolescentes atendidos que acceden a servicios de salud para prevención del embarazo	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R80	Informe de número de parejas protegidas que acceden a métodos de Planificación Familiar.	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R81	Informe de número de sintomáticos respiratorios con despistaje de tuberculosis.	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R82	Informe de número monitoreo, supervisión y control de VIH/SIDA	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R83	Informe de número de personas atendidas con infecciones de transmisión sexual	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R84	Informe de monitoreo, supervisión, evaluación y control Metaxénicas y Zoonosis	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R85	Informe de número de personas con diagnóstico y tratamiento de casos de enfermedades zoonóticas.	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto

R86	Informes de monitoreo, supervisión, evaluación control de enfermedades no transmisibles.	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R87	Informe de Número de personas tratadas y controladas con Hipertensión Arterial	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R88	Informe de Número de personas tratadas con diabetes	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R89	Informe de Número de personas con atención estomatológica preventiva básica	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R90	Informe de Monitoreo, supervisión, evaluación y control de prevención y control de cáncer	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R91	Informe de Número de personas con evaluación médica preventiva en cáncer de colon y recto, hígado, leucemia, linfoma, piel y otros	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto

Tabla N° 09. Matriz de Riesgos

Fuente: Elaboración propia

5.3.3.-Plan Tratamiento de riesgos

Luego de definir los niveles de riesgos respecto a las vulnerabilidades de cada activo y las amenazas que puedan afectar su integridad, confidencialidad o disponibilidad; se definió un criterio de aceptación del riesgo el cual determina si el riesgo es aceptable o si requiere de algún tratamiento. Finalmente, se obtiene el plan de tratamiento de los riesgos identificados previamente.

A continuación, se presenta el plan de tratamiento de los riesgos:

Nivel de Riesgo	Política para la toma de acciones
Crítico	Riesgo no aceptable
Alto	Riesgo no deseable
Relevante	Riesgo aceptable
Moderado	Riesgo aceptable
Bajo	Riesgo aceptable

Tabla N° 10. Plan de Tratamiento de Riesgos

Fuente: Elaboración propia

Se realiza las siguientes actividades del plan de tratamientos de riesgos:

Descripción de actividades	Recursos generales y financieros necesarios	Responsabilidades
Reunión con la Gerencia para la aprobación del SGSI.	Red de Servicios de Salud de Lambayeque.	Gerencia y Bachiller encargado del desarrollo del SGSI.
Reunión para implementar el tratamiento de los riesgos a mitigar que no pueden ser aceptados	Red de Servicios de Salud de Lambayeque.	Informático de la Red de Servicios de Salud, Bachiller encargado del SGSI.
Reuniones del comité de seguridad del SGSI.	Auditorio de Centro de Salud de Toribia Castro	Informático de la Red de Salud
Auditoria de la eficiencia de la implementación de los controles en el SGSI.	Red de Servicios de Salud de Lambayeque	Informático de la Red de Salud.
Prueba de la eficiencia del proceso de continuidad de negocio para ver la respuesta de los controles ante alguna emergencia.	Red de Salud de Lambayeque	Informático de la Red de Salud, usuarios de las áreas dentro del alcance del SGSI.

Tabla N° 11. Actividades del Plan de tratamiento riesgos

Fuente: Elaboración propia

A continuación, se muestra la tabla N° 12 los riesgos que se toman en cuenta para el tratamiento de riesgos según el plan de tratamiento de riesgos; en total resulto 75:

MATRIZ DE RIESGO						
ID DE RIESGO	**ACTIVO**	**VULNERABILIDAD**	**AMENAZA**	**Posibilidad de que la amenaza explote la vulnerabilidad**	**Impacto estimado en la Institución**	**Nivel de Riesgo**
R1	Computadora de escritorio	Falta de cierre de sesión al momento de salir del área de trabajo	Manipulación de información	Alto	Alto	Alto
R2	Computadora de escritorio	Sensibilidad a la humedad, polvo y al calor	Polvo, corrosión, congelamiento	Medio	Muy Alto	Alto
R3	Computadora de escritorio	Susceptibilidad a variaciones en el voltaje	Perdida de suministro de energía	Alto	Muy Alto	Crítico

R5	Computadora de escritorio	Falta de backups de información	Robo de información o del mismo equipo	Muy Alto	Muy Alto	Crítico
R6	Computadora de escritorio	Mala seguridad de contraseñas	Divulgación de la información	Alto	Muy Alto	Crítico
R9	Licencia de Microsoft Windows 7	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Muy Alto	Alto
R12	Licencia de Microsoft Office 2013	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Alto	Alto
R14	Página web del Minsa	Defectos en el funcionamiento del software	Abuso de derechos	Alto	Medio	Alto
R15	Página web del Minsa	Interfaz de usuario complicada	Error en el uso del software	Alto	Medio	Alto
R17	Página web del Minsa	Servicios innecesarios para el usuario	Procesamiento ilegal de los datos	Alto	Medio	Alto
R18	Antivirus	Interfaz de usuario complicada	Error en el uso del software	Alto	Medio	Alto
R21	Email (para el envío electrónico de información)	Defectos en el funcionamiento del software	Abuso de derechos	Alto	Alto	Alto
R22	Email (para el envío electrónico de información)	Falta de un log de pistas de auditoria	Abuso de derechos	Medio	Alto	Alto
R24	Email (para el envío electrónico de información)	Falta de mecanismos de autenticación e identificación de usuarios	Abuso de derechos	Medio	Alto	Alto
R25	Email (para el envío electrónico de información)	Falta de backups de información	Manipulación de información	Medio	Alto	Alto
R26	Cableado Ethernet	Trafico de información desprotegido	Escuchar información ilegalmente	Medio	Alto	Alto
R27	Cableado Ethernet	Cableado desprotegido	Falla en los equipos de Red	Alto	Alto	Alto
R29	Cableado Ethernet	Gestión inadecuada de la red	Saturación de los sistemas de información	Alto	Alto	Alto

R30	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Falta de controles en el traspaso de información	Robo de documentos o de equipos tecnológicos	Alto	Alto	Alto
R31	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Falta de privilegios en los permisos	Manipulación de información	Muy Alto	Alto	Crítico
R32	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Mala seguridad de contraseñas	Manipulación de información	Alto	Alto	Alto
R33	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Gestión inadecuada de la red	Saturación de los sistemas de información	Alto	Alto	Alto
R34	Red Informática de la Red de Salud de Lambayeque (carpetas compartidas)	Conexiones de red desprotegidas	Uso no autorizado de los equipos de red	Medio	Alto	Alto
R35	SISMED	Interfaz de usuario complicada	Error en el uso del software	Alto	Muy Alto	Crítico
R36	SISMED	Falta de documentación	Error en el uso del software	Medio	Muy Alto	Alto
R38	SISMED	Falta de backups de información	Manipulación de información con software	Medio	Muy Alto	Alto
R39	SISMED	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Muy Alto	Crítico
R40	Llaves de ingreso	Uso inadecuado o sin cuidado de accesos a instalaciones o habitaciones	Destrucción o robo de equipos o medios de comunicación	Alto	Muy Alto	Crítico
R41	Documento de Consumo Promedio Mensual Acumulado	Falta de mecanismos de backup	Robo o manipulación del activo	Media	Alto	Alto

R42	Formato de Informe de Consumo Integrado(ICI)	Falta de mecanismos de backup	Robo o pérdida de documentos	Muy Alto	Medio	Crítico
R43	Formato de Informe de Consumo Integrado(ICI)	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R44	Formato de Informe de Consumo Integrado(ICI)	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R45	Guías de Remisión de abastecimiento	Falta de mecanismos de backup	Robo o pérdida de documentos	Muy Alto	Medio	Crítico
R46	Guías de Remisión de abastecimiento	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R47	Guías de Remisión de abastecimiento	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R48	Movimiento Biológico o de vacunas	Falta de mecanismos de backup	Robo o pérdida de documentos	Muy Alto	Medio	Crítico
R49	Movimiento Biológico o de vacunas	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R50	Movimiento Biológico o de vacunas	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R51	Formato de Informe de Movimiento Económico(IME)	Falta de mecanismos de backup	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R52	Formato de Informe de Movimiento Económico(IME)	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R53	Formato de Informe de Movimiento Económico(IME)	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R54	Voucher de vacunas(deposito del banco)	Falta de mecanismos de backup	Robo o manipulación del activo	Media	Alto	Alto
R55	Voucher de vacunas(deposito del banco)	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Media	Alto	Alto

R56	Voucher de vacunas(deposito del banco)	Pocos o nulos controles de acceso	Robo o manipulación del activo	Media	Alto	Alto
R57	Formato de Requerimientos	Falta de mecanismos de backup	Robo o manipulación del activo	Media	Alto	Alto
R58	Formato de Requerimientos	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Media	Alto	Alto
R59	Formato de Requerimientos	Pocos o nulos controles de acceso	Robo o manipulación del activo	Media	Alto	Alto
R60	Informe de porcentaje de disponibilidad	Falta de mecanismos de backup	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R61	Informe de porcentaje de disponibilidad	Falta de cuidado en el transporte o en su transferencia	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R62	Informe de porcentaje de disponibilidad	Pocos o nulos controles de acceso	Robo o manipulación del activo	Muy Alto	Medio	Crítico
R63	Consulta de envío de información	Consulta errónea en el sistema	Error en el uso del software	Alto	Medio	Alto
R66	Control de Calidad de la información	Consulta errónea en el sistema	Error en el uso del software	Alto	Medio	Alto
R67	Medicamentos sin fecha de vencimiento	Consulta errónea en el sistema	Error en el uso del software	Alto	Medio	Alto
R68	Medicamentos vencidos en el mes	Consulta errónea en el sistema	Error en el uso del software	Alto	Medio	Alto
R71	Informe de número de niños con vacunas completos	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R72	Informe de número de niños con CRED completo	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R73	Informe de número de niños con suplemento de hierro Población total de niños programados	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto

R74	Informe de número de casos de infecciones respiratorias agudas(IRAS)	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R75	Informe de número de casos de enfermedad diarreica aguda(EDA)	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R76	Informe de número de casos de Infecciones respiratorias agudas (IRAS) complicadas.	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R77	Informe de número de casos de enfermedad diarreica aguda (EDA) complicada.	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R78	Informe de número de gestantes con suplemento de hierro y ácido fólico.	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R79	Informe de número de adolescentes atendidos que acceden a servicios de salud para prevención del embarazo	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R80	Informe de número de parejas protegidas que acceden a métodos de Planificación Familiar.	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R81	Informe de número de sintomáticos respiratorios con despistaje de tuberculosis.	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto

R82	Informe de número monitoreo, supervisión y control de VIH/SIDA	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R83	Informe de número de personas atendidas con infecciones de transmisión sexual	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R84	Informe de monitoreo, supervisión, evaluación y control Metaxénicas y Zoonosis	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R85	Informe de número de personas con diagnóstico y tratamiento de casos de enfermedades zoonóticas.	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R86	Informes de monitoreo, supervisión, evaluación control de enfermedades no transmisibles.	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R87	Informe de Número de personas tratadas y controladas con Hipertensión Arterial	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R88	Informe de Número de personas tratadas con diabetes	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto
R89	Informe de Número de personas con atención estomatológica preventiva básica	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto

R90	Informe de Monitoreo, supervisión, evaluación y control de prevención y control de cáncer	Falta de mecanismos de backup	Robo o pérdida de documentos	Alto	Alto	Alto
R91	Informe de Número de personas con evaluación médica preventiva en cáncer de colon y recto, hígado, leucemia, linfoma, piel y otros	Falta de mecanismos de backup	Robo o manipulación del activo	Alto	Alto	Alto

Tabla N° 12. Lista de Riesgos no aceptables

Fuente: Elaboración propia

5.3.4.- Controles para el tratamiento de riesgos.

Primero se definen las políticas, en total se definieron 26:

Cláusula	Categoría de Seguridad	Nombre del control	Descripción
Políticas de seguridad	**Directrices de la Dirección en seguridad de la información.**	**Conjunto de políticas para la seguridad de la información.**	Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes.
		Revisión de las políticas para la seguridad de la información.	Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y

			efectividad.
Aspectos organizativos de la seguridad de la información	**Organización interna**	**Asignación de responsabilidades para la seguridad de la información**	Se deberían definir y asignar claramente todas las responsabilidades para la seguridad de la información.
		Segregación de tareas	Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.
		Seguridad de la información en la gestión de proyectos.	Se debería contemplar la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización.
Gestión de activos	**Responsabilidad sobre los activos**	**Inventario de activos**	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
		Propiedades de los activos	Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la

			Organización.
		Uso aceptable de los activos	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
		Devolución de activos	Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/ responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.
	Clasificación de la información	**Directrices de clasificación**	La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.
		Etiquetado y manipulación de la información	Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
		Manipulación de activos.	Se deberían desarrollar e implantar procedimientos para la manipulación de

			los activos acordes con el esquema de clasificación de la información adoptado por la organización.
Gestión de incidentes.	**Gestión de incidentes de seguridad de la información y mejoras**	**Responsabilidades y procedimientos.**	Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
		Notificación de los eventos de seguridad de la información.	Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.
		Notificación de puntos débiles de la seguridad.	Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.
		Aprendizaje de los incidentes de seguridad de la información	Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
		Recopilación de evidencias	La organización debería definir y aplicar los

			procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.
Cumplimiento	**Cumplimiento de los requisitos legales y contractuales.**	**Derechos de propiedad intelectual**	Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original.
		Protección de los registros de la organización	Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
		Protección de datos y privacidad de la información personal	Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.
	Revisiones de la seguridad de la información	**Comprobación del cumplimiento**	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas

			de seguridad dispuestas por la información de la organización.
Seguridad en la operativa	**Responsabilidades y procedimientos de operación**	**Documentación de procedimientos de operación**	Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.
	Protección contra código malicioso	**Controles contra el código malicioso**	Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.
	Copias de seguridad	**Copias de seguridad de la información**	Se deberían realizar pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.
Control de accesos	**Gestión de acceso de usuario**	**Revisión de los derechos de acceso de los usuarios**	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.
		Retirada o adaptación de los derechos de acceso	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo,

			contrato o acuerdo, o ser revisados en caso de cambio.

Tabla N° 13. Políticas de Seguridad

Fuente: Elaboración propia

Luego de definir las políticas de seguridad que serán adoptadas por la institución pública, se procede a realizar un listado de los controles para el tratamiento de riesgos que se identificaron; especificando el control, su descripción según la norma ISO 27002:2013, los riesgos que mitigará y la adaptación de dicho control con la realidad organizacional de la Red de Salud de Lambayeque en la tabla Nº 14.

Se detalla que significa cada columna:

- Cláusula.- Se refiere al nombre del dominio de los controles de la norma ISO 27002:2013.
- Categoría de seguridad: Es el nombre del objetivo de control de la lista de controles de la norma ISO 27002:2013.
- Nombre del Control.- Control de la lista de 114 de la ISO 27002:2013.
- Descripción.- Son las actividades que se realiza en cada control.
- Riesgos a controlar.- Es el riesgo o los riesgos que se van a controlar; está representado por la letra R seguido del número del riesgo según el orden que tiene en la tabla de riesgos Nº 12.

Clausula	Categoría de Seguridad	Nombre Control	Descripción	Riesgos a Controlar	Adaptación a la Red de Salud
Seguridad física y ambiental	Áreas seguras	Seguridad de oficinas, despachos y recursos	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.	R40,R51, R54, R57, R60, R71,R72, R73, R78,R79 R80, R81, R82,R83, R84, R85,R87, R88, R89, R91.	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la Red de Salud de Lambayeque
	Seguridad de los equipos	Instalaciones de suministro	Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.	R3	Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo en la red de Salud de Lambayeque.
		Seguridad del cableado	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.	R3, R26 R27, R29	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información dentro de la Red de Salud de Lambayeque se deberían proteger contra la interferencia o posibles daños.
		Mantenimiento de los equipos	Los equipos deberían mantenerse adecuadamente con el	R2, R3, R14.	Los equipos de la Red de Salud de Lambayeque deberían

			objeto de garantizar su disponibilidad e integridad continuas.		Darse mantenimiento una vez al mes para garantizar su disponibilidad e integridad.
		Salida de activos fuera de las dependencias de la empresa	Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.	R5	Los equipos, la información, no se deberían retirar de la Red de Salud de Lambayeque sin previa autorización de la gerencia y el responsable de informática.
		Equipo informático de usuario desatendido	Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.	R1, R2	Los usuarios en la Red de Salud de Lambayeque se deberían asegurar de que los equipos informáticos tengan la protección adecuada por parte del responsable de informática.
		Política de puesto de trabajo despejado y bloqueo de pantalla	Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones	R1	Se debería adoptar en la Red de Salud una política de puesto de trabajo despejado para la documentación y para medios de almacenamiento extraíbles.

			de procesamiento de información		
Seguridad en las telecomunicaciones	Gestión en la seguridad de redes	Controles de red	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.	R33	Se debería formular una política respecto al uso de redes, donde solo los usuarios de la Red de Salud de Lambayeque que sean responsables del área puedan manejarlo.
	Intercambio de información con partes externas.	Políticas y procedimientos de intercambio de información	Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.	R14, R15,R17, R21,R30,R33,R43, R46,R49, R52, R55,R58,R61	Debe haber controles y procedimientos que permitan a un usuario de la Red de Salud de Lambayeque poder asegurar que la transferencia de información de manera externa no falle en ningún momento.
		Mensajería electrónica	Se debería proteger adecuadamente la información referida en la mensajería electrónica.	R22,R24,R25	La Institución debe implantar controles adecuados para evitar la pérdida de información contenida en los correos electrónicos.
		Acuerdos de confidencialidad y secreto	Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de	R38,R39,R41,R42,R45,R48,R51,R54, R57,R60	Se debe fijar controles donde se mantenga el acceso de la información solo al personal autorizado

			confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.		según corresponda.
Seguridad en la operativa	Protección contra código malicioso	Controles contra el código malicioso	Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.	R14,R21	La protección de códigos maliciosos se deben tratar detectando código malicioso en los sistemas de la Red de Salud de Lambayeque y el uso de adecuados controles para el acceso a los sistemas.
	Copias de seguridad	Copias de seguridad de la información	Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.	R38,R39,R41,R42,R45,R48,R74,R75,R76,R77,R86,R90	La Red de Salud de Lambayeque debe proporcionar medios de respaldo de información para garantizar la total recuperación de la misma ante algún desastre o falla de medios de almacenamiento.
	Registro de actividad y supervisión	Registro y gestión de eventos de actividad	Se deberían producir, mantener y revisar periódicamente los registros	R22	La institución debería implementar logs de auditoria y eventos de seguridad de

			relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.		información, con el fin de guardar los registros para futuras investigaciones.
	Consideraciones de las Auditorias de los Sistemas de Información	Controles de auditoría de los sistemas de información.	Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.	R18,R35,R36R63,R66,R67,R68	Se debe implementar las auditorias necesarias para verificar los sistemas operacionales de la Red de Salud de Lambayeque con la finalidad de no interrumpir los procesos de negocio.
Control de accesos	Requisitos de negocio para el control de acceso	Control de acceso a las redes y servicios asociados	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.	R34	Se debe establecer una política que permita a los solo a los usuarios que tienen acceso al uso de la Red según las funciones que hayan sido asignadas
	Gestión de acceso de usuario.	Gestión de altas/bajas en el registro de Usuarios	Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.	R9,R12,R17, R31, R32,R44 R47, R50, R53, R56, R59, R62,	Se debe aplicar los controles necesarios para dar de alta y baja a los usuarios que tienen acceso a diferentes tipos de información importante

					en la Red de Salud de Lambayeque.
		Retirada o adaptación de los derechos de acceso	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.	R6,R30,R40	Se deberían aplicar controles que impliquen retirar los derechos de acceso a los sistemas o instalaciones que tengan que ver con información importante de la Red de Salud de Lambayeque una vez que los empleados terminen su contrato o servicio con la Institución.
	Control de acceso a Sistemas y Aplicaciones	Restricción del acceso a la información	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.	R36	Se debe establecer una política donde restrinja el acceso a los usuarios o personal que maneja los sistemas de acuerdo a la función que cumple cada uno dentro de la Red de Salud de Lambayeque.
		Gestión de contraseñas de usuario	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.	R6,R32	La persona encargada de sistemas deberá proporcionar las contraseñas correspondientes para acceder a Windows y a las aplicaciones del SISMED,

					entre otros. Esta política incluye la generación, cambio de la misma.

Tabla N° 14. Controles para el tratamiento de riesgos

Fuente: Elaboración propia

5.3.5.- Mapeo de los Controles con COBIT 5.

En ésta parte se van a identificar los objetivos corporativos que COBIT 5 propone, pero que estén relacionados con los objetivos de negocio de la Red de Salud de Lambayeque. Luego se relacionará las metas de TI asociadas a dichos objetivos organizacionales, seguido se continuará con la identificación de los procesos habilitadores que dan soporte al cumplimiento de dichas metas de TI. Finalmente se comparará y evaluará los procesos habilitadores finales con los controles para el tratamiento de riesgos que se establecieron en el tema anterior.

Este proceso de mapeo se realizará siguiendo el esquema de COBIT 5 llamado "Cascada de objetivos",

Los objetivos organizacionales que propone COBIT 5 y que la Red de Salud desea lograr se puede observar en la tabla Nº 15:

- La columna de dimensión de cuadro de mando integral indica las dimensiones a las cuales se ajustan las metas corporativas.
- La columna de metas de la Institución son metas genéricas propuestas por COBIT a las cuales se puede adaptar la Red de Salud de Lambayeque.
- No se considera el meta Nº 01 "Valor para las partes interesadas de las Inversiones de Negocio" porque trata sobre inversiones de productos y servicios, y según el proceso los productos son en función de requerimientos.

- No se considera la meta Nº 10 “optimización de costes de entrega del servicio”, ya que es una institución que brinda servicios de salud sin costo, es del Estado.
- No se considera la meta N° 13 ya que trata de gestión de programas de TI en el negocio. La red de Salud no produce software ni hardware.
- La lista completa de metas de COBIT se encuentra en el anexo 05 de la tesis.
- Los ejemplos sobre las métricas de los objetivos de COBIT se encuentran en el anexo 06 de la tesis.

Dimensión de cuadro de mando integral	N°	Metas de la Institución
Financiera	2	Cartera de productos y servicios competitivos
Financiera	3	Riesgos de negocio gestionados (salvaguarda de activos)
Financiera	4	Cumplimiento de leyes y regulaciones externas
Financiera	5	Transparencia financiera
Cliente	6	Cultura de servicio orientada al cliente
Cliente	7	Continuidad y disponibilidad del servicio
Cliente	8	Respuestas ágiles a un entorno de negocio cambiante
Cliente	9	Toma estratégica de Decisiones basada en Información
Interna	11	Optimización de la funcionalidad de los procesos de negocio
Interna	12	Optimización de los costes de los procesos de negocio
Interna	14	Productividad operacional y de los empleados
Interna	15	Cumplimiento con las políticas internas
Aprendizaje y Crecimiento	16	Personas preparadas y motivadas
Aprendizaje y Crecimiento	17	Cultura de innovación de producto y negocio

Tabla N° 15. Objetivos organizacionales de la Institución según COBIT 5

Fuente: (ISACA, 2012)

A continuación, se detalla la relación de los objetivos TI requeridos para lograr los objetivos de la institución en la tabla Nº 16:

- La columna de metas de la Institución son metas genéricas propuestas por COBIT a las cuales se puede adaptar la Red de Salud de Lambayeque.
- La columna objetivos de TI representa las metas relacionadas a las tecnologías de la información alineadas a las metas de la institución, en total son un total de 17 que propone COBIT y se detalla en el Anexo 8 de la tesis.

N°	Metas de la Institución	ID TI	Objetivos de TI
2	Cartera de productos y servicios competitivos	1	Alineamiento de TI y estrategia de negocio
		5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
		7	Entrega de servicios de TI de acuerdo a los requisitos del negocio
		9	Agilidad de las TI
		12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
3	Riesgos de negocio gestionados (salvaguarda de activos)	4	Riesgos de negocio relacionados con las TI gestionados.
		10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
		16	Personal del negocio y de las TI competente y motivado
4	Cumplimiento de leyes y regulaciones externas	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
		10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
5	Transparencia financiera	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI

		6	Transparencia de los costes, beneficios y riesgos de las TI
6	Cultura de servicio orientada al cliente	1	Alineamiento de TI y estrategia de negocio
		7	Entrega de servicios de TI de acuerdo a los requisitos del negocio
7	Continuidad y disponibilidad del servicio	1	Alineamiento de TI y estrategia de negocio
		4	Riesgos de negocio relacionados con las TI gestionados
		10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
		14	Disponibilidad de información útil y relevante para la toma de decisiones
8	Respuestas ágiles a un entorno de negocio cambiante	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio
		9	Agilidad de las TI
		17	Conocimiento, experiencia e iniciativas para la innovación de negocio
9	Toma estratégica de Decisiones basada en Información	1	Alineamiento de TI y estrategia de negocio
		14	Disponibilidad de información útil y relevante para la toma de decisiones
11	Optimización de la funcionalidad de los procesos de negocio	1	Alineamiento de TI y estrategia de negocio
		7	Entrega de servicios de TI de acuerdo a los requisitos del negocio
		8	Uso adecuado de aplicaciones, información y soluciones tecnológicas
		9	Agilidad de las TI
		12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
12	Optimización de los costes de los procesos de negocio	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
		6	Transparencia de los costes, beneficios y riesgos de las TI
		11	Optimización de activos, recursos y

			capacidades de las TI
14	Productividad operacional y de los empleados	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas.
		16	Personal del negocio y de las TI competente y motivado
15	Cumplimiento con las políticas internas	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
		10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
		15	Cumplimiento de las políticas internas por parte de las TI
16	Personas preparadas y motivadas	16	Personal del negocio y de las TI competente y motivado

Tabla N° 16. Objetivos de TI de la Institución según los objetivos organizacionales.

Fuente: (ISACA, 2012)

Relacionar los objetivos de TI con los procesos habilitadores que COBIT 5.0 define se muestra en la tabla N° 17:

- La Columna ID TI es el identificador de Los objetivos de TI.
- La columna Objetivos de TI se refiera a las metas de TI relacionadas con la Institución.
- La columna ID Proceso es el identificador de los procesos que propone COBIT 5.O.
- La columna procesos habilitadores presenta los procesos que propone COBIT que toda empresa debe tener y que apoyan a los Objetivos de TI.

El detalle de todos los procesos habilitadores de COBIT 5.0 se encuentra en el anexo N° 09 de la presente Tesis.

Id TI	Objetivos de TI	Id Proceso	Procesos Habilitadores
1	Alineamiento de TI y la estrategia de negocio	EDM01	Asegurar el establecimiento y mantenimiento del marco de Gobierno
		BAI02	Gestionar la definición de requisitos
2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	APO12	Gestionar el riesgo
		BAI10	Gestionar la configuración
		MEA02	Supervisar, evaluar y valorar el Sistema de Control Interno
		MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos.
3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	EDM01	Asegurar el establecimiento y mantenimiento del marco de Gobierno.
		EDM05	Asegurar la transparencia hacia las partes interesadas
4	Riesgos de negocio relacionados con las TI gestionados	APO10	Gestionar los proveedores
		APO12	Gestionar el riesgo
		BAI06	Gestionar los cambios
		DSS03	Gestionar los problemas
		DSS06	Gestionar los controles de los procesos del negocio.
		MEA01	Supervisar, evaluar y valorar rendimiento y conformidad.
		MEA02	Supervisar, evaluar y valorar el Sistema de control interno.
		MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos.
5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	APO10	Gestionar los Proveedores.
6	Transparencia de los costes,	APO12	Gestionar el riesgo.

	beneficios y riesgos de las TI	BAI09	Gestionar los activos.
		EDM05	Asegurar la transparencia hacia las partes interesadas.
7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	APO10	Gestionar los proveedores
		BAI02	Gestionar la definición de requisitos.
		BAI06	Gestionar los cambios.
		DSS03	Gestionar los problemas.
		DSS06	Gestionar los controles de los procesos dela empresa
		EDM01	Asegurar el establecimiento y mantenimiento del marco de Gobierno
		EDM05	Asegurar la transparencia hacia las partes interesadas.
		MEA01	Supervisar, evaluar y valorar rendimiento y conformidad.
8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	BAI07	Gestionar la aceptación del cambio y de la transición.
9	Agilidad de las TI	APO10	Gestionar los proveedores
		BAI08	Gestionar el conocimiento
10	Seguridad de la información, infraestructura de procesamiento y aplicaciones	APO12	Gestionar el riesgo
		BAI06	Gestionarlos Cambios
11	Optimización de activos, recursos y capacidades de las TI	BAI09	Gestionar los activos
		BAI10	Gestionar la configuración
		DSS03	Gestionar los problemas
		MEA01	Supervisar, evaluar y valorar rendimiento y conformidad
12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	BAI01	Gestionar los programas y proyectos
		BAI07	Gestionar la aceptación del cambio y de la transición
14	Disponibilidad de información útil y relevante para la toma de decisiones	BAI10	Gestionar la configuración.
		DSS03	Gestionarlos problemas
15	Cumplimiento de las políticas internas por parte de las TI	MEA01	Supervisar, evaluar y valorar rendimiento y conformidad
		MEA02	Supervisar, evaluar y valorar el Sistema de control interno
16	Personal del negocio y de las TI competente y motivado	APO12	Gestionar el riesgo

17	Conocimiento, experiencia e iniciativas para la innovación de negocio	BAI08	Gestionar el conocimiento

Tabla N° 17. Procesos habilitadores de COBIT 5 según los objetivos de TI de la Institución

Fuente: (ISACA, 2012)

Finalmente, se muestra la tabla detallando el mapeo de los procesos habilitadores y los controles para el tratamiento de riesgos de los activos en la Red de Salud de Lambayeque.

En la Tabla N° 18 se tiene:

- La columna ID, es el identificador de los procesos habilitadores que COBIT propone.
- La columna Proceso Habilitador, es el nombre de los Procesos habilitadores que COBIT propone.
- La columna Id Control, es el identificador del Control de la ISO 27002:2013.
- La columna Nombre de Control, muestra el nombre del Control según la ISO 27002:2013
- La columna Descripción, muestra cual es el objetivo del control según como lo especifica la norma ISO 27002:2103.

ID	Proceso Habilitador	Id Control	Nombre del Control	Descripción
APO10	Administrar proveedores.	13.2.4	Acuerdos de confidencialidad y secreto.	Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.
		13.2.1	Políticas y procedimientos de intercambio de información.	Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de

				comunicación.
APO12	Gestionar el riesgo.	16.1.2	Notificación de los eventos de seguridad de la información.	Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.
		16.1.3	Notificación de puntos débiles de seguridad.	Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.
BAI02	Gestionar la definición de los requisitos.	12.7.1	Controles de auditoria de los sistemas de información	Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.
BAI06	Gestionar los cambios.	12.4.1	Registro y gestión de evento de actividad.	Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
BAI07	Gestionar la aceptación del cambio y de la transición.	9.2.6	Retirada o adaptación de los derechos de acceso	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.
BAI08	Gestionar el conocimiento.	16.1.6	Aprendizaje de los incidentes de seguridad de la	Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes

			información	de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
		16.1.7	Recopilación de la información.	La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.
BAI09	Gestionar los activos	8.1.1	Inventario de activos	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
		8.1.2	Propiedades de los activos.	Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
		8.1.3	Uso aceptable de los activos.	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
		8.1.4	Devolución de activos.	Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.
		8.2.1	Directrices de clasificación.	La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización. Se debería desarrollar e implantar un conjunto apropiado de

				procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
		8.2.2	Etiquetado y manipulación de la información.	Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
		8.2.3	Manipulación de activos.	Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
BAI10	Gestionar la configuración	8.1.1	Inventario de activos.	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
		8.2.2	Etiquetado y manipulación de la información.	Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
DSS03	Gestionar los problemas	16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en

				el futuro.
DSS06	Gestionar los controles de los procesos de negocio.	12.3.1	Copias de seguridad de la información.	Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.
		13.1.1	Controles de Red	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
		13.2.3	Mensajería electrónica.	Se debería proteger adecuadamente la información referida en la mensajería electrónica.
		9.1.2	Control de acceso a las redes	Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.
EDM05	Asegurar la transparencia hacia las partes interesadas	18.1.2	Derechos de propiedad intelectual.	Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original.
		18.1.3	Protección de los registros de la Organización.	Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
		18.1.4	Protección de datos y privacidad de la información personal.	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la

				organización.
MEA01	Supervisar, evaluar y valorar rendimiento y conformidad.	5.1.2	Revisión de las políticas para la seguridad de la información.	Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad.
		18.2.3	Comprobación del cumplimiento	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.
MEA02	Supervisar, evaluar y valorar el Sistema de Control interno.	5.1.2	Revisión de las políticas para la seguridad de la información.	Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad.
		18.2.3	Comprobación del cumplimiento	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.
		12.1.1	Documentación de procedimientos de operación.	Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.
MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos externos.	18.1.4	Protección de datos y privacidad de la información personal.	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

Tabla N° 18. Mapeo de procesos habilitadores

Fuente: (ISACA, 2012)

5.3.6.- Declaración de Aplicabilidad

Luego de la evaluación de riesgos se presenta el siguiente documento donde se lista los controles que mitigarán los riesgos encontrados anteriormente, la adaptación de los controles a la organización, riesgos a controlar, si aplica o no y la justificación del porque se está proponiendo los controles.

Nombre Control	Adaptación a la Red de Salud de Lambayeque	Riesgos a controlar	Aplica	Justificación
Seguridad de oficinas, despachos y recursos	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la Red de Salud de Lambayeque	R40,R51, R54, R57, R60, R71,R72, R73, R78,R79 R80, R81, R82,R83, R84, R85,R87, R88, R89, R91.	Si	Actualmente la Red de Salud de Lambayeque carece de controles adecuados para proteger sus instalaciones
Instalaciones de suministro	Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo en la red de Salud de Lambayeque.	R3	Si	La Red de Salud de Lambayeque actualmente carece de un sistema alterno de alimentación de energía.
Seguridad del cableado	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información dentro de la Red de Salud de Lambayeque se deberían proteger contra la interferencia o posibles daños.	R3,R26,R27 ,R29	Si	La implantación de un cableado nuevo es una propuesta vital ya que en la actualidad está deteriorado en un 30%. Esto aseguraría la base de una buena infraestructura respecto a la red de la Institución.
Mantenimiento de los equipos	Los equipos de la Red de Salud de Lambayeque deberían darse mantenimiento una vez al mes para garantizar su disponibilidad e integridad.	R2,R3,R14	Si	La Red de Salud de Lambayeque no cuenta con controles de mantenimiento de los equipos, solo se hace por requerimiento de los usuarios.

Salida de activos fuera de las dependencias de la empresa	Los equipos, la información, no se deberían retirar de la Red de Salud de Lambayeque sin previa autorización de la gerencia y el responsable de informática.	R5	Si	Actualmente en la Red de Salud de Lambayeque no existe un documento o control para dar salida a los equipos fuera de la institución, pero se considera formalizarlo.
Equipo informático de usuario desatendido	Los usuarios en la Red de Salud de Lambayeque se deberían asegurar de que los equipos informáticos tengan la protección adecuada por parte del responsable de informática.	R1,R2	Si	Es una buena política a implantar ya que mejorará la concientización de los usuarios por cuidar sus pertenencias.
Política de puesto de trabajo despejado y bloqueo de pantalla	Se debería adoptar en la Red de Salud una política de puesto de trabajo despejado para la documentación y para medios de almacenamiento extraíbles.	R1	Si	Es una política importante que se va tomar en cuenta porque actualmente los usuarios no están consiente de la seguridad que deben tener con sus equipos.
Controles de red	Se debería formular una política respecto al uso de redes, donde solo los usuarios de la Red de Salud de Lambayeque que sean responsables del área puedan manejarlo.	R33	Si	La seguridad en la Red de Salud de Lambayeque es importante ya que se manejan sistemas en línea y además del correo electrónico.
Políticas y procedimientos de intercambio de información	Debe haber controles y procedimientos que permitan a un usuario de la Red de Salud de Lambayeque poder asegurar que la transferencia de información de manera externa no falle en ningún momento.	R14,R15,R17,R21,R30,R33,R43,R46,R49,R52,R55,R58,R61	Si	Este control se implementará y está ligado a las políticas de seguridad propuestas en la Red de Salud de Lambayeque
Mensajería electrónica	La Institución debe implantar controles adecuados para evitar la pérdida de información contenida en los correos electrónicos.	R22,R24,R25	Si	No se tiene aún un control implementado para el correo electrónico, pero es muy importante ya que la información que se envía y recibe es mayormente a través de ésta vía.

Acuerdos de confidencialidad y secreto	Se debe fijar controles donde se mantenga el acceso de la información solo al personal autorizado según corresponda.	R38,R39,R41,R42,R45, R48,R51,R54,R57,R60	Si	Aún no está contemplado dentro de los contratos de los trabajadores como una cláusula que deban cumplir los trabajadores, solo existe como recomendación dentro de la Institución.
Controles contra el código malicioso	La protección de códigos maliciosos se deben tratar detectando código malicioso en los sistemas de la Red de Salud de Lambayeque y el uso de adecuados controles para el acceso a los sistemas.	R14,R21	Si	Actualmente existen dos tipos de antivirus en la Red de Salud, el Avast y el Nod 32 que siempre están desactualizados, razón por la cual se debe implementar este control que permita usar las aplicaciones sin temor a cualquier contagio en la misma Pc o algún dispositivo de almacenamiento.
Copias de seguridad de la información	La Red de Salud de Lambayeque debe proporcionar medios de respaldo de información para garantizar la total recuperación de la misma ante algún desastre o falla de medios de almacenamiento.	R38,R39,R41,R42,R45, R48,R74,R75,R76,R77, R86,R90	Si	Actualmente existe una política de backups de seguridad que se realiza mensualmente, pero no son las más adecuadas. Por ese motivo se propondrán modificarlas según el nivel de seguridad y la importancia que éstas tengan.
Registro y gestión de eventos de actividad	La institución debería implementar logs de auditoria y eventos de seguridad de información, con el fin de guardar los registros para futuras investigaciones.	R22	Si	No existe actualmente un sistema o mecanismo que registre la actividad o eventos de los usuarios, pero es necesario debido a que se debe mejorar la seguridad que se plantea en la Red de Salud.
Controles de auditoría de los sistemas de información.	Se debe implementar las auditorias necesarias para verificar los sistemas operacionales de la Red de Salud de Lambayeque con la finalidad de no interrumpir los procesos de negocio.	R18,R35,R36 R63,R66,R67,R68	Si	Es necesario implementar estos controles para garantizar la operatividad de los sistemas que forman parte dentro del proceso de suministro de medicamentos.
Control de acceso a las redes y servicios asociados	Se debe establecer una política que permita a los solo a los usuarios que tienen acceso al uso de la Red según las	R34	Si	La red informática cumple un papel muy importante, entonces un control para acceder a la misma es necesario para mejorar la seguridad.

	funciones que hayan sido asignadas			
Gestión de altas/bajas en el registro de Usuarios	Se debe aplicar los controles necesarios para dar de alta y baja a los usuarios que tienen acceso a diferentes tipos de información importante en la Red de Salud de Lambayeque.	R9,R12,R17 ,R31, R32,R44 R47, R50, R53, R56, R59, R62,	Si	La Red de Salud de Lambayeque maneja sus procedimientos para dar de alta y baja a los usuarios, del sistema y de Windows y/o correo, pero no son los más adecuados. Sin embargo, se ajustarán de acuerdo a los niveles de seguridad de la organización.
Retirada o adaptación de los derechos de acceso	Se deberían aplicar controles que impliquen retirar los derechos de acceso a los sistemas o instalaciones que tengan que ver con información importante de la Red de Salud de Lambayeque una vez que los empleados terminen su contrato o servicio con la institución.	R6,R30,R40	Si	Este control está alineada a las políticas que se piensa implementar en la Red de Salud de Lambayeque, debido a la concurrencia de personal de otras áreas y sedes, lo cual es muy necesario.
Restricción del acceso a la información	Se debe establecer una política donde restrinja el acceso a los usuarios o personal que maneja los sistemas de acuerdo a la función que cumple cada uno dentro de la Red de Salud de Lambayeque.	R36	Si	Actualmente no existe una política para acceso a la información, son solo procedimientos comunes. Se empleará de acuerdo con las necesidades de la Organización.
Gestión de contraseñas de usuario	La persona encargada de sistemas deberá proporcionar las contraseñas correspondientes para acceder a Windows y a las aplicaciones del SISMED, entre otros. Esta política incluye la generación, cambio de la misma.	R6,R32	Si	El responsable de informática es quien gestiona las contraseñas de los sistemas en general, pero no hay una política formal; por lo cual se creará para garantizar la seguridad en los equipos y en el Sistema.

Tabla N° 19. Declaración de Aplicabilidad

Fuente: Elaboración propia

5.4.- Implementar y Utilizar el SGSI

En la siguiente figura Nº 13 se muestra como es la situación actual y lo que se plantea implementar a través de procedimientos y políticas:

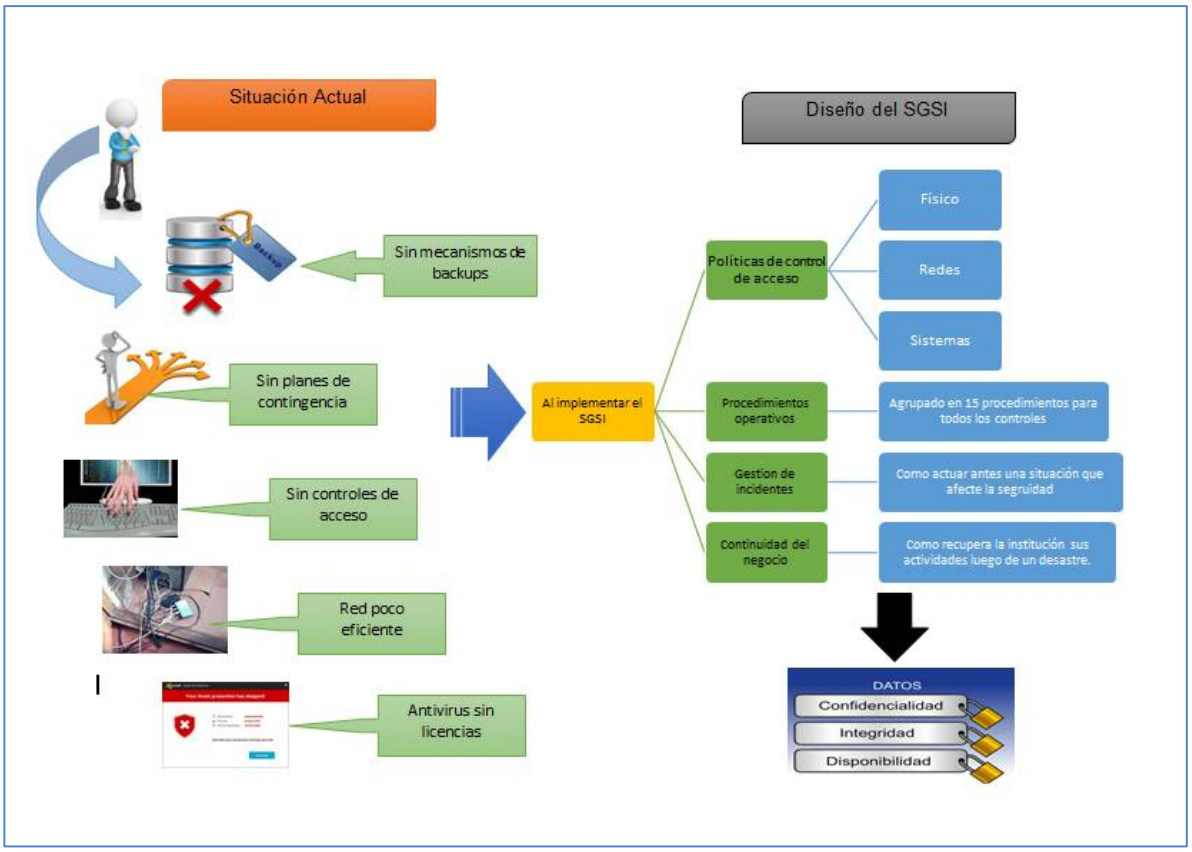


Figura Nº 13: Implementar el SGSI

Fuente: Elaboración propia

5.4.1.- Gestión de la seguridad de la información

A continuación, se presenta los roles y responsabilidades por parte del personal de la Institución.

5.4.1.1.- Comité de seguridad

Los representantes del comité de seguridad se detallan en la siguiente tabla Nº 20:

Área	Cargo
Gerencia	Gerente
Unidad de medicamentos	Coordinador de SISMED
Almacén	Responsable de almacén

Tabla Nº 20. Integrantes del Comité de seguridad

Fuente: Elaboración propia

Funciones:

- Informar la situación institucional en temas de seguridad de la información.
- Proponer la designación del Oficial de seguridad de la información.
- Revisar periódicamente el estado general de la seguridad de la información.
- Revisar y monitorear los incidentes de seguridad de la información.
- Revisar y aprobar los proyectos respecto a la seguridad de la información.
- Aprobar las modificaciones o nuevas políticas o controles relacionados a la seguridad de la información.

5.4.1.2.- Matriz de responsabilidades

Área	Rol	Nombre	Responsabilidades
Gerencia	Director de Comité de Seguridad	Anita Zevallos	▪ Quien preside el Comité de seguridad de la información.
Informática	Oficial de seguridad	Alex Chavez	▪ Definir y actualizar políticas, procedimientos definidos en el SGSI. ▪ Realizar el análisis de riegos a las aplicaciones. ▪ Asesorar en la aplicación de una metodología para el mantenimiento de los procedimientos de planes de contingencia y continuidad del negocio. ▪ Evaluar, seleccionar e implantar herramientas para facilitar la tarea de la seguridad de la información. ▪ Dar los lineamientos para los procedimientos de control de acceso a los sistemas de información. ▪ Promover en la Red de

			Salud de Lambayeque la formación, educación y el entrenamiento en seguridad de la información. ▪ Mantenerse actualizado respecto a nuevas amenazas y vulnerabilidades que se presenten. ▪ Recibir capacitaciones en el tema de seguridad de la información. ▪ Realizar pruebas de seguridad en todas las áreas de la institución.
Unidad de Medicamentos	Coordinador del Sismed.	Carlos Peña	▪ Miembro del comité de seguridad de la información, ayuda a coordinar que se cumplan los acuerdos del comité.

Tabla Nº 21. Matriz de responsabilidades

Fuente: Elaboración propia

5.4.2.- Política de control de acceso

Ámbito:

Controles de acceso físico de personas y acceso a los sistemas.

Roles y Responsabilidades:

- **Director de comité de Seguridad**
  - ✓ Aprobar condiciones de seguridad para todos los equipos que tengan información clasificada como confidencial.
  - ✓ Definir los niveles de seguridad para cada área, además de los controles adecuados para cada nivel.

- **Oficial de seguridad**
  - ✓ Habilitar los permisos para el acceso a las áreas donde se encuentras los equipos que hacen de servidores.
  - ✓ Actualizar el inventario de equipos informáticos y comunicaciones.

- ✓ Autorizar la creación de usuarios para el acceso a los equipos.

Reglas de la Política:

I. Para el acceso físico de las personas:

a) Personal

El personal de la Red de Salud de Lambayeque debe portar su identificación cuando estén dentro de la institución.

b) Visitas

Las personas externas a la institución que están de visita se les deben exigir una identificación y firma en la entrada.

c) Áreas que contienen información critica

- El acceso a las oficinas que contengan información muy importante deben estar físicamente restringido.
- El comité de seguridad debe definir los niveles de seguridad para cada área.

d) Accesos Revocados

Cuando un trabajador termina su vínculo laboral, sus permisos de acceso a las áreas de la institución deben ser revocados

e) Sala de computadoras y comunicaciones

Todo equipo informático que tenga información confidencial, debe estar configurado con las medidas de seguridad definidas en el Ministerio de Salud.

f) Personal autorizado

El director del comité de seguridad debe generar un listado del personal que trabaja en la institución para que solo éstos puedan tener acceso a las áreas de mayor importancia en información.

g) Señalización

Las áreas de mayor información primordial no deben ser anunciadas mediante señales en áreas de acceso público.

h) Identificación y traslado de equipos

- Todo equipo informático o de comunicaciones deben ser rotulados para su identificación.
- Todo traslado de equipos de cómputo o de comunicaciones debe estar autorizado por el responsable de informática y el gerente de la Red de Salud, y además se debe actualizar en el inventario.
- Los equipos ingresados de forma temporal por terceros deben ser anotados en un registro para su control de entrada, salida y usuario.
- Antes que un equipo sea dado de baja debe ser examinado por el responsable de informática y proceder a la eliminación de toda la información que contenga.

II.- Control de acceso a las redes

a) Política de utilización de los servicios de red.

Desarrollar procedimientos para activación o desactivación de derechos de acceso a redes. A continuación, se presenta lo siguiente:

- Controlar el acceso a los servicios de red interno y externo.
- Identificar redes y servicios de red a los cuales se permite el acceso.
- Establecer controles y procedimientos de administración para proteger el acceso y servicios de red

b) Identificación de equipos en la Red

- El responsable de informática controlará e identificará los equipos conectados a su red, mediante controlador de dominio, y un portal para la conexión wifi.

c) Diagnostico remoto

- Los trabajadores deben permitir el control remoto de sus equipos para dar cualquier soporte.

d) Control de conexión a redes

- **Conexión Inalámbrica:**

  Se restringirá totalmente el inalámbrico a los trabajadores salvo autorización del responsable de informática.

- **Conexión cableada:**

  Se restringirá el acceso a:

  - ✓ Correo electrónico, que no sea de la institución o autorizado.
  - ✓ Videoconferencia a través de internet.
  - ✓ Descarga de sitios per to per.
  - ✓ Conexiones a sitios streaming no autorizado.
  - ✓ Acceso a sitios de pornografía.
  - ✓ Servicios de escritorio remoto por internet.
  - ✓ Redes Sociales.
  - ✓ Cualquier otro servicio que vulnere la seguridad de la red o atente con la seguridad de la información de la institución.

III.- Para el acceso al Sistema Operativo

a) Registro de inicio seguro

- No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
- Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos.
- No mostrar las contraseñas digitadas.
- No transmitir la contraseña en texto claro.

b) Gestión de contraseñas

- No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
- No habilitar la opción “recordar clave en este equipo“, que ofrecen los programas
- No enviarla por correo electrónico
- Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.

- Selecciona contraseñas que no sean fáciles de adivinar.
- Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres predefinido.
- Cambia tus contraseñas regularmente.
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia etc.
- No utilizar contraseña con variables (soporte1, soporte2, soporte3, etc.)

5.4.2.- Procedimientos operativos para la gestión de TI

5.4.2.1.- Procedimiento para la seguridad de las oficinas, despachos y recursos

5.4.2.1.1.- Objetivo

Prevenir el acceso físico no autorizado, además de evitar daño o robo a los activos de la institución.

5.4.2.1.2.- Roles y Responsabilidades.

Este procedimiento es responsabilidad del responsable de informática.

5.4.2.1.3.- Control de acceso físico a las áreas seguras

Todos los sitios seguros en donde se encuentren sistemas de procesamiento informático o de almacenamiento, deben ser protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo y registro de entradas y salidas.

- **Aspectos a ser considerados:**

✓ Personal no autorizado puede llegar a tener acceso a las áreas restringidas.

- Personal de la Red de Salud, visitantes o terceras personas, que ingresen a un área definida como segura por la Red de Salud, deberán portar una identificación a la vista claramente que los identifique, además será intransferible.
- No deberá existir señales, ni indicaciones de ningún tipo sobre la ubicación de los centros de procesamiento de información.
- En caso de pérdida de llaves, deberán existir procedimientos que

garanticen que las mismas no podrán ser utilizadas por otras personas, como por ejemplo; el almacén.

- ✓ Equipos como fotocopiadoras, impresoras deben estar en áreas definidas por la Red de Salud como seguras, aplica también para equipos de red como switches, módems.
- ✓ Las puertas y ventanas deben estar cerradas

5.4.2.2.- Procedimiento para la seguridad de los equipos.

A continuación, se describe el procedimiento necesario cuando existe una amenaza por alguna falla que atente contra el buen funcionamiento de los equipos en la Red de Salud de Lambayeque.

5.4.2.2.1.- Procedimiento para la seguridad en las instalaciones de suministro.

Se deberá realizar lo siguiente:

- Inundación o falta de suministro
  - ✓ Las salas de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en un número suficiente como para detectar cualquier tipo de contacto de incendio.
  - ✓ Las cañerías de desagüe de dichas salas y ubicadas en el piso, deberán poseer las válvulas de retención de líquidos en flujo inverso a fin de que no sirvan como bocas de inundación.

- Interferencia eléctrica
  - ✓ El cableado de red de estar protegido contra interferencias, por ejemplo: canaletas que la protejan, además de un buen material del cableado bien revestido.
  - ✓ Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

- Se debe usar estabilizadores UPS o un UPS en general para toda la institución, probarlo según las recomendaciones del fabricante, de tal forma que garanticen el suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones.

- Se debe tener interruptores eléctricos adicionales, localizados cerca de las salidas de emergencia, para que se pueda realizar un rápido apagado de los sistemas en caso de falla o contingencia. Las luces de emergencia deben funcionar en caso se de una falla en la potencia eléctrica.

5.4.2.2.2.- Procedimiento para la seguridad del cableado.

- **Objetivo**

  Protección contra la intercepción o daños del cableado de energía y de telecomunicaciones.

- **Alcance**

  Planificación del servicio, diseño del servicio, ejecución del servicio.

- **Responsabilidad**

  El responsable de informática se encarga del procedimiento

- **Descripción del proceso.**
  - ✓ Las conexiones de potencia deben tener su propio pozo a tierra.
  - ✓ El cableado de red deberá ser protegido de cualquier intercepción o daño, como el uso de canaletas.
  - ✓ Los cables de potencia deben estar separados de los de telecomunicaciones de acuerdo a las normas técnicas.

5.4.2.2.3.- Procedimiento para el mantenimiento de equipos.

- **Objetivo**

  Indicar las actividades a seguir, cuando los equipos de cómputo de la Red de Salud de Lambayeque presentan alguna falla técnica o avería.

- **Alcance**

  Aplica a todas las áreas involucradas según el alcance del SGSI

- **Procedimiento de verificación de equipo**

  Cuando es solicitado un mantenimiento ya sea preventivo o correctivo, se debe ejecutar los siguientes pasos:

1.- Verificar la computadora en el sitio junto con el dueño o responsable del equipo en el momento en que es traída al área de informática.

2.- Llenar la siguiente información en una lista de verificación:

- ✓ Estado de la computadora.
- ✓ Deben estar a la vista los siguientes componentes:
  - Tarjeta de video
  - Tarjeta de Sonido
  - Lectora de DVD/CD
  - Unidades de disco o de USB
  - Tarjeta de red (alámbrica o inalámbrica)
- ✓ Luego debe de encenderse el equipo. En caso de que no lo haga, abrir el CPU y verificar que exista lo siguiente:
  - Placa
  - Disco Duro
  - Memoria RAM
  - Tarjeta de video
  - Otros componentes internos
- ✓ En caso de que faltase alguno, no recibir el equipo y reportarlo inmediatamente al responsable y a su jefe inmediato.
- ✓ Si no faltan componentes recibir el equipo.

- **Procedimiento de seguridad física**
  - ✓ Mantener el área de trabajo limpia.
  - ✓ Mantener las herramientas a utilizar de forma ordenada y en su lugar que le corresponde.
  - ✓ Verificar que lo cables de alimentación estén bien y que no tengan roturas.
  - ✓ No usar guantes de látex.
  - ✓ Cuando sopletee y use la aspiradora o limpie con alcohol isopropílico hágalo en un área ventilada.
  - ✓ Usar un cubre bocas cuando se haga el sopleteo y aspiración del equipo.
  - ✓ Evitar en lo posible respirar el polvo o el alcohol isopropílico porque puede ser perjudicial para la salud.

- ✓ Evitar tocar las áreas plateadas o doradas de los componentes de las tarjetas.

- **Procedimiento de seguridad lógica**
  - ✓ Verificar que el equipo encienda
  - ✓ Anotar la información de los controladores: video, sonido, red, etc.
  - ✓ Anotar los parámetros de la tarjeta de red: IP, DNS primario y secundario, puerta de enlace.
  - ✓ Anotar la información del nombre del equipo y grupo de trabajo.
  - ✓ Anotar la información de la impresora, nombre y controlador.
  - ✓ Anotar la información de los recursos compartidos, unidades de red.
  - ✓ Anotar el software usado por el usuario

- **Procedimiento de limpieza**
  - ✓ **Procedimiento de CPU y monitor**
    - Para el CPU use una franela y un limpiador de cubiertas de plástico antiestático.
    - Para el monitor usar aire comprimido para retirar el polvo interior.
    - Para los cables de alimentación usar una franela y alcohol isopropílico.

  - ✓ **Procedimiento de limpieza de los componentes principales**
    - Quitar la tapa del CPU. Cuando abrimos el CPU directamente y se manipula los circuitos directamente la descarga electrostática puede dañar los circuitos; para ello debemos descargarnos encima del CPU o usando una pulsera antiestática.
    - Identificar los componentes principales
    - Retirar de los slots la tarjeta de video y las demás tarjetas.
    - Desconectar los cables de alimentación y cables de las unidades.
    - Retirar el microprocesador, la pila y los módulos de memoria RAM.
    - Quitar las unidades de almacenamiento.
    - Con una goma blanda limpiar los contactos de todas las tarjetas incluyendo de las memorias; las tarjetas manipular de los extremos sin tocar los conectores plateados o dorados.

- La placa madre debe ser sopleteada con aire comprimido y aspirar al mismo tiempo para reducir la exposición del polvo.
- Aplicar en todas las tarjetas un limpiador de tarjetas electrónicas. En caso de no contar, usar alcohol isopropílico.

✓ **Procedimiento de la fuente de alimentación**

- Para limpiar la fuente, quitar la cubierta, y use aire comprimido para quitar todo el polvo en todos los circuitos y el ventilador.
- Aplicar el limpiador de tarjetas electrónicas
- Colocar la cubierta de la fuente de alimentación

✓ **Procedimiento de limpieza del teclado.**

- Debe de sopletear y aspirar el polvo de las teclas.
- Limpie tecla por tecla con limpiador para cubiertas de plástico antiestático con una franela.
- Evite desarmar todo el teclado y si lo hace, sólo debe desarmarse en el caso de que se haya introducido algún líquido pegajoso como un refresco, café u otro.

✓ **Procedimiento del armado del equipo**

- Ensamblar nuevamente los componentes, asegurando que la placa madre no tenga corto circuito con la carcasa.
- Verificar la conectividad de los circuitos de la placa y sus componentes para ver si hay paso de energía en todos los componentes.
- Encender el equipo y comprobar que funcione correctamente.
- En caso no arranque se usara los procedimientos de mantenimiento correctivo.

✓ **Procedimientos de mantenimiento correctivo**

▪ **Procedimiento para verificar fallas de alimentación de energía**

♦ Hacer una verificación de los cables de alimentación con un multímetro.

♦ Verificar los cables de alimentación estén bien conectados a la

fuente de alimentación.

- ♦ Verificar que la fuente este recibiendo energía eléctrica, para ello probarlo en la misma PC o por separado.
- ♦ Finalmente colocar la carcasa del CPU.

- **Procedimiento para verificar código de error al prender la PC**

  Se puede presentar los siguientes errores más importantes:

  - ♦ Un pitido largo: problema de memoria. Comprobar si se ha insertado correctamente los módulos de memoria en la placa madre.

5.4.2.2.4.- Procedimiento para la salida de activos fuera de las dependencias de la empresa

El uso de los equipos informáticos o cualquier software de la institución, fuera de las instalaciones de la misma, debe primero ser autorizado por la gerente de la Red de Salud de Lambayeque.

Se debe aplicar las siguientes acciones:

- No dejar los equipos desatendidos en una zona pública.
- Los equipos portátiles deben ser llevados en un maletín de mano, para evitar que sea muy vistoso.
- Se debe considerar las especificaciones que dan los fabricantes.
- Se debe considerar además tener un seguro contra robo o pérdida de cualquier equipo, así estaríamos asegurando el reemplazo inmediato de cualquier equipo.

5.4.2.2.5.- Procedimiento para equipo informático de usuario desatendido.

Se debe tener en cuenta lo siguiente:

- Los usuarios de la Red de Salud de Lambayeque deben mantener sus equipos de cómputo con controles de contraseña y protectores de pantalla, autorizados por el responsable de informática o la gerente de la Institución, cuando no se encuentren en su lugar de trabajo.

5.4.2.2.6.- Procedimiento para política de puesto de trabajo despejado y bloqueo de pantalla.

- Los puestos de trabajo deben estar limpios de cualquier tipo de papeles, o dispositivos de almacenamiento extraíbles.
- Cuando un equipo de cómputo esté desatendido después de un determinado tiempo debe bloquearse la pantalla.
- Los papeles y medios extraíbles deben estar en un armario bien asegurados sobre todo fuera de las horas normales de trabajo.
- La información más importante y crítica de la Red de Lambayeque debe estar asegurado en un armario resistente a un impacto y al fuego.

5.4.2.3.- Procedimientos de controles de red

- **Para el acceso a los usuarios a los recursos de la red.**
  - ✓ **Password y Login**
    - Determinar el tipo de cuenta de usuario.
    - Verificar la validez de la contraseña del usuario.
    - Usar adecuadamente las aplicaciones dentro del sistema.
    - Cerrar adecuadamente el Sistema.
  - ✓ **Límite de recursos**
    - Determinar los recursos disponibles en el sistema para desempeñar correctamente las labores diarias.
  - ✓ **Archivos compartidos**
    - Determinar la ubicación dentro del Sistema para compartir archivos como carpetas.
    - Identificar el tamaño y tipo de archivo para compartir.
    - Verificar los permisos y acceso para compartir los archivos en la Red interna.

- **Para seguridad en la Red**

  - ✓ **Cuentas de usuario**
    - Creación de cuentas con privilegios limitados para los usuarios de la Red de Salud.
    - Asignar una cuenta administrador con cifrado, solo para dar soporte y mantenimiento a los equipos de cómputo.

  - ✓ **Vulnerabilidad de la red**
    - Analizar con una herramienta informática como Wireshark los puntos críticos que proporcionen fácil acceso al sistema.
    - Evaluar alternativas físicas y lógicas disponibles para la seguridad en la red.
    - Establecer estrategias o procesos que se adapten mejor a la topología de la red.
    - Implementar dichas estrategias seleccionadas.
    - Realizar un monitoreo continuo de las actividades de la red.

5.4.2.4.- Procedimientos para intercambio de información.

- **Intercambio de información manual**

  - ✓ El intercambio de información manual con otras organizaciones externas, solo se debe utilizar correos autorizados en el Ministerio de Salud, controlar su eventual trazabilidad.

  - ✓ La entrega por mano, debe ser entregada personalmente al destinatario en un sobre sellado y además la entrega debe quedar registrada.

- **Intercambio vía correo electrónico institucional**

  - ✓ Toda información enviada desde la Red de Salud debe incluir en su pie de página, una advertencia en cuanto al uso y autorización al respecto, quedando bajo responsabilidad del receptor el cuidado de la información recibida.

  - ✓ La información debe ser encriptado para la protección de la información en los mensajes de correo.

- **Intercambio vía teléfono**

  - ✓ El intercambio de información sensible no se está permitido.

- **Intercambio vía acceso remoto**

  - ✓ Todo intercambio por este medio, debe cumplir con las políticas de control de acceso y procedimientos de seguridad de Red, establecidos en la Red de Salud de Lambayeque.

5.4.2.5.- Procedimiento para mensajería electrónica.

- No enviar correos electrónicos en cadena por motivo de que puede contener archivos maliciosos. Es preferible enviar correos electrónicos con copia oculta (CCO) a varios destinatarios.
- No hacer público el correo electrónico, debe ser privado.
- Utilizar cuenta de correo alternativas para el caso de que tenga que registrarse en sitios donde se puede recepcionar una determinada cantidad de spam.
- Utilizar el correo institucional solo para enviar y recibir información del trabajo, para evitar cualquier tipo de contaminación de los correos.
- No responder a los correos de tipo spam.
- Utilizar contraseñas seguras con un cifrado adecuado para el acceso a la cuenta de correo electrónico.
- No descargar archivos adjuntos si no se está seguro de la procedencia de los correos.

5.4.2.6.- Procedimiento de acuerdos de confidencialidad y secreto.

- Todos los trabajadores y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, que reflejan los compromisos de protección y divulgación de la información.

- Educar a los empleados sobre la política de la institución, referente a la revelación de información confidencial de valor para la Institución.

- Se debe revisar anualmente los requisitos para protección de la información dentro de los contratos de los trabajadores.

5.4.2.7.- Procedimiento para controles contra código malicioso.

- **Objetivo General**

  Contar con una plataforma de hardware y software que proteja la integridad y disponibilidad de la información y software que procesa en la red local de malware, troyanos y otros virus que atenten contra la integridad y disponibilidad de la información almacenada en estaciones de trabajo y cualquier otro medio magnético.

- **Alcance**

  Aplica a todos los procesos dentro del alcance del Sistema de Gestión de Seguridad de información de la Institución.

- **Descripción del procedimiento**

  ✓ Aplicar parches de seguridad al software que se utilice.

  ✓ Usar un software antivirus que trabajen en tiempo real y que sus componentes (programas, motor de búsqueda de virus y patrones de virus) puedan ser programados para su actualización de forma periódica.

  ✓ Usar un software anti troyano, programas especializados en la detección de troyanos de la PC, un tipo de código malicioso que trabaja de forma oculta al usuario robando información como cuentas bancarias, usuarios, contraseñas, etc.

  ✓ Usar un software firewall, programa especializado en el bloqueo del acceso a intrusos a nuestro equipo informático.

  ✓ Indicar a los trabajadores no instalar software no autorizado por la gerencia de la Institución y el responsable de informática.

  ✓ No descargar software ni aplicaciones desde Internet sin previa autorización del responsable de informática de la Institución.

- ✓ El área de informática debe estar suscrita a los boletines de alerta tanto del fabricante como del proveedor del antivirus, así como de los principales fabricantes de antivirus más usados del mercado a fin de recibir las recomendaciones de terceros en caso de ataques, además de poder diferenciar y saber sobre las nuevas amenazas y/o virus falsos de cada día.

- ✓ La herramienta de Antivirus que se implemente en la institución debe ser corporativo y por ende debe ser instalado en todas las estaciones de trabajo, servidores, y otros dispositivos ya sea móviles o fijos. Cualquier equipo informático que no cuente con la protección del antivirus no podrá ser conectado a la Red de la Institución.

- ✓ El antivirus debe instalarse solo en equipos de cómputo que cumplan con los requerimientos mínimos de instalación para que el programa pueda correr y desarrollarse con normalidad. En caso no cumple este no podrá conectarse a la Red de la Institución.

- ✓ En el caso de que un usuario detecte un código malicioso, paralelo a que el antivirus emita una alarma, debe avisar inmediatamente al encargado de informática para que pueda dar una solución rápida y eficaz.

5.4.2.8.- Procedimiento para copias de seguridad.

- **Objetivo**

  Definir el procedimiento de aplicable a la generación de copias de seguridad de la información.
- **Ámbito de aplicación**
  - ✓ Este procedimiento es de aplicación a todo el alcance definido para el SGSI.
  - ✓ El presente procedimiento es de aplicación y de cumplimiento para todo el personal de la Institución según e alcance del SGSI.
- **Descripción del procedimiento**

  Se debe seguir las siguientes actividades:
  - ✓ Determinar o identificar el número de aplicaciones y/o base de datos,

servidores para el respaldo.

- ✓ Determinar los mecanismos de copias de seguridad según la información y/o servidores a respaldar, automático o manual.
- ✓ Si el backup es de forma automática, especificar la fecha de creación de la base de datos.
- ✓ Comprimir los archivos en caso la copia se realice correctamente.
- ✓ Verificar las copias que se comprimieron para verificar si se pueden descomprimir en caso se necesite.
- ✓ Realizar una copia de seguridad completa en un medio de almacenamiento externo todos los viernes a las 4:30 pm del Sistema SISMED.
- ✓ Realizar una copia de seguridad completa en un medio de almacenamiento externo cada viernes a las 4:30 pm Sistema Operativo y archivos de las PCS de la Institución.
- ✓ Para realizar las copias de seguridad se usará el software Acronis.

- **Ciclo de vida del proceso**

  Se usará el PHVA.

  - ✓ Estrategia del proceso: Ubicación de la información.
  - ✓ Diseño del proceso: Diseñar el proceso de backups, y diseño de manuales.
  - ✓ Transición del proceso: Capacitación a los trabajadores.
  - ✓ Operación del proceso: Implementación de backups.

- **Lineamientos de la implementación**

  - ✓ Definir el nivel necesario de respaldo de la información.
  - ✓ Producir registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración.
  - ✓ La extensión (respaldo completo o diferencial) y la frecuencia de los respaldos debe reflejar los requerimientos de la institución.
  - ✓ Las copias de seguridad se deben almacenar en un lugar apartado, lo suficiente como para evitar cualquier desastre en la Institución. Sería bueno que un fuera externo a la Institución.
  - ✓ A la información de respaldo se le debe de dar una protección física y un ambiente apropiado.
  - ✓ Los medios de respaldo se deben probar regularmente para asegurar

la confianza en ellos, para usarlos cuando sea necesario en caso haya una emergencia.

- ✓ Los procedimientos de restauración se deben verificar y probar regularmente para asegurar su efectividad.

5.4.2.9.- Procedimiento de registro y gestión de eventos de actividad.

- **Sincronización del reloj**

  Los relojes de todos los sistemas deber ser sincronizados para asegurar la consistencia de todos los registros de la auditoria.

- **Responsabilidades**

  Los administradores o informáticos encargados de los sistemas deben realizar un monitoreo periódico de los sistemas como parte de la rutina diaria de trabajo al finalizar sus labores. El monitoreo no se basara solo a la utilización del sistema sino también al acceso de los usuarios al sistema.

- **Descripción del procedimiento**
  - ✓ La actividad de los usuarios que esté relacionada al acceso de información confidencial deberá ser registrada para luego realizar una verificación de la misma. El propietario de la información debe revisar el registro de forma mensual.
  - ✓ Los eventos de seguridad más importantes de una computadora deben ser registrados en un log de eventos de seguridad.
  - ✓ Un evento a registrar puede referirse a: autenticación, modificaciones en los datos, utilizar cuentas privilegiadas, cambios en la configuración para acceder a archivos, modificación en el sistema operativo o algún programa/ aplicación instalados, cambios en los privilegios o permisos de los usuarios, o el uso de cualquier función con privilegios en el sistema.
  - ✓ Los “logs” deben ser almacenados por un periodo mínimo de 4 meses.
  - ✓ El acceso a los “logs” debe ser solo a personal autorizado, en este caso por los administradores o informáticos de los sistemas instalados o si en algún momento lo requiera solicitar los

propietarios de la información.

- ✓ Los logs deben ser almacenados en medios de solo lectura por una medida de seguridad.

5.4.2.10.- Procedimiento para controles de auditoria de sistemas de información.

Este procedimiento involucra:

- La evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.

1.- Solicitar la información a las áreas respectivas de la institución:

- Recursos y materiales.
  - ✓ Estudios de viabilidad.
  - ✓ Número de equipos, localización y características.
  - ✓ Fechas de instalaciones de equipos.
  - ✓ Configuración de los equipos y capacidades actuales y máximas.
  - ✓ Ubicación general de equipos.
  - ✓ Políticas de uso de equipos.
- Sistemas**:** Descripción de los Sistemas instalados.
  - ✓ Manual de procedimiento de los sistemas.
  - ✓ Diagramas de entrada, archivos, salidas.
  - ✓ Fechas de instalación de los sistemas.

2.- Evaluación de sistemas de información

Las características que deben evaluarse en los sistemas son:

- Dinámicos, susceptibles a modificarse.
- Integrados, que habrá sistemas que puedan ser interrelacionados y no estar aislados.
- Accesibles, es decir que estén disponibles.
- Necesarios, que pruebe su utilización.
- Comprensibles, que contengan todos los atributos.
- Oportuno, que esté la información cuando se requiere.
- Funcionales, que proporcionen la información correspondiente al área que lo solicita.
- Seguros, que solo las personas autorizadas tengan acceso al sistema.

3.- Procedimiento de respaldo del sistema ante desastres.

- Los sistemas deberán ser probados y utilizados en condiciones anormales, para asegurarse que funcione en situaciones de emergencia.

4.- Software de sistema

- Verificar la legalidad del software utilizado.
- Verificar la existencia y actualización de la documentación del sistema.

5.- Seguridad en aspectos técnicos de la aplicación.

- Verificar la existencia de controles de acceso al sistema
- Solicitar los manuales técnicos, de operación y comprobar que estén actualizados.
- Evaluar los procedimientos de backup a la aplicación.
- Comprobar que los usuarios del sistema no puedan modificar los programas fuente de la aplicación.
- Comprobar que el uso de la computadora solo se lleve a cabo por personal autorizado.
- Revisar los procedimientos relacionados con la seguridad física y lógica de los datos transmitidos.
- Revisar las políticas de seguridad que están relacionadas con el sistema operativo.

5.4.2.11.- Procedimiento de control de acceso a redes y servicios asociados.

- **Utilización de los servicios de red.**

  Se desarrollarán procedimientos para la activación de los derechos de acceso.

  - ✓ Controlar el acceso a los servicios de red
  - ✓ Identificar las redes y servicios a los cuales se tendrá acceso los usuarios.

- **Identificación de equipos en la Red.**

  El responsable de informática controlará e identificará los equipos conectados a la red, mediante uso de controladores de dominio, asignación manual de IP.

- **Separaciones de redes.**
  - ✓ Se plantea el uso de firewall para controlar el acceso de una red a otra, para tal caso se tomará en cuenta la de un hardware marca fortinet.
  - ✓ Se plantea el uso de VLANS para la segmentación en los equipo de diferentes sedes, ejemplo: red de salud y centros de salud, micro redes y otras redes.

- **Protección de los puertos de configuración y diagnostico remoto.**
  - ✓ Los puertos que permitan realizar mantenimiento o dar soporte remoto a los equipos de red, servidores, equipos de usuario final, estará restringido al responsable de informática.
  - ✓ Los usuarios deberán permitir el acceso remoto de sus equipos para el área de informática de la Red de Salud de Lambayeque o al área de informática de la Gerencia Regional de Salud. Se recomienda no tener información sensible o confidencial a la vista y no dejar desatendido el equipo mientras se dé el acceso remoto.

- **Control de conexión de las redes**

  No se tendrá en cuenta seguridad WIFI debido a que está restringido el uso de una red inalámbrica dentro de la institución como política de seguridad.

  Dentro de la Red se realizará las siguientes restricciones de acceso:

  - ✓ Mensajería instantánea.
  - ✓ Videoconferencias por internet.
  - ✓ Correo electrónico comercial que no esté autorizado por la Institución.
  - ✓ Conexiones a sitios de streaming no autorizados.
  - ✓ Descargar archivos peer to peer.
  - ✓ Cualquier otro sitio que vulnere la seguridad de la red.

5.4.2.12.- Procedimiento para la gestión de altas, bajas de registro de usuarios.

- **Solicitud de alta y/o baja de Usuarios.**

  Para la solicitar el alta o baja el responsable de informática enviará un correo al área de informática de la Gerencia de Salud de Lambayeque para autorizar la creación de usuarios o la baja de los mismos, adjuntando los datos necesarios para la creación.

  Se propone la creación de un formato de formulario, que contenga lo siguiente en los 2 casos.

  ✓ **Alta de Usuario:**

  - Alta.
  - Sistema SISMED.
  - Dependencia: CS (Centro de Salud), PS (Puesto de Salud).
  - Cargo.
  - Nombres y apellidos completos del usuario.
  - DNI.
  - Correo electrónico
  - Teléfono
  - Funciones a realizar

  ✓ **Baja de Usuario:**

  - Sistema SISMED.
  - Dependencia: CS (Centro de Salud), PS (Puesto de Salud).
  - Cargo.
  - Nombres y apellidos completos del usuario.
  - Indicar que cuenta se dará de baja.

- ✓ **Desbloqueo de Usuario:**

  - Sistema SISMED.
  - Dependencia: CS (Centro de Salud), PS (Puesto de Salud).
  - Cargo.
  - Nombres y apellidos completos del usuario.
  - Indicar que cuenta se desbloqueará.

5.4.2.13. Procedimiento de retirada o adaptación de los derechos de acceso.

Los derechos de acceso de todos los empleados y/o contratistas de la información e instalaciones de informática serán retirados en el momento de retiro de su empleo y/o terminación de contrato.

5.4.2.14. Procedimiento de restricción de acceso a la información

Para la generación de cuentas de usuario en los sistemas, así como la asignación de perfiles, el informático de la red de salud de Lambayeque es el responsable de enviar las solicitudes de usuarios y perfiles de acceso al informático de la Gerencia Regional de Salud.

Se otorgará el acceso a los usuarios solo a la información mínima necesaria para la realización de sus actividades diarias.

Se puede utilizar las siguientes estrategias:

- Seguridad lógica de la aplicación.
- Restringir el acceso a línea de comando.
- Los permisos en los archivos que sean de solo lectura.
- También se recomienda la aplicación de directivas de grupo de local.

5.4.2.15. Procedimiento de gestión de contraseñas de usuario.

- **Disposiciones generales:**
  - ✓ Todas las claves a nivel de usuarios finales, deben ser cambiadas cada 60 días para todos los usuarios.
  - ✓ Todas las contraseñas a nivel administrador deben ser cambiadas cada 60 días.
  - ✓ Se deshabilitarán las cuentas por defecto, que estén configuradas en los sistemas.

- **Directrices**

  Directriz para construcción de contraseñas
  - ✓ La contraseña debe contener por lo menos tres tipos de caracteres:
    - Letras mayúsculas
    - Letras minúsculas
    - Números
    - Signos de puntuación.
    - Caracteres especiales (@, #, &, %, <>, etc.)
  - ✓ La contraseña debe tener una longitud mínima de 8 caracteres para usuarios y de 10 para administradores.
  - ✓ No se debe utilizar contraseñas que contengan las siguientes características:
    - Contraseñas que estén basadas en palabras del diccionario.
    - Palabras de uso común: información personal como fechas de cumpleaños, nombres de familiares, mascotas, amigos, direcciones, patrones de letras o números (lia1234).
  - ✓ Se debe crear claves que deben ser fácilmente recordadas por el usuario únicamente.

- **Estándares de protección para accesos no autorizados**
  - ✓ Todas las claves se deberán tratar como información confidencial, el único responsable de la clave será el usuario final.
  - ✓ Se deberá configurar un bloqueo automático de sesión en un equipo de usuario final luego de 30 minutos de sesión inactiva en sistema o aplicaciones.
  - ✓ Se recomienda que las claves que son utilizadas para los sistemas sean

diferentes a las que se usan en aplicaciones de acceso personal, como cuentas de correo, cuentas de almacenamiento en la nube como dropbox.

- ✓ No compartir la credencial de acceso con ningún personal, ya sea asistente o algún reemplazo.
- ✓ Las contraseñas de los usuarios que salgan de la institución por renuncia, licencia de salud o estudios, o alguna ausencia prolongada, no deberá ser proporcionadas a otros usuarios internos de la Institución. Estos usuarios deberán ser desactivados.
- ✓ No revelar las contraseñas vía correo electrónico, vía telefónica o cualquier otro medio que solicite información.
- ✓ No recordar las contraseñas en las aplicaciones o navegadores.
- ✓ Para cualquier tipo de acceso y para cualquier usuario se debe configurar que al tercer intento fallido de inicio de sesión se bloquee el acceso al sistema y solo el informático de la institución podrá reportarlo a través de un informe a la Gerencia Regional de Salud para su desbloqueo.
- ✓ Se debe configurar en el sistema una opción para que el usuario en su primer inicio de sesión pueda resetear la clave.

- **Restauración de contraseñas**
  - ✓ La restauración de contraseñas será solicitada vía correo electrónico o personalmente a través del informático de la Red de Salud para que solicite la autorización al área de informática de la Gerencia Regional de Salud con un respectivo sustento del motivo.
  - ✓ Esta solicitud será evaluada y en un plazo de 24 horas como máximo se habilitará la nueva clave para que el mismo usuario la resetee en el inicio de sesión.

5.4.3.- Procedimiento para gestión de incidentes

5.4.3.1.- Objetivo

Establecer las actividades necesarias en la Red de Salud de Lambayeque, para la detección oportuna y tratamiento de situaciones o eventos que comprometan la seguridad de los activos de información.

5.4.3.2.- Alcance

Área de Informática, Almacén, Estrategias Sanitarias, SISMED.
Incidentes de Seguridad que afecten a los activos de información de los siguientes tipos: base de datos, documentos, equipo informático, infraestructura física, personal, sistema de información, software, respecto a;

- Confidencialidad, para el acceso no autorizado a la información.
- Integridad, modificación sin autorización, destrucción o pérdida de la información.
- Disponibilidad, es decir sin acceso a la información.

El procedimiento es aplicable a los funcionarios nombrados, contratados, personal a honorarios (servicio de terceros y snp) que presten servicios en las áreas: Informática, Almacén, Estrategias Sanitarias, SISMED de la Red de Salud de Lambayeque.

5.4.3.3.- Desarrollo del Procedimiento

5.4.3.3.1.- Responsabilidades

- **Funcionarios:** Informar acerca de cualquier situación o evento que pueda afectar a la seguridad de la información.

- **Responsable de Informática:** Responsable de aplicar este procedimiento, gestionar las situaciones o eventos e incidentes de seguridad de la información.

5.4.3.3.2.- Reporte de eventos y debilidades en la Seguridad de la Información.

1.- Todo personal de la red según el alcance del SGSI en coordinación con la jefatura de cada área es responsable de notificar cualquier tipo de evento que pueda afectar al normal funcionamiento del Sistema de Seguridad de la Información de la Institución.

2.- La notificación se hará de manera personal, vía telefónica o por correo electrónico, al responsable de informática, quien registrará el evento.

3.- Según el impacto del incidente o evento del Sistema de Información debe contactar con la persona que reporta y Jefatura de área en un plazo no menor de 24 horas para recolectar toda la información necesaria para el análisis del evento.

4.- Una vez hecha la recolección de información sobre el incidente, el responsable de informática debe analizar los antecedentes. El resultado del análisis puede tener las siguientes opciones:

- El evento no es una amenaza: Se cierra el registro de eventos, informando a la persona que lo reporto.
- El evento es una debilidad: Se coordina las actividades para la mitigación con los activos que están comprometidos, el área que corresponde y el responsable de informática.
- El evento se dio y debe ser gestionado como un incidente: Se activa el procedimiento de incidente de seguridad de la información.

5.4.3.3.3.- Gestión de incidentes de seguridad de la información

- ✓ **Registro y Clasificación del Incidente**

Registro: El responsable de informática debe registrar el incidente y su tratamiento en un documento de registro de incidentes.

Clasificación: El responsable de informática debe clasificar el incidente, de acuerdo al origen, tipo y el nivel de criticidad.

A continuación, se muestra los tipos de incidente en la tabla Nº 22:

Tipo de incidente:

Tipo	Descripción	Ejemplos
Informático	Todos los incidentes que comprometan o afecten a la infraestructura tecnológica.	▪ Denegación de servicios informáticos. ▪ Fallas en el sistema de información. ▪ Códigos maliciosos por algún por algún tipo de virus. ▪ Accesos no autorizados a los Sistemas de información. ▪ Fallas en la infraestructura tecnológica.
No informático	Todos los incidentes que no se menciona en el punto anterior.	▪ Vulneración a la confidencialidad, integridad y disponibilidad en algún documento. ▪ Incidentes ocasionados por la naturaleza. ▪ Acceso físico no autorizado.

Tabla Nº 22. Tipo de incidente

Fuente: Elaboración propia

A continuación, se muestra los niveles de criticidad en la siguiente tabla Nº 23:

Nivel de Criticidad:

Parámetro	Descripción	Variables
Impacto	Importancia del incidente	• Bajo: No interrumpe los procesos críticos, solo afecta a un usuario. • Medio: Interrumpe por un momento los procesos y afecta a más de un usuario, por los menos 4. • Alto: Interrumpe gravemente los procesos de la Red de Salud y afecta a más de 4 personas
Urgencia	Tiempo máximo que el proceso puede aceptar para resolver el incidente.	• Bajo: Mas de 1 hora • Medio: Entre 10 a 60 minutos • Alto: Menos de 10 minutos.

Tabla Nº 23. Nivel de criticidad

Fuente: Elaboración propia.

✓ **Escalamiento**

Si el responsable de informática junto con la gerencia determina que el incidente necesita un tratamiento especial, deberán proceder con la mayor rapidez posible.

Cada vez que se registra un incidente el responsable de informática debe resolverlo de acuerdo a la clasificación del incidente; en caso no pueda resolverlo porque le corresponde a otra área, se realizará un escalamiento interno o externo.

El criterio principal del escalado es el de la transferencia a una persona de soporte que tenga lo siguiente:

- ✓ Mayor conocimiento o experiencia.
- ✓ Recursos para solucionar problemas más complejos.
- ✓ Mayor cargo para la toma de decisiones

Dependiendo el tipo de incidente los responsables para ejecutar y dar la respuesta inmediata son los siguientes:

Tipo de activo presente en el incidente	Responsable de la respuesta inmediata
Sistema del SISMED	Responsable de informática
Otros Sistemas	
Software	
Equipos de TIC	
Base de datos	
Correo electrónico	
Documentos	Área donde se desarrolla el proceso
Informes	
Personal	Coordinador de RRHH

Tabla Nº 24. Responsables de la Gestión de incidentes

Fuente: Elaboración propia

- **Proceso Disciplinario**

Si el incidente fuera de mayor gravedad o se considera algún delito, se pide asesoría a la Región de Salud, al área donde ven temas legales para el tratamiento correspondiente.

Si en caso existieran responsabilidades administrativas, el responsable de la respuesta inmediata solicitará a quien corresponda la aplicación de un proceso disciplinario según la ley de procesos administrativos.

Cuando el incidente involucre a un personal contratado por servicio por terceros u honorarios, se evaluará permanencia de su contrato o en dado caso el término del mismo.

- **Continuidad del Negocio**

En caso el incidente no se pueda resolver y ponga en riesgo las operaciones del proceso critico de negocio de la institución entonces la gerencia junto con el responsable de informática evaluará la activación de los procesos de continuidad de negocio, visto en el próximo tema.

- **Recolección de Evidencia**

La recolección de la evidencia es responsabilidad del responsable de informática de la Red de Salud de Lambayeque. Para esto debe tomar las siguientes acciones:

✓ **Para documentos en papel:**

El original debe ser guardado de forma segura, indicando en un registro que persona, donde cuando se encontró el documento.

✓ **Para información sobre medios informáticos:**

- Las imágenes o copias de cualquier medio extraíble, o disco duro deben ser resguardadas para asegurar la disponibilidad de la misma.
- Esta evidencia debe ser analizada por el responsable de informática, de no poder hacer deberá elevarla a soporte que sería el responsable de informática de la Región de Salud por ser la que está encima en la jerarquía.

- **Comunicación**

Una vez controlado el sistema, el responsable de informática debe informar a los que estuvieron involucrados en el incidente.

- **Cierre del incidente**

El responsable de informática debe hacer lo siguiente:

✓ Realizar un análisis de las causas del incidente.

✓ Si el incidente aún no ha sido resuelto, implementar un plan adecuado y definir el plazo para su implementación.

✓ Registra el incidente.

✓ Una vez que se cierra el incidente, elaborar un informe de Incidentes de seguridad de información.

5.4.3.4.- Documentos aplicables

- ISO IEC 27035
- Ley del Procedimiento administrativo General 27444
- ISO 27001:2013

5.4.3.5.- Indicadores

Fórmula de Cálculo	Periodo de cálculo de indicador	Evidencia	Supuestos
Número de incidentes de la categoría Denegación de servicios/ Total de incidentes registrados	1 mes	Procedimiento gestión de incidentes de seguridad de la información. Registro de incidentes de seguridad.	Deben existir incidentes dentro del periodo.
Número de incidentes de la categoría código malicioso/total de incidentes registrados.	1 mes	Procedimiento gestión de incidentes de seguridad de la información. Registro de incidentes de seguridad.	Deben existir incidentes dentro del periodo.
Número de incidentes de la categoría fallas del sistema de información/ total de incidentes registrados.	1 mes	Procedimiento gestión de incidentes de seguridad de la información. Registro de incidentes de seguridad.	Deben existir incidentes dentro del periodo.
Número de incidentes de la categoría de violaciones a confidencialidad, integridad y disponibilidad (documento)/ total de incidentes registrados.	1 mes	Procedimiento gestión de incidentes de seguridad de la información. Registro de incidentes de seguridad.	Deben existir incidentes dentro del periodo.
Número de incidentes de la categoría accesos no autorizado a los sistemas de	1 mes	Procedimiento gestión de incidentes de seguridad de la información. Registro de	Deben existir incidentes dentro del periodo.

información/total de incidentes registrados		incidentes de seguridad.	
Número de incidentes de la categoría Infraestructura tecnológica TI/ total de incidentes registrados.	1 mes	Procedimiento gestión de incidentes de seguridad de la información. Registro de incidentes de seguridad.	Deben existir incidentes dentro del periodo.

Tabla Nº 25. Indicadores

Fuente: Elaboración propia

5.4.4.- Procedimientos de la continuidad del negocio

Plan de continuidad de negocio

5.4.4.1. -Objetivo

El objetivo del Plan de continuidad del negocio es definir de forma precisa cómo la Red de Salud de Lambayeque gestionará los incidentes en caso de un desastre o de otro incidente disruptivo y cómo recuperará sus actividades dentro de plazos establecidos. El objetivo de este plan es mantener en un nivel aceptable el daño producido por un incidente disruptivo.

5.4.4.2.-Alcance

Este plan se aplica a todas las actividades críticas dentro del alcance del Sistema de gestión de seguridad de la información (SGSI). Los usuarios de este documento son todos los trabajadores, tanto internos como externos, que cumplan una función en la continuidad del negocio.

5.4.4.3.-Conceptos básicos

- **Administración de plan de Continuidad de Negocios:**

Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio.

- **Problema de continuidad de negocio:**

Es un evento interno o externo que interrumpe uno o más de los procesos de negocio. El tiempo de la interrupción determina que una situación sea un incidente o un desastre.

✓ **Planes de contingencia:**

Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

✓ **Plan de Continuidad de Negocio:**

Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

✓ **Plan de recuperación de desastres:**

Es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.

✓ **Análisis de impacto de negocio:**

Es la etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción.

5.4.4.4.- Causas de interrupción

Los planes de contingencia se definen en base a las causas de las posibles interrupciones que se puedan presentar en la continuidad de una empresa o negocio. A partir de estas causas es donde se deben tomar las acciones pertinentes del caso.

Se podrían presentar en los siguientes casos:

a) Ausencia de personal:

Se presenta cuando el funcionario, responsable del proceso no puede asistir a trabajar para cumplir con sus actividades propias a su cargo.

b) No acceso al sitio normal de trabajo:

Se presenta cuando por algún evento como desastre natural, enfermedad contagiosa, huelgas, problemas de transporte, etc., el personal no puede acceder a su centro de trabajo para desarrollar sus actividades propias a su cargo. Para este caso y con la finalidad de no interrumpir con el proceso crítico de negocio, se debería contar con algún sitio alterno para continuar con las labores.

Tomando en cuenta la Red de Salud de Lambayeque puede ser suministrada por la misma entidad o la que esté directamente responsable que sería la Gerencia Regional de Salud de Lambayeque.

c) Caída de los Infraestructura tecnológica:

Se presenta cuando el hardware o software que soporta los proceso presenta fallas, también se pueden presentar interrupciones en las comunicaciones provocadas por datos corruptos, fallas en algún componente, aplicaciones o error humano.

d) No contar con los proveedores externos:

Se presenta cuando una o varias actividades de un proceso crítico son realizadas por el proveedor y cualquier falla en éste, generaría la no realización efectiva del proceso. Para el caso de la Red de Salud de Lambayeque se le considera proveedor al almacén especializado de la Gerencia Regional de Salud de Lambayeque quien provee de insumos al almacén de la Red de Salud para su oportuna distribución a los puestos y establecimientos de Salud a los cuales pertenece, por lo que la Gerencia deberá contar con un Plan de Continuidad de Negocio que asegure el normal funcionamiento de estas actividades.

5.4.4.5.- Gobierno de Continuidad

- **Lineamientos**

El objetivo de la administración de continuidad del negocio es planificar las acciones necesarias para responder de forma adecuada ante un incidente de trabajo, desde el momento en que se declare la contingencia hasta la vuelta a la normalidad, de forma que se reduzca al mínimo su impacto sobre el negocio.

Los lineamientos se sustentan en un conjunto de principios que han sido formulados basándose en las necesidades del negocio y en el entendimiento de los riesgos asociados, ellos son:

- ✓ El plan de continuidad de negocio está orientado a la protección de las personas, así como al restablecimiento oportuno de los procesos, servicios críticos e infraestructura, frente a eventos de interrupción o desastre.

- ✓ Todo el personal de la Entidad debe estar entrenado y capacitado en los procedimientos definidos y conocer claramente los roles y responsabilidades que le competen en el marco de la continuidad del negocio, mediante labores periódicas de formación, divulgación y prueba de los Planes de Contingencia del Negocio.

- ✓ La Gerencia de la Red de Salud debe designar un Líder de Plan de Continuidad de Negocio, quien será el encargado de apoyar las actividades del Programa de Plan de Continuidad de Negocio.

- ✓ Los planes de contingencia deben mantenerse actualizados, por lo tanto se deben desarrollar, probar y mejorar de forma periódica, o si existen cambios en procesos, políticas, tecnología, personas, donde es necesario que en lats revisiones participen las áreas involucradas.

- **Normas Externas**
  - ✓ **RM 28-2015-PCM:** Lineamientos para la gestión de la continuidad operativa de las entidades públicas en los tres niveles de gobierno.
    Las entidades públicas en los tres niveles de gobierno, integrantes del Sistema Nacional de Gestión del Riesgo de Desastres, implementan la Gestión de la Continuidad Operativa, adecuándola a su alcance y a la complejidad de sus operaciones y servicios, bajo responsabilidad de la máxima autoridad de las mismas.

  - ✓ **Ley N° 29664** Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD) donde se encuentra el Ministerio de Salud.

5.4.4.6.- Estructura de la Gestión de la Continuidad del Negocio

Para asegurar una adecuada administración de la continuidad de negocio se estableció una estructura, que incluye la definición de los roles y responsabilidades.

La administración está conformada por:

5.4.4.6.1.- Comité de Gestión de Continuidad

La gestión de la continuidad del negocio requiere de una de una estructura organizacional encargada de promover los lineamientos necesarios para un óptimo desarrollo. Los integrantes del comité de continuidad son los mismos del comité de gestión de seguridad de la información.

.

A continuación, se mencionan los integrantes del comité:

Comité de Gestión de Continuidad	Roles de contingencia
Gerente de Institución, quien preside el comité.	Director de comité de seguridad.
Responsable de Informática.	Oficial de seguridad
Coordinador de SISMED.	Coordinador de SISMED

Tabla Nº 26. Comité de Gestión de continuidad

Fuente: Elaboración propia

- **Roles y Responsabilidades**

A continuación, se describen los roles y responsabilidades de los integrantes del comité para el plan de continuidad.

- **Director de Comité de seguridad**

El director del comité de seguridad es el encargado de dirigir y liderarlas actividades del plan de continuidad del negocio. Es responsable de declarar la contingencia ante el escenario de interrupción del lugar de trabajo.

Responsabilidades:

- Delegar de manera expresa en el Comité de Continuidad de Negocio, además de la responsabilidad de actualizar mantener y probar el plan de continuidad con orientación del informático de la Red de Salud.
- Evaluar y aprobar los recursos requeridos para establecer y mantener la estrategia de recuperación y contingencia de la institución.
- Liderar las reuniones del Comité de Gestión de Continuidad.
- Monitorear los reportes sobre el estado de recuperación o evaluación durante una contingencia.
- Velar por la seguridad del personal que actúa en el área del evento.
- Establecer los objetivos de recuperación y activar el plan de continuidad ante el escenario de interrupción de lugar teniendo en cuenta el resultado de la evaluación.
- Velar por la ejecución del debido análisis de las causas que ocasionan la contingencia.

- **Oficial de seguridad de la información**

Es la persona encargada de liderar la recuperación de la tecnología, basados en las estrategias de continuidad implementadas.

Responsabilidades:

- Liderar la recuperación tecnológica, basados en las estrategias de continuidad implementados.
- Identificar los posibles riesgos de aspectos tecnológicos que afectan la continuidad de la operación normal de la Entidad.
- Entregar los reportes correspondientes al Comité de Gestión de Continuidad sobre el estado de recuperación.
- Velar por la actualización de la estrategia tecnológica en los casos de: cambio o actualización de aplicaciones, cambio de roles y responsabilidades, etc.
- Velar por la realización de las pruebas del plan de continuidad y revisar los resultados obtenidos de las mismas.

- **Coordinador de Sismed**

  Responsable de liderar la recuperación de los procesos de negocio crítico, basados en estrategias de contingencia.

  Responsabilidades:

  - Liderar reuniones del equipo de recuperación, para diagnosticar y evaluar las interrupciones que afectan al desarrollo normal de los procesos.
  - Ejecutar los planes de contingencia ante un incidente presentado.
  - Mantener la comunicación constante durante un estado de contingencia.
  - Velar por la realización de pruebas del plan de continuidad y revisar los resultados obtenidos.
  - Entregar los reportes al Comité sobre el estado de la recuperación de sus áreas.

5.4.4.7.- Elementos que conforman la administración del plan de continuidad del negocio

Está conformado por los siguientes elementos:

- Planes de Contingencia de Proceso:
  Que abarca los escenarios de la falta de personal, disponibilidad del lugar de trabajo, y no contar son los proveedores críticos para el negocio.

- Planes de recuperación de desastres:
  Abarca las diferentes estrategias definidas para la recuperación de los sistemas.

- Plan de continuidad del Negocio:
  Se definen los procedimientos y estrategias para asegurar la reanudación oportuna y eficiente de los procesos de negocio.

5.4.4.8.- Fase de Administración del plan de continuidad del negocio

Se conocen las necesidades reales de la Institución y sobre esto se desarrollan los diferentes mecanismos de prevención ante incidentes o desastres.

Sus etapas son las siguientes:

- **Etapa de análisis de negocio y evaluación de riesgos**

Para desarrollar un plan de continuidad con éxito, primero es conocer cuáles son los procesos de negocios primordiales dentro de la institución.

- **Análisis de Impacto de Negocio:**

  - ✓ Determinar los procesos críticos de negocio.
  - ✓ Obtener relación de procesos.
  - ✓ Obtener relación de aplicaciones.
  - ✓ Tiempo de recuperación de cada objetivo.

- **Análisis de Riesgos:**

  El objetivo de éste análisis es manifestar aquellas debilidades que por su importancia pueden poner en marcha antes de lo pensado el plan de recuperación del negocio.

  Pasos para el análisis:

  - ✓ Identificar las amenazas físicas y los controles de seguridad.
  - ✓ Análisis de vulnerabilidad.
  - ✓ Desarrollar sugerencia y recomendaciones para reducir la probabilidad de ocurrencia de la amenaza.
  - ✓ Evaluar las amenazas y aplicar los controles
    La mitigación de riesgos y los controles se detalla en la Tabla N° 19 de éste informe.

- **Etapa estrategia de continuidad**

  - ✓ **Concepto.**

    Corresponden a las acciones que se deben tomar para restablecer las operaciones de negocio en un plazo determinado, una vez que ocurra alguna interrupción o falla en los procesos o funciones críticas.

- ✓ **Objetivos.**

  - Permitir a la institución trascender ante una crisis y recomponerse en el menor tiempo posible.
  - Garantizar que los empleados estén protegidos y comprendan su papel para saber qué hacer en el momento de la interrupción.
  - Ayudar a planificar la recuperación y reanudación de los procesos.
  - Validar formas de recuperación de la Institución.

- ✓ **Alcance**

Se pueden aplicar diferentes estrategias de recuperación en las siguientes situaciones:

- Ausencia de personal
- Lugar de trabajo alterno
- Fallas en la tecnología

- ✓ **Estrategias por ausencia de personal**

Se presenta cuando los trabajadores que ejecutan un proceso no pueden asistir a trabajar para desarrollar sus actividades. Se debe establecer la siguiente cadena de comunicación:

- El trabajador ausente activa la cascada telefónica y se comunica con el jefe inmediato.
- El Jefe inmediato se comunica con el jefe de área y actica la contingencia por ausencia de personal. Asigna las funciones para el trabajador y solicita la reasignación de perfiles para el acceso a los sistemas al responsable de informática de ser necesario.
- El jefe inmediato confirma al Jefe de área la continuidad exitosa de los procesos.
  - ♦ El documento de cascada telefónica se encuentra la información básica de los trabajadores y del almacén de Gerencia Regional de Salud de Lambayeque con la finalidad de utilizarlos en el evento de contingencia.
  - ♦ El documento debe estar colocado en un lugar visible de cada área y además debe tenerlo cada trabajador.

- ✓ **Estrategias por lugar alterno**

Es una estrategia para el traslado del personal a otras instalaciones, cuando los funcionarios a cargo de ejecutar un proceso no pueden acceder a la Red de Salud de Lambayeque.
La Gerencia de la Red de Salud de Lambayeque en coordinación de con la Gerencia Regional de Lambayeque decidirán qué ambiente se utilizará en caso de un evento de así.

- ✓ **Estrategias por fallas tecnológicas**

La contingencia se presenta cuando el hardware y/o software presenta fallas, o cuando las telecomunicaciones son interrumpidas.

Se debe plantear estrategias de recuperación para base de datos, para la Red LAN, para el Sistema Operativo que se utilizan para la recuperación de la infraestructura de la Red de Lambayeque.

Se presentan los siguientes aplicativos y la infraestructura sobre los cuales se realizara la estrategia de contingencia:

Aplicativos:

- SISMED
- Correo Electrónico
- Página Web MINSA
- ARFSIS
- SIP
- HIS
- SIEM

Red:

- Switch
- Modem
- Cableado estructurado
- Firewall

✓ **Estrategia de recuperación de LAN – SWITCH**

1.- Objetivo

Recuperar el switch que se encuentra en la Red de Salud de Lambayeque.

2.- Alcance

El procedimiento aplica para daños en el switch o a nivel de hardware o software.

3.- Condiciones Generales

Para el desarrollo de este procedimiento se debe tener los siguientes recursos disponibles:

- La disponibilidad del responsable de informática.
- Contar con un switch de backup.
- Disponibilidad de presupuesto de parte de la Gerencia.

4.- Descripción

Actividades:

N° Actividad	Descripción de la Actividad	Observaciones	Responsable
1	Identificar la falla y realizar un diagnóstico.		Responsable de informática
2	Solicitar al almacén el switch de recambio.		Responsable de informática
3	Tomar el switch de recambio		Responsable de informática
4	Solicitar la configuración del switch.	Lo suministrará el proveedor del switch o en todo caso el operador de servicio de internet.	Proveedor de switch y el responsable de informática.
5	Resetear el switch y		Responsable de

	aplicar la configuración respectiva.		informática
6	Verificar que el switch funciona correctamente.	Se realiza la conexión del switch y se realiza las pruebas de enrutamiento respectiva.	Responsable de informática
7	El switch funciona correctamente.	Si los resultados de la prueba son correctos se sigue con el siguiente paso, sino se regresa al paso 5.	Responsable de informática
8	Se informa al Gerente de la Red de Salud sobre el restablecimiento del servicio.	Reporte de funcionamiento correcto y se documenta el proceso.	Responsable de informática
9	Reporte del servicio restablecido.	El gerente de la Red de Salud o el responsable de informática informan que la contingencia ha sido restablecida.	Gerente de la Red de Salud o el responsable de informática.

Tabla Nº 27. Actividades de estrategia de recuperación LAN –SWITCH

Fuente: Elaboración propia

- **Etapa de pruebas**

  ✓ **Concepto**

  Consiste en verificar la efectividad de las estrategias diseñadas y permitir la mejora continua del Plan de continuidad de negocio.

  Es una etapa de identificar y prevenir fallas y como poder afrontarlas en una situación real.

✓ **Objetivos**

- Practicar los procedimientos para saber cómo actuar ante un incidente.
- Demostrar la capacidad de recuperación.
- Identificar las áreas que necesitan una mejoría.

✓ **Alcance**

- Verificar la efectividad del plan.
- Evaluar la coordinación de los involucrados en el plan de pruebas.
- Identificar la capacidad de recuperar información crítica.
- Medir el rendimiento del sistema operativo y los sistemas.

✓ **Tipo de pruebas**

Se plantea usar 2 tipos de pruebas

Tipo de Prueba	Técnica utilizada	Actividad
Integrada	▪ Se creará un escenario. ▪ Seguimiento de las estrategias de recuperación. ▪ Con previo aviso.	Prueba integrada con todos los elementos que hacen parte del plan de contingencia.
Escritorio	▪ Se creará un escenario. ▪ Con previo aviso	Se realizará un ejercicio de escenario en una de las áreas de la Red según el alcance del proyecto

Tabla Nº 28. Tipo de pruebas

Fuente: Elaboración propia

- **Etapa de Mantenimiento:**

a) Concepto

Es la revisión de lineamientos, estrategias, planes, capacitación al personal, para que el plan de continuidad de negocio este actualizado con el objetivo que éste sea capaz de recuperar las actividades críticas.

b) Objetivos

Verificación y validación de lineamientos, estrategias y planes de del plan de continuidad de negocio.

c) Factores de actualización

Son los eventos que pueden generar una revisión al Plan de continuidad de negocio.

- ✓ Nuevo hardware, aplicaciones, sistemas operativos, base de datos.
- ✓ Cambios en las telecomunicaciones
- ✓ Cambio en las instalaciones
- ✓ Cambios en el personal

CAPITULO VI: Costos y Beneficios

6.1.- Análisis de Costos y Beneficios

6.1.1. Costo de Software

Descripción	Cantidad	Costo(S/.)
Licencia de ESET Endpoit antivirus	14	1684.33
Licencia Completa Software de Copia de Seguridad Acronis.	1	292.51
Software de monitoreo de red (suscripción por un año)	1	98.00
TOTAL		**2074.84**

Tabla Nº 29. Costo de Software

Fuente: Elaboración propia

6.1.2.- Costo de Personal

Personal	Precio(S/.)	Unidad	Cantidad	Total
Ingeniero de Computación e Informática	1500	mes	6	9000
TOTAL				**9000**

Tabla Nº 30. Costo de Personal

Fuente: Elaboración propia

6.1.3.- Costo de Servicio y Materiales

Servicios	Tiempo(meses)	Tarifa(S/.)/mes	Importe
Agua	6	310	1860
Luz	6	310	1860
Teléfono +Internet	6	140	1860
TOTAL			**5580**

Tabla Nº 31. Costo de servicios

Fuente: Elaboración Propia

Materiales	Precio (S/.)	Unidad	Cantidad	Total
Papel Bond A4	20	millar	4	80
Cable UTP Categoría 6.0	metros	200	1	200
Canaleta x 2 m	Unidad	100	2	200
Conectores RJ45	Bolsa x100	1	40	40
TOTAL				**520**

Tabla Nº 32. Costo de materiales

Fuente: Elaboración propia

6.1.4.- Costos de Hardware

Descripción	Unidad	Cantidad	Costo(S/.)	Total
Switch D-Link DES-1024D de 10/100 Mbps de 24 puertos	Unidad	1	158	158
Router inalámbrico N 450 Mbps TL-WR940N	Unidad	1	170	170
Firewall marca Fortinet	Unidad	1	800	800
UPS CDP R-UPR508i de 500VA, 240W	Unidad	10	145	1450
TOTAL				**2578**

Tabla Nº 33. Costo de Hardware

Fuente: Elaboración Propia

6.1.5. Costos de Implementación

Sin costos.

6.1.6. Costo de Mantenimiento

Sin costos.

6.1.7. Otros costos

Sin costos.

6.1.8. Resumen de Costos

Categoría	Costo
Costo de software	2074.84
Costo de personal	9000.00
Costo de servicios	7600.00
Costo de materiales	520
Costo de hardware	2578
TOTAL	**21772.84**

Tabla Nº 34. Resumen de costos

Fuente: Elaboración propia

6.2.- Recuperación de la Inversión.

Para hallar la recuperación de la inversión se hizo uso del periodo de recuperación de la información.

Desarrollo:

Se realiza un cuadro con los flujos dinero, a partir de ahí se halla el periodo de recuperación como se muestra en la tabla 35:

Periodo(año)	Flujo	Flujo acumulado
0	**-21772.84**	**-21772.84**
1	20000	-1772.84
2	20000	18227.16
3	20000	38227.16
4	20000	58227.16

Tabla Nº 35. Flujo de efectivo

Fuente: Elaboración propia

Explicación:

- El periodo 0: Es la inversión inicial o el costo total del proyecto
- Periodo 1-4: Son los ingresos anuales de la red de Salud de Lambayeque

Fórmula:

$$\boxed{\boldsymbol{PRI = A + \frac{B}{C}}}$$

Donde:

A = Año último flujo acumulado negativo.

B = Último flujo acumulado negativo.

C = Flujo no acumulado del año siguiente.

Datos:

A = 1

B = 1772.84

C = 20000

Reemplazando:

$$\boldsymbol{PRI} = 1 + \frac{1772.84}{20000} = 1.088642$$

Luego se procede a convertir los decimales para hallar el periodo aproximado de recuperación en días y meses como se ve en la siguiente tabla Nº 36:

Años	Meses	Días
1	12 x 0.088642	
1	1.063704	
1	1	30*0.063704
1	1	1.91

Tabla Nº 36. Periodo de recuperación de la inversión

Fuente: Elaboración propia

Análisis:

En un plazo de 1 año y 1 mes y 2 días aproximadamente lo que se invierto en diseño del sistema de gestión de seguridad de la información podrá ser recuperado.

CAPITULO VII: Conclusiones

- ✓ Se identificó os procesos de negocio haciendo uso de la herramienta de BIZAGI y con la notación BPMN 2.0 para los procesos siguientes: de gestionar compra, distribución de medicamentos, gestionar el control de calidad de los alimentos, permitió establecer como se delimitaría nuestro sistema de gestión de seguridad de la información.

- ✓ Se valorizó los activos de información aplicando la Norma ISO/IEC 27005 encontrándose un total de 47 cuya criticidad tenían un valor alto los cuales se tomaron en cuenta para el desarrollo del SGSI.

- ✓ La evaluación de los riesgos aplicando la Norma ISO/IEC 27005 se inició con los riesgos con criticidad alta con un total de 75 se usaron para trabajar las vulnerabilidades y amenazas a mitigar a través de un plan de tratamiento de riesgos y 5 actividades planificadas

- ✓ Los controles seleccionados de la Norma ISO/IEC 207002 para su implementación son un total de 20 los cuales se eligieron para mitigar los riesgos más críticos dentro del proceso de suministro de medicamentos de la red de salud de Lambayeque, plasmado en la declaración de aplicabilidad.

- ✓ La documentación exigida por la norma ISO7IEC 27001 que se adoptó para el diseño del SGSI fue: el alcance del SGSI, políticas y objetivos de seguridad de la información, metodología de evaluación y tratamiento de riesgos, la declaración de aplicabilidad, plan de tratamiento de riesgos, inventario de activos, política de control de acceso, procedimiento para gestión de incidentes, procedimientos de la continuidad de negocios.

CAPITULO VIII: Recomendaciones

- ✓ Es recomendable que se haga un seguimiento sobre el funcionamiento del SGSI para una futura certificación según la ISO 27001.
- ✓ Es necesario que la gerencia pueda presupuestar la implementación de los controles propuestos para una mejora en la seguridad de los sistemas y procesos.
- ✓ Se recomienda que se establezca el comité de seguridad que pueda dedicarse a la continuidad del sistema de gestión en la institución.
- ✓ Es recomendable que exista reuniones periódicas por parte del comité de seguridad para verificar un avance correcto del sistema de gestión de seguridad de la información.

CAPÍTULO IX: Referencias Bibliográficas

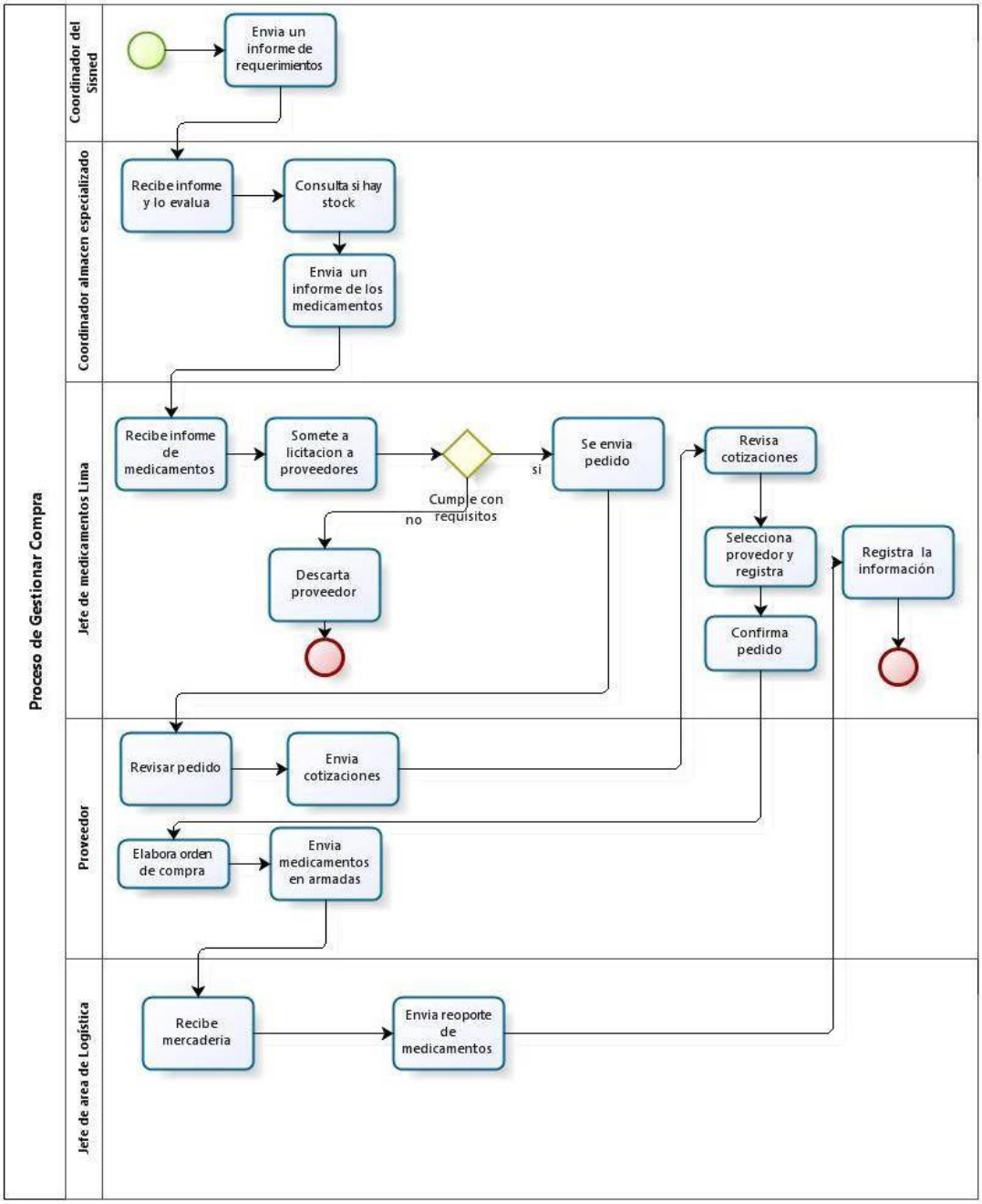
- Aguirre Cardona, J. D., & Aristizabal Betancourt, C. (2013). *Diseño del Sistema de Gestión de seguridad de la información para el grupo empresarial La Ofrenda.* Proyecto de grado, Universidad Tecnológica de Pereira, Colombia.
- Agustín , L. N., & Javier, L. S. (13 de Setiembre de 2015). *ISO2700.ES El portal de 27001 en español*. Obtenido de http://www.iso27000.es/sgsi.html
- Agustín, L. N., & Javier, R. S. (15 de Setiembre de 2015). *ISO 27002.ES El portal de ISO 27002 en Español*. Obtenido de http://www.iso27000.es/iso27002.html
- Alcántara Flores, J. C. (2015). *Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo.* Tesis, Chiclayo Perú.
- Aliaga Flores, L. (2013). *Diseño de un sistema de gestión de seguridad de información para un instituto educativo.Tesis para optar por el Título de Ingeniero Informático, que presenta el bachiller.* Lima: Pontificia Universidad Católica del Perú. Facultad de Ciencias e Ingeniería.
- Ampuero Chang, C. E. (2011). *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros.* Tesis de Pregrado, Pontificia Universidad Católica del Perú, Lima-Perú.
- Barrantes Porras, C. E., & Hugo Herrera, J. R. (2012). *Diseño e implementación de un Sistema de Gestión de Seguridad de información en procesos tecnológicos.* Tesis, Universidad San Martin de Porres, Lima Perú.
- Caita Castro, C. A. (29 de Septiembre de 2015). *Modelos & Estándares de Seguridad Informatica*. Recuperado el 25 de Diciembre de 2015, de https://prezi.com/ofvgu85tpu5e/modelos-estandares-de-seguridad-informatica/
- Casadiegos Santana, A. L., Quintero Jimenez, M., & Toro Rueda, M. (2014). *Sistema de gestión de seguridad de la información (SGSI) para el área de contabilidad de la E.S.E. Hospital local de rio de Oro César.* Trabajo de Grado, Universidad Francisco de Paula Santander Ocaña, Colombia.
- De la cruz Guerrero, C. W., & Vasquez Montenegro, J. C. (2008). *Elaboración y aplicación de un sistema de gestión de la seguridad de la información (SGSI) para la realidad tecnológica de la USAT.* Tesis de Pregrado, Universidad Católica Santo Toribio de Mogrovejo, Chiclayo-Perú.
- Excellence, I. (25 de Setiembre de 2015). *Blog especializado en Sistemas de Gestión* . Obtenido de http://www.pmg-ssi.com/2014/03/iso-27001-la-declaracion-de-aplicabilidad/
- Fernández, E., & Piattini, M. (2003). *Seguridad de las tecnologías de la Información: La construcción de la confianza para una sociedad conectada.* (Primera ed.). Madrid: Ediciones Aenor.

- García, A., & Alegre, M. (2011). *Seguridad Informática* (Primera ed.). Madrid: Paraninfo S.A.
- Gobierno de España. (13 de Setiembre de 2015). *Seguridad Informática*. Obtenido de http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/isoirc_27001_pdca.html
- INSTITUTE, I. G. (2012). *COBIT 5.* Illinois USA.
- ISACA. (2012). *COBIT® 5 Procesos Catalizadores.* Illinois, EE.UU: ISACA.
- ISO. (15 de Setiembre de 2015). *ISO/IEC 27002:2013(en)*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en
- ISO. (15 de Setiembre de 2015). *ISO/IEC 27003:2010(en)*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-1:v1:en
- ISO. (15 de Setiembre de 2015). *ISO/IEC 27005:2011(en)*. Obtenido de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27005:ed-2:v1:en
- Padilla Ramos, S. (2013). *Estándar ISO/IEC Internacional 27001*. Recuperado el 20 de Diciembre de 2015, de https://itic12sistemasdecalidad.wordpress.com/ensayo-de-investigacion/
- Red de Salud de Lambayeque. (2015). *Manual de Organizacion y Funciones 2015.* Lambayeque.
- Red de Salud de Lambayeque. (2015). *Plan Operativo Institucional 2015.* Lambayeque.
- Sinnexus. (01 de Abril de 2016). *Sinnexus Business Intelligence Informática estratégica*. Obtenido de http://www.sinnexus.com/business_intelligence/cuadro_mando_integral.aspx
- Tupia, M. (2011). *Principios de auditoría y control de sistemas de información* (Segunda ed.). Lima: Tupia Consultores y Auditores.
- Wikipedia. (25 de setiembre de 2015). *Entregable*. Obtenido de https://es.wikipedia.org/wiki/Entregable
- Wikipedia. (13 de Setiembre de 2015). *ISO/IEC 27001 Wikipedia, La Enciclopedia Libre*. Obtenido de https://es.wikipedia.org/wiki/ISO/IEC_27001

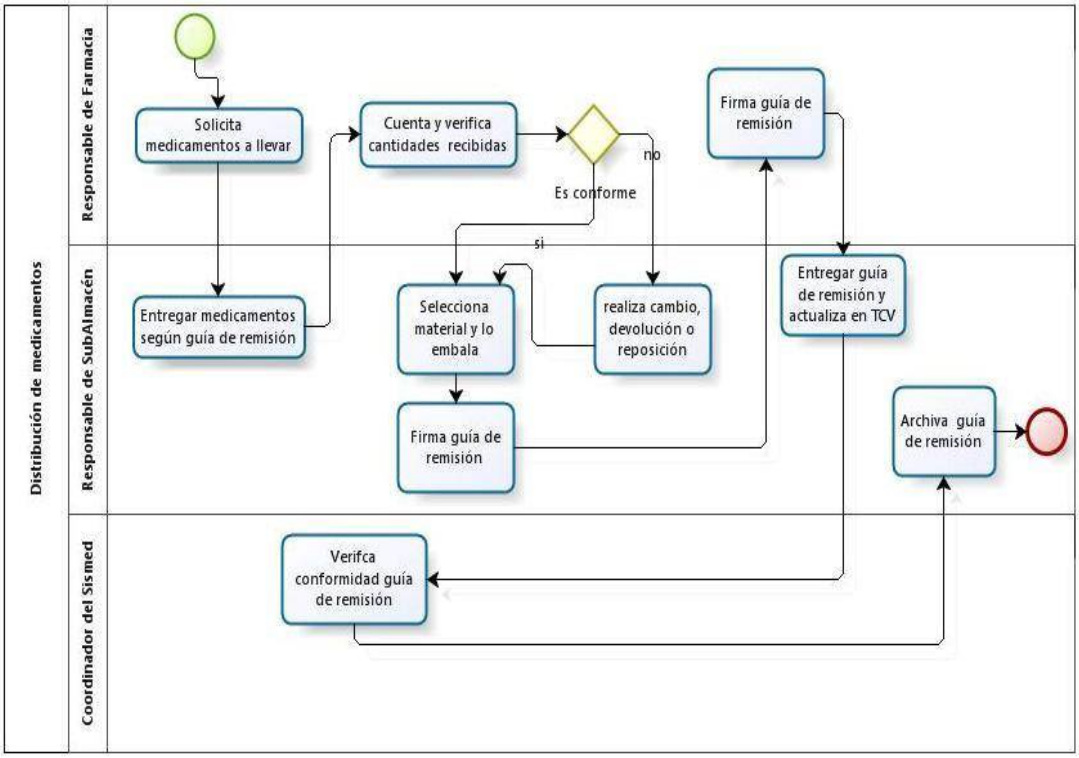
ANEXOS

ANEXO Nº 01:

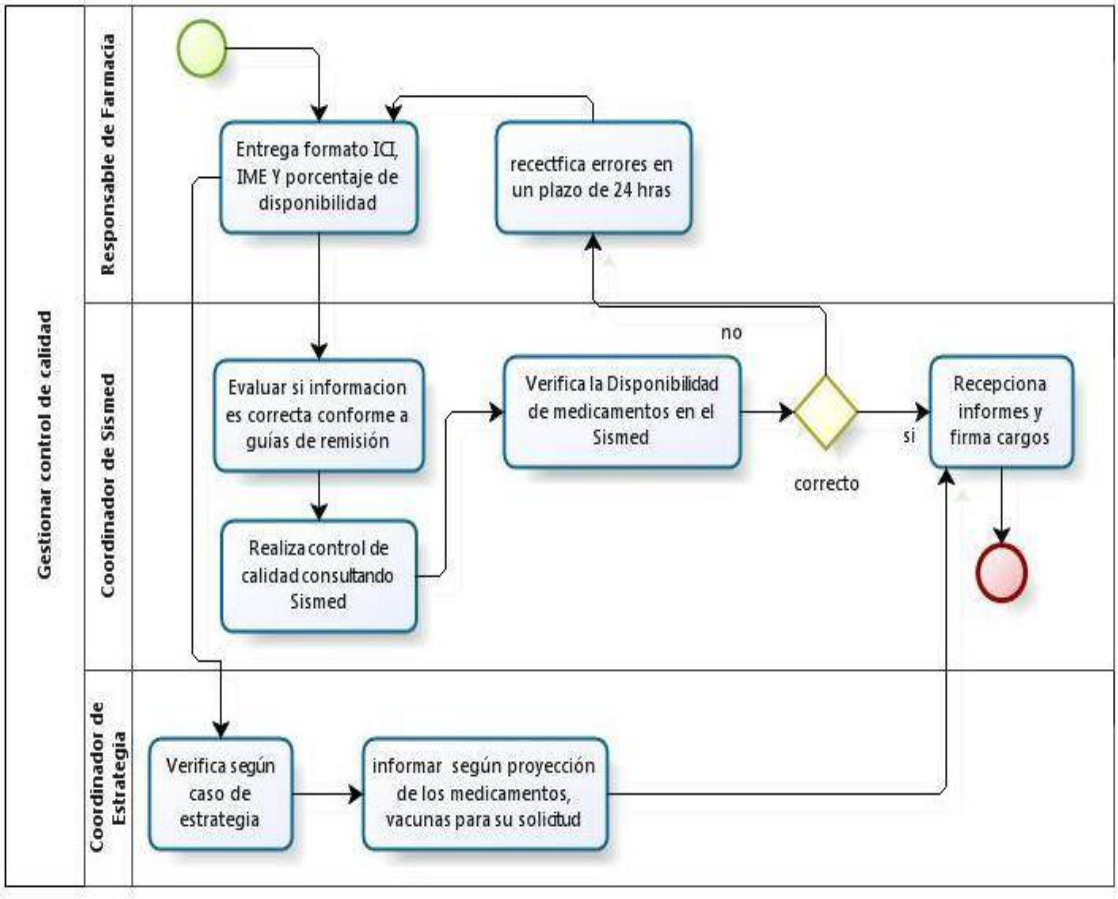
ANEXO 1.1 FLUJOGRAMA GESTIONAR COMPRA



ANEXO 1.2 FLUJOGRAMA GESTIONAR DISTRIBUCIÓN



ANEXO 1.3 FLUJOGRAMA GESTIONAR CONTROL DE CALIDAD



ANEXO N° 02

ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN

Dirigido al responsable de informática de la Red de Salud de Lambayeque, tomando en cuenta las áreas de almacén, SISMED y Estrategias sanitarias como alcance.

Instrucciones:

Para desarrollar este cuestionario, usted debe leer cada pregunta y escoger una de las alternativas propuestas con una "X" dentro de los paréntesis o escribir dentro de las líneas punteadas según sea su criterio.

Políticas de Seguridad:

1. Existe políticas de seguridad implementadas en la Red de Salud de Lambayeque.
   SI ( ) NO ( )

2. Si existe políticas de seguridad, especifique a qué nivel abarca.
   ……

Aspectos Organizativos:

3. Los trabajadores cuentan con algún mecanismo para reducir algún riesgo de seguridad de información.
   SI ( ) NO ( )
   Si la respuesta es Sí:
   Cuenta con
   a) Manual de usuario ( )
   b) Guía ( )
   c) Página Web ( )
   d) Otro ( ), especifique:
   ……

4. Los equipos informáticos cuentan con antivirus.

SI ( ) NO ( )

Si la respuesta es sí:

¿Qué antivirus utilizan?

- Kaspersky ( )
- Eset No 32 ( )
- Avira ( )
- Avast ( )
- Otro ( ), especifique:

  ……

¿Cada qué tiempo actualizan la versión de antivirus?

a. Mensual ( )
b. Trimestral ( )
c. Semestral ( )
d. Anual ( )
e. Otros ( ), especifique:

   ……

5. Numero de computadoras que cuentan con antivirus a nivel de Sismed, Almacén y Estrategias Sanitarias:

……

6. Cuentan con una política de seguridad para protección de equipos móviles o portátiles

SI ( ) NO ( )

Que política de seguridad utiliza:……

7. Cuentan con herramientas o utilidades para controlar el uso y acceso de escritorio remoto.

SI ( ) NO ( )

Que herramienta utiliza……

Seguridad de RRHH:

8. Se ha realizado en este año capacitación sobre seguridad de información en la Red de Salud de Lambayeque.
   SI () NO ()

Gestión de activos:

9. Los equipos informáticos y otros recursos de información están identificados e inventariados.
   SI ( ) NO ( )

10. Conoce de algún documento donde se registre la entrega y recepción de equipos informáticos a los trabajadores.
    SI ( ) NO ( )

11. La información que se maneja en la Red de Salud de Lambayeque está clasificada, ejemplo, de acuerdo a su valor, legalidad, criticidad para la institución:
    SI ( ) NO ( )
    Si la respuesta es sí.
    Indique el tipo de
    clasificación……..

12. Existe algún procedimiento registrado para la protección de medios extraíbles.
    SI ( ) NO ( )

Control de accesos

13. Se tienen implementado un control para acceso a la red LAN de la Red de Salud.
    SI ( ) NO ( )

14. Se tiene un procedimiento para gestionar el alta y baja de usuarios, así como la asignación de privilegios a los sistemas de información.
    SI ( ) NO ( )

15. Existe una guía de buenas prácticas de seguridad para el uso contraseñas y seguridad de equipos informáticos.

SI ( ) NO ( )

Criptografía

16. Alguna vez se ha implementado el uso de criptografía para la protección de claves de acceso en los documentos de mayor valor en la Red de salud.

SI ( ) NO ( )

Seguridad física y ambiental

17. Existe un sistema de seguridad física en las oficinas de la red de Salud.

SI ( ) NO ( )

18. Existe una medida o control contra desastres naturales, ataques maliciosos o accidentes dentro de las instalaciones.

SI ( ) NO ( )

19. Existe un plan o control para protección contra cortes de luz u otras interrupciones que puedan provocar algún daño en las instalaciones.

SI ( ) NO ( )

20. El cableado eléctrico y las de telecomunicaciones están debidamente protegidos

SI ( ) NO ( )

21. Cada cuanto tiempo se le da mantenimiento a los equipos informáticos

a. Mensual ( )
b. Trimestral ( )
c. Semestral ( )
d. Otros ( ), especifique: ……

22. Existe alguna medida para garantizar la seguridad de los equipos informáticos fuera de la institución.

SI ( ) NO ( ) No salen ( )

23. Existe un procedimiento para los espacios de trabajo, para el uso adecuado de los equipos herramientas informáticas.

SI ( ) NO ( )

Operativas

24. Los procedimientos que se aplican para dar soporte a las incidencias están registrados en algún documento.

SI ( ) NO ( )

25. Ha habido alguna capacitación sobre protección correos electrónicos e información código malicioso que existen en la actualidad.

SI ( ) NO ( )

26. Se realizan copias de seguridad o backups a los sistemas o información más importante.

SI ( ) NO ( )

Si la respuesta es sí. Cada que tiempo se realiza

a. Diario ( )
b. Semanal ( )
c. Mensual ( )
d. Otros ( ), Especifique:

…….

27. Los eventos y registros de accesos de los usuarios son controlados con alguna aplicación

SI ( ) NO ( )

Si la respuesta es sí, que aplicación utilizan:……..

28. Se les capacita a los trabajadores de los cambios o actualizaciones que puedan haber en los sistemas que utilizar para el trabajo diario.

SI ( ) NO ( )

Si la respuesta es sí, cual es la forma de capacitación:……

Telecomunicaciones

29. Hay un mecanismo para administrar la red LAN en la Institución.
SI ( ) NO ( )

30. Sabe si existe algún acuerdo de confidencialidad y no divulgación en la Institución.
SI ( ) NO ( )

Proveedores

31. Trabajan con servicio de terceros que les brinda soporte para equipos en TI
SI ( ) NO ( )
Si la respuesta es sí, que requisitos de seguridad les facilita:……..
……

Incidencia

32. Hay algún procedimiento para dar apoyo en caso ocurra incidentes con los sistemas de información.
SI ( ) NO ( )

33. Existe algún sistema de contingencia o redundancia para garantizar el nivel de disponibilidad de los sistemas o base de datos.
SI ( ) NO ( )

34. Existe algún tipo de servidor implementado en la Institución, como por ejemplo de aplicaciones o de archivos
SI ( ) NO ( )
Si la respuesta es sí, que tipos de servidores están funcionando actualmente:
……

Cumplimiento

35. Qué tipo de software se utiliza en la red:

a. Licenciado ( )
b. Libre ( )
c. Otros ( ), especifique:
……

36. Se cumple con la normativa legal sobre el uso de aplicaciones.

SI ( ) NO ( )

37. Numero de computadoras con licencia del office:

…….

38. Numero de computadoras con licencia del Windows:

…….

39. Numero de computadoras con licencia de otros programas (especifique):

……

ANEXO N° 03

ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN

Dirigido a los Coordinadores de las áreas del Sismed, Almacén y Estrategias de la Red de Salud de Lambayeque.

Objetivos:

- Conocer que tan involucrados están los trabajadores respecto a la protección de la información.
- Saber si los trabajadores utilizan de manera óptima las tecnologías de información y de qué manera ayudarían a salvaguardar la misma.

Instrucciones:

Para desarrollar este cuestionario, usted debe leer cada pregunta y escoger una de las alternativas propuestas con una "X" dentro de los paréntesis o escribir dentro de las líneas punteadas según sea su criterio.

---

1. Sexo

Masculino ( ) Masculino ( )

2. Cargo**:**

……

3. A qué área pertenece**:**

……

4. Usted apaga los equipos informáticos debidamente después de utilizarlos

SI ( ) NO ( )

Si tu respuesta es Sí, Cómo apagas tu equipo después de trabajar

a. Apagando directamente el estabilizador. ( )

b. Desenchufando el cable de energía de la computadora. ( )

c. Manteniendo presionado el botón de apagado del CPU. ( )

d. Haciendo clic en el botón de apagado del menú del sistema operativo. ( )

e. Bajando la llave de energía. ( )

f. Otros,
Especificar……
( )

g. Ninguno. ( )

5. Se siente seguro en los ambientes donde se encuentran los equipos informáticos dentro de la Red de Salud donde labora frente a cualquier desastre natural o humano.

SI ( ) NO ( )

6. Ha observado algún extinguidor cerca de los equipos informáticos

SI ( ) NO ( )

7. Ha observado algún tipo de señalización de emergencia en los ambientes donde existen equipos informáticos

SI ( ) NO ( )

8. Sabe utilizar de forma adecuada un extintor

SI ( ) NO ( )

Si la respuesta es **Sí;** Lo aprendió a utilizar a través de:

a. Charlas y capacitaciones fuera de la Red de Salud ( )
b. Charlas y capacitaciones dentro de la Red de Salud ( )
c. Manuales de extintores ( )
d. Internet ( )

9. Ha participado de algún simulacro frente a cualquier desastre natural o humano, especialmente en áreas donde hay equipos informáticos.

SI ( ) NO ( )

Si tu respuesta es **No;**

Como nos sugieres que se realice y cada que tiempo:

.....

10. Ud. ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en la computadora

SI ( ) NO ( )

11. Ha manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse, impresora y conexiones de red que conectan al CPU para hacerlos funcionar.

SI ( ) NO ( )

12. Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa en la Red de Salud de Lambayeque.

SI ( ) NO ( )

13. Si en el transcurso del uso de su equipo informático se detecta alguna actividad sospechosa como por ejemplo ingresando a lugares restringidos, usted sería capaz de afrontarla (por la responsabilidad que asume en ese determinado momento sobre el equipo asignado)

SI ( ) NO ( )

14. Usted saca información en algún dispositivo de almacenamiento, como USB, CD, etc.

Si ( ) A veces ( ) Nunca ( )

15. Que hace cuando detecta un virus en la computadora donde trabaja en la Red de Salud

a. Activa el antivirus ( )
b. Activa el antivirus, detecta los virus y los elimina ( )
c. Borra el archivo ( )
d. Formatea el dispositivo de almacenamiento ( )
e. No hago nada (Por desconocimiento) ( )
f. Otros, Especificar …….……. ( )

16. Usted ha detectado que el antivirus de la Red de Salud de Lambayeque funciona correctamente y que se encuentra actualizado.

SI ( ) NO ( )

17. Usted ha tenido algún problema cuando ha hecho uso del correo electrónico para el trabajo, como por ejemplo: no se envían o reciben correos.

SI ( ) NO ( )

18. A usted le han asignado un usuario y una clave de acceso para que ingrese a su computadora.

SI ( ) NO ( )

19. Usted es la única persona que utiliza su computadora para las labores diarias de la Red de Salud.

SI ( ) NO ( )

20. Utiliza el servicio de correo electrónico que se le asigna en la Red de Salud de Lambayeque

SI ( ) NO ( ) No tienen correo institucional ( )

Si su respuesta es **Sí**; Con qué frecuencia recibe correos no deseados o spam:

a. De 1 a 10 correos al día ( )
b. De 11 a 20 correos al día ( )
c. De 21 a más correos al día ( )

21. Usted recibió alguna capacitación acerca de Seguridad de la Información en la Red de Salud de Lambayeque

SI ( ) NO ( )

22. Le interesaría conocer o tener un mayor conocimiento respecto a Seguridad de la Información

SI ( ) NO ( )

Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:

a. Folletos y boletines ( )
b. Charlas o conferencias ( )
c. Foros a través del portal WEB del MINSA ( )
d. Otros, Especifique:..... ( )

23. Usted ha realizado alguna de las siguientes actividades en su PC:

a. Instalando algún software (programa) que necesitaba ( )
b. Haciendo limpieza de componente de su PC (teclado, mouse, cpu, etc.) ( )
c. Desarmando el CPU por algún sonido o falla ( )
d. Otros, Especifique**……..** ( )
e. Ninguna ( )

24. ¿Qué hace usted cuando uno de sus aplicativos no funcionan adecuadamente en su PC?

a. Intenta arreglarlo ( )
b. Lo arregla mi compañero de trabajo más cercano ( )
c. Llamo al responsable de informática ( )
d. No sabe que hacer en esos momentos ( )

25. ¿Con qué frecuencia solicita usted que se le realice mantenimiento a la PC que se le asigno?

Mensual ( ) Trimestral ( ) Semestral ( ) Anual ( ) Nunca ( )

26. ¿Con qué frecuencia solicita que le revisen su PC frente a cualquier falla?

A veces ( ) Casi Siempre ( ) Siempre ( ) Nunca ( )

27. Cree usted que su equipo se encuentra seguro frente a cualquier peligro como:

a. Acceso a sus cuentas personales ( )
b. Ingreso de Virus ( )
c. Existencia de un extinguidor o medida de seguridad de los equipos cerca ( )
d. No lo sé ( )
e. Otros, Especificar……. ( )

28. Cada vez que ocurre algún incidente con la PC o aplicación , porque medio informa o lo reporta:

a. Teléfono (anexo) ( )
b. Correo electrónico al área de informática ( )
c. Voy físicamente a buscar algún responsable de informática ( )
d. Espero a que pasen por mi área de trabajo ( )
e. Otros, Especifique……..…… ( )
f. Ninguna

29. Alguna vez se ha perdido su información cuando estaba en pleno trabajo, ya sea ingresando información o usando un medio extraíble como USB.

SI ( ) NO ( )

30. Usted realiza su trabajo a través de un sistema de información o de manera manual.

Usa un sistema ( ) Manualmente ( )

31. Si necesita utilizar un programa que no se encuentra instalado en la computadora, como procede usted:

a. Lo descargo de internet ( )
b. Pido ayuda al responsable de informática ( )
c. Lo compro en una tienda ( )
d. Otros ( )

32. Usted visualiza una correcta instalación del cableado de red y las conexiones eléctricas donde se encuentra conectada su computadora.

SI ( ) NO ( )

33. Usted sabe si los equipos informáticos que utiliza y sus componentes están debidamente codificados e inventariados.

SI ( ) NO ( )

34. Usted tienen conocimiento si existe un documento en la institución para la no divulgación de información, es decir que la información que se maneja en la Institución no puede salir de ésta.

SI ( ) NO ( )

ANEXO 04:

A.5 Políticas de seguridad		
A.5.1 Política de seguridad de la información Objetivo: Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.		
A.5.1.1	**Políticas para la seguridad de la información**	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados, así como a todas las partes externas relevantes.
A.5.1.2	**Revisión de las políticas para la seguridad de la información**	Control: Las políticas para la seguridad de la información se deberían planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad.
A.6 Aspectos Organizativos de la seguridad de la información		
A.6.1 Organización interna Objetivo: Establecer un esquema directivo de gestión para iniciar y controlar la implementación y operativa de la seguridad de la información en la organización.		
A.6.1.1	Asignación de responsabilidades para la SI	Control: Se deberían definir y asignar claramente todas las responsabilidades para la seguridad de la información.
A.6.1.2	Segregación de tareas	Control: Se deberían segregar tareas y las áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no

		autorizada o no intencionada, o el de un mal uso de los activos de la organización.
A.6.1.3	Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	Control: Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.
A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: Se debería contemplar la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización.
A.6.2 Dispositivos para movilidad y teletrabajo Objetivo: garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.		
A.6.2.1	Política de uso de dispositivos para movilidad	Control: Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.
A.6.2.2	Teletrabajo	Control: Se debería desarrollar e implantar una política y medidas de seguridad de apoyo para proteger a la información accedida,

		procesada o almacenada en ubicaciones destinadas al teletrabajo.
A.7 Seguridad ligada a los recursos humanos		
A.7.1 Antes de la contratación **Objetivo:** asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.		
A.7.1.1	Investigación de antecedentes	Control : Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.7.1.2	Términos y condiciones de contratación	Control: Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.
A.7.2 Durante la contratación **Objetivo:** asegurarse de que los empleados y contratistas están en conocimiento y cumplen con sus responsabilidades en seguridad de la información.		
A.7.2.1	Responsabilidades de gestión	Control: La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en

		concordancia con las políticas y los procedimientos.
A.7.2.2	Concienciación, educación y capacitación en SI	Control: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.
A.7.2.3	Proceso disciplinario	Control: Debería existir un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.
A.7.3 Cese o cambio de puesto de trabajo **Objetivo:** proteger los intereses de la organización durante el proceso de cambio o finalización de empleo por parte de empleados y contratistas.		
A.7.3.1	Cese o cambio de puesto de trabajo	Control: Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente.
A.8 Gestión de activos		
A.8.1 Responsabilidad sobre los activos **Objetivo:** identificar los activos en la organización y definir las responsabilidades para una protección adecuada.		

A.8.1.1	Inventario de activos	Control: Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.
A.8.1.2	Propiedad de los activos	Control: Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.
A.8.1.3	Uso aceptable de los activos	Control: Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de terceras partes deberían devolver todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo.
A.8.2 Clasificación de la Información **Objetivo:** Asegurar que se aplica un nivel de protección adecuado a la información.		
A.8.2.1	Directrices de clasificación	Control: La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la

		Organización.
A.8.2.2	Etiquetado y manipulado de la información	Control: Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.2.3	Manipulación de activos	Control: Se deberían desarrollar e implantar procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización.
A.8.3 Manejo de los Soportes de Almacenamiento: **Objetivo:** Evitar la divulgación, modificación, retirada o destrucción de activos no autorizada almacenada en soportes de almacenamiento.		
A.8.3.1	Gestión de soportes extraíbles	Control: Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de soportes	Control: Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.
A.8.3.3	Soportes físicos en tránsito	Control: Se deberían proteger los medios que contienen información contra acceso no

		autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.
A.9Control de Accesos		
A.9.1 Requisitos de negocio para el control de accesos **Objetivo:** controlar los accesos a la información y las instalaciones utilizadas para su procesamiento.		
A.9.1.1	Política de control de accesos	Control: Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.
A.9.1.2	Control de acceso a las redes y servicios asociados	Control: Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.
A.9.2 Gestión de acceso al usuario **Objetivo:** garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información y servicios.		
A.9.2.1	Gestión de altas/bajas en el registro de usuarios	Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	Se debería de implantar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.
A.9.2.3	Gestión de los derechos de	La asignación y uso de derechos de

	acceso con privilegios especiales	acceso con privilegios especiales debería ser restringido y controlado.
A.9.2.4	Gestión de información confidencial de autenticación de usuarios	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.
A.9.2.6	Retirada o adaptación de los derechos de acceso	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.
A.9.3 Responsabilidades del usuario **Objetivo:** hacer que los usuarios sean responsables de la protección de la información para su identificación.		
A.9.3.1	Uso de información confidencial para la autenticación	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación.
A.9.4 Control de acceso a Sistemas y Aplicaciones **Objetivo:** impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones.		
A.9.4.1	Restricción del acceso a la información	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de

		control de accesos definida.
A.9.4.2	Procedimientos seguros de inicio de sesión	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on.
A.9.4.3	Gestión de contraseñas de usuario	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad.
A.9.4.4	Uso de herramientas de administración de sistemas	El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.
A.9.4.5	Control de acceso al código fuente de los programas	Se debería restringir el acceso al código fuente de las aplicaciones software.
A.10 Cifrado		
A.10.1 Controles criptográficos **Objetivo:** garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.1	Política de uso de los controles criptográficos	Se debería desarrollar e implementar una política que regule el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de claves	Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.
A.11 Seguridad Física y Ambiental		
A.11.1 Áreas seguras **Objetivo:** Evitar el acceso físico no autorizado, los daños e interferencias a la		

información de la organización y las instalaciones de procesamiento de la información.		
A.11.1.1	Perímetro de seguridad física	Control: Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica.
A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso.
A.11.1.3	Seguridad de oficinas, despachos y recursos	Control: Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.
A.11.1.4	Protección contra las amenazas externas y ambientales	Control: Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	El trabajo en áreas seguras:	Control: Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.
A.11.1.6	Áreas de acceso público, carga y descarga	Control: Se deberían controlar puntos de acceso a la organización como las áreas de entrega

		y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información.
A.11.2 Seguridad de los equipos **Objetivo:** Evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.		
A.11.2.1	Emplazamiento y protección de equipos	Control: Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.
A.11.2.2	Instalaciones de suministro	Control: Los equipos deberían estar protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo.
A.11.2.3	Seguridad del cableado	Control: Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.
A.11.2.4	Mantenimiento de los equipos	Control Los equipos deberían mantenerse adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas.

A.11.2.5	Salida de activos fuera de las dependencias de la empresa	Control: Los equipos, la información o el software no se deberían retirar del sitio sin previa autorización.
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Control: Se debería aplicar la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos.
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	Control: Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.
A.11.2.8	Equipo informático de usuario desatendido	Control: Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Control: Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.

A.12Seguridad en la operativa		
A.12.1 Responsabilidades y procedimientos de operación. **Objetivo:** Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.		
A.12.1.1	Documentación de procedimientos de operación	Control: Se deberían documentar los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	Control: Se deberían controlar los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.
A.12.1.3	Gestión de capacidades	Control: Se debería monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.
A.12.1.4	Separación de entornos de desarrollo, prueba y producción.	Control: Los entornos de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.
A.12.2 Protección contra código malicioso **Objetivo:** Garantizar que la información y las instalaciones de procesamiento de información estén protegidas contra el malware.		

A.10.2.1	Controles contra el código malicioso	Control: Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.
A.12.3 Copias de Seguridad **Objetivo:** Alcanzar un grado de protección deseado contra la pérdida de datos.		
A.12.3.1	Copias de seguridad de la información	Control: Se deberían realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.
A.12.4Registro de actividad y supervisión **Objetivo:** Registrar los eventos relacionados con la seguridad de la información y generar evidencias.		
A.12.4.1	Registro y gestión de eventos de actividad	Control: Se deberían producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de los registros de información	Control: Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.
A.12.4.3	Registros de actividad del administrador y operador del sistema	Control: Se deberían registrar las actividades del administrador y del operador del sistema y

		los registros asociados se deberían proteger y revisar de manera regular.
A.12.4.4	Sincronización de relojes	Control: Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia.
A.12.5 Control del software en explotación **Objetivo:** garantizar la integridad de los sistemas operacionales para la organización.		
A.12.5.1	Instalación del software en sistemas en producción	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.
A.12.6 Gestión de la vulnerabilidad técnica **Objetivo:** Evitar la explotación de vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.
A.12.6.2	Restricciones en la instalación de software	Control: Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.

A.12.7 Consideraciones de las Auditorías de los sistemas de información **Objetivo:** Minimizar el impacto de actividades de auditoría en los sistemas operacionales.		
A.12.7.1	Controles de auditoría de los sistemas de información	Control: Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.
A.13 Seguridad en las Telecomunicaciones		
A.13.1 Gestión de la seguridad de redes **Objetivo:** Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.		
A.13.1.1	Controles de red	Control: Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	Control: Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.
A.13.1.3	Segregación de redes	Control: Se deberían segregar las redes en función de los grupos de servicios, usuarios y

		sistemas de información.
A.13.2 Intercambio de información con partes externas **Objetivo:** Mantener la seguridad de la información que transfiere un organización internamente o con entidades externas.		
A.13.2.1	Políticas y procedimientos de intercambio de información	Control: Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.
A.13.2.2	Acuerdos de intercambio	Control: Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información referida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad y secreto	Control: Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.
A.14 Adquisición, desarrollo y mantenimiento de los Sistemas de Información		
A.14.1 Requisitos de seguridad de los Sistemas de Información **Objetivo:** garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para		

aquellos que proporcionan servicios en redes públicas.		
A.14.1.1	Análisis y especificación de los requisitos de seguridad	Control: Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	Control: La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.
A.14.1.3	Protección de las transacciones por redes telemáticas	**Control** La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.
A.14.2 Seguridad en los procesos de desarrollo y soporte **Objetivo:** garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro de software.	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en los sistemas	Control: En el ciclo de vida de desarrollo se

		deberían hacer uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Control: Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones a los cambios en los paquetes de software	Control: Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	Control: Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.
A.14.2.6	Seguridad en entornos de desarrollo	Control: Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.
A.14.2.7	Externalización del desarrollo de software	Control: La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.

A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	Control: Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
A.14.2.9	Pruebas de aceptación	Control: Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.
A.15. Relaciones con suministradores		
A.15.1 Seguridad de la información en las relaciones con suministradores **Objetivo:** garantizar la protección de los activos de la organización que son accesibles a proveedores.		
A.15.1.1	Política de seguridad de la información para suministradores	Control: Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas.
A.15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización.

A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	Control: Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.
A.15.2 Gestión de la prestación del servicio por suministradores **Objetivo:** mantener el nivel en la prestación de servicios conforme a los acuerdos con el proveedor en materia de seguridad de información.		
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	Control: Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	Control: Se deberían administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.
A.16 Gestión de incidentes		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras **Objetivo:** garantizar una administración de incidentes de seguridad de la información coherente y eficaz en base a un enfoque de comunicación de los eventos y las debilidades de seguridad.		

A.16.1.1	Responsabilidades y procedimientos	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Notificación de los eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.
A.16.1.3	Notificación de puntos débiles de la seguridad	Control: Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización.
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	Control: Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.
A.16.1.5	Respuesta a los incidentes de seguridad	Control: Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Control: Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información

		para reducir la probabilidad y/o impacto de incidentes en el futuro.
A.16.1.7	Recopilación de evidencias	Control: La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.
A.17 Aspectos de seguridad de la información en la Gestión de la Continuidad del negocio		
A.17.1 Continuidad de la Seguridad de la Información **Objetivo:** Mantener la seguridad de la información integrada en los sistemas de gestión de continuidad del negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
A.17.1.2	Implantación de la continuidad de la seguridad de la información	Control: La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder

		garantizar su validez y eficacia ante situaciones adversas.
A.17.2 Redundancias **Objetivo:** garantizar la disponibilidad de las instalaciones de procesamiento de información.		
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	Control: Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.
A.18 Cumplimiento		
A.18.1 Cumplimiento de los requisitos legales y contractuales **Objetivo:** evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales.		
A.18.1.1	Identificación de la legislación aplicable	Control: Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.
A.18.1.2	Derechos de propiedad intelectual (DPI)	Control: Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar

		productos software original.
A.18.1.3	Protección de los registros de la organización	Control: Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
A.18.1.4	Protección de datos y privacidad de la información personal	Control: Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.
A.18.1.5	Regulación de los controles criptográficos	Control: Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.
A.18.2 Revisiones de la seguridad de la información **Objetivo:** garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales.		
A.18.2.1	Revisión independiente de la seguridad de la información	Control: Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la

		organización.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	Control: Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.
A.18.2.3	Comprobación del cumplimiento	Control: Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

Anexo 5:

Objetivos de la Empresa de COBIT 5		
Dimensión de cuadro de mando integral	**N°**	**Objetivos de Información y tecnología relacionada**
Financiera	1	Alineamiento de TI y estrategia de negocio
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	4	Riesgos de negocio relacionados con las TI gestionados
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
	6	Transparencia de los costes, beneficios y riesgos de las TI
Cliente	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	9	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y relevante para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI

Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

Anexo 6:

Métricas de Metas Corporativas		
Dimensión de CMI	**Meta Corporativa**	**Métrica**
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio	• Porcentaje de inversiones en las que la entrega cumple con las expectativas de los interesados • Porcentaje de productos y servicios en los que se realizan los beneficios esperados • Porcentaje de inversiones en los que se cumplen o superan los beneficios establecidos
	2. Cartera de productos y servicios competitivos	• Porcentaje de productos y servicios que alcanzan o exceden los objetivos de ingresos y/o cuota de mercado • Relación de productos y servicios por fase del ciclo de vida • Porcentaje de productos y servicios que alcanzan o exceden los objetivos de satisfacción al cliente • Porcentaje de productos y servicios que proporcionan ventaja competitiva
	3. Riesgos de negocio gestionados (salvaguarda de activos)	• Porcentaje de objetivos de negocio críticos y servicios cubiertos por gestión del riesgo • Relación de incidentes significativos que no fueron identificados en las evaluaciones de riesgo respecto al número total de incidentes • Frecuencia de actualización del perfil de riesgos
	4. Cumplimiento de leyes y regulaciones externas	• Coste de incumplimientos regulatorios incluyendo acuerdos y sanciones • Número de incumplimientos regulatorios causantes de comentarios públicos o publicidad negativa • Número de incumplimientos regulatorios en relación con acuerdos contractuales con socios de negocios
	5. Transparencia financiera	• Porcentaje de casos de negocio de inversión con costes y beneficios esperados claramente definidos y aprobados • Porcentaje de productos y servicios con costes operativos y beneficios esperados definidos y

		aprobados • Encuestas de satisfacción a interesados clave en relación con la transparencia, comprensión y precisión de la información financiera corporativa • Porcentaje del coste del servicio que puede ser asignado a usuarios
Cliente	6. Cultura de servicio orientada al cliente	• Número de trastornos del servicio al cliente debidos a incidentes relacionados con el servicio TI (fiabilidad) • Porcentaje de interesados del negocio que se encuentran satisfechos con que la entrega del servicio de cliente cumpla con los niveles acordados • Número de quejas de clientes • Tendencia de los resultados de las encuestas de satisfacción al cliente
	7. Continuidad y disponibilidad del servicio de negocio	• Número de interrupciones de servicio al cliente causantes de incidentes significativos • Coste de negocio de los incidentes • Número de horas de procesamiento perdidas debido a interrupciones del servicio no planificadas • Porcentaje de quejas en función de los objetivos de disponibilidad del servicio comprometidos
	8. Respuestas ágiles a un entorno de negocio cambiante	• Nivel de satisfacción del Consejo de Administración con la capacidad de respuesta corporativa a nuevos requerimientos • Número de productos y servicios críticos sustentados por procesos de negocio actualizados • Tiempo medio de conversión de objetivos estratégicos corporativos en iniciativas acordadas y aprobadas
	9. Toma estratégica de Decisiones basada en Información	• Grado de satisfacción del Consejo de Administración y la alta dirección con la toma de decisiones • Número de incidentes causados por decisiones de negocio incorrectas basadas en información imprecisa • Tiempo requerido para ofrecer información de apoyo que permita decisiones de negocio efectivas

	10. Optimización de costes de entrega del servicio	• Frecuencia de las evaluaciones de optimización del coste de entrega del servicio • Tendencia de la evaluación de costes respecto a los resultados del nivel de servicio
Interna	11. Optimización de la funcionalidad de los procesos de negocio	• Frecuencia de las evaluaciones de madurez de la capacidad de los procesos de negocio
	12. Optimización de los costes de los procesos de negocio	• Frecuencia de evaluaciones de optimización de costes de los procesos de negocio • Tendencia de la evaluación de costes respecto a los resultados del nivel de servicio
	13. Programas gestionados de cambio en el negocio	• Número de programas cumplidos en tiempo y en presupuesto • Porcentaje de interesados satisfechos con la ejecución y resultados del programa • Nivel de concienciación de cambios en el negocio inducidos por TI Iniciativas de negocio posibilitadas
	14. Productividad operacional y de los empleado	• Número de programas/proyectos en tiempo y presupuesto • Niveles de coste y de personal comparados con los análisis comparativos
	15. Cumplimiento con las políticas internas	• Número de incidentes relacionados con el incumplimiento de políticas • Porcentaje de interesados que entienden las políticas • Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivos
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	• Nivel de satisfacción de los interesados con el conocimiento y la cualificación del personal • Porcentaje de personal cuya cualificación es insuficiente para la competencia requerida por su rol • Porcentaje de personal satisfecho
	17. Cultura de innovación de producto y negocio	• Nivel de concienciación y comprensión de las oportunidades de innovación del negocio • Satisfacción de los interesados con los niveles de conocimiento e ideas de innovación y productos • Número de iniciativas de productos y

		servicios aprobadas resultantes de ideas innovadoras

Anexo 7:

Objetivos de las TI		
Dimensión del CMI TI	**Objetivo de la información y tecnología relacionada**	
Financiera	**1**	Alineamiento de TI y estrategia de negocio
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	4	Riesgos de negocio relacionados con las TI gestionados
	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
	6	Transparencia de los costes, beneficios y riesgos de las TI
Cliente	**7**	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	**9**	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y relevante para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI

Aprendizaje y crecimiento	**16**	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

Anexo 8:

Métricas de Muestra de Metas de TI		
Dimensión de CMI	**Objetivos de las TI**	**Métricas**
Financiera	01 Alineamiento de TI y estrategia de negocio	•Porcentaje de metas estratégicas y requerimientos corporativos apoyados por metas TI estratégicas • Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado • Porcentaje de factores de valor TI mapeados a factores de valor del negocio
	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	•Coste de incumplimientos TI, incluyendo acuerdos y sanciones e impacto en pérdida de reputación •Número de incumplimientos TI reportados al Consejo de Administración o causantes de comentarios o vergüenza públicos •Número de incumplimientos relacionados con proveedores de servicios TI • Cobertura de evaluaciones de cumplimiento
	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	• Porcentaje de roles de la dirección ejecutiva con responsabilidad claramente definida en decisiones TI • Número de veces que TI está en la agenda del Consejo de Administración de manera proactiva • Frecuencia de reuniones del comité ejecutivo de

		estrategia de TI • Tasa de ejecución de decisiones TI ejecutivas
	04 Riesgos de negocio relacionados con las TI gestionados	• Porcentaje de procesos TI de negocio críticos, servicios TI y programas de negocio habilitados por TI cubiertos por evaluaciones de riesgo • Número de incidentes TI significativos que no fueron identificados en evaluaciones de riesgos • Porcentaje de evaluaciones de riesgo corporativas que incluyen riesgo TI • Frecuencia de actualización del perfil de riesgo
	05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	• Porcentaje de inversiones TI donde la obtención del beneficio se supervisa a lo largo de todo el ciclo de vida económico • Porcentaje de servicios TI donde se obtienen los beneficios esperados • Porcentaje de inversiones TI donde se cumplen o exceden los beneficios esperados
	06 Transparencia de los costes, beneficios y riesgos de las TI	• Porcentaje de casos de negocio de inversiones TI con costes TI y beneficios esperados claramente definidos y aprobados • Porcentaje de servicios TI con costes operativos y

		beneficios esperados claramente definidos y aprobados • Encuesta de satisfacción de interesados clave en relación con el nivel de transparencia, comprensión y precisión de información financiera TI
Cliente	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	• Número de interrupciones de negocio debidas a incidentes de servicios TI • Porcentaje de partes interesadas en el negocio satisfechas de que la entrega de servicios TI cumpla los niveles de servicio acordados • Porcentaje de usuarios satisfechos con la calidad de la entrega de servicios TI
	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	• Porcentaje de propietarios de procesos de negocio satisfechos con el apoyo de productos y servicios TI • Nivel de entendimiento de los usuarios del negocio sobre cómo las soluciones tecnológicas apoyan sus procesos • Nivel de satisfacción de los usuarios de negocio con la formación y los manuales de usuario • Valor presente neto (NPV) mostrando el nivel de satisfacción del negocio con

		la calidad y utilidad de las soluciones tecnológicas
Interno	09 Agilidad de las TI	• Nivel de satisfacción de la alta dirección del negocio con la capacidad de respuesta de TI a nuevos requerimientos • Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas • Tiempo medio de conversión de objetivos TI estratégicos en una iniciativa acordada y aprobada
	10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública • Número de servicios TI sin requerimientos de seguridad destacables • Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados • Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías
	11 Optimización de activos, recursos y capacidades de las TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las

		evaluaciones • Niveles de satisfacción de la alta dirección del negocio y de TI con los costes y capacidades TI
	12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	• Número de incidentes del procesamiento de negocio causados por errores de integración de la tecnología • Número de cambios en los procesos de negocio que tienen que ser retrasados o revisados debido a problemas de integración de la tecnología • Número de programas de negocio facilitados por TI retrasados o incurriendo en costes adicionales debido a problemas de integración de la tecnología • Número de aplicaciones o infraestructuras críticas operando aisladamente y no integradas
	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	• Número de programas/proyectos en tiempo y en presupuesto • Porcentaje de interesados satisfechos con la calidad del programa/proyecto • Número de programas que necesitan revisiones significativas debido a defectos de calidad • Coste de mantenimiento de las aplicaciones respecto al coste TI global
	14 Disponibilidad de información útil y	• Nivel de satisfacción del

	relevante para la toma de decisiones	usuario del negocio con la calidad y la puntualidad (o disponibilidad) de la información de gestión • Número de incidentes de procesos de negocio causados por la indisponibilidad de la información • Relación y alcance de decisiones de negocio erróneas donde la información errónea o no disponible fue un factor clave
	15 Cumplimiento de las políticas internas por parte de las TI	• Número de incidentes relacionados con el incumplimiento de políticas • Porcentaje de interesados que entienden las políticas • Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas • Frecuencia de revisión y actualización de políticas
Aprendizaje y Crecimiento	16 Personal del negocio y de las TI competente y motivado	• Porcentaje de personal cuyas habilidades TI son suficientes para la competencia requerida por sus roles • Porcentaje de personal satisfecho con sus roles en TI • Número de horas de aprendizaje/ formación por miembro del personal
	17 Conocimiento,	• Nivel de concienciación y

	experiencia e iniciativas para la innovación de negocio	comprensión de la alta dirección del negocio sobre las posibilidades de innovación TI • Nivel de satisfacción de los interesados con los niveles de experiencia e ideas de innovación de TI • Número de iniciativas aprobadas resultantes de ideas TI innovadoras

Anexo 09:

Procesos Habilitadores de COBIT 5

1. **Evaluar, Orientar y Supervisar (EDM)**

Etiqueta del Proceso	Nombre	Descripción	Principales Metas de TI
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	1 Alineamiento de TI y estrategia de negocio.
			3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.
			7 Entrega de servicios de TI de acuerdo a los requisitos del negocio.
EDM02	Asegurar la Entrega de Beneficios	Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.	01 Alineamiento de TI y estrategia de negocio
			05 Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI
			06 Transparencia de los costes, beneficios y riesgos de las TI
			07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
			17 Conocimiento, experiencia e iniciativas para la innovación de negocio
EDM03	Asegurar la Optimización del Riesgo	Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa	04 Riesgos de negocio relacionados con las TI gestionados

		relacionado con el uso de las TI es identificado y gestionado	06 Transparencia de los costes, beneficios y riesgos de las TI
			10 Seguridad de la información, infraestructura de procesamiento y aplicaciones
			15 Cumplimiento de las políticas internas por parte de las TI
EDM04	Asegurar la Optimización de Recursos	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo	09 Agilidad de las TI.
			11 Optimización de los activos, recursos y capacidades de las TI.
			16 Personal del negocio y de las TI competente y motivado
EDM05	Asegurar la Transparencia hacia las Partes Interesadas	Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
			06 Transparencia de los costes, beneficios y riesgos de las TI
			07 Entrega de servicios de TI de acuerdo a los requisitos del negocio

2. Alinear, Planificar y Organizar (APO)

Etiqueta del Proceso	Nombre	Descripción	Principales Metas de TI que apoya
APO01	Gestionar el Marco de Gestión de TI	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.	01 Alineamiento de TI y estrategia de negocio
			02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
			09 Agilidad de las TI
			11 Optimización de activos, recursos y capacidades de las TI
			15 Cumplimiento de las políticas internas por parte de las TI
			16 Personal del negocio y de las TI competente y motivado
			17 Conocimiento, experiencia e iniciativas para la innovación de negocio
APO02	Gestionar la Estrategia	Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.	01 Alineamiento de TI y estrategias de negocio
			07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
			17 Conocimiento, experiencia e iniciativas para la innovación del negocio
APO03	Gestionar la Arquitectura Empresarial	Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las	01 Alineamiento de TI y estrategia de negocio
			09 Agilidad de las TI

		normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.	
			11 Optimización de activos, recursos y capacidades de las TI
APO04	Gestionar la Innovación	Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa.	05 Realización de beneficios del portafolio de inversiones y servicios relacionados con TI
			08 Uso adecuado de aplicaciones, información y soluciones tecnológicas
			09 Agilidad de las TI
			11 Optimización de activos, recursos y capacidades de las TI
			17 Conocimiento, experiencia e iniciativas para la innovación de negocio.
APO05	Gestionar el Portafolio	Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y	01 Alineamiento de TI y estrategia de negocio

		recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos, así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.	05 Realización de beneficios del portafolio de servicios y Servicios relacionados con TI
			13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad
APO06	Gestionar el Presupuesto y los Costes	Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.	05 Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI
			06 Transparencia de los costes, beneficios y riesgos de las TI
APO07	Gestionar los Recursos Humanos	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.	01 Alineamiento de TI y estrategia de negocio
			11 Optimización de activos, recursos y capacidades de las TI
			13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad
			16 Personal del negocio y de las TI competente y motivado
			17 Conocimiento, experiencia e iniciativas para la innovación de negocio

APO08	Gestionar las relaciones	Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.	01 Alineamiento de TI y estrategia de negocio
			07 Entrega de servicios TI de acuerdo a los requisitos del negocio
			12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
			17 Conocimiento, experiencia e iniciativas para la innovación de negocio
APO09	Gestionar los acuerdos de servicio	Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
			14 Disponibilidad de información útil y relevante para la toma de decisiones
APO10	Gestionar los Proveedores	Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.	04 Riesgos de negocio relacionados con las TI gestionados
			07 Entrega de servicios TI de acuerdo a los requisitos del negocio
			09 Agilidad de las TI
APO11	Gestionar la Calidad	Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.	05 Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI
			07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
			13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad

APO12	Gestionar el Riesgo	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.	02 Cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas
			04 Riesgos de negocio relacionados con las TI gestionados
			06 Transparencia de los costes, beneficios y riesgo de las TI
			10 Seguridad de la información, infraestructura de procesamiento y aplicaciones
			13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad
APO13	Gestionar la Seguridad	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
			04 Riesgos de negocio relacionados con las TI gestionados
			06 Transparencia de los costes, beneficios y riesgo de las TI
			10 Seguridad de la información, infraestructura de procesamiento y aplicaciones
			14 Disponibilidad de información útil y relevante para la toma de decisiones

3. Construir, Adquirir e Implementar (BAI)

Etiqueta del Proceso	Nombre	Descripción	Principales Metas de TI que apoyan
BAI01	Gestión de Programas y Proyectos	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.	01 Alineamiento de TI y la estrategia de negocio
			04 Riesgos de negocio relacionados con las TI gestionados
			05 Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI
			13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad
BAI02	Gestionar la Definición de Requisitos	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.	01 Alineamiento de TI y estrategia de negocio
			07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
			12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio

BAI03	Gestionar la Identificación y Construcción de Soluciones	Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
BAI04	Gestionar la Disponibilidad y la Capacidad	Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
			11 Optimización de activos, recursos y capacidades de TI
			14 Disponibilidad de información útil y relevante para la toma de decisiones
BAI05	Gestionar la Facilitación del Cambio Organizativo	Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todos las partes interesadas del negocio y de TI.	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas

			13 Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
			17 Conocimiento, experiencia e iniciativas para la innovación de negocio
BAI06	Gestionar los Cambios	Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.	04 Riesgos de negocio relacionados con las TI gestionados
			07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
			10 Seguridad de la información, infraestructura de procesamiento y aplicaciones
BAI07	Gestionar la Aceptación del Cambio y la Transición	Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas
			12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
BAI08	Gestionar el Conocimiento	Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación,	09 Agilidad de las TI

		organización, mantenimiento, uso y retirada de conocimiento.	17 Conocimiento, experiencia e iniciativas para la innovación de negocio
BAI09	Gestionar los Activos	Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento(acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.	06 Transparencia de los costes, beneficios y riesgo de las TI
			11 Optimización de activos, recursos y capacidades de TI
BAI10	Gestionar la Configuración	Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.	02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas.
			11 Optimización de activos, recursos y capacidades de TI
			14 Disponibilidad de información útil y relevante para la toma de decisiones

4. Entrega, Servicio y Soporte (DSS)

Etiqueta del Proceso	Nombre	Descripción	Principales Metas de TI que apoya
DSS01	Gestionar operaciones.	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	04 Riesgos de negocio relacionados con las TI gestionados
			07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
			11 Optimización de activos recursos y capacidades de TI
DSS02	Gestionar Peticiones e Incidentes de Servicio	Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.	04 Riesgos de negocio relacionados con las TI gestionados
			07 Entrega de servicios de TI de acuerdo a los requisitos del negocio
DSS03	Gestionar Problemas	Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.	04 Riesgos de negocio relacionados con las TI gestionados
			07 Entrega de servicios TI de acuerdo a los requisitos del negocio
			11 Optimización de activos, recursos y capacidades y de TI
			14 Disponibilidad de información útil y relevante para la toma de decisiones
DSS04	Gestionar la Continuidad	Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.	04 Riesgos de negocio relacionados con las TI gestionados
			07 Entrega de servicios TI de acuerdo a los requisitos del negocio
			14 Disponibilidad de información útil y relevante para la toma de

			decisiones
DSS05	Gestionar Servicios de Seguridad	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
			04 Riesgos de negocio relacionados con las TI gestionados
			10 Seguridad de la información, infraestructura de procesamiento y aplicaciones
DSS06	Gestionar Controles de Proceso de Negocio	Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.	04 Riesgos de negocio relacionados con las TI gestionados
			07 Entrega de servicios TI de acuerdo a los requisitos del negocio

5. Supervisar, Evaluar y Valorar (MEA)

Etiqueta del Proceso	Nombre	Descripción	Principales Metas de TI que apoya
MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad.	Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.	04 Riesgos de negocio relacionados con las TI gestionados
			07 Entrega de servicios TI de acuerdo a los requisitos del negocio
			11 Optimización de activos, recursos y capacidades de TI
			15 Cumplimiento de las políticas internas por parte de TI
MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.	02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
			04 Riesgos de negocio relacionados con las TI gestionados
			15 Cumplimiento de las políticas internas por parte de TI
MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos.	Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.	02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas
			04 Riesgos del negocio relacionados con las TI gestionados