UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"

"Facultad de Ciencias Físicas y Matemáticas"

Escuela Profesional de Ingeniería en Computación e Informática

"Auditoría Informática bajo el estándar COBIT en el Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque – 2015"

AUTORAS:

Bach. Shirley Lizeth Carrillo Prada

Bach. Kely Karina Suclupe Tejada

ASESORA:

MSc. Ing. Jessie Leila Bravo Jaico

Para optar el Título Profesional de
Ingeniera en Computación e Informática

Chiclayo, Abril del 2016

DEDICATORIA

Al creador de todas las cosas, el que me ha dado fortaleza para continuar cuando he estado a punto de caer, por permitirme llegar a este momento tan especial en mi vida, por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más, con toda humildad dedico este trabajo a Dios.

A mi madre, por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional sin importar nuestras diferencia de opiniones. A mi padre quien con sus sabios consejos ha sabido guiarme para culminar mi carrera profesional. Gracias a ellos que me han dado todo lo que soy como persona, mis valores, mis principios, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

A mis hermanos por estar siempre presentes, acompañándome para poder realizarme, apoyándome no sólo con los recursos necesarios, sino también con sus consejos y su ejemplo de perseverancia. A mi sobrino Camilo quien ha sido y es mi motivación, inspiración y felicidad.

Autora: Shirley Lizeth Carrillo Prada

DEDICATORIA

Primeramente a Dios como ser supremo y creador nuestro, el centro de mi vida y mi fortaleza, al forjador de mi camino, él que siempre me acompaña y derrama sus bendiciones sobre mí y llenarme de su fuerza para vencer todos los obstáculos desde el principio de mi vida, a él por habernos permitido llegar hasta este punto brindándonos su amor, paciencia y sabiduría.

A mis padres Adelaida Tejada y José Suclupe a quienes admiro de todo corazón por todo el esfuerzo y sacrificio que hicieron por mí a pesar de las dificultades, por brindarme todo su amor, la comprensión, el apoyo incondicional y la confianza en cada momento de mi vida.

A mi hermana a quien es un ejemplo a seguir, porque juntas podemos formar un futuro mejor para nuestra familia, por brindarme sus sabios consejos y su más sincero apoyo.

Autora: Kely Karina Suclupe Tejada

AGRADECIMIENTO

A Dios por haberme dado fuerza y valor para culminar esta etapa en mi vida.

Agradezco también la confianza y el apoyo brindado por parte de mis padres que sin duda alguna en el trayecto de mi vida me han demostrado su amor, corrigiendo mis faltas y celebrando mis triunfos.

Autoras: Shirley Lizeth Carrillo Prada

A mis padres porque creyeron en mí, brindándome una carrera para mi futuro, dándome ejemplos dignos de superación y entrega, por su amor, paciencia y sabios consejos para ser unas personas de bien.

A mi hermana y abuelos por haberme fomentado en mí, el deseo de superación y el anhelo de triunfo en la vida.

Autoras: Kely Karina Suclupe Tejada

A la ingeniera Jessie Bravo Jaico, por el asesoramiento y tiempo brindado, por su apoyo que nos permitió culminar el desarrollo de nuestra tesis.

Autoras: -Shirley Lizeth Carrillo Prada
-Kely Karina Suclupe Tejada

RESUMEN

El presente proyecto se desarrolló en la Gerencia Regional de Salud Lambayeque, en la cual se realizará una auditoría informática bajo el estándar COBIT para su Centro de Sistemas de Información.

A través de encuestas, checklist y entrevistas aplicadas, se determinó diversos problemas en lo que concierne a gestión de TI, entre los principales hallamos la congestión de problemas en los sistemas y redes, que se presentan a diario en las diferentes áreas de la GERESA, debido a que no existe un proceso que contrate, mantenga y motive los recursos humanos de TI para la creación y entrega de servicios de TI al negocio.

Además se identificó que el personal TI no tiene conocimiento de todos los problemas que existen en el área, cómo funciona cada proceso y esto se debe a que no se realiza una supervisión de manera continua. Otro problema es el inminente peligro de pérdida de información en la GERESA, debido a que no existen mecanismos de seguridad que permitan proteger la integridad de la información de la empresa.

Para esto se identificó los controles que aplican a la auditoría, entre algunos de ellos tenemos al Gestionar los Recursos Humanos, Gestionar las Peticiones y los Incidentes del Servicio y al Gestionar los servicios de seguridad; para lo cual se está utilizando COBIT versión 5, la cual nos sirve como guía de buenas prácticas en lo que respecta a la gestión de TI.

Para el desarrollo de la Auditoría se utilizó la metodología PDCA, lo cual permitió eliminar procesos repetitivos, logrando así reducir tiempos y mejoras en el análisis de cada proceso.

Determinándose después de aplicada la evaluación, que no existe un proceso que contrate, mantenga y motive los recursos humanos de TI para entrega de servicios de TI al negocio, lo que genera que el poco personal de TI se congestione con los problemas en los sistemas y redes, que se presentan a diario en la empresa. Además si bien el área del CSI, cuenta con algunos controles que permiten verificar los procesos TI, hace falta que se realice una correcta supervisión para brindar un mayor aseguramiento de las políticas de la empresa.

Llegándose a desarrollar observaciones de manera detallada, fijándose riesgos por cada observación y generándose así, recomendaciones que ayuden a corregir las falencias encontradas.

Palabras Claves: COBIT 5, PDCA, objetivos de control y procesos TI.

ABSTRACT

This thesis proyect,"Computer Audit under COBIT standar in the Centro de Sistemas de Información of the Gerencia Regional de Salud Lambayeque – 2015”, contains the next:

In the development of the Audit in the CSI's area, it was detected that doesn't exist a process that engage, keep and motivate the human resources of TI for installment of TI's services at business, generating that the few number of staff get congested with the problems in the systems and networks, presented diary in the different areas of the GERESA.

Besides in this thesis proyect was used COBIT 5, which serve like a good practice guide respecting to TI's management of the business.

For apply this audit we had to apply a quiz to CSI's coordinator and responsible ok a few areas that have relation with the process that COBIT 5 has detailed. In agreement to those results were selected the controls that would take into account for this Audit.

Then we did an analysis for evaluate the control's objectives that are effectives in the business and which not, in agreement of COBIT 5.

Likewise we developed the audit detailing each one of the control's objectives like (Observation and risk), allowing generate recommendations to each one of these.

The CSI's area have some controls that allow to check the TI's process but it needs a correct supervision to provide an increase in the security of business policies. That area doesn't realize the correct measure of security that verify the theft information of the business.

The staff of CSI's area is trained, but the training is realized once a year when it should be made steadily for keep to staff updated.

Keywords: COBIT 5, PDCA, and Process Control Objectives IT.

INDICE GENERAL

Contenido

DEDICATORIA 1
DEDICATORIA 2
AGRADECIMIENTO 3
RESUMEN 4
ABSTRACT 5
INDICE DE CUADROS 9
INDICE DE FIGURAS 12
INTRODUCCIÓN 14
CAPITULO I 16
Datos Generales de la Organización 16
1.1.- Descripción de la Organización 17
1.2.-Misión, Visión y Objetivos de la Organización 17
1.2.1. Misión 17
1.2.2. Visión 17
1.2.3. Objetivos de la empresa 18
1.2.4. Misión, Visión y Objetivo del Área del Centro de Sistemas de Información 19
1.3.-Estructura Orgánica 20
CAPITULO II 21
PROBLEMÁTICA DE LA INVESTIGACIÓN 21
2.1.- Realidad Problemática 22
2.1.1. Planteamiento del Problema 22
2.2.- Formulación del Problema 23
2.3.- Justificación e Importancia de la Investigación 24
2.4.- Objetivos de la Investigación 25
2.4.1. Objetivo General 25
2.4.2. Objetivos Específicos 25
2.5.- Limitaciones de la Investigación 26
CAPITULO III 27
MARCO METODOLÓGICO 27
3.1.- Tipo de Investigación 28
3.2.- Hipótesis 28

3.3.- Variables....28
3.3.1. Variable Independiente: Auditoría Informática....28
3.3.2. Variable Dependiente: Gestión Tecnología de Información....29
3.4.- Criterios de Selección de la Metodología empleada....29
3.5.- Selección de la Metodología a utilizar para el Desarrollo de la Investigación....30
3.5. 1. PDCA O Círculo de Deming....31
CAPITULO IV....34
MARCO TEÓRICO....34
4.1.- Antecedentes de la Investigación:....35
4.1.1. Antecedentes en el contexto internacional....35
4.1.2. Antecedentes en el contexto nacional....37
4.1.3. Antecedentes en el contexto local....39
4.2.- Desarrollo de la Temática....41
4.2.1. AUDITORÍA....41
4.2.2. TECNOLOGÍA DE LA INFORMACIÓN....45
4.2.3. COBIT 5....49
CAPITULO V....60
DESARROLLO DE LA PROPUESTA....60
5.1.-Plan de Auditoría para la Gestión de TI....61
5.1.1. Alcance dela Auditoría de la Gestión de TI....61
5.2. Determinación de los Procesos COBIT aplicables a la auditoría en ejecución.....62
5.3.-Programa de Auditoría y Matriz de Prueba de los Procesos y Objetivos de Control..77
5.4.- Análisis de Verificación....116
5.5.-Informe Preliminar....136
5.6.- Informe Final De Auditoría....144
CAPITULO VI....154
COSTOS Y BENEFICIOS....154
6.1.-Análisis de Costos....155
6.1.1. Costo de Servicio y Materiales....155
6.1.2.-Beneficios....156
6.2.- Recuperación de la Inversión....157
CAPITULO VII....166
CONCLUSIONES....166
CAPITULO VIII....168
RECOMENDACIONES....168

CAPITULO IX.....171

REFERENCIAS BIBLIOGRÁFICAS 171

ANEXOS 174

INDICE DE CUADROS

Cuadro Nº 1. Comparación de Metodologías……..……..30
Cuadro Nº 2. Comparación de Estándares…….....58
Cuadro Nº 3. Programa de Auditoría APO07.01……..…....78
Cuadro Nº 4. Matriz de Pruebas APO07.01…….....79
Cuadro Nº 5. Programa de Auditoría APO07.03……..…….....80
Cuadro N º 6. Matriz de Pruebas APO07.03 ……81
Cuadro N º 7. Programa de Auditoría APO07.04…….…….....82
Cuadro Nº 8. Matriz de Pruebas APO07.04…….....83
Cuadro Nº 9. Programa de Auditoría APO07.06……..……84
Cuadro Nº 10. Matriz de Pruebas APO07.06……..…….85
Cuadro Nº 11. Programa de Auditoría DSS02.01……..…….....86
Cuadro Nº 12. Matriz de Pruebas DSS02.01……...87
Cuadro Nº 13. Programa de Auditoría DSS02.02……..…….....88
Cuadro Nº 14. Matriz de Pruebas DSS02.02…….....89
Cuadro Nº 15. Programa de Auditoría DSS02.04…….....90
Cuadro Nº 16. Matriz de Pruebas DSS02.04……..…….....91
Cuadro Nº 17. Programa de Auditoría DSS05.02…….....92
Cuadro Nº 18. Matriz de Pruebas DSS05.02……..…….....93
Cuadro Nº 19. Programa de Auditoría DSS05.03……...……94
Cuadro Nº 20. Matriz de Pruebas DSS05.03…….....…….95
Cuadro Nº 21. Programa de Auditoría DSS06.01…….....96
Cuadro Nº 22. Matriz de Pruebas DSS06.01……...……97
Cuadro Nº 23. Programa de Auditoría DSS06.06…….....98
Cuadro Nº 24. Matriz de Pruebas DSS06.06…….....99
Cuadro Nº 25. Programa de Auditoría MEA01.01……100
Cuadro Nº 26. Matriz de Pruebas MEA01.01……101
Cuadro Nº 27. Programa de Auditoría MEA01.04…….....102
Cuadro Nº 28. Matriz de Pruebas MEA01.04……..……..103
Cuadro Nº 29. Programa de Auditoría MEA01.05……...…….....104
Cuadro Nº 30. Matriz de Pruebas MEA01.05……105

Cuadro Nº 31. Programa de Auditoría MEA02.01……...106
Cuadro Nº 32. Matriz de Pruebas MEA02.01……107
Cuadro Nº 33. Programa de Auditoría MEA02.02…….....108
Cuadro Nº 34. Matriz de Pruebas MEA02.02…….....109
Cuadro Nº 35. Programa de Auditoría MEA02.03…….....110
Cuadro Nº 36. Matriz de Pruebas MEA02.03…….....111
Cuadro Nº 37. Programa de Auditoría MEA02.06…….....112
Cuadro Nº 38. Matriz de Pruebas MEA02.06…….....113
Cuadro Nº 39. Programa de Auditoría MEA02.07……114
Cuadro Nº 40. Matriz de Pruebas MEA02.07…….....115
Cuadro Nº 41. Evaluación de Pruebas APO07.01…….....117
Cuadro Nº 42. Evaluación de Pruebas APO07.03……...118
Cuadro Nº 43. Evaluación de Pruebas APO07.04……...119
Cuadro Nº 44. Evaluación de Pruebas APO07.06……120
Cuadro Nº 45. Evaluación de Pruebas DSS02.01…….....121
Cuadro Nº 46. Evaluación de Pruebas DSS02.02……..……..122
Cuadro Nº 47. Evaluación de Pruebas DSS02.04……..……..123
Cuadro Nº 48. Evaluación de Pruebas DSS05.02……124
Cuadro Nº 49. Evaluación de Pruebas DSS05.03……125
Cuadro Nº 50. Evaluación de Pruebas DSS06.01……126
Cuadro Nº 51. Evaluación de Pruebas DSS06.01……127
Cuadro Nº 52. Evaluación de Pruebas MEA01.01……...128
Cuadro Nº 53. Evaluación de Pruebas MEA01.04……129
Cuadro Nº 54. Evaluación de Pruebas MEA01.05……...130
Cuadro Nº 55. Evaluación de Pruebas MEA02.01……131
Cuadro Nº 56. Evaluación de Pruebas MEA02.02……....132
Cuadro Nº 57. Evaluación de Pruebas MEA02.03……133
Cuadro Nº 58. Evaluación de Pruebas MEA02.06……...134
Cuadro Nº 59. Evaluación de Pruebas MEA02.07……...135
Cuadro Nº 60. Costos por Licencias……...157
Cuadro Nº 61. Costo por Capacitación……..158
Cuadro Nº 62. Costos por Viáticos...…….....158
Cuadro Nº 63. Costos Total de Inversión…….....159

Cuadro Nº 64. Costos por Soporte Técnico……....159

Cuadro Nº 65. Costos por Auditaría. ……..…..159

Cuadro Nº 66. Costo Total de Operación…….....160

Cuadro Nº 67. Reducción Costos en Multa……....160

Cuadro Nº 68. Ahorro de pérdidas de información……....161

Cuadro Nº 69. Actualización del Plan de Contingencia…….....161

Cuadro Nº 70. Ahorro de Capacitación de Personal…….....162

Cuadro Nº 71. Total de Beneficios Tangibles…….……...162

Cuadro Nº 72. Resultados de CI, CO y B. …….…….....163

Cuadro Nº 73. Valor Actual Neto……...…....164

Cuadro Nº 74. Resultado del Tasa Interna de Retorno……..…....165

INDICE DE FIGURAS

Figura Nº 1. Organigrama GERESA.....20
Figura Nº 2. Círculo de Deming…….....30
Figura Nº 3. Tecnología de la Información.....47
Figura Nº 4. Evolución del alcance. 49
Figura Nº 5. Comparación de Estructura de COBIT 4.1 y COBIT 5….....52
Figura Nº 6. Niveles del COBIT.....53

INDICE DE ANEXOS

ANEXO Nº 1. Encuesta Aplicada al Coordinador del Área del CSI…….…....175

ANEXO Nº 2: Encuesta Aplicada A Los Trabajadores de GERESA.……179

ANEXO Nº3. Checklist Aplicada al Coordinador del CSI……....184

ANEXO Nº4. Checklist Aplicada al Jefe de Gestión y Desarrollo de Potencial Humano (RR.HH) …….…….186

ANEXO Nº 5. Checklist Aplicada al Responsable de Soporte Técnico-CSI…….187

ANEXO Nº 6. Checklist Aplicada al Responsable de Control Interno……..189

ANEXO Nº 7. Acta de conformidad de Entrevistas y Checklist aplicados……...190

ANEXO Nº 8. Configuración de los Equipos……....191

ANEXO Nº 9. Plan de Contingencia…….....194

ANEXO Nº 10. Directiva Nº. -2015-GR.LAMB……..201

ANEXO Nº 11. Capacitaciones y Proformas……..203

ANEXO Nº 12. INDECOPI……..…….....204

ANEXO Nº 13. Pérdidas de Información……....205

ANEXO Nº 14. Actualización del Plan de Contingencia……...205

ANEXO Nº 15. Gerencia Regional de Salud Lambayeque……..……...206

INTRODUCCIÓN

A través de las encuestas, checklist y entrevistas aplicados, se determinó diversos problemas en lo que concierne a gestión de TI, entre los principales hallamos la congestión de problemas en los sistemas y redes, que se presentan a diario en las diferentes áreas de la Gerencia Regional de Salud Lambayeque, debido a que no existe un proceso que contrate, mantenga y motive los recursos humanos de TI para la creación y entrega de servicios de TI al negocio.

Además se identificó que el personal TI no tiene conocimiento de todos los problemas que existen en el área, cómo funciona cada proceso y esto se debe a que no se realiza una supervisión de manera continua. Otro problema es el inminente peligro de pérdida de información en la GERESA, debido a que no existen mecanismos de seguridad que permitan proteger la integridad de la información de la empresa.

Como objetivos en este proyecto de tesis tenemos el realizar la auditoría informática en el Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque, utilizando el estándar COBIT (Control Objectives For Information and Related Technology), con el fin de mejorar la gestión de TI en la empresa, luego tenemos el describir la situación actual del área a auditar, respecto a los procesos TI que se ejecutan en el área, especificar los controles del estándar COBIT que se aplicarán, con respecto a los procesos de Gestión de TI y emitir recomendaciones que permitan mejorar la gestión en el área del CSI bajo el estándar COBIT en la GERESA.

Al aplicar esta auditoría, permitirá aumentar la eficiencia y eficacia en el desarrollo de las operaciones, haciendo los procedimientos más seguros y brindando mayor agilidad de las actividades de la organización.

Anteriormente se han hecho estudios similares en diversos países del mundo al igual que en nuestro país, uno de ellos es la tesis realizada en la Universidad Peruana de Ciencias Aplicadas, la cual tiene por título "Adaptación de Modelo de Gobierno y Gestión para la empresa VirtIT Expert Basado en COBIT 5", otro proyecto interesante que nos sirvió como antecedente fue la tesis realizada en la Universidad Católica Santo Toribio de Mogrovejo, teniendo como título "Auditoría de Sistemas Informáticos".

Para el presente proyecto, se hizo un estudio y verificación de documentos, luego de llevar a cabo la revisión de la documentación del CSI, que es utilizado en la GERESA, y de ejecutar el análisis respectivo, de acuerdo al estándar COBIT 5, se

pudo obtener evaluación de las pruebas efectuadas sobre la gestión de TI que nos permitieron generar objetivos de control efectivos y no efectivos, las mismas que se indican en el INFORME PRELIMINAR, la cual en base a la evaluación de las pruebas efectuadas sobre la gestión de TI de la GERESA se determinó que 9 de los objetivos de control detallados, cumplen con las condiciones necesarias, por lo cual se consideran **efectivos,** el cual tuvieron su discusión y análisis previo con el responsable del área del CSI, dentro de la organización, en este caso el Coordinador del CSI, Responsable de Soporte Técnico y Responsable del Área de Recursos Humanos. Así mismo se determinó que 10 de los objetivos de control analizados, no cumplen con las condiciones necesarias, por lo cual se consideran **no efectivos**. El cual fue presentado y discutido con el Coordinador del CSI, recibiendo del mismo las justificaciones respectivas, relacionadas con algunas observaciones, riesgos y recomendaciones.

Posteriormente se elaboró el INFORME FINAL de la auditoría, detallando cada uno de los 10 Observaciones de los objetivos de control no efectivos en la empresa, permitiendo generar recomendaciones, el cual ha sido presentado al Coordinador del CSI. El documento incluye un resumen gerencial junto con las conclusiones y recomendaciones obtenidas.

CAPITULO I

Datos Generales de la Organización

1.1.- Descripción de la Organización

La Gerencia Regional de Salud Lambayeque, es una institución que promueve la prevención y vela por la apropiada atención integral de salud de todos los habitantes en distintos centros de la Región Lambayeque.

El 11 de Diciembre de 1942, fue creado el Ministerio de Salubridad y Asistencia Social de acuerdo a la Ley N° 3679, durante los próximos años, se optó por la necesidad de descentralizar las acciones de salud en todo el país, por tal motivo en el año 1964 se crea en nuestra ciudad la Unidad de Salud nombrándose como su primer Jefe al Dr. Francisco Cabrera, Médico Sanitario y como Enfermera a la Sra. Noemí Polo; funcionando esta Entidad en la calle Vicente de la Vega N° 1149.

Actualmente tienen por Gerente al Dr. Víctor Hugo Torres Anaya, así mismo la Gerencia Regional de Salud Lambayeque, se encuentra ubicada en la ciudad de Chiclayo en la Av. Salaverry N° 1610 - Urb. Quiñones.

1.2.-Misión, Visión y Objetivos de la Organización

En esta parte se detallará la misión, visión y objetivos de la empresa Gerencia Regional de Salud Lambayeque. (Lambayeque, 2016)

1.2.1. Misión

Somos una Gerencia Regional de Salud que gobierna el sistema regional de salud y que genera las condiciones adecuadas para promover el derecho a la salud con la corresponsabilidad del Estado, el individuo, la familia y la comunidad con calidad y equidad.

1.2.2. Visión

Ser una Gerencia Regional de Salud eficiente y líder que garantice la atención de las necesidades de salud con recurso humano competente, servicios de salud organizados y articulando diversos actores estratégicos, en concordancia con las prioridades regionales, que contribuya al desarrollo integral y sostenido de la Región Lambayeque.

1.2.3. Objetivos de la empresa

- Lograr que las personas adquieran capacidades y desarrollen actitudes, para su desarrollo físico, mental y social, para fomentar una cultura de salud basada en la familia como unidad básica de salud y para que difundan un entorno ambiental saludable en su comunidad.
- Lograr que todos los niños reciban lactancia materna exclusiva, ablactancia nutritiva y adecuada nutrición infantil.
- Reducir significativamente la morbimortalidad causada por enfermedades transmisibles y no transmisibles.
- Lograr la protección de la vida y la salud de todas las personas desde su concepción y durante sus etapas de vida hasta su muerte natural.
- Reducir significativamente la morbimortalidad materno-infantil.
- Reducir significativamente la prevalencia de la desnutrición infantil.
- Reducir significativamente las causas y la ocurrencia de las enfermedades crónicas y degenerativas.
- Optimizar el acceso de la población de pobreza y extrema pobreza al Seguro Integral de Salud (SIS).
- Incrementar el acceso oportuno y uso racional de medicamentos eficaces, seguros y de calidad.
- Lograr la calidad, seguridad y disponibilidad de los productos farmacéuticos y afines en su jurisdicción para toda la población.
- Incrementar significativamente la salubridad del ambiente.
- Incrementar significativamente la capacidad de gestión administrativa y la capacidad resolutiva de las entidades del sector salud.
- Reestructurar y modernizar los sistemas administrativos y operativos.
- Desarrollar capacidades de respuesta necesarias para reducir el impacto de las emergencias y desastres sobre la salud de la población, el ambiente y los servicios de salud.

1.2.4. Misión, Visión y Objetivo del Área del Centro de Sistemas de Información

A continuación se detallará la misión, visión y objetivo del área del Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque. (GERESA, 2013)

1.2.4.1. Misión

Diseño, implementación y control de métodos y procedimientos bajo un entorno organizacional alineado al Plan Operativo Institucional de la Gerencia Regional de Salud; asimismo facilita las condiciones técnicas para el uso racional de los Sistemas de Información haciendo uso de la tecnología Web y el Software Libre.

1.2.4.2. Visión

Posicionarse en el contexto regional como la Unidad Informática líder en Gestión de Tecnologías de Información y Comunicación, que brinda el soporte tecnológico en el moderno desarrollo de la Administración Pública Regional con servicios de calidad, seguros y confiables.

1.2.4.3. Objetivo del área del Centro de Sistemas de Información

Brindar soporte Técnico para la comunicación, sistematización y administración de hardware de las Direcciones y áreas administrativas para el cumplimiento de la misión y objetivos de la Gerencia Regional de Salud Lambayeque, promoviendo así mismo el uso y la aplicación de la informática para la simplificación y mayor eficacia de los procesos que desarrollan.

1.3.-Estructura Orgánica

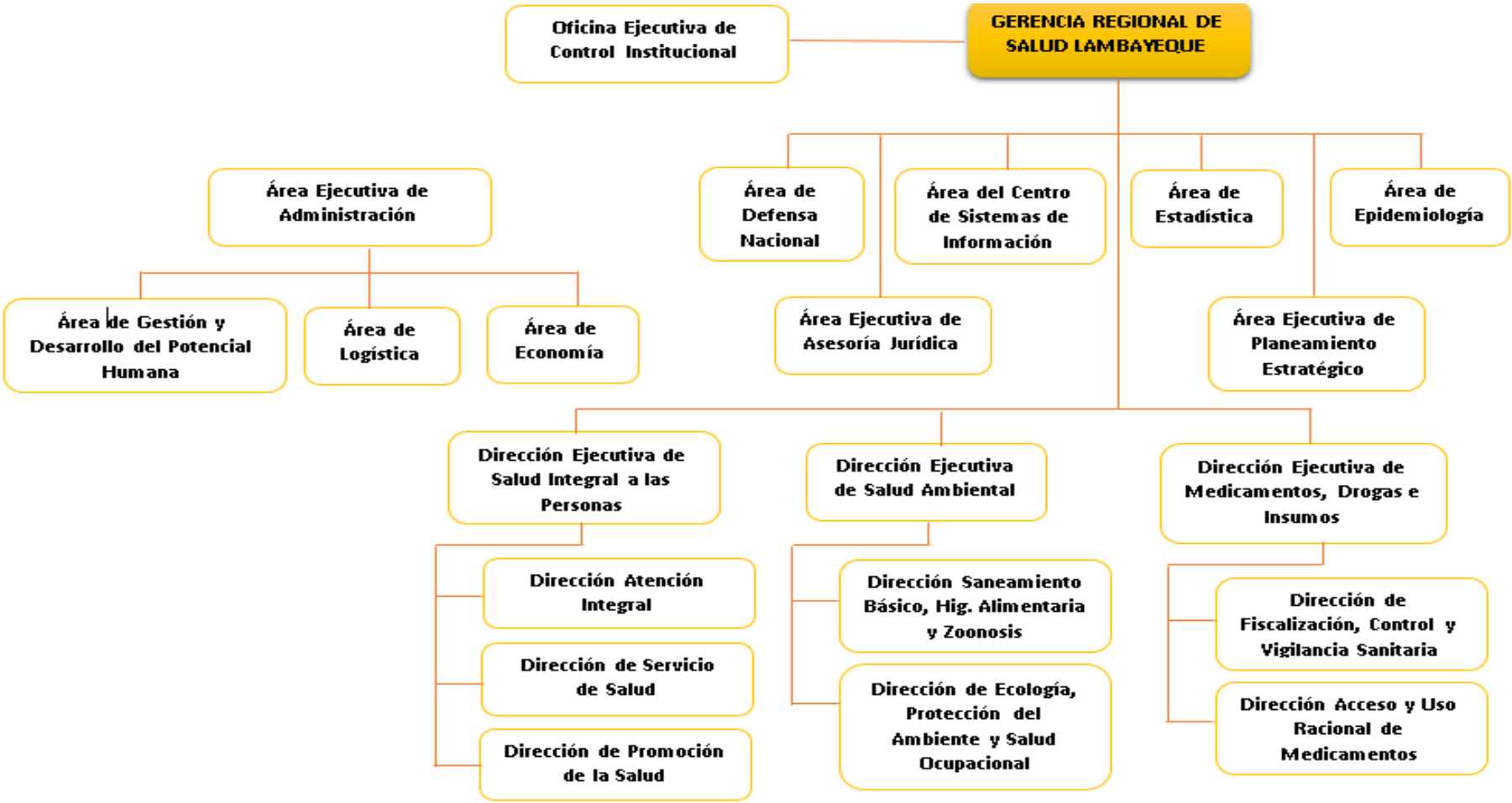


Figura Nº1. Organigrama GERESA
Fuente: (Lambayeque, 2016)

CAPITULO II

PROBLEMÁTICA DE LA INVESTIGACIÓN

2.1.- Realidad Problemática

En el siguiente punto se detallará los problemas hallados, en el área del Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque.

2.1.1. Planteamiento del Problema

El avance tecnológico de los sistemas, las telecomunicaciones ha logrado posicionarse tanto en los sectores públicos como privados en todo el mundo, teniendo un crecimiento muy acelerado, esto ha dado paso a que los sistemas informáticos necesiten un adecuado control. Todas las Tecnologías de Información desde el punto de vista de la Auditoría, presenta una problemática común: la falta de un marco de dominios, procesos y control. La falta de auditoría informática en las empresas, genera una falta grave en el alineamiento con los objetivos del negocio TI, ya que no existe un marco de gobernabilidad TI que ayude a las buenas prácticas que COBIT presenta.

La Gerencia Regional de Salud, ubicada en la ciudad de Chiclayo, inicio su actividad en el año 1964, cuando se optó por la necesidad de descentralizar las acciones de salud en todo el país, sede la cual tuvo por jefe al Dr. Francisco Cabrera.

Según la encuesta realizada en el área del Centro de Sistemas de Información el día 15 de Octubre del 2015, encontramos diversos problemas en lo que concierne a gestión de TI, uno de ellos es que no existe un proceso que contrate, mantenga y motive los recursos humanos de TI para la creación y entrega de servicios de TI al negocio, lo que genera que el poco personal de TI se congestione con los problemas en los sistemas y redes, que se presentan a diario en las diferentes áreas de la GERESA.

Otra irregularidad que se tiene es que no se realiza de manera continua una supervisión, evaluación y valorización del rendimiento y conformidad en el desempeño de las TI, lo cual genera que el personal TI no tenga conocimiento de todos los problemas que existen en el área, cómo está funcionando cada proceso, y qué se puede hacer para arreglar los problemas que existen.

Así mismo las revisiones actuales y proyecciones sobre la capacidad y desempeño de los recursos TI no están sincronizadas con las proyecciones de demanda del negocio, esto genera que no se tenga un control adecuado de si se está o no, actuando conforme con los requerimientos externos.

Tenemos también inconvenientes debido a que las necesidades y requerimientos futuros de información no se exploran de manera proactiva, y esto no permite satisfacer las necesidades de los usuarios que es una de las cosas que deben ser primordiales.

Otro importante problema es que no existen mecanismos de seguridad que permitan proteger la integridad de la información de la empresa, lo cual genera que haya un inminente peligro de pérdida de información de las diferentes áreas de la GERESA.

Finalmente también se realizó una encuesta a los trabajadores de la Gerencia Regional de Salud Lambayeque, de acuerdo a los resultados obtenidos, encontramos que el 65% de usuarios tiene problemas con la caída del sistema que utilizan (SIGA, SIAF, SISMED y SISGEDO), el 18% tiene problemas con virus en sus computadoras, el 11% tiene problemas con el internet ya que es lento en determinada ocasiones y el 6% tiene problemas para poder instalar un programa porque es necesario una contraseña para esto, lo que ocasiona insatisfacción por parte de los usuarios y no permite ofrecer un servicio de calidad.

2.2.- Formulación del Problema

¿La realización de una Auditoría Informática bajo el estándar COBIT en el Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque, mejorará la gestión de TI?

2.3.- Justificación e Importancia de la Investigación

Seguidamente explicaremos a detalle la justificación e importancia de la presente investigación.

2.3.1. Justificación:

- **Justificación Económica:** Porque aquello que vamos a plantear, una vez terminado el proyecto de investigación, permitirá a la Gerencia Regional de Salud Lambayeque intercomunicarse con todas sus áreas minimizando costos y tener un mayor rendimiento.
- **Justificación Operativa**: Porque la Auditoría Informática permitirá aumentar la eficiencia y eficacia en el desarrollo de las operaciones, haciendo los procedimientos más seguros y brindando mayor agilidad de las actividades de la organización.
- **Justificación Académica:** Porque este presente proyecto permitirá aplicar conceptos de auditoría informática y además el marco de referencia de buenas prácticas COBIT, además de la metodología PDCA.
- **Justificación Tecnológica:** El resultado del trabajo de investigación permitirá optimizar los recursos tecnológicos de la organización.

2.3.2. Importancia:

La situación actual por la que atraviesa la Gerencia Regional de Salud Lambayeque, requiere que, mediante el uso de un conjunto de procedimientos y técnicas, se proceda a evaluar y controlar los sistemas de información y el ambiente informático, con el fin de constatar si sus procesos y actividades son correctos y, se encuentran enmarcados y en conformidad con las mejores normativas informáticas y generales de la organización.

La auditoría informática en el Centro de Sistemas de Información es importante ya que proporcionará controles necesarios y harán las operaciones más confiables y tendrán un buen nivel de seguridad, equipos tecnológicos y personal capacitado; aumentando la eficiencia en el desarrollo de estas, propiciando mayor rendimiento en la empresa.

2.4.- Objetivos de la Investigación

En el siguiente punto se dará a conocer cuál es el objetivo General y Objetivos específicos del presente proyecto.

2.4.1. Objetivo General

Realizar la auditoría informática en el Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque, utilizando el estándar COBIT (Control Objectives For Information and Related Technology), con el fin de mejorar la gestión de TI de la empresa.

2.4.2. Objetivos Específicos

- Describir la situación actual del área del Centro de Sistemas de Información, respecto a los procesos TI que se ejecutan en esta área.
- Especificar los controles del estándar COBIT que se aplicará en el Centro de Sistemas de Información.
- Aplicar el estándar COBIT en el Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque con respecto a los procesos de Gestión de TI.
- Emitir recomendaciones que permitan mejorar la gestión en el Centro de Sistemas de Información bajo el estándar COBIT en la Gerencia Regional de Salud Lambayeque.
- Determinar la rentabilidad de la auditoría, señalando los costos y beneficios que se obtendrían al aplicar las recomendaciones emitidas en el informe de auditoría, mediante una evaluación económica.

2.5.- Limitaciones de la Investigación

En este presente proyecto de Investigación encontramos las siguientes limitaciones:

- Limitaciones de Tiempo: Debido a la duración limitada del proyecto, podemos tener inconvenientes en el tiempo con el que contamos para desarrollar la investigación y el estudio.
- Limitaciones de Tiempo por parte de los trabajadores de la empresa: Debido a sus labores no cuentan con el tiempo disponible para brindarnos la información requerida para el desarrollo de nuestro informe.
- Escasa bibliografía referida a la temática de investigación, tanto en la biblioteca central de nuestra Universidad como la de la facultad.

CAPITULO III

MARCO METODOLÓGICO

3.1.- Tipo de Investigación

Investigación Tecnológica Formal

3.2.- Hipótesis

La realización de una auditoría informática bajo el estándar COBIT, mejorará la gestión de TI del Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque.

3.3.- Variables

A continuación se definirá las variables del proyecto, tanto la variable independiente como la variable dependiente.

3.3.1. Variable Independiente: Auditoría Informática

- **Definición Conceptual:** Es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas
- **Definición Operacional:** La revisión crítica construida de las operaciones efectuadas, en las empresa, así como en los procedimientos seguido para su desarrollo y registros tendientes a obtener un seguro como oportuna información constituye la esencia de esta auditoría, se centra en la calidad de operaciones.

3.3.2. Variable Dependiente: Gestión Tecnología de Información

- **Definición Conceptual:** Son aquellas tareas y funciones que se realizan en las diferentes áreas de la informática como son: Software, Redes, Base de Datos, etc.
- **Definición Operacional:** Por actividades de TI entendemos que son aquellas tares que se realizan dentro del área de informática de una empresa tales como: mantenimiento preventivo y/o correctivo del Hardware y Software, Creación de Usuarios Locales, Administración de Servidores, Administración de base de Datos, etc.

3.4.- Criterios de Selección de la Metodología empleada

De acuerdo a la investigación de este proyecto de tesis optamos por elegir la Metodología PDCA, una importante herramienta de gestión, ya que es aplicable a cualquier actividad, la cual conduce a las mejoras continuas de gestión.

El círculo de Deming o PDCA lo componen 4 etapas cíclicas, de forma que una vez acabada la etapa final se debe volver a la primera y repetir el ciclo de nuevo, de forma que las actividades son reevaluadas periódicamente para incorporar nuevas mejoras. La aplicación de esta metodología está enfocada principalmente para para ser usada en empresas y organizaciones.

3.5.- Selección de la Metodología a utilizar para el Desarrollo de la Investigación

La Metodología que se está utilizando para el desarrollo de la Auditoría es la PDCA, también conocida como el ciclo o círculo de Deming, la cual se explicará y comparará con otras metodologías en el cuadro que se muestra a continuación:

COMPARACIÓN DE METODOLOGÍAS PDCA, KAYZEN Y DMAIC			
	PDCA	**KAIZEN**	**DMAIC**
DESCRIPCIÓN	Esta metodología describe los cuatro pasos esenciales como son: Planificar, Hacer, Verificar y Actuar; que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales).	El término Kaizen es de origen japonés, y significa "cambio para mejorar", lo cual con el tiempo se ha aceptado como "Proceso de Mejora Continua". Consiste en integrar de forma activa a todos los trabajadores de una organización en sus continuos procesos de mejora, a través de pequeños aportes.	Es un acrónimo de los pasos de la metodología: Definir, Medir, Analizar, Mejorar y Controlar. Es una herramienta de la metodología Seis Sigma, enfocada en la mejora incremental de procesos existentes.
VENTAJAS	-Consiguen mejoras en un corto plazo y resultados visibles. -Incrementa la productividad y dirige a la organización hacia la competitividad, lo cual es de vital importancia para las actuales organizaciones. -Permite eliminar procesos repetitivos.	- Reducción en fallas de los equipos y herramientas.	-Promueve cambios en la organización de manera continua.
DESVENTAJAS	En vista de que los gerentes en la pequeña y mediana empresas son muy conservadores, el mejoramiento continuo se hace un proceso muy largo.	-Debe existir un fuerte compromiso por parte de la dirección o gerencia. -Se deben hacer inversiones importantes de dinero.	-Lleva mucho esfuerzo, tiempo y recursos aplicar todos los pasos cada vez que en necesario aplicar un problema. -No se ven resultados en el corto plazo.

Cuadro Nº 1. Comparación de Metodologías

Fuente: (Shewhart, Elaboración Propia)

- ✓ **Elección de la Metodología a utilizar**

Se optó por la metodología PDCA, ya que se adapta mejor a este tipo de proyectos, a comparación de las otras metodologías, no solo por ser una de las más utilizadas, sino porque se enfoca en un proceso idóneo para auditorias informáticas.

3.5. 1. PDCA O Círculo de Deming

Es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter Andrew Shewhart.

Los resultados de la implementación de este ciclo permiten a las empresas una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo los costes, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad de la empresa u organización.

Resume en sus siglas: Planear, Do (hacer), Check (revisar) y Actuar haciendo un procesa de mejora.

- Plan
- Hacer
- Verificar
- Actuar

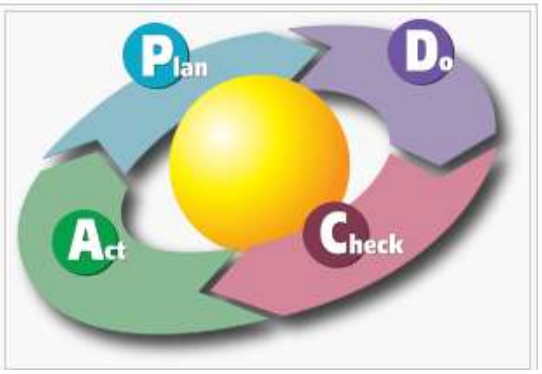


Figura Nº 2. Círculo de Deming

Fuente: (Shewhart, PDCA, 2016).

- **Planificar.-** Busca la mejora y se establece los objetivos a alcanzar. Para buscar posibles mejoras en los grupos de trabajo. Establece los objetivos y procesos necesarios para obtener el resultado esperado.

- **Hacer.-** Realizar los cambios para implantar la mejora propuesta. Haciendo una prueba para el funcionamiento, antes de realizar los cambios a gran escala.

- **Verificar.-** Una vez implantada la mejora, se deja un periodo de prueba para verificar su funcionamiento. Si la mejora no cumple las expectativas habrá que modificarla. Por último, una vez finalizado el período de prueba se deben estudiar los resultados y compararlos con el funcionamiento de las actividades antes implantar la mejora.

- **Actuar.-** Ajustar, corregir o consolidar los resultados obtenidos. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desecharla. (Shewhart, PDCA, 2016).

3.5.1.1. Ventajas

- Se concentra el esfuerzo en ámbitos organizativos y de procedimientos puntuales.
- Consiguen mejoras en un corto plazo y resultados visibles.
- Si existe reducción de productos defectuosos, trae como consecuencia una reducción en los costos, como resultado de un consumo menor de materias primas.
- Incrementa la productividad y dirige a la organización hacia la competitividad, lo cual es de vital importancia para las actuales organizaciones.
- Contribuye a la adaptación de los procesos a los avances tecnológicos.
- Permite eliminar procesos repetitivos.
- Mejora continua de la calidad.

3.5.1.2. Desventajas

- En vista de que los gerentes en la pequeña y mediana empresas son muy conservadores, el mejoramiento continuo se hace un proceso muy largo.
- Hay que hacer inversiones importantes.

3.5.1.3. Relación de la metodología PDCA con COBIT

Como resumen, COBIT vincula los procesos de TI para conseguir objetivos de empresa y mediante una medición constante conseguir una mejora continua de procesos. Todo ello supervisado con responsable de procesos que advierten de necesidades de mejora para implementar el círculo del PDCA, todo ello soportando un pilar para la toma de decisiones. (Shewhart, PDCA DEMING, 2014)

CAPITULO IV

MARCO TEÓRICO

4.1.- Antecedentes de la Investigación:

A continuación se detallara los antecedentes de contexto internacional, nacional y local.

4.1.1. Antecedentes en el contexto internacional

4.1.1.1. Tema: "Auditoría de la Gestión de Seguridad en la Red de Datos de Swissotel Basada en COBIT". (Herrera, 2006)

Autores:

- María del Carmen Matute Macias.
- Transito del Rosario Quispe Cando.

Año: 2006.

Institución: Escuela Politécnica Nacional.

Lugar/País: Quito/Ecuador

Resumen:

El presente proyecto de tesis, abarca los siguientes aspectos:

- Proporcionar a la Gerencia de normas basadas en buenas prácticas para el control de la información y la Tecnología de la Información, lo que incluye a la seguridad informática. COBIT es la herramienta de Gobierno de TI que ayude al entendimiento y a la administración de los riesgos así como de los beneficios asociados con la información y sus tecnologías relacionadas.
- Dar a los usuarios una base confiable para administrar los recursos de TI.
- Proveer a los auditores de buenos criterios para las tareas de evaluación, control y auditoría.
- Suministrar a la Gerencia, responsables de procesos de negocio y auditores, el respaldo suficiente para mejorar la administración de la TI.
- COBIT está diseñado para ser utilizado por los propietarios de los procesos de negocio como una guía clara y entendible para que estos tengan total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio.

Conclusiones:

En este proyecto de tesis se realizó la revisión de los planes estratégicos de la institución para conocer el estado interno en cuanto a TI concierne. Tomando en cuenta que COBIT no proporciona una estructura formal y especifica de cómo desarrollar un plan de auditoría y su ejecución posterior, en su lugar, ofrece una serie de guías de cómo realizar el análisis y evaluación de los controles existentes en la empresa en el área de tecnología de la información y que están relacionados con el alcance de los objetivos de la empresa.

4.1.1.2. Tema: "Diagnóstico para la Implantación de COBIT 4.1 en una Empresa de Producción". (Sánchez, 2012)

Autores:

- Martha Elizabeth de la Torre Morales.
- Ingrid Kathyuska Giraldo Martínez.

Año: 2012.

Institución: Universidad Politécnica Salesiana Ecuador

Lugar/País: Guayaquil/ Ecuador

Resumen:

El presente proyecto de tesis, abarca los siguientes aspectos:

- Contribuir a mejorar los procesos del Departamento de Sistemas mediante el diagnóstico con la metodología COBIT aplicada en la empresa EP.
- Estudiar los treinta y cuatro procesos de COBIT para poder evaluar la situación del departamento de sistemas de la empresa EP.
- Realizar el Diagnóstico de los Procesos y Objetivos de Control de COBIT en el departamento de sistemas.
- Determinar los riesgos relacionados con la prestación de servicios de TI en el departamento de sistemas.
- Evaluar el resultado del diagnóstico realizado en el departamento de sistemas considerando los procesos críticos y las falencias de los controles para extender las recomendaciones respectivas.
- Definir políticas a desarrollar de cinco de los objetivos críticos para el

control de TI en el departamento de sistemas de la empresa EP.

Conclusiones:

Mediante esta Tesis, se pudo evaluar y diagnosticar los procesos de TI; se concluye que los objetivos de control son necesarios para garantizar el correcto funcionamiento, la calidad de los resultados y la mejora continua de las operaciones así como también para detectar debilidades y riesgos potenciales de cada proceso del departamento.

4.1.2. Antecedentes en el contexto nacional

4.1.2.1. Tema: "Adaptación de Modelo de Gobierno y Gestión para la empresa VirtIT Expert Basado en COBIT 5" (Urueña, 2015)

Autores:

- Omar Jesús Bugosen Abi-Gosen
- Christian Daniel Tejada Ruiz

Año: 2015.

Institución: Universidad Peruana de Ciencias Aplicadas

Lugar/País: Lima/Perú

Resumen:

El presente proyecto de tesis, abarca los siguientes aspectos:

- Proponer un modelo un modelo de Gobierno y Gestión enfocado en la entrega de servicios de TI basado en COBIT 5.
- Realizar mapeos de los objetivos de la empresa con los objetivos del Gobierno Empresarial, estos con los objetivos de TI y estos a su vez con los objetivos específicos de los procesos de la empresa.
- Evaluar los procesos actuales con la finalidad de proponer mejoras y definir correctamente los procesos necesarios para una adecuada entrega de servicios de TI.
- Implementar las mejoras propuestas y se presentan los resultados obtenidos, de manera que se garantiza la efectividad de la solución al comparar los resultados finales con los inicialmente obtenidos.

Conclusiones:

En este Proyecto se planteó una solución probada de modelo de Gobierno y Gestión de TI basado en COBIT 5 enfocado en el dominio de gestión Entregar, Dar Servicio y Soporte. Así mismo se concluyó, que es plenamente necesario contar con un adecuado modelo de Gobierno de TI, para garantizar la correcta operación en la entrega de servicios de infraestructura y aplicaciones de TI, apoyado en la mitigación de riesgos y evitando los problemas expuestos.

4.1.2.2. Tema: **"Diseño de un modelo de gobierno de TI con enfoque de seguridad de información para empresas prestadoras de servicios de salud bajo la óptica de cobit 5.0."** (Hoces, 2014)

Autora: Diana Estefanía Lepage Hoces

Año: 2014.

Institución: Pontificia Universidad Católica del Perú.

Lugar/País: Lima/Perú

Resumen:

El presente proyecto de tesis, abarca los siguientes aspectos:

- Diseñar un modelo de gobierno de tecnologías de información, bajo la óptica del marco de negocios COBIT 5.0 para empresas prestadoras de servicios de salud.
- Elaborar el Caso de negocio que justifique la implementación del Gobierno de TI en la organización.
- Mapear las fases del ciclo de vida del Gobierno de TI según COBIT 5.0 para la empresa.
- Elaborar el balance scorecard de TI de la empresa que refleje las necesidades y expectativas de los stakeholders.
- Elaborar a declaración de aplicabilidad de COBIT 5.0 para el enfoque de Seguridad de Información dentro de la empresa
- Elaborar las políticas de gobierno de TI a aplicarse dentro de la empresa.
- Evaluar el estado de los procesos habilitadores, correspondientes a los enfoques de gobierno de TI que aplican en la empresa, su evolución y nivel de madurez.

Conclusiones:

En este Proyecto se planteó una solución integrada que brindará a la institución un valor agregado por el lado de gestión tecnológica, pues se garantiza el alineamiento estratégico y la entrega de beneficios a los stakeholders siguiendo actividades y estableciendo roles y responsabilidades de acuerdo un enfoque identificado y que se adapte a lo que la empresa pueda alcanzar en un determinado espacio de tiempo.

4.1.3. Antecedentes en el contexto local

4.1.3.1. Tema: "Auditoría Informática de los Sistemas Informáticos de la Unidad de Informática de la Escuela de Postgrado de la Universidad Nacional "Pedro Ruiz Gallo"** (Rado, 2008)

Autor: Víctor Carlos Quiñones Rado.

Año: 2008.

Institución: Universidad Nacional Pedro Ruiz Gallo.

Lugar/País: Lambayeque/Perú

Resumen:

El presente proyecto de tesis, abarca los siguientes aspectos:

- Determinar la capacidad de los Sistemas Informáticos de la Escuela de Postgrado de la Universidad Nacional Pedro Ruiz Gallo.
- Delinear los elementos de la Auditoría de los Sistemas Informáticos.
- Aplicar los lineamientos de Auditoría a los Sistemas Informáticos de la Escuela de Postgrado de la Universidad Nacional Pedro Ruiz Gallo.
- Elaborar la propuesta para el mejor uso de la capacidad instalada de los Sistemas Informáticos de la Escuela de Postgrado de la Universidad Nacional Pedro Ruiz Gallo.

Conclusiones:

En este proyecto se planteó diseñar un Gobierno de Tecnología de Información con enfoque a seguridad de información, en el cual se consideró, realizar copias de seguridad y llevar un registro de accesos diarios de usuarios. También ubicar el Servidor Dedicado en un lugar apropiado donde el acceso es restringido y alejado de personas extrañas a la Unidad. Así como realizar el manejo de fallas para prevenir, diagnosticar y reparar posibles fallas en los diferentes componentes de la red.

4.1.3.2. Tema: "Auditoría de Sistemas Informáticos" (Vera, 2006)

Autores:

- Christian Omar Lluén Lozano
- José Nelson Delgado Gonzales

Año: 2006.

Institución: Universidad Católica Santo Toribio de Mogrovejo.

Lugar/País: Chiclayo/Perú

Resumen:

El presente proyecto de tesis, abarca los siguientes aspectos:

- Verificar el estado de sus equipos de cómputo.
- Reestructurar la red existente tanto con normas de cableado estructurado como la ubicación adecuada de sus equipos.
- Brindar una mayor seguridad a la información de la empresa.
- Realizar un sistema el cual ayude al área de administración a poder tener un control de ingresos y salidas del personal que labora en la empresa.

Conclusiones:

En este proyecto se concluyó que es necesario contar con un adecuado sistema para garantizar la correcta operación de control de ingresos y salidas del personal de trabajo, a la vez reestructurando la red y verificando periódicamente el estado en que se encuentran los equipos de cómputo, así mismo con su apropiada ubicación, la cual tiene como finalidad, contar con una mayor seguridad de la información de la empresa.

4.2.- Desarrollo de la Temática

A continuación se desarrollará la temática de la investigación de Auditoría, TI y COBIT 5.

4.2.1. AUDITORÍA

El concepto de auditoría es más amplio: no sólo detecta errores, sino que es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo.

La palabra auditoría viene del latín auditorius, y de ésta proviene auditor, que tiene la virtud de oír, y el diccionario lo define como "revisor de cuentas auditor". El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de recursos alternativos de acción, se tome decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

4.2.1.1. Tareas principales de la Auditoría

Según Jiménez nos menciona las siguientes tareas principales de la Auditoría:

- Estudiar y actualizar permanentemente las áreas susceptibles de revisión.
- Apegarse a las tareas que desempeñen las normas, políticas, procedimientos y técnicas de auditoría establecidas por organismos generalmente aceptados a nivel nacional e internacional.
- Evaluación y verificación de las áreas requeridas por la alta dirección o responsables directos del negocio.
- Elaboración del informe de auditoría (debilidades y recomendaciones).
- Otras recomendadas para el desempeño eficiente de la auditoría. (Jiménez, 2013)

4.2.1.2. Formas de Auditoría:

- **Auditoría Interna:** Es aquella que se hace adentro de la empresa; sin contratar a personas de afuera. La auditoría interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados económicamente. La auditoría interna existe por expresa decisión de la empresa, o sea, que puede optar por su disolución en cualquier momento.

- **Auditoría Externa:** Como su nombre lo dice es aquella en la cual la empresa contrata a personas de afuera para que haga la auditoría en su empresa. Es realizada por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la auditoría Interna, debido al mayor distanciamiento entre auditores y auditados.

  Según el autor Rivas menciona que en una empresa, los responsables de Informática escuchan, orientan e informan sobre las posibilidades técnicas y los costos de tal sistema. Con voz, pero a menudo sin voto, el área de informática trata de satisfacer lo más adecuadamente, posible aquellas necesidades. La empresa necesita controlar su Informática y ésta; necesita que su propia gestión esté sometida a los mismos procedimientos y estándares que el resto de aquella. La conjunción de ambas necesidades cristaliza en la figura del auditor interno en informática.

  Una Empresa o Institución que posee auditoría interna puede y debe en ocasiones contratar servicios de auditoría externa. Las razones para hacerlo suelen ser:

  - Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.
  - Contrastar algún Informe interno con el que resulte del externo, en aquellos supuestos de emisión interna de graves recomendaciones que chocan con la opinión generalizada de la propia empresa.
  - Servir como mecanismo protector de posibles auditorías en informática externas decretadas por la misma empresa.

- Aunque la auditoría interna sea independiente del Departamento de

  Sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se le realicen auditorías externas como para tener una visión desde afuera de la empresa. (Chillida, 2013)

4.2.1.3. Auditoría en Informática

Se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional; por ello, nada más señalarán algunos aspectos básicos para su entendimiento.

Así, la ***auditoría en informática*** es:

- Proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.
- Un proceso formal ejecutado por especialistas del área de auditoría y de informática; se orienta a la verificación y aseguramiento para que las políticas y procedimientos en la organización se realicen de una manera oportuna y eficiente.

- Las actividades ejecutadas por profesionales del área de informática y de auditoría encaminadas a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección, etc.).Dicha evaluación deberá ser la pauta para la entrega del informe de auditoría en informática, el cual debe contener las observaciones, recomendaciones y áreas de oportunidad para el mejoramiento y optimización permanente de la tecnología de informática en el negocio.

- El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de

que los recursos de informática operen en un ambiente de seguridad y control eficientes, con la finalidad de proporcionar a la alta dirección o niveles ejecutivos la certeza de que la información que circula por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud, confiabilidad, etcétera.

- Proceso metodológico que tiene el propósito principal de evaluar los recursos (humanos, materiales, financieros, tecnológicos, etc.) relacionados con la función de informática para garantizar al negocio que dicho conjunto opere con un criterio de integración y desempeño de niveles altamente satisfactorios, para que a su vez apoyen la productividad y rentabilidad de la organización. (Simón, 2012)

4.2.1.3.1. La importancia de la Auditoría en Informática

Según el autor nos recalca que la tecnología de informática, traducida en hardware, software, sistemas de Información, investigación tecnológica, redes locales, base de datos, ingeniería de software, telecomunicaciones, servicios y organización de informática, permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

4.2.1.3.2. Los objetivos de la auditoría Informática son:

- El análisis de la eficiencia de los Sistemas Informáticos
- La verificación del cumplimiento de la Normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.

4.2.1.3.3. Sus beneficios son:

- Mejora la imagen pública.
- Confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad (reprocesos, rechazos, reclamos, entre otros).
- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible. (García, 2013)

4.2.2. TECNOLOGÍA DE LA INFORMACIÓN

Desde el surgimiento de Internet, se ha incorporado masivamente a la TI el aspecto de comunicación, con lo cual se suele hacer referencia a un tema aún más amplio, conocido como Tecnología de Información.

TI, o más conocida como IT por su significado en inglés: information technology, es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas. El término es comúnmente utilizado como sinónimo para los computadores, y las redes de computadoras, pero también abarca otras tecnologías de distribución de información, tales como la televisión y los teléfonos.

Las tecnologías de la información son una herramienta de proceso de información básica para cualquier actividad, que se derivan de los primeros ordenadores y de la informática que nacieron en el siglo pasado. Están cambiando la sociedad y prometen seguir haciéndolo hacia límites y de formas que hoy no podemos ni siquiera imaginar.

Múltiples industrias están asociadas con las tecnologías de la información, incluyendo hardware y software de computador, electrónica,

semiconductores, internet, equipos de telecomunicación, e-commerce y servicios computaciones.

Según el autor Chillida nos dice que en este mundo globalizado las Tecnologías de Información han tomado un papel muy importante, ya no existen fronteras ni distancias, la diferencia de horarios ya no es un problema, se puede decir que ya existe un clic para dar solución a cualquier situación sin importar su origen o clasificación, se pueden hacer negocios en cualquier parte del mundo, etc. Las Tecnologías de Información permiten ser cada vez más competitivos, ofrecer mejor calidad al consumidor, reducir costos, innovar con mayor rapidez y obtener resultados sorprendentes.

Si hablamos del software, los sistemas operativos, las bases de datos, los procesadores de texto, las hojas de cálculo, los lenguajes de programación, los programas de edición o los navegadores multiplican por infinitivo las posibilidades del equipamiento. Las opciones de todas esas variantes del software son muy numerosas y están a disposición de los usuarios de diferentes formas, siendo algunas de ellas gratuitas. (Chillida, 2013)

Con la popularización de los teléfonos móviles inteligentes (Smartphones) y las tabletas se ha producido una explosión de programa específicos, las aplicaciones o apps, que potencian la utilidad y la necesidad de esos dispositivos, en combinación con las prestaciones de movilidad que ofrecen las telecomunicaciones.

Uno de los aspectos de las tecnologías de la información que más importancia tiene en la actualidad es el de la seguridad, entendida en un doble sentido. Por una parte seguridad para evitar accesos indeseados a los centros de datos, versión moderna de los antiguos centros de cálculo, a los ordenadores y a los programas e información contenidos en ellos, que con la facilidad de acceso a las redes y el desarrollo de medios como Internet se han multiplicado. Por otro lado, y dada la presencia de ordenadores en todo tipo de negocios, empresas o instituciones, es necesario un tipo de seguridad que garantice la continuidad de las actividades y de los negocios. Una parte de los profesionales del sector de las tecnologías de la información centra sus

esfuerzos en todos los temas de seguridad como soporte a la gestión de las entidades y trata de reducir y eliminar los riesgos y amenazas, los ciberataques, etc.

Hay otros muchos aspectos que destacan en la evolución de las TI en la actualidad, como son la factura electrónica, que tiene como finalidad eliminar este tipo de documentos en papel y ofrecer todas las posibilidades que brinda la digitalización, y el manejo de grandes volúmenes de datos que se generan en muchos campos de actividad. Es lo que se denomina business intelligence en el entorno empresarial o de forma más general big data. La gestión y el aprovechamiento de esa información que se genera y almacena en algunos de esos campos traen consigo importantes retos para las tecnologías de la información y muchas oportunidades de desarrollo comercial y de beneficio para la sociedad.

En este repaso no se puede olvidar otro aspecto muy destacado en los últimos años y que está produciendo muchas expectativas y en muchos casos realidades. Según el autor Coltell Simón nos recalca que se trata de almacenamiento en la nube o cloud computing. Mediante una combinación de tecnologías de la información y telecomunicaciones, el almacenamiento en la nube permite que las empresas y las Administraciones Públicas puedan establecer nuevas formas de trabajar, basadas en la agilidad, la flexibilidad y la adaptación a diferentes tamaños y necesidades. En el nuevo modelo que trae consigo la nube, los servicios, los programas y las aplicaciones están disponibles allí donde los necesita el usuario, más allá de la estructura y de las infraestructuras de la empresa o institución. Las entidades contratan un servicio global y no se preocupan de cómo se materializa. Sólo saben que está disponible cuándo y dónde lo necesitan. Este tipo de servicio en la nube va muy asociado a la movilidad e implica ahorros económicos para los usuarios y vuelve a poner el énfasis en los temas de seguridad, privacidad y continuidad en la actividad o en el negocio. (Simón, 2012)

Figura Nº 3. Tecnología de la Información.

Fuente: (Chillida, 2013)

4.2.2.1. Tecnología de Información en la Empresa

El departamento o equipo que dentro de una organización ejerce las funciones de TI se encarga de estudiar, diseñar, desarrollar, implementar y administrar los sistemas de información utilizados para el manejo de datos e información de toda la organización. Estos sistemas, a su vez, comprenden aplicaciones o software, y equipos o hardware.

Llevar a cabo las tareas de la organización apoyándose en la Tecnología de información, generalmente redunda en un procesamiento más rápido y confiable de su datos. La información resultante tiene mayor movilidad y accesibilidad, y cuenta con mayor integridad, que cuando se procesa en forma manual. Igualmente, las computadoras relevan a los empleados de numerosas actividades repetitivas y aburridas, permitiéndoles aprovechar mejor su tiempo en actividades que agregan más valor.

A medida que los precios de los equipos de computación bajan, su capacidad aumenta, y se hacen más fáciles de usar, la TI se utiliza en nuevas

y variadas formas. En las empresas, sus aplicaciones son diversas. Hoy en día, la mayoría de las empresas medianas y grandes (y cada día más pequeñas y micro-empresas) utilizan la TI para gestionar casi todos los aspectos del negocio, especialmente el manejo de los registros financieros y transaccionales de las organizaciones, registros de empleados, facturación, cobranza, pagos, compras, y mucho más. (Chillida, 2013)

4.2.3. COBIT 5

4.2.3.1. Introducción

- El 9 de abril de 2012 fue publicado oficialmente por ISACA el marco de referencia COBIT 5.
- Es la evolución de la familia COBIT, aprovechando las versiones anteriores y las practicas actuales.
- Está apoyado en más de 15 años de experiencia global.
- Es resultado del trabajo de expertos de los 5 continentes y de la retroalimentación de cientos de miembros de ISACA.
- COBIT 5 Conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI).
- Cobit 5 provee la Gestión de TI para las empresas y el Gobierno de TI. COBIT es un marco de referencia para la dirección de TI, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio.
- COBIT permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. Enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de COBIT. (Chillida, 2013)

EVOLUCIÓN DE COBIT

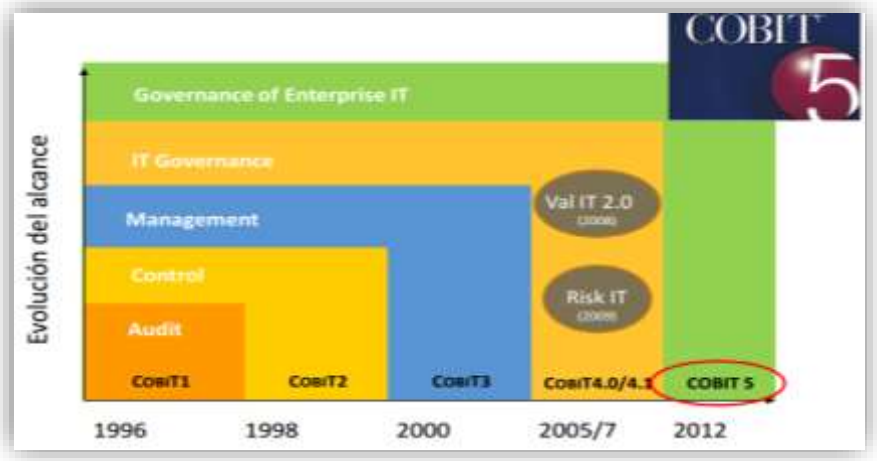


Figura Nº 4. Evolución del alcance.

Fuente: (Chillida, 2013)

4.2.3.2. ¿Qué es COBIT?

Es un conjunto de buenas prácticas para el manejo de información. Cobit consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. Se aplica a los sistemas de información de toda la empresa, incluyendo computadoras personales, mini computadoras y ambientes distribuidos.

COBIT son las siglas para definir Control Objectives for Information and related Technology (Objetivos de Control para la información y tecnología relacionada. Es un conjunto de herramientas de soporte que permite a la gerencia de las organizaciones el cerrar la brecha entre los requerimientos de control, problemas técnicos y los riesgos del negocio.

Este marco presenta actividades para el Gobierno de TI en una estructura manejable y lógica. Las buenas prácticas de COBIT reúnen el consenso de expertos, quienes ayudarán a optimizar la inversión en TI y proporcionarán un mecanismo de medición que permitirá juzgar cuando las actividades van por el camino equivocado.

4.2.3.3. ¿Para qué se utiliza?

- Para planear, implementar, controlar y evaluar el gobierno sobre TI; incorporando objetivos de control, directivas de auditoria, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.
- COBIT permite el desarrollo claro de políticas y la práctica buena para el control de TI en todas las partes de la organización.
- El modelo COBIT es constantemente actualizado; el cual permite a las empresas aumentar su valor en TI y reduce los riesgos asociados a proyectos tecnológicos.

  Gracias a que COBIT se estructura a partir de parámetros generalmente aplicables y aceptados, para mejorar las prácticas de planeación, control y seguridad de las Tecnologías de Información**.** (López, 2009)

4.2.3.4. La Misión COBIT

La misión de COBIT es el investigar, desarrollar, publicar y promover un conjunto de objetivos de control generalmente aceptados, autorizados, actualizados por ISACA para ser utilizadas en el día a día por la gerencia del negocio, los profesionales de IT y de la seguridad.

4.2.3.5. Objetivos y Beneficios

- Proveer un marco único reconocido a nivel mundial de las "mejores prácticas" de control y seguridad de TI.
- Consolidar y armonizar estándares originados en diferentes países desarrollados.
- Concientizar a la comunidad sobre importancia del control y la auditoría de TI.
- Enlaza los objetivos y estrategias de los negocios con la estructura de control de la TI, como factor crítico de éxito.

- Aplica a todo tipo de organizaciones independiente de sus plataformas de TI.
- Ratifica la importancia de la información, como uno de los recursos más valiosos de toda organización exitosa. (Ron, 2010)

4.2.3.6. Beneficios para las Organizaciones

Las organizaciones y sus ejecutivos están haciendo esfuerzos para:

- Mantener información de calidad para apoyar las decisiones del negocio.
- Generar un valor comercial de las inversiones habilitadas por la Tecnología de la Información (TI), o sea: lograr metas estratégicas y mejoras al negocio mediante el uso eficaz e innovador de la TI.
- Lograr una excelencia operativa mediante la aplicación eficiente y fiable de la tecnología.
- Mantener el riesgo relacionado con TI a niveles aceptables.
- Optimizar el costo de la tecnología y los servicios de TI.

4.2.3.7. ¿Quiénes utilizan COBIT?

- **La Gerencia:**

Para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

- **Los Usuarios Finales:**

Quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

- **Los Auditores:**

Para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

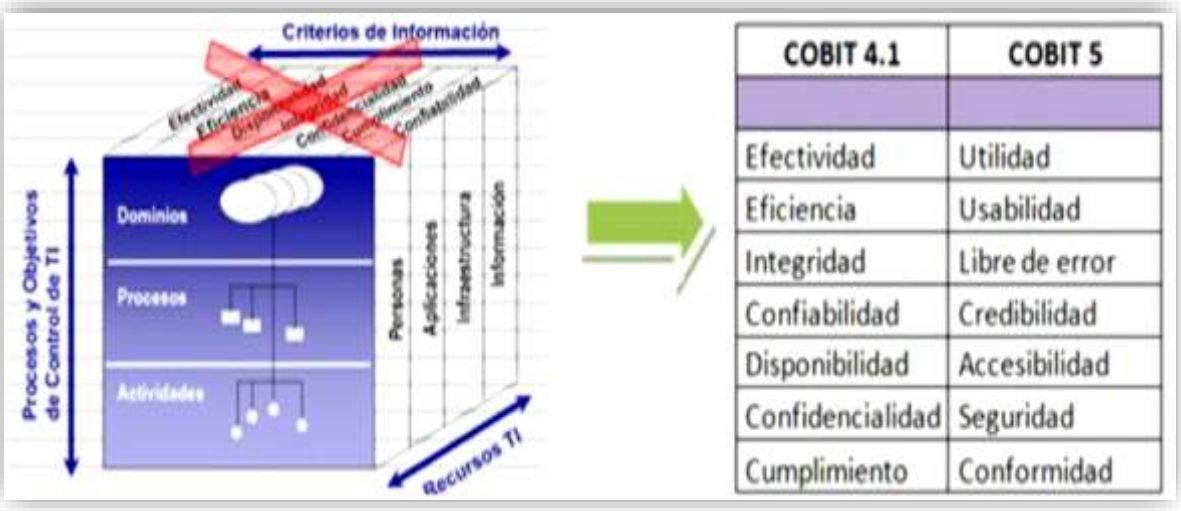
- **Los Responsables de TI:**

Para identificar los controles que requieren en sus áreas. También puede ser utilizado dentro de las empresas por el responsable de un proceso de

negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas. (ISACA, COBIT 5 - Cambios de la nueva versión, 2011).

4.2.3.8. Estructura de COBIT

Según ISACA hace una comparación con respecto a los criterios de Información entre COBIT 4.1 y COBIT 5.



COBIT 4.1	COBIT 5
Efectividad	Utilidad
Eficiencia	Usabilidad
Integridad	Libre de error
Confiabilidad	Credibilidad
Disponibilidad	Accesibilidad
Confidencialidad	Seguridad
Cumplimiento	Conformidad

Figura Nº 5. Comparación de Estructura de COBIT 4.1 y COBIT 5

Fuente: (ISACA, COBIT 5 - Cambios de la nueva versión, 2011).

✓ **Conceptos básicos de TI**

- **Dominio:** Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
- **Procesos:** Conjuntos o series de actividades unidas con delimitación o cortes de control.
- **Actividades:** Acciones requeridas para lograr un resultado medible.

Figura Nº 6. Niveles del COBIT

Fuente: (ISACA, COBIT 5 - Cambios de la nueva versión, 2011).

- ✓ **Recursos de TI**
  - Personas
  - Aplicaciones
  - Infraestructura
  - Información

- ✓ **Criterios de Información**

  Son:
  - Utilidad
  - Usabilidad
  - Libre de Error
  - Credibilidad
  - Accesibilidad
  - Seguridad
  - Conformidad

4.2.3.9. El Marco de Referencia COBIT 5

Según ISACA menciona puntos de Marco de Referencia que son los siguientes:

- COBIT 5 ayuda a las organizaciones o empresas a crear/obtener valor óptimo de la TI, para la disciplina específica de gestión de TI dentro de la organización, manteniendo un balance entre los beneficios, riesgos y recursos. COBIT 5 apoya la planeación, construcción, ejecución y monitoreo de actividades en alineamiento con la dirección establecida por gobierno, para alcanzar los objetivos estratégicos de negocio, mantener información de calidad para toma de decisiones al igual que optimización de riesgos y costos.

  Las organizaciones pueden estructurar sus procesos como mejor consideren, siempre y cuando se cubran los objetivos necesarios de gobierno y gestión. Estas organizaciones pueden cumplir sus objetivos adoptando diferentes procesos de acuerdo a su tamaño y tipo de industria, sin embargo, COBIT 5 carece de un planteamiento para la selección de procesos relevantes a implementar y fortalecer en un tipo de industria específica como es el caso de la industria editorial.

- COBIT 5 tiene un enfoque holístico para administrar y gobernar la información y tecnología relacionada en toda la empresa,
- COBIT 5 establece principios y habilitadores genéricos que son útiles para empresas de todos tamaños y giros.

Gobierno y Administración

- El Gobierno o Gobernanza se asegura de que los objetivos de la empresa son logrados, evaluando las necesidades de los interesados, condiciones y opciones; estableciendo la dirección mediante prioridades y toma de decisiones; y monitoreando el desempeño, cumplimiento y progreso respecto a los objetivos (EDM).

  La Administración planea, construye, ejecuta y monitorea (plans, builds, runs and monitors) actividades en alineamiento con la dirección establecida

por el cuerpo de gobierno para alcanzar los objetivos de la empresa (PBRM). (ISACA, COBIT 5 - Cambios de la nueva versión, 2011) y (ISACA, COBIT 5 , 2015)

4.2.3.10. Dominios y Procesos de COBIT 5

COBIT define las actividades de TI en 5 dominios que contienen 37 procesos, los cuales detallaremos a continuación:

- ✓ **Evaluar, Orientar y Supervisar (EDM)**
  - EDM01Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.
  - EDM02 Asegurar la Entrega de Beneficios
  - EDM03 Asegurar la Optimización del Riesgo
  - EDM04 Asegurar la Optimización de los Recursos
  - EDM05 Asegurar la Transparencia hacia las partes interesadas

- ✓ **Alinear, Planear y organizar (PO)**
  - APO01 Gestionar el Marco de Gestión de TI.
  - APO02 Gestionar la Estrategia.
  - APO03 Gestionar la Arquitectura Empresarial.
  - APO04 Gestionar la Innovación.
  - APO05 Gestionar el portafolio.
  - APO06 Gestionar el Presupuesto y los Costes.
  - APO07 Gestionar los Recursos Humanos.
  - APO08 Gestionar las Relaciones.
  - APO09 Gestionar los Acuerdos de Servicio.
  - APO10 Gestionar los Proveedores.
  - APO11 Gestionar la Calidad.
  - APO12 Gestionar el Riesgo.
  - APO13 Gestionar la Seguridad.

- ✓ **Construcción, Adquisición e Implementación (AI)**
  - BAI01Gestionar los Programas y Proyectos.
  - BAI02 Adquirir y mantener el software aplicativo.
  - BAI03 Gestionar la Identificación y la Construcción de Soluciones.
  - BAI04 Gestionar la Disponibilidad y la Capacidad.
  - BAI05 Gestionar la introducción de Cambios Organizativos.
  - BAI06 Gestionar los Cambios.
  - BAI07 Gestionar la Aceptación del Cambio y de la Transición.
  - BAI08 Gestionar el Conocimiento.
  - BAI09 Gestionar los Activos.
  - BAI10 Gestionar la Configuración.

- ✓ **Entregar, dar Servicios y soporte (DS)**
  - DSS01 Gestionar las Operaciones.
  - DSS02 Gestionar las Peticiones y los Incidentes del Servicio.
  - DSS03 Gestionar los Problemas.
  - DSS04 Gestionar la continuidad.
  - DSS05 Gestionar los servicios de seguridad.
  - DSS06 Gestionar los Controles de los Procesos del Negocio.

- ✓ **Supervisión, Evaluación y Verificación (ME)**
  - MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad.
  - MEA02Supervisar, Evaluar y Valorar el Sistema de Control Interno.
  - MEA03Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos. (ISACA, COBIT 5, 2013).

4.2.3.11. Comparación y elección del estándar a utilizar

COMPARACIÓN DE ESTÁNDARES COBIT, ITIL Y COSO			
	COBIT	**ITIL**	**COSO**
DESCRIPCIÓN	Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA) y el Instituto de Administración de las Tecnologías de la Información (ITGI).	Es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la Información (TI).	Se dedica a proporcionar liderazgo de pensamiento a través de la creación de marcos y orientación sobre la gestión del riesgo empresarial, el control interno y la disuasión del fraude.
VENTAJAS	-Proporciona las mejores prácticas y herramientas para monitorear y gestionar las actividades de TI. -Mejor alineación de una empresa, enfocándose en sus recursos de TI.	-La organización TI desarrolla una estructura más clara, se vuelve más eficaz, y se centra más en los objetivos de la organización.	-Permite a la dirección de la empresa poseer una visión global del riesgo y accionar los planes para su correcta gestión.
DESVENTAJAS	- Se requieren de un esfuerzo de la organización, para adoptar los estándares.	-Tiempo y esfuerzo necesario para su implementación. -Que no se dé el cambio en la cultura de las áreas involucradas. -La mejora del servicio y la reducción de costos puede no ser visible.	-No existe la seguridad total o absoluta de lograr los objetivos fijados, ya que pueden tomarse decisiones erróneas o producirse acuerdos entre varias personas que vulneren el sistema de control interno. -Todos los integrantes de la organización son responsables por el Control Interno, ya que lo llevan a cabo las personas que actúan en todos los niveles, no tratándose solamente de manuales de organización y procedimientos que indican lo que se debe hacer.

Cuadro Nº 2. Comparación de Estándares

Fuente: (COBIT 5, Elaboración Propia)

- ✓ **Elección del Estándar a utilizar**

  - Encontramos que COBIT a diferencia de ITIL, tiene mayor alcance que ITIL ya que abarca todo el espectro de actividades de IT, mientras que ITIL está centrado solo en lo que respecta a gestión del servicio.
  - COSO se enfoca estrictamente en lo que es Control Interno, a diferencia de COBIT, el cual es más propicio para el trabajo que se quiere realizar.

CAPITULO V

DESARROLLO DE LA PROPUESTA

5.1.-Plan de Auditoría para la Gestión de TI

En este punto se desarrollará la Propuesta del Plan de Auditoría, el cual se menciona a continuación:

5.1.1. Alcance de la Auditoría de la Gestión de TI

El siguiente trabajo de auditoría aplicará COBIT como metodología para la evaluación y análisis de los diferentes procesos y controles que se aplican en el área de la tecnología de la información.

A pesar de que COBIT es una herramienta que trabaja conjuntamente con los objetivos principales de la organización, la auditoría se centrara en el análisis de las tecnologías de la información, aplicada actualmente en el área del Centro de Sistemas de Información de GERESA.

Debido a que la Gerencia Regional de Salud es una organización dedicada exclusivamente a garantizar la atención de las necesidades de salud con recurso humano competente, servicios de salud organizados y articulando diversos actores estratégicos, en concordancia con las prioridades regionales. Todo esto debe contribuir al desarrollo integral y sostenido de la Región Lambayeque. Para llegar a este nivel de servicio; cada área unas en mayor proporción que otras deben asegurarse de dar lo mejor de sí, de aquí que se identifican aquellos que para mantenerse en operación constante dependen del servicio que les brinda el Centro de Sistemas de Información.

De aquí partirá el análisis donde se identificaran las debilidades existentes y sus riesgos potenciales, se expondrán una serie de conclusiones sobre los actuales procedimientos en lo que refiere a TI, el cual nos ayudará a emitir recomendaciones para el mejoramiento de gestión TI.

Objetivos de la Auditoría

- Analizar y diagnosticar la actual gestión del CSI de la GERESA.
- Plantear las mejoras para la gestión del CSI.
- Proponer nuevos procesos y actividades que ayudaran a identificar los controles que se requieren para garantizar la gestión del CSI.

5.2. Determinación de los Procesos COBIT aplicables a la auditoría en ejecución.

La determinación de los procesos COBIT involucrados dentro de la gestión de procesos TI que permitirán llevar a cabo el desarrollo de la presente auditoría, fue realizada siguiendo las recomendaciones de COBIT que fue publicado a inicios del 2013. Este documento expone los objetivos de control detallados de COBIT que tienen relación con la gestión de TI.

Del estudio de estos, se han seleccionado aquellos que tienen relación con la gestión de TI del área del CSI de acuerdo a la encuesta realizada a dicha área y en otras áreas de manera general, las cuales contribuirán a alcanzar los objetivos del negocio. A continuación se exponen los objetivos de control por dominios que han sido escogidos para la ejecución del trabajo de auditoría de la gestión de TI del área del CSI.

❖ **Dominio: Alinear, Planificar Y Organizar (APO)**

De este dominio se ha elegido el proceso Gestionar los Recursos Humanos, de los cuales aplican 4 objetivos de control y se mencionan a continuación:

APO07 Gestionar los Recursos Humanos.

- APO07.01 Mantener la dotación de personal suficiente y adecuado
- APO07.03: Mantener las habilidades y competencias del personal.
- APO07.04: Evaluar el desempeño laboral de los empleados.
- APO07.06: Gestionar el personal contratado.

❖ **Dominio: Entrega De Servicios Y Soporte (DSS)**

De este dominio se ha elegido los siguientes procesos: Gestionar las Peticiones y los Incidentes del Servicio, Gestionar los servicios de seguridad y Gestionar los Controles de los Procesos del Negocio, de los cuales aplican los objetivos de control que se detallarán más adelante.

DSS02 Gestionar las Peticiones y los Incidentes del Servicio

- DSS02.01: Definir esquemas de clasificación de incidentes y peticiones de servicio.
- DSS02.02: Registrar, clasificar y priorizar peticiones e incidentes.
- DSS02.04: Investigar, diagnosticar y localizar incidentes.

DSS05 Gestionar los servicios de seguridad

- DSS05.02: Gestionar la seguridad de la red y las conexiones.
- DSS05.03: Gestionar la seguridad de los puestos de usuario final.

DSS06 Gestionar los Controles de los Procesos del Negocio

- DSS06.01: Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos.
- DSS06.06: Asegurar los activos de información.

❖ **Dominio: Supervisar, Evaluar Y Valorar (MEA)**

De este dominio se ha elegido los siguientes procesos: Supervisar, Evaluar y Valorar Rendimiento y Conformidad y Supervisar, Evaluar y Valorar el Sistema de Control Interno, de los cuales aplican los objetivos de control que se detallarán más adelante.

MEA01. Supervisar, Evaluar y Valorar Rendimiento y Conformidad

- MEA01.01: Establecer un enfoque de la supervisión.
- MEA01.04: Analizar e informar sobre el rendimiento.
- MEA01.05: Asegurar la implantación de medidas correctivas.

MEA02. Supervisar, Evaluar y Valorar el Sistema de Control Interno

- MEA02.01: Supervisar el control interno.
- MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio.
- MEA02.03: Realizar autoevaluaciones de control.
- MEA02.06: Planificar iniciativas de aseguramiento.
- MEA02.07: Estudiar las iniciativas de aseguramiento.

❖ **Dominio: Alinear, Planificar y Organizar**

A continuación se detallará los objetivos de control del dominio Alinear, Planificar y Organizar, que se aplicarán en la auditoría de acuerdo a las actividades de cada uno de estos objetivos.

- **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.

Los objetivos de control detallados a ser considerados son:

- ***APO07.01: Mantener la dotación de personal suficiente y adecuado***

Se eligió este subproceso ya que evaluar las necesidades de personal en forma regular o en cambios importantes en la empresa, operativos o en los entornos, es indispensable para asegurar que la empresa tenga los suficientes recursos humanos para apoyar las metas y objetivos empresariales.

- ***APO07.02: Identificar personal clave de TI***

No sé eligió este subproceso porque identificar el personal clave de TI trata de reducir al mínimo la dependencia de una sola persona en la realización de una función crítica de trabajo mediante la captura de conocimiento

(documentación), el intercambio de conocimientos, la planificación de la sucesión y el respaldo (*backup*) del personal, y este no es un problema en el área del CSI ,ya que el jefe de cada sub área y sus respectivos equipos de trabajo tienen asignada una determinada labor que complementa el trabajo de sus demás compañeros.

- ***APO07.03: Mantener las habilidades y competencias del personal***

Se eligió este subproceso ya que se debe definir y gestionar las habilidades y competencias necesarias del personal en el área del CSI, además de verificar regularmente que el personal tenga las competencias necesarias para cumplir con sus funciones sobre la base de su educación, formación y/o experiencia y verificar que estas competencias se mantienen, con programas de capacitación y certificación en su caso y por supuesto también proporcionar a los empleados aprendizaje permanente y oportunidades para mantener sus conocimientos, habilidades y competencias al nivel requerido para conseguir las metas empresariales.

- ***APO07.04: Evaluar el desempeño laboral de los empleados***

Se eligió este subproceso ya que es vital que se realicen oportunamente evaluaciones de rendimiento de manera regular respecto a los objetivos individuales derivados de los objetivos de la empresa, las normas establecidas, las responsabilidades específicas del trabajo y el marco de habilidades y competencias, para poder saber si el actual desempeño del personal en sus funciones es el óptimo.

- ***APO07.05: Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio***

No se eligió este subproceso ya que comprender y realizar un seguimiento de la demanda actual y futura de recursos humanos para el negocio y TI con responsabilidades en TI corporativa e identificar las carencias y proporcionar datos de entrada a los planes de aprovisionamiento, planes de abastecimiento de procesos de contratación del negocio y de TI y procesos de contratación del negocio y de TI, si bien es importante esto, no es una actividad primordial en la

cual se tenga problemas claros y urgentes por corregir como lo es en los demás subprocesos.

- ***APO07.06: Gestionar el personal contratado***

  Se eligió este subproceso ya que se debe asegurar que los consultores y el personal contratado que apoyan a la empresa con capacidades de TI conozcan y cumplen las políticas de la organización así como los requisitos contractuales previamente acordados.

❖ **Dominio: Entrega De Servicios y Soporte**

A continuación se detallará los objetivos de control del dominio Entrega de Servicios y Soporte, que se aplicarán en la auditoría de acuerdo a las actividades de cada uno de estos objetivos

- **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.

Los objetivos de control detallados a ser considerados son:

- ***DSS02.01: Definir esquemas de clasificación de incidentes y peticiones de servicio***

  Se eligió este subproceso ya que al definir esquemas de clasificación y priorización de incidentes y peticiones de servicio y criterios para el registro de problemas, se podrá asegurar enfoques consistentes en el tratamiento, informando a los usuarios y realizando análisis de tendencias.

- ***DSS02.02: Registrar, clasificar y priorizar peticiones e incidentes***

  Se eligió este subproceso ya que no sólo se podrá identificar, registrar y clasificar peticiones de servicio e incidentes, sino también asignar una prioridad según la criticidad del negocio y los acuerdos de servicio.

- ***DSS02.03: Verificar, aprobar y resolver peticiones de servicio***

No se eligió este subproceso ya que si bien se debe seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos, se tendrá también que obtener aprobación financiera y funcional o firmada, si se requiere, o aprobaciones predefinidas para cambios estándar acordados y en este proyecto se requiere plantear alternativas de solución ya que la implementación de estas se llevarán a cabo, siempre y cuando la empresa así lo desee hacer más adelante.

- ***DSS02.04: Investigar, diagnosticar y localizar incidentes***

Se eligió este subproceso ya que el identificar y registrar síntomas de incidentes, determinará las posibles causas y asignar recursos a su resolución.

- ***DSS02.05: Resolver y recuperarse ante incidentes***

No se eligió este subproceso ya que aquí se requiere documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI relacionado, y en este proyecto se requiere plantear alternativas de solución ya que la implementación de estas se llevarán a cabo, siempre y cuando la empresa así lo desee hacer más adelante.

- ***DSS02.06: Cerrar peticiones de servicio e incidentes***

No se eligió este subproceso ya que aquí se requiere verificar la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre, pero esto se da cuando ya se resolvieron las peticiones o incidentes, y en este proyecto la resolución de estas se llevarán a cabo, siempre y cuando la empresa así lo desee hacer más adelante.

- ***DSS02.07: Seguir el estado y emitir de informes***

No se eligió este subproceso ya que aquí se hará un seguimiento, y un análisis e informes de incidentes y tendencias de cumplimiento de peticiones, regularmente, para proporcionar información para la mejora continua, pero esto se da cuando ya se resolvieron dichas peticiones o incidentes, y en este

proyecto la resolución de estas se llevarán a cabo, siempre y cuando la empresa así lo desee hacer más adelante.

- **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.

Los objetivos de control detallados a ser considerados son:

- ***DSS05.01: Proteger contra software malicioso (Malware)***

No se eligió este subproceso ya que no vamos a Implementar y ni mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) a lo largo de la empresa para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware). Pero lo que si se podría realizar es revisar y evaluar regularmente la información sobre nuevas posibles amenazas (por ejemplo, revisando productos de vendedores y servicios de alertas de seguridad).

- ***DSS05.02: Gestionar la seguridad de la red y las conexiones***

Se eligió este subproceso ya que se recomendable utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión de la GERESA.

- ***DSS05.03: Gestionar la seguridad de los puestos de usuario final***

Se eligió este subproceso ya que se recomienda asegurar que los puestos de usuario se eligió a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida. Así mismo gestionar la configuración de la red de forma segura ya que esto permitirá asegurar el correcto funcionamiento de los procesos que existen.

- ***DSS05.04: Gestionar la identidad del usuario y el acceso lógico***

  No se eligió este subproceso ya que se recomienda asegurar que todos los usuarios tengan derechos de acceso a la información de acuerdo con los requerimientos de negocio y coordinar con las unidades de negocio que gestionan sus propios derechos de acceso con los procesos de negocio, ya que no es correcto que el personal no autorizado tengan acceso a toda la información del CSI.

- ***DSS05.05: Gestionar el acceso físico a los activos de TI***

  No se eligió este subproceso ya que define e implementar procedimientos para conceder, limitar y revocar acceso a locales, edificios y áreas de acuerdo con las necesidades de la empresa, incluyendo emergencias. El acceso a locales, edificios y áreas debe estar justificado, autorizado, registrado y supervisado. Ya que esto aplicará a todas las personas que entren en el área del CSI, incluyendo empleados, empleados temporales, clientes, vendedores, visitantes o cualquier otra tercera parte.

- ***DSS05.06: Gestionar documentos sensibles y dispositivos de salida***

  No se eligió este subproceso ya que establece salvaguardas físicas apropiadas, prácticas de contabilidad para activos de TI sensibles, tales como formularios especiales, títulos negociables, impresoras de propósito especial o credenciales (token) de seguridad, ya que no se establecerá procedimientos para la recepción, uso, eliminación de formularios especiales y dispositivos de salida, dentro y fuera de la empresa.

- ***DSS05.07: Monitorear la infraestructura para detectar eventos relacionados con la seguridad***

  No se eligió este subproceso ya que utilizará herramientas de detección de intrusiones, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes, ya que no utilizaremos herramientas de detección sino supervisar la infraestructura de TI del CSI.

- **DSS06 -Gestionar controles de procesos 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.

Los objetivos de control detallados a ser considerados son:

- ***DSS06.01: Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos***

  Se eligió este subproceso ya que se evaluará y supervisará continuamente la ejecución de las actividades de los procesos de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de controles está alineado con las necesidades del negocio y mejore los procesos del CSI.

- ***DSS06.02: Controlar el procesamiento de la información***

  No se eligió este subproceso ya que va a operar, implementar la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado), ya que no vamos implementar actividades del proceso de negocio ahora si la empresa lo desea lo llevara a cabo más adelante.

- ***DSS06.03: Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización***

  No se eligió este subproceso ya que va a gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio.

  Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio,

de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quien los está manejando en su nombre, ya que para asignar roles se tiene que aprobar y esto se dará durante la implementación; se realizará si la empresa lo requiere más adelante.

- ***DSS06.04: Gestionar errores y excepciones***

No se eligió escogimos este subproceso ya que esto se trata de gestionar las excepciones y errores de los procesos de negocio y facilitar su corrección. Incluir escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas definidas. Esto proporciona garantía de precisión e integridad del proceso de información del negocio, ya que para asignar errores y excepciones se tiene que aprobar y esto se dará durante la implementación; se realizará si la empresa lo requiere más adelante.

- ***DSS06.05: Asegurar la trazabilidad de los eventos y responsabilidades y de información***

No se eligió este subproceso ya que si bien asegura que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan, aquí solo se plantearan alternativas de solución la implementación de esta, se realizará si la empresa lo requiere más adelante.

- ***DSS06.06: Asegurar los activos de información***

Se eligió este subproceso ya que asegurará los activos de información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento), información en formato físico (tales como documentos fuente o informes de salida. Ya que permitirá asegurar los activos de información así mismo beneficiará al negocio proporcionando una salvaguarda de la información de comienzo a fin.

❖ **Dominio: Supervisar, Evaluar y Valorar**

A continuación se detallará los objetivos de control del dominio Supervisar, Evaluar y Valorar, que se aplicarán en la auditoría de acuerdo a las actividades de cada uno de estos objetivos

- **MEA01. Supervisar, evaluar y valorar el rendimiento y la conformidad**

Recolectar, validar y evaluar métricas y objetivos de negocio, de las TI y de procesos. Supervisar que los procesos se están realizando según el rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

Los objetivos de control detallados a ser considerados son:

- ***MEA01.01: Establecer un enfoque de la supervisión***

  Se eligió este subproceso ya que si bien involucrará a las partes interesadas (dirección, propietarios de procesos o usuarios) en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía. Ya que esto permitirá involucrar a las partes interesadas y comunicar los objetivos para la supervisión, consolidación e información del área del CSI.

- ***MEA01.02: Establecer los objetivos de cumplimiento y rendimiento***

  No se eligió este subproceso ya que si bien colaborará con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento, ya que se tiene que aprobar objetivos de rendimiento y cumplimiento y esto se dará durante la implementación; se realizará si la empresa lo requiere más adelante.

- ***MEA01.03: Recopilar y procesar los datos de cumplimiento y rendimiento***

  No se eligió este subproceso ya que si bien recopila y procesa datos oportunos y precisos de acuerdo con los enfoques del negocio, ya que para recopilar y procesar datos se tiene que aprobar y esto se dará durante la implementación; se realizará si la empresa lo requiere más adelante.

- ***MEA01.04: Analizar e informar sobre el rendimiento***

  Se eligió este subproceso ya que si bien revisará e informará de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y sucinta del rendimiento de las TI y encaje con el sistema corporativo de supervisión, ya que esto permitirá al personal del CSI documentar las incidencias para contar con guía adicional si el problema vuelve a aparecer y documentar los resultados.

- ***MEA01.05: Asegurar la implantación de medidas correctivas.***

  Se eligió este subproceso ya que si bien apoyará a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías, ya que esto permitirá al personal del CSI informar de los resultados a la Gerencia de la empresa.

- **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.

Los objetivos de control detallados a ser considerados son:

- ***MEA02.01: Supervisar el control interno***

  Se eligió este subproceso ya que se realizará, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de TI y el marco de control para alcanzar los objetivos organizativos, ya que esto

permitirá al personal del CSI identificar los límites del sistema de control interno de TI.

- ***MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio***

  Se eligió este subproceso ya que se revisará la operación de controles, incluyendo la revisión de las evidencias de supervisión y pruebas, para asegurar que los controles incorporados en los procesos de negocio operan de manera efectiva. Ya que se debe incluir actividades de mantenimiento de evidencias de la operación efectiva de controles a través de mecanismos como la comprobación periódica de controles, supervisión continua de controles, evaluaciones independientes, centros de mando y control y centros de operación de red.

- ***MEA02.03: Realizar autoevaluaciones de control***

  Se eligió este subproceso ya que se estimulará a la Gerencia de la empresa y a los propietarios de los procesos a tomar posesión de manera firme del procedimiento de mejora del control, a través de programas continuos de autoevaluación que valoren la completitud y efectividad del control de la Gerencia de la empresa sobre los procesos, políticas y contratos, ya que permitirá en el área del CSI determinar la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua.

- ***MEA02.04: Identificar y comunicar las deficiencias de control***

  No Se eligió este subproceso ya que se identificará deficiencias de control y analizar e identificar las causas raíz subyacente. Escalar las deficiencias de control y comunicarlas a las partes interesadas, ya que para identificar y comunicar datos se tiene que aprobar y esto se dará durante la implementación; se realizará si la empresa lo requiere más adelante.

- ***MEA02.05: Garantizar que los proveedores de aseguramiento son independientes y están cualificados***

  No se eligió este subproceso ya que asegurará que las entidades que realizan el aseguramiento son independientes de la función, grupo u organización en el alcance, ya que la información de proveedores no se da a ninguna persona externa de acuerdo a las políticas de la empresa.

- ***MEA02.06: Planificar iniciativas de aseguramiento***

Se eligió este subproceso ya que planificará las iniciativas de aseguramiento basándose en los objetivos empresariales y las prioridades estratégicas, riesgo inherente, restricciones de recursos y suficiente conocimiento de la compañía, ya que permitirá realizar una evaluación del riesgo a alto nivel y/o evaluar la capacidad del proceso para diagnosticar el riesgo e identificar los procesos críticos de TI.

- ***MEA02.07: Estudiar las iniciativas de aseguramiento***

Se eligió este subproceso ya que se definirá y acordará con la dirección, el ámbito de la iniciativa de aseguramiento, basándose en los objetivos de aseguramiento, ya que permitirá definir el alcance actual mediante la identificación de los objetivos del área CSI.

- ***MEA02.08: Ejecutar las iniciativas de aseguramiento***

No se eligió este subproceso, ya que este se debe ejecutar durante la implementación de las iniciativas de aseguramiento y para ello primero se deben aprobar dichas iniciativas y si la empresa lo requiere lo realizará más adelante.

- **MEA03. Supervisar, evaluar y valorar la conformidad con los requerimientos externos**

Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de las 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 las TI en el cumplimiento de la empresa general.

Los objetivos de control detallados a ser considerados son:

- ***MEA03.01: Identificar requisitos externos de cumplimiento***

  No se eligió este subproceso ya que identificará y supervisará, de manera continuada, cambios en las legislaciones y regulaciones tanto locales como internacionales, así como otros requisitos externos de obligado cumplimiento en el área de TI, ya que para los cambios legislaciones y regulaciones se tiene que aprobar y esto se dará durante la implementación; se realizará si la empresa lo requiere más adelante.

- ***MEA03.02: Optimizar la respuesta a requisitos externos.***

  No se eligió este subproceso ya que revisará y ajustará políticas, principios, estándares, procedimientos y metodologías para asegurar la adecuada gestión y comunicación de los requisitos legales, regulatorios y contractuales. Considerar qué estándares sectoriales, códigos de buenas prácticas y guías de mejores prácticas pueden adoptarse y adaptarse, ya que para optimizar la respuesta a requisitos externos se tiene que aprobar y esto se dará durante la implementación; se realizará si la empresa lo requiere más adelante.

- ***MEA03.03: Confirmar el cumplimiento de requisitos externos.***

  No se eligió este subproceso ya que confirmará el cumplimiento de las políticas, los principios, los estándares, los procedimientos y las metodologías con los requisitos legales, regulatorios y contractuales, ya que para confirmar el cumplimiento a requisitos externos se tiene que aprobar y esto se dará durante la implementación; se realizará si la empresa lo requiere más adelante.

- ***MEA03.04: Obtener garantía del cumplimiento de requisitos externos***.

No se eligió este subproceso ya que se obtendrá y notificará garantías de cumplimiento y adherencia a políticas, principios, estándares procedimientos y metodologías, ya que para obtener garantía del cumplimiento de requisitos externos se tiene que aprobar y esto se dará durante la implementación; se realizará si la empresa lo requiere más adelante.

5.3.-Programa de Auditoría y Matriz de Prueba de los Procesos y Objetivos de Control

En este punto se detallará los procesos y objetivos de control que aplican a la auditoría, mediante:

- **Programa de Auditoría**

En este cuadro podremos observar las actividades de cada *objetivo de control detallado*, pertenecientes a cada dominio. En el cual también se detallan los *factores de riesgo* que implicaría el no cumplirse dichas actividades.

- **Matriz de Prueba**

En este cuadro podremos observar que se mantiene cada *objetivo de control detallado* del Programa de Auditoría, pertenecientes a cada dominio, así mismo se realiza la *revisión* de estos *a través de Evaluaciones de Controles* para probar que se cumplan con dichos objetivos y mediante la *Descripción de la Prueba*, se tomaran como tales: los documentos, entrevistas y checklist que se aplicarán en la Auditoría.

A continuación se muestran los cuadros de: Programas de Auditoría y Matriz de Pruebas, agrupados de acuerdo a los dominios de COBIT versión 5.

PROCESOS DEL DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)	
APO07. Gestionar los Recursos Humanos	
Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
APO07.01 Mantener la dotación de personal suficiente y adecuado • Evaluar las necesidades de personal de forma regular o ante cambios importantes. • Mantener los procesos de contratación y de retención del personal TI y del negocio en línea con las políticas y procedimientos de personal globales de la empresa. • Incluir controles de antecedentes en el proceso de contratación de TI para empleados. • Establecer mecanismos flexibles de dotación de recursos para apoyar a las necesidades cambiantes del negocio, tales como el uso de transferencias y acuerdos de servicio con terceras partes.	• Riesgo de no poder corregir algún incidente ocurrido en una de las áreas por falta de personal TI. • No contar con el personal capacitado para las actividades que se requieren.

Cuadro Nº 3. Programa de Auditoría APO07.01
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR		
APO07. Gestionar los Recursos Humanos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
APO07.01 Mantener la dotación de personal suficiente y adecuado • Evaluar las necesidades de personal de forma regular o ante cambios importantes. • Mantener los procesos de contratación y de retención del personal de TI y del negocio en línea con las políticas y procedimientos de personal globales de la empresa. • Incluir controles de antecedentes en el proceso de contratación de TI para empleados. • Establecer mecanismos flexibles de dotación de recursos para apoyar a las necesidades cambiantes del negocio, tales como el uso de transferencias y acuerdos de servicio con terceras partes.	***Evaluación de Controles:*** Cumplimiento de política de contrataciones de personal, mediante los procedimientos de contratación y capacitación del personal TI, política y manual de funciones de la GERESA. ***Probando que:*** El personal TI es suficiente, adecuado y sobre todo, si está suficientemente capacitado para desempeñar las funciones que tienen asignadas.	• Revisión del Plan Anual de Capacitación del personal TI. • Check List. • Entrevista al Coordinador del CSI. • Entrevista al Jefe de Gestión y Desarrollo de Potencial Humano.

Cuadro Nº 4. Matriz de Pruebas APO07.01
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR	
APO07. Gestionar los Recursos Humanos	
Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
APO07.03 Mantener las habilidades y competencias de Personal. • Definir las habilidades y competencias necesarias y disponibles actualmente tanto de recursos internos como externos para lograr los objetivos de empresa, de TI y de procesos. • Identificar las diferencias entre las habilidades necesarias y disponibles y desarrollar planes de acción para hacerles frente de manera individual y colectiva. • Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos.	• Riesgo de no saber cuáles son las habilidades necesarias y disponibles que debe tener el personal TI. • Falta de productividad del personal.

Cuadro Nº 5. Programa de Auditoría APO07.03
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR		
APO07. Gestionar los Recursos Humanos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
APO07. 03 Mantener las habilidades y competencias de Personal. • Definir las habilidades y competencias necesarias y disponibles actualmente tanto de recursos internos como externos para lograr los objetivos de empresa, de TI y de procesos. • Identificar las diferencias entre las habilidades necesarias y disponibles y desarrollar planes de acción para hacerles frente de manera individual y colectiva. • Llevar a cabo revisiones periódicas para evaluar la evolución de las habilidades y competencias de los recursos internos y externos.	***Evaluación de Controles:*** Verificar procedimientos de evaluaciones periódicas para identificar si las habilidades y competencias del personal TI son óptimas para lograr los objetivos de empresa. ***Probando que:*** El personal TI, mantiene y está en constante mejora de sus competencias y habilidades para desarrollar eficientemente sus labores.	• Revisión del Plan Anual de Capacitación del personal TI. • Checklist. Entrevista al Jefe de Gestión y Desarrollo de Potencial Humano.

Cuadro Nº 6. Matriz De Pruebas APO07.03
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)	
APO07. Gestionar los Recursos Humanos	
Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
APO07.04 Evaluar el desempeño laboral de los empleados. • Considerar los objetivos funcionales de empresa como el contexto para establecer las metas individuales. • Establecer los objetivos individuales alineados con los objetivos de los procesos relevantes, de modo que exista una clara contribución a los objetivos de TI y empresariales. • Recopilar los resultados de la evaluación de desempeño de 360 grados. • Implementar y comunicar un proceso disciplinario. • Proporcionar instrucciones específicas para el uso y almacenamiento de información personal en el proceso de evaluación.	• El riesgo de que los empleados no realicen un correcto desempeño en sus funciones. • El riesgo de que los empleados no cumplan con los objetivos de la empresa. • El riesgo de que no haya un orden dentro de las diferentes áreas por falta de un proceso disciplinario.

Cuadro Nº 7. Programa de Auditoría APO07.04
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)		
APO07. Gestionar los Recursos Humanos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
APO07. 04 Evaluar el desempeño laboral de los empleados. • Considerar los objetivos funcionales de empresa como el contexto para establecer las metas individuales. • Establecer los objetivos individuales alineados con los objetivos de los procesos relevantes, de modo que exista una clara contribución a los objetivos de TI y empresariales. • Recopilar los resultados de la evaluación de desempeño de 360 grados. • Implementar y comunicar un proceso disciplinario. • Proporcionar instrucciones específicas para el uso y almacenamiento de información personal en el proceso de evaluación.	***Evaluación de Controles:*** Verificar un proceso de evaluación para determinar el desempeño de las labores del personal TI que permitan cumplir con los objetivos funcionales de la empresa. ***Probando que:*** Los empleados desempeñan una correcta labor en sus funciones diarias.	• Checklist. • Entrevista al Jefe de Gestión y Desarrollo de Potencial Humano.

Cuadro Nº 8. Matriz de Pruebas APO07.04
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)	
APO07. Gestionar los Recursos Humanos	
Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
APO07.06 Gestionar el personal contratado. • Implementar políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por consultores y/o contratistas, de acuerdo con la política de contratación de TI de la organización. • Proporcionar a los contratistas una definición clara de sus funciones y responsabilidades como parte de sus contratos. • Llevar a cabo revisiones periódicas para asegurarse de que el personal contratado ha firmado y aceptado todos los acuerdos necesarios.	• Riesgo de contratar personal que no cumpla con los requerimientos que necesita la empresa. • Riesgo de contratar personal no apto para las funciones requeridas en la empresa. • Riesgo de que el personal contratado tenga discrepancias con algún punto específico acerca de su contrato.

Cuadro Nº 9. Programa de Auditoría APO07.06
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)		
APO07. Gestionar los Recursos Humanos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
APO07. 06 Gestionar el personal contratado. • Implementar políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por consultores y/o contratistas, de acuerdo con la política de contratación de TI de la organización. • Proporcionar a los contratistas una definición clara de sus funciones y responsabilidades como parte de sus contratos. • Llevar a cabo revisiones periódicas para asegurarse de que el personal contratado ha firmado y aceptado todos los acuerdos necesarios.	***Evaluación de Controles:*** Verificar que existan políticas y procedimientos para gestionar el personal TI contratado en el área del CSI. ***Probando que:*** Se está gestionando de manera apropiada el personal contratado, de acuerdo a las políticas y procedimientos de la empresa.	• Revisiones de la Ley de Contrataciones del Estado. • Checklist. • Entrevista al Jefe de Gestión y Desarrollo de Potencial Humano.

Cuadro Nº 10. Matriz de Pruebas APO07.06
Fuente: Elaboración Propia

PROCESOS DEL DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)	
DSS02. Gestionar Peticiones e Incidentes de Servicio	
Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio. • Definir esquemas de clasificación y priorización de incidentes y peticiones de servicio y criterios para el registro de problemas • Definir modelos de incidentes para errores conocidos con el fin de facilitar su resolución eficiente y efectiva. • Definir modelos de peticiones de servicio según el tipo de petición de servicio correspondiente para facilitar la auto-ayuda y el servicio eficiente para las peticiones estándar. • Definir fuentes de conocimiento de incidentes y peticiones y su uso.	• Riesgo de no poder corregir eficiente y efectivamente errores frecuentes. • Riesgo de no tener definido un modelo de incidentes para poder corregir errores ya conocidos.

Cuadro Nº 11. Programa de Auditoría DSS02.01
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS02. Gestionar Peticiones e Incidentes de Servicio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio. • Definir esquemas de clasificación y priorización de incidentes y peticiones de servicio y criterios para el registro de problemas • Definir modelos de incidentes para errores conocidos con el fin de facilitar su resolución eficiente y efectiva. • Definir modelos de peticiones de servicio según el tipo de petición de servicio correspondiente para facilitar la auto-ayuda y el servicio eficiente para las peticiones estándar. • Definir fuentes de conocimiento de incidentes y peticiones y su uso.	***Evaluación de Controles:*** Verificar que cuente con un esquema de clasificación para priorizar peticiones de servicio e incidentes que se presentan diariamente. ***Probando que:*** La definición de modelos de incidentes para errores ya conocidos, nos facilitará su resolución de manera eficiente y eficaz.	• Checklist. • Entrevista al Responsable de Soporte Técnico – CSI.

Cuadro Nº 12. Matriz de Pruebas DSS02.01
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)	
DSS02. Gestionar Peticiones e Incidentes de Servicio	
Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes. • Registrar todos los incidentes y peticiones de servicio, registrando toda la información relevante de forma que pueda ser manejada de manera efectiva y se mantenga un registro histórico completo. • Para posibilitar análisis de tendencias, clasificar incidentes y peticiones de servicio identificando tipo y categoría. • Priorizar peticiones de servicio e incidentes.	• Riesgo de no registrar información relevante de todas las peticiones e incidentes. • No poder resolver de manera correcta los incidentes y peticiones que se den, debido a la falta de orden y adecuada clasificación estos. • Riesgo de no priorizar las peticiones e incidentes de servicio, según el impacto que pueda tener en la empresa.

Cuadro Nº 13. Programa de Auditoría DSS02.02
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS02. Gestionar Peticiones e Incidentes de Servicio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes. • Registrar todos los incidentes y peticiones de servicio, registrando toda la información relevante de forma que pueda ser manejada de manera efectiva y se mantenga un registro histórico completo. • Para posibilitar análisis de tendencias, clasificar incidentes y peticiones de servicio identificando tipo y categoría. • Priorizar peticiones de servicio e incidentes.	***Evaluación de Controles:*** Verificar que se cuente con un registro de clasificación y priorización de peticiones de servicios e incidentes. ***Probando que:*** El priorizar las peticiones e incidentes, ayudará a solucionarlos de una mejor manera, ya que se resolverá de acuerdo al tipo y categoría que tengan.	• Checklist. • Entrevista al Responsable de Soporte Técnico – CSI. • Revisión de Registro de incidentes y servicios solucionados.

Cuadro Nº 14. Matriz de Pruebas DSS02.02
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)	
DSS02. Gestionar Peticiones e Incidentes de Servicio	
Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DSS02.04 Investigar, diagnosticar y localizar incidentes. • Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes • Registrar un nuevo problema si un problema relacionado o error conocido no existe aún y si el incidente satisface los criterios acordados para registro de problemas. • Asignar incidentes a funciones especialistas si se necesita de un conocimiento más profundo, e implicar al nivel de gestión apropiado, cuando sea necesario.	• No identificar los síntomas relevantes para establecer las causas de los incidentes ocurridos. • Riesgo que no se realice un profundo análisis de los incidentes para su correcta resolución.

Cuadro Nº 15. Programa de Auditoría DSS02.04
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS02. Gestionar Peticiones e Incidentes de Servicio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DSS02.04 Investigar, diagnosticar y localizar incidentes. • Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes • Registrar un nuevo problema si un problema relacionado o error conocido no existe aún y si el incidente satisface los criterios acordados para registro de problemas. • Asignar incidentes a funciones especialistas si se necesita de un conocimiento más profundo, e implicar al nivel de gestión apropiado, cuando sea necesario.	***Evaluación de Controles:*** Verificar que cuente con síntomas relevantes que permiten diagnosticar y localizar incidentes de manera que se asignen especialistas con un nivel de gestión apropiado cuando se es necesario. ***Probando que:*** Al registrar nuevos problemas se definen fuentes de conocimientos de incidentes y peticiones para lograr resolverlos de manera idónea.	• Checklist. • Entrevista al Responsable de Soporte Técnico – CSI.

Cuadro Nº 16. Matriz de Pruebas DSS02.04
Fuente: Elaboración Propia

PROCESOS DEL DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)

DOMINIO: ENTREGA, SERVICIO Y SOPORTE (DSS)	
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.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DSS05.02: Gestionar la seguridad de la red y las conexiones. • Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. • Aplicar los protocolos de seguridad aprobados a las conexiones de red. • Configurar los equipamientos de red de forma segura. • Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información. • Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red. • Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	• Pérdida y/o daño de equipos. • Pérdida de tiempo en la labor de los trabajadores, debido a la falta de una correcta transmisión y recepción de información. • Conflicto de duplicidad en la red debido a la incorrecta configuración de los equipos de red.

Cuadro Nº 17. Programa de Auditoría DSS05.02
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS05. Gestionar servicios de seguridad		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DSS05.02: Gestionar la seguridad de la red y las conexiones. • Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. • Aplicar los protocolos de seguridad aprobados a las conexiones de red • Configurar los equipamientos de red de forma segura. • Establecer mecanismos de confianza para dar soporte a la transmisión y recepción segura de información. • Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red. • Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema.	***Evaluación de Controles:*** Verificar que cuente con protocolos de seguridad aprobados para brindar soporte a la trasmisión y recepción segura de información mediante las conexiones de red. ***Probando que:*** La seguridad ofrecida por los protocoles aprobados establecerá mecanismos de confianza para dar soporte a las conexiones de red y una adecuada protección al sistema.	• Checklist. • Entrevista al Responsable de Soporte Técnico – CSI. • Revisión de la Configuración de los equipos. .

Cuadro Nº 18. Matriz De Pruebas DSS05.02
Fuente: Elaboración Propia

DOMINIO: ENTREGA, SERVICIO Y SOPORTE (DSS)	
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.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DSS05.03: Gestionar la seguridad de los puestos de usuario final. • Configurar los sistemas operativos de forma segura. • Gestionar la configuración de la red de forma segura. • Realizar mecanismos de bloqueo de los dispositivos. • Proteger la integridad del sistema. • Proveer de protección física a los dispositivos de usuario final.	• Retraso en las funciones de los trabajadores debido a una mala configuración de los sistemas operativos. • Perdida de información debido a fallas en la configuración de la red. • Daños en los equipos y/o dispositivos debido a la falta de protección física de los mismos.

Cuadro Nº 18. Programa de Auditoría DSS05.03
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS05. Gestionar servicios de seguridad		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DSS05.03: Gestionar la seguridad de los puestos de usuario final. • Configurar los sistemas operativos de forma segura. • Gestionar la configuración de la red de forma segura. • Realizar mecanismos de bloqueo de los dispositivos. • Proteger la integridad del sistema. • Proveer de protección física a los dispositivos de usuario final.	***Evaluación de Controles:*** Verificar que exista protección física y mecanismos de bloqueo a los dispositivos de los usuarios finales ***Probando que:*** Mediante la protección física de los dispositivos se logrará proteger la integridad del sistema y de la red.	• Checklist. • Entrevista al Responsable de Soporte Técnico – CSI. • Revisión del Plan de Contingencia.

Cuadro Nº 20. Matriz de Pruebas DSS05.03
Fuente: Elaboración Propia

DOMINIO: ENTREGA, SERVICIO Y SOPORTE (DSS)	
DSS06. Gestionar Controles de Proceso de Negocio	
Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o externalizados.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos. • Identificar y documentar las actividades de control de los procesos de negocio claves para satisfacer los requerimientos de control para los objetivos estratégicos, operacionales, de informes y cumplimiento. • Supervisar las actividades de control de extremo a extremo para identificar oportunidades de mejora. • Mejorar el control de los procesos de negocio.	• Riesgo de estancarse en las mismas actividades de control y no detectar ni plantear oportunidades de mejora. • Lentitud en los procesos de negocio.

Cuadro Nº 21. Programa de Auditoría DSS06.01
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS06. Gestionar Controles de Proceso de Negocio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos. • Identificar y documentar las actividades de control de los procesos de negocio claves para satisfacer los requerimientos de control para los objetivos estratégicos, operacionales, de informes y cumplimiento. • Supervisar las actividades de control de extremo a extremo para identificar oportunidades de mejora. • Mejorar el control de los procesos de negocio.	***Evaluación de Controles:*** Verificar que exista documentación y supervisión de actividades de control de los procesos de negocio, el cual satisface los requerimientos de control para los objetivos estratégicos y corporativos de la GERESA. ***Probando que:*** Con la supervisión de las actividades de extremo a extremo, se identificará oportunidades de mejora para el negocio.	• Checklist. • Entrevista al Coordinador del CSI.

Cuadro Nº 22. Matriz de Pruebas DSS06.01
Fuente: Elaboración Propia

DOMINIO: ENTREGA, SERVICIO Y SOPORTE (DSS)	
DSS06. Gestionar Controles de Proceso de Negocio	
Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o externalizados.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DSS06.06: Asegurar los activos de información. • Aplicar las políticas de clasificación de datos y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio. • Restringir el uso, la distribución y el acceso físico a la información acorde a su clasificación. • Identificar procesos, herramientas y técnicas para verificar razonablemente el cumplimiento. • Informar al negocio y otros grupos de interés acerca de violaciones y desviaciones.	• Daño de los activos de información de la empresa debido al no aseguramiento de los mismos • Pérdida de información. • Uso indebido de los activos de información por parte de personas no autorizadas.

Cuadro Nº 23. Programa de Auditoría DSS06.06
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS06. Gestionar Controles de Proceso de Negocio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DSS06.06: Asegurar los activos de información. • Aplicar las políticas de clasificación de información y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio. • Restringir el uso, la distribución y el acceso físico a la información acorde a su clasificación. • Identificar procesos, herramientas y técnicas para verificar razonablemente el cumplimiento. • Informar al negocio y otros grupos de interés acerca de violaciones y desviaciones.	***Evaluación de Controles:*** Verificar que existan políticas de clasificación de datos y procedimientos para proteger los activos de información, bajo el control de negocio así mismo restringiendo el uso, distribución y el acceso físico a la información. ***Probando que:*** Al asegurar los activos de información no solo se podrá restringir el acceso físico a la información, sino que además logrará informar a la Gerencia, acerca de violaciones y desviaciones.	• Checklist. • Entrevista al Coordinador del CSI.

Cuadro Nº 24. Matriz de Pruebas DSS06.06
Fuente: Elaboración Propia

PROCESOS DE DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)	
MEA01 -Supervisar, evaluar y valorar el rendimiento y la conformidad.	
Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
MEA01.01: Establecer un enfoque de la supervisión. • Involucrar a las partes interesadas y comunicar los objetivos y requisitos empresariales para la supervisión, consolidación e información, utilizando definiciones comunes. • Acordar un proceso de control de cambios y de gestión del ciclo de vida de la supervisión y la presentación de informes. • Solicitar, priorizar y reservar recursos para la supervisión (considerando oportunidad, eficiencia, efectividad y confidencialidad).	• Conflicto con los objetivos y requisitos empresariales de la empresa ante una supervisión que se realice al área del CSI • La falta de eficiencia, efectividad y confidencialidad en los procesos realizados dentro de la empresa debido a la no priorización y reserva de recursos.

Cuadro Nº 25. Programa de Auditoría MEA01.01
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)		
MEA01 -Supervisar, evaluar y valorar el rendimiento y la conformidad.		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
MEA01.01: Establecer un enfoque de la supervisión. • Involucrar a las partes interesadas y comunicar los objetivos y requisitos empresariales para la supervisión, consolidación e información, utilizando definiciones comunes. • Acordar un proceso de control de cambios y de gestión del ciclo de vida de la supervisión y la presentación de informes. • Solicitar, priorizar y reservar recursos para la supervisión (considerando oportunidad, eficiencia, efectividad y confidencialidad).	***Evaluación de Controles:*** Verificar que exista un proceso de control de cambios, así mismo se comunica los objetivos y requisitos empresariales para lograr eficiencia, efectividad y confidencialidad en la supervisión. ***Probando que:*** Al establecer una supervisión eficiente y efectiva se logrará involucrar a las partes interesadas y acordar un proceso de control de cambios.	• Checklist. • Entrevista al Coordinador del CSI.

Cuadro Nº 26. Matriz de Pruebas MEA01.01
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)	
MEA01 -Supervisar, evaluar y valorar el rendimiento y la conformidad.	
Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
MEA01.04: Analizar e informar sobre el rendimiento. • Recomendar cambios a los objetivos (p. ej., cumplimiento, rendimiento, valor, riesgo), cuando sea procedente. • Distribuir los informes a las partes interesadas relevantes. • Documentar las incidencias para contar con una guía adicional si el problema vuelve a aparecer y documentar los resultados.	• La no documentación de las incidencias y resultados. • Riesgo de que la Gerencia de la empresa desconozca acerca de los informes de incidencias, debido a la falta de distribución de dichos informes.

Cuadro 27. Programa de Auditoría MEA01.04
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)		
MEA01 -Supervisar, evaluar y valorar el rendimiento y la conformidad.		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
MEA01.04: Analizar e informar sobre el rendimiento. • Recomendar cambios a los objetivos (p. ej., cumplimiento, rendimiento, valor, riesgo), cuando sea procedente. • Distribuir los informes a las partes interesadas relevantes. • Documentar las incidencias para contar con guía adicional si el problema vuelve a aparecer y documentar los resultados.	***Evaluación de Controles:*** Verificar que exista documentación de incidencias que permiten contar con una guía adicional para la resolución de los problemas más comunes, los cuales también se debe documentar. ***Probando que:*** El analizar e informar sobre el rendimiento, nos permitirá recomendar cambios a los objetivos del área del CSI, distribuir los informes a la Gerencia de la empresa y documentar las incidencias.	• Checklist. • Entrevista al Coordinador del CSI.

Cuadro Nº 28. Matriz de Pruebas MEA01.04
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)	
MEA01 -Supervisar, evaluar y valorar el rendimiento y la conformidad.	
Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
MEA01.05: Asegurar la implantación de medidas correctivas. • Revisar las respuestas, alternativas y recomendaciones de la dirección con el fin de tratar los problemas y desviaciones mayores. • Informar de los resultados a las partes interesadas.	• No enmendar los errores y desviaciones relevantes. • No comunicar de resultados a la Gerencia de la empresa.

Cuadro Nº 29. Programa de Auditoría MEA01.05
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)		
MEA01 -Supervisar, evaluar y valorar el rendimiento y la conformidad.		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
MEA01.05: Asegurar la implantación de medidas correctivas. • Revisar las respuestas, alternativas y recomendaciones de la dirección con el fin de tratar los problemas y desviaciones mayores. • Informar de los resultados a las partes interesadas.	***Evaluación de Controles:*** Verificar que exista revisión de respuestas, alternativas y recomendaciones para poder tratar los mayores problemas que se tienen, informando los resultados a la Gerencia de la empresa. ***Probando que:*** Mediante la implantación de medidas correctivas se podrá informar sobre los resultados a la Gerencia de la empresa.	• Checklist. • Entrevista al Coordinador del CSI. • Informe de medidas preventivas y correctivas. • Revisión de la Directiva Nº001-2015-GR.LAMB.GERESA

Cuadro Nº 30. Matriz de Pruebas MEA01.05
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)	
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.	
Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
MEA02.01 Supervisar el control interno. • Realizar actividades de evaluación y supervisión del control interno basadas en los estándares de gobierno organizativos. • Considerar las evaluaciones independientes del sistema de control interno. • Identificar los límites del sistema de control interno de TI. • Asegurar que las actividades de control están operativas y que las excepciones son comunicadas puntualmente, seguidas y analizadas.	• Evaluaciones y supervisiones no eficaces si es que no se basan en estándares. • Limitaciones en el sistema de control interno del área del CSI. • Falta de un óptimo rendimiento del sistema de control de TI, por falta de evaluaciones constantes.

Cuadro Nº 31. Programa de Auditoría MEA02.01
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)		
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
MEA02.01 Supervisar el control interno. • Realizar actividades de evaluación y supervisión del control interno basadas en los estándares de gobierno organizativos. • Considerar las evaluaciones independientes del sistema de control interno. • Identificar los límites del sistema de control interno de TI. • Asegurar que las actividades de control están operativas y que las excepciones son comunicadas puntualmente, seguidas y analizadas.	***Evaluación de Controles:*** Verificar que exista una evaluación del área de control interno e independiente que permitan mantener los cambios en el curso del negocio y el riesgo de TI. ***Probando que:*** Mediante las actividades de evaluación y supervisión del control interno, se asegurará que las actividades de control estén operativas y se evaluará regularmente el rendimiento de control de TI.	• Checklist. • Entrevista al Responsable de la Oficina de Control Institucional.

Cuadro Nº 32. Matriz de Pruebas MEA02.01
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)	
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.	
Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio. • Priorizar el riesgo de acuerdo con los objetivos organizativos. • Identificar los controles. • Identificar la información que indica de forma convincente si el entorno de control interno está operando de forma efectiva. • Mantener evidencia de la efectividad del control.	• Riesgo de no poder corregir oportunamente los procesos que se requieren, debido a la falta de priorización y de acuerdo a los objetivos de la empresa. • Riesgo de que no existan controles necesarios que permitan mejorar los procesos de negocio.

Cuadro Nº 33. Programa de Auditoría MEA02.02
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)		
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio. • Priorizar el riesgo de acuerdo con los objetivos organizativos. • Identificar los controles clave. • Identificar la información que indica de forma convincente si el entorno de control interno está operando de forma efectiva. • Mantener evidencia de la efectividad del control.	***Evaluación de Controles:*** Verificar que existan controles para desarrollar una estrategia adecuada e identificación de la información de forma convincente respecto al entorno de control interno y mantenga evidencia de la efectividad. ***Probando que:*** Al identificar la información se priorizará el riesgo de acuerdo con los objetivos organizativos de la empresa.	• Checklist. • Entrevista al Coordinador del CSI.

Cuadro Nº 34. Matriz de Pruebas MEA02.02
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)	
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.	
Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
MEA02.03 Realizar autoevaluaciones de control. • Identificar los criterios que se deben tener cuenta para la realización de las autoevaluaciones. • Determinar la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua. • Comparar los resultados de las autoevaluaciones con estándares y buenas prácticas. • Resumir y comunicar los resultados de las autoevaluaciones y los estudios comparativos para considerar acciones correctivas.	• Riesgo de no considerar acciones correctivas de control, debido a la falta de conocimiento de los riesgos que existen. • Riesgo de realizar autoevaluaciones inadecuadas debido a la no alineación con estándares y buenas prácticas.

Cuadro Nº 35. Programa de Auditoría MEA02.03
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)		
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
MEA02.03 Realizar autoevaluaciones de control. • Identificar los criterios para la realización de las autoevaluaciones. • Determinar la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua. • Comparar los resultados de las autoevaluaciones con estándares y buenas prácticas. • Resumir y comunicar los resultados de las autoevaluaciones y los estudios comparativos para considerar acciones correctivas.	***Evaluación de Controles:*** Verificar que existan criterios para la realización de las autoevaluaciones, comparando los resultados con las buenas prácticas y comunicando dichos resultados. ***Probando que:*** Mediante las autoevaluaciones se podrá resumir y comunicar los resultados de estas y se considerarán acciones correctivas.	• Checklist. • Entrevista al Coordinador del CSI.

Cuadro Nº 36. Matriz de Pruebas MEA02.03
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)	
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.	
Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
MEA02.06: Planificar iniciativas de aseguramiento. • Realizar una evaluación del riesgo y/o evaluar la capacidad del proceso para diagnosticar el riesgo e identificar los procesos críticos de TI. • Seleccionar, adaptar y llegar a un acuerdo sobre los objetivos de control para los procesos críticos que serán la base para la evaluación de control.	• Riesgo de no realizar evaluaciones adecuadas, acorde a los controles de los procesos críticos de TI.

Cuadro Nº 37. Programa de Auditoría MEA02.06
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)		
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
MEA02.06: Planificar iniciativas de aseguramiento. • Realizar una evaluación del riesgo y/o evaluar la capacidad del proceso para diagnosticar el riesgo e identificar los procesos críticos de TI. • Seleccionar, adaptar y llegar a un acuerdo sobre los objetivos de control para los procesos críticos que serán la base para la evaluación de control.	***Evaluación de Controles:*** Verificar que existan objetivos de control para los procesos críticos y evaluación de la capacidad del proceso para diagnosticar riesgos. ***Probando que:*** Mediante la evaluación de riesgo y la capacidad de diagnosticarlo, se podrá seleccionar los procesos críticos fundamentales para la evaluación de control.	• Checklist. • Entrevista al Coordinador del CSI.

Cuadro Nº 38. Matriz de Pruebas MEA02.06
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)	
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.	
Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.	
OBJETIVOS DE CONTROL DETALLADO	**FACTORES DE RIESGO**
MEA02.07: Estudiar las iniciativas de aseguramiento. • Definir el alcance actual mediante la identificación de los objetivos empresariales y de TI. • Evaluación de la información de los procesos bajo revisión para identificar los controles a ser validados y los hallazgos reales (tanto aseguramiento positivo como cualquier deficiencia) para la evaluación del riesgo.	• No identificación de las iniciativas de aseguramiento más relevantes que existen en la empresa. • No saber qué medidas tomar, debido a la falta de conocimiento respecto a los procesos que ayuden a identificar los controles que deben ser validados.

Cuadro Nº 39. Programa de Auditoría MEA02.07
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)		
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
MEA02.07: Estudiar las iniciativas de aseguramiento. • Definir el alcance actual mediante la identificación de los objetivos empresariales y de TI. • Evaluación de la información de los procesos bajo revisión para identificar los controles a ser validados y los hallazgos reales (tanto aseguramiento positivo como cualquier deficiencia) para la evaluación del riesgo.	***Evaluación de Controles:*** Verificar que exista una evaluación de la información de los procesos e identificación de los controles y los hallazgos reales de riesgo. ***Probando que:*** Mediante la evaluación de los procesos se definirá la situación actual de los objetivos empresariales y de TI.	• Checklist. • Entrevista al Coordinador del CSI.

Cuadro 40. Matriz de Pruebas MEA02.07
Fuente: Elaboración Propia

5.4.- Análisis de Verificación

En los siguientes cuadros podremos observar que se mantiene la *revisión* de los objetivos de control detallados, *a través de Evaluaciones de Controles* para probar que se cumplan con dichos objetivos, mediante la *Descripción de la Prueba,* se tomarán como tales: los documentos, entrevistas y checklist que se aplicarán en la Auditoría.

En la columna *Evaluación* se colocará una de 2 respuestas: **Efectivos**, el cual se dará cuando se cumplan los requerimientos y **No efectivos** cuando no se cumplan.

En la columna *Documentos de Soporte*, se mencionarán los documentos que ayudarán a la revisión del cumplimiento de cada objetivo. Por último en la columna *Recomendaciones,* se emitirán de manera general las medidas que se deberían tomar para lograr el cumplimiento de cada objetivo.

En base a esto se presentará más adelante: observaciones, riesgos y recomendaciones de manera más detallada en el informe final de auditoría.

A continuación se muestran los cuadros de Evaluación de Pruebas, agrupados de acuerdo a los dominios de COBIT versión 5.

PROCESOS DEL DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
APO07 Dominio Alinear, Planificar y Organizar				
APO07.01 Mantener la dotación de personal suficiente y adecuado				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Cumplimiento de política de contrataciones de personal, mediante los procedimientos de contratación y capacitación del personal TI, política y manual de funciones de la GERESA. ***Probando que:*** El personal TI es suficiente, adecuado y sobre todo si está suficientemente capacitado para desempeñar las funciones que tienen asignadas.	• Revisión del Plan Anual de Capacitación del personal TI. • Entrevista al Coordinador del CSI. • Entrevista al Jefe de Gestión y Desarrollo de Potencial Humano.	NO EFECTIVO	• Plan Anual de Capacitación del personal TI. • Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)** • Checklist al Jefe de Gestión y Desarrollo de Potencial Humano.**(Ver Anexo Nº 4)**	-Realizar evaluaciones periódicas para detectar las necesidades de personal TI en el área del CSI. -Elaborar un documento dirigido a la oficina de RR.HH., solicitando personal idóneo (ingenieros y/o técnicos), de acuerdo a las necesidades del área del CSI.

Cuadro Nº 41. Evaluación De Pruebas APO07.01
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR				
APO07. Gestionar los Recursos Humanos				
APO07.03 Mantener las habilidades y competencias de Personal.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar procedimientos de evaluaciones periódicas para identificar si las habilidades y competencias del personal TI son óptimas para lograr los objetivos de empresa. ***Probando que:*** El personal TI mantiene y está en constante mejora de sus competencias y habilidades para desarrollar eficientemente sus labores.	• Revisión del Plan Anual de Capacitación del personal TI. • Entrevista al Jefe de Gestión y Desarrollo de Potencial Humano.	NO EFECTIVO	• Plan Anual de Capacitación del personal TI. • Checklist al Jefe de Gestión y Desarrollo de Potencial Humano. **(Ver Anexo Nº 4)**	-Establecer un plan de revisiones periódicas para evaluar la evolución de las habilidades y competencias del personal TI en el área del CSI.

Cuadro Nº 42. Evaluación de Pruebas APO07.03
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR				
APO07. Gestionar los Recursos Humanos				
APO07. 04 Evaluar el desempeño laboral de los empleados.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar un proceso de evaluación para determinar el desempeño de las labores del personal del CSI que permitan cumplir con los objetivos funcionales de la empresa. ***Probando que:*** Los empleados desempeñan una correcta labor en sus funciones diarias.	• Entrevista Jefe de Gestión y Desarrollo de Potencial Humano.	EFECTIVO	• Checklist al Jefe de Gestión y Desarrollo de Potencial Humano **(Ver Anexo Nº 4)**	_

Cuadro Nº 43. Evaluación de Pruebas APO07.04
Fuente: Elaboración Propia

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR				
APO07. Gestionar los Recursos Humanos				
APO07. 06 Gestionar el personal contratado.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que existan políticas y procedimientos para gestionar el personal contratado en el área del CSI. ***Probando que:*** Se está gestionando de manera apropiada el personal contratado, de acuerdo a las políticas y procedimientos de la empresa.	• Revisión de la Ley de Contrataciones del Estado. • Entrevista al Jefe de Gestión y Desarrollo de Potencial Humano	EFECTIVO	• Ley de Contrataciones del Estado Nº 30225. • Checklist al Jefe de Gestión y Desarrollo de Potencial Humano **(Ver Anexo Nº 4)**	–

Cuadro Nº 44. Evaluación de Pruebas APO07.06
Fuente: Elaboración Propia

PROCESOS DEL DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)				
DSS02. Gestionar Peticiones e Incidentes de Servicio				
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que cuente con un esquema de clasificación para priorizar peticiones de servicio e incidentes que se presentan diariamente. ***Probando que:*** La definición de modelos de incidentes para errores ya conocidos, nos facilitará su resolución de manera eficiente y eficaz.	• Entrevista al Responsable de Soporte Técnico-CSI .	NO EFECTIVO	• Checklist al Responsable de Soporte Técnico-CSI **(Ver Anexo Nº 5)**	-Establecer una política de gestión de incidentes, teniendo en cuenta la clasificación y priorización de incidentes para el registro de problemas.

Cuadro Nº 45. Evaluación de Pruebas DSS02.01
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)				
DSS02. Gestionar Peticiones e Incidentes de Servicio				
DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que cuente con un registro de clasificación y priorización de peticiones de servicios e incidentes. ***Probando que:*** El priorizar las peticiones e incidentes ayudará a solucionarlos de una mejor manera, ya que se resolverá de acuerdo al tipo y categoría que tengan.	• Entrevista al Responsable de Soporte Técnico- CSI. • Revisión de Registro de incidentes y servicios solucionados. .	NO EFECTIVO	• Checklist al Responsable de Soporte Técnico- CSI. **(Ver Anexo Nº 5)** • Registro de incidentes y servicios solucionados.	-Establecer un registro de toda la información relevante de los incidentes y peticiones de servicios de acuerdo al tipo y categoría de estos.

Cuadro Nº 46. Evaluación de Pruebas DSS02.02
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)				
DSS02. Gestionar Peticiones e Incidentes de Servicio				
DSS02.04 Investigar, diagnosticar y localizar incidentes.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que cuente con síntomas relevantes que permiten diagnosticar y localizar incidentes de manera que se asignen especialistas con un nivel de gestión apropiado cuando se es necesario. ***Probando que:*** Al registrar nuevos problemas se definen fuentes de conocimientos de incidentes y peticiones para lograr resolverlos de manera idónea.	• Entrevista al Responsable de Soporte Técnico-CSI. .	EFECTIVO	• Checklist al Responsable de Soporte Técnico-CSI. **(Ver Anexo Nº 5)**	–

Cuadro Nº 47. Evaluación de Pruebas DSS02.04
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)				
DSS05. Gestionar servicios de seguridad				
DSS05.02: Gestionar la seguridad de la red y las conexiones.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que cuente con protocolos de seguridad aprobados para brindar soporte a la trasmisión y recepción segura de información mediante las conexiones de red. ***Probando que:*** La seguridad ofrecida por los protocoles aprobados establecerá mecanismos de confianza para dar soporte a las conexiones de red y una adecuada protección al sistema.	• Entrevista al Responsable de Soporte Técnico-CSI. • Revisión de la Configuración de los equipos. .	EFECTIVO	• Checklist al Responsable de Soporte Técnico-CSI. **(Ver Anexo Nº 5)** • Configuración de equipos. **(Ver Anexo Nº 8)**	_

Cuadro Nº 48. Evaluación de Pruebas DSS05.02
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)				
DSS05. Gestionar servicios de seguridad				
DSS05.03: Gestionar la seguridad de los puestos de usuario final.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que exista protección física y mecanismos de bloqueo a los dispositivos de los usuarios finales. ***Probando que:*** Mediante la protección física de los dispositivos se logrará proteger la integridad del sistema y de la red.	• Entrevista al Responsable de Soporte Técnico-CSI. • Revisión del Plan de Contingencia.	EFECTIVO	• Checklist al Responsable de Soporte Técnico-CSI. **(Ver Anexo Nº 5)** • Plan de Contingencia - 2014. **(Ver Anexo Nº 9)**	_

Cuadro Nº 49. Evaluación de Pruebas DSS05.03
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)				
DSS06. Gestionar Controles de Proceso de Negocio				
DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que exista documentación y supervisión de actividades de control de los procesos de negocio, el cual satisface los requerimientos de control para los objetivos estratégicos y corporativos de la GERESA. ***Probando que:*** Con la supervisión de las actividades de extremo a extremo, se identificará oportunidades de mejora para el negocio.	• Entrevista al Coordinador del CSI.	NO EFECTIVO	• Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)**	-Establecer procesos, herramientas y técnicas que permitan verificar el cumplimiento de las políticas y procedimientos.

Cuadro Nº 50. Evaluación de Pruebas DSS06.01
Fuente: Elaboración Propia

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)				
DSS06. Gestionar Controles de Proceso de Negocio				
DSS06.06: Asegurar los activos de información.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que existan políticas de clasificación de datos y procedimientos para proteger los activos de información, bajo el control de negocio así mismo restringiendo el uso, distribución y el acceso físico a la información. ***Probando que:*** Al asegurar los activos de información no solo se podrá restringir el acceso físico a la información, sino que además logrará informar al negocio y a otros grupos de interés, acerca de violaciones y desviaciones.	• Entrevista al Coordinador del CSI. • Revisión de las políticas de clasificación de información y protección de activos.	EFECTIVO	• Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)**	–

Cuadro Nº 51. Evaluación de Pruebas DSS06.06
Fuente: Elaboración Propia

PROCESOS DEL DOMINIO SUPERVISAR, EVALUAR Y VALORAR (MEA)

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)				
MEA01. Supervisar, evaluar y valorar el rendimiento y la conformidad.				
MEA01.01: Establecer un enfoque de la supervisión.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que exista un proceso de control de cambios, así mismo se comunica los objetivos y requisitos empresariales para lograr eficiencia, efectividad y confidencialidad en la supervisión. ***Probando que:*** Al establecer una supervisión eficiente y efectiva se logrará involucrar a la Gerencia de la empresa y acordar un proceso de control de cambios.	• Entrevista al Coordinador del CSI.	NO EFECTIVO	• Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)**	-Establecer un proceso de control de cambios y de gestión en la supervisión y presentación de los informes generados en el área.

Cuadro Nº 52. Evaluación de Pruebas MEA01.01
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)				
MEA01. Supervisar, evaluar y valorar el rendimiento y la conformidad				
MEA01.04: Analizar e informar sobre el rendimiento.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que exista documentación de incidencias que permiten contar con una guía adicional para la resolución de los problemas más comunes, los cuales también se debe documentar. ***Probando que:*** El analizar e informar sobre el rendimiento, nos permitirá recomendar cambios a los objetivos del área del CSI, distribuir los informes a la Gerencia de la empresa y documentar las incidencias.	• Entrevista al Coordinador del CSI.	NO EFECTIVO	• Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)**	-Definir e implementar cambios en los objetivos y métricas cuando sea procedente así mismo distribuir informes sobre el rendimiento a la Gerencia.

Cuadro Nº 53. Evaluación de Pruebas MEA01.04
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)				
MEA01. Supervisar, evaluar y valorar el rendimiento y la conformidad				
MEA01.05: Asegurar la implantación de medidas correctivas.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que exista revisión de respuestas, alternativas y recomendaciones para poder tratar los mayores problemas que se tienen, informando los resultados a la Gerencia de la empresa. ***Probando que:*** Mediante la implantación de medidas correctivas se podrá informar sobre los resultados a la Gerencia de la empresa.	• Entrevista al Coordinador del CSI. • Revisión de Informe de medidas preventivas y correctivas. • Revisión de la Directiva Nº001-2015-GR.LAMB.GERESA.	EFECTIVO	• Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)** • Informe de medidas preventivas y correctivas. • Directiva Nº001-2015-GR.LAMB.GERESA **(Ver Anexo Nº 11)**	_

Cuadro Nº 54. Evaluación de Pruebas MEA01.05
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)				
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.				
MEA02.01: Supervisar el control interno.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que existan evaluaciones del área de control interno e independiente que permitan mantener los cambios en el curso del negocio y el riesgo de TI. **Probando que:** Mediante las actividades de evaluación y supervisión del control interno asegurará que las actividades de control estén operativas y se evaluará regularmente el rendimiento de control de TI.	• Entrevista al Responsable de la Oficina de Control Institucional.	EFECTIVO	• Checklist al Responsable de la oficina de Control Institucional. **(Ver Anexo Nº 6)**	_

Cuadro Nº 55. Evaluación de Pruebas MEA02.01
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)				
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.				
MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que existan controles para desarrollar una estrategia adecuada e identificación de la información de forma convincente respecto al entorno de control interno y mantenga evidencia de la efectividad. ***Probando que:*** Al identificar la información se priorizará el riesgo de acuerdo con los objetivos organizativos de la empresa.	• Entrevista al Coordinador del CSI.	EFECTIVO	• Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)**	_

Cuadro Nº 56. Evaluación de Pruebas MEA02.02
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)				
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.				
MEA02.03 Realizar autoevaluaciones de control.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMEND ACION**
Evaluación de Controles: Verificar que existan criterios de evaluación para la realización de las autoevaluaciones, comparando y comunicando los resultados con las buenas prácticas. ***Probando que:*** Mediante las autoevaluaciones se podrá resumir y comunicar los resultados de estas y se considerarán acciones correctivas**.**	• Entrevista al Coordinador del CSI.	NO EFECTIVO	• Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)**	-Establecer criterios para realizar autoevaluaciones de control de manera periódica, considerando la efectividad y eficiencia en la supervisión.

Cuadro Nº 57. Evaluación de Pruebas MEA02.03
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)				
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.				
MEA02.06: Planificar iniciativas de aseguramiento.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de Controles: Verificar que existan objetivos de control para los procesos críticos y evaluación de la capacidad del proceso para diagnosticar dicho riesgo. ***Probando que:*** Mediante la evaluación de riesgo y la capacidad de diagnosticarlo, se podrá seleccionar los procesos críticos fundamentales para la evaluación de control.	• Entrevista al Coordinador del CSI.	NO EFECTIVO	• Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)**	-Establecer evaluaciones que permitan diagnosticar el riesgo e identificar los procesos críticos de TI.

Cuadro Nª 58. Evaluación de Pruebas MEA02.06
Fuente: Elaboración Propia

DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)				
MEA02 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.				
MEA02.07: Estudiar las iniciativas de aseguramiento.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACIÓN**
Evaluación de Controles: Verificar que exista una evaluación de la información de los procesos e identificación de los controles y los hallazgos reales de riesgo. ***Probando que:*** Mediante la evaluación de los procesos se definirá la situación actual de los objetivos empresariales y de TI.	• Entrevista al Coordinador del CSI.	NO EFECTIVO	• Checklist al Coordinador del CSI. **(Ver Anexo Nº 3)**	-Definir el alcance actual de las iniciativas de aseguramiento mediante identificación de los objetivos de la empresa y de TI. Así mismo evaluar la información de los procesos del área bajo revisión para identificar los controles y hallazgos reales.

Cuadro Nº 59. Evaluación de Pruebas MEA02.07
Fuente: Elaboración Propia

5.5.-Informe Preliminar

En base a la evaluación de las pruebas efectuadas sobre la gestión de TI de la GERESA se determinó que el 47% de los objetivos de control detallados, cumplen con las condiciones necesarias, por lo cual se consideran **efectivos** y el 53% de los objetivos de control analizados, no cumplen con las condiciones necesarias, por lo cual se consideran **no efectivos**.

Los informes preliminares que se presentan a continuación, tuvieron su discusión y análisis previo con el responsable del área del CSI, dentro de la organización, en este caso el Coordinador del CSI, Responsable de Soporte Técnico y Responsable del Área de Recursos Humanos.

5.5.1. Objetivos de Control Efectivos

A continuación se detalla el funcionamiento actual de los controles encontrados efectivos**:**

- **APO07.04 Evaluar el desempeño laboral de los empleados**

Actualmente, existen documentos que consideran los objetivos funcionales de la empresa, al establecer las metas individuales, también se implementa y comunica un proceso disciplinario en el área del CSI, por parte del Coordinador de dicha área. Según la entrevista realizada al Responsable de Recursos Humanos, recalca que existe un proceso de evaluación y se dan instrucciones del uso y almacenamiento de información al personal, además se recopila los resultados de las evaluaciones de desempeño el cual se comunica al Gerente de la empresa.

- **APO07.06 Gestionar el personal contratado**

El documento de las políticas del personal contratado, es proporcionado por la Gerencia de la empresa, sin embargo puede ser modificado para adaptarse a las necesidades locales de la misma, y se les requiere su firma de aceptación sobre las posibles acciones a tomar si este no es cumplido a cabalidad, en cuanto al manejo de información a los recursos de TI. El documento antes mencionado, describe el trabajo realizado de acuerdo con la política de contratación de TI de la empresa y el marco de control de TI. Así mismo se requiere contratistas para los procesos de selección y contratación de personal.

- **DSS02.04 Investigar, diagnosticar y localizar incidentes**

Existen registros de los principales incidentes identificados en el área del CSI, los cuales se localizan y se corrigen oportunamente, según lo mencionado en la entrevista al Responsable de Soporte Técnico, señala que en los documentos del área del CSI, se registran los diagnósticos de incidentes en las diferentes áreas de la empresa, consignando las causas más probables que pudieron ocasionarlos, registrando no solo lo más relevante sino todos los datos que sean necesarios para diagnosticar y localizar dichos incidentes, para ello se asignan especialistas con un buen nivel de gestión para lograr la resolución idónea e inmediata de los problemas que se presenten de forma eficiente.

- **DSS05.02: Gestionar la seguridad de la red y las conexiones**

Existen protocolos de seguridad que establecen mecanismos de confianza, las cuales brindan soporte a la trasmisión y recepción segura de información, mediante las conexiones de red para poder acceder a este, cada empleado cuenta con usuario y clave de acceso, previo la creación de usuario se define por parte del Responsable de Soporte Técnico, de acuerdo a las Políticas de la empresa. Además existe una

definición de perfiles de usuario para el ingreso al sistema, las cuales están establecidas en las Políticas de contraseñas y Seguridad de la Información del área del CSI de la GERESA, para el cambio de passwords, y se cuenta con solicitudes formales para la creación de usuarios y acceso al sistema, que deben ser presentadas a la Gerencia de la empresa.

Cuando un empleado deja de trabajar para la empresa, la oficina de Recursos Humanos informa al área del CSI sobre la separación del trabajador para deshabilitar el usuario respectivo.

- **DSS05.03: Gestionar la seguridad de los puestos de usuario final**

Existe protección física y mecanismos de bloqueo a los dispositivos de los trabajadores, mediante la protección física de los dispositivos se logra proteger la integridad del sistema y de la red, para esto se configura los sistemas operativos y se gestiona la configuración de la red de forma segura, asignándose un IP diferente a cada ordenador para evitar conflictos entre estos y sobretodo caídas de red en todas las áreas de la GERESA.

- **DSS06.06: Asegurar los activos de información**

Existen documentos de políticas de clasificación de información y procedimientos, los cuales ayudan a proteger los activos de información, bajo el control de la Gerencia, así mismo se restringe el uso, distribución y el acceso físico a la información. Durante la entrevista al Coordinador del CSI, también recalcó que se informa a la Gerencia, acerca de las violaciones y desviaciones que se dan dentro del área del CSI y demás áreas de la empresa, para que se tomen las acciones correspondientes.

- **MEA01.05: Asegurar la implantación de medidas correctivas**

Actualmente se implementan medidas correctivas en el área del CSI, según lo señalado por el Coordinador del CSI, se realizan revisiones de alternativas y recomendaciones, para poder tratar los problemas y desviaciones más importantes que se presentan en cada área, informando los resultados a la Gerencia de la empresa.

- **MEA02.01 Supervisar el control interno**

Las evaluaciones del área de control interno, según lo mencionado en la entrevista al Responsable de la Oficina de Control Institucional, permiten mantener los cambios en los procesos de la empresa y los riesgos TI, esto conlleva asegurar que las actividades de control estén operativas y se evalúe regularmente el rendimiento de los controles. Además se tienen establecidos los límites del sistema de control interno, el cual permite identificar los procesos más relevantes. Así mismo las excepciones son comunicadas de manera puntual al Gerente de la empresa.

- **MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio**

Existen controles que permiten desarrollar una estrategia adecuada y ayudan a identificar la información de forma precisa, así mismo el Coordinador del CSI recalcó que se priorizará el riesgo de acuerdo con los objetivos de la empresa, los cuales permiten tener un adecuado control sobre los procesos de negocio.

5.5.2. Objetivos de Control No Efectivos

A continuación se detallan los controles encontrados No efectivos y la discusión de estos, con el coordinador del área del Centro de Sistemas de Información.

- **APO07.01 Mantener la dotación de personal suficiente y adecuado**

No existe un procedimiento específico que permita identificar la cantidad de personal necesario para las labores que se requieren, además que tampoco existe un proceso para evaluar las necesidades de personal de manera periódica.

- **Resultado de la discusión con el Coordinador de CSI:**

  La falta de personal en el área del CSI no es considerada relevante ya que se considera las dos personas que conforman esta área y los practicantes pueden resolver los incidentes que se den en la empresa.

- **APO07.03 Mantener las habilidades y competencias de Personal**

No existen procesos que ayuden a identificar las diferencias entre las habilidades necesarias y habilidades disponibles del personal del área del CSI. Además no se lleva a cabo revisiones de manera periódica que permitan evaluar la evolución de las habilidades y competencias del personal de la misma área.

- **Resultado de la discusión con el Coordinador de CSI:**

  La falta de evaluaciones que identifiquen las habilidades y competencias del personal del área del CSI, no se da de manera regular. Lo que si se da son capacitaciones de 1 a 2 veces al año.

- **DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio**

No existen esquemas de clasificación y priorización de incidentes, peticiones de servicios y criterios para el registro de problemas que puedan existir en el área del CSI. Además no existen modelos de peticiones de servicios ni fuentes de conocimientos de incidentes y peticiones ocurridos en la GERESA.

- **Resultado de la discusión con el Coordinador de CSI:**

  Se registran los incidentes y peticiones de servicio que se dan en la empresa, pero no se cuenta con un esquema de clasificación de dichos incidentes y peticiones, ya que no se tiene la suficiente información acerca de esto.

- **DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes**

No se tiene identificado el tipo y categoría de incidentes y peticiones de servicio, además son pocas las veces que se registra la información relevante de los incidentes y peticiones de servicio que se dan en las diferentes áreas de la empresa.

- **Resultado de la discusión con el Coordinador de CSI:**

  Se registran las peticiones e incidentes que se dan en la empresa pero no se cuenta con una clasificación y priorización de estos, ya que no se cuenta con el tiempo disponible para realizarse.

- **DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos**

Se documenta las actividades de control en los procesos del negocio de la GERESA, pero no se supervisa que dichas actividades ayuden a identificar oportunidades de mejora en la empresa.

- **Resultado de la discusión con el Coordinador de CSI:**

  Se tiene documentación de las actividades de control en los procesos del negocio sin embargo no se realizan supervisiones que permitan hallar oportunidades de mejora para la GERESA.

- **MEA01.01: Establecer un enfoque de la supervisión**

El personal del área del CSI no tiene conocimiento sobre todos los objetivos de la empresa. Además de que no existe un proceso de control de cambios y de gestión en la supervisión del área de CSI, solo está documentado.

- **Resultado de la discusión con el Coordinador de CSI:**

  Se encuentra documentado la supervisión que se debe realizar, pero por falta de tiempo y por el poco personal con el que cuenta el área de CSI, no se da de manera continua.

- **MEA01.04: Analizar e informar sobre el rendimiento**

No se recomienda cambios en los objetivos del área del CSI cuando se es necesario, además no se documenta toda la información de las incidencias que se presenta en las diversas áreas de la GERESA, si es que el problema vuelve aparecer. Así mismo no se distribuye periódicamente informes sobre el rendimiento en el área del CSI a la Gerencia de la empresa.

- **Resultado de la discusión con el Coordinador de CSI:**

  No se considera documentar toda la información de las incidencias que puedan ocurrir en las diversas áreas de la Geresa, solo se documenta lo más relevante y así mismo no se distribuye informes de rendimiento del área del CSI a la Gerencia de la empresa, ya que esta solo requiere de estos informes una vez al año.

- **MEA02.03 Realizar autoevaluaciones de control.**

No se realizan autoevaluaciones periódicas, las cuales consideren efectividad y eficiencia en la supervisión. Tampoco se identifican criterios que ayuden a realizarlas, además no se comunican los resultados de las autoevaluaciones a la Gerencia de la empresa.

- **Resultado de la discusión con el Coordinador de CSI:**

  No se considera importante realizar autoevaluaciones, ya que la Oficina de Control Institucional se encarga de hacer la respectiva supervisión al área del CSI.

- **MEA02.06: Planificar iniciativas de aseguramiento.**

No se realizan evaluaciones constantes que permitan diagnosticar el riesgo e identificar los procesos críticos de TI.

- **Resultado de la discusión con el Coordinador de CSI:**

  Por falta de disponibilidad de tiempo, no se realizan evaluaciones que permitan diagnosticar el riesgo y procesos críticos, respecto a las tecnologías de información de la empresa.

- **MEA02.07: Estudiar las iniciativas de aseguramiento.**

No se define el alcance actual de las iniciativas de aseguramiento las cuales se deben identificar mediante los objetivos del área del CSI y de la empresa.

- **Resultado de la discusión con el Coordinador de CSI:**

  Por falta de capacitación referente a las iniciativas de aseguramiento, se desconoce cuáles son los tipos y que iniciativas de aseguramiento se deben implementar para poder reducir riesgos.

5.6.- Informe Final De Auditoría

En este informe se detallará a profundidad las observaciones encontradas respecto a Gestión de TI en el Centro de Sistemas de Información de Gerencia Regional de Salud Lambayeque, así mismo se explicarán los riesgos y se emitirán recomendaciones acerca de dichos objetivos de control hallados No efectivos.

INFORME

Gerencia Regional de Salud Lambayeque

Febrero de 2016

Señores

Gerencia Regional de Salud Lambayeque

Ing. Yoverth Torres Monje

De nuestra consideración:

Nos dirigirnos a Ud. a efectos de poner a consideración el Informe de Auditoría aplicada a la Gestión de Tecnologías de Información, bajo el Estándar COBIT (Control Objetives Information Technologies) practicada desde Diciembre a Febrero del corriente, y en base al análisis y procedimientos aplicados a las informaciones recopiladas se emite el presente informe.

Fecha de Inicio de la Auditoría: Diciembre del 2015

Fecha de Redacción del Informe de la Auditoría: Febrero del 2016

Equipo Auditor:

- Shirley Lizeth Carrillo Prada.
- Kely Karina Suclupe Tejada

5.6.1. Observaciones de los objetivos de control no efectivos en la empresa

- **Observación 1:**

Por medio de la entrevista y checklist aplicados al Coordinador del CSI y al Responsable de Recursos Humanos, no se detectó procedimientos que permitan identificar la cantidad de personal necesario para las labores que se requieren, además no se detectó procesos para evaluar las necesidades de personal de manera periódica, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control *APO07.01* Mantener la dotación de personal suficiente y adecuado. La cual señala que se debe implementar estos procesos y actualmente no se realiza en la GERESA.

- **Riesgo:**

  Al no existir un procedimiento que permita identificar las necesidades de personal, genera el riesgo de no poder corregir algún incidente que pueda ocurrir en algunas de las áreas de la GERESA por falta de personal TI.

- **Recomendación:**

  Planear y ejecutar evaluaciones periódicas para detectar las necesidades de personal en el área del CSI. Elaborar un documento dirigido solicitando personal idóneo (ingenieros y/o técnicos) de acuerdo a las necesidades del área del CSI.

- **Observación 2:**

Por medio de la entrevista y checklist aplicado al Responsable de Recursos Humanos, no se detectó procesos que ayuden a identificar las diferencias entre las habilidades necesarias y habilidades disponibles del personal del área del CSI. Por otra parte también se constató, que no se realizan revisiones periódicas que permitan evaluar la evolución de las habilidades y competencias del personal de la misma área, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control *APO07.03* Mantener las habilidades y competencias de Personal. La cual señala que se debe implementar estos procesos y actualmente no se realiza en la GERESA.

- **Riesgo:**

  El no llevar a cabo revisiones periódicas para evaluar al personal, genera el no saber cuáles son las habilidades necesarias y disponibles que debe tener el personal de CSI, además de la falta de productividad en sus labores.

- **Recomendación:**

  Definir un plan de revisiones periódicas para evaluar la evolución de las habilidades y competencias del personal del área del CSI.

- **Observación 3:**

Por medio de la entrevista y checklist aplicado al Responsable de Soporte Técnico – CSI, no se identificó esquemas de clasificación y priorización de incidentes, peticiones de servicios y criterios para el registro de problemas que puedan existir en el área del CSI. También se determinó que no se cuenta con modelos de peticiones de servicios ni fuentes de conocimientos de incidentes y peticiones ocurridos en la GERESA, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control *DSS02.01* Definir esquemas de clasificación de incidentes y peticiones de servicio, la cual señala que se debe definir dichos esquemas y modelos, que actualmente no se realizan en el área del CSI.

- **Riesgo:**

  Al no contar con esquemas de clasificación y priorización de incidentes y peticiones de servicios, ocasiona que no se pueda corregir eficiente y efectivamente los errores más frecuentes que ocurren en la GERESA.

- **Recomendación:**

  Establecer nuevas políticas de gestión de incidentes, teniendo en cuenta la clasificación y priorización de incidentes, los cuales pueden ser por tipo y severidad de incidentes, y en el caso de peticiones pueden ser: peticiones de consulta, peticiones de cambios y peticiones de acceso.

- **Observación 4:**

Por medio de la entrevista y checklist aplicado al Responsable de Soporte Técnico – CSI, se corroboró que no se tiene identificado el tipo y categoría de incidentes y peticiones de servicio, además no se registra toda la información de los incidentes y peticiones de servicio que se dan en las diferentes áreas de la empresa, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control *DSS02.02*.- Registrar, clasificar y priorizar peticiones e incidentes. La cual señala que se debe identificar e implementar dichos procesos y actualmente no se realiza en la GERESA.

- **Riesgo:**

  No registrar información relevante de todas las peticiones e incidentes y el no contar con un orden o una adecuada clasificación de estas, ocasiona el no poder resolver de manera correcta y efectiva los incidentes y peticiones que se presentan en la GERESA.

- **Recomendación:**

  Establecer un registro de toda la información relevante de los incidentes y peticiones de servicio de acuerdo al tipo y categoría de estos; en tipo pueden ser: acceso no autorizado al sistema, denegación de servicios, divulgación de información, infección de malware, entre otros.

- **Observación 5:**

Por medio de la entrevista y checklist aplicado al Coordinador del CSI, se verificó que existe documentación de las actividades de control en los procesos del negocio de la GERESA, pero no se supervisa que dichas actividades ayuden a identificar oportunidades de mejora en la empresa, de acuerdo al objetivo de control *DSS06.01*.- Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos. Si bien se encuentran documentadas las actividades de control que se deben realizar en la empresa, no se supervisa que dichas actividades se realicen, una clara evidencia de esto, es que todos los puertos de las computadoras de la empresa, están activos y cualquier persona puede grabar información por medio de algún dispositivo, así como adjuntar

información de dichas computadoras mediante algún correo electrónico, así como también no existe un programa o mecanismo de bloqueo que restringa el subir a la red o adjuntar desde un correo electrónico, la información que se encuentren en estas.

- **Riesgo:**

  Mantenerse en las mismas actividades de control y no detectar oportunidades de mejora en los procesos de negocio, lo cual puede ocasionar lentitud en dichos procesos.

- **Recomendación:**

  Establecer procesos, herramientas y técnicas que permitan verificar el cumplimiento de las políticas y procedimientos, ya que si bien estas políticas están documentadas, no se toman ninguna de estas medidas para verificar que se cumplan. Uno de estos procesos podría ser, el deshabilitar los puertos de las computadoras en todas las áreas para que no puedan copiar la información de estas a algún dispositivo, además de establecer un mecanismo de bloqueo en las computadoras para evitar que se pueda adjuntar información desde las computadoras de la empresa a algún correo electrónico o página web.

- **Observación 6:**

Por medio de la entrevista y checklist aplicado al Coordinador del CSI, se verificó que el personal del área del Centro de Sistemas de Información, no tiene conocimiento de todos los objetivos de su área. Además se detectó que no existe un proceso de control de cambios y de gestión en la supervisión del área de CSI, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control *MEA01.01*.- Establecer un enfoque de la supervisión. La cual señala que se debe implementar estos procesos y actualmente no se realizan.

- **Riesgo:**

  La falta de eficiencia, efectividad y confidencialidad en los procesos realizados dentro de la empresa debido a la no priorización y reserva de recursos.

- **Recomendación:**

  Establecer un proceso de control de cambios y de gestión en la supervisión y presentación de informes por parte del área del CSI a la gerencia.

- **Observación 7:**

Por medio de la entrevista y checklist aplicado al Coordinador del CSI, se detectó la no documentación de las incidencias que se presentan en las diversas áreas de la GERESA, si es que el problema vuelve aparecer. Además no se distribuye informes sobre el rendimiento en el área del CSI a la Gerencia de la empresa, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control *MEA01.04.-* Analizar e informar sobre el rendimiento. Lo cual actualmente no se realiza en la GERESA.

- **Riesgo:**

  Al no documentarse todas las incidencias y resultados de estas, genera que la Gerencia de la empresa desconozca los informes de los resultados de las incidencias presentadas, debido a la falta de distribución de dichos informes.

- **Recomendación:**

  Definir e implementar cambios en los objetivos del área del CSI cuando sea procedente, además emitir informes sobre el rendimiento de dicha área a la Gerencia de la empresa.

- **Observación 8:**

Por medio de la entrevista y checklist aplicado al Coordinador del CSI, se determinó que no se llevan a cabo autoevaluaciones periódicas, las cuales consideren efectividad y eficiencia en la supervisión. Así mismo no se identifican criterios que ayuden a realizarlas y no se comunican los resultados de

las autoevaluaciones a la Gerencia de la empresa, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control MEA02.03.- Realizar autoevaluaciones de control. Lo que actualmente no se realiza en la GERESA.

- **Riesgo:**

  Al no tomar en cuenta criterios alineados con estándares y buenas prácticas genera que no se puedan realizar autoevaluaciones efectivas. Además debido a la falta de conocimiento de los riesgos que existen, suscita a que no se consideren acciones correctivas de control para dichos riesgos.

- **Recomendación:**

  Establecer criterios de acuerdo a estándares y buenas prácticas, para realizar autoevaluaciones de manera periódica considerando efectividad y eficiencia de la supervisión.

- **Observación 9:**

Por medio de la entrevista y checklist aplicado al Coordinador del CSI, se corroboró que no se realizan evaluaciones constantes que permitan diagnosticar el riesgo e identificar los procesos críticos de TI, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control *MEA02.06.- Planificar iniciativas de aseguramiento.* Las cuales actualmente no se realizan en la GERESA.

- **Riesgo:**

  Al no planificar iniciativas de aseguramiento y al no diagnosticar riesgos en las diversas áreas de la empresa, genera realizar evaluaciones inadecuadas a los controles de los procesos críticos de TI.

- **Recomendación:**

  Planear y ejecutar evaluaciones de manera periódica, las cuales permitan diagnosticar riesgos e identificar los procesos críticos de TI.

- **Observación 10:**

Por medio de la entrevista y checklist aplicado al Coordinador del CSI, se constató que no se tiene definido el alcance actual de las iniciativas de aseguramiento las cuales se deben identificar mediante los objetivos del área del CSI y de la empresa, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control *MEA02.07*.- Estudiar las iniciativas de aseguramiento. Lo cual actualmente no se realiza en la GERESA.

- **Riesgo:**

  La no identificación de las incitativas de aseguramiento y el no tener conocimiento de los hallazgos reales que se presenten, genera no saber qué medidas se deban tomar para corregir dichas deficiencias.

- **Recomendación:**

  Definir el alcance actual de las iniciativas de aseguramiento, mediante la identificación de los objetivos del área del CSI y de la empresa. Así mimo evaluar la información de los procesos para identificar los hallazgos reales.

Conclusiones de la Auditoría Aplicada

- ✓ Si bien el área del Centro de Sistemas de Información, cuenta con algunos controles que permiten verificar los procesos TI, hace falta que se realice una correcta supervisión de estos procesos para brindar un mayor aseguramiento de las políticas de la empresa.

- ✓ El área de CSI no supervisa que se cumplan con las medidas de seguridad, las cuales deben verificar el robo de información de la empresa, ya que los puertos de las computadoras se encuentran habilitados y además no existen un filtro que no permita adjuntar información, ya sea mediante correo o mediante páginas, programas en la nube, lo cual es un riesgo inminente de que el personal o personas externas puedan sustraer información de la empresa.

- ✓ El plan de contingencia es del año 2014, lo que hace que no se tenga medidas correctivas actualizadas ante posibles sucesos de desastres tales como: terremotos, inundaciones, incendios etc., lo cual generaría, sino se toma una correcta acción, grandes pérdidas materiales y por ende un gasto mayor al no actualizar el plan de contingencia actual.

- ✓ Si bien el personal del área del CSI está capacitado, las capacitaciones que se le brindan son realizadas una vez al año cuando deberían hacerse de manera constante para mantener a dicho personal actualizado. Además que el personal del área no se abastece para realizar todos los incidentes que se dan en la empresa, lo cual genera insatisfacción por parte de los usuarios finales.

- ✓ La supervisiones que se dan en el área del CSI, las realiza la oficina de Control Institucional, anualmente, pero esto se dan de manera general, por lo que no se revisan a detalle los procesos TI y las autoevaluaciones que deberían realizarse en el área del CSI no se hacen debido a la falta de tiempo y la aglomeración de tareas en las diferentes área de la empresa.

- ✓ De acuerdo a la auditoría aplicada en el área del Centro de Sistema de Información de la Gerencia Regional de Salud, para la cual se tomó en cuenta: encuestas, entrevistas y checklist según los objetivos de control detallados en COBIT 5, se encontró que 9 de los 19 objetivos de control evaluados, son efectivos por lo que el resultado es Favorable con excepciones, las cuales se deben a que no se mantiene la dotación de personal suficiente en el área, así mismo no existe un proceso que permita mantener las habilidades y competencias del personal TI. Además de que no se tienen definidos esquemas de clasificación de incidentes y peticiones de servicio, los cuales permitan priorizarlos de manera que se les dé una eficaz y eficiente resolución. También una de estas excepciones se da, ya que no se analiza ni se informa sobre el rendimiento del área de CSI a la Gerencia de manera constante. Por otro lado, no se planifican ni estudian iniciativas de aseguramiento que permitan diagnosticar el riesgo e identificar los procesos críticos de TI.

CAPITULO VI

COSTOS Y BENEFICIOS

6.1.-Análisis de Costos

Se detallarán a continuación los costos que se realizaron en el proyecto de investigación:

6.1.1. Costo de Servicio y Materiales

a. Servicios

- Servicios de Internet	S/. 300.00
- Viáticos	S/. 500.00
- Movilidad	S/. 400.00
- Llamadas	S/. 150.00
- Luz	S/. 420.00
- Impresiones	S/. 250.00
- Fotocopias	S/. 180.00
Subtotal (1):	S/. 2,200.00

b. Materiales

-1 Laptop Lenovo - Intel Core i5	S/. 2,800.00
-5 Recarga de cartuchos	S/. 100.00
-2 USB	S/. 60.00
-2 Millares de Hojas Bond	S/. 50.00
-4 Lapiceros	S/. 8.00
-8 Fólderes Manilas	S/. 4.00
Subtotal (2):	S/. 3,022.00

6.1.2. Resumen de Costos

Subtotal (1)	S/. 2,200.00
Subtotal (2)	S/. 3,022.00
Total	S/. 5,222.00

6.1.2.-Beneficios

En el siguiente punto señala los beneficios del Proyecto de Investigación, tal como: Tangible e Intangibles.

6.1.2.1. Beneficios Tangibles

- Al contar con suficiente personal del CSI la atención al usuario final será más eficiente y eficaz.
- Mayor capacitación al personal de CSI.
- Protección de información.
- Se podrán generar todos los reportes de los incidentes de cada área de la empresa a Gerencia.

6.1.2.2. Beneficios Intangibles

- Mejoremos la producción del personal.
- Aumentará la calidad de satisfacción.
- Mejoraremos la satisfacción en el trabajo.
- Mayor seguridad de la información.

6.2.- Recuperación de la Inversión

A continuación se detallará los costos y beneficios que se tendría al implantar las recomendaciones brindadas en esta auditoría, así mismo señalando el Valor Absoluto Neto y la Tasa Interna de Retorno.

Consideraciones

Las Cifras en este estudio están basadas en los siguientes criterios:

- Para estimar los costos de Plataforma Propietaria se ha considerado las cotizaciones de Windows 7 Professional, puesto que en la actualidad ya no se están licenciando productos esa versión.
- Todos los precios están expresados en soles.

6.2.1. Distribuciones de los costos para software Propietario

6.2.2.1. Costo de Inversión

- **Costo por Licencias**

El total de computadoras en GERESA son 190, de las cuales 50 tienen instalado Sistema Operativo Ubuntu, 140 tienen instalado W7 Professional (40 cuentan con licencia original OEM y 100 no cuentan con dicha licencia). Además de las 140 computadoras no cuentan con Antivirus con licencia original. Los costos de Licencia Original de software propietario y Antivirus son:

Costos por Licencias	**CANT.**	**P.UNIT. S/.**	**TOTAL S/.**
Windows 7 Professional (64 y X86)	100	825.00	82,500.00
Eset NOD32 Antivirus (para 3 PC)	47	185.00	8,695.00
		Total	91,195.00

Cuadro Nº 60. Costos por Licencias

Fuente: Elaboración Propia

Esta información se puede corroborar por medio de la información mostrada en el **(Ver Anexo Nº 11)**

- **Capacitación**

Esta capacitación estará destinada a tres de los responsables del área del Centro de Sistemas de Información de los servicios de la GERESA, durante 5 días, 8 horas al día.

El costo para esta capacitación en **"Gobierno y Gestión de las TI"** es de S/.300.00 **(Ver Anexo Nº 11)**

Costos por Capacitación	**Nº Per.**	**P.UNIT. S/.**	**TOTAL S/.**
Capacitación	3	900.00	2,700.00

Cuadro Nº 61. Costo por Capacitación
Fuente: Elaboración Propia

Gastos adicionales por viáticos son los siguientes:

Costos por Viáticos	**Nº Per.**	**Días**	**P.UNIT. S/.**	**TOTAL S/.**
Hospedaje	3	5	40.00	600.00
Movilidad	3	5	5.00	75.00
Comida	3	5	25.00	375.00
Pasajes (Ida y Vuelta)	3		120.00	360.00
			Total	1410.00

Cuadro Nº 62. Costos por Viáticos
Fuente: Elaboración Propia

- **Costo Total de Inversión**

Costos de Inversión	**CANT.**	**P.UNIT. S/.**	**TOTAL S/.**
Windows 7 Professional (64 y X86)	100	825.00	82,500.00
Eset NOD32 Antivirus (para 3 PC)	47	185.00	8,695.00
Capacitación	3	900.00	2,700.00
Viáticos	3	470.00	1410.00
		Total	95,305.00

Cuadro Nº 63. Costos Total de Inversión
Fuente: Elaboración Propia

6.2.2.2. Costos de operación

- **Soporte Técnico**

El soporte técnico para el Antivirus está incluido en el costo por licencias durante los siguientes 3 meses.

Costos por Soporte Técnico	**Mes 1 S./**	**Mes 2 S./**	**Mes 3 S./**
Soporte Técnico	0.00	0.00	0.00

Cuadro Nº 64. Costos por Soporte Técnico
Fuente: Elaboración Propia

- **Recursos Humanos**

Los servicios por Auditoría Informática en el área del CSI de la GERESA por 3 meses.

Costos por Auditaría	**Mes 1 S./**	**Mes 2 S./**	**Mes 3 S./**
Equipo Auditor (2)	4,000.00	4,000.00	4,000.00

Cuadro Nº 65. Costos por Auditaría
Fuente: Elaboración Propia

- **Costo Total de Operación**

Costo de Operación	**Mes 1 S./**	**Mes 2 S./**	**Mes 3 S./**
Soporte Técnico	0.00	0.00	0.00
Equipo Auditor (2)	4,000.00	4,000.00	4,000.00
Total	4,000.00	4,000.00	4,000.00

Cuadro Nº 66. Costo Total de Operación

Fuente: Elaboración Propia

6.2.2. Beneficio del Proyecto

A continuación detallaremos los Beneficios Tangibles e Intangibles del proyecto.

6.2.2.1. Beneficios tangibles

- **Reducción de Costos en Multa**

Las Licencias originales de software W7 Professional y Eset NOD32 Antivirus son necesarias, para el buen funcionamiento de las Computadoras del área del CSI y de GERESA. La multa según INDECOPI por no contar con licencia original en las computadoras de cualquier entidad es S/. 693,000.00 **(Ver Anexo Nº 12)**

Descripción	**Cobro S./**
Ahorro de multa de licencia no original	693,000.00

Cuadro Nº 67. Reducción Costos en Multa

Fuente: Elaboración Propia

- **Ahorro de pérdidas de información**

Descripción	**Cobro S./**
Ahorro de pérdidas de información	885,000.00

Cuadro Nº 68. Ahorro de pérdidas de información

Fuente: Elaboración Propia

Esta información se puede verificar por medio de la información mostrada en **(Ver Anexo Nº 13)**

- **Actualización del Plan de Contingencia**

Descripción	**Cobro S./**
Ahorro por Actualización	548,700.00

Cuadro Nº 69. Actualización del Plan de Contingencia

Fuente: Elaboración Propia

Esta información se puede corroborar a través de la información presentada en el **(Ver Anexo Nº 14)**

- **Ahorro de Capacitación de Personal**

  Criterios que se deben considerar para capacitación del personal:

  - La gente sin capacitación tarda hasta seis veces más en realizar su trabajo, que una persona capacitada y motivada.
  - La capacitación mejora la retención. En aquellas empresas en las que no hay capacitación de ningún tipo, 41% de las personas quieren irse. En aquellas en las que sí la hay, sólo 12% busca irse. (Harris, 2012)

    Esto implica un gran costo para la organización.

  - Un estudio longitudinal realizado por la Sociedad Americana de Capacitación y Desarrollo muestra que las empresas que invierten

$1500 dólares en capacitación por empleado, comparado con aquellos que invierten $125, experimentan, en promedio, un aumento del 24% en margen de ganancia y 218% mayor productividad por empleado!

- Así, la capacitación debe verse como una inversión, no un gasto. Exija calidad, garantía, flexibilidad y compromiso por parte de las firmas de capacitación que contrate.

Descripción	**Cobro S./**
Ahorro por Capacitación Personal	3,000.00

Cuadro Nº 70. Ahorro de Capacitación de Personal

Fuente: Elaboración Propia

6.2.2.2. Total de Beneficios Tangibles

Descripción	**Cobro S./**
Ahorro de multa de licencia no original	693,000.00
Ahorro de pérdidas de información	885,000.00
Ahorro por Actualización Plan de Contingencia	548,700.00
Ahorro por Capacitación Personal	3,000.00

Suma Total	**S./** 2,129,700.00
Proyectado por 3 meses	**S./** 709,900.00

Cuadro Nº 71. Total de Beneficios Tangibles

Fuente: Elaboración Propia

6.2.2.3. Beneficios intangibles

- Propiedad y decisión de uso del software por parte de la empresa.
- Garantiza un soporte de hardware seguro.
- Facilidad de uso.
- Interfaces amigables.
- Toma de decisiones centralizada.

6.2.2.4. Valor Actual Neto

En el siguiente punto se detallará el procedimiento del desarrollo del Valor Actual Neto, la cual se estima la duración del Proyecto en 3 meses, así mismo señala la Tasa de Interés, los resultados del Costo de Inversión, Costo de Operación y Beneficio Actual, la cual ayudará a obtener dicho valor.

El valor mostrado a continuación, es un valor promedio extraído de tres bancos importantes del país como: Banco de Crédito, BBVA y ScotiaBank.

I = Tasa de Interés FA bancaria mensual: 1,4%

	Mes 0 S./	**Mes 1 S./**	**Mes 2 S./**	**Mes 3 S./**
Costo de Inversión (CI)	95,305.00	0.00	0.00	0.00
Costo de Operación (CO)	0,00	4,000.00	4,000.00	4,000.00
Beneficio Mensual (B)	0,00	709,900.00	709,900.00	709,900.00

Cuadro Nº 72. Resultados de CI, CO y B.
Fuente: Elaboración Propia

Como podemos observar se procede a aplicar la fórmula del Valor Actual Neto y a reemplazar los resultados del Beneficio, Costo de Inversión y Costo de Operación.

$$\mathbf{V\ A\ N} = \sum_{i=0}^{n} \frac{B_i - C_i}{\left(1 + \frac{i}{100}\right)^n}$$

$$\mathbf{V\ A\ N} = \frac{B_0 - CI_0}{\left(1 + \frac{1{,}4}{100}\right)^0} + \frac{B_1 - CO_1}{\left(1 + \frac{1}{100}\right)^1} + \frac{B_2 - CO_2}{\left(1 + \frac{1}{100}\right)^2} + \frac{B_3 - CO_3}{\left(1 + \frac{1}{100}\right)^3}$$

$$\mathbf{V\ A\ N} = \frac{-95{,}305}{\left(1 + \frac{1{,}4}{100}\right)^0} + \frac{709{,}900.00 - 4{,}000}{\left(1 + \frac{1{,}4}{100}\right)^1} + \frac{709{,}900.00 - 4{,}000}{\left(1 + \frac{1{,}4}{100}\right)^2} + \frac{709{,}900.00 - 4{,}000}{\left(1 + \frac{1{,}4}{100}\right)^3}$$

	Mensual 0 S/.	**Mensual 1 S/.**	**Mensual 2 S/.**	**Mensual 3 S/.**
Costo de Inversión (CI)	95,305.00	0.00	0.00	0.00
Costo de Operación (CO)	0,00	4,000.00	4,000.00	4,000.00
Beneficio Mensual (B)	0,00	709,900.00	709,900.00	709,900.00
VAN	-95,305.00	696,153,85	686,542,25	677,063.38
V A N = S/. 1, 964,454.48				

Cuadro Nº 73. Valor Actual Neto

Fuente: Elaboración Propia

6.2.2.5. Tasa Interna de Retorno

A continuación se procede a aplicar la fórmula de la Tasa Interna de Retorno y reemplazar los resultados del Beneficio, Costo de Inversión y Costo de Operación; lo cual nos permitirá saber el tiempo en el que se podría recuperar la inversión que se realice.

$$\mathbf{T\ I\ R\ =}\ \frac{\text{Inversión total}}{\text{Promedio Beneficio Neto}}$$

Donde: Promedio Beneficio Neto = Beneficio – Costo Operación

$$\mathbf{TIR\ =}\ \frac{95{,}305.00}{709{,}900.00 - 4000.00}$$

TIR = 0.14 meses.

- Por lo tanto el tiempo en el que se podrá recuperar la inversión será aproximadamente **1 mes y 20 días**.

Meses	**Días**
1,68	20,4

Cuadro Nº 74. Resultado del Tasa Interna de Retorno

Fuente: Elaboración Propia

CAPITULO VII

CONCLUSIONES

- ✓ Aplicando encuestas, entrevistas y checklist, se pudo determinar cuál es la situación problemática de la Gerencia Regional de Salud, encontrándose como principales problemas el no mantener la dotación de personal suficiente en el área, así mismo no existe un proceso que permita mantener las habilidades y competencias del personal TI. Además de que no se tienen definidos esquemas de clasificación de incidentes y peticiones de servicio, los cuales permitan priorizarlos de manera que se les dé una eficaz y eficiente resolución. Tampoco se analiza, ni se informa sobre el rendimiento del área de CSI a la Gerencia de manera constante. Por otro lado, no se planifican ni estudian iniciativas de aseguramiento que permitan diagnosticar el riesgo e identificar los procesos críticos de TI.

- ✓ Utilizando el estándar COBIT 5, se determinó que de los 37 objetivos de control que tiene COBIT, 19 aplican a nuestro proyecto, los cuales se detallaron a lo largo de la auditoría.

- ✓ Se aplicó el estándar COBIT, mediante el cual se evaluó cada uno de los objetivos de control aplicados, de los cuales se encontraron 9 objetivos de control efectivos y 10 objetivos de control no efectivos.

- ✓ Utilizando la metodología PDCA, se pudo desarrollar el informe final de auditoría, en el cual se plantearon observaciones, y de cada observación se determinó los riesgos que generaría el no levantar dichas observaciones, asimismo se emitieron recomendaciones para poder subsanar las observaciones hechas en la auditoría aplicada. Llegándose a la conclusión de que la auditoría es Favorable con excepciones.

CAPITULO VIII

RECOMENDACIONES

- ✓ Se recomienda aplicar controles en lo que respecta a Recursos humanos, específicamente al personal TI, el cual debe ser suficiente y adecuado para poder cumplir con todas las actividades que se les asigne, además de mantener las habilidades y competencias de dicho personal.

- ✓ Es recomendable aplicar controles en lo referente a Incidentes y Peticiones de Servicio, el cual señala que se debe definir esquemas de clasificación tanto de incidentes como de peticiones, así mismo, estos se deben registrar y clasificar, ya que realizando estas actividades, se logrará priorizarlos de manera que se les dé una eficaz y eficiente resolución.

- ✓ Se sugiere supervisar las actividades de control constantemente en la empresa, ya que estas actividades solo se encuentran documentadas, más no se realizan dichas supervisiones, tales como las de verificar que todos los puertos de las computadoras de la empresa no estén activos, con el fin de que ninguna persona pueda grabar información por medio de algún dispositivo, ni tampoco adjuntar información de las computadoras mediante correos electrónicos.

- ✓ Es recomendable aplicar controles, referente al proceso de control de cambios y de gestión en la supervisión del área de CSI, ya que uno de los objetivos de control de COBIT 5, señala que se debe establecer un enfoque en la supervisión, lo cual actualmente no se realiza en el área.

- ✓ Se sugiere evaluar el rendimiento del área del CSI, mediante autoevaluaciones periódicas en el área e informar los resultados a la Gerencia, ya que si bien se le informa sobre los avances del área, se hace de manera general y solo una vez al año.

- ✓ Se recomienda planificar y estudiar iniciativas de aseguramiento que permitan diagnosticar el riesgo e identificar los procesos críticos de TI en el Centro de Sistemas de Información de la GERESA.

- ✓ Se recomienda realizar auditorías periódicamente a la GERESA, las cuales permitan identificar las falencias que se tienen en la empresa y las medidas correctivas que se pueden tomar para corregirlas.
- ✓ Se sugiere actualizar el Plan de Contingencia, para lo cual se debe establecer un nuevo procedimiento para su creación, definición y realización de pruebas de funcionamiento, etc.

CAPITULO IX

REFERENCIAS BIBLIOGRÁFICAS

- Misión, Visión y Objetivos - Portal GERESA - Lambayeque, 2016. http://www.regionlambayeque.gob.pe/
- Misión, Visión y Objetivo - Diagnostico Situacional CSI - GERESA Lambayeque, 2013.
- Organigrama GERESA - Portal GERESA - Lambayeque, 2016.- http://www.regionlambayeque.gob.pe/
- Walter Andrew Shewhart,- PDCA- 2016. https://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming
- Walter Andrew Shewhart - PDCA DEMING -2014 https://prezi.com/i962uslrmsrr/pdca-deming/
- Auditoría de la Gestión de Seguridad en la Red de Datos de Swissotel Basada en COBIT - Juan Herrera, Escuela Politécnica Nacional, Qutio-Ecuador, 2006.
- Diagnóstico para la Implantación de COBIT 4.1 en una Empresa de Producción- Bertha Alice Naranjo Sánchez - Universidad Politécnica Salesiana Ecuador - Quito-Ecuador, 2012.
- Adaptación de Modelo de Gobierno y Gestión para la empresa VirtIT Expert Basado en COBIT 5- Marcela María Escobar Urueña - Universidad Peruana de Ciencias Aplicadas - Lima - Perú, 2015.
- Diseño de un modelo de gobierno de TI con enfoque de seguridad de información para empresas prestadoras de servicios de salud bajo la óptica de cobit 5.0 - Diana Estefanía Lepage Hoces, Pontificia Universidad Católica, Lima - Perú, 2014.
- Auditoría Informática de los Sistemas Informáticos de la Unidad de Informática de la Escuela de Postgrado de la Universidad Nacional "Pedro Ruiz Gallo - Víctor Carlos Quiñones Rado, Universidad Nacional Pedro Ruiz Gallo, Lambayeque-Perú, 2008.
- Auditoría de Sistemas Informáticos - Juan Carlos Vera Callacná - Universidad Católica Santo Toribio de Mogrovejo, Chiclayo-Perú, 2006.
- La Auditoría en La Informática - Lorena Carmina Moreno Jiménez- Universidad de Colima - Colima 2013.
- Auditoría Informática - Carol Rivas Mendoza – 2012.

- Auditoría de los Sistemas de Información- Rafael Bernal Montañés, Oscar Coltell Simón. Servicio de Publicaciones de la Universidad Politécnica de Valencia - Valencia, 2012.
- Guía de Auditoría Informática - José Echenique García - McGrawHill, México, 2013
- Tecnología de la Información- José Miguel Roca Chillida, 2013.
- Generalidades de la Auditoría- Roberto Gómez López -2009
- Auditoría - Mario Bernabe Ron Egas, 2010.
- ISACA COBIT 5 – Cambios de la nueva versión, 2011. http://www.isaca.org/Groups/Professional-English/cobit-5-use-it-effectively/Pages/ViewDiscussion.aspx?PostID=18
- ISACA. COBIT 5 – 2015. http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx
- ISACA - COBIT 5-2013.
- Capacitación Empresarial ¿Gasto o Inversión? - Louis Harris, 2012. https://crecerh.wordpress.com/

ANEXOS

ANEXO Nº 1. Encuesta Aplicada al Coordinador del Área del CSI

El objetivo de la siguiente encuesta es obtener información para determinar el nivel de aplicación de los dominios COBIT en el Centro de Sistemas de Información de la Gerencia Regional de Salud – Lambayeque.

Evaluar, Orientar y Supervisar (EDM)

1. La administración y dirección de todos los recursos de TI están alineados con la estrategia de negocio.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

2. La gerencia asume la responsabilidad de comunicar las políticas de control interno a la unidad de TI.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

3. La empresa define requerimientos, procedimientos y/o políticas claras de calidad de las TI.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

4. En la empresa existe un procedimiento para evaluar y administrar los riesgos de TI.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

5. En la empresa existen procedimientos para administrar los proyectos TI.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

Alinear, Planificar y Organizar (APO)

1. Existe un presupuesto definido para la inversión en TI.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

2. La empresa identifica y controla los costos/beneficios de la inversión realizada en TI.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

3. Existe un proceso de contratar, mantener y motivar los recursos humanos de TI, para la creación y entrega de servicios de TI al negocio.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

4. Existen actividades que permiten revisar la calidad de los proyectos y operaciones TI.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

5. Existe un monitoreo y control por parte de un equipo especializado para que los activos de TI no se deterioren, dañen o tengan un mal uso por parte de los usuarios

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

6. Cuando hay una pérdida de productividad en los procesos, las operaciones de soporte de TI son efectivas, eficientes y flexibles para cumplir con las necesidades de niveles de servicio.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

Construir, Adquirir e Implementar (BAI)

1. Existen iniciativas que permiten identificar nuevas necesidades de aplicaciones tecnológicas, para facilitar el logro de los objetivos del negocio.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

2. La empresa cuenta con un proceso de adquisición, desarrollo, configuración y mantenimiento de software aplicativo.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

3. Se cuenta con pruebas que permiten evaluar la efectividad y eficiencia de la integración de las aplicaciones.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

4. Los procesos de seguridad de las TI están integrados a lo largo de toda la organización.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

5. Existe un proceso definido de adquisición de:

Hardware: Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

Software: Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

Servicios TI: Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

6. Existe preocupación de que las adquisiciones cumplan con los requerimientos del negocio.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

7. Existen normas de pruebas durante la instalación y antes de dejar en explotación las soluciones y cambios de TI.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

Entrega, Servicio y Dar Soporte (DSS)

1. En caso de interrupción de un servicio TI, no hay problemas porque se dispone de un Plan de Contingencia.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

2. Los procesos de seguridad (respaldos) de las TI están integrados a lo largo de toda la organización.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

3. Los procesos de seguridad (respaldos) se realizan periódica y regularmente en la empresa.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

4. Se dispone de información desglosada de costos respecto a los distintos elementos que intervienen en la unidad TI.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

5. El uso efectivo y eficiente de las soluciones y aplicaciones tecnológicas por parte de los usuarios, se logra mediante una capacitación adecuada

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

6. Se dispone de un procedimiento para responder de manera oportuna y efectiva a las consultas y problemas de los usuarios

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

7. Se dispone de un procedimiento para identificar problemas, sus causas y soluciones que estén asociadas a las TI.

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

8. Las necesidades y requerimientos futuros de información se exploran de manera proactiva para satisfacer las necesidades de los usuarios

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

9. La información del negocio que generan las TI están disponibles en cualquier momento en que se requiera

   Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

Supervisar, Evaluar y Valorar (MEA)

1. Los niveles de satisfacción respecto del cumplimiento de los niveles de servicio de las TI son monitoreados y administrados de manera continua.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

2. Las revisiones actuales y proyecciones sobre la capacidad y desempeño de los recursos TI están sincronizados con las proyecciones de demanda del negocio.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

3. Se monitorea y evalúa el desempeño de las TI.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

4. Se controla si las TI satisfacen los requerimientos del negocio.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

5. Se realiza un control interno en la unidad de TI, para realizar mejoras o correcciones en los sistemas.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

6. La empresa se preocupa de que los sistemas TI cumplan las leyes o regulaciones vigentes o pertinentes (leyes del entorno del negocio).

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

7. Las soluciones informáticas están alineadas con la estrategia de negocio de la empresa.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

8. La estructura de TI está organizada de modo tal que permite responder a una administración efectiva y eficiente del negocio.

Siempre ☐ Casi siempre ☐ Algunas Veces ☐ Nunca ☐

ANEXO 2: Encuesta Aplicada A Los Trabajadores De Geresa

El objetivo de esta encuesta es hallar el grado de satisfacción del personal de la Gerencia Regional de Salud Lambayeque, respecto al servicio brindado por el área del Centro de Sistemas de Información.

1.-Como califica usted el servicio brindado por parte del área del CSI?

Excelente ( ) Bueno ( ) Regular ( ) Malo ( )

2.- ¿Está usted de acuerdo con la atención brindada por parte se servicio técnico?

SI ( ) No ( )

3.- ¿Con qué periodo se les da mantenimiento a las computadoras de su área?

Mensualmente ( ) Semestralmente ( ) Anualmente ( )

4.- ¿Considera usted que el servicio de internet es importante al momento de laborar?

SI ( ) No ( )

5.- ¿Cómo califica usted el servicio de internet?

Excelente ( ) Bueno ( ) Regular ( ) Malo ( )

6.- ¿Tiene usted restricciones para ingresar a algún sitio web?

SI ( ) No ( )

7.- ¿Sufre usted de constantes caídas en el servicio de internet?

SI ( ) No ( )

8.- ¿Cuentan con manuales de usuario para los sistemas informáticos que maneja?

SI ( ) No ( )

9.- ¿Usted sabe del contenido de estos manuales?

SI ( ) No ( )

10.- ¿Cuál es el mayor problema que tiene al realizar su trabajo?

_____

_____

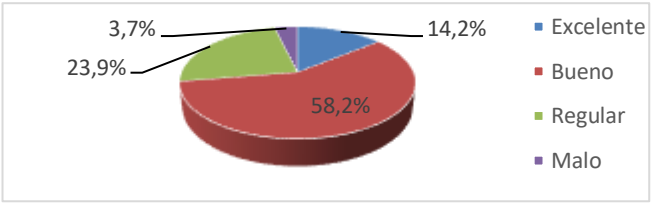
_____

ENCUESTA APLICADA A LOS TRABAJADORES DE GERESA

Tabla Nº 01. El servicio brindado por parte del CSI

	n	porcentaje
Excelente	19	14,2%
Bueno	78	58,2%
Regular	32	23,9%
Malo	5	3,7%
Total	134	100,0%

Gráfica Nº 01. Servicio El brindado por parte del CSI

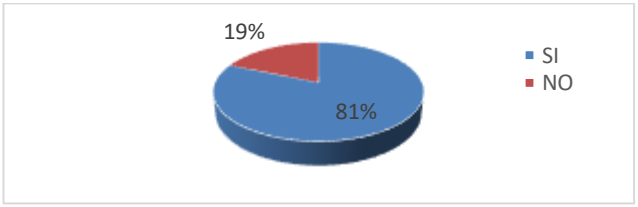


Fuente: GERESA-Lambayeque

Tabla Nº 02. La atención brindada por parte se servicio técnico

	n	porcentaje
SI	109	81%
NO	25	19%
	134	100%

Gráfico Nº 02. Atención El brindado por parte del CSI

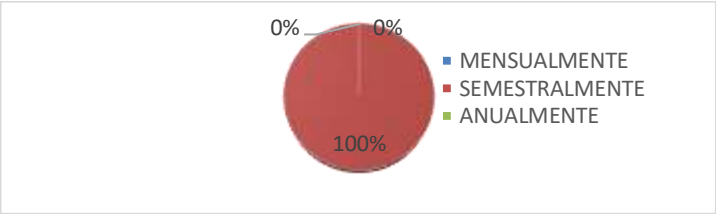


Fuente: GERESA-Lambayeque

Tabla Nº 03. Período se les da mantenimiento a las computadoras de su área

	n	porcentaje
MENSUALMENTE	0	0%
SEMESTRALMENTE	134	100%
ANUALMENTE	0	0%
Total	134	100%

Gráfica Nº 03. Período de mantenimiento a las computadoras de su área

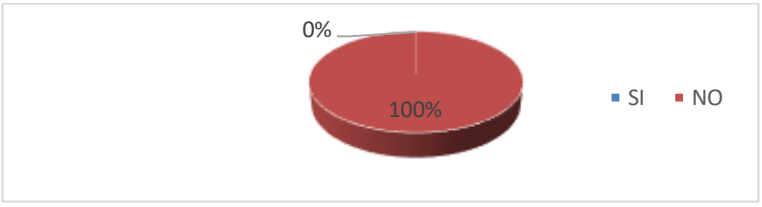


Fuente: GERESA-Lambayeque

Tabla Nº 04. El servicio de internet es importante al momento de laborar

	n	porcentaje
SI	0	0%
NO	134	100%
Total	134	100%

Gráfico Nº 04. El servicio de internet es importante al momento de laborar

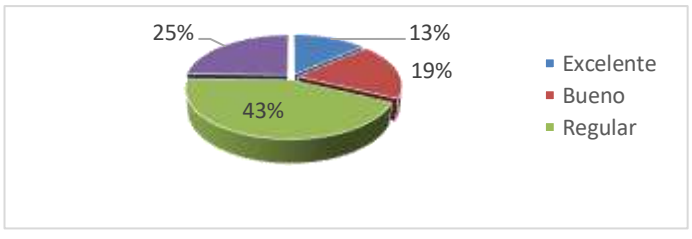


Fuente: GERESA-Lambayeque

Tabla Nº 05. Calificación del servicio de internet

	n	porcentaje
Excelente	18	13%
Bueno	25	19%
Regular	58	43%
Malo	33	25%
Total	134	100%

Gráfico Nº 05. Calificación del servicio de internet

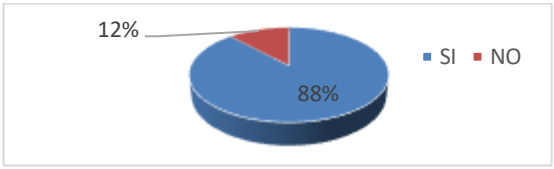


Fuente: GERESA-Lambayeque

Tabla Nº 06. Restricciones para ingresar a alguna sitio web

	n	porcentaje
SI	118	88%
NO	16	12%
Total	134	100%

Gráfico Nº 06. Restricciones para ingresar a alguna sitio web

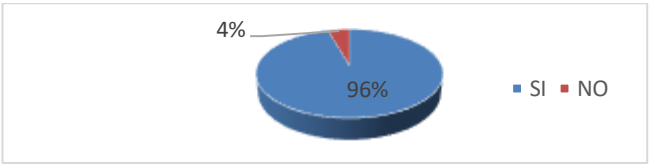


Fuente: GERESA-Lambayeque

Tabla Nº 07. Constantes caídas en el servicio de internet

	n	porcentaje
SI	128	96%
NO	6	4%
Total	134	100%

Gráfico Nº 07. Constantes caídas en el servicio de internet

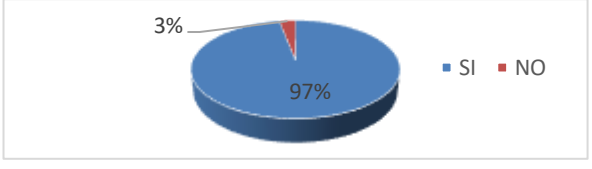


Fuente: GERESA-Lambayeque

Tabla Nº 08. Manual para cada sistema informático que se maneja

	n	porcentaje
SI	130	97%
NO	4	3%
Total	134	100%

Gráfico Nº 08. Manual para cada sistema informático que se maneja

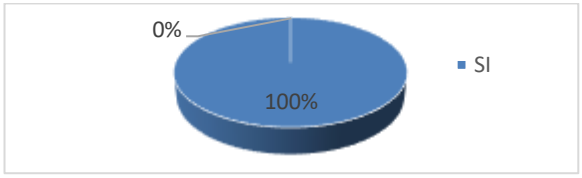


Fuente: Geresa-Lambayeque

Tabla Nº 09. Sabe del contenido de estos manuales

	n	porcentaje
SI	134	100%
NO	0	0%
Total	134	100%

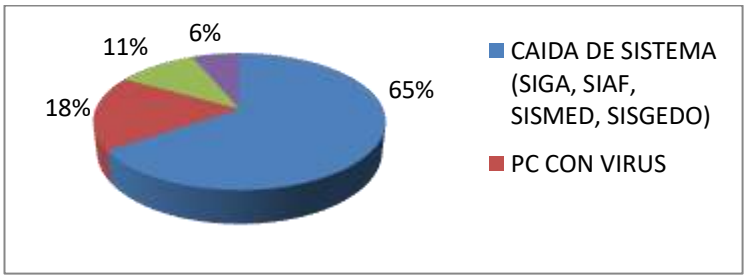
Gráfico Nº 09. Sabe del contenido de estos manuales



Fuente: GERESA-Lambayeque

Tabla Nº10. Mayor problema que tiene al realizar su trabajo

	n	porcentaje
CAIDA DE SISTEMA (SIGA, SIAF, SISMED, SISGEDO)	155	65%
PC CON VIRUS	42	18%
PROBLEMAS CON LA SEÑAL DE INTERNET	25	11%
CONTRASEÑA PARA INSTALAR PROGRAMAS	15	6%
Total	237	100%



Fuente: GERESA-Lambayeque

ANEXO Nº3.- Checklist Aplicada al Coordinador del CSI

PREGUNTA	SI	NO	No Aplica	OBSERVACIONES
➢ **APO07 DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)**				
APO07.01 Mantener la dotación de personal suficiente y adecuado				
1. ¿Se capacita al personal constantemente?		X		
2.- ¿Hay personal suficiente para las labores que se requieren?		X		
3.- ¿Existen procesos de contratación de personal de TI?		X		
DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos.				
1.- ¿Se documenta las actividades de control de los procesos de negocio?		X		
2.- ¿Se supervisa las actividades de control que ayuden a identificar oportunidades de mejora?		X		
DSS06.06: Asegurar los activos de información.				
1.- ¿Se aplican las políticas y los procedimientos para proteger los activos de información?	X			
2.- ¿Existen procesos, herramientas y técnicas que verifiquen el cumplimiento de las políticas y procedimientos?	X			
3.- ¿Se informa a Gerencia de la empresa sobre las violaciones y desviaciones de las políticas y procedimientos?	X			
➢ **DOMINIO: SUPERVISAR, EVALUAR Y VALORAR (MEA)**				
MEA01.01: Establecer un enfoque de la supervisión.				
1.- ¿Se comunica a todo el personal del CSI sobre los objetivos y requisitos empresariales?		X		
2.- ¿Existe un proceso de control de cambios y de gestión en la supervisión y la presentación de informes?		X		

3.- ¿Se priorizan y reservan recursos para la supervisión?		X		
MEA01.04: Analizar e informar sobre el rendimiento.				
1.- ¿Se recomiendan cambios a los objetivos y métricas cuando se es procedente?		X		
2.- ¿Se distribuyen informes sobre el rendimiento a Gerencia de la empresa?		X		
3.- ¿Se documentan las incidencias presentadas si el problema vuelve a aparecer?		X		
MEA01.05: Asegurar la implantación de medidas correctivas.				
1.- ¿Se revisan las alternativas y recomendaciones del Coordinador del CSI para tratar los problemas y desviaciones más relevantes?	X			
2.- ¿Se informa de los resultados a la Gerencia de la empresa?	X			
MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio.				
1.- ¿Se prioriza el riesgo de acuerdo con los objetivos de la empresa?	X			
2.- ¿La información generada del control interno opera de forma efectiva?	X			
MEA02.03 Realizar autoevaluaciones de control.				
1.- ¿Se toman en cuenta criterios de evaluación para realizar autoevaluaciones de control?		X		
2.- ¿Se realizan autoevaluaciones periódicas, considerando la efectividad y eficiencia de la supervisión?		X		
3.- ¿Se comparan y comunican los resultados a la Gerencia de las autoevaluaciones con estándares?		X		
MEA02.06: Planificar iniciativas de aseguramiento.				
1.- ¿Se realiza una evaluación para diagnosticar el riesgo e identificar los procesos críticos de TI?		X		
MEA02.07: Estudiar las iniciativas de aseguramiento.				
1.- ¿Se define el alcance actual de las iniciativas de aseguramiento, mediante la identificación de los objetivos de la empresa y de TI?		x		

2.- ¿Se evalúa la información de los procesos bajo revisión para identificar los controles y hallazgos reales?		x		

ANEXO Nº4.- Checklist Aplicada al Jefe de Gestión y Desarrollo de Potencial Humano (RR.HH)

PREGUNTA	SI	NO	No Aplica	OBSERVACIONES
➢ **APO07 DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)**				
APO07.01 Mantener la dotación de personal suficiente y adecuado				
1.- ¿Se cumplen con las políticas y procedimientos para contratar personal en la empresa?		X		
2.- ¿Se evalúa las necesidades de personal regularmente?		X		
APO07.03 Mantener las habilidades y competencias de Personal.				
1. ¿El personal cuenta con habilidades y competencias para desarrollar eficientemente sus labores?		X		
2.- ¿Existen procesos que ayuden a identificar las diferencias entre las habilidades necesarias y habilidades disponibles del personal?		X		
3.- ¿Se lleva a cabo revisiones de manera periódica para evaluar la evolución de las habilidades y competencias del personal.				
APO07.04 Evaluar el desempeño laboral de los empleados.				
1.- ¿Se consideran objetivos funcionales de la empresa establecer las metas individuales?	X			
2.- ¿Se recopila los resultados de las evaluaciones de desempeño?	X			
3.- ¿Se implementa y comunica un proceso disciplinario?	X			

6.- ¿En el proceso de evaluación, se dan instrucciones en el uso y almacenamiento de información personal?	X			
APO07.06 Gestionar el personal contratado.				
1.- ¿Se implementan políticas y procedimientos que describan el trabajo que puede ser realizado de acuerdo con la política de contratación de TI de la empresa y el marco de control de TI?	X			
2. ¿Se requiere de contratistas para la selección y contratación de personal en la empresa?	X			
3.- ¿Se proporciona a los contratistas una definición clara de sus funciones y responsabilidades?	X			
4.- ¿Se lleva a cabo revisiones de manera periódicas para asegurar que el personal contratado firme y acepte todos los acuerdos necesarios?	X			

ANEXO Nº 5.-Checklist Aplicada al Responsable de Soporte Técnico-CSI

PREGUNTA	SI	NO	No Aplica	OBSERVACIONES
➢ **DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE (DSS)**				
DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.				
1.- ¿Se tienen definido esquemas de clasificación y priorización de incidentes y peticiones de servicio y criterios para el registro de problemas?		X		
2.- ¿Se tienen definido modelos de incidentes para errores conocidos?		X		
3.- ¿Existen modelos de peticiones de servicio según el tipo de petición de servicio correspondiente?		X		
4.- ¿Se tienen definido fuentes de conocimiento de incidentes y peticiones?		X		

DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes.				
1.- ¿Se registran toda la información relevante de los incidentes y peticiones de servicio?		X		
2.- ¿Se tienen identificados el tipo y categoría de incidentes y peticiones de servicios?		X		
DSS02.04 Investigar, diagnosticar y localizar incidentes.				
1.- ¿Se puede determinar las causas más probables de los incidentes?	X			
2.- ¿Se registran todos los problemas que se presentan?	X			
3.- ¿Se asignan especialistas para resolver incidentes cuando se es necesario?	X			
DSS05.02: **Gestionar la seguridad de la red y las conexiones.**				
1.- ¿Se restringe el acceso a la información y a la red de la empresa?	X			
2.- ¿Se aplican protocoles de seguridad aprobados a las conexiones de red?	X			
3.- ¿Se configura los equipos de red de forma segura?	X			
4.- ¿Hay mecanismos establecidos de confianza para dar soporte a la transmisión y recepción segura de información?	X			
5.- ¿Se realizan pruebas para una adecuada protección de la red y del sistema?	X			
DSS05.03: Gestionar la seguridad de los puestos de usuario final.				
1.- ¿Se configura los sistemas operativos de forma segura?	X			
2.- ¿Se gestiona la configuración de la red de forma segura?	X			
3.- ¿Se realizan mecanismos de bloqueo en los dispositivos?	X			

4.- ¿Se protege la integridad del sistema?	X			
5.- ¿Se provee de protección física a los dispositivos de usuario final?	X			

ANEXO Nº 6. Checklist Aplicada al Responsable de Control Institucional.

PREGUNTA	SI	NO	No Aplica	OBSERVACIONES
MEA02.01. Supervisar el Control Interno				
1.- ¿Se realizan actividades de evaluación y supervisión del control interno?	X			
2.- ¿Existen un sistema de control interno en la GERESA?	X			
3.- ¿Explique el sistema del control interno que se maneja en GERESA?	X			
4.- ¿Existen procesos que identifiquen los límites del sistema de control interno?	X			
5.- ¿Las actividades de control están operativas?	X			
6.- ¿Las excepciones son comunicadas puntualmente?	X			
7.- ¿El sistema de control considera los cambios y riesgos de TI?	X			

ANEXO Nº 7. Acta de conformidad de Entrevistas y Checklist aplicados

Proyecto: Auditoría Informática bajo el estándar COBIT en el Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque - 2015

Fecha: 04/01/2016

ACTA

1. Información General

Nombre del Proyecto:
Auditoría Informática bajo el estándar COBIT en el Centro de Sistemas de Información de la Gerencia Regional de Salud Lambayeque – 2015

Elaborado por:
Shirley Carrillo / Kely Suclupe

Asistentes:	Cargo	Asistió
Bch. Shirley Lizeth Carrillo Prada	Jefe de Proyecto	Si
Bch. Kely Karina Suclupe Tejada	Jefe de Proyecto	Si
Ing. Yoverth Torres Monje	Coordinador del Centro de Sistema de Información	Si
Ing. Willy Antonio Burga Alvarado	Soporte Técnico - CSI	Si
Tco. Ricardo Jaime Ortega Lara	Jefatura de Gestión y Desarrollo del Potencial Humano	Si
CPC. Soledad Cotrina Bustamante	Oficina de Control Institucional	Si

2. Temas tratados

En la entrevista aplicada el día 04//01/2016, estuvieron presentes las personas antes mencionadas, en dicha entrevista se hicieron preguntas, las cuales fueron hechas mediante diversos **checklist** a cada uno de los encargados de las áreas requeridas. Respuestas que se detallaron verbalmente y las cuales se explicaran en los cuadros de evaluación y observaciones que se realizaran en el proyecto.

3. Firmas

En señal de conformidad del contenido de la presente acta, los asistentes proceden a firmarla en señal de conformidad.

Bch. Shirley Carrillo
Jefe de Proyecto

Bch. Kely Suclupe
Jefe de Proyecto

Ing. Yoverth Torres Monje
Coordinador de CSI

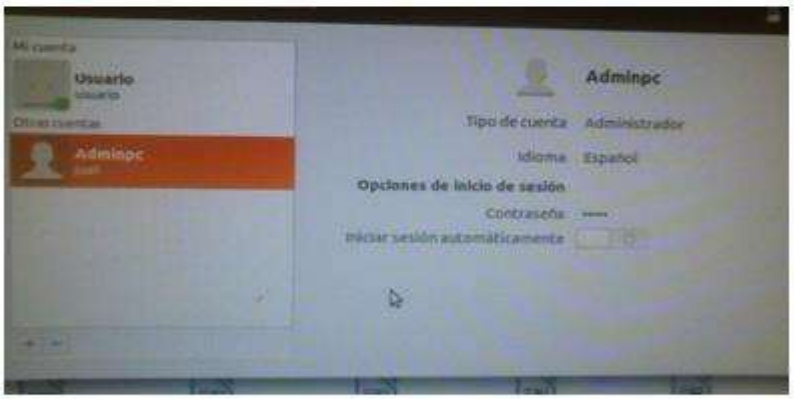
Ing. Willy Antonio Burga Alvarado
Soporte Técnico - CSI

Tco. Ricardo Jaime Ortega Lara
Jefatura de Gestión y Desarrollo del Potencial Humano

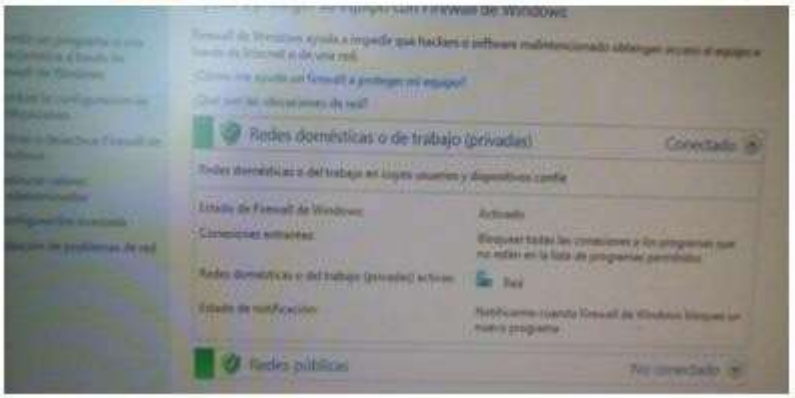
CPC. Soledad Cotrina Bustamante
Oficina de Control Institucional

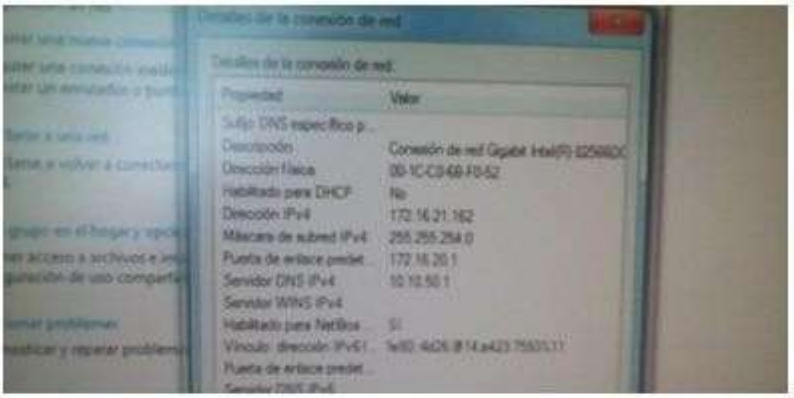
ANEXO Nº 8.- Configuración de los Equipos

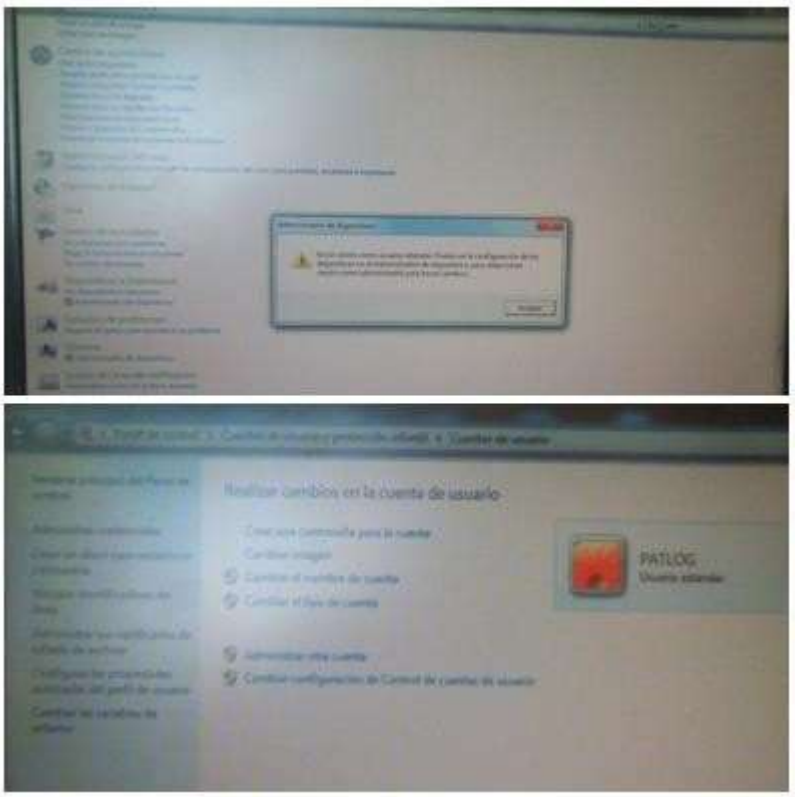
- ✓ **Área de Asesoría Jurídica**



- ✓ **Área de Patrimonio**







ANEXO Nº 9. Plan de Contingencia

GOBIERNO REGIONAL DE LAMBAYEQUE
GERENCIA REGIONAL DE SALUD
CHICLAYO

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

INFORME N°. 000006 -2014-GR.LAMB/GERESA.L--CSI-WBURGA

A : **Ing. Yoverth Torres Monje**
Coordinador del Centro de Sistemas de Información

ASUNTO : PLAN DE CONTINGENCIA 2014

FECHA : Chiclayo, 23 de Julio de 2014

Por medio del presente, me dirijo a Usted para saludarlo cordialmente y a la vez adjuntarle el Plan de Contingencia 2014 de la Gerencia Regional de Salud (GERESA), el mismo que entrará en vigencia a partir de su aprobación.

Sin otro particular, reitero a Ud. Los sentimientos de mi especial consideración y estima-

Atentamente,

GERENCIA REGIONAL DE SALUD LAMBAYEQUE V° B° SOPORTE TECNICO CSI

Ing. Willy Antonio Burga Alvarado
Soporte Técnico - CSI

7. IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS

La siguiente tabla muestra las amenazas más comunes que podrían impactar la continuidad componentes de sistemas y su administración.

GOBIERNO REGIONAL DE LAMBAYEQUE
GERENCIA REGIONAL DE SALUD
CHICLAYO

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

Ocurrencia
1. Daño a la integridad del Personal.
2. Pérdida de comunicación.
3. Destrucción de información.
4. Falla del aire acondicionado.
5. Corte eléctrico / Interrupción.
6. Fuego.
7. Inundación / Daño por agua.
8. Terremotos.
9. Amenazas de bomba.
10. Sabotaje / Terrorismo.
11. Vandalismo.

8. ACCIONES DE RESPALDO

8.1 Generales

- ✓ Contar con un directorio de los responsables de los servicios obtenidos de terceros: suministro eléctrico, servicio de telefonía, servicio de Internet y servicios de mantenimiento.
- ✓ Contar con procedimiento de ejecución de respaldos de emergencia a la información de los servidores de la Red Informática.
- ✓ Colocar letreros que impidan el acceso al personal no autorizado al Área de los Servidores y Unidades de Distribución de Datos.

8.2 Documentos necesarios previos a las contingencias.

a. Contar con una copia del inventario del equipamiento existente.
b. Contar con un listado de configuraciones de los equipos de cómputo.

8.3 Medios y Materiales.

a. Contar con una copia de cada paquete de software.

GOBIERNO REGIONAL DE LAMBAYEQUE
GERENCIA REGIONAL DE SALUD
CHICLAYO

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

b. Programar las tareas de respaldo de la información de los servidores de la Red Informática en periodos que aseguren al máximo el estado de actualización de la misma, ante la eventualidad.
c. Contar con un set de herramientas (maletín o caja) que permitan los trabajos de cambio o instalación de componentes en los equipos del área de Servidores.

8.4 ACCIONES PREVENTIVAS A LA CONTINGENCIA RESPECTO A CADA OCURRENCIA.

8.4.1 Daño a la integridad del Personal

a. Programar al menos 1 simulacro al año.
b. Contar con extintores.
c. Conocer el manejo de los extintores.
d. Contar con botiquines de primeros auxilios.
e. Contar con capacitación de primeros auxilios.
f. Difundir las rutas de evacuación, así como los sitios de localización de extintores.
g. Establecer procedimientos de evacuación.
h. Contar con un directorio del personal y de familiares del personal que labora en el área.

8.4.2 Pérdida de comunicación

a. Contar con los planos de Red: Mapa de Distribución de Equipos y Troncales en los Switch's.
b. Establecer medios y servicios alternativos ante la pérdida de comunicación interna y externa; esto es, contar con equipos para la rápida habilitación de unidades de distribución de datos alternativas.

8.4.3 Destrucción de información

a. El lugar físico donde se encuentran resguardados los expedientes sea un lugar aislado y seguro.
b. Verificar el estado de los equipos de restauración de la información.
c. Contar con medios de respaldo de información.
d. Contar con una bitácora de respaldados de información de los Servidores.
e. Evitar el acceso a personal no autorizado al Área de servidores; es decir limitarlo solamente al administrador de los Servidores de la Red Informática.

GOBIERNO REGIONAL DE LAMBAYEQUE
GERENCIA REGIONAL DE SALUD
CHICLAYO

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

8.4.4 Falla del aire acondicionado

a. Efectuar el mantenimiento de los equipos de aire acondicionado con una frecuencia de 6 meses.

8.4.5 Corte eléctrico / Interrupción

a. Contar con diagrama UNIFILAR (Tipo de llaves, potencia, tipo de cable, identificación de circuitos, etc.).
b. Contar con cableado Eléctrico Estructurado.
c. Contar con mecanismos (dispositivos, tablero de control) de intercambio de alimentación de energía automática ante la caída de línea de del servicio público de energía.
d. Contar con un UPS en el Área de Servidores y Unidades de Distribución de Datos.
e. Contar con luces de emergencia.

8.4.6 Fuego

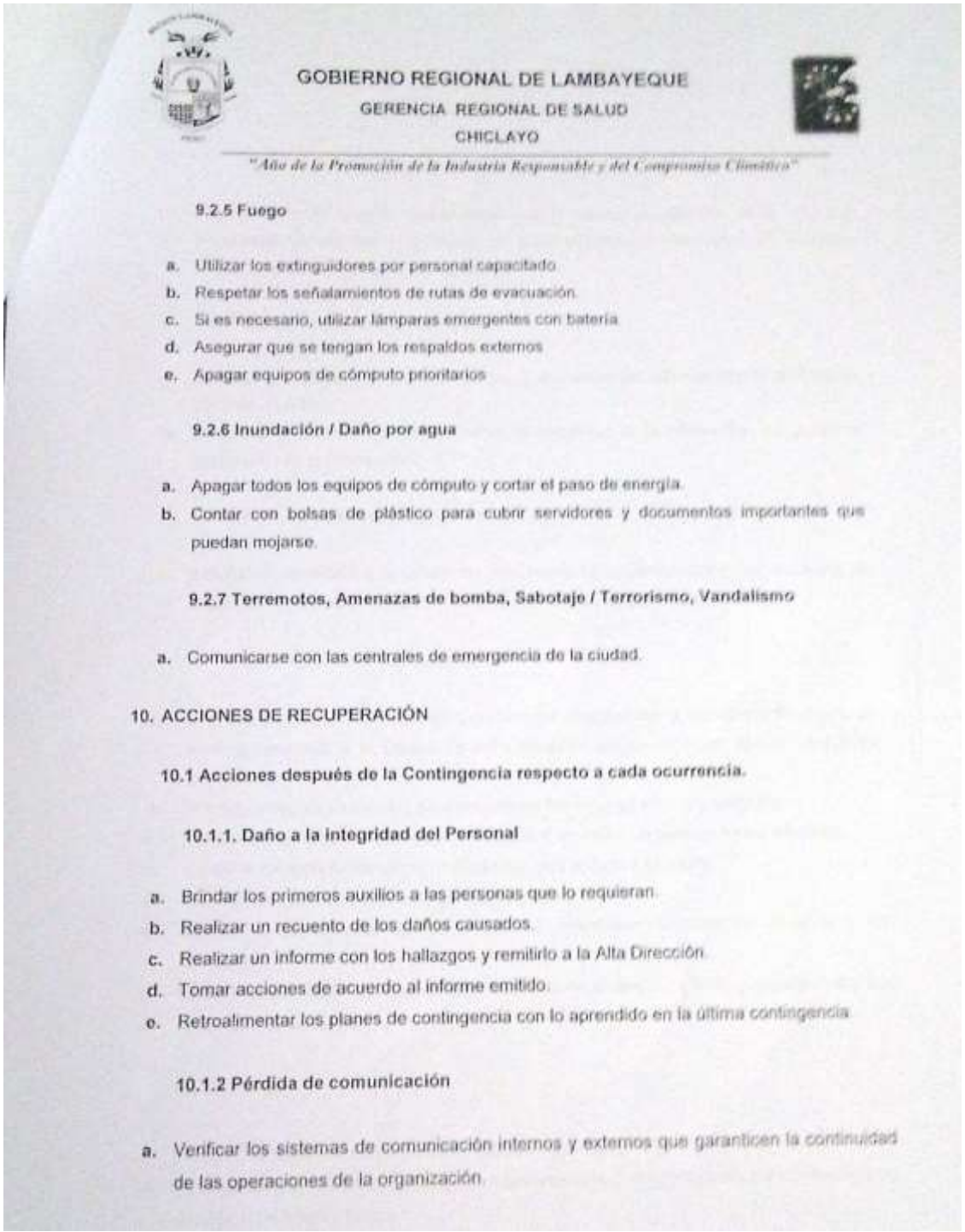
a. La Oficina de administración a través de la coordinación de Logística, deberá contar con diagramas de instalaciones de agua, electricidad y el coordinador del Centro de Sistemas de Información deberá tener una copia.
b. Contar con extinguidores cargados.
c. Contar con señalamientos de rutas de evacuación.
d. Contar con lámparas emergentes con batería.
e. Contar con sistemas de detección, alarmas de fuego y humo.

8.4.7 Inundación / Daño por agua

a. Colocar en lugares seguros el hardware, software y documentos importantes, evitando las zonas propensas a la inundación ya sea por fenómenos naturales como el Fenómeno del Niño o por problemas en los ductos de agua y alcantarillado.

8.4.8 Terremotos, Amenazas de bomba, Sabotaje / Terrorismo, Vandalismo

a. Contar con sistemas de emergencia (redundante) en una oficina remota, que se presume no será afectada por el evento o será afectada en un momento diferente.



GOBIERNO REGIONAL DE LAMBAYEQUE
GERENCIA REGIONAL DE SALUD
CHICLAYO

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

9.2.5 Fuego

a. Utilizar los extinguidores por personal capacitado.
b. Respetar los señalamientos de rutas de evacuación.
c. Si es necesario, utilizar lámparas emergentes con batería.
d. Asegurar que se tengan los respaldos externos.
e. Apagar equipos de cómputo prioritarios.

9.2.6 Inundación / Daño por agua

a. Apagar todos los equipos de cómputo y cortar el paso de energía.
b. Contar con bolsas de plástico para cubrir servidores y documentos importantes que puedan mojarse.

9.2.7 Terremotos, Amenazas de bomba, Sabotaje / Terrorismo, Vandalismo

a. Comunicarse con las centrales de emergencia de la ciudad.

10. ACCIONES DE RECUPERACIÓN

10.1 Acciones después de la Contingencia respecto a cada ocurrencia.

10.1.1. Daño a la integridad del Personal

a. Brindar los primeros auxilios a las personas que lo requieran.
b. Realizar un recuento de los daños causados.
c. Realizar un informe con los hallazgos y remitirlo a la Alta Dirección.
d. Tomar acciones de acuerdo al informe emitido.
e. Retroalimentar los planes de contingencia con lo aprendido en la última contingencia.

10.1.2 Pérdida de comunicación

a. Verificar los sistemas de comunicación internos y externos que garanticen la continuidad de las operaciones de la organización.

GOBIERNO REGIONAL DE LAMBAYEQUE
GERENCIA REGIONAL DE SALUD
CHICLAYO

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

b. Para el caso de Internet, comunicarse con la central de atención de la empresa proveedora del servicio y la Oficina de Racionalización e Informática del Gobierno Regional, quien nos proporciona un enlace.

10.1.3 Destrucción de información

a. Identificar y analizar los medios de acceso y el mecanismo utilizado para la destrucción de la información.
b. Establecer mecanismos y procedimiento de seguridad de la información que eviten la destrucción de la información.

10.1.4 Falla del aire acondicionado

a. Solicitar de inmediato a la Oficina de Administración en coordinación con la Oficina de Logística, el servicio de mantenimiento de los equipos de aire acondicionado.

10.1.5 Corte eléctrico / Interrupción

a. Si el tendido eléctrico fue afectado o dañado, se debe solicitar la reparación del mismo de manera inmediata a la Oficina de Administración en coordinación con la Oficina de Logística.
b. Brindar un tiempo prudencial, para restablecer los equipos activos y servicios.
c. Restablecer los equipos activos y servicios que se dieron de baja, en forma paulatina.
d. Validar el correcto funcionamiento de los equipos activos y servicios.
e. Identificar los posibles daños de los equipos activos.
f. Notificar a los usuarios afectados sobre el restablecimiento de los servicios y su condición.
g. Evaluar los daños de los equipos activos, planta de emergencia, UPS y canalizarlos a las áreas correspondientes.

10.1.6 Fuego

a. Verificar los sistemas de detección y alarmas de fuego y humo.
b. De considerarlo necesario, solicitar el mantenimiento o reemplazo de los dispositivos de detección de fuego y humo.

GOBIERNO REGIONAL DE LAMBAYEQUE

GERENCIA REGIONAL DE SALUD

CHICLAYO

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

10.1.7 Inundación / Daño por agua

a. Verificar los sistemas de abastecimiento y de drenaje de agua

10.1.8 Terremotos, Amenazas de bomba, Sabotaje / Terrorismo, Vandalismo

a. Verificar los sistemas de comunicación y alerta temprana ante eventos de estas categorías

11 RECOMENDACIONES FINALES.

a. Realizar un reporte de los daños, y documentar las actividades desarrolladas durante todo el proceso de la contingencia
b. Cuantificar y valorizar las pérdidas, que permitan tomar mejores decisiones respecto a la seguridad de la información y la continuidad de los servicios informáticos

ANEXO Nº 10.- Directiva Nº. -2015-GR.LAMB

GOBIERNO REGIONAL LAMBAYEQUE

DIRECTIVA No. -2015-GR.LAMB

(Aprobada con R.E.R. No. -2015-GERESA.LAMB/CSI)

ORDENAMIENTO Y ORGANIZACIÓN DE LAS REDES SOCIALES A CUMPLIRSE POR LAS GERENCIA DE RED DE SALUD, HOSPITALES, CENTROS Y PUESTOS DE SALUD DEL AMBITO DE LA GERENCIA REGIONAL DE SALUD LAMBAYEQUE.

1.0 FINALIDAD

Ordenar y organizar el Sistema de Redes Sociales – Página Web, Facebook y Fan Page de los diferentes establecimientos de salud del ámbito jurisdiccional de la Gerencia Regional de Salud Lambayeque: sedes administrativas de las Gerencias de Redes, Hospitales, Centros y Puestos de Salud de la provincia de Chiclayo, Lambayeque y Ferreñafe, así mantener actualizada la información en las herramientas informáticas de los órganos estructurados.

2.0 BASE LEGAL

2.1 Decreto Supremo No. 043-2003-PCM. Aprueba Texto Único Ordenado de la Ley No. 27806, Ley de Transparencia y Acceso a la Información.

2.2 Decreto Supremo No. 072-2003-PCM, aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información.

2.3 Ordenanza Regional No. 002-2003-GR.LAMB y modificatorias, aprueba Reglamento de Organización y Funciones del Gobierno Regional Lambayeque.

3.0 ALCANCE

Esta Directiva es de aplicación en todos los establecimientos de salud pertenecientes a la GERESA Lambayeque, con carácter de obligatorio y bajo responsabilidad deberán publicar (compartir) diariamente en sus respectivas redes sociales.

5.0 DISPOSICIONES GENERALES

5.1 Cuando en esta Directiva se menciona "Redes Sociales", se refiere a la información que oficialmente se publica en el Facebook: Gerencia Regional Lambayeque y Fan Page, twitter: Geresa Lambayeque.

5.2 Son dependencias de la Gerencia Regional de Salud Lambayeque: Sede Salud Región Lambayeque; sedes administrativas de las Gerencias de Redes, Hospitales, Centros y Puestos de Salud de la Provincia de Chiclayo, Lambayeque y Ferreñafe.

6.0 DISPOSICIONES ESPECÍFICAS

6.1 Los portales electrónicos de las dependencias de la Gerencia Regional de Salud Lambayeque son:

a) Gerencia Regional de Salud Lambayeque: http://salud.regionlambayeque.gob.pe

b) Hospital Las Mercedes: http://hospitallasmercedes.regionlambayeque.gob.pe

c) Hospital Belén: http://hospitalbelen.regionlambayeque.gob.pe

d) Hospital Regional de Lambayeque: http://hospitallambayeque.regionlambayeque.gob.pe

6.2 La actualización de los portales electrónicos será teniendo en cuenta los siguientes criterios:

a) El responsable de todas las informaciones que se publique en el Facebook será el Jefe de la oficina de

Imagen Institucional en la GERESA Lambayeque y en los Hospitales serán así los jefes de dicha área correspondientemente, en el caso de los establecimientos de salud serán los usuarios que el jefe designe.

6.3 El ingreso de datos que permitan mantener actualizado al portal institucional será necesariamente por intermedio del Sistema, teniendo como supervisor del ingreso o la actualización, a la persona asignada por el Jefe de la Unidad Orgánica correspondiente. En los casos que el Sistema no genere la información, el CSI o SGRI, según corresponda, por única vez apoyará con el direccionamiento del archivo hacia el componente del portal denominado TRANSPARENCIA PUBLICA, en los periodos subsiguientes será responsabilidad de la Unidad Orgánica que corresponda dicha actualización.

7.0 MECANICA OPERATIVA

7.1 El ingreso y actualización de información publicada en las redes sociales constituyen o está a cargo del denominado “Usuario Operativo”, quién es asignado por el Jefe de la respectiva unidad orgánica. Dicho usuario, formalmente, debe contar con una cuenta (usuario y contraseña) en el Sistema para el ingreso de la información que corresponda.

7.2 Entre el día uno y siete del mes siguiente al periodo vencido (mensual, trimestral o semestral), el Usuario Operativo debe “subir” la información que corresponda a su Unidad Orgánica. Si no hay necesidad de cambiarla o actualizarla, se debe mencionar en el mismo reporte la expresión INFORMACION VALIDA AL 30 DE xxxx DE 20xx; INFORMACION VALIDA AL xx TRIMESTRE DE 20xx; o, INFORMACION VALIDA AL xx SEMESTRE DE 20xx, según sea el caso.

8.0 RESPONSABILIDAD

8.1 Los Gerentes de Redes. Directores de Hospitales y jefes de los centros y puestos de salud, deberán designar a un responsable, que se encargue de manera permanente, de la labor del manejo de las redes sociales institucionales, en su respectivo establecimiento de salud.

8.2 El CSI, según sea el caso, brindarán la asistencia técnica a los usuarios de las redes sociales para facilitar el cumplimiento de sus funciones.

Chiclayo, Julio de 2015.

ANEXO 11.- Capacitaciones y Proformas

Capacitación en Gobierno y Gestión de las TI

CAPACITACIÓN EN GOBIERNO Y GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.

Contenido:

CODIGO	CURSO	DURACIÓN
PDTI-103	Fundamentos de Cobit para el Gobierno de TI	8 horas
PDTI-102	Planeamiento Estratégico de las TI	8 horas
PDTI-104	Fundamentos de TOGAF para la Arquitectura Empresarial de Información	8 horas
PDTI-108	Fundamentos de la Norma ISO 27001 Gestión de la Seguridad de la Información	8 horas
PDTI-105	Fundamentos de ITIL para la Gestión de Servicios de TI	8 horas
	TOTAL	40 horas

Objetivos:

- Proporcionar al participante una capacitación avanzada en los marcos de trabajo (modelos, marcos de referencia y metodologías) más utilizados en el Gobierno y Gestión de las Tecnologías de la Información.
- Facilitar el aprendizaje de dichos marcos de trabajo mediante una exposición teórica y práctica, de la mano con la experiencia real del docente en el uso de los mismos.
- Contribuir al incremento de la efectividad del participante en sus distintos centros laborales.

Dirigido a:

- Gerentes y Jefes de Sistemas y/o Informática.
- Gerentes y Jefes de Proyectos de TI.
- Profesionales expertos en la mejora de Procesos de Ingeniería de Software.

LUGAR

Lima

FECHA DE INICIO

16 Abril 2016

REQUISITOS PARA LA INSCRIPCIÓN (PERSONAS NATURALES)

Carta de compromiso de pago entregada
Copia de documento de identidad
Copia recibo de luz, agua o teléfono
Letra por el saldo del programa firmada

INVERSIÓN

S/ 900 al contado

CIERRE DE INSCRIPCIONES

13 Abril 2016

INSCRIPCIÓN ONLINE PARA PERSONAS NATURALES

Para continuar con la inscripción, haga clic en una de las formas de pago que a continuación se listan:
✔ Inscripción con depósito bancario (sólo pago al contado)
✔ Inscripción en línea con tarjeta de crédito (sólo pago al contado)

FICHA DE INSCRIPCIÓN PARA EMPRESAS

Ficha de Inscripción (PDF)

FICHA DE INSCRIPCIÓN PARA PERSONA NATURAL

Ficha de Inscripción (PDF)
Llenar los datos solicitados y enviar por fax al número 3173901 al área de: Servicio al Cliente - Informes e Inscripciones.

Proforma de Licencia Original
Windows 7 Professional (32 y 64 bits)

Proforma de Licencia de Antivirus
ESET NOD 32 para 3 PC

ANEXO Nº 12. INDECOPI

APESOFT
ASOCIACIÓN PERUANA DE SOFTWARE Y TECNOLOGÍAS

APESOFT Afiliación CITEsoftware Catálogo de soluciones Contáctanos

Indecopi ordena pago de más de S/. 200,000 a empresa por uso de software ilegal

Diario Gestión, 01 de junio del 2015

Indecopi realizó una inspección a Setech SAC en la que corroboró la existencia de **software de procedencia ilegal** instalado en las computadoras de la empresa.

El **Indecopi** continúa en su lucha contra la piratería en diversos ámbitos de la economía peruana, y esta vez impuso una multa a la empresa de call center Setech SAC por infracción a los derechos de autor por **uso de software** sin contar con las correspondientes licencias de uso.

La multa es por un monto de S/. 38,500 pero adicionalmente, el Indecopi ordenó el pago de US$ 54,296.54 (S/. 171,578.00) por concepto de derechos de autor devengados.

Indecopi realizó una inspección en la que corroboró la existencia de software de procedencia ilegal instalado en las computadoras de la empresa.

De esta manera, la Sala Especializada en Propiedad Intelectual del Tribunal de Defensa de la Competencia y de la Propiedad Intelectual emitió la resolución N° 2151-2014TPI, que multa a la empresa denunciada y confirma el pago de derechos de autor devengados por uso de software ilegal.

Cabe recordar que en el marco de la actual campaña de Software Legal, Indecopi está llevando a cabo inspecciones a aquellas empresas que no han declarado el inventario detallado del software instalado en sus equipos a través de la página web de **Indecopi**.

El software ilegal no cuenta con el soporte necesario, ni con las actualizaciones que protegen la información y la privacidad de los usuarios, exponiéndolos al robo y pérdida de información sensible.

Asimismo, la comercialización y/o utilización de software no licenciado constituye una violación a los derechos y un delito que puede ser sancionado hasta con 180 UIT de multa (S/.693,000), sin desmedro de ordenar pagos por el concepto de derechos de autor devengados en función del tiempo de utilización del software sin licencia.

Presidencia del Consejo de Ministros

23. ¿Qué tipo de sanciones puede imponer la Comisión dentro de un procedimiento de denuncia?

La Comisión puede imponer, conjunta o indistintamente, las siguientes sanciones:

a) Amonestación.
b) Multa de hasta 180 Unidades Impositivas Tributarias.
c) Reparación de las omisiones.
d) Cierre temporal hasta por noventa días del establecimiento.
e) Cierre definitivo del establecimiento.
f) Incautación o comiso definitivo.
g) Publicación de la resolución a costa del infractor.

24. ¿Cuáles son los criterios que tiene en cuenta la Comisión para la imposición de multas?

Actualmente la Comisión aplica como criterios para la imposición de multas los establecidos en el Decreto Supremo N° 006-2014-PCM[8], siendo los mismos los siguientes:

a) Beneficio ilícito: el cual en los casos de los programas de ordenador corresponde al monto de las remuneraciones devengadas reconocidas a favor del titular de derecho afectado.

b) Probabilidad de detección: en relación al mismo se toma en cuenta la información desarrollada en la versión actualizada del Documento de Trabajo N° 014-2012-GEE, desarrollado por la Gerencia de Estudios Económicos del Indecopi en el cual se ha señalado el siguiente cuadro:

ANEXO 13.- Pérdidas de Información

JUEVES 03 DE MARZO DEL 2016 | HORA 5:53 PM

RPP NOTICIAS — En Vivo ROTATIVA DEL AIRE

POLÍTICA | ACTUALIDAD | DEPORTES | ENTRETENIMIENTO | PERÚ | MUNDO | ECONOMÍA | VIDA | TECN

Fenómeno El Niño | Elecciones Perú 2016 | Anel Townsend | Encuestas | The Rolling Stones | Claudio

Lima 25/05/12 23:20

Cómo impedir el acceso ilegal y robo de información de nuestras web

Más de US$300 mil es el promedio de pérdidas totales anuales registradas por las pequeñas empresas por fallas de seguridad en el software y la acción de ciberdelincuentes.

La empresa Corero Network Security, informa que piratas cibernéticos conocidos como TheWikiBoat planean dejar fuera de servicio los sitios web de hasta 46 empresas mundiales durante al menos dos horas y difundir valiosos datos privados. Entre las empresas que podrían ser afectadas se encuentra IBM, HP y Apple.

Francisco Robledo Saavedra, Gerente de cuentas corporativas de Softline Perú, advierte que estas amenazas pueden quebrar el ritmo de la empresa y vale la pena tomar en serio este tipo de mensajes, para poder responder y estar preparados para cualquier ataque. "La falta adecuada de prevención en seguridad informática sigue siendo alarmante en nuestro país porque las empresas todavía no toman conciencia del valor de la protección del activo más importante: la información. Ésta en cuestión de segundos puede desaparecer por diferentes razones y hacer que la empresa quede fuera del mercado, es decir, del negocio", señala el ejecutivo.

Para evitar el robo de su información, las empresas deben tener en cuenta el filtro de datos salvar la integridad de su compañía.

ANEXO 14- Actualización del Plan de Contingencia

Fuente: Proyecto de Investigación elaborado por Diego Lobertti (Octubre 2015)

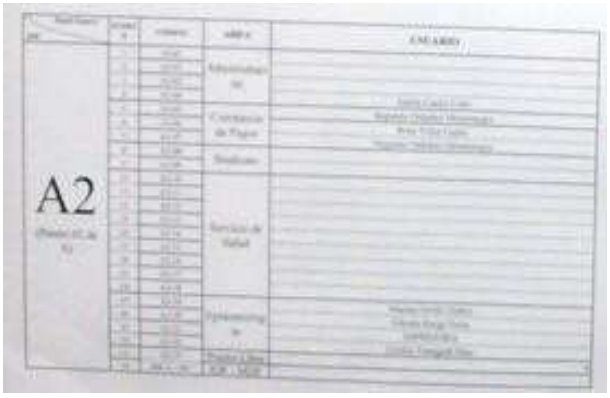
Costo del Plan de Contingencia:

- Gastos de mantenimiento de la red: Costo: $20.000.
- Generador eléctrico, detectores de humo, extinguidores: Costo: $80.000.
- Seguro contra incendio y robo Casa Central: Costo: $50.000 por mes.
- Backup: se encarga el Dpto. de Sistemas de Casa Central: Costo: $5000.
- Costo total por mes del Plan de Contingencia: Costo: $155.000.

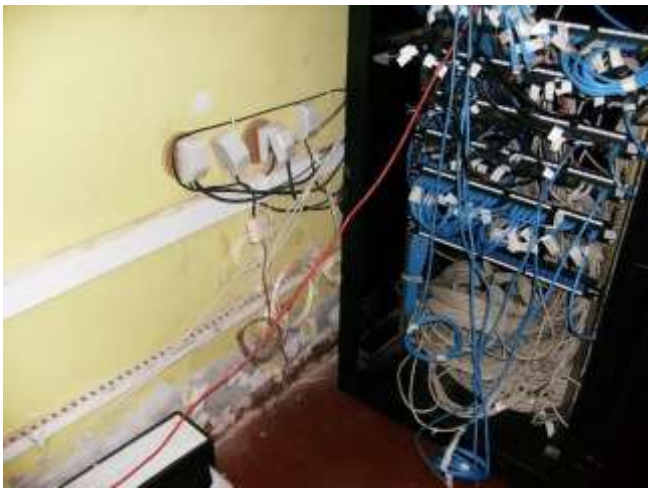
ANEXO Nº 15. Gerencia Regional de Salud Lambayeque y Autoridades

AREA DEL CENTRO DE SISTEMAS DE INFORMACIÓN
***INGENIEROS DEL CSI**

***SALA DE SERVIDORES DEL AREA DEL CSI**



IDF - A



IDF DISTRIBUIDOS POR GERESA