UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL ÁREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017"

TESIS PARA OPTAR POR EL TÍTULO PROFESIONAL DE

INGENIERO DE SISTEMAS

MARCOS ALEXIS BAUTISTA USHIÑAHUA

PUCALLPA - PERÚ

2020

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE INGENIERIA DE SISTEMAS E INGENIERIA CIVIL
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

INFORME DE ASESORÍA DE TESIS

1. TESISTA : Bach. Bautista Ushiñahua Marcos Alexis

2. TESIS : **AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL ÁREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**

3. Referencia : Resolución de comité de planeamiento FIS Y De IC-UNU

Que, el Tesista ha cumplido con ejecutar la tesis titulada: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL ÁREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL E UCAYALI: 2017**", de conformidad con el reglamento general de grados y títulos de la universidad nacional de Ucayali, así mismo, habiendo sido evaluada en la aplicación **URKUND** y estando dentro de lo permitido (9%) en 245, por lo que mi asesoría declara: aprobado y, encontrándose apta para ser presentada y evaluada por la comisión de grados y títulos de la facultad de ingeniería de sistemas e ingeniería civil de la universidad nacional de Ucayali.

Se expide el presente documento, a solicitud de los interesados para los fines consiguientes.

UNU, 23 julio del 2019

Ing. Mg. Cesar Augusto Agurto Cherre
Asesor de tesis

ii

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERIA DE SISTEMAS E INGENIERIA CIVIL

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

COMISION DE GRADOS Y TITULOS

ACTA DE EVALUACION DE SUSTENTACION DE TESIS N° 009-2020

GRADUANDO : **Bach. BAUTISTA USHIÑAHUA, MARCOS ALEXIS**

TEMA : **"AUDITORIA INFORMATICA CON METODOLOGIA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017"**

ASESOR : **ING. MG. CESAR AUGUSTO AGURTO CHERRE**

CRITERIOS	PUNTAJE			
	3	2	1	0
I- PRESENTACION				
* MOTIVACION		X		
* TONO DE VOZ		X		
* CALIDAD DE MATERIAL AUDIOVISUAL		X		
II- DESARROLLO DE CONTENIDO				
* SECUENCIA		X		
* DOMINIO DE VOZ		X		
* USO ADECUADO DE MATERIAL		X		
* VALIDEZ DE LOS HALLAZGOS			X	
III- ABSOLUCION DE PREGUNTAS				
* RESPONDE A LAS PREGUNTAS FORMULADAS POR EL JURADO		X		
IV- APORTE CIENTIFICO Y TECNOLOGICO				
* AL DESARROLLO DE LA COMUNIDAD			X	
* A LA PROFESION			X	

EVALUACION

- EXCELENCIA 26 A 30 PUNTOS
- UNANIMIDAD 21 A 25 PUNTOS
- MAYORIA 16 A 20 PUNTOS
- DESAPROBADO 15 A MENOS

CALIFICACION FINAL:

PUNTAJE : 17/30

CONCLUSIONES:

APROBADO POR : MAYORIA
DESAPROBADO POR :

JURADO EVALUADOR

- ING. MG. FREDDY ELAR FERRARI FERNANDEZ — Presidente
- ING. MSC. EUCLIDES PANDURO PADILLA — Miembro
- ING. MG. DIANA MARGARITA DIAZ ESTRADA — Miembro

SECRETARIO ACADÉMICO: ING. MSC. CLOTILDE RÍOS HIDALGO DE CERNA

PUCALLPA, 11 DE SEPTIEMBRE DEL 2020

"AUDITORÍA INFORMÀTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL ÁREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017"

Por:

Bach. Bautista Ushiñahua Marcos Alexis

Aprobado:

Ing. Mg. Freddy Elar Ferrari Fernández

Ing. M.Sc. Euclides Panduro Padilla

Ing. Mg. Diana Margarita Díaz Estrada

Asesor:

Ing. Mg. Cesar Augusto Agurto Cherre

iv

UNIVERSIDAD NACIONAL DE UCAYALI
VICERRECTORADO DE INVESTIGACION
DIRECCION GENERAL DE PRODUCCION INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACION

SISTEMA ANTIPLAGIO URKUND

N°038-2020

La **Dirección General de Producción Intelectual**, hace constar por la presente, que el Informe Final (Tesis), titulado:

AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL ÁREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI - 2017.

Cuyo autor (es)	:	**BAUTISTA USHIÑAHUA, MARCOS ALEXIS**
Facultad	:	INGENIERIA DE SISTEMAS Y DE INGENIERIA CIVIL
Escuela Profesional	:	INGENIERIA DE SISTEMAS.
Asesor	:	Mg. Agurto Cherre, Cesar

Después de realizado el análisis correspondiente en el Sistema Antiplagio URKUND, dicho documento presenta un **porcentaje de similitud de 09%**.

En tal sentido, de acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO URKUND, el cual indica que no se debe superar el 10%. Se declara, que el trabajo de investigación: SI Contiene un porcentaje aceptable de similitud, por lo que SI se aprueba su originalidad.

En señal de conformidad y verificación se FIRMA Y SELLA la presente constancia.

Fecha: 27/01/2020

Dra. DINA PARI QUISPE
Dirección General de Producción Intelectual

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, MARCOS ALEXIS BAUTISTA USHIÑAHUA

Autor de la TESIS titulada:
AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL ÁREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI : 2017

Sustentada el año: 2020
Con la asesoría de: Ing. Mg. CÉSAR AUGUSTO ACUÑA CHERIÑE
En la Facultad de: INGENIERÍA DE SISTEMAS Y INGENIERÍA CIVIL
Carrera Profesional de: INGENIERÍA DE SISTEMAS

Autorizo la publicación:

PARCIAL ☐ Significa que se publicará en el repositorio institucional solo La caratula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida marcar **si su tesis o documento presenta material patentable**, para ello deberá presentar el trámite de CATI y/o INDECOPI cuando se lo solicite la DGPI UNU.

TOTAL ☒ Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional.

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali **licencia no exclusiva** para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la **tesis es una creación de mi autoría** y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali y del Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

DEDICATORIA

A mi madre y a mi padre que estuvieron en todo momento apoyándome para poder concluir mis estudios superiores satisfactoriamente, brindándome muchos consejos positivos para el nivel que estaba llevando, también dedico este trabajo de investigación a mis docentes por brindarme sus conocimientos, como también consejos en la vida cotidiana.

AGRADECIMIENTO

A Dios, por brindarme la vida y sabiduría para concluir mis estudios satisfactoriamente sin ningún inconveniente.

Al Ing. MSc. Oscar Amado Ruiz Torres, Dr. Cesar Nilton Ayra Apac, Ing Mg. Cesar Augusto Agurto Cherre y al Prof. Glaydis Ushiñahua Fernández.

RESUMEN

El presente proyecto de investigación con título “Auditoría Informática con Metodología COBIT 4.5 para el Registro de Software y Hardware del Área de Patrimonio de la Universidad Nacional de Ucayali: 2017”, cuyo Objetivo general es Realizar una Auditoria Informática con metodología COBIT 4.5, para el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017 cuya población Para llevar a cabo esta investigación serán los 8 trabajadores del área de patrimonio de la universidad nacional de Ucayali así mismo la muestra probabilística va ser la misma que la población porque si la población es relativamente pequeña, de modo que puede ser abarcada en el tiempo y con los recursos del investigador. En base a ello la muestra es del mismo tamaño de la población n<=30 entonces decimos que es no probabilístico. De tal manera el nivel de investigación hará referencia al nivel Descriptivo correlacional, de corte transversal, según lo propuesto por Hernández, R; Fernández, C. & Batista, R. (2010), define que este nivel de investigación se encarga de relacionar dos o más variables dentro de un mismo contexto en un tiempo determinado, cuyo instrumento de datos que utilizamos es la encuesta. Como resultado final de nuestra investigación y con la información recopilada y analizada en todo el proceso, se proporcionan las conclusiones respectivas, concernientes a la elaboración de la auditoria informática en el área de patrimonio de la universidad nacional de Ucayali.

Palabras claves: Auditoría informática, Registro, software, hardware, metodología COBIT 4.5.

ABSTRACT

The present research project with the title Computer Audit with Cobit 4.5 Methodology for the Registry of Software and Hardware of the Heritage Area of the National University of Ucayali: 2017, whose general objective is to determine the level of relationship between the Computer Audit with COBIT 4.5 methodology , with the software and hardware registry of the heritage area of the National University of Ucayali, 2017 whose population To carry out this research will be the 8 workers of the heritage area of the national university of Ucayali as well as the probabilistic sample will be the same as the population because if the population is relatively small, so that it can be covered in time and with the resources of the researcher. Based on this, the sample is the same population size n <= 30 so we say it is not probabilistic. In this way the level of research will refer to the correlational descriptive level, cross-sectional, as proposed by Hernández, R; Fernández, C. & Batista, R. (2010), defines that this level of research is responsible for relating two or more variables within the same context in a given time, whose data instrument we use is the survey. As a final result of our research and with the information collected and analyzed throughout the process, the respective conclusions are provided, concerning the elaboration of the computer audit in the area of heritage of the national university of Ucayali.

Keywords: Computer audit, Registration, software, hardware, COBIT methodology 4.5.

INDICE DE CONTENIDO

DEDICATORIA vii
AGRADECIMIENTO viii
RESUMEN ix
ABSTRACT x
INDICE DE FIGURAS ixvi
INDICE DE TABLAS xvii
ÍNDICE DE CUADROS xviii
INTRODUCCIÓN xx
CAPITULO I: PLANTEAMIENTO DEL PROBLEMA 1
1 .1. ANTECEDENTES DEL PROBLEMA 1
1.1.1. Delimitaciones de la investigación 4
1 .2. FORMULACIÓN DEL PROBLEMA 7
1.2.1. General 8
1.2.2. Específicos 8
1.3. OBJETIVOS DE LA INVESTIGACIÓN 9
1.3.1. Objetivo general 9
1.3.2. Objetivos específicos 9
1.4. JUSTIFICACIÓN E IMPORTANCIA 10
1.4.1. Justificación teórica 11
1.4.2. Justificación práctica 12
1.4.3. Justificación metodológica 12
1.4.4. Importancia 13
1.5. HIPÓTESIS Y VARIABLES DE LA INVESTIGACIÓN 13
1.5.1. Hipótesis general 13
1.5.2. Hipótesis Específicas 13
1.6. VARIABLES (DEFINICIÓN CONCEPTUAL Y OPERACIONAL) 14
1.6.1. Definición conceptual de la variable 14
1.6.2. Definición operacional de la variable 15
1.6.3. Operalización de las variables 15
CAPITULO II: MARCO TEÓRICO 18
2.1. ANTECEDENTES DE LA INVESTIGACIÓN 18
2.1.1. Tesis Internacionales 18
2.1.2. Tesis nacionales 21
2.2. DEFINICIÓN DE TÉRMINOS BÁSICOS 26

2.2.1. Auditoria informática....26
2.2.2. COBIT 4.5....30
2.2.3. Registro de Software y Hardware....41
3.1. MÉTODO DE INVESTIGACIÓN....44
3.1.1. Tipo de investigación....44
3.1.3. Diseño de la investigación....45
3.1.4. Método de la investigación....45
3.2. POBLACIÓN Y MUESTRA....46
3.2.1. Población....46
3.2.1. Muestra....46
3.3. PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS....48
3.3.1. Técnicas de recolección de datos....48
3.3.2. Instrumentos de recolección de datos....49
3.5. PROCESAMIENTO PARA RECOLECCIÓN DE DATOS....50
3.6. TRATAMIENTO DE DATOS....51
CAPITULO IV: RESULTADOS....53
4.1. PROCESAMIENTO DE LA VARIABLE AUDITORIA NFORMÁTICA....53
4.1.1. Procesamiento de datos de la dimensión informe preliminar....54
4.1.2. Procesamiento de datos de la dimensión Análisis de la situación actual....55
4.1.3. Procesamiento de datos de la dimensión Control y gestión de la....56
4.1.4. Procesamiento de datos de la dimensión del informe final....57
4.2. PROCESAMIENTO DE DATOS DE LA VARIABLE REGISTRO DE....58
4.2.1. Procesamiento de datos de la dimensión manejo de información de software y hardware....59
4.2.2. Procesamiento de datos de la dimensión fines de la....60
4.2.3. Procesamiento de datos de la dimensión Software....61
4.2.4. Procesamiento de datos de la dimensión de la dimensión hardware....62
4.3. PRUEBA DE HIPÓTESIS....63
4.3.1. Prueba de la hipótesis general....64
4.3.2. Prueba de la hipótesis especifica 1....67
4.3.3. Prueba de la hipótesis especifica 2....70
4.3.4. Prueba de la hipótesis especifica 3....73
4.3.5. Prueba de la hipótesis especifica 4....76
CAPITULO V: DISCUSIÓN....82
5.1. Plan de auditoria....82
1. Objetivo general de la auditoria....87

2. Alcance de la auditoria 88
3. Responsable 89
4. Usuarios 89
5. Documentos de referencia 89
6. Criterios de la auditoria interna 89
7. Recursos 90
Etapas de trabajo 90
1. Recopilacion de informacion básica 90
2. Objetivos de control 91
3. Determinacion de los procedimientos de control 91
4. Pruebas a realizar. 93
5. Obtencion de los resultados 93
6. Conclusiones y Comentarios: 93
7. Riesgos con la aplicación de instrumentos 94
8. Redaccion de la ficha técnica 97
9. Presentación del borrador del informe, al responsable del area de patrimonio 97
10. Redacción del Informe Resumen y Conclusiones. 97
11. Entrega del informe a los jefes del área patrimonio y de la oficina general de tecnologías de información, sistemas y estadística. 99
5.2. Recursos (Humanos, Materiales y costos) 99
5.3. Presupuesto 100
5.4. Cronograma de actividades 101
5.5. Ejecución de la auditoria usando COBIT 4.5 106
DOMINIO: ALINEAR, PLANIFICAR Y ORGANIZAR (APO) 108
APO1.Definir un Plan Estratégico de TI. 109
APO7. Administrar los Recursos Humanos de TI 110
DOMINIO: ADQUIRIR E IMPLANTAR 112
AI1. Identificar soluciones automatizadas. 112
AI5. Adquirir recursos de TI. 113
DOMINIO: MONITOREAR Y EVALUAR 114
MEA1. Monitorear y evaluar el desempeño de TI. 114
MEA2. Supervisar, evaluar y valorar el sistema de control 114
DOMINIO: PRESTACIÓN Y SOPORTE 116
DSS2. Gestionar las Peticiones y los Incidentes del servicio. 116
DSS3. Administrar desempeño y capacidad. 117
DSS5. Garantizar la seguridad de los sistemas. 117

DSS 6. Gestionar los Controles de los Procesos del negocio.....118
5.6. Programa de auditoria y matriz de prueba de los procesos y objetivos de control.....119
5.6.1. Programa de auditoria.....119
5.6.2. Matriz de prueba.....119
5.7. Análisis de verificación de resultados.....149
5.8. Informe Preliminar.....169
5.5.1. Objetivos de control de efectivos.....169
5.5.2. Objetivos de control no efectivos.....174
5.5.3. Informe final.....179
CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES.....230
6.1. CONCLUSIONES.....230
6.2. RECOMENDACIONES.....231
REFERENCIAS BIBLIOGRÁFICAS.....233
ANEXOS.....236
Anexo 1: Mapa de identificación de problemas.....237
Anexo 2: Mapa de variables.....238
Anexo 3: hoja de ruta de variables.....239
Anexo 4: Matriz de consistencia sistémica.....240
Anexo 5: Base de datos del Alfa de Cronbach de la variable 1.....241
Anexo 6: Base de datos del Alfa de Cronbach de la variable 2.....241
Anexo 7: Confiabilidad De La Variable Auditoria Informática.....242
Anexo 8: Confiabilidad de la variable Registro de Software y Hardware.....243
Anexo 9: Oficio N° 001-2007.....244
Anexo 10: Validación de los Instrumentos, por los expertos.....245
Anexo 11: Arquitectura de equipos informáticos (Vigentes).....258
Anexo 12: Recursos Humanos y materiales.....259
Anexo 13: Encuesta para medir la variable Auditoria Informática.....260
Anexo 14: Encuesta para medir la variable Registro de Software y Hardware.....262
Anexo 15: modelo de Informe de auditoría informática.....264
Anexo 16: Ficha Técnica.....266
Anexo 17: Informe Mantenimiento Preventivo/Correctivo del Campus Universitario.....267
Anexo 18: inventario de equipos del área de informática.....270
Anexo 19: Análisis y evaluación de riesgos.....274
Anexo 20: Carta de presentación al área de patrimonio.....276
Anexo 21: Check List al jefe de soporte técnico.....277

Anexo 22: Checklist Aplicada Al jefe del área de patrimonio.....281
Anexo 24: Acta de reunión de registro.....288
Anexo 25: Cuestionario 1.....290
Anexo 26: Cuestionario 2.....294
Anexo 27: Cuestionario 3.....298
Anexo 28: Cuestionario 4.....302
Anexo 29: Cuestionario 5.....306
Anexo 30: Cuestionario 6.....310
Anexo 31: Cuestionario 7.....314
Anexo 32: Cuestionario 8.....318

ÍNDICE DE FIGURAS

Figura 1: Organigrama del área de patrimonio....3
Figura 2: Cubo COBIT....32
Figura 3: Dominios COBIT....33
Figura 4: Principios de COBIT 34
Figura 5: Instrumento de recolección de datos 50
Figura 6: Esquema de correlación de sampieri 52
Figura 7: Auditoria informática 54
Figura 8: Dimensión Informe preliminar 55
Figura 10: dimensión control y gestión de la información....57
Figura 11: Dimensión informe final....58
Figura 12: Variable Registro de Software y Hardware 59
Figura 13: Dimensión manejo de información de software y hardware....60
Figura 14: Dimensión fines de la adquisición 61
Figura 15: Dimensión Software....62
Figura 16: Dimensión hardware....63

ÍNDICE DE TABLAS

Tabla 1: Auditoria informática 53
Tabla 2: Dimensión Informe preliminar 54
Tabla 3: Dimensión análisis de la situación actual 55
Tabla 4: Dimensión Control y gestión de la información. 56
Tabla 5: Dimensión informe final. 57
Tabla 6: Variable Registro De Software Y Hardware. 58
Tabla 7: Dimensión manejo de información de software y hardware. 59
Tabla 8: Dimensión fines de la adquisición. 60
Tabla 9: Dimensión Software. 61
Tabla 10: Dimensión hardware 62
Tabla 11: Prueba de normalidad Shapiro-Wilk 65
Tabla 12: Toma de decisión de la hipótesis general 65
Tabla 13: Prueba de Correlación de Rho de Spearman. 66
Tabla 14: Prueba de normalidad Shapiro-Wilk. 68
Tabla 15: Toma de decisión de la hipótesis especifica 1 68
Tabla 16: Prueba de Correlación de Rho de Spearman, de la hipótesis especifica 1 69
Tabla 17: Prueba de normalidad Shapiro-Wilk. 71
Tabla 18: Toma de decisión de la hipótesis especifica 2 71
Tabla 19: Prueba de Correlación de Rho de Spearman, de la hipótesis 72
Tabla 20: Prueba de normalidad Shapiro-Wilk. 74
Tabla 21: Toma de decisión de la hipótesis especifica 3 74
Tabla 22: Prueba de Correlación de Rho de Spearman, de la hipótesis especifica 3 75
Tabla 23: Prueba de normalidad Shapiro-Wilk. 77
Tabla 24: Toma de decisión de la hipótesis especifica 4 77
Tabla 25: Prueba de Correlación de Rho de Spearman, de la hipótesis especifica 4 78
Tabla 26: Presupuesto de desarrollo de la auditoria 100
Tabla 27: Cronograma de Actividades 101
Tabla 28: A asignación de horas de auditoría 104
Tabla 29: Estimación de días por etapa 105

ÍNDICE DE CUADROS

Cuadro 1: Operacionalización de la variable auditoria informática 16
Cuadro 2: Operacionalización de la variable Registro de software y hardware 17
Cuadro 3: Auditoria, control, Control de Gestión 27
Cuadro 4: Cuadro comparativo Marcos de Trabajo 30
Cuadro 5: Cuadro comparativo Marcos de Trabajo 35
Cuadro 6: Adquirir e implantar 37
Cuadro 7: Entregar y dar soporte 39
Cuadro 8: Matriz de medición de probabilidad 95
Cuadro 9: Matriz de Probabilidad 95
Cuadro 10: Evaluación y medidas de respuesta 96
Cuadro 11: Programa de Auditoría APO7.4 122
Cuadro 12: Programa de Auditoría APO7.4 123
Cuadro 13: Matriz de prueba APO7.4 124
Cuadro 14: Programa de Auditoría APO7.6 125
Cuadro 15: Matriz de prueba APO7.6 126
Cuadro 16: Programa de Auditoría Al1.2 127
Cuadro 17: Matriz de prueba Al1.2 128
Cuadro 18: Programa de Auditoría Al5.1 129
Cuadro 19: Matriz de prueba Al5.1 130
Cuadro 20: programa de auditoría MEA1.1 131
Cuadro 21: Matriz de prueba MEA1.1 132
Cuadro 22: Programa de auditoria MEA1.4 133
Cuadro 23: Matriz de prueba MEA1.4 134
Cuadro 24: Programa de Auditoría MEA2.7 135
Cuadro 25: Matriz de prueba MEA2.7 136
Cuadro 26: Programa de Auditoría DSS2.1 137
Cuadro 27: Matriz de prueba 2.1 138
Cuadro 28: Programa de Auditoría DSS2.2 139
Cuadro 29: Matriz de prueba DSS2.2 140
Cuadro 30: Programa de Auditoría DSS2.4 141
Cuadro 31: Matriz de prueba DSS2.4 142
Cuadro 32: Programa de Auditoría DSS5.3 143
Cuadro 33: Matriz de prueba DSS5.3 144
Cuadro 34: Programa de Auditoría DSS6.1 145
Cuadro 35: Matriz de prueba DSS6.1 146
Cuadro 36: Programa de Auditoría DSS6.6 147
Cuadro 37: Matriz de prueba DSS6.6 148
Cuadro 38: Evaluación de pruebas APO1.4 150
Cuadro 39: Evaluación de pruebas APO1.5 151
Cuadro 40: Evaluación De Pruebas APO7.1 152
Cuadro 41: Evaluación De Pruebas APO7.3 153
Cuadro 42: Evaluación de pruebas APO7.4 154
Cuadro 43: Evaluación de pruebas APO 7.6 155
Cuadro 44: Evaluación de pruebas Al1.2 156
Cuadro 45: Evaluación de pruebas Al 5.1 157
Cuadro 46: Evaluación de pruebas MEA1.1 158
Cuadro 47: Evaluación de pruebas MEA1.4 159

Cuadro 48: Evaluación de pruebas MEA2.1 160
Cuadro 49: Evaluación de pruebas MEA2.2 161
Cuadro 50: Evaluación de pruebas MEA2.7 162
Cuadro 51: Evaluación de pruebas DSS2.1 163
Cuadro 52: Evaluación de pruebas DSS2.2 164
Cuadro 53: Evaluación de pruebas DSS2 165
Cuadro 54: Evaluación de pruebas DSS5.3 166
Cuadro 55: Evaluación de pruebas DSS6.1 167
Cuadro 56: Evaluación de pruebas DSS5.3 168

INTRODUCCIÓN

El presente Proyecto “Auditoría Informática Con Metodología Cobit 4.5 Para el Registro de Software Y Hardware del Área de Patrimonio de la Universidad Nacional de Ucayali: 2017”, consta de 5 capítulos.

Capítulo I: “**DESCRIPCIÓN DE PROBLEMA”** se describe el problema que la empresa y como daremos solución a ese problema usando metodologías que sean capaces de resolver.

Capítulo II: “MARCO TEÓRICO”, este capítulo recopila los conocimientos necesarios para comprender el problema y plantear una propuesta solución al mismo, conceptos básicos y necesarios para realizar el proyecto de investigación por medio de investigaciones.

.

Capítulo III: “**METODOLOGIA**”, Este capítulo es donde se verá que variables se usará para el proyecto de investigación realizando preguntas hipótesis

Capítulo IV: “RESULTADOS”, en este capítulo daremos a conocer los resultados adquiridos por las hipótesis plasmadas, los cuadros estadísticos, etc.

Capítulo V: “DISCUSIÓN”, se describe las formas del trabajo realizado las comparaciones y afirmaciones desarrolladas durante la investigación desarrollada.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1 .1 ANTECEDENTES DEL PROBLEMA

El llevar a cabo los objetivos y mantener la integridad de los datos para proteger los activos se han convertido en los fines principales dentro de las organizaciones, en este caso los procesos y objetivos que cuenta el área de patrimonio están siendo manipulados de forma errónea, uno de los procesos más afectados es el registro de software y hardware, existe mucha deficiencia en el manejo de información del área de patrimonio de la universidad nacional de Ucayali.

La Auditoría Informática permitirá la revisión y la evaluación de los controles, sistemas, procedimientos informáticos, equipos de cómputo, su utilización, eficiencia y seguridad de la organización que está inmersa en el procesamiento de la información con el fin de lograr una utilización más eficiente y segura de la misma que servirá para una adecuada toma de decisiones.

Los procesos necesitan estar en constante evaluación para el buen desarrollo de las actividades y funciones que cumplen el área para el funcionamiento de los bienes que cuentan la Universidad Nacional

De Ucayali esto ayudará al cumplimento de las normativas que establece el ministerio de economía y finanzas en cuanto al registro de los bienes que son adquiridos facilitando el buen manejo de información del software y hardware.

El área de patrimonio de la Universidad Nacional de Ucayali no cuenta con los recursos humanos suficientes para un buen desempeño laboral y así cumplir con la política que obliga el estado para las áreas de patrimonio, como también en la deficiencia del manejo de información de datos del software y hardware, las deficiencias que se encuentran son la falta de información detallada de cada equipo de cómputo. El mayor riesgo que se puede encontrar es que si el equipo informático no está correctamente registrado puede ser falsificado, no se sabe ¿para qué? o ¿Por qué? fueron adquiridos, o que beneficios traerán esas adquisiciones.

A menudo dentro de las áreas administrativas de la universidad nacional de Ucayali en especial el área de patrimonio encontramos problemas frecuentes en cuanto al manejo de información de los equipos informáticos; además no cuentan con los recursos humanos para el buen funcionamiento del área, como también no están siendo controlados de forma correcta el inventario de los equipos informáticos. La falta de un plan de contingencia y un plan de evaluación para el cumplimiento de las normas que establece el MEF; para el inventario de los bienes. Esto ocasiona a que se tenga problemas en el déficit de información. Ver cada punto del manejo de información de los bienes informáticos de toda la Universidad Nacional de Ucayali se necesita realizar ciertas medidas; se debe tener en orden toda la información de los bienes con las recomendaciones precisas y claras para la mejora del área de patrimonio de la Universidad Nacional de Ucayali se debe

Realizar medidas que sean para el beneficio del área como también de la Universidad Nacional de Ucayali.

Misión

El Servicio de contratación tiene como misión gestionar y asesorar, en la tramitación de expedientes de contratos mayores y menores, así como controlar y mantener el inventario de bienes y derechos de la Universidad de Nacional de Ucayali, gestionar los espacios y servicios comunes, todo ello para la satisfacción de las necesidades de la comunidad universitaria, observando los principios de legalidad, economía, eficacia y eficiencia.

Visión

Nuestra vocación es, dentro del ámbito de las directrices estratégicas de la Universidad Nacional de Ucayali, ser una unidad administrativa eficaz y eficiente en el cumplimiento de sus objetivos, con una asignación racional de recursos, un adecuado sistema de información y un compromiso permanente con la Institución, la calidad y la mejora continua orientada a la prestación del servicio asignado.

Organigrama del área de patrimonio

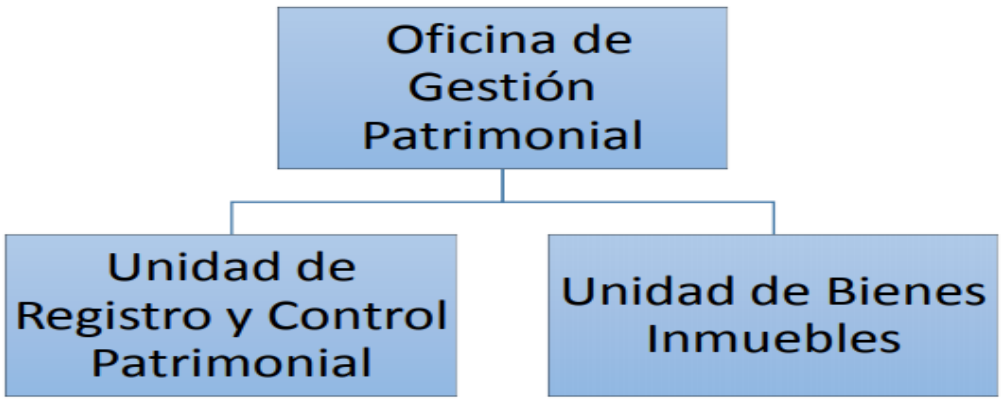


Figura 1: *Organigrama del área de patrimonio*

1.1.1. Delimitaciones de la investigación

Delimitación espacial

La presente investigación se realizará en el área de patrimonio de la Universidad Nacional de Ucayali.

Delimitación social

El proyecto de investigación se va a realizar en el área de patrimonio junto con la oficina general de tecnologías de información, sistemas y estadística (OGTISE) de la Universidad Nacional de Ucayali con cada uno de los trabajadores.

Delimitación temporal

La presente investigación se realizará en el período de 2 años a partir de la aprobación del comité de planeamiento de la Facultad de Ingeniería en Sistemas e ingeniería civil.

Delimitación conceptual

a) Auditoria informática: variable independiente

Auditoria informática: Es la evaluación y verificación de las políticas, controles, procedimientos y la seguridad en general, correspondiente al uso de los recursos de informática por el personal de la empresa (usuarios, informática, alta dirección), a fin de que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

b) Registro de software y hardware: Variable dependiente.

Registro: consiste en una base de datos que incluye todas las configuraciones y opciones relativas a todas las aplicaciones, programas, usuarios y configuraciones del equipo (es decir, a todo lo relativo al Software) mientras que también incluye información y configuración de los dispositivos conectados (esto es, el Hardware del sistema).

Software: Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados, que forman parte de las operaciones de un sistema de computación.

Hardware: Hardware es la parte física de un ordenador o sistema informático. Está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables y luz, placas, memorias, discos duros, dispositivos periféricos y cualquier otro material en estado físico que sea necesario para hacer que el equipo funcione.

Síntomas

1. No cuenta con el personal suficiente para realizar las actividades de registro de software y hardware que tiene el área de patrimonio.

La falta de recursos humanos hace que la función del área de patrimonio no sea eficiente, actualmente solo existen 4 personas que están laborando en dicha área, el jefe del área, su secretaria y 2 practicantes. Para que el área sea muy eficiente se necesita de más recursos humanos para que los procesos sean más rápidos y más eficientes.

2. Existe deficiencia en el registro de software y hardware del área de patrimonio, existen equipos informativos que no están registrados en el sistema SINABIP (sistema de información nacional de bienes estatales)[1], software donde se registran todos los bienes que cuenta el área de patrimonio.

El registro de datos del software y hardware están siendo manejados erróneamente ocasionando déficit en el manejo de información, entonces el jefe del área conjuntamente con los 3 trabajadores lo registran como un bien rotulado poniendo un código interno para su reconocimiento.

3. Al momento que se desea adquirir información de la condición de los equipos informáticos tenemos que ir a buscar información en las propias en las oficinas administrativas y eso causa perdida de tiempo para la elaboración de los objetivos del área de patrimonio.

Existen equipos informáticos que no se encuentran registrados en el área de patrimonio pero que están utilizados en distintas áreas y para saber el funcionamiento de dichos equipos se tiene que hacer visitas a cada área y recién poder registrar los equipos; cuando esa función se debe realizar al momento de la adquisición del bien.

4. No se solucionan los problemas del registro de hardware, ni se resuelven incidencias a su tiempo.

Uno de los problemas más claros es la falta de información del hardware, es escasa la información que no se entiende por qué de la compra, que beneficios traería al área o que si cuentan con una garantía en caso se tenga problemas al momento de utilizarlos.

[1] SBN, tecnologías de información , SINABIP, Sistema de información nacional de bienes estatales

Consecuencias

1. Pérdida de tiempo, retraso en las actividades programadas por el área de patrimonio y propagando déficit en el manejo de información.

Al no contar con personal suficiente para el registro de software y hardware hace que se retrase las actividades que realiza el área de patrimonio y se tenga problemas en el manejo de información.

2. Pérdida de información, extravíos de equipos informáticos.

3. Mayores tiempos en la obtención de información de software y hardware, retrasando las actividades que se desea realizar.

El tiempo es el peor enemigo de las funciones mientras más se demora saber él porque de la adquisición y beneficio que traerá.

4. Genera conflictos con los usuarios encargados del manejo información del registro de software y hardware.

Existen escases en el registro de información de software y hardware. No hay una información clara y precisa de la información.

1 .2. FORMULACIÓN DEL PROBLEMA

Problema

Realizando nuestro análisis y las evaluaciones correspondientes nos encontramos que existe una deficiencia en el manejo de información del registro de software y hardware del área de patrimonio.

Esta dicha deficiencia de registro de software y hardware se está dando por la falta de personal en el área, al no contar con suficiente personal hace que el inventario de cada bien informático no sea la eficiente para el buen registro de la información, los equipos informáticos que no están en el inventario son registrados de manera interna que quiere decir esto; que son registrados como bienes rotulados, el software con el que trabaja el área no es suficiente para realizar estos procesos de registros, se pide adquirir el software SIGA – MODELO PATRIMONIAL (sistema integrado de gestión administrativa)[2].

1.2.1. General

¿Cómo la Auditoria Informática con metodología COBIT 4.5 podrá mejorar el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017?.

1.2.2. Específicos

- ¿Cómo se analiza los procesos y riesgos relativos que se llevan a cabo en el área de patrimonio de la Universidad Nacional de Ucayali?.

- ¿Cómo el plan de auditoria basado en la metodología COBIT 4.5 podrá definir los métodos, técnicas, procedimientos, plan de pruebas para la evaluación de los procesos del área de patrimonio de la Universidad Nacional de Ucayali?.

[2] RYC, Consulting, SIGA, Sistema integrado de gestión administrativa, Perú, 2019

- ¿En qué medida la auditoria informática con metodología COBIT 4.5 se relaciona con el software y hardware del área de patrimonio de la universidad nacional de Ucayali?.

- ¿Cómo la auditoria informática con metodología COBIT 4.5, se relaciona con el manejo con el manejo de información de software y hardware del área de patrimonio de la Universidad Nacional de Ucayali?.

- ¿Cómo reportar los hallazgos de la auditoria y recomendaciones para que el área de patrimonio establezca el plan de mejoramiento y el sistema de control adecuado?.

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo general

Realizar una auditoria informática con metodología COBIT 4.5 para el registro de software y hardware del área de patrimonio de la Universidad Nacional de Ucayali: 2017.

1.3.2. Objetivos específicos

- Analizar los procesos y riesgos relativos del área de patrimonio, desarrollando la metodología COBIT 4.5.

- Desarrollar un plan de auditoria basado en la metodología COBIT 4.5 definiendo los métodos, técnicas, procedimientos, plan de pruebas para la evaluación de los procedimientos del área de patrimonio de la Universidad Nacional de Ucayali.

- Establecer el nivel de relación entre la auditoria informática con metodología COBIT 4.5 con el software y hardware del área de patrimonio de la universidad nacional de Ucayali.

- Establecer el nivel de relación entre la auditoria informática con metodología COBIT 4.5, con el manejo de información de software y hardware del área de patrimonio de la Universidad Nacional de Ucayali.

- Elaborar un informe final de auditoria con los hallazgos y recomendaciones para que el área de patrimonio establezca el plan de mejoramiento y el sistema de control adecuado.

1.4. JUSTIFICACIÓN E IMPORTANCIA

Con el manejo de diversos sistemas de información y automatización en sus procesos, El área de patrimonio y el área de informática de la Universidad Nacional de Ucayali necesita corregir fallas, ejecutar procesos de calidad y, entregarlos en el momento oportuno; detectar los errores mediante una Auditoría Informática, realizada y ejecutada por un grupo personal establecido, que proponga soluciones efectivas, para minimizar riesgos y mejorar el empleo de la tecnología de información en la organización.

Actualmente los procesos del área de patrimonio de la Universidad Nacional de Ucayali tienen un desempeño no muy efectivos, el más afectado es el proceso de registro de software y hardware, lo cual no significa que se encuentre vulnerable, ya que el sistema con el que cuenta el área se encuentra en constante desarrollo, esto puede causar que se pierda información de gran

importancia para el área de patrimonio, como por ejemplo Información de los bienes tangibles y intangibles, así como también la información de los equipos informáticos, que son de igual importancia para que el área de patrimonio tenga un mejor panorama de sus procedimientos y brindar una seguridad lógica y física a las diferentes áreas que cuenta la Universidad Nacional de Ucayali y se pueda desenvolver de manera óptima.

Es importante determinar cuál es el funcionamiento actual de los de los procesos del área de patrimonio para poder tener una perspectiva clara del estado de los mismos y realizar un informe en el punto de la forma de resolver la problemática. La solución tiene que ser eficaz y clara.

La realización de una Auditoría Informática presentaría grandes beneficios, permitiéndole al área de patrimonio en conjunto con el área de informática estar a la vanguardia de la tecnología alcanzando de esta manera un desempeño óptimo para sus estudiantes, directivos y administrativos, haciendo que el área de patrimonio sea ejemplo a seguir dentro de la Universidad Nacional de Ucayali.

1.4.1. Justificación teórica

Desde el punto de vista teórico la presente investigación servirá como base para otras investigaciones, y de apoyo para la realización de trabajos basados en el modelamiento de Procesos realizados en el área de patrimonio y la oficina general de tecnologías de información, sistemas y estadística (OGTISE) y/o construcción de Sistemas de Información, ya que se desarrollará de manera integral desde la planeación, el análisis, el diseño, la construcción, y las pruebas realizadas, todo ello paso a paso y con las observaciones de los por menores encontrados. Además

contará con un marco teórico resumido y seleccionado de los mejores autores brindando información de correcciones de las fallas en el registro de software y hardware.

1.4.2. Justificación práctica

Desde el punto de vista práctico, la investigación nos ayudará a resolver el problema del riesgo en cuanto al manejo de información, esto con el objetivo de emitir una validez y la confiabilidad de la información que es generada por el sistema auditado. Las personas beneficiadas serán primeramente el área de patrimonio de la Universidad Nacional de Ucayali ya que se le realizará un trabajo limpio y sin ningún costo, por medio de la auditoría podrá visualizar qué es lo se está haciendo incorrectamente y corregirlo, qué se está haciendo bien, pero que se puede hacer mejor y cuáles van a ser los protocolos de actuación en el caso de los problemas para que esto no afecte directamente a la productividad de dicha área.

1.4.3. Justificación metodológica

Desde el punto de vista metodológico, la adecuada implementación de la metodología COBIT 4.5 nos ayudará a evaluar de manera ágil y consistente el cumplimiento de los objetivos de control de los recursos de la información y tecnologías en el área de patrimonio, con un mejor control de la información, un eficaz manejo de información para minimizar los riesgos para la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones del área de patrimonio.

1.4.4. Importancia

La presente Tesis, es de suma importancia porque está marcada dentro del enfoque de Auditoría Informática, doctrina de poca información en el sector privado del país.

El progreso de la tecnología de la computación y la informática está mejorando día a día, esto a la vez genera problemas en el desarrollo de oportunidades y lleva a cometer errores. Entonces para que no suceda eso es necesario revisar e inspeccionar los procesos y objetivos desarrollados en el área de patrimonio para poder brindar un mejor trabajo de control para los estudiantes y personal contratado de la Universidad Nacional de Ucayali. Por tanto la oficina auditada trabaja bajo inspección de las regulaciones y leyes propias de auditoria, en la construcción de sistemas de control para la ejecución de proceso, almacenamiento de datos y revisión. Debido a la probabilidad de cometer errores es sugerido a las instituciones que estén bajo inspección por lo menos una vez al año.

1.5. HIPÓTESIS Y VARIABLES DE LA INVESTIGACIÓN

1.5.1. Hipótesis general

La Auditoria Informática con metodología COBIT 4.5 mejora el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

1.5.2. Hipótesis Específicas

- El análisis de los procedimientos y riesgos relativos del área de patrimonio, se desarrolla con la metodología COBIT 4.5.

.

- El desarrollo de un plan de auditoria basado en la metodología COBIT 4.5 define los métodos, técnicas, procedimientos, plan de pruebas para la evaluación de los procedimientos del área de patrimonio de la Universidad Nacional de Ucayali.

- La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el software del área de patrimonio de la Universidad Nacional de Ucayali.

- La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el Manejo de información de software y hardware del área de patrimonio de la universidad Nacional de Ucayali.

- El informe final de auditoria nos reporta los hallazgos y recomendaciones para que el área de patrimonio establezca el plan de mejoramiento y el sistema de control adecuado.

1.6. VARIABLES (DEFINICIÓN CONCEPTUAL Y OPERACIONAL)

1.6.1. Definición conceptual de la variable

Auditoria informática

Según Fernández la auditoria informática es un concepto genérico que engloba los distintos tipos de auditoría, que globalmente puede definirse como el "examen y verificación de registros, procesos, circuitos e información de diversa índole, con objeto de expresar una opinión sobre la perfección o fiabilidad de los datos reflejados en las anotaciones" (Fernández García, 2007).

Hardware

Según Juan Pérez Porto el hardware Está formado por los dispositivos electrónicos y mecánicos que realizan los cálculos y el manejo de la información. (Porto, 2008).

Software

De acuerdo a, Alcalde García Eduardo. El software es un conjunto de elemento lógicos necesarios para que se pueda Realizar las tareas encomendadas al mismo, se puede definir de la siguiente forma: en la parte lógica que dota al equipo físico de capacidad para realizar cualquier tipo de trabajo (Alcalde Garcia, 1994).

1.6.2. Definición operacional de la variable

Variable independiente

Auditoria informática

Variable dependiente

Registro de software y hardware

Variable interviniente

Área de patrimonio de la universidad Nacional de Ucayali.

1.6.3. Operalización de las variables

A continuación mostraré el cuadro de Operalización de las variables:

Cuadro 1: *Operacionalización de la variable auditoria informática*

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Categorías
Auditoria informática	Refiere a la revisión práctica del manejo de información y recursos informáticos con que cuenta la entidad en este caso el área de patrimonio.	0-Inexistente 1-Inicial 2-Intuitivo 3-Definido 4-administrador 5-Optimizado	Informe preliminar o de datos	Elaboración de una ficha técnica.	1;2	Incorrecto [6 – 9] Moderado [10 – 13] Correcto [14 – 18]
				Informe de la Situación actual del área en cuanto al manejo de datos.	3;4	
				Recolección de información o datos	5;6	
			Análisis de la situación actual	Tratamiento de la documentación.	7;8	Incorrecto [4 – 6] Moderado [7 – 9] Correcto [10 – 12]
				Análisis previos	9;10	
			Control y gestión de la información	Verificación	11;12	Incorrecto [6 – 9] Moderado [10 – 13] Correcto [14 – 18]
				Planificación	13;14	
				Control detallado de la información	15;16	
			Informe final	Observaciones	17;18	Incorrecto [4 – 6] Moderado [7 – 9] Correcto [10 – 12]
				Conclusiones	19;20	

Fuente: Elaboración propia

Cuadro 2: *Operacionalización de la variable Registro de software y hardware*

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Categorías
Registro de software y hardware	Software. Son las instrucciones que el ordenador necesita para su funcionamiento. Hardware. Componentes físicos del ordenador, es decir, todo lo que se puede ver y tocar.	0-Inexistente 1-Inicial 2-Intuitivo 3Definido 4-Administrado 5-Optimizado	Manejo de información de software y hardware	Usuario encargado de la recepción de software y hardware	1;2	Malo [6 - 9] Regular [10 - 13] Bueno [14 - 18]
				Fabricante que brinda los software y hardware	3;4	
				Recolección de información	5;6	
			fines de la adquisición	Inventariado de los hardware y software del área.	7;8	Malo [4 – 6] Regular [7 – 9] Bueno [10 – 12]
				Propósito de adquisición	9;10	
			Software	Seguridad	11;12	Malo [6 - 9] Regular [10 - 13] Bueno [14 - 18]
				Actualización	13;14	
				Tipo de uso	15;16	
			Hardware	Mantenimiento	17;18	Malo [4 – 6] Regular [7 – 9] Bueno [10 – 12]
				Reparación	19;20	

Fuente: Elaboración propia

CAPITULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Tesis Internacionales

1. “Auditoría Informática a la Superintendencia de Telecomunicaciones”. 1) El objetivo de la investigación es realizar una Auditoria informática a la Superintendencia de telecomunicaciones.2) Tesis realizada en la Universidad De cuenca- Ecuador. 3) Elaborado en el Año 2016. 4) La Ciudad de cuenca. 5) Conclusión, COBIT provee objetivos de control y métricas validadas globalmente para cada proceso de tecnología informática, esto ha brindado una guía pragmática de control para la auditoría realizada a la Superintendencia de Telecomunicaciones. (Rodriguez Quitnuña, 2017).

2. “Auditoria al sistema de información Alpwin 2.0 en el rubro cuentas cobrar del módulo de ventas de la compañía Syscompsa S.A”. Tesis para obtención del de título de ingeniería en contabilidad y auditiva 1) El objetivo de la investigación es evaluar el módulo de ventas de la compañía Syscompsa mediante una

Una auditoria de sistemas para mejorar los controles de créditos. 2) Tesis realizada en la Universidad Politécnica Salesiana de Guayaquil-Ecuador. 3) Elaborado en el año 2015. 4) Elaborado en la ciudad de Guayaquil. 5) Conclusión general De la tesis, No existe el manual de políticas de crédito formal que permita controlar las operaciones crediticias de la empresa, además no ayudan a la organización a tener mayor rentabilidad (Sobeyda Monica & Bonilla Díaz, 2015).

3. “Auditoría Informática de la Cooperativa de Ahorro y Crédito “Alianza del Valle” Ltda. Aplicando Cobit 4.0”. 1) Objetivo de la tesis, Implementar una Auditoria Informática de la cooperativa de ahorro y crédito. 2) Tesis realizada en la Escuela politécnica del ejército. 3) Elaborado en el año 2018. 4) En la ciudad Sangolquí. 5) Conclusión, Logramos desarrollar una auditoria informática para evitar distorsiones en la escuela. (Marcillo Barros, 2012).

4. “Auditoría Informática Basada En Norma Iso 27004 Para El Control Del Parque Tecnológico De Uniandes Puyo”. 1) Objetivo general de la tesis es Realizar una Auditoria informática basada en norma ISO 27004 para el control del parque tecnológico de Unidades Puyo. 2) Tesis realizada en la Universidad Regional Autónoma De Los Andes. 3) Elaborado en el año 2017.4) Elaborado en la ciudad de Ambato – Ecuador.5) Conclusión, Se ha demostrado que la norma ISO 27004 se adapta a la Auditoria Informática aplicada en Uniandes Puyo puesto que nos facilitó el proceso a seguir en el momento de desarrollar nuestra investigación. (Becerra Arévalo, 2017).

5. Auditoría informática para la optimización del funcionamiento de los sistemas y equipos informáticos de la facultad de ingeniería en sistemas, electrónica e industrial de la universidad Ambato - Ecuador". 1) Objetivo general Realizar una Auditoría Informática para optimizar el funcionamiento de los sistemas y equipos informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial (Gabriela Acosta, 2016).

6. "Auditoría Informática en el Área Administrativa de la Pontificia Universidad Católica Del Ecuador Sede Esmeraldas." 1) Objetivo de la investigación, Fortalecer la estructura y los procesos administrativos y académicos, - Identificar los departamentos del área administrativa y analizar las funciones de cada uno de ellos. 2) La tesis fue elaborado en la Universidad Pontificia Universidad Católica del Ecuador sede Esmeraldas. 3) Elaborado en el año 2017.4) Ciudad Esmeraldas.5) Conclusión, Realizar una auditoría informática beneficia al Área Administrativa y a la Universidad porque de ahí desprenden sus servicios, mejorando así la experiencia de los usuarios, trabajadores como estudiantes. (Nazareno Vivero, 2016).

7. "Implementación de Una Auditoría Informática al Sistema de Matriculación De Estudiantes (Sais) de la Universidad Agraria Del Ecuador". 1) Objetivo de la investigación, Valorar los resultados obtenidos durante la Auditoría Informática realizada para que de esta manera se logre una apropiada integridad y disponibilidad de las Tecnologías de información. 2) La tesis fue elaborado en la Escuela Superior Politécnica Del Litoral. 3) Elaborado en el año 2016.4) Ciudad de Guayaquil- Ecuador. 5) Conclusión, Luego de la implementación del Sistema de

Matriculación SAIS en la UAE, se determinó que se requería una Auditoría del Sistema de Matriculación para determinar las fortalezas y debilidades del Sistema y todos los procesos informáticos que involucran el Departamento del Centro de Cómputo, para lo cual se realizó un Plan de Auditoría Informática. (Avilés Freire, 2016).

8. “Auditoria al Control y Mantenimiento de la Infraestructura Tecnológica Del Departamento Tecnológico De La Espam Mfl”.1) Objetivo de la investigación, Aplicar Auditoria al control y mantenimiento de la infraestructura tecnológica del Departamento Tecnológico de la ESPAM MFL, para evaluar el nivel de cumplimiento de aplicaciones de buenas prácticas, estándares y normas de control interno informático y tecnológico de la Contraloría General del Estado Ecuatoriano. 2) La tesis fue elaborado en la Escuela Superior Politécnica Agropecuaria De Manabí Manuel Félix López. 3) Elaborado en el año 2015.4) Ciudad de Calceta-Ecuador. 5) Conclusión, Al evaluar los checklist de la Norma de Control Interno de TI 410-09 Infraestructura Tecnológica y la Norma ISO 27000, se determinó que el departamento tecnológico no está cumpliendo en su totalidad con las buenas prácticas, estándares y normas que dispone la Ley. (Rivera Chávez & Zambrano Bravo, 2016).

2.1.2. Tesis nacionales

1. “Propuesta de un Plan de Auditoria Informática para el "Sistema de Información en Salud" y el "Aplicativo para el Registro de Formatos Sis" en los Establecimientos de Salud De la Unidad Ejecutora 400 en la Región Piura en

el Año 2015". El objetivo de la investigación Proponer un plan de auditoría informática en los establecimientos de salud de la Unidad Ejecutora 400 en la Región Piura para el Sistema de Información en Salud y el Aplicativo para el Registro de Formatos SIS en el año 2015. Sus conclusiones son: 1) En base al marco normativo peruano se desarrolló la propuesta del plan de auditoría informática que permite obtener una guía para las futuras auditorías a los sistemas informáticos del estado peruano (Aplicativo para el Registro de Formatos SIS y al Sistema de Información en Salud). 2) obtención de los requerimientos para el desarrollo del sistema. (Ramos Arca, 2015) .

2. "Auditoría Informática Usando Las Normas Cobit En El Centro De Sistemas De Información Del Hospital Regional Docente Las Mercedes De Chiclayo – 2016". 1). Objetivo general, Realizar la auditoría informática en el área del Centro de Sistemas de Información del Hospital Regional Docente Las Mercedes de Chiclayo, usando las normas COBIT (Control Objectives For Information and Related Technology), con el fin de aumentar la eficiencia y eficacia en el área indicada. Ciudad Lambayeque. 2). Conclusión, dar función de procedimientos de inventario y facturación (Samillan, 2016).

3. "Metodología para auditoría informática en entidades públicas", objetivo general, Asignar adecuadamente las áreas de estudio a los estudiantes. Las conclusiones son: 1) Objetivo, la metodología propuesta permite revisar el uso de la tecnología de información en la entidad, utilizando técnicas modernas para la recopilación de información y análisis detallado, con la finalidad de identificar los riesgos y evaluar los controles en el uso de

las mismas. 2) Conclusión, el diseño de los cuestiones, permite recopilar información acerca de las causas que motivaron al auditor a calificar el riesgo a un área, el mismo que sirve como punto de partida para posteriores auditorías. (Ramirez Reyes, 2015).

4. “Auditoria al Control y Mantenimiento de la Infraestructura Tecnológica del Departamento Tecnológico de la Espam Mfl”. El objetivo general es Aplicar Auditoria al control y mantenimiento de la infraestructura tecnológica del Departamento Tecnológico de la ESPAM MFL, para evaluar el nivel de cumplimiento de aplicaciones de buenas prácticas, estándares y normas de control interno informático y tecnológico de la Contraloría General del Estado peruano. Las conclusiones son: 1). El departamento tecnológico no cuenta con documentación de los procesos que se realizan dentro de éste.2) cuentan con un manual de funciones y organizaciones, un plan de mantenimiento y un organigrama funcional desactualizado.3) no tiene un plan de contingencias. Departamento de Junín. (Briones Véliz, 2015) .

5. “Diseño de un Sistema de Gestión de Seguridad de Información para una Compañía De Seguros “. Objetivo general, brindar un sistema de gestión de seguridad de información para una compañía de seguros. pontificia Universidad católica del Perú, ciudad lima, Conclusión. 1) Partiendo de esta premisa, es importante contar con un Sistema de Gestión de Seguridad de la Información para poder asegurar, a un nivel aceptable, la información de la compañía y, dado que se trata de una compañía de seguros peruana, poder cumplir con las regulaciones de la SBS cumpliendo con el contenido de la circular G-140 y evitar así que la compañía incumpla con las regulaciones

de la superintendencia. 2) Para poder desarrollar el sistema, es necesario poder conocer los procesos de la compañía. En este documento se consideraron los procesos que tiene una compañía de seguros en general, pero es importante considerar siempre que el SGSI debe estar enfocado en las necesidades del negocio. Es decir, si la compañía considera un proceso en particular como crítico, se deben implementar controles necesarios para asegurar el mismo. (Ampuero Chang, 2016).

6. “Metodología para la Auditoría Integral de la Gestión de la Tecnología de Información”. El objetivo general es Analizar y evaluar las instalaciones eléctricas de los equipos de cómputo y redes de la organización, con el fin de identificar la probable pérdida de valor debido a fallas en los diversos procesos involucrados. pontificia universidad católica del Perú, ciudad de lima, conclusión. 1) La decisión de aplicar estándares internacionales de calidad para la auditoría de la gestión de tecnología de información, puede partir del área de Auditoría Interna, y no necesariamente de la Gerencia General o el Directorio. Por ello es muy importante tener personal de auditoría muy competente para ayudar al logro de los objetivos organizacionales. (Alfaro Paredes, 2016).

7. “Propuesta De metodológica de auditoría informática para realizar la auditoria informática en el sector financiero”. El objetivo general es desarrollar una Propuesta De metodología de auditoria informática para realizar la auditoria informática en el sector financiero, Universidad Nacional de Trujillo, Ciudad Trujillo, Conclusión. 1) Durante el desarrollo del presente trabajo de tesis, se analizó trabajos previos en auditorias informáticos

orientados en el área del sector financiero. 2) Con la metodología propuesta, a diferencia de una tradicional en el sector financiero, se ha obtenido una significativa ventaja al evaluar criterios de tiempo, simplicidad y rapidez. (Flores Rubio, 2015).

8. “Auditoria Informática al departamento de informática del hospital de belén de Trujillo”. Objetivo general es Aplicar una auditoria informática, utilizando herramientas y técnicas de auditoria informática a fin de identificar debilidades y emitir recomendaciones que permitan eliminar o minimizar los riesgos de la organización. Universidad Nacional de Trujillo, Ciudad de Trujillo, Conclusión. 1) Durante el desarrollo de la auditoria, se observó que hay una desactualización en la documentación disponible (inventarios, manual de procedimientos) así como también la inexistencia de documentos importantes para el desarrollo de las actividades (documentación del desarrollo de sistemas). 2) El departamento de informática presenta debilidad en cuanto a la falla de presupuesto para adquirir recursos humanos, solo cuenta con 3 colaboradores encargados de las áreas de redes, soporte y jefatura; el área de desarrollo de sistemas no cuenta con un responsable por lo que muchas veces el jefe del departamento debe asumir las funciones de dicha área. (Henriquez Zavaleta, 2015).

9. “Auditoría del sistema de seguridad de información en el hospital III José Cayetano Heredia - castilla; 2016”. 1) Objetivo General, realizar una auditoría del sistema de seguridad de información en el hospital III José Cayetano Heredia. 2) Tesis realizada en la Universidad Católica los Ángeles de Chimbote, 3) Año del desarrollo de la tesis

2016 4) Departamento de Piura. 5) Conclusión, Se recomienda que la Gerencia General del Hospital III José Cayetano Heredia – Castilla, impulse un cambio de cultura de seguridad de información en los diferentes departamentos y áreas del hospital, ya que es de vital importancia la información y uno de los bienes más preciados en esta institución de la salud. (Albán Gramonte, 2016).

10. “Auditoria de seguridad informática aplicada a la Municipalidad Distrital de Santa María”. 1) Objetivo General, recopilar información de las políticas de seguridad con las que cuenta la municipalidad y analizar la seguridad física y lógica de la infraestructura para así poder detectar las vulnerabilidades de esta institución. Para realizar la auditoria se apoyó en la herramienta COBIT. 2) Tesis elaborado en la Universidad Nacional San Pedro. 3) Elaborado en el año 2017. 4) La Ciudad de Huacho. 5) Conclusión, podemos aplicar todos los conocimientos adquiridos durante la construcción de este proyecto de investigación, realizando así un trabajo de amplia magnitud en lo que respecta a seguridad informática (Urbizagastegui Aguilar, 2016).

2.2. DEFINICIÓN DE TÉRMINOS BÁSICOS

2.2.1. Auditoria informática

“Según Juan Ramón Santillana González el concepto de auditoría significa verificar que la información financiera, Administrativa y operacional de una entidad es confiaba, veraz y oportuna; en otras palabras, es revisar que los hechos, fenómenos y operaciones se den en la forma en que

fueron planeados, que las políticas y lineamientos se hayan observado y respetado, que se cumple con las obligaciones fiscales, jurídicas y reglamentarias en genera" (Santillana González, 2002).

Según Fernández la Auditoría Informática es un concepto genérico que engloba los distintos tipos de auditoría, que globalmente puede definirse como el "examen y verificación de registros, procesos, circuitos e información de diversa índole, con objeto de expresar una opinión sobre la perfección o fiabilidad de los datos reflejados en las anotaciones" (Fernández García, 2007).

Con vistas a mejorar en:

- Seguridad
- Rentabilidad
- Eficacia

Cuadro 3: *Auditoria, control, Control de Gestión*

	AUDITORÍA	CONTROL	CONTROL DE GESTIÓN
¿QUÉ HACE?	Examina, enjuicia y recomienda	Establece dispositivos de seguridad	Evalúa el coeficiente objetivos/realización
¿CUANDO SE HACE?	Dando un corte en el calendario	Permanentemente	Permanentemente
¿COMOSE HACE?	Desmonta los mecanismos	Vigila	Acciones correctivas.

Fuente: Elaboración propia

ESTÁNDARES DE AUDITORÍA INFORMÁTICA

Los auditores de procesos de TI tienen una variada gama de herramientas y/o marcos de trabajo que pueden asistirle al momento de aplicar la auditoría que corresponda, dando una visión objetiva para que el auditor decida qué marco es el mejor para usarse en base al medio donde realice su trabajo y dependiendo de la función que cumple la organización.

A continuación, en el siguiente cuadro comparativo los marcos de trabajo que se han considerado importantes, cuya principal diferencia entre ellos es el enfoque que manejan para atender y desarrollar las áreas de TI y su cobertura:

INFORME PRELIMINAR

Según Donoso es un informe realizado por un auditor externo donde expresa una opinión no vinculante sobre las cuentas anuales o estados financieros que presenta una empresa (Donoso Yáñez, 2018).

a) Análisis

Según la definición clásica de Berelson (1971, citado por Hernández, Fernández y Baptista, 2003), "el análisis de contenido es una técnica para estudiar y analizar la comunicación de una manera objetiva, sistemática y cuantitativa" (Berelson, 1971).

Según Arthur George Es la desintegración de un todo en las partes que lo componen, para llegar a conocer sus elementos y /o principios. Ese todo puede ser obra de la naturaleza, como cuando se analiza una planta, o un producto cultural, como cuando se estudian los elementos del sistema comunicacional. La función del análisis es conocer mejor el objeto de estudio. Cuando

uno habla de un estudiante analítico, nos referimos a aquel que estudia pormenorizadamente los detalles del tema, objeto de su conocimiento, cuando hablamos de un estudio sintético, es solo poner de relieve los aspectos esenciales del tema, considerándolo como un todo, sin desmenuzarlo (Tansley, 1939).

b) Control y gestión de la información

Según Taylor es el proceso administrativo que sirve para evaluar el grado de cumplimiento de los objetivos organizacionales previstos por la dirección o gobierno corporativo verificando el buen manejo de la información, detalla de en forma práctica y precisa (Winslow Taylor, 1895).

Según García (1975), el control de gestión (CG) es ante todo un método, un medio para conducir con orden el pensamiento y la acción, lo primero es prever, establecer un pronóstico sobre el cual fijar objetivos y definir un programa de acción. Lo segundo es controlar, comparando las realizaciones con las previsiones al mismo tiempo que se ponen todos los medios para compensar las diferencias constatadas (Garcia, 1975).

c) Informe final

Según María Del Lourdes Martínez Montaño se denomina informe final a la comunicación que prepara y alcanza un investigador acerca de un estudio que realiza según exigencias y criterios instituidos por una de alto nivel de estudio para ver la problemática de la auditoria en diferentes entidades , de acuerdo a las pautas de la investigación científica, para alcanzar un grado académico o título profesional. (vea bayarre, 2004).

2.2.2. COBIT 4.5

Según Karina Baquero, COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso. (Baquero, 2012).

***Cuadro 4**: Cuadro comparativo Marcos de Trabajo*

ÁREA	COBIT(Gestión de la Seguridad de la Información)	ITIL(Gestión de la Seguridad de la Información)	ISO 27000(Gestión de la Seguridad de la Información)
ALCANCE	Abarca todo el espectro de las actividades de TI (seguridad, control, servicios y riesgos)	Muy centrado en la administración de servicios	Cubre todo lo referente a la entrega de servicios de TI
OBJETIVO PRINCIPAL	Establece controles internos para asegurar buenas prácticas de gestión de IT y un gobierno de IT exitoso)	Dar soporte a los procesos del negocio desde una perspectiva de gestión de servicios	Definir los requerimientos necesarios para realizar una entrega de servicios de TI alineados con las necesidades del negocio.
FUNCIONES	Mapeo de Procesos IT	Mapeo de la Gestión de Niveles de Servicio de IT	Marco de referencia de seguridad de la información.
ÁREAS	4 Procesos y 34 Dominios	9 Procesos	10 Dominios
CREADOR	ISACA	OGC	ISO International
¿Para qué se implementa?	Auditoría de Sistemas de Información	Gestión de Niveles de Servicio	Cumplimiento del estándar de seguridad

Fuente: Elaboración propia

Control Objectives for Information and related Technology. Desarrollado por Information Systems Audit and Control Association (ISACA). Centra su interés en la gobernabilidad, aseguramiento, control y auditoría para Tecnologías de la Información y Comunicación (TI).

Las TI están presentes en todas las áreas de las organizaciones, se hace necesario mejorar la planificación de futuras implementaciones, la compatibilidad entre sistemas y la organización del personal y de la empresa, COBIT siendo está metodología el marco de una definición de estándares y conducta profesional para la gestión y el control de las TI, en todos sus aspectos, unificando diferentes estándares, métodos de evaluación y controles anteriores.

COBIT propone 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.

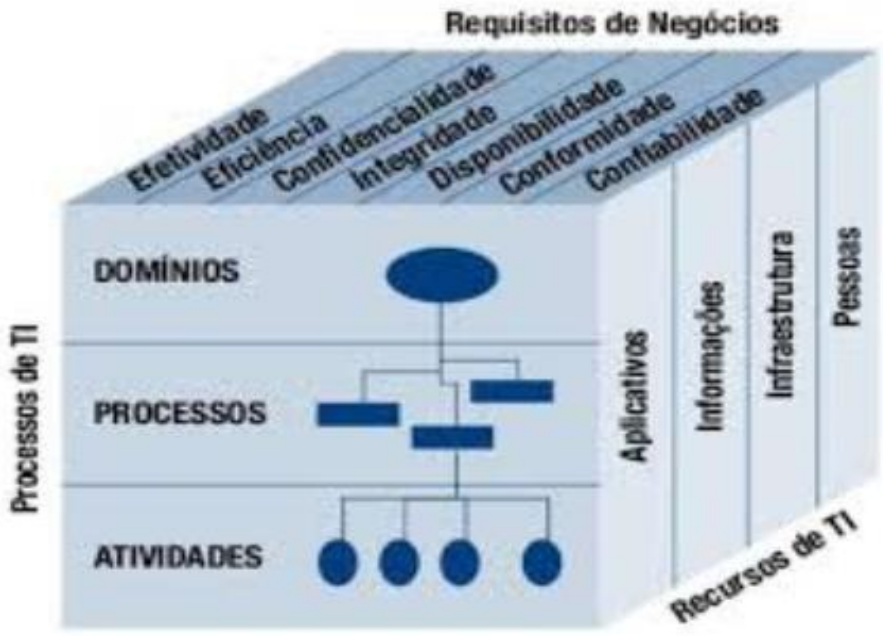
Fases en el COBIT 4.5

El marco de referencia de COBIT consta de objetivos de control de TI de alto que han sido en tres niveles de actividades de TI al considerar la administración de sus recursos estos son:

Actividades: las actividades y tareas son las acciones requeridas para lograr un resultado medible. Las actividades tienen un ciclo de vida, mientras que las tareas son más discretas.

Procesos: son conjuntos de actividades o tareas con delimitación o cortes de control**.**

Dominios: Es la agrupación natural de procesos denominador frecuentemente como dominios que corresponden a la responsabilidad organizacional. Es decir, el marco de referencia conceptual de COBIT puede ser enfocado desde tres puntos estratégicos: Criterios de información Recursos de TI Procesos de TI.



Fuente: Internet

Figura 2: *Cubo COBIT*

DOMINIOS

COBIT presenta treinta y cuatro objetivos generales, uno para cada uno de los procesos de las TI, estos procesos están agrupados en cuatro dominios como lo muestra la figura:



Fuente: Internet

Figura 3: *Dominios COBIT*

PLANEAR Y ORGANIZAR (PO)

Este Dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera que TI pueda contribuir de la mejor manera el logro de los objetivos del negocio. Además, realiza la visión Estratégica que requiere ser planeada, comunicada y administrada desde diferentes perspectivas.

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas, así como la implementación e integración en los procesos de negocio. Como también, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes informáticos.

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de los datos y de las instalaciones operacionales.

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la 15 administración del desempeño, el cumplimiento regulatorio y la aplicación del gobierno.



Fuente: Internet

Figura 4: *Principios de COBIT*

COBIT 4.5

OBJETIVOS DE CONTROL

Un objetivo de control de TI es una declaración o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de TI. Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y un número de objetivos de control detallados.

MARCO DE TRABAJO COMPLETO DE COBIT 4.5

DOMINIO: PLANEAR Y ORGANIZAR

Cuadro 5: *Cuadro comparativo Marcos de Trabajo*

DIMENSION	PROCESOS	OBJETIVO DE CONTROL
	PO1. Definir un Plan Estratégico de TI	PO1.1 Administración del Valor de TI PO1.2 Alineación de TI con el Negocio PO 1.3 Evaluación del Desempeño y la Cap. Actual PO 1.4 Plan Estratégico de TI PO 1.5 Planes Tácticos de TI PO1.6 Administración del Portafolio de TI
	PO2. Definir la Arquitectura de la Información	PO 2.1 Modelo de Arq. de Información Empresarial PO 2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos PO2.3 Esquema de Clasificación de Datos PO 2.4 Administración de Integridad.
	PO3. Determinar la Dirección **Tecnología**	PO 3.1 Planeación de la Dirección Tecnológica PO 3.2 Plan de Infraestructura Tecnológica PO 3.3 Monitoreo de Tendencias y Regulaciones Futuras PO 3.4 Estándares Tecnológicos PO 3.5 Consejo de Arquitectura de TI.
	PO4. Definir los Procesos, Organización y Relaciones de TI.	PO 4.1 Marco de Trabajo de Procesos de TI PO 4.2 Comité Estratégico de TI PO 4.3 Comité Directivo de TI PO 4.4 Ubicación Organizacional de la Función de TI PO4.5 Estructura Organizacional PO 4. 6 Establecimiento de Roles y Responsabilidades PO 4.7 Responsabilidad y Aseguramiento de Calidad de TI PO 4.8 Responsabilidad sobre el Riesgo, la

		Seguridad y el Cumplimiento. PO 4.9 Propiedad de Datos y Sistemas PO 4.10 Supervisión PO 4.11 Segregación de Funciones PO 4.12 Personal de TI PO 4.13 Personal clave de TI PO 4.14 Políticas y Procedimientos para Personal Contratado PO 4. 15 Relaciones
	PO5. Administrar la Inversión en TI.	PO 5.1 Marco de Trabajo para la administración Financiera PO 5.2 Prioridades dentro del Presupuesto de TI PO 5.3 Proceso Presupuestal PO 5.4 Administración de Costos de TI PO 5.5 Administración de Beneficios
	PO6. Comunicar las Aspiraciones y la Dirección de la Gerencia	PO 6.1 Ambiente de Políticas y de Control PO 6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI PO 6.3 Administración de Políticas para TI. PO 6.4 Implantación de Políticas de TI PO 6.5 Comunicación de los Objetivos y la Dirección de TI.
	PO7. Administrar los Recursos Humanos de TI	PO 7.1 Reclutamiento y Retención del Personal PO 7.2 Competencias del Personal PO 7.3 Asignación de Roles PO 7.4 Entrenamiento del Personal de TI PO 7.5 Dependencia sobre los individuos PO 7.6 Procedimientos de Investigación del Personal PO 7.7 Evaluación del Desempeño del Empleado

Fuente: Elaboración propia

DOMINIO: ADQUIRIR E IMPLANTAR

Cuadro 6: *Adquirir e implantar*

DOMINIO	PROCESOS	OBJETIVOS DE CONTROL
	AI1. Identificar soluciones automatizadas	AI 1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio AI 1.2 Reporte de Análisis de Riesgos AI 1.3 Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos. AI 1.4 Requerimientos, Decisión de Factibilidad y Aprobación.
	AI2. Adquirir y mantener software aplicativo	AI 2.1 Diseño de Alto Nivel AI 2.2 Diseño Detallado AI 2.3 Control y Posibilidad de Auditar las Aplicaciones AI 2.4 Seguridad y Disponibilidad de las Aplicaciones. AI 2.5 Configuración e Implantación de Software Aplicativo Adquirido AI 2.6 Actualizaciones Importantes en Sistemas Existentes. AI 2.7 Desarrollo de Software Aplicativo. AI 2.8 Aseguramiento de la Calidad del Software AI 2.9 Administración de los Requerimientos de Aplicaciones. AI 2.10 Mantenimiento de Software Aplicativo
	AI3. Adquirir y mantener infraestructura tecnológica	AI 3.1 Plan de Adquisición de Infraestructura Tecnológica AI 3.2 Protección y Disponibilidad del Recurso de Infraestructura. AI 3.4 Ambiente de Prueba de Factibilidad.
	AI4. Facilitar la operación y el uso	AI 4.1 Plan para Soluciones de Operación AI 4.2 Transferencia de Conocimiento a la Gerencia del negocio

		AI 4.3 Transferencia de Conocimiento a usuarios finales AI 4.4 Transferencia de Conocimiento al Personal de Operaciones y Soporte.
	AI5. Adquirir Recursos de TI	AI 5.1 Control de Adquisición AI 5.2 Administración de Contratos con Proveedores AI 5.3 Selección de Proveedores AI 5.4 Adquisición de Recursos de TI
	AI6. Administrar Cambios	AI 6.1 estándares y Procedimientos para Cambios AI 6.2 Evaluación de Impacto, Priorización y Autorización AI 6.3 Cambio de Emergencia AI 6.4 Seguimiento y Reporte del Estatus de Cambio AI 6.5 Cierre y Documentación del Cambio
	AI6. Administrar Cambios	AI 6.1 estándares y Procedimientos para Cambios AI 6.2 Evaluación de Impacto, Priorización y Autorización AI 6.3 Cambio de Emergencia AI 6.4 Seguimiento y Reporte del Estatus de Cambio AI 6.5 Cierre y Documentación del Cambio
	AI7. Instalar y acreditar soluciones y cambios	AI 7.1 Entrenamiento AI 7.2 Plan de Prueba AI 7.3 Plan de Implantación AI 7.4 Ambiente de Prueba AI 7.5 Conversión de Sistemas y Datos AI 7.6 Pruebas de Cambios AI 7.7 Prueba de Aceptación Final AI 7.8 Promoción a Producción AI 7.9 Revisión Posterior a la Implantación

Fuente: Elaboración propia

DOMINIO: ENTREGAR Y DAR SOPORTE

Cuadro 7: *Entregar y dar soporte*

DOMINIO	PROCESOS	OBJETIVO DE CONTROL
	DS1. Definir y administrar los niveles de servicio	DS 1.1 Marco de Trabajo de la Administración de los Niveles de Servicio DS 1.2 Definición de Servicios DS 1.3Acuerdos de Niveles de Servicio DS 1.4 Acuerdos de Niveles de Operación DS 1.5 Monitoreo y Reporte del Cumplimiento de los Niveles de Servicio DS 1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos
	DS2. Administrar los servicios de terceros	DS 2.1 Identificación de todas las relaciones con Proveedores DS 2.2 Gestión de Relaciones con Proveedores DS2.3 Administración de Riesgos del Proveedor DS 2.4 Monitoreo del Desempeño del Proveedor
	DS3. Administrar el desempeño y la capacidad	DS 3.1 Planeación del Desempeño y la Capacidad. DS 3.2 Capacidad y Desempeño Actual DS 3.3 Capacidad y Desempeño Futuros DS 3.4 Disponibilidad de Recursos de TI DS 3.5 Monitoreo y Reporte
	DS4. Garantizar la continuidad del Servicio	DS 4.1 Maco de Trabajo de Continuidad de TI Ds 4.2 Planes de Continuidad DS 4.3 Recursos Críticos de TI DS 4.4 Mantenimiento del Plan de Continuidad de TI DS 4.5 Pruebas del Plan de Continuidad de TI DS 4.6 Entrenamiento del Plan de Continuidad de TI DS 4.7 Distribución del Plan de

		Continuidad de TI DS 4.8 Recuperación y Reanudación de los Servicios de TI DS 4.9 Almacenamiento de Respaldos Fuera de las Instalaciones DS 4.10 Revisión Port Reanudación
	DS5. Garantizar la seguridad de los sistemas	DS 5.1 Administración de la Seguridad de TI DS 5.2 Plan de Seguridad de TI DS 5.3 Administración de Identidad DS 5.4 Administración de Cuentas de Usuario DS 5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad DS 5.6 Definición de Incidente de Seguridad DS 5.7 Protección de la Tecnología de Seguridad DS 5-8 Administración de las Llaves Criptográficas DS 5.9 Prevención, Detección y Corrección de Software Malicioso DS 5.10 Seguridad de la Red DS 5.11 Intercambio de servicios Sensitivos
	DS6. Identificar y asignar costos	DS 6.1 Definición de Servicios DS 6.2 Contabilización de TI DS 6.3 Modelación de Costos y Cargos DS 6.4 Mantenimiento del Modelo de Costos
	DS7. Educar y entrenar a usuarios	DS 7.1 Identificación de Necesidades de Entrenamiento y Educación DS 7.2 Impartición de Entrenamiento y Educación DS 7.3 Evaluación del Entrenamiento Recibido
	DS8. Administrar la mesa de servicio y los incidentes	DS 8.1 Mesa de Servicios DS 8.2 Registro de Consultas de Clientes DS 8.3 Escalamiento de Incidentes DS 8.4 Cierre de Incidentes DS 8.5 Análisis de Tendencias

Fuente: Elaboración propia

Propuesta de Solución

La Auditoría Informática con metodología COBIT 4.5 permitirá realizar un mejor control de registro software y hardware del área de patrimonio de la universidad nacional de Ucayali, a través de la correcta aplicación del informe de auditoría.

COBIT 4.5 consiste en vincular las metas del negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los propietarios de los procesos de negocio y TI, para ello establece vínculos con los requerimientos del negocio, organiza las actividades de TI en un modelo de procesos, identifica los principales recursos de TI y define los objetivos de control gerencial.

2.2.3. Registro de Software y Hardware

Al no encontrar un concepto adecuado se llegó a realizar un concepto propio de acuerdo a nuestro análisis de cada significado.

Deducimos que el registro de software y hardware es la relación de software y hardware en lo cual podemos acumular información detallada de los procesos que puedan estar realizando, guardar información que se requiere a lo largo del proceso de la etapa de desarrollo.

a) Manejo de información

Es un proceso que exige informarse e informar. Es decir, exige construir, primero, una representación de una determinada realidad con los datos que adquirimos de ella para poder darla a conocer, disponiendo esa representación al alcance de los demás o comunicarla (Tamara Oppenheime, 2017).

b) Fines de la adquisición

Según la real academia española es un vocablo que proviene del término latino adquisitĭo*:* la acción de conseguir una determinada cosa**,** la cosa en sí que se ha adquirido y la persona cuyos servicios o intervención están ampliamente valorados. (real academia española, 2009).

c) Hardware

Según juan cherre el hardware es el substrato físico en el cual existe el software. El hardware abarca todas las piezas físicas de un ordenador (que se pueden tocar), en el caso de una computadora personal serían los discos, unidades de disco, monitor, teclado, la placa base, el microprocesador, étc (juan cherre, 2017).

Hardware es el término inglés que hace referencia a cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora. No sólo incluye elementos internos como el disco duro, CD-ROM, disquetera, sino que también hace referencia al cableado, circuitos, gabinete, etc. E incluso hace referencia a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos (Soto Sánchez, 2018).

d) Software:

De acuerdo a, Alcalde García Eduardo. El software es un conjunto de elemento lógicos necesarios para que se pueda realizar las tareas encomendadas al mismo, se puede definir de la siguiente forma: en la parte

lógica que dota al equipo físico de capacidad para realizar cualquier tipo de trabajo (Alcalde Garcia, 1994).

De acuerdo a, Castellano Casas Ricardo. El software es el conjunto de instrucciones y datos en formato binario almacenados en la memoria principal, que le indica a una computadora que debe hacer y cómo. Es decir, el software Dirige al hardware el software es la parte lógica del sistema informático (Castellano Casas, 2001).

Según Jamrich parsons June. El software de acuerdo a su uso se clasifica en software de sistema: el software se clasifica como software de aplicación o de sistema (Jamrich parsons, 2004).

Según la real academia española el software es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora (real academia española, 2009).

CAPITULO III

METODOLOGÍA DE INVESTIGACIÓN

3.1. MÉTODO DE INVESTIGACIÓN

3.1.1. Tipo de investigación

Se desarrollará un proyecto de investigación aplicada (I), dado que se van a aplicar conocimientos científicos nuevos.

De acuerdo a Carrasco, S. (2010), será una Investigación aplicada, porque mediante este tipo de investigación aplica la ciencia para mejorar y ampliar el dominio del hombre sobre la realidad con el fin de resolver los problemas importantes del quehacer.

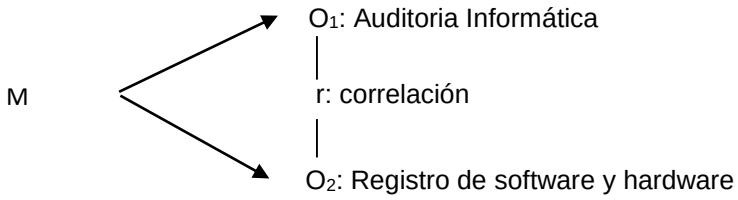
Según (Barrantes, 2008) el tipo de investigación es Investigación aplicada: Busca solucionar un problema práctico para transformar las condiciones de un hecho.

3.1.2. Nivel de Investigación

El presente estudio hará referencia al nivel Descriptivo correlacional, de corte transversal, según lo propuesto por Hernández, R; Fernández, C. & Batista, R. (2010), define que este nivel de investigación se encarga de relacionar dos o más variables dentro de un mismo contexto en un tiempo determinado (Hernández & Fernández, 2010).

3.1.3. Diseño de la investigación

El diseño de la investigación será correlacional y se esquematizará siguiendo el esquema sugerido por (Sánchez Carlessi & Reyes Meza, 1996)



Dónde:

- M: Muestra.
- O1: Variable 1. Auditoria Informática
- O2: variable 2. Registro de software y hardware
- r: Relación entre las dos variables.

3.1.4. Método de la investigación

Como método principal se utilizó el método científico.

Como métodos auxiliares se utilizó los métodos:

- **Método descriptivo.** El método descriptivo, que se orienta hacia el presente y actúa en los niveles de investigación

aplicada y activa, intenta una observación sistemática, estudiando la realidad educativa tal y como se desarrolla. (Serrano, 2000).

- **Método inductivo.** Con este método se utiliza el razonamiento para obtener conclusiones que parten de hechos particulares aceptados como válidos, para llegar a conclusiones, cuya aplicación sea de carácter general. (Torres, 2006).

3.2. POBLACIÓN Y MUESTRA.

3.2.1. Población

Según Carrasco, S. (2010), la Población es un conjunto de elementos que forman parte del espacio territorial al que pertenece el problema de investigación y poseen características mucho más concretas que el universo. (Carrasco Díaz, 2010).

Para llevar a cabo esta investigación la población serán los 4 trabajadores del área de patrimonio y los 4 trabajadores de la oficina general de tecnologías de información, sistemas y estadística (OGTISE) Universidad Nacional de Ucayali.

3.2.1. Muestra

La muestra es un fragmento representativo de la población, que debe poseer las mismas propiedades y características de ella, Para ser objetiva requiere ser seleccionada con técnicas adecuadas. (Carrasco Díaz, 2010).

Sin embargo, existen unidades de estudio que no requieren ningún tipo de muestreo al respecto De Barrera (2008), expresa que:

No hace falta hacer un muestreo cuando:

- La población es conocida y se puede identificar a cada uno de sus integrantes (…).
- La población, además de ser conocida es accesible, es decir, es posible ubicar a todos los miembros (…).
- La población es relativamente pequeña, de modo que puede ser abarcada en el tiempo y con los recursos del investigador.

En base a ello la muestra es del mismo tamaño de la población.

Población:

8 personas

Muestra:

Método no probabilístico, muestreo por conveniencia:

Si la muestra < 30

$\Rightarrow$ Muestra = Población

8 personas

3.3. PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS

3.3.1. Técnicas de recolección de datos

En opinión de (Rodríguez Sosa & Rodríguez Rivas, 1990) las técnicas, son los medios empleados para recolectar información, entre las que destacan la observación, cuestionario, entrevistas (Sosa & Rodríguez , 1990).

Las técnicas que se utilizará en esta investigación son:

La observación.

En opinión de (Ruiz Medina, 2017), quien cita a Sabino (1992:111-113), la observación es una técnica antiquísima, cuyos primeros aportes sería imposible rastrear. A través de sus sentidos, el hombre capta la realidad que lo rodea, que luego organiza intelectualmente y agrega: La observación se define, como el uso sistemático de nuestros sentidos en la búsqueda de los datos que necesitamos para resolver un problema de investigación (Medina, 2017).

La observación es directa cuando el investigador forma parte activa del grupo observado y asume sus comportamientos; recibe el nombre de observación participante. Cuando el observador no pertenece al grupo y sólo se hace presente con el propósito de obtener la información (como en este caso), la observación, recibe el nombre de no participante o simple.

Cuestionario

El cuestionario, es un procedimiento que permite explorar cuestiones que hacen a la subjetividad y al mismo tiempo obtener esa información de un número considerable de personas, así, por ejemplo:

Permite explorar la opinión pública y los valores vigentes de una sociedad, temas de significación científica y de importancia en las sociedades democráticas (Grasso, 2006:13), citado por (Ruiz Medina, 2017).

3.3.2. Instrumentos de recolección de datos

Encuesta. A diferencia de un censo, donde todos los miembros de la población son estudiados, los cuestionarios recopilan información de una porción de la población de interés, dependiendo del tamaño de la muestra en el propósito del estudio. La información se recoge usando procedimientos estandarizados de manera que a cada individuo se les hacen las mismas preguntas, más o menos de la misma manera. La intención de la ladera no es describir a los individuos particulares, quienes por azar, son parte de la muestra, sino obtener un perfil compuesto de la población (juan, 2008).

3.4. TÉCNICAS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS

Se utilizarán 2 tipos de fuentes de información: Primaria y secundaria, la cuales se van a detallar que técnicas e instrumentos se utilizarán en el siguiente cuadro.

FUENTES	TIPO DE INVESTIGACIÓN	TÉCNICAS	INSTRUMENTO
Primarias	Aplicada	Encuestas	Cuestionario
Secundarias	Aplicada	Observación	Ficha de observación
Primarias	Aplicada	Fichas (Textuales y de resumen)	Referencias bibliográficas
Secundarias	Aplicada		Internet
Primarias	Aplicada		Libros

Fuente: elaboración propia

Figura 5: *Instrumento de recolección de datos*

3.5. PROCESAMIENTO PARA RECOLECCIÓN DE DATOS

Estrategias

En la utilización de los recursos para el procesamiento de información se necesitará la colaboración de 1 digitador, sillas, mesas y el software IBM SPSS.

Y en los recursos logísticos, para la ejecución del plan de procesamiento se utilizará 1 computadora. La encuesta se va a realizar en un solo día, se dará inicio a las ocho de la mañana a doce del mediodía, es decir se tendrá un tiempo de tres horas para terminar la encuesta, para posteriormente comenzar con el procesamiento de datos.

3.6. TRATAMIENTO DE DATOS

MICROSOFT EXCEL

Según Iván Uscanga es un programa de hoja de cálculo de Microsoft Office system. Permite crear y aplicar formato a libros (un conjunto de hojas de cálculo) para analizar datos y tomar decisiones fundadas sobre aspectos de su negocio. En concreto, se puede utilizar para hacer un seguimiento de datos, crear modelos para analizar datos, escribir fórmulas para realizar cálculos con tales datos, dinamizar los datos de diversas maneras y presentarlos en una variedad de gráficos con aspecto profesional (CRUZ, 2009).

IBM SPSS Statistics

Es un software estadístico líder de mercado, en el mundo usado para solucionar una amplia variedad de problemas de negocios y de investigación. Ofrece un amplio conjunto de recursos, incluyendo análisis ad hoc, pruebas de hipótesis e informes, facilitando la gestión de datos, la selección y ejecución de análisis y el intercambio de sus resultados (IBM, 2017).

Coeficiente de correlación por jerarquías de Spearman (Rho de Spearman). Es una medida de asociación lineal que utiliza los rangos, números de orden, de cada grupo de sujetos y compara dichos rangos. Éste coeficiente es muy útil cuando el número de pares de sujetos (n) que se desea asociar es pequeño (menor de 30). Aparte de permitir conocer el grado de asociación entre ambas variables, con Rho de Spearman es posible determinar la dependencia o independencia de dos variables aleatorias (Mondragon Barrera, 2014).

RANGO	RELACIÓN
-0.91 a -1.00	Correlación negativa perfecta
-0.76 a -0.90	Correlación negativa muy fuerte
-0.51 a -0.75	Correlación negativa considerable
-0.11 a -0.50	Correlación negativa media
-0.01 a -0.10	Correlación negativa débil
0.00	No existe correlación
+0.01 a +0.10	Correlación positiva débil
+0.11 a +0.50	Correlación positiva media
+0.51 a +0.75	Correlación positiva considerable
+0.76 a +0.90	Correlación positiva muy fuerte
+0.91 a +1.00	Correlación positiva perfecta

Fuente: Elaboración propia, basada en Hernández Sampieri & Fernández Collado, 1998.

Fuente: Internet

***Figura 6**: Esquema de correlación de sampieri*

CAPITULO IV

RESULTADOS

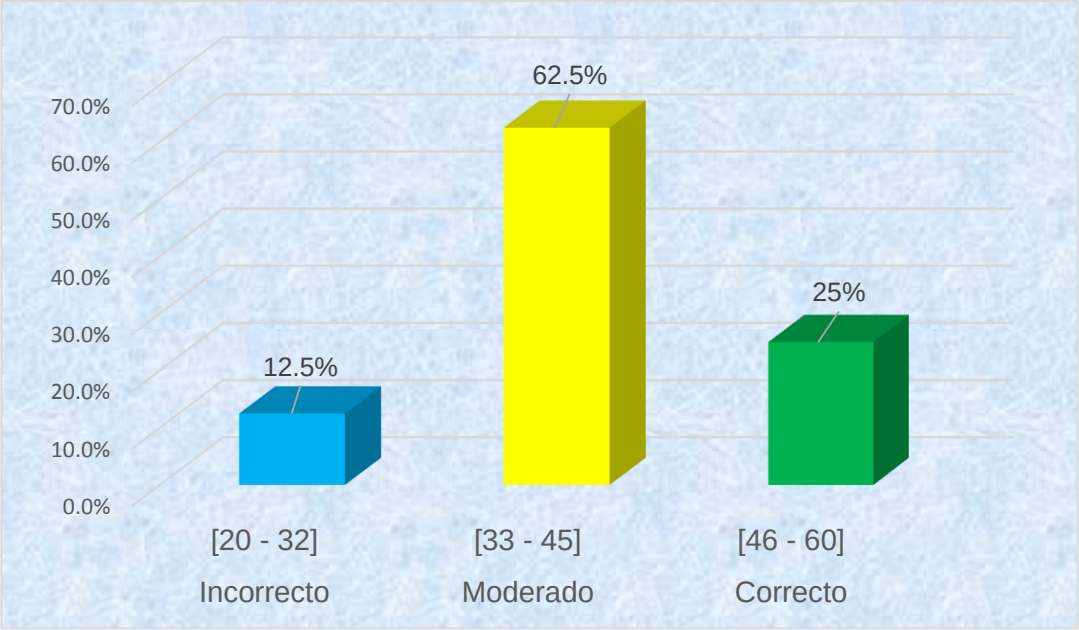
En la descripción de resultados se muestra la información recopilada a través de la encuesta aplicada a la muestra de trabajadores administrativos del área de patrimonio y de Informática de la universidad nacional de Ucayali, cuyas respuestas procesadas y analizadas nos brindan la siguiente realidad:

4.1. PROCESAMIENTO DE LA VARIABLE AUDITORIA NFORMÁTICA

Tabla 1: *Auditoria informática*

Auditoria Informática		fi	Fi	hi%	Hi%
Incorrecto	[20 - 32]	1	1	12.5%	12.5%
Moderado	[33 - 45]	5	6	62.5%	75%
Correcto	[46 - 60]	2	8	25%	100%
Total		*8*		*100%*	

Fuente: Base de datos. Anexo 2



Fuente: Tabla 1. Auditoria informática

Figura 7: *Auditoria informática*

Descripción.

Luego de aplicar la encuesta, y en base a la Tabla 1 y figura 7, se afirma que el 12,5% de los encuestados indican que la Auditoria informática es incorrecta, mientras que el 62,5%, manifiestan que es moderado, y el 25% de las personas encuestadas afirman que es correcta.

4.1.1. Procesamiento de datos de la dimensión informe preliminar

Tabla 2: *Dimensión Informe preliminar*

Informe preliminar o de datos		fi	Fi	hi%	Hi%
Incorrecto	[6 - 9]	1	1	12.5%	12.5%
Moderado	[10 - 13]	3	4	37.5%	50%
Correcto	[14 - 18]	4	8	50%	100%
Total		8		100%	

Fuente: Base de datos. Anexo 2

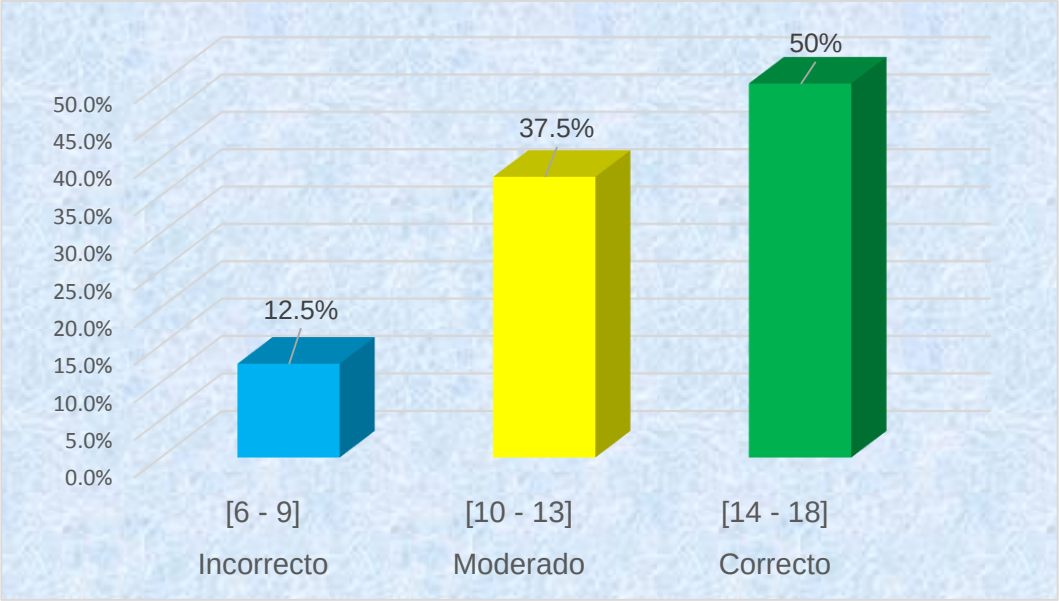


Figura: Tabla 2. Dimensión Informe preliminar

Figura 8: *Dimensión Informe preliminar*

Descripción.

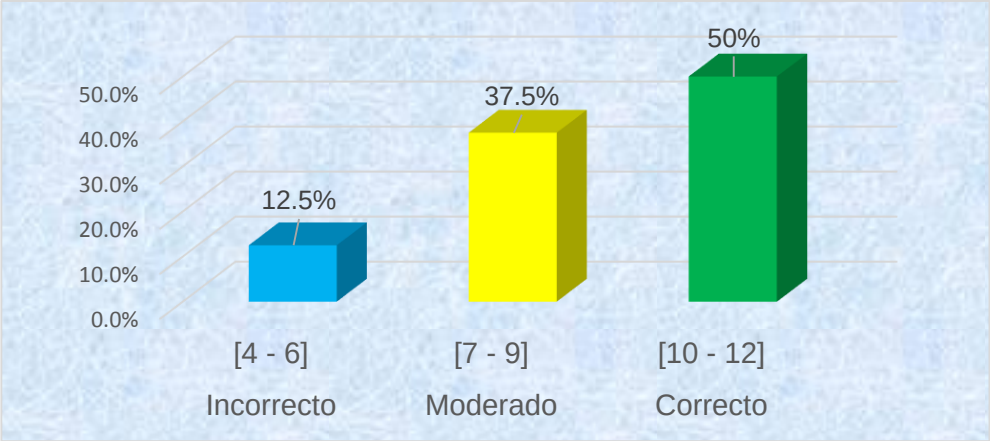
El siguiente punto trata, y en base a la Tabla 2 y figura 8, se afirma que el 12,5% de los encuestados indican que la dimensión Informe preliminar de la variable Auditoria informática es incorrecta, mientras que el 37.5%, manifiestan que es moderado, y el 50% de las personas encuestadas afirman que es correcta.

4.1.2. Procesamiento de datos de la dimensión Análisis de la situación actual

Tabla 3: *Dimensión análisis de la situación actual*

Análisis de la situación actual		fi	Fi	hi%	Hi%
Incorrecto	[4 - 6]	1	1	12.5%	12.5%
Moderado	[7 - 9]	3	4	37.5%	50%
Correcto	[10 - 12]	4	8	50%	100%
Total		8		100%	

Fuente: Base de datos. Anexo 2



Fuente: Dimensión análisis de la situación actual

***Figura 9**: Dimensión análisis de la situación actual*

Descripción.

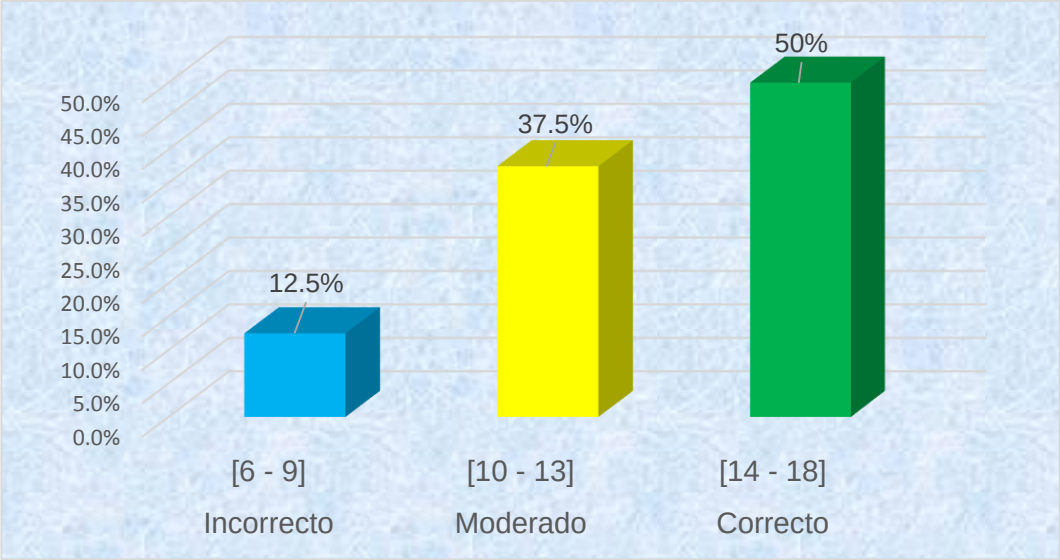
Ahora veamos, en base a la Tabla 3 y figura 9, se afirma que el 12,5% de los encuestados indican que la dimensión análisis de la situación actual de la variable Auditoria informática es incorrecta, mientras que el 37.5%, manifiestan que es moderado, y el 50% de las personas encuestadas afirman que es correcta.

4.1.3. Procesamiento de datos de la dimensión Control y gestión de la Información

***Tabla 4:** Dimensión Control y gestión de la información*

Control y gestión de la información		fi	Fi	hi%	Hi%
Incorrecto	[6 - 9]	1	1	12.5%	12.5%
Moderado	[10 - 13]	3	5	37.5%	50%
Correcto	[14 - 18]	4	13	50%	100%
Total		8		100%	

Fuente: Base de datos. Anexo 2



Fuente: Tabla 4. Dimensión Control y gestión de la información

Figura 9: *dimensión control y gestión de la información*

Descripción.

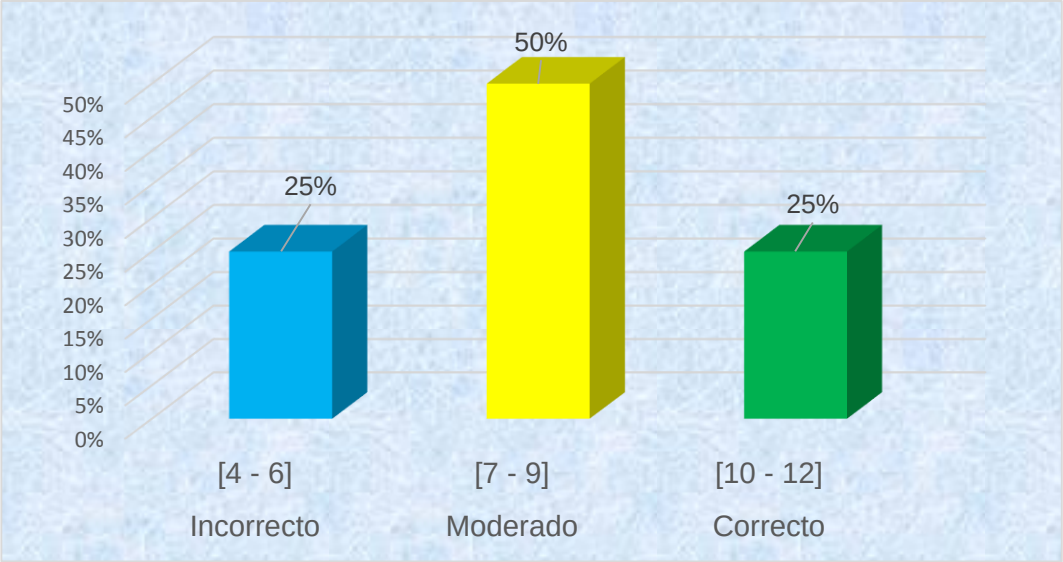
Ahora veamos, en base a la Tabla 4 y figura 10, se afirma que el 12,5% de los encuestados indican que la dimensión Control y gestión de la información de la variable Auditoria informática es incorrecta, mientras que el 37.5%, manifiestan que es moderado, y el 50% de las personas encuestadas afirman que es correcta.

4.1.4. Procesamiento de datos de la dimensión del informe final

Tabla 5: *Dimensión informe final*

Informe final		fi	Fi	hi%	Hi%
Incorrecto	[4 - 6]	2	2	25%	25%
Moderado	[7 - 9]	4	6	50%	75%
Correcto	[10 - 12]	2	8	25%	100%
Total		8		100%	

Fuente: Base de datos. Anexo 2



Fuente: Tabla 5. Dimensión informe final

Figura 10: *Dimensión informe final*

Descripción.

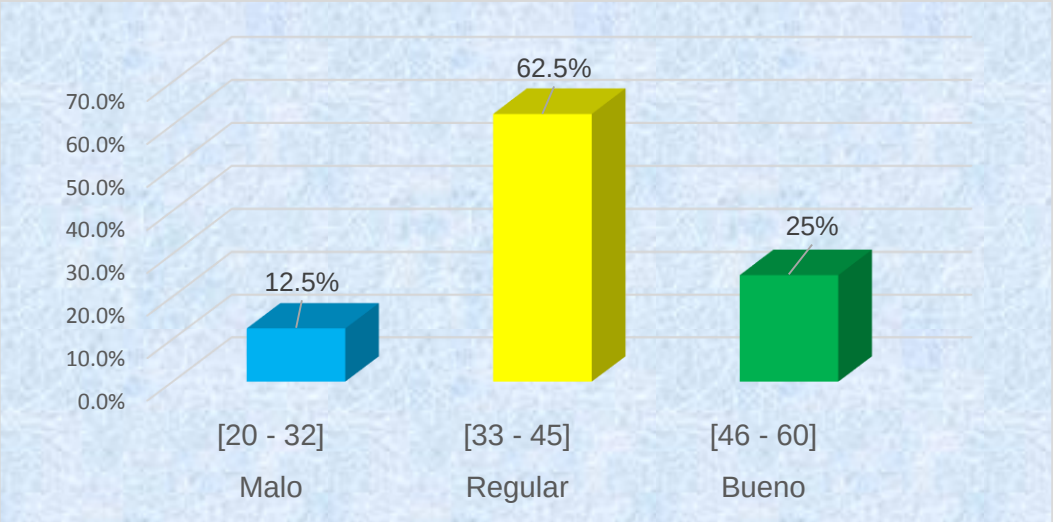
Ahora puedo decir, en función a la Tabla 5 y figura 11, se afirma que el 25% de los encuestados indican que la dimensión informe final de la variable Auditoria informática es incorrecta, mientras que el 50 %, manifiestan que es moderado, y el 25% de las personas encuestadas afirman que es correcta.

4.2. PROCESAMIENTO DE DATOS DE LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE

Tabla 6: *Variable Registro de Software y Hardware*

Registro de software y hardware		fi	Fi	hi%	Hi%
Malo	[20 - 32]	1	1	12.5%	12.5%
Regular	[33 - 45]	5	6	62.5%	75%
Bueno	[46 - 60]	2	8	25%	100%
Total		8		100%	

Fuente: Base de datos. Anexo 2



Fuente: Tabla 6. Variable Registro de Software y Hardware

Figura 11: *Variable Registro de Software y Hardware*

Descripción.

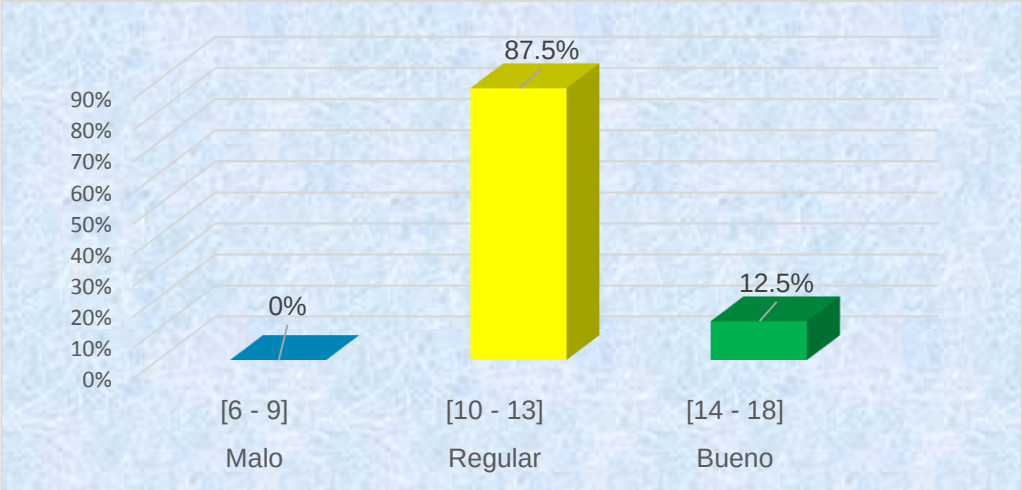
El siguiente aspecto tratamos en base a la Tabla 6 y figura 12, se afirma que el 12,5% de los encuestados indican que la Variable Registro de Software y Hardware es malo, mientras que el 62.5 %, manifiestan que es regular, y el 25% de las personas encuestadas afirman que es bueno.

4.2.1. Procesamiento de datos de la dimensión manejo de información de software y hardware

Tabla 7: *Dimensión manejo de información de software y hardware*

Manejo de información de software y hardware		fi	Fi	hi%	Hi%
Malo	[6 - 9]	0	0	0%	0%
Regular	[10 - 13]	7	7	87.5%	87.5%
Bueno	[14 - 18]	1	8	12.5%	100%
Total		8		100%	

Fuente: Base de datos. Anexo 2



Fuente: tabla 7. Dimensión manejo de información de software y hardware

Figura 12: *Dimensión manejo de información de software y hardware*

Descripción.

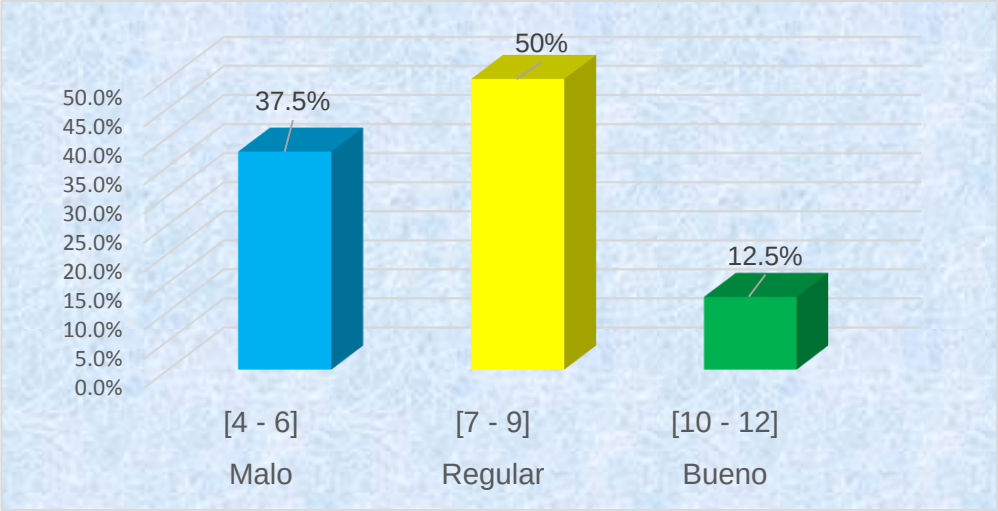
Se debe agregar, en base a la Tabla 7 y figura 13, se afirma que no existe encuestados que indican que la Dimensión manejo de información de software y hardware de la Variable Registro de Software y Hardware es malo, mientras que el 87.5 %, manifiestan que es regular, y el 12,5% de las personas encuestadas afirman que es bueno.

4.2.2. Procesamiento de datos de la dimensión fines de la Adquisición

Tabla 8: *Dimensión fines de la adquisición*

Fines de la adquisición		fi	Fi	hi%	Hi%
Malo	[4 - 6]	3	3	37.5%	37.5%
Regular	[7 - 9]	4	7	50%	87.5%
Bueno	[10 - 12]	1	8	12.5%	100%
Total		8		100%	

Fuente: Base de datos. Anexo 2



Fuente: Tabla 8. Dimensión fines de la adquisición

Figura 13: *Dimensión fines de la adquisición*

Descripción.

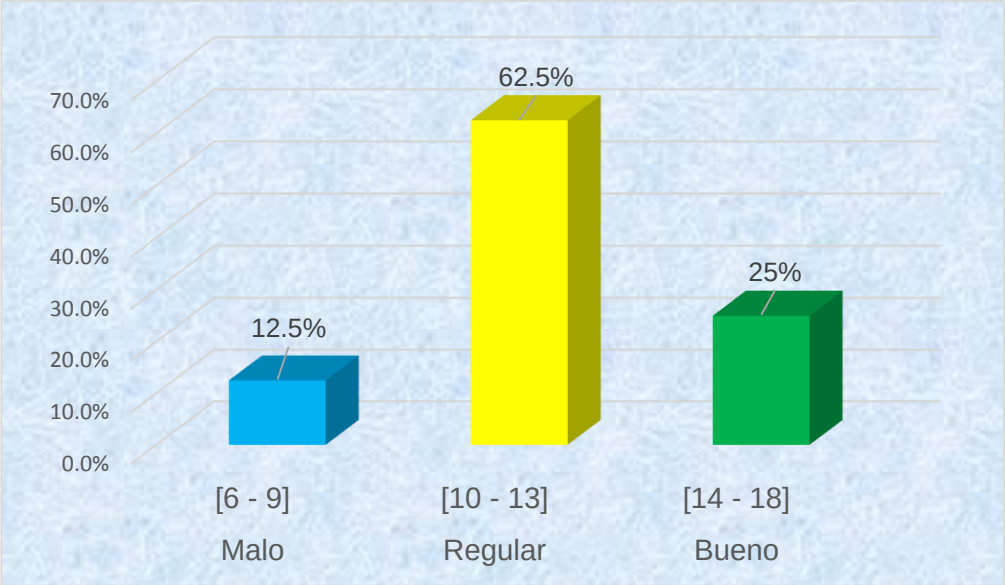
En lo que toca a, la Tabla 8 y figura 14, los encuestados afirma con un 37.5% que la Dimensión fines de la adquisición de la Variable Registro de Software y Hardware es malo, mientras que el 50 %, manifiestan que es regular, y el 12,5% de las personas encuestadas afirman que es bueno.

4.2.3. Procesamiento de datos de la dimensión Software

Tabla 9: *Dimensión Software*

Software		fi	Fi	hi%	Hi%
Malo	[6 - 9]	1	1	12.5%	12.5%
Regular	[10 - 13]	5	6	62.5%	75%
Bueno	[14 - 18]	2	8	25%	100%
Total		8		100%	

Fuente: Base de datos. Anexo 2



Fuente: Tabla 9. Dimensión Software

***Figura 14**: Dimensión Software*

Descripción.

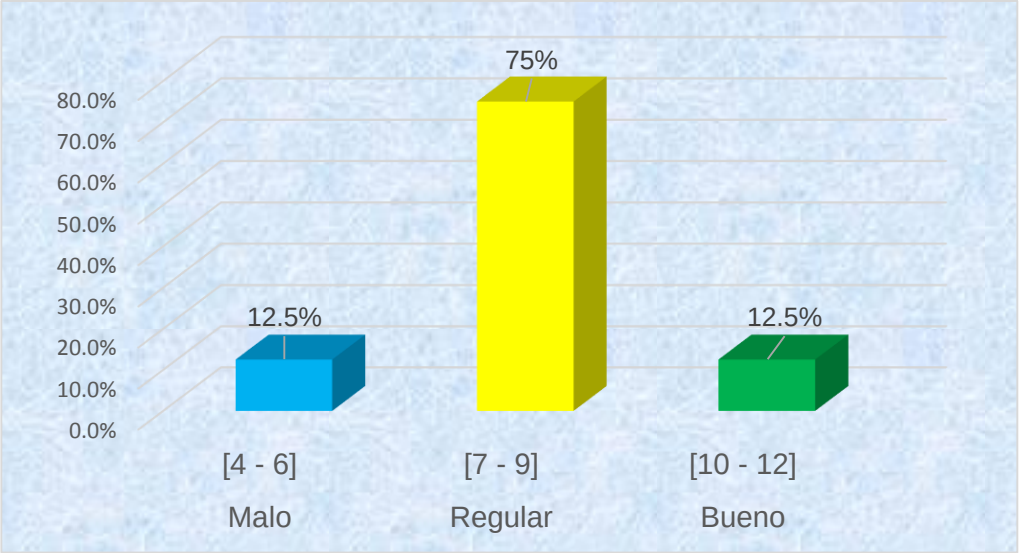
En lo que toca a, la Tabla 9 y figura 15, los encuestados afirma con un 12.5% que la Dimensión software de la Variable Registro de Software y Hardware es malo, mientras que el 62.5 %, manifiestan que es regular, y el 25% de las personas encuestadas afirman que es bueno.

4.2.4. Procesamiento de datos de la dimensión hardware

***Tabla 10:** Dimensión hardware*

Hardware		fi	Fi	hi%	Hi%
Malo	[4 - 6]	1	1	12.5%	12.5%
Regular	[7 - 9]	6	7	75%	87.5%
Bueno	[10 - 12]	1	8	12.5%	100%
Total		8		100%	

Fuente: Base de datos. Anexo 2



Fuente: Tabla 10. Dimensión hardware

Figura 15: *Dimensión hardware*

Descripción.

En lo que toca a, la Tabla 10 y figura 16, los encuestados afirma con un 12.5% que la Dimensión hardware de la Variable Registro de Software y Hardware es malo, mientras que el 75 %, manifiestan que es regular, y el 12.5% de las personas encuestadas afirman que es bueno.

4.3. PRUEBA DE HIPÓTESIS.

La prueba de hipótesis es un procedimiento que conduce a una decisión sobre una hipótesis en particular, entonces recibe el nombre de prueba de hipótesis. Los procedimientos de prueba de hipótesis dependen del empleo de la información contenida en la muestra aleatoria de la población de interés. Los pasos a seguir para la prueba de hipótesis está en base, a (Córdova Zamora, 1999), quien establece que:

- Redactar las hipótesis
- Determinar el nivel α.
- Elección de la prueba estadística.
- Lectura del P – valor.

- Aplicación de la prueba estadística.

4.3.1. Prueba de la hipótesis general

I. Redacción de hipótesis

Ho: La Auditoria Informática con metodología COBIT 4.5 no, se relaciona directamente, con el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

H1: La Auditoria Informática con metodología COBIT se relaciona directamente, con el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

II. Determinar el nivel de Alfa

El nivel de significancia: $\alpha = 5\% = 0{,}05$.

III. Elección de la prueba estadística

Es un estudio trasversal, en la que se aplicó la prueba de Correlación de Rho de Spearman.

- **Lectura de P – Valor. Normalidad** se debe de corroborar que la variable aleatoria en ambos grupos se distribuye normalmente. Para ello se utilizara la prueba de Shapiro-Wilk, por que el tamaño de la muestra es menor a 30 individuos. El criterio para determinar si la (VA) se distribuye normalmente es:

a) **P–valor$> \alpha$. Aceptar la Ho =** Los datos provienen de una distribución normal.

b) **P–valor$\leq \alpha$. Aceptar la H_1 =** Los datos no provienen de una distribución normal.

Tabla 11: *Prueba de normalidad Shapiro-Wilk.*

Pruebas de normalidad							
		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Hipótesis general	Estadístico	gl	Sig.	Estadístico	gl	Sig.
	Auditoria informática	,233	8	,200*	,940	8	,610
	Registro de Software	,191	8	,200*	,936	8	,568
*. Esto es un límite inferior de la significación verdadera.							
a. Corrección de significación de Lilliefors							

Fuente: Base de datos, Anexo N° 2

Tabla 12*: Toma de decisión de la hipótesis general*

P–valor de la variable Auditoria Informática = 0.610	>	0.05
P–valor de la variable Registro de software y hardware.= 0.568	>	0.05
Conclusión: Las variables: Auditoria Informática y Registro de software y hardware, se comporta normalmente por lo que se confirma la aplicación de la prueba de Rho de Spearman.		

Fuente: Tabla 11

IV. Aplicación de la prueba de Rho de Spearman

Tabla 13: *Prueba de Correlación de Rho de Spearman.*

Correlaciones				
			Auditoria Informática	Registro de software y hardware
Rho de Spearman	Auditoria Informática	Coeficiente de correlación	1,000	,739*
		Sig. (bilateral)	.	,036
		N	8	8
	Registro de software y hardware	Coeficiente de correlación	,739*	1,000
		Sig. (bilateral)	,036	.
		N	8	8
*. La correlación es significativa en el nivel 0,05 (bilateral).				

Fuente: Base de datos, Anexo N° 2

V. Toma de decisión

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y Registro de software y hardware.

Además, basándonos en la tabla N° 11. Afirmamos que el p valor (Sig.) 0.036, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.74. Indica que existe un grado de Correlación positiva considerable entre las variables: Auditoria Informática y registro de software y Hardware.

4.3.2. Prueba de la hipótesis especifica 1

I. Redacción de hipótesis

Ho: La Auditoria Informática con metodología COBIT no, se relaciona directamente, con el Manejo de información de software y hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

H1: La Auditoria Informática con metodología COBIT se relaciona directamente, con el Manejo de información de software y hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

II. Determinar el nivel de Alfa.

El nivel de significancia: $\alpha = 5\% = 0{,}05$.

III. Elección de la prueba estadística

Es un estudio trasversal, en la que se aplicó la prueba de Correlación de Rho de Spearman.

- **Lectura de P – Valor. Normalidad** se debe de corroborar que la variable aleatoria en ambos grupos se distribuye normalmente. Para ello se utilizara la prueba de Shapiro-Wilk, por que el tamaño de la muestra es menor a 30 individuos. El criterio para determinar si la (VA) se distribuye normalmente es:

a) **P–valor$> \alpha$. Aceptar la Ho =** Los datos provienen de una distribución normal.

b) **P–valor$\leq \alpha$. Aceptar la H_1 =** Los datos no provienen de una distribución normal.

Tabla 14: *Prueba de normalidad Shapiro-Wilk.*

Pruebas de normalidad							
		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Hipótesis Especifica 1	Estadístico	Gl	Sig.	Estadístico	gl	Sig.
	Auditoria informática	,233	8	,200*	,940	8	,610
	Manejo de información de software y hardware	,330	8	,010*	,858	8	,114
*. Esto es un límite inferior de la significación verdadera.							
a. Corrección de significación de Lilliefors							

Fuente: Base de datos, Anexo N° 2

Tabla 15: *Toma de decisión de la hipótesis especifica 1*

P–valor de la variable Auditoria Informática = 0.610	>	0.05
P–valor de la Dimensión manejo de información de software y hardware= 0.114	>	0.05
Conclusión: La variable: Auditoria Informática y la dimensión Manejo de información de software y hardware, se comporta normalmente por lo que se confirma la aplicación de la prueba de Rho de Spearman.		

Fuente: Tabla 14

IV. Aplicación de la prueba de Rho de Spearman

Tabla 16: *Prueba de Correlación de Rho de Spearman, de la hipótesis especifica 1*

Correlaciones				
			Auditoria Informática	Manejo de información de software y hardware
Rho de Spearman	Auditoria Informática	Coeficiente de correlación	1,000	,707
		Sig. (bilateral)	.	,0498
		N	8	8
	Manejo de información de software y hardware	Coeficiente de correlación	,707	1,000
		Sig. (bilateral)	,0498	.
		N	8	8

Fuente: Base de datos, Anexo N° 2

V. Toma de decisión.

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y la dimensión manejo de información de software y hardware.

Además, basándonos en la tabla N° 16. Afirmamos que el p valor (Sig.) 0.0498, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT se relaciona directamente, con el Manejo de información de software y hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.71. Indica que existe un grado de Correlación positiva considerable entre la variable Auditoria Informática y la dimensión Manejo de información de software y hardware.

4.3.3. Prueba de la hipótesis especifica 2

I. Redacción de hipótesis

Ho: La Auditoria Informática con metodología COBIT no se relaciona directamente, con los fines de la adquisición del área de patrimonio de la universidad Nacional de Ucayali, 2017.

H1: La Auditoria Informática con metodología COBIT se relaciona directamente, con los fines de la adquisición del área de patrimonio de la universidad Nacional de Ucayali, 2017.

II. Determinar el nivel de Alfa.

El nivel de significancia: $\alpha = 5\% = 0{,}05$.

III. Elección de la prueba estadística

Es un estudio trasversal, en la que se aplicó la prueba de Correlación de Rho de Spearman.

- **Lectura de P – Valor. Normalidad** se debe de corroborar que la variable aleatoria en ambos grupos se distribuye normalmente. Para ello se utilizara la prueba de Shapiro-Wilk, por que el tamaño de la muestra es menor a 30 individuos. El criterio para determinar si la (VA) se distribuye normalmente es:

  a) **P–valor** $> \alpha$**. Aceptar la Ho =** Los datos provienen de una distribución normal.

b) **P–valor≤ α. Aceptar la H_1 =** Los datos no provienen de una distribución normal.

Tabla 17: *Prueba de normalidad Shapiro-Wilk.*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Hipótesis Especifica 2	Estadístico	Gl	Sig.	Estadístico	gl	Sig.
Auditoria informática	,233	8	,200*	,940	8	,610
Fines de la adquisición	,257	8	,0127*	,848	8	,091
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Fuente: Base de datos, Anexo N° 2

Tabla 18: *Toma de decisión de la hipótesis especifica 2*

P–valor de la variable Auditoria Informática = 0.610	>	0.05
P–valor de la Dimensión Fines de la adquisición = 0.091	>	0.05
Conclusión: La variable: Auditoria Informática y la dimensión Fines de la adquisición, se comporta normalmente por lo que se confirma la aplicación de la prueba de Rho de Spearman.		

Fuente: Tabla 1

IV. Aplicación de la prueba de Rho de Spearman

Tabla 19: *Prueba de Correlación de Rho de Spearman, de la hipótesis Especifica 2*

Correlaciones				
			Auditoria Informática	Fines de la adquisición
Rho de Spearman	Auditoria informática	Coeficiente de correlación	1,000	,646
		Sig. (bilateral)	.	,043
		N	8	8
	Fines de la adquisición	Coeficiente de correlación	,646	1,000
		Sig. (bilateral)	,043	.
		N	8	8

Fuente: Base de datos, Anexo N° 2

V. Toma de decisión.

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y la dimensión Fines de la adquisición.

Además, basándonos en la tabla N° 19. Afirmamos que el p valor (Sig.) 0.043, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT se relaciona directamente, con los fines de la adquisición del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.646. Indica que existen un grado de Correlación positiva considerable entre la variable Auditoria Informática y la dimensión fines de la adquisición.

4.3.4. Prueba de la hipótesis especifica 3

I. Redacción de hipótesis

Ho: La Auditoria Informática con metodología COBIT no, se relaciona directamente, con el software del área de patrimonio de la universidad Nacional de Ucayali, 2017.

H1: La Auditoria Informática con metodología COBIT se relaciona directamente, con el software del área de patrimonio de la universidad Nacional de Ucayali, 2017.

II. Determinar el nivel de Alfa.

El nivel de significancia: $\alpha = 5\% = 0{,}05$.

III. Elección de la prueba estadística

Es un estudio trasversal, en la que se aplicó la prueba de Correlación de Rho de Spearman.

- **Lectura de P – Valor. Normalidad** se debe de corroborar que la variable aleatoria en ambos grupos se distribuye normalmente. Para ello se utilizara la prueba de Shapiro-Wilk, porque el tamaño de la muestra es menor a 30 individuos. El criterio para determinar si la (VA) se distribuye normalmente es:

  a) **P–valor** $> \alpha$**. Aceptar la Ho =** Los datos provienen de una distribución normal.

b) **P–valor≤ α. Aceptar la H_1 =** Los datos no provienen de una distribución normal.

Tabla 20: *Prueba de normalidad Shapiro-Wilk.*

Pruebas de normalidad							
		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Hipótesis Especifica 2	Estadístico	gl	Sig.	Estadístico	gl	Sig.
	Auditoria informática	,233	8	,200*	,940	8	,610
	Software	,222	8	,200*	,886	8	,217
*. Esto es un límite inferior de la significación verdadera.							
a. Corrección de significación de Lilliefors							

Fuente: Base de datos, Anexo N° 2

Tabla 21: *Toma de decisión de la hipótesis especifica 3*

P–valor de la variable Auditoria Informática = 0.610	>	0.05
P–valor de la Dimensión Fines de la adquisición = 0.217	>	0.05
Conclusión: La variable: Auditoria Informática y la dimensión Software, se comporta normalmente por lo que se confirma la aplicación de la prueba de Rho de Spearman.		

Fuente: Tabla 20

IV. Aplicación de la prueba de Rho de Spearman

Tabla 22: *Prueba de Correlación de Rho de Spearman, de la hipótesis especifica 3*

Correlaciones				
			Auditoria Informática	Software
Rho de Spearman	Auditoria Informática	Coeficiente de correlación	1,000	,379
		Sig. (bilateral)	.	,034
		N	8	8
	Software	Coeficiente de correlación	,379	1,000
		Sig. (bilateral)	,034	.
		N	8	8

Fuente: Base de datos, Anexo N° 2

V. Toma de decisión.

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y la dimensión Software.

Además, basándonos en la tabla N° 22. Afirmamos que el p valor (Sig.) 0.034, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT se relaciona directamente, con el software del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.38. Indica que existe un grado de Correlación positiva media entre la variable Auditoria Informática y la dimensión software.

4.3.5. Prueba de la hipótesis especifica 4

I. Redacción de hipótesis

Ho: La Auditoria Informática con metodología COBIT no, se relaciona directamente, con el hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

H1: La Auditoria Informática con metodología COBIT se relaciona directamente, con el hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

II. Determinar el nivel de Alfa

El nivel de significancia: $\alpha = 5\% = 0{,}05$.

III. Elección de la prueba estadística

Es un estudio trasversal, en la que se aplicó la prueba de Correlación de Rho de Spearman.

- **Lectura de P – Valor. Normalidad** se debe de corroborar que la variable aleatoria en ambos grupos se distribuye normalmente. Para ello se utilizara la prueba de Shapiro-Wilk, por que el tamaño de la muestra es menor a 30 individuos. El criterio para determinar si la (VA) se distribuye normalmente es:

  a) **P–valor**$> \alpha$**. Aceptar la Ho =** Los datos provienen de una distribución normal.

b) **P–valor≤ α. Aceptar la H_1 =** Los datos no provienen de una distribución normal.

Tabla 23: *Prueba de normalidad Shapiro-Wilk.*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
Hipótesis Especifica 2	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Auditoria informática	,233	8	,200*	,940	8	,610
Hardware	,193	8	,200*	,994	8	,651
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Fuente: Base de datos, Anexo N° 2

Tabla 24: *Toma de decisión de la hipótesis especifica 4*

P–valor de la variable Auditoria Informática = 0.610	>	0.05
P–valor de la Dimensión Fines de la adquisición = 0.651	>	0.05
Conclusión: La variable: Auditoria Informática y la dimensión Hardware, se comporta normalmente por lo que se confirma la aplicación de la prueba de Rho de Spearman.		

Fuente: Tabla 23

IV. Aplicación de la prueba de Rho de Spearman

Tabla 25: *Prueba de Correlación de Rho de Spearman, de la hipótesis especifica 4*

Correlaciones				
			Auditoria Informática	Hardware
Rho de Spearman	Auditoria Informática	Coeficiente de correlación	1,000	,815*
		Sig. (bilateral)	.	,014
		N	8	8
	Hardware	Coeficiente de correlación	,815*	1,000
		Sig. (bilateral)	,014	.
		N	8	8
*. La correlación es significativa en el nivel 0,05 (bilateral).				

V. Toma de decisión.

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y la dimensión Hardware.

Además, basándonos en la tabla N° 25. Afirmamos que el p valor (Sig.) 0.014, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.82. Indica que existe un grado de Correlación positiva muy fuerte entre la variable Auditoria Informática y la dimensión hardware.

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y Registro de software y hardware.

Además, basándonos en la tabla N° 11. Afirmamos que el p valor (Sig.) 0.036, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.74. Indica que existe un grado de Correlación positiva considerable entre las variables: Auditoria Informática y registro de software y Hardware.

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y la dimensión manejo de información de software y hardware.

Además, basándonos en la tabla N° 16. Afirmamos que el p valor (Sig.) 0.0498, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el Manejo de información de software y hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.71. Indica que existe un grado de Correlación positiva considerable entre la

variable Auditoria Informática y la dimensión Manejo de información de software y hardware.

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y la dimensión Fines de la adquisición.

Además, basándonos en la tabla N° 19. Afirmamos que el p valor (Sig.) 0.043, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con los fines de la adquisición del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.646. Indica que existen un grado de Correlación positiva considerable entre la variable Auditoria Informática y la dimensión fines de la adquisición.

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y la dimensión Software.
Además, basándonos en la tabla N° 22. Afirmamos que el p valor (Sig.) 0.034, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el software del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.38. Indica que

existe un grado de Correlación positiva media entre la variable Auditoria Informática y la dimensión software.

Afirmamos que existe una relación directamente proporcional entre la variable: Auditoria Informática y la dimensión Hardware.

Además, basándonos en la tabla N° 25. Afirmamos que el p valor (Sig.) 0.014, es menor que el nivel de significancia de 0,05. Por lo tanto, se toma la decisión de rechazar la hipótesis Nula y de aceptar la hipótesis de investigación, el cual manifiesta que: La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017.

Además, basado en lo que determinan Hernández Sampieri, Fernández Collado, y Baptista Lucio (2010), r = 0.82. Indica que existe un grado de Correlación positiva muy fuerte entre la variable Auditoria Informática y la dimensión hardware.

CAPITULO V

DISCUSIÓN

DESARROLLO DE LA AUDITORIA

5.1. Plan de auditoria

PLANIFICACIÓN

Es vital planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de auditoría y para cumplir con las normas aplicables de auditoría.

Por ello el debido cuidado profesional debe extenderse en cada aspecto de la auditoría, incluyendo: la evaluación del riesgo, formulación de objetivos y alcance de auditoría, así como la selección de pruebas y evaluación de los resultados de estas.

EJECUCIÓN DEL TRABAJO DE AUDITORÍA

El personal de auditoría debe contar con la supervisión apropiada para proporcionar la garantía de cumplir con los objetivos de auditoría establecidos.

Durante el transcurso de la auditoría, el auditor colecciona información, conocida también como evidencia, misma que deberá ser suficiente, confiable, relevante y útil, quedando a juicio del auditor determinar la naturaleza de esta.

Los hallazgos y conclusiones de auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia, de allí la importancia de documentarla y organizarla apropiadamente.

Son varios los tipos de evidencia que el auditor puede utilizar, entre ellas: evidencia física: Observación de actividades, bienes y funciones de sistemas, inventarios.

Evidencia documentaria: Registros de transacciones, listados de Programas, logos de control, entre otros.

Los procedimientos usados para recolectar la evidencia pueden variar, mismos que pueden incluir: averiguaciones, observaciones, inspección, confirmación o re ejecución, entre otros.

El uso de valoración de riesgos es imprescindible durante la planeación de auditoría, puesto que facilitara la toma de decisiones durante el desarrollo de esta, ya que sumados a la documentación respectiva y la evidencia de

auditoría obtenida, soportarán de mejor manera las conclusiones del auditor.

ACTIVIDADES DE SEGUIMIENTO

Se deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han desarrollado las acciones apropiadas de manera oportuna.

En este caso realizaremos de forma personal bajo la supervisión del encargado del área de patrimonio conjuntamente con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE) [3]para que ellos sean parte de los problemas que están aconteciendo en el área y así brindar una posible solución o mejora de la problemática.

FASES O ETAPAS, ACTIVIDADES A DESARROLLAR

Fase de Conocimiento

1. Realizar visitas al área de patrimonio y la oficina general de tecnologías de información, sistemas y estadística (OGTISE).

2. Realizar observaciones de cada uno de los procesos que se lleva a cabo.

3. Establecer los recursos de TI involucrados en el manejo de la información.

4. Determinar las entradas y salidas de la información.

[3] Universidad Nacional de Ucayali, OGTISE, oficina general de tecnologías de información, sistemas y estadística, 2019.

5. Revisar la documentación existente.

6. Identificar las vulnerabilidades y amenazas a que está expuesta la organización.

7. Identificar los riesgos iniciales.

8. Hacer el análisis y evaluación de riesgos preliminar.

Fase de Planeación de la Auditoría

1. Identificar el origen de la auditoría.

2. Determinar el estándar que será aplicado para la auditoría.

3. Elaborar plan de auditoría: establecer los objetivos, alcances, metodología, recursos y cronograma de actividades de la auditoría.

4. Elaborar el programa de auditoría: grupo auditor, definir responsabilidades y actividades a desarrollar.

5. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría.

6. Diseñar los papeles de trabajo: entrevistas, listas de chequeo, cuestionarios, otros.

7. Elaborar el plan de pruebas de análisis y ejecución.

Fase de Ejecución de la Auditoría

1. Realizar las acciones programadas para la auditoría.

2. Aplicar los instrumentos diseñados para la auditoría.

3. Aplicar las pruebas diseñadas.

4. Aplicar el proceso de análisis y evaluación de riesgos aplicando una metodología.

5. Elaborar la matriz de riesgos.

6. Identificar los controles definidos para cada dominio y proceso.

7. Elaborar los formatos de hallazgos: identificar proceso, describir riesgos, identificar las causas, identificar los recursos afectados, identificar posibles soluciones en el contexto.

Fase de Resultados de la Auditoría

1. Definir tratamiento de los riesgos.

2. Determinar los controles y tipos de control: preventivos, detectivos, correctivos, recuperación.

3. Elaborar el Dictamen de la auditoría para cada dominio y procesos evaluado.

4. Elaborar el informe preliminar y presentarlo a discusión.

5. Elaborar el informe final de auditoría.

6. Integrar el legajo de papeles de trabajo de la auditoría.

7. Presentar el informe final de Auditoría y documentación.

Código: SGSI. 100.2.1.1

Versión: 1

Fecha de la versión: 30-07-2019.

Creado por: Marcos Alexis Bautista Ushiñahua.

Aprobado por: jefe del área de patrimonio universidad nacional de Ucayali con ayuda del área de informática.

Nombre del proyecto: plan general de auditoria informática para el área de patrimonio de la universidad nacional de Ucayali.

Nivel de confidencialidad: baja

Lugar a auditar: área de patrimonio de la universidad nacional de Ucayali.

Tiempo de la auditoria: 6 meses.

1. Objetivo general de la auditoria

Realizar un plan de auditoria informática basada en la metodología COBIT 4.5 para el análisis de los procesos del área de patrimonio.

Objetivos específicos de la auditoria

Analizar y diagnosticar la actual gestión del proceso del manejo de información de software y hardware utilizando la metodología cobit 4.5.

Identificar el nivel de relación de la Auditoria Informática con metodología COBIT con los fines de la adquisición.

Fortalecer la funcionalidad de la entidad realizando las Auditorias en cumplimiento de políticas, planes, procedimiento leyes y regulaciones todo relacionado con la misión, política de calidad y objetivos de calidad que rigen.

Verificar la efectividad de los controles frente a la materialización de los riesgos, evaluando si han sido efectivos para evitar su ocurrencia.

2. Alcance de la auditoria

La auditoría abarcará el área de patrimonio conjunta con la oficina general de tecnologías de información, sistemas y estadística (OGTISE), se examinará detalladamente el manejo de información del registro de software y hardware, brindando mayor integridad, confidencialidad y confiabilidad de la información, realizando un análisis en forma detallada y precisa. Se comprobará si el área de patrimonio cumple con las expectativas que el gobierno dictamina para la comprobación y reparación de errores y si este los enmendada de manera eficiente los procesos y actividades que debe tener un área de patrimonio.

3. Responsable

Es responsabilidad de la aplicación de este procedimiento es el Jefe Interno del área de patrimonio y la responsabilidad de la presentación y ejecución de los Planes de Mejoramiento derivados de cada proceso auditor es del personal externo que realizará la auditoria.

4. Usuarios

- Jefe del área de patrimonio
- Jefe del área de la oficina general de tecnologías de información, sistemas y estadística (OGTISE).
- Persona encargada de la auditoria
- Encargado del proyecto de auditoria

5. Documentos de referencia

- Modelo estándar de control interno MECI
- Sistema de gestión de seguridad de la información
- ISO 9001

6. Criterios de la auditoria interna

La auditoría es un proceso sistemático, independiente y documentado para obtener evidencias de la auditoría, y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría.

Teniendo en cuenta los insumos anteriores se procede a hacer el proceso de evaluación de los riesgos encontrados en cada uno de los procesos evaluados, teniendo en cuenta los riesgos en cuanto a la probabilidad

de ocurrencia de los mismos y el impacto que pueden causar al área de patrimonio.

- Norma ISO 9001:2015.
- Procedimientos Operacionales
- Puntualidad.
- Capacidad de análisis.

7. Recursos

El numero de personas que integraran el equipo de auditoria sera de 1 solo , con un tiempo maximo de ejecucion de 4 a 5 semanas.

Etapas de trabajo

1. Recopilacion de informacion básica

Una semana antes del comienzo de la auditoria se envia un cuestionario a los gerentes o responsables de las distintas areas a auditar. El objetivo de este cuestionario es saber los equipos que usan y los procesos que realizan en ellos.

Los gerentes se encargaran de distribuir este cuestionario a los distintos empleados con acceso a los computadores, para que tambien lo completen. De esta manera, se obtendra una vision mas global del sistema.

Es importante tambien reconocer y entrevistarse con los responsables del area de sistemas de la empresa para conocer con mayor profundidad el hardware y el software utilizado.

En las entrevistas incluiran:

- Jefe del área de patrimonio.
- Trabajadores del área de patrimonio.
- Jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE).
- Tecnicos de soporte técnico.

2. Objetivos de control

Se evaluaran la existencia y la aplicación correcta de las politicas de seguridad, emergencia y disaster recovery de la empresa.

- Se hara una revicion de los manuales de politica de la empresa, que los procedimientos de los mismos se encuentren actualizados y que sean claros y que el personal los comprenda.

- Debe existir en la Empresa un programa de seguridad, para la evaluación de los riesgos que puedan existir, respecto a la seguridad del mantenimiento de los equipos, programas y datos.

3. Determinacion de los procedimientos de control

Se determinarán los procedimientos adecuados para aplicar a cada uno de los objetivos definidos en el paso anterior.

Objetivo N 1: Existencia de normativa de hardware.

- ✓ El hardware debe estar correctamente identificado y documentado.

- ✓ Se debe contar con todas las órdenes de compra y facturas con el fin de contar con el respaldo de las garantías ofrecidas por los fabricantes.

- ✓ El acceso a los componentes del hardware esté restringido a la directo a las personas que lo utilizan.

- ✓ Se debe contar con un plan de mantenimiento y registro de fechas, problemas, soluciones y próximo mantenimiento propuesto.

Objetivo N 2: Política de acceso a equipos.

- ✓ Cada usuario deberá contar con su nombre de usuario y contraseña para acceder a los equipos.

- ✓ Las claves deberán ser seguras (mínimo 8 caracteres, alfanuméricos y alternando mayúsculas y minúsculas).

- ✓ Los nuevos usuarios deberán ser autorizados mediante contratos de confidencialidad y deben mantenerse luego de finalizada la relación laboral.

- ✓ Uso restringido de medios removibles (USB, CD-ROM, discos externos etc).

4. **Pruebas a realizar**.

Son los procedimientos que se llevaran a cabo a fin de verificar el cumplimiento de los objetivos establecidos. Entre ellas podemos mencionar las siguientes técnicas:

- ✓ Tomar 2 máquinas al azar y evaluar la dificultad de acceso a las mismas.
- ✓ Intentar sacar datos con un dispositivo externo.
- ✓ Facilidad para desarmar un pc.
- ✓ Ver los inventarios de cada equipo informático.

5. Obtencion de los resultados

En esta etapa se obtendrán los resultados que surjan de la aplicación de los procedimientos de control y las pruebas realizadas a fin de poder determinar si se cumple o no con los objetivos de control antes definidos. Los datos obtenidos se registrarán en planillas realizadas a medida para cada procedimiento a fin de tener catalogado perfectamente los resultados con el objetivo de facilitar la interpretacion de los mismos y evitar interpretaciones erroneas.

6. Conclusiones y Comentarios

En este paso se detallará el resumen de toda la información obtenida, así como lo que se deriva de esa información, sean fallas de seguridad, organización o estructura empresarial. Se expondrán las fallas encontradas, en la seguridad física sean en temas de resguardo de información (Casos de incendio, robo), manejo y obtención de copias de seguridad, en las normativas de seguridad como por ejemplo normativas de uso de passwords, formularios de

adquisición de equipos, y estudios previos a las adquisiciones para comprobar el beneficio que los mismos aportarían. Finalmente se verán los temas de organización empresarial, como son partes responsables de seguridad, mantenimiento y supervisión de las otras áreas.

7. Riesgos con la aplicación de instrumentos

RIESGOS INICIALES:

De los riesgos iniciales, de acuerdo al proceso que se está evaluando, debe mirar que riesgos son los que están relacionados directamente con el proceso evaluado y deben listarse como riesgos.

Posteriormente, al aplicar los instrumentos como entrevistas se descubrieron nuevos riesgos, al aplicar la lista de chequeo se descubre que faltan algunos controles en el proceso evaluado de acuerdo a la normativa, y en el cuestionario están prácticamente, todos los riesgos detectados en el proceso evaluado y se hace una lista de ellos.

Posteriormente y de acuerdo a las normas aplicadas se construye las escalas de medición del impacto y la probabilidad de ocurrencia de los riesgos, hay que tener en cuenta que puede haber una valoración cuantitativa y cualitativa y que deben describirse los valores correspondientes tal y como aparece en las siguientes matrices:

MATRIZ PARA MEDICIÓN DE PROBABILIDAD E IMPACTO DE RIESGOS

Cuadro 8: *Matriz de medición de probabilidad*

IMPACTO		
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**
1	Insignificante	Si el caso llegara a presentarse, tendría consecuencias o efectos mínimos sobre el área de patrimonio.
2	Menor	Si el caso llegara a presentarse, tendría bajo impacto o efecto sobre el área de patrimonio.
3	Moderado	Si el caso llegara a presentarse, tendría medianas consecuencias o efectos sobre el área de patrimonio.
4	Mayor	Si el caso llegara a presentarse, tendría altas consecuencias o efectos sobre la área de patrimonio.
5	Catastrófico	Si el caso llegara a presentarse, tendría desastrosas consecuencias o efectos sobre el área de patrimonio.

Fuente: Elaboración propia

Cuadro 9*: Matriz de Probabilidad*

PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**DESCRIPCIÓN**	**FRECUENCIA**
1	Raro	El acontecimiento puede ocurrir sólo en circunstancias excepcionales y claras.	Hasta la fecha no se ha presentado.
2	Improbable	El acontecimiento puede ocurrir en algún momento y en cualquier circunstancia sin excepciones.	Se ha presentado al menos 1 vez en los últimos 3 años.
3	Posible	El acontecimiento puede ocurrir en algún momento	Hasta la fecha no se ha presentado.
4	Probable	El acontecimiento probablemente ocurrirá en la mayoría de las circunstancias	Se ha presentado al menos 1 vez en los últimos 2 años.
5	Casi Seguro	Se espera que el acontecimiento ocurra en la mayoría de las circunstancias	Hasta la fecha no se ha presentado.

Fuente: Elaboración propia

Con las escalas de medición se construye la matriz de riesgos general que se aplica para cualquiera de los procesos, teniendo en cuenta los riesgos encontrados.

Cuadro 10: *Evaluación y medidas de respuesta*

EVALUACIÓN Y MEDIDAS DE RESPUESTA					
PROBABILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

IMPACTO
Insignificante = 1
Menor = 2
Moderado = 3
Mayor = 4
Catastrófico = 5

PROBABILIDAD
Raro = 1
Improbable = 2
Posible = 3
Probable = 4
Casi Seguro = 5

Fuente: Elaboración propia

8. Redaccion de la ficha técnica

Se detalla de manera concisa y clara un informe de todos los problemas encontrados, anotando los datos técnicos de cada una de las maquinas auditadas:

- ✓ Marca
- ✓ Modelo
- ✓ Número de Serie
- ✓ Problema encontrado
- ✓ Solución recomendada

9. Presentación del borrador del informe, al responsable del area de patrimonio

Se le presentara el informe borrador a un responsable del área informática, como se aclaró en el punto anterior, con el máximo de detalle posible de todos los problemas y soluciones posibles recomendadas, este informe se pasará por escrito en original y copia firmando un documento de conformidad del mismo para adquirir un compromiso fuerte en la solución de los mismos, de sta forma evitaremos posibles confusiones futuras.

10. Redacción del Informe Resumen y Conclusiones.

Se realizará dos informes para la realización de la auditoria con metodología COBIT 4.5.

Los cuales son:

- Informe preliminar
- Informe final
- Ficha técnica (Anexo 16).
- Inventario de equipos informáticos (Anexo 18).

En el momento de completar el trabajo de auditoría, se deberá proporcionar un informe, de formato apropiado a los destinatarios en cuestión. El informe de auditoría deberá enunciar su alcance, los objetivos, el período de cobertura, naturaleza y amplitud del trabajo de auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los hallazgos, las conclusiones, recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

- Análisis de riesgos (Anexo 19).
- Informe de mantenimiento (Anexo 17).
- Acta de reunión (Anexo 24).

Es en este paso es donde se muestran los verdarderos resultados a los responsables del área de patrimonio, el informe presentado dará a conocer todos los puntos evaluados durante la auditoria, resultados, conclusiones, puntaje y posibles soluciones.

La conclusión tendrá como temas los resultados, errores, puntos críticos y observaciones de los auditores. Mientras que en el resumen se verán las posibles soluciones de esos puntos críticos y fallas, así como recomendaciones para el buen uso y también recomendaciones sobre la forma incorrecta de realizar algunos procedimientos.

11. Entrega del informe a los jefes del área patrimonio y de la oficina general de tecnologías de información, sistemas y estadística.

Esta es la ultima parte de la auditoria y en una reunion se formaliza la entrega del informe final con los resultados obtenidos en la auditoria.

Tambien se fijan los parametros si asi se requieren para realizar el seguimientos de los puntos en los que el resultado no haya sido satifactorio o simplemente se quiera verificar que los que los objetivos de control se sigan cumpliendo a lo largo del tiempo.

5.2. Recursos (Humanos, Materiales y costos)

RECURSOS HUMANOS

a) Encuestas

- ✓ Encuestador
- ✓ Digitador
- ✓ Encuestados
- ✓ Asesor

MATERIALES

- ✓ Hoja papel bond A4
- ✓ Lapiceros
- ✓ Tinta a color y blanco y negro
- ✓ Laptop HP
- ✓ Impresora
- ✓ Folder

COSTOS

Items	Cantidad	Precio	Total/soles
Hoja papel bond A4	3 millares	12 soles	72
Lapiceros	15	5	75
Tinta a color, blanco y negro	2 cartuchos	24	48
Laptop HP	2	500	1000
Impresora	1	200	200
Folder	14	0.50	7

Fuente: elaboración propia

5.3. Presupuesto

Tabla 26: *Presupuesto de desarrollo de la auditoria*

AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL ÁREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017		
Actividades	Recursos para el desarrollo del proyecto	Costo Soles
Análisis Del Proyecto	Total Trabajo Personal	S/.1000
Planificación		S/. 1000
Desarrollo De La Auditoria	Papeleos E Impresiones	S/100
Gastos Del Desarrollo	Telefonía Celular	S/.150
Ejecución O Resultado	Materiales De Escritorio	S/.200
	Equipos Y Bienes Duraderos	S/.70
	Total Gastos Aprovisionamiento	S/.1520
Total Del Presupuesto		S/2520

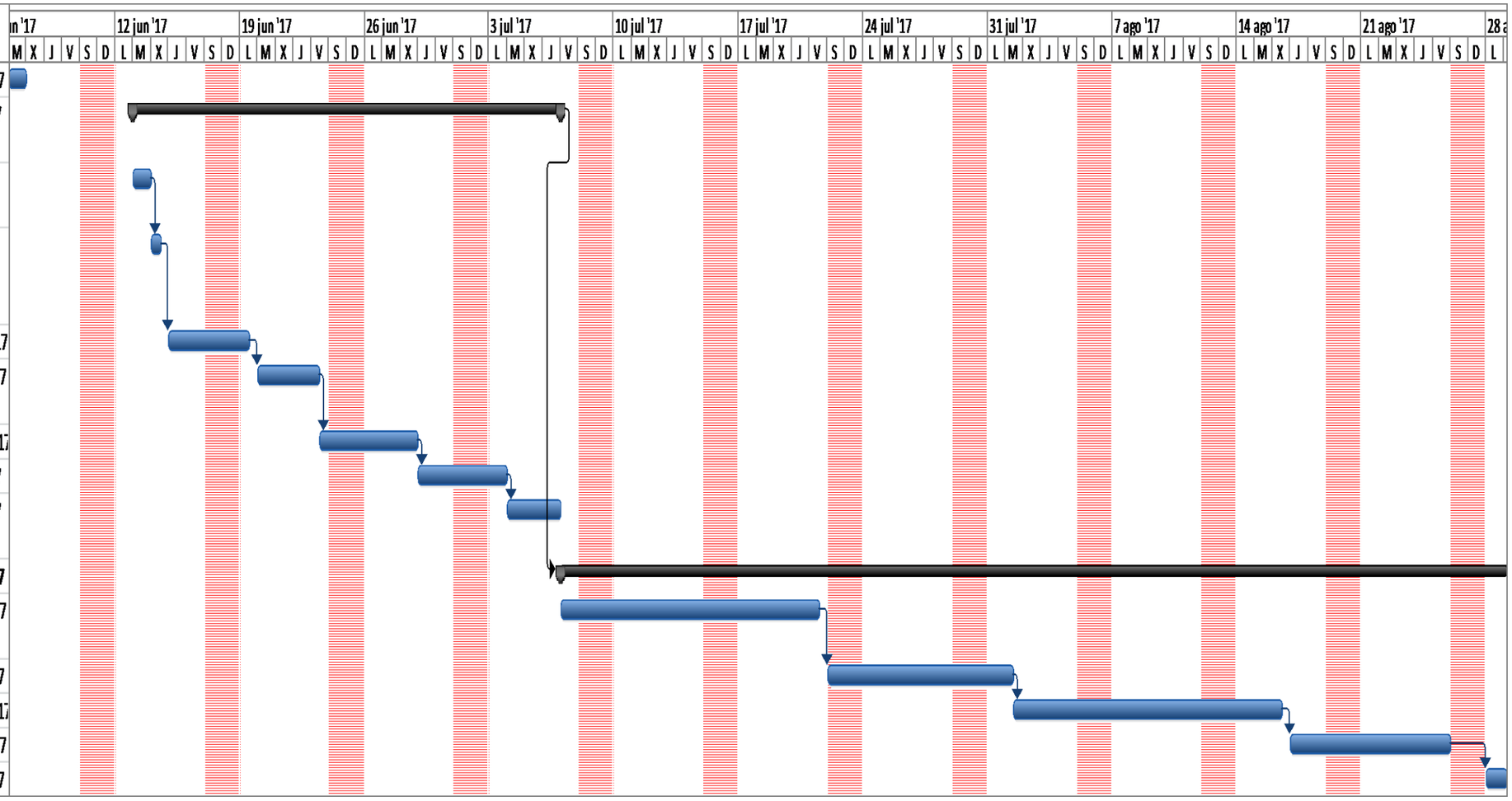
Fuente: Elaboración propia

5.4. Cronograma de actividades

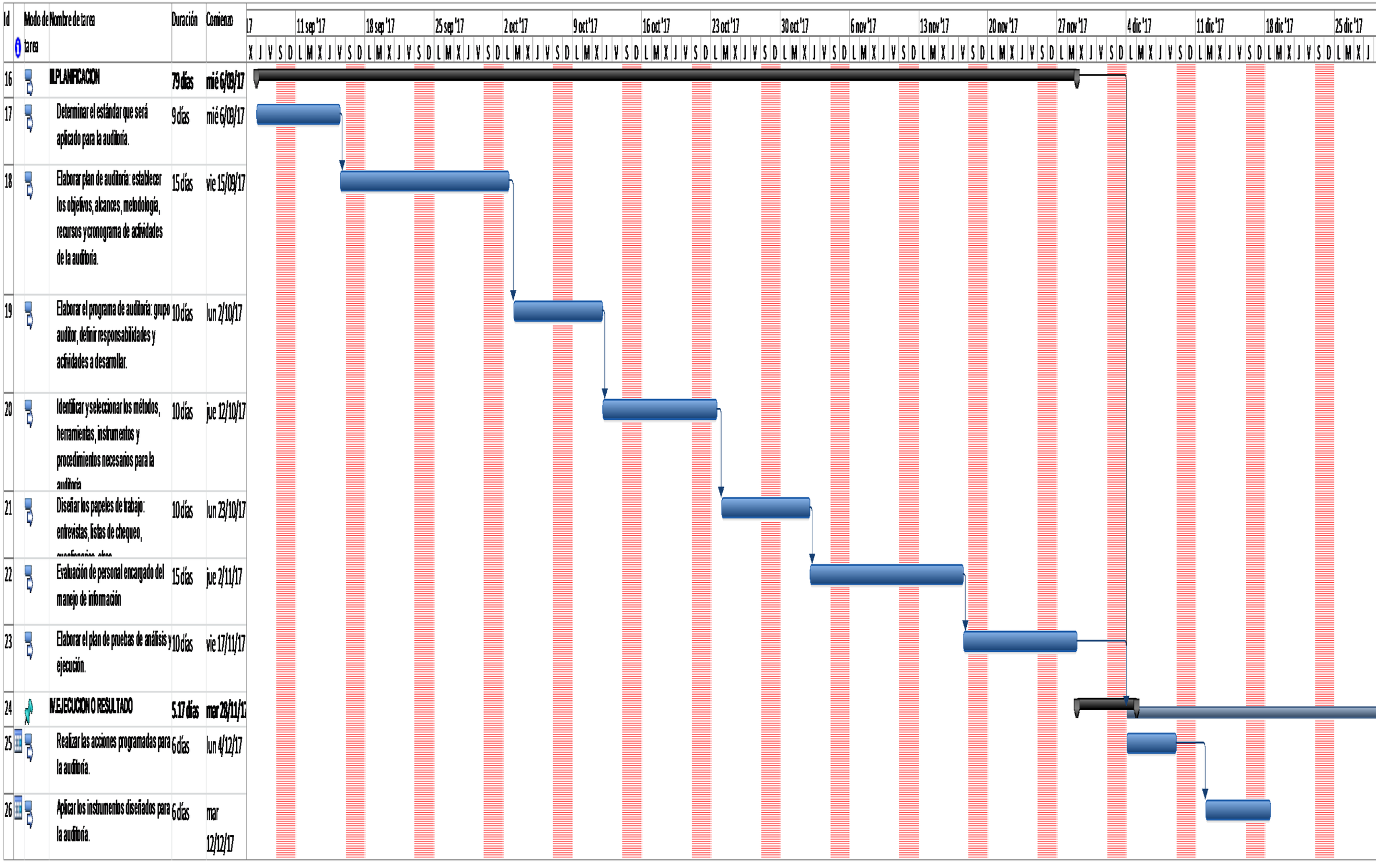
Tabla 27: *Cronograma de Actividades*

Cronograma de actividades

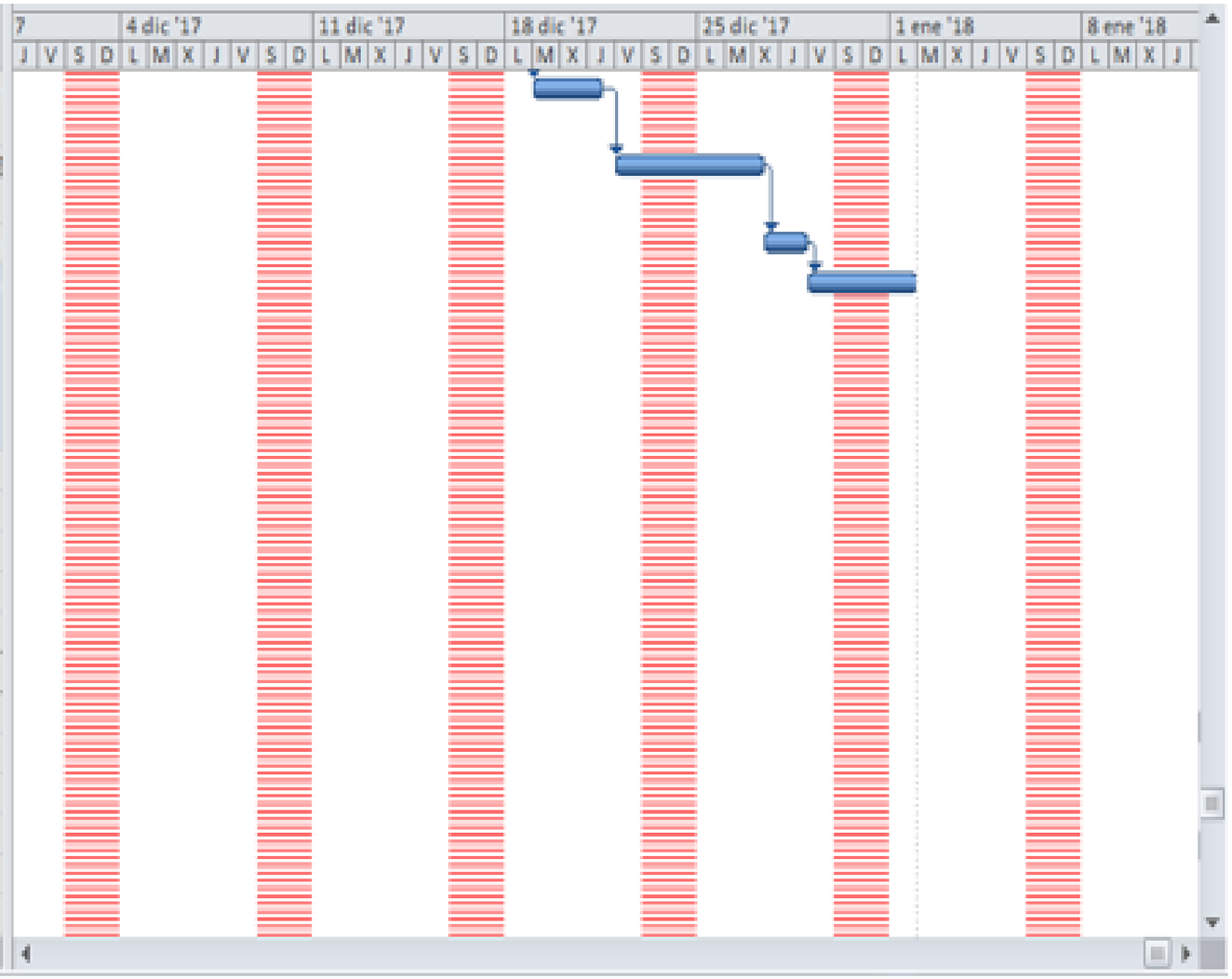
Id	Nombre de tarea	Duración	Comienzo	Fin
1	PROYECTO DE INVESTIGACIÇ	1 día?	mar 6/06/17	mar 6/06/17
2	**I.DEFINIR LA ESTRUCTURA DEL PROYECTO**	**24 días**	**mar 13/06/17**	**jue 6/07/17**
3	Definir el lugar y tema de investigación	1 día	mar 13/06/17	mar 13/06/17
4	Entrevista con el jefe del área de patrimonio y con el jefe de informática.	1 día	mar 13/06/17	mié 14/06/17
5	Recopilación de información	4 días	mié 14/06/17	lun 19/06/17
6	Describir la situación actual de la organización	5 días	lun 19/06/17	vie 23/06/17
7	Definir los problemas de investigaci	5 días	vie 23/06/17	mié 28/06/17
8	Definir los riesgos encontrados	4 días	jue 29/06/17	lun 3/07/17
9	Recopilar información mediante la observación	4 días	mar 4/07/17	jue 6/07/17
10	**II. ANALISIS DEL PROYECTO**	**58 días**	**vie 7/07/17**	**mié 6/09/17**
11	Realizar observaciones de cada uno de los procesos que se lleva a	14 días	vie 7/07/17	vie 21/07/17
12	A nalizar lo s posibles riesgo	9 días	vie 21/07/17	mar 1/08/17
13	Análisis funcional	15 días	mar 1/08/17	mié 16/08/17
14	Diseño	10 días	mié 16/08/17	vie 25/08/17
15	Análisis orgánico y Pruebas	10 días	lun 28/08/17	mié 6/09/17


n '17
12 jun '17
19 jun '17
26 jun '17
3 jul '17
10 jul '17
17 jul '17
24 jul '17
31 jul '17
7 ago '17
14 ago '17
21 ago '17
28 a
M X J V S D L M X J V S D L M X J V S D L

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
16		**II.PLANIFICACION**	**79 días**	**mié 6/09/17**
17		Determinar el estándar que será aplicado para la auditoría.	9 días	mié 6/09/17
18		Elaborar plan de auditoría: establecer los objetivos, alcances, metodología, recursos y cronograma de actividades de la auditoría.	15 días	vie 15/09/17
19		Elaborar el programa de auditoría: grupo auditor, definir responsabilidades y actividades a desarrollar.	10 días	lun 2/10/17
20		Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría	10 días	jue 12/10/17
21		Diseñar los papeles de trabajo: entrevistas, listas de chequeo, cuestionarios, otros	10 días	lun 23/10/17
22		Evaluación de personal encargado del manejo de información	15 días	jue 2/11/17
23		Elaborar el plan de pruebas de análisis y ejecución.	10 días	vie 17/11/17
24		**IV.EJECUCION O RESULTADO**	**5.17 días**	**mar 28/11/17**
25		Realizar las acciones programadas para la auditoría.	6 días	lun 4/12/17
26		Aplicar los instrumentos diseñados para la auditoría.	6 días	mar 12/12/17



		Modo de	Nombre de tarea	Duración	Comienzo	Fin
27			Aplicar el proceso de análisis y evaluación de riesgos aplicando una metodología.	4 días	lun 18/12/17	jue
28			Identificar los controles definidos para cada dominio y proceso.	5 días	jue 21/12/17	mié
29			Elaborar la matriz de riesgos.	2 días	mié 27/12/17	jue
30			Elaborar los formatos de hallazgos: identificar proceso, describir riesgos, identificar las causas, identificar los recursos afectad1os, identificar posibles soluciones en el contexto.	3 días	jue 28/12/17	lun



Fuente: Elaboración propia

Asignación de Horas de Auditoría

Se pretende trabajar en la auditoría durante el tiempo de realización de tesis, un total de 700 horas, las cuales se han dividido el 15% para labores de supervisión, 20% a cargo del Interlocutor y el 65% para la auditora.

Tabla 28: *A asignación de horas de auditoría*

N°	**Nivel de Responsabilidad**	**Horas/ Asignadas**
1	Supervisor de la oficina general de tecnologías de información, sistemas y estadística. Ing. Jorge trigueros bellido	120
2	Supervisor del área de patrimonio C.P.C. Sergio Cárdenas	160
3	Auditor BACH. Marcos Alexis Bautista Ushiñahua	520

Fuente: elaboración propia

Estimación de días por etapas

Tabla 29: *Estimación de días por etapa*

Nº	ETAPAS DE LA METODOLOGÍA	DIAS
1	Plan de auditoría preliminar	**5 días**
2	Comprensión de la organización, procesos de negocio y sistemas	**4 días**
3	Definición del programa y su alcance de la auditoría	**6 días**
4	Análisis de riesgos del área de patrimonio.	**8 días**
5	Definición y diseño de las pruebas de auditoría	**7 días**
6	Ejecución de las pruebas de auditoría	**8 días**
7	Evaluación de los resultados obtenidos en las pruebas de auditoría	**5 días**
8	Elaboración informe final con los resultados de la auditoría	**7 días**

Fuente: elaboración propia

En esta parte no es necesario realizar un diagrama de GANT, porque solo es una estimación de la metodología lo cual está visualizado en el cronograma de actividades tabla.27.

5.5. Ejecución de la auditoria usando COBIT 4.5

Determinaré los Procesos COBIT 4.5 aplicables a la auditoría en ejecución en este caso es el área de patrimonio de la universidad nacional de Ucayali.

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 4.5 que fue publicado a inicios del 2013. Este documento expone los objetivos de control detallados de COBIT 4.5 que tienen relación con la gestión de TI. Del estudio de estos, se han seleccionado aquellos que tienen relación con la gestión de TI para ver el estado del área patrimonio junto con el área de informática de acuerdo a la encuesta realizada a dicha área, 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 de patrimonio.

DOMINIO: ALINEAR, PLANIFICAR Y ORGANIZAR (APO)

De este dominio se ha elegido los siguientes procesos, Definir un Plan Estratégico de TI y Gestionar los Recursos Humanos, de los cuales aplican 2 objetivos de control y se mencionan a continuación:

APO1: Definir un Plan Estratégico de TI

APO1.3. Evaluación del Desempeño y la Cap. Actual

APO1.4.Plan Estratégico de TI

APO1.5. Planes Tácticos de TI

APO7: Administrar los Recursos Humanos de TI

APO7.1 Mantener la dotación de personal suficiente y adecuado

APO7.3. Mantener las habilidades y competencias del personal.

APO7.4. Evaluar el desempeño laboral de los empleados.

APO7.6. Gestionar el personal contratado.

DOMINIO: ADQUIRIR E IMPLANTAR

De este dominio se ha elegido los siguientes procesos, Identificar soluciones y Adquirir recursos de TI , de los cuales aplican 4 objetivos de control y se mencionan a continuación:

Al1: Identificar soluciones

AI5: Adquirir recursos de TI.

DOMINIO: MONITOREAR Y EVALUAR

MEA1: Monitorear y evaluar el desempeño de TI.

MEA1.2. Establecer un enfoque de la supervisión

MEA1.2. Analizar e informar sobre el rendimiento.

MEA1.2. Asegurar la implantación de medidas correctivas.

DOMINIO: PRESTACIÓN Y SOPORTE

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.

DSS3: Administrar desempeño y capacidad.

DSS2: Gestionar las Peticiones y los Incidentes del Servicio

Registrar, clasificar y priorizar peticiones e incidentes.

DSS5: Garantizar la seguridad de los sistemas.

DSS5.3. Gestionar la seguridad de los puestos de usuario Final

.

DSS6: Gestionar los Controles de los Procesos del negocio

Asegurar los activos de información.

DOMINIO: ALINEAR, PLANIFICAR Y ORGANIZAR (APO)

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.

APO1.Definir un Plan Estratégico de TI

Al hacer las evaluaciones correspondientes del área, nos encontramos con una gran sorpresa que no cuentan con un plan de trabajo o un plan estratégico para lograr la mejora de información y eficacia del área, por eso motivo decidimos optar por este proceso para la solución del área a auditar; minimizando los posibles riesgos que pudiéramos encontrar.

Los objetivos de control detallados a ser considerados son:

APO1.4 Plan Estratégico de TI

Al hacer un análisis minucioso de las actividades del área de patrimonio en conjunta con el área de informática nos dimos cuenta que no cumplen con una metodología apropiada para el mejor desarrollo de un plan que permita tener una mejor seguridad en el manejo de información de datos del registro de software y hardware, de acuerdo a ese análisis escogimos este subproceso y ver en que si se puede dar una mejora a ese problema.

APO1.5. Planes Tácticos de TI

Decidí optar por este sub proceso para proponer crear un plan de estrategia para la mejora del área de patrimonio y tratar de minimizar los riesgos encontrados durante el

proceso de la auditoria, mediante la propuesta se podrá tener el conocimiento de las tareas que se están dando y como también a lo que se quiere llegar, monitoreando las actividades propias del área.

APO7. Administrar los Recursos Humanos de TI

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:

APO7.1.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 el área de patrimonio tenga los suficientes recursos humanos para apoyar las metas y los objetivos.

APO7.3. Mantener las habilidades y competencias del personal

Opté por este sub proceso para mejorar el desempeño de los trabajadores al encontrarse poco recurso humano, estos de multiplican y pueden realizar tareas erróneas al no estar en su función verdadera, mediante este sub proceso daremos a conocer el nivel de cada personal.

APO7.4. Evaluar el desempeño laboral de los empleados

Elegí este subproceso ya que es vital que se realicen oportunamente evaluaciones de rendimiento de manera regular y precisa respecto a los objetivos individuales derivados de los objetivos de la empresa, para tener personal capaz de afrontar situaciones adversas que pudieran ocurrir con 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.

APO7.6. Gestionar el personal contratado

Elegí este subproceso ya que se debe asegurar que los consultores y el personal contratado que apoyan al área de patrimonio con

capacidades de TI conozcan y cumplen las políticas del área, así como los requisitos contractuales previamente acordados para tener un buen desempeño y brindando eficacia en el trabajo que se va a realizar.

DOMINIO: ADQUIRIR E IMPLANTAR

Elegimos este dominio para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas en los procesos del área de patrimonio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del área de patrimonio. Este dominio, por lo general, cubrirá la normativa de los procesos y actividades del área, adquirir algunas herramientas que minimizaran los tiempos de ejecución de los procesos que tenga el área de patrimonio.

AI1. Identificar soluciones automatizadas

Elegí este proceso para dar a conocer q el software que cuenta el área de patrimonio, si es el adecuado para el inventario del registro de información del software y hardware y poner automatizar los procesos y objetivos que tenga el área, además el ministerio de economía y finanzas está brindando un reglamento nacional que toda área de patrimonio tenga acceso al sistema SIGA-patrimonio.

AI1.2 Reporte de Análisis de Riesgos

Escogí este sub proceso para mencionar cada riesgo que se logra encontrar en la aplicación de la auditoria.

AI5. Adquirir recursos de TI.

Escogí este proceso para poder suministrar los recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la cual se realiza una selección de proveedores, el ajuste de arreglos contractuales y la adquisición de en sí de los equipos informáticos. El hacerlo va a garantizar que el área de patrimonio tenga todos los recursos de TI que se requieren de una manera oportuna y rentable para la mejora de las funciones correspondientes.

Al 5.1. Control de adquisición

Escogí este sub proceso para poder desarrollar y seguir los procedimientos y estándares consistente con el proceso general de adquisiciones del área de patrimonio con la estrategia de adquisición, para garantizar que la adquisición de la infraestructura, instalaciones, hardware y software, satisfagan los requerimientos del área de patrimonio.

DOMINIO: MONITOREAR Y EVALUAR

MEA1. Monitorear y evaluar el desempeño de TI

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.

MEA1.1 Establecer un enfoque de la supervisión

Elegí este sub proceso para establecer un mayor control de los objetivos y procesos que realiza el área de patrimonio para lograr un mejor enfoque del conocimiento del manejo de datos.

MEA1.4 Analizar e informar sobre el rendimiento

Elegí este sub proceso para indicar el análisis de la problemática el cual nos basaremos a realizar, informando los procedimientos a realizar.

MEA2. 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 auditor 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:

MEA2.1. Supervisar el control interno

Elegí este subproceso ya que se realizará, de forma continua, la supervisión, los estudios comparativos y la mejora el entorno de control de información de datos de los software y hardware del área de patrimonio y el marco de control para alcanzar los objetivos organizativos, ya que esto permitirá al personal del área de informática identificar los límites del sistema de control interno de del registro.

MEA2.2: Revisar la efectividad de los controles sobre los Procesos de negocio

Elegí 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 del área 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 continúa de controles, evaluaciones independientes, centros de mando y control de cada proceso que hacen conjuntamente con el área de informática.

MEA2.7: Estudiar las iniciativas de aseguramiento.

Elegí este sub proceso para lograr un estudio de la problemática que está ocurriendo en el área de patrimonio conjuntamente con el área de informática logrando minimizar dichos problemas mediante informes y procesos.

DOMINIO: PRESTACIÓN 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.

DSS2. Gestionar las Peticiones y los Incidentes del 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.

DSS2.1. Definir esquemas de clasificación de incidentes y Peticiones de servicio

Escogí este sub proceso para poder verificar cada incidente que se pueda encontrar durante la auditoria y tratar de dar solución a cada una.

DSS2.2. Registrar, clasificar y priorizar peticiones 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 área de patrimonio y los acuerdos de servicio que se llevaran a cabo.

DSS2.4. 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 y darnos un diagnóstico claro y preciso para mejorar la problemática.

DSS3. Administrar desempeño y capacidad

Elegí este proceso para lograr administrar los procesos y brindar una mejor seguridad, calculando el desempeño que se puede establecer durante la auditoria.

DSS5. Garantizar la seguridad de los sistemas

Proteger la información del área de patrimonio 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:

DSS 5.3. Gestionar la seguridad de los puestos de usuario Final

Se eligió este subproceso ya que se recomienda asegurar que los puestos de usuario se eligieron 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.

DSS 6. Gestionar los Controles de los Procesos del negocio

Asegurar los activos de información hace que el área de patrimonio sea un área eficiente en lograr sus objetivos trazados, mediante este proceso podremos gestionar cada actividad y proceso que realiza el área brindando un mejor desarrollo en sus trabajos.

El criterio de elección de los dominios y procesos fue el análisis y comparación de los procedimientos que se logró recopilar durante la entrevista con los jefes de las áreas, una vez recopilado la información se pasó a la alineación de los procedimientos con sus errores mediante las matrices de pruebas y de los riesgos encontrados.

Comparando los hallazgos con las funciones de los dominios y procesos se dedujo que procesos vamos a tomar en cuenta para la alineación de los procedimientos y la problema de la auditoria.

5.6. Programa de auditoria y matriz de prueba de los procesos y objetivos de control

En este punto se va a detallar los procesos y objetivos que aplican la auditoria.

5.6.1. Programa de auditoria

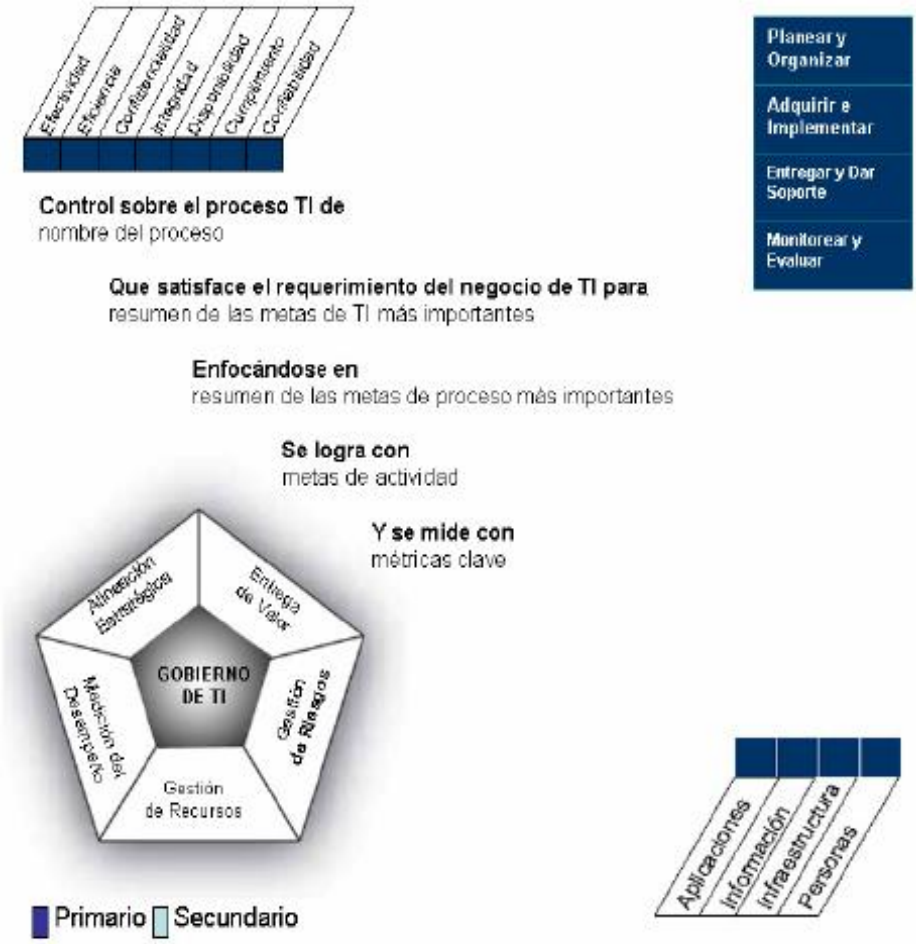
En este cuadro se observará las actividades de cada objetivo de control detallado anteriormente. Cada dominio estará detallado y verificado. En el cual también se va a detallar los factores de riesgos de acuerdo al análisis desarrollado que se va a realizar.

5.6.2. 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 4.5**.**

Para la realización de la auditoria se procederá a realizar la navegación en el Marco de Trabajo COBIT 4.5, cada uno de los procesos seleccionados de COBIT 4.5 está cubierto en cuatro secciones, dentro de cada uno de los procesos de TI, proporciona objetivos de control como de declaración de acciones genéricas de la gestión de buenas prácticas para asegurar que el proceso se mantiene bajo control.



Fuente: IT Governance Institute, COBIT Framework 4.5 en Español Pág. 27

Beneficios

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

Beneficios Tangibles

- Al contar con suficiente personal del área patrimonio la atención al usuario final será más eficiente y eficaz.
- Mayor capacitación al personal de Informática.
- Protección de información.
- Se podrán generar todos los reportes de los incidentes de Cada área.

Beneficios Intangibles

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

    - **Matrices de pruebas**

Cuadro 11: *Programa de Auditoría APO7.4*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)	
APO7. Gestionar los Recursos Humanos	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
APO7. 1 .Mantener la dotación de personal suficiente y adecuado ▪ Brindar al personal seleccionado funciones específicas para poder hacer actividades sin interrupciones. ▪ Generar una armonía en el ambiente de trabajo. ▪ Realizar capacitaciones a todo el personal en el manejo de Tl.	▪ 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 del área. ▪ El riesgo de que no haya un orden dentro de las diferentes áreas por falta de un proceso disciplinario.

Fuente: Elaboración propia

Cuadro 12: *Programa de Auditoría APO7.4*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)	
APO7. Gestionar los Recursos Humanos	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
APO7. 4 Evaluar el desempeño laboral de los empleados. ▪ Considerar los objetivos funcionales del área como el contexto para establecer las metas individuales del personal. ▪ Establecer los objetivos individuales alineados con los objetivos de los y actividades del área, de manera que exista una contribución de los objetivos de TI. ▪ Proporcionar instrucciones claras y precisas para el buen uso de TI manteniendo una buena estabilidad.	▪ 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 del área. ▪ El riesgo de que no haya un orden dentro de las diferentes áreas por falta de un proceso disciplinario.

Fuente: Elaboración propia

Cuadro 13: *Matriz de prueba APO7.4*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)		
APO7. Gestionar los Recursos Humanos		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
APO7. 4 Evaluar el desempeño laboral de los empleados. ▪ Considerar los objetivos funcionales del área como el contexto para establecer las metas individuales del personal. ▪ Establecer los objetivos individuales alineados con los objetivos de los y actividades del área, de manera que exista una contribución de los objetivos de Tl. ▪ Proporcionar instrucciones claras y precisas para el buen uso de Tl manteniendo una buena estabilidad.	**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 puedan desempeñar una correcta labor en sus funciones que se les otorga .	▪ Checklist. ▪ Entrevista al Jefe del área de patrimonio.

Fuente: Elaboración propia

Cuadro 14: *Programa de Auditoría APO7.6*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)	
A**PO7.1 Gestionar los Recursos Humanos**	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
APO7. 6 Gestionar el personal contratado. ▪ Implementar políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por el jefe del área, de acuerdo con la política de contratación de TI. ▪ Proporcionar a los encargados al personal a contratar 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 al personal no adecuado para la labor De los procesos del área. ▪ Riesgo de contratar personal no apto para las funciones requeridas para el área ▪ Riesgo que el personal a contratar no se adecue a la labor de las funciones.

Fuente: Elaboración propia

***Cuadro 15**: Matriz de prueba APO7.6*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)		
APO7. Gestionar los Recursos Humanos		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
APO7. 6 Gestionar el personal contratado. ▪ Implementar políticas y procedimientos que describan cuándo, cómo y qué tipo de trabajo puede ser realizado o incrementado por el jefe del área, de acuerdo con la política de contratación de TI. ▪ Proporcionar a los encargados al personal a contratar 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 de patrimonio. **Probando que:** Se está gestionando de manera apropiada el personal contratado, de acuerdo a las políticas y procedimientos del área.	▪ Checklist. ▪ Entrevista al Jefe del área de patrimonio.

Fuente: Elaboración propia

***Cuadro 16**: Programa de Auditoría AI1.2*

DOMINIO: ADQUIRIR E IMPLANTAR	
AI1. Identificar soluciones automatizadas	
Identificación de soluciones técnicamente factibles y rentables para definición de los requerimientos técnicos y del área	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
AI1.2 Reporte de Análisis de Riesgos ▪ Identificar los posibles riesgos del área. ▪ Analizar la posible solución para los riesgos encontrados. ▪ Entregar un informe con todos los riesgos encontrados durante la auditoria. ▪ Cumplir con los requisitos legales de las normativas nacionales e internacionales que persiguen los mismos objetivos: ISO 9001	▪ Riesgo de Operaciones, es decir, errores humanos durante las mismas, fallos técnicos y de funcionamiento de los equipos, fallos de contención, parámetros del proceso fuera de los límites fijados, deficiencias en el registro. ▪ Riesgo en la construcción y gestión de la seguridad, como errores de diseño, procedimientos operacionales, modificaciones de procesos o equipos inadecuadas, fallos en el sistema de permisos de trabajo, mantenimiento inapropiado, etc.

Fuente: Elaboración propia

Cuadro 17: *Matriz de prueba AI1.2*

DOMINIO: ADQUIRIR E IMPLANTAR		
AI1. Identificar soluciones automatizadas		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
AI1.2 Reporte de Análisis de Riesgos ▪ Identificar los posibles riesgos del área. ▪ Analizar la posible solución para los riesgos encontrados. ▪ Entregar un informe con todos los riesgos encontrados durante la auditoria. ▪ Cumplir con los requisitos legales de las normativas nacionales e internacionales que persiguen los mismos objetivos: ISO 9001	**Evaluación de Controles:** Cumplimiento de los requisitos establecidos por las normas legales. **Probando que:** Mediante el análisis minimizaremos los riesgos del área.	▪ Checklist. ▪ Revisión del informe de análisis de riesgos ▪ Entrevista con el jefe del área de patrimonio.

Fuente: Elaboración propia

Cuadro 18: *Programa de Auditoría AI5.1*

DOMINIO: ADQUIRIR E IMPLANTAR	
AI5. Adquirir recursos de TI.	
Mantener las aplicaciones que se adquieran, para que estén disponibles de acuerdo con los requerimientos del área.	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
AI 5.1 Control de Adquisición ▪ Realizar estudios de factibilidad como se define en los estándares de desarrollo para la adquisición de recursos. ▪ Implementar un plan de procesos de adquisiciones del área de patrimonio y con la estrategia de adquisición. ▪ Proponer un manual de repositorio de adquisiciones para el área.	▪ Riesgo en la pérdida de bienes que se adquieren. ▪ Riesgo en la pérdida de información de los bienes del área. ▪ Riesgo en la cotización de los bienes adquiridos.

Fuente: Elaboración propia

Cuadro 19: *Matriz de prueba AI5.1*

DOMINIO: ADQUIRIR E IMPLANTAR		
AI5. Adquirir recursos de TI.		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
AI5.1 Control de Adquisición ▪ Realizar estudios de factibilidad como se define en los estándares de desarrollo para la adquisición de recursos. ▪ Implementar un plan de procesos de adquisiciones del área de patrimonio y con la estrategia de adquisición. ▪ Proponer un manual de repositorio de adquisiciones para el área.	**Evaluación de Controles:** Cumplimiento en los procedimientos de los estándares y consistentes con el proceso de adquisiciones del área y con la estrategia de adquisición. **Probando que:** Realizará un seguimiento más estricto en el control de las adquisiciones hechas por el área	▪ Checklist. ▪ Revisión detallada de cada bien a adquirir. ▪ Revisión del costo de cada bien a adquirir. ▪ Entrevista con el jefe de patrimonio.

Fuente: Elaboración propia

***Cuadro 20**: programa de auditoría MEA1.1*

DOMINIO: MONITOREAR Y EVALUAR	
MEA1. Monitorear y evaluar el desempeño de TI.	
Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
MEA1.1 Establecer un enfoque de la supervisión. ▪ Involucrar a las partes interesadas y comunicar los objetivos y requisitos 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 del área de patrimonio ante una supervisión que se realice al área informática. ▪ La falta de eficiencia, efectividad y confidencialidad en los procesos realizados dentro del área de patrimonio debido a la no priorización y reserva de recursos.

Fuente: Elaboración propia

Cuadro 21: *Matriz de prueba MEA1.1*

DOMINIO: MONITOREAR Y EVALUAR		
MEA1. Monitorear y evaluar el desempeño de TI.		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
MEA1.1 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 con el jefe oficina general de tecnologías de información, sistemas y estadística (OGTISE) y con el jefe de patrimonio.

Fuente: Elaboración propia

Cuadro 22: *Programa de auditoria MEA1.4*

DOMINIO: MONITOREAR Y EVALUAR	
MEA1. Monitorear y evaluar el desempeño de TI.	
Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
MEA1.4. 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.

Fuente: Elaboración Propia

Cuadro 23: *Matriz de prueba MEA1.4*

DOMINIO: MONITOREAR Y EVALUAR		
MEA1. Monitorear y evaluar el desempeño de TI.		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
MEA1.4. 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.	**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 informática, distribuir los informes al área de patrimonio documentar las incidencias.	▪ Checklist. ▪ Entrevista con oficina general de tecnologías de información, sistemas y estadística (OGTISE) y con el jefe de patrimonio.

Fuente: Elaboración propia

Cuadro 24: *Programa de Auditoría MEA2.7*

DOMINIO: MONITOREAR Y EVALUAR	
MEA 2. 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 del área	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
MEA2.7: Estudiar las iniciativas de aseguramiento. ▪ 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.	▪ 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.

Fuente: Elaboración propia

Cuadro 25: *Matriz de prueba MEA2.7*

DOMINIO: MONITOREAR Y EVALUAR		
MEA 2. Supervisar, evaluar y valorar el sistema de control interno		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
MEA2.7: Estudiar las iniciativas de aseguramiento. ▪ 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 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 informática, distribuir los informes al área de patrimonio documentar las incidencias.	▪ Checklist. ▪ Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE) y con el jefe de patrimonio.

Fuente: Elaboración propia

PROCESOS DEL DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE (DSS)

Cuadro 26: *Programa de Auditoría DSS2.1*

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
DSS 2.1 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.	▪ 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.

Fuente: Elaboración propia

Cuadro 27: *Matriz de prueba 2.1*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS 2. Gestionar Peticiones e Incidentes de Servicio		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
DSS 2.1 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.	**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 con el jefe oficina general de tecnologías de información, sistemas y estadística (OGTISE)

Fuente: Elaboración propia

Cuadro 28: *Programa de Auditoría DSS2.2*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)	
DSS 2. 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
DSS 2.2 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.	▪ 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 el área de patrimonio.

Fuente: Elaboración propia

Cuadro 29: *Matriz de prueba DSS2.2*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS 2. Gestionar Peticiones e Incidentes de Servicio		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
DSS2.2 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 con el jefe oficina general de tecnologías de información, sistemas y estadística (OGTISE). ▪ Revisión de registro de incidentes

Fuente: Elaboración propia

***Cuadro 30**: Programa de Auditoría DSS2.4*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)	
DSS 2. 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
DSS 2.4 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.

Fuente: Elaboración propia

Cuadro 31: *Matriz de prueba DSS2.4*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS 2. Gestionar Peticiones e Incidentes de Servicio		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
DSS2.4 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 con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE) y con el jefe de patrimonio.

Fuente: Elaboración propia

Cuadro 32: *Programa de Auditoría DSS5.3*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)	
DSS 5. 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.	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
DSS 5.3: Gestionar la seguridad de los puestos de usuario final. ▪ Configurar los sistemas operativos de forma segura. ▪ Proteger la integridad del sistema del inventario (INABIF). ▪ Proveer de protección física a los equipos informáticos de usuario final.	▪ Retraso en las funciones de los trabajadores debido a una mala configuración de los sistemas operativos. ▪ Perdida de información debido a la deficiencia en el registro. ▪ Daños en los equipos y/o debido a la falta de protección física de los mismos.

Fuente: Elaboración propia

Cuadro 33: *Matriz de prueba DSS5.3*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS 5. Gestionar Peticiones e Incidentes de Servicio		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
DSS5.3: Gestionar la seguridad de los puestos de usuario final. ▪ Configurar los sistemas operativos de forma segura. ▪ Proteger la integridad del sistema del inventario (INABIF). ▪ Proveer de protección física a los equipos informáticos de usuario final.	**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 con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE) y con el jefe de patrimonio.

Fuente: Elaboración propia

Cuadro 34: *Programa de Auditoría DSS6.1*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)	
DSS 6. Gestionar Controles de Proceso de Negocio	
Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos del área	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
DSS 6.1 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.

Fuente: Elaboración propia

Cuadro 35: *Matriz de prueba DSS6.1*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS 6. Gestionar Controles de Proceso de Negocio		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
DSS6.1 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 del área de patrimonio, el cual satisface los requerimientos de control para los objetivos estratégicos. **Probando que:** Con la supervisión de las actividades de extremo a extremo, se identificará oportunidades de mejora para el área.	▪ Checklist. ▪ Entrevista con el jefe de soporte técnico (informática).

Fuente: Elaboración propia

Cuadro 36: *Programa de Auditoría DSS6.6*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)	
DSS 6. Gestionar Controles de Proceso de Negocio	
Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos del área	
OBJETIVO DE CONTROL DETALLADO	FACTORES DE RIESGO
DSS 6.6: 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 área. ▪ 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 área 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.

Fuente: Elaboración propia

Cuadro 37: *Matriz de prueba DSS6.6*

DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)		
DSS6. Gestionar Controles de Proceso de Negocio		
OBJETIVO DE CONTROL DETALLADO	REVISIÓN ATRAVES DE :	DESCRIPCIÓN DE LA PRUEBA
DSS 6.6: 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 área. ▪ 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 área 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 con el jefe de soporte técnico (informática).

Fuente: Elaboración propia

5.7. Análisis de verificación de resultados

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.

PROCESOS DEL DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)

Cuadro 38: *Evaluación de pruebas APO1.4*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
APO1.Definir un Plan Estratégico de TI				
APO.4 Plan Estratégico de TI				
REVISION A TRAVES DE:	DESCRIPCION DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÒN
Evaluación de controles: Cumplimiento de la normativa establecida por la entidad del ministerio de economía y finanzas para el manejo de información de TI. **Probando que:** El desarrollo de un plan estratégico ayudará mucho en la mejora de los procesos y actividades del área de patrimonio	▪ Planificar el desarrollo del plan estratégico para la mejora del área de patrimonio. ▪ Check List. ▪ Desarrollar una estrategia de manejo de información que se adecue a la planificación del estratégico.	NO EFECTIVO	▪ Plan de trabajo estratégico de TI. ▪ Check List al jefe del área de patrimonio (Anexo 22). ▪ Check List al jefe Entrevista con oficina general de tecnologías de información, sistemas y estadística (OGTISE) (Anexo 23).	▪ Elaborar un plan estratégico para la mejora de los procesos del área. ▪ Elaborar un plan de trabajo para la mejora de los objetivos de las áreas.

Fuente: Elaboración propia

Cuadro 39: *Evaluación de pruebas APO1.5*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
APO1.Definir un Plan Estratégico de TI				
APO1.5 Planes tácticos de TI				
REVISIÓN A TRAVES DE:	DESCRIPCION DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
Evaluación de controles: Cumplimiento de metas, estableciendo los estándares de calidad y cumplimiento de procesos. **Probando que:** El desarrollo de los tácticos nos darán mejor manejo de actividades y procesos se establezcan en el área.	▪ Revisión del plan estratégico siguiendo los procesos y actividades establecidas. ▪ Check List. ▪ Entrevista al jefe del área de patrimonio. ▪ Entrevista al jefe del área de informática.	NO EFECTIVO	▪ Plan de trabajo estratégico de TI. ▪ Check List al jefe del área de patrimonio (Anexo 22).	▪ Se recomienda realizar una revisión periódica del plan de producción establecido. ▪ reflejar la optimización en la asignación y el dimensionamiento de los recursos de que dispondrá el área para sus operaciones futuras. .

Fuente: Elaboración propia

Cuadro 40: *Evaluación De Pruebas APO7.1*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
APO7. Gestionar los recursos humanos de TI				
APO7.1 Mantener la dotación de personal suficiente y adecuado				
REVISION A TRAVES DE:	DESCRIPCION DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
Evaluación de controles: Cumplimiento de política de contrataciones de personal, mediante los procedimientos de contratación y capacitación del personal TI. **Probando que:** El personal de las TI es suficiente y adecuado para el buen manejo de información, sobre todo, si está suficientemente capacitado para desempeñar las funciones que tienen asignadas.	▪ Identificar la capacidad del personal para la buena labor en el área. ▪ Check List. ▪ Entrevista con el jefe del área de patrimonio. ▪ Entrevista con el jefe del área de informática	NO EFECTIVO	▪ Plan Anual de Capacitación del personal TI. ▪ Checklist al jefe del área de patrimonio (Ver Anexo Nº 22). ▪ Checklist Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE). (Anexo Nº23).	▪ Realizar evaluaciones periódicas para detectar las necesidades de personal TI en el área de patrimonio. ▪ Elaborar un documento dirigido a la oficina de RR.HH., solicitando personal idóneo, de acuerdo a las necesidades del área de patrimonio.

Fuente: Elaboración propia

Cuadro 41: *Evaluación De Pruebas APO7.3*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
APO7. Gestionar los recursos humanos de TI				
APO7.3 Mantener las habilidades y competencias del personal				
REVISION A TRAVES DE:	DESCRIPCION DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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 tiene la capacidad de desarrollar las actividades correspondientes bajo presión cumpliendo con sus funciones.	▪ Identificar la capacidad del personal para la buena labor en el área. ▪ Check List. ▪ Entrevista con el jefe del área de patrimonio. ▪ Entrevista con el jefe del área de informática.	NO EFECTIVO	▪ Plan Anual de Capacitación del personal TI. ▪ Checklist al Jefe del área de patrimonio (Ver Anexo Nº 22). ▪ Checklist Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE). (Anexo Nº23).	▪ Establecer un plan de revisiones periódicas para evaluar la evolución de las habilidades y competencias del personal TI en el área de patrimonio.

Fuente: Elaboración propia

Cuadro 42: *Evaluación de pruebas APO7.4*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
APO7. Gestionar los recursos humanos de TI				
APO7. 4 Evaluar el desempeño laboral de los empleados.				
REVISION A TRAVES DE:	DESCRIPCION DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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 del área patrimonio. **Probando que:** Los empleados puedan desempeñar una correcta labor en sus funciones que se les brinda.	▪ Entrevista con el jefe del área de patrimonio.	EFECTIVO	▪ Checklist al Jefe del área de patrimonio (Ver Anexo Nº22). ▪ Checklist Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE). (Anexo Nº23).	▪ Verificar la capacidad del personal que será contratado para el buen desarrollo de las actividades del área de patrimonio.

Fuente: Elaboración propia

Cuadro 43: *Evaluación de pruebas APO 7.6*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
APO7. Gestionar los recursos humanos de TI				
APO7. 6 Gestionar el personal contratado.				
REVISION A TRAVES DE:	DESCRIPCION DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
Evaluación de Controles: Verificar que existan políticas y procedimientos para gestionar el personal TI contratado en el área de patrimonio. **Probando que:** Se está gestionando de manera apropiada el personal contratado, de acuerdo a las políticas y procedimientos del área.	▪ Entrevista con el jefe del área de patrimonio.	EFECTIVO	▪ Checklist al Jefe del área de patrimonio (Ver Anexo Nº25).	▪ Manejar la política de seguridad brindada por el estado al momento de contratar personal para el área patrimonio.

Fuente: Elaboración propia

PROCESOS DEL DOMINIO ADQUIRIR E IMPLEMENTAR

Cuadro 44: *Evaluación de pruebas AI1.2*

DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
AI1. Identificar soluciones automatizadas				
AI1.2 Reporte de Análisis de Riesgos				
REVISION A TRAVES DE:	DESCRIPCION DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
Evaluación de Controles: Cumplimiento de los requisitos establecidos por las normas legales. **Probando que:** Mediante el análisis minimizaremos los riesgos del área.	▪ Checklist. ▪ Revisión del informe de análisis de riesgos	NO EFECTIVO	▪ Cuadro de análisis de riesgos (ANEXO N°19)	▪ Identificar los posibles riesgos. ▪ Elaborar un informe con los posibles riesgos que se puedan encontrar.

Fuente: Elaboración propia

Cuadro 45: *Evaluación de pruebas Al 5.1*

DOMINIO ADQUIRIR E IMPLEMENTAR				
AI5. Adquirir recursos de TI.				
AI 5.1 Control de Adquisición				
REVISIÓN A TRAVES DE:	DESCRIPCION DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
Evaluación de Controles: Cumplimiento en los procedimientos de los estándares y consistentes con el proceso de adquisiciones del área y con la estrategia de adquisición. **Probando que:** Realizará un seguimiento más estricto en el control de las adquisiciones hechas por el área	▪ Checklist. ▪ Revisión detallada de cada bien a adquirir. ▪ Revisión del costo de cada bien a adquirir.	EFECTIVO	▪ Inventario de adquisiciones ▪ Checklist al jefe del área de patrimonio.	▪ Llevar un control detallado de cada adquisición que el área puede adquirir ▪ Realizar un manual de adquisición físico.

Fuente: Elaboración propia

PROCESOS DEL DOMINIO MONITOREAR Y EVALUAR

Cuadro 46: *Evaluación de pruebas MEA1.1*

DOMINIO MONITOREAR Y EVALUAR				
MEA1. Monitorear y evaluar el desempeño de TI.				
MEA1.1 Establecer un enfoque de la supervisión.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
Evaluación de Controles: Verificar que exista un proceso de control de cambios, así mismo se comunica los objetivos y requisitos 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.	▪ Entrevista con el jefe del área de patrimonio.	NO EFECTIVO	▪ Checklist al Jefe del área de patrimonio (Ver Anexo Nº 25).	▪ Establecer un proceso de control de cambios y de gestión en la supervisión y presentación de los informes generados en el área.

Fuente: Elaboración propia

Cuadro 47: *Evaluación de pruebas MEA1.4*

DOMINIO MONITOREAR Y EVALUAR				
MEA1. Monitorear y evaluar el desempeño de TI.				
MEA1.4. Analizar e informar sobre el rendimiento				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÓN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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 informática, distribuir los informes al área de patrimonio documentar las incidencias.	▪ Checklist. ▪ Entrevista con el jefe de informática y con el jefe de patrimonio.	NO EFECTIVO	▪ Checklist al Jefe del área de patrimonio (Ver Anexo Nº 25). ▪ Checklist Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE). (Anexo Nº23).	▪ Definir e implementar cambios en los objetivos y métricas cuando sea procedente así mismo distribuir informes sobre el rendimiento al área de informática.

Fuente: Elaboración propia

Cuadro 48: *Evaluación de pruebas MEA2.1*

DOMINIO MONITOREAR Y EVALUAR				
MEA2 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.				
MEA2.1: Supervisar el control interno.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÓN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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.	▪ Checklist. ▪ Entrevista con el jefe de patrimonio.	EFECTIVO	▪ Checklist al Jefe del área de patrimonio (Ver Anexo Nº 25).	▪ Controlar el ingreso de los registros de software y hardware del área de patrimonio.

Fuente: Elaboración propia

Cuadro 49: *Evaluación de pruebas MEA2.2*

DOMINIO MONITOREAR Y EVALUAR				
MEA2 -Supervisar, Evaluar y Valorar el Sistema de Control Interno.				
MEA2.2: Revisar la efectividad de los controles sobre los procesos de negocio.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÓN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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 del área de patrimonio.	▪ Entrevista con el jefe de patrimonio	EFECTIVO	▪ Checklist al Jefe del área de patrimonio (Ver Anexo Nº 25).	▪ Establecer criterios para realizar autoevaluaciones de control de manera periódica, considerando la efectividad y eficiencia en la supervisión.

Fuente: Elaboración propia

Cuadro 50: *Evaluación de pruebas MEA2.7*

DOMINIO MONITOREAR Y EVALUAR				
ME 2. Supervisar, evaluar y valorar el sistema de control interno				
MEA 2.7: Estudiar las iniciativas de aseguramiento.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÓN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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 informática, distribuir los informes al área de patrimonio documentar las incidencias.	▪ Checklist. ▪ Entrevista con el jefe de informática y con el jefe de patrimonio.	EFECTIVO	▪ Checklist al Jefe del área de patrimonio (Ver Anexo Nº 25).	▪ Evaluar las incidencias que permitan la resolver los problemas del área de patrimonio.

Fuente: Elaboración propia

PROCESOS DEL DOMINIO ENTREGA DE SERVICIOS Y SOPORTE (DSS)

Cuadro 51: *Evaluación de pruebas DSS2.1*

DOMINIO SERVICIO Y SOPORTE				
DSS 2. Gestionar Peticiones e Incidentes de Servicio				
DSS 2.1 Definir esquemas de clasificación de incidentes y peticiones de servicio.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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 con el jefe de soporte técnico (informática). ▪ Revisión de registro de incidentes	NO EFECTIVO	▪ Checklist Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE). (Anexo Nº23).	▪ Establecer una política de gestión de incidentes, teniendo en cuenta la clasificación y priorización de incidentes para el registro de problemas.

Fuente: Elaboración propia

Cuadro 52: *Evaluación de pruebas DSS2.2*

DOMINIO SERVICIO Y SOPORTE				
DSS2. Gestionar Peticiones e Incidentes de Servicio				
DSS2.2 Registrar, clasificar y priorizar peticiones e incidentes.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
Evaluación de Controles: Verificar que se cuente con un registro de clasificación y priorización de peticiones de servicios e incidentes. **Probando que:** Al establecer una supervisión eficiente y efectiva se logrará involucrar a las partes interesadas y acordar un proceso de control de cambios.	▪ Entrevista con el jefe del área de patrimonio.	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.

Fuente: Elaboración propia

Cuadro 53: *Evaluación de pruebas DSS2*

DOMINIO SERVICIO Y SOPORTE				
DSS 2. Gestionar Peticiones e Incidentes de Servicio				
DSS 2.4 Investigar, diagnosticar y localizar incidentes.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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 con el jefe de soporte técnico (informática).	NO EFECTIVO	▪ Checklist Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE). (Anexo Nº23).	▪ Diagnosticar los síntomas del problema que ocurre en el área de patrimonio.

Fuente: Elaboración propia

***Cuadro 54**: Evaluación de pruebas DSS5.3*

DOMINIO SERVICIO Y SOPORTE				
DSS5. Gestionar servicios de seguridad				
DSS5.3: Gestionar la seguridad de los puestos de usuario final.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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 con el jefe de soporte técnico (informática).	EFECTIVO	▪ Checklist Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE). (Anexo Nº23).	▪ Elaborar un diagnóstico de seguridad para el área de patrimonio.

Fuente: Elaboración propia

Cuadro 55: *Evaluación de pruebas DSS6.1*

DOMINIO SERVICIO Y SOPORTE				
DSS 6. Gestionar Controles de Proceso de Negocio				
DSS 6.1 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
Evaluación de Controles: Verificar que exista documentación y supervisión de actividades de control de los procesos del área de patrimonio, el cual satisface los requerimientos de control para los objetivos estratégicos. **Probando que:** Con la supervisión de las actividades de extremo a extremo, se identificará oportunidades de mejora para el área.	▪ Checklist. ▪ Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE)	NO EFECTIVO	▪ Checklist al jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE).	Establecer procesos, herramientas y técnicas que permitan verificar el cumplimiento de las políticas y procedimientos.

Fuente: Elaboración propia

Cuadro 56: *Evaluación de pruebas DSS5.3*

DOMINIO SERVICIO Y SOPORTE				
DSS 6. Gestionar Controles de Proceso de Negocio				
DSS 6.6: Asegurar los activos de información.				
REVISIÓN A TRAVES DE:	DESCRIPCIÓN DE LA PRUEBA	EVALUACIÖN	DOCUMENTOS DE SOPORTE	RECOMENDACIÓN
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 con el jefe de soporte técnico (informática).	EFECTIVO	▪ Checklist Entrevista con el jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE). (Anexo Nº23).	▪ Verificar la política de seguridad del área de informática.

Fuente: Elaboración propia

5.8. Informe Preliminar

En base a la evaluación de las pruebas efectuadas sobre la gestión de TI del área de patrimonio 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 de informática.

5.8.1. Objetivos de control de efectivos

Continuación, se detalla el funcionamiento actual de los controles encontrados efectivos**:**

APO7.4 Evaluar el desempeño laboral de los empleados

Actualmente, existen documentos de los procesos que consideran funcionales del área de patrimonio, al establecer las metas individuales, también se logra implementar un Proceso disciplinario en el área de informática, por parte del jefe de dicha área. Según la entrevista realizada al jefe del área de patrimonio, 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 área de patrimonio.

APO7.6 Gestionar el personal contratado

El documento de las políticas del personal contratado, es proporcionado por la Oficina ejecutiva de recursos humanos de la universidad nacional de Ucayali, 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 del registro de software y hardware. El documento antes mencionado, describe el trabajo realizado de acuerdo con la política de contratación de TI de la universidad y el marco de control de TI. Así mismo se requiere personal calificado para los procesos de selección y contratación de personal.

AI 5.1 Control de Adquisición

Actualmente el área de patrimonio cuenta con un sistema propio donde se registran cada bien adquirido y registrándolo en el entorno externo del área.

MEA1.5: Asegurar la implantación de medidas correctivas

Actualmente se implementan medidas correctivas en el área de patrimonio, según lo señalado por el jefe de informática, se realizan

revisiones de alternativas y recomendaciones, para poder tratar los problemas más importantes que se presentan en el área de patrimonio, informando los resultados.

MEA2.1 Supervisar el control interno

Las evaluaciones del área de informática, según lo mencionado en la entrevista al Responsable de dicha área, permiten mantener los cambios en los procesos del área de patrimonio 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 control interno, el cual permite identificar los procesos más relevantes. Así mismo las excepciones son comunicadas de manera puntual al jefe del área de patrimonio.

MEA2.2 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 jefe del área de informática recalcó que se priorizará el riesgo de acuerdo con los objetivos del área de patrimonio, los cuales permiten tener un adecuado control sobre los procesos del área.

DSS2.4 Investigar, Diagnosticar Y Localizar Incidentes

Existen registros de los principales incidentes identificados en el área de patrimonio, los cuales se localizan y se corrigen oportunamente, según lo mencionado en la entrevista al Responsable de Soporte Técnico del área de informática, señala que en los documentos del área de patrimonio, se registran los diagnósticos de incidentes en las diferentes áreas, 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 problemas, 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.

DSS5.2: Gestionar las Peticiones y los Incidentes del servicio

Proveer una respuesta oportuna y efectiva a las peticiones del 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 del área de patrimonio.

DSS5.3. Gestionar la seguridad de los puestos de usuario final

Se necesita proteger la información del área de patrimonio 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 para lograr tener una seguridad buena y cumplir con las expectativas realizadas.

DSS6.6. 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 jefe de informática, también recalcó que se informa a la Gerencia, acerca de las violaciones y desviaciones que se dan dentro del área de informática y demás áreas de la empresa, para que se tomen las acciones correspondientes.

5.8.2. Objetivos de control no efectivos

Se mostrará el contenido de los controles que no son efectivos que se desarrollaron.

APO1.4 Plan Estratégico de TI

El área de patrimonio no cuenta con un plan estratégico y/o un plan de trabajo para definir los objetivos que se tiene plasmado y poder llevar una mejor gestión y facilitar el cumplimiento de las actividades que se requiere establecer.

Resultado de la discusión con el jefe del área de patrimonio

La falta de un plan de trabajo y/o un plan estratégico hace que el área tenga problemas en el registro de software y hardware maximizando los riesgos que el área pueda tener el transcurso del tiempo.

APO1.5 Planes tácticos de TI

No existe un plan táctico de TI para la seguridad de la

Información de los bienes.

Resultado de la discusión con el jefe del área de patrimonio

La falta del plan táctico de Tl hace que el área tenga inconvenientes en el manejo de información del registro del software y hardware generando pérdidas de información y retraso en los procedimientos que realiza el área de patrimonio.

APO7.1 Mantener la dotación de personal suficiente y adecuado

No existen evaluaciones de requisitos del personal para evaluar las necesidades de personal en forma regular o cambios importantes en el área.

Resultado de la discusión con el jefe del área de patrimonio

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro del área de patrimonio la supervisión de roles y funciones del personal dentro de cada proceso. Para gestionar el adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación del nuevo personal.

APO7.3 Mantener las habilidades y competencias de personal

No existen procesos que puedan ayudar a identificar las diferencias entre las habilidades necesarias y habilidades disponibles del personal del área de patrimonio logrando un control inadecuado en las evaluaciones del personal.

Resultado de la discusión con el jefe del área de patrimonio

La falta de evaluaciones serán identificadas tanto para el personal del área de patrimonio como también el área de informática que utilizan los servicios de información, los cuales constarán en un plan de capa citación de Tl, formulado conjuntamente con el área de informática. El plan está orientado a la gestión del personal que se requiere para el área de patrimonio y minimizando los riesgos que se encontraron al momento de realizar la auditoria determinado la evaluación del personal.

AI1.2 Reporte de Análisis de Riesgos

No existe un proceso de análisis por parte del área de informática para el área de patrimonio, al tener conocimientos en Tl pueden lograr encontrar posibles riesgos que logran afectar al área de patrimonio y brindar una mejora y protección al área.

Resultado de la discusión con el jefe del área de patrimonio

La falta de análisis de riesgos hace que el área de patrimonio no está protegida y pueda causar problemas en la seguridad del registro del software y hardware perjudicando a los usuarios y personal del área de patrimonio.

MEA01.1 Establecer un enfoque de la supervisión

No existe un conocimiento sobre todos los objetivos del personal referentes al área de patrimonio. Además de que no existe un proceso de control de cambios y de gestión en la supervisión del área de patrimonio.

Resultado de la discusión con el jefe del área de patrimonio

Se encuentra documentada la supervisión que se debe realizar, pero por falta de personal con el que cuenta el área de patrimonio, no se da de manera continua.

MEA1.4 Analizar e informar sobre el rendimiento

No existe una documentación de incidencias que permiten contar con una guía adicional para la resolución de los problemas más comunes, los cuales también se debe documentar.

Resultado de la discusión con el jefe del área de patrimonio

La falta de documentación hace que el análisis de rendimiento no sea la adecuada para el área de patrimonio, solo se recomienda documentar lo más relevante y así mismo no se distribuye realizar informes.

MEA2.7 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 de patrimonio.

Resultado de la discusión con el jefe del área de patrimonio

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.

DSS2.1 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 de patrimonio. Además no existen modelos de peticiones de servicios ni fuentes de conocimientos de incidentes y peticiones ocurridos.

Resultado de la discusión con el jefe del área de patrimonio.

Se registran una variedad de incidencias y peticiones de servicio que se dan en el área de patrimonio, pero no se cuenta con un esquema de incidentes y peticiones, ya que no se tiene la suficiente información acerca de esto.

DSS02.2 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 por falta de personal hace este retraso.

Resultado de la discusión con el jefe del área de patrimonio

No existen registros de las peticiones e incidentes que se dan en el área de patrimonio y a la vez no se cuenta con una clasificación y priorización de estos, ya que no se cuenta con el tiempo disponible para realizarse.

5.8.3. Informe final

En este informe se detallará a profundidad las observaciones, recomendaciones y hallazgos encontrados respecto a la auditoria informática en el área de patrimonio de la Universidad Nacional de Ucayali, así

mismo se explicarán los riesgos y se emitirán recomendaciones acerca de dichos objetivos de control hallados No efectivos como también los procesos mal desarrollados.

Identificación del informe

Auditoria informática

Identificación del cliente

Universidad Nacional de Ucayali: 2017

Identificación de la entidad auditada

Área de patrimonio de la Universidad Nacional de Ucayali
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 4.5 (Control Objetives Information Technologies) realizada en el área de patrimonio, y en base al análisis y procedimientos aplicados a las informaciones recopiladas se emite el presente informe.

Fecha de Inicio de la Auditoría: 06 de Junio del 2017
Fecha de Redacción del Informe de la Auditoría: 16 de agosto del 2019

Auditoría realizada por: Bach. Marcos Alexis Bautista Ushiñahua

Objetivo General

Realizar una auditoria informática basada en la metodología COBIT 4.5 para el análisis de los procesos y hallazgos del área de patrimonio.

Objetivos específicos

- Verificar si el hardware y software se adquieren siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.

- Verificar si la selección de equipos y sistemas de computación es adecuada.

- Verificar la existencia de un plan de actividades previo a la instalación.

- Verificar que los procesos de compra de Tecnología de Información, deben estar sustentados en Políticas, Procedimientos, Reglamentos y Normatividad en general, que aseguren que todo el proceso se realiza en un marco de legalidad y cumpliendo con las verdaderas necesidades de la organización para hoy y el futuro, sin caer en omisiones, excesos o incumplimientos.

- Verificar si existen garantías para proteger la integridad de los recursos informáticos.

- Verificar la utilización adecuada de equipos acorde a planes y objetivos.

Resultados de la auditoria

DICTAMEN DE LA AUDITORIA

Para elaborar el dictamen de la auditoría, se tuvo en cuenta los hallazgos encontrados en el proceso evaluado y los controles existentes. El dictamen se basa en las entrevistas, observaciones y las matrices de pruebas que se hizo durante el proceso evaluado respecto a los procesos del área de patrimonio y la, oficina general de tecnologías de información, sistemas y estadística. La escala de medición se encuentra en la norma COBIT 4.5, los valores son de tipo cuantitativo, pero se convierten a cualitativos para explicar el porqué de esa valoración.

A continuación se presenta un ejemplo de la valoración de dos procesos evaluados en un sistema y la escala de medición:

DICTAMEN DE LA AUDITORÍA

A continuación se presentan los resultados definitivos de la auditoria y las recomendaciones de mejoramiento por cada proceso COBIT 4.5 auditado, una vez revisadas las observaciones y aclaraciones hechas por el área auditada.

Observaciones de los objetivos de control no efectivos del área de patrimonio

Observación 1

Por medio de la entrevista y checklist aplicado al jefe del área de patrimonio se detectó que no cuentan con un plan estratégico para desarrollar los procedimientos y políticas con la cuenta el área. Por otra parte también se constató, que no se

cuenta con una metodología para alinear los procesos que realiza el área, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control APO1.4 Plan Estratégico de TI. La cual señala que se debe implementar estos procesos y actualmente no se realiza en el área.

Riesgo

Al no contar con un plan estratégico, el área pierde credibilidad en los procedimientos y políticas con las que cuenta.

Recomendación

Creación de un plan estratégico basándose en la metodología COBIT 4.5 para la mejora del área en cuanto al manejo de información de software y hardware.

Observación 2

Por medio de la entrevista y checklist aplicado al jefe del área de patrimonio y al jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE), se detectó que no cuentan con un plan trabajo actualizado para desarrollar actividades que establecen en el cronograma de actividades. Por otra parte también se constató, que no cuentan con un plan de contingencia, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control APO1.5 Planes tácticos de TI. La cual señala que se debe implementar estos procesos y actualmente no se realiza en el área.

Riesgo

Al no contar con un plan trabajo y un plan de contingencia hace que las áreas estén expuestos a pérdidas de información y expuestos a robos de información.

Recomendación

Crear un plan de trabajo y un plan de contingencia con las actividades específicas que realizará el área.

Observación 3

Por medio de la entrevista y checklist al área de patrimonio 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 APO7.1 Mantener la dotación de personal suficiente y adecuado. La cual señala que se debe implementar estos procesos y actualmente no se realiza en el área.

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 del área de patrimonio por falta de personal para desarrollar los procedimientos que cuenta.

Recomendación:

Planear y ejecutar evaluaciones periódicas para detectar las necesidades de personal en el área de patrimonio. Elaborar un documento dirigido solicitando personal idóneo de acuerdo a las necesidades del área de patrimonio.

Observación 4

Por medio de la entrevista y checklist aplicado al jefe del área de patrimonio, no se detectó procesos que ayuden a identificar las diferencias entre las habilidades necesarias y habilidades disponibles del personal del área. 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 APO7.3 Mantener las habilidades y competencias de Personal. La cual señala que se debe implementar estos procesos y actualmente no se realiza en el área.

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 del área de patrimonio, 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 de patrimonio.

Observación 5

Al realizar el análisis con la metodología COBIT y mediante las entrevistas al jefe del área de patrimonio y al jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE), se llegó a la conclusión de que no existe un proceso de análisis por parte del área de informática con también no existe un informe de dichos riesgos para el área de patrimonio, al tener conocimientos en TI como dice AI1.2 Reporte de Análisis de Riesgos, pueden lograr encontrar posibles riesgos que logran afectar al área de patrimonio y brindar una mejora y protección al área.

Riesgo

Al no tener el conocimientos en los análisis de riesgo hace que el área de patrimonio esté expuestos al fraude robo de información por parte de personas externas.

Recomendación

Realizar un análisis de riesgo detallado indicando los riesgos más relevantes y realizar soluciones para erradicar esos riesgos.

Observación 6

Por medio de la entrevista y checklist al jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE), se verificó que el personal del área de patrimonio, 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 la oficina general de tecnologías de información, sistemas y estadística

(OGTISE), no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control MEA1.1. 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 del área de patrimonio 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 de la oficina general de tecnologías de información, sistemas y estadística (OGTISE) al área de patrimonio.

Observación 7

Por medio de la entrevista y checklist aplicado al jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE), se detectó la no documentación de las incidencias que se presentan en las diversas áreas de la Universidad Nacional de Ucayali más claro en el área de patrimonio, si es que el problema vuelve aparecer. Además no se distribuye informes sobre el rendimiento en el área de la oficina general de tecnologías de información, sistemas y estadística (OGTISE), no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control MEA1.4.Analizar e informar sobre el rendimiento. Lo cual actualmente no se realiza en el área.

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 de la oficina general de tecnologías de información, sistemas y estadística (OGTISE) cuando sea procedente, además emitir informes sobre el rendimiento de dicha área.

Observación 8

Por medio de la entrevista y checklist aplicado al Responsable de Soporte Técnico – Oficina General De Tecnologías De Información, Sistemas Y Estadística (OGTISE), 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 de patrimonio. También se determinó que no se cuenta con modelos de peticiones de servicios ni fuentes de conocimientos de incidentes y peticiones ocurridos, no cumpliendo con las buenas prácticas de COBIT, según el objetivo de control DSS2.1 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.

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 el área.

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 9

Por medio de la entrevista y checklist al jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE), 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 DSS2.2.Registrar, clasificar y priorizar peticiones e incidentes. La cual señala que se debe identificar e implementar dichos procesos y actualmente no se realiza.

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 el área.

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 10

Por medio de la entrevista y checklist al jefe del área de patrimonio se verificó que no cuentan 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. De acuerdo al objetivo de control DSS 2.4 Investigar, diagnosticar y localizar incidentes que se deben realizan en el área.

Riesgo

Al no contar con los diagnósticos de incidentes hace que el área esté vulnerable a cualquier circunstancia del entorno

Recomendación

Realizar diagnósticos de las incidencias que retrasan los procesos y reportarlos.

Observación 11

Por medio de la entrevista y checklist aplicado al jefe de la oficina general de tecnologías de información, sistemas y estadística (OGTISE), se verificó que existe documentación de las actividades de control en los procesos del negocio del área

de patrimonio, 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.

Procesos más relevantes que se midió durante la auditoria informática

PROCESO COBIT 4.5: APO 4: definir las relaciones entre el personal con los procedimientos y políticas del área.

1. Objetivo de la Auditoria: Conceptuar sobre la organización y relaciones entre el personal, los recursos de hardware y software, los documentos soporte, con el fin de establecer el grado de eficiencia de los procesos que se ejecutan en el área de patrimonio.

2. Dictamen**:** Se califica un nivel de madurez definido, por cuanto los procesos, organización y relaciones del área evaluada están contenidos en un manual de procesos y los recursos de hardware y software son adecuados. Sin embargo, al no contar con el personal suficiente este manual no se ha actualizado, pues por no cuentan con el manual de repositorio, lo que hace que no sea posible medirlo y redefinirlo. En procesos clave de administración del área de patrimonio se observa excesiva dependencia en la capacidad y conocimiento que empleados clave tienen del sistema.

3. Hallazgos que soportan el Dictamen:

   - El manual de procesos y perfiles no se ha actualizado de acuerdo a los módulos del sistema, acorde con la estructura de cargos del área lo que dificulta ejecutar planes de contingencia. plan de trabajo capacitación

cruzada, en caso de necesidad de reemplazar o rotar personal clave en las operaciones y administración del sistema.

- Se encontró que la empresa contratista del sistema ejecuta labores de captura de la información, operación directa sobre tablas de la base de datos. Igualmente, realiza labores de auditoría y también administra el sistema operativo, la aplicación y la base de datos. Se considera un nivel de acceso amplio que dificulta establecer controles por parte del área.

- Se encontró que no cuenta con el personal suficiente para realizar los procesos del área.

- Se encontró que el funcionario encargado del módulo de auditoría, realiza solamente el control de usuarios con niveles de seguridad inmediatamente inferiores a él, pero nadie realiza auditoria a las entradas de los súper usuarios del sistema.

4. Recomendaciones:

- Diseñar Bitácora de procesos y perfiles de acuerdo al manual actualizado de funciones y procedimientos del Área patrimonial.

- Documentar los procesos de consulta, lecturas y facturación realizados por fuera del software, para que sean integrados al software. Implementar registro de solicitudes de modificaciones y diseño de soluciones y actualizaciones.

- Documentar y diferenciar en forma precisa los procesos, políticas administrativas y procedimientos de la administración de riesgos, la seguridad de la información, la propiedad de datos y del sistema. Esto es, separar completamente en diferentes responsables los procesos de captura de lecturas, correcciones masivas sobre las tablas de la base de datos, administración de la base de datos, auditoria.

- Contratar más personal y adecuado para las labores de los procesos del área de patrimonio.

- Asignar funciones de auditoría a uno de los trabajadores del área que esté en capacidad de registrar los movimientos realizados por los súper usuarios del sistema, pudiendo el mismo realizar auditorías y ejerciendo controles adecuados sobre la seguridad del servidor e producción y sobre la base de datos.

PROCESO COBIT: Al1: Evaluar y administrar los riesgos encontrados durante la auditoria.

1. Objetivo de la Auditoria**:** Medir los riesgos, su probabilidad e impacto sobre el aplicativo, personal, recursos, procesos, soportes, etc.

2. Dictamen: Se estableció un nivel de proceso a tener en observación por cuanto se hacen análisis y evaluación a la problemática, pero no son permanentes, ni se ha documentado suficientemente. Además, falta capacitación del personal encargado. La detección de riesgos y el establecimiento de controles se hacen, en

gran parte, por iniciativa propia de los empleados, y no en un procedimiento regular de auditoría.

3. Hallazgos que soportan el Dictamen:

- Aunque existe documentación sobre auditorias anteriores y análisis y evaluación de riesgos, no se ha destinado personal para establecer un plan de controles sobre el mismo, lo que impide prevenir posibles fraudes, inconsistencias o pérdidas de información y económicas. Los riesgos tampoco se han clasificado por niveles de criticidad, no se han establecido riesgos residuales.

- No se encontró una política claramente documentada para el manejo de riesgos que presentan nivel de criticidad medio o moderada en el sistema, tales como: infección por virus, plan para enfrentar contingencias en el sistema, plan para detectar y corregir debilidades o huecos en las operaciones, y errores de digitación de datos por parte de los usuarios, generación de pistas de administración y auditoria de datos, actividades de supervisión para detectar el nivel de confianza en los controles automatizados, difusión y adopción de las políticas de seguridad en el procesamiento de datos, revisión metodológica del sistema para proponer mejoras al diseño inadecuado o cuestionable de algunos módulos, corrección de las deficiencias u obsolescencias de los mecanismos de control interno, determinación de especificaciones técnicas inapropiadas, detección de deficiencias en el entrenamiento de los funcionarios que ejecutan los procesos, determinación de estándares de control de

calidad de la información de la base de datos, análisis de cumplimiento de la validación de las reglas del área, Cumplimiento normativo y de las políticas internas en el proceso.

4. Recomendaciones:

- Implementar un software y una metodología para el mejor manejo de los procesos y como también de los riesgos y establecimiento de controles para el mejor desarrollo de los procedimientos y políticas de las áreas, como parte de la Función del área.

- Capacitar al personal encargado de realizar los registros de cada bien informático al sistema, sobre la identificación de riesgos, medición e implementación de controles, enfocada en la seguridad de acceso e integridad de la base de datos.

- Implementar un estándar como metodología para el análisis y la evaluación de riesgos informáticos, que permita que este proceso se lleve a cabo de manera adecuada se debe tener en cuenta que los estándares son apropiados a ciertos tipos de evaluación, como ejemplo COBIT 4.5 que nos brindan los estándares y las escalas de evaluación.

- Retomar las recomendaciones que han realizado en las auditorias anteriores para realizar el análisis, evaluación y gestión de los riesgos encontrados; establecer un sistema de control adecuado al sistema de información y trabajar en la documentación del proceso.

Los resultados obtenidos fueron los siguientes.

- Después de realizar las pruebas y la verificación de procedimientos realizados sobre los módulos que conforman las áreas se relacionan algunos aspectos favorables generales extraídos del informe de la presente auditoría.

- La auditoría se realizó con buena disposición por parte del personal encargado del manejo de los módulos del software de registro de los bienes.

- El software SIGA posee un buen proceso de generación de informes lo que permite la automatización de los procesos, agilizando la generación de informes del área requeridos por las instituciones de control patrimonial minimizando trabajos operativos y estandarizar los procesos.

- Cada proceso para generación de informes tiene incluido Filtros lo que facilita la recolección de datos y su correcto procesamiento para desarrollar mejor el manejo de información de software y hardware de las áreas.

- COBIT 4.5 permitirá alinear los procesos de las áreas minimizando riesgos que puedan afectar los procedimientos que realizan las áreas auditadas.

- El área de patrimonio tiene 6 módulos de trabajo en los cuales solo funcionan 2, esos dos módulos no se abastecen para desarrollar los procedimientos que tiene el área establecida eso es un riesgo muy importante, ya que se puede perder mucha información del área.

- Se recomienda usar el software SIGA patrimonial que permite llevar de manera automatizada el Inventario de existencias organizando y realizando un seguimiento de su inventario fácilmente teniendo en cuenta aspectos como:

- Niveles óptimos de inventario.

- Advertencias de niveles de stock bajos.

- Organización de bienes informáticos del inventario por nombre, descripción, ítem, descripción, etc.

- En cuanto a su funcionamiento, su desempeño es bueno, procesa los datos y realiza las acciones debidas que ofrece al área, ya que es un sistema de información que registra, procesa y almacena datos importantes los cuales se deben manejar con la responsabilidad que amerita.

Hallazgos del Área de patrimonio

Respecto a la Arquitectura de la Información.
Hallazgos 1

El jefe del área de patrimonio no entregó un diccionario de datos donde se recolecte, confirme y se especifique entradas y salidas de los equipos informáticos como manual de repositorio, como también los bienes intangibles y los problemas que está ocurriendo en el área.

Haremos mención a las siguientes:

- Falta de licencias de software.

Se encontró en el área que existe software que no cuentan con licencia para su mejor funcionamiento.

- Falta de software de aplicaciones actualizados.

  Se encontró software que no cuentan con la actualización recomendable para su mejor desarrollo.

- Falta de manejo de información de software y hardware.
  Se encontró deficiencia en el registro de los bienes informáticos.

- No existen diagramas de flujo de los módulos del software adquiridos.

  No cuentan con diagramas de flujos y manuales del software.

- No existen esquemas de diseño donde se detallen la lógica de los procesos que se realiza el área.

  No tienen claro los procesos que se desarrollan en el área.

Recomendaciones

- Documentar el diccionario de datos de los módulos de cada software adquirido y adquirir licencias para un mejor desarrollo de las mismas.

- Incorporar dentro del diccionario de datos, una descripción detallada del personal encargado de actualizar el diccionario de datos con cada actualización del software que se adquiere, la clasificación de tipos de usuarios, los

niveles de acceso y las restricciones para el ingreso de los mismos.

- Tener actualizado el diccionario de datos ante cambios o implementación de nuevas funcionalidades.

- Adquisición de un software para el mejor registro de datos del área.

- Realizar diagramas de flujos para cada proceso que realice el área.

Hallazgos 2

- No existen esquemas de clasificación de la información basada en que tan confidencial son los datos administrados por el área.

- No existen diagramas de flujo de datos o pseudocódigo de las partes de los módulos y sus especificaciones.

- No existen esquemas donde se definan niveles apropiados de seguridad y de controles de protección de datos como controles de acceso.

Recomendaciones

- Diseñar un plan de administración de seguridad de la información que proporcionen los controles de seguridad suficientes que protejan los activos de información.

- Tener adecuadas políticas, procedimientos relacionados con la seguridad de los activos, considerando que la

información debe estar clasificada según la necesidad de acceso.

- Verificar que los controles de información garanticen que la información sea accesible y utilizable solo por el personal autorizado.

- Revisar y evaluar el desempeño (eficiencia y eficacia) del plan de seguridad implementado.

Hallazgos 3

- No existe un manual de diseño del software donde se especifiquen requerimientos del software y hardware para su funcionamiento.

- No existe documentación donde se describa la configuración y funcionamiento del software con lo cuenta el área (INABIF).

- No existen diagramas de flujo de datos o pseudocódigo de las partes de los módulos y sus especificaciones.

Recomendaciones

- Implementar planes de seguridad con el fin de garantizar que la información almacenada en la base de datos permanezca inalterada a menos que sea modificado por personal autorizado manteniendo así la integridad de la información.

- Garantizar la integridad de los datos mediante la implementación de:

  - ✓ Reglas de normalización de datos.
  - ✓ Integridad referencial.

- ✓ Validación de los datos.

Respecto A Procesos Y Relaciones Ti

Hallazgo

- Existe dependencia excesiva hacia el personal que posee conocimiento único ya que no existen políticas que permitan capturar el conocimiento de estos empleados este motivo es por la falta de personal con lo que cuenta el área.

Recomendaciones

- identificar al personal clave de recursos TI y minimizar la dependencias de unos cuantos miembros del área y así generar planes estratégicos y tácticos para la captura documental del conocimiento con el fin de recolectar la mayor cantidad de recursos escritos en donde se especifique una bitácora de los errores más frecuentes presentados en el software y hardware y las soluciones a implementarse.

- Implementar planes fuertes de entrenamiento para hacia el personal nuevo, con el fin de lograr la calidad deseada por la entidad.

- El área debe tener los manuales de funcionamiento de software actualizados, como también los manuales de repositorio de altas y bajas de los bienes y estar al alcance de todos los empleados ya que servirán de material de apoyo para el buen ejercicio de sus actividades.

Respecto A Administra Recursos Ti

Hallazgos 1

- No existe capacitación continua para el personal.

- El proveedor del software realizó una capacitación inicial en el año 2010 fecha en la cual se adquirió el software posterior a este facha no se han realizado capacitaciones pese a las actualizaciones y cambios funcionales en los módulos del software de registro de bienes.

- Dificultad de los empleados para llevar a cabo su trabajo ya que no se realizó la capacitación necesaria y además no existe un manual de software que les permita conocer sus manejo, es por eso que les toma más tiempo familiarizarse con el software que cuenta el área como también con los procedimientos que cuenta el área con el que laboran.

Recomendaciones

- Establecer procesos de capacitación a los operarios de los módulos del software que debe incluir además de charlas acerca del funcionamiento del software los manuales de usuario donde se especifique su funcionalidad.

- La capacitación debe ser obligatoria y continua, ya que es un factor importante que ayuda a los empleados a ser competitivos y más eficientes, dando como resultado una excelente prestación de servicio a los usuarios.

Hallazgo 2

- No existen documentación de control y registro de errores presentados de cada software con el fin de evitar dependencia hacia el personal clave.

Recomendación

- Implementar procesos de gestión del conocimiento que promuevan la captura, evaluación, recuperación, preservación y aprovechamiento del conocimiento y la experticia de los empleados encargados de la operación del personal, con el fin de generar una retroalimentación positiva en los procesos administrados.

Hallazgo 3

- No se toman medidas de seguridad como eliminar privilegios de acceso al Software cuándo se presenta terminación de contrato del personal.

Recomendación

- Establecer políticas generales para la gestión de seguridad de la información que establezcan estrategias como:
  - ✓ Administración de cuentas de usuarios.
  - ✓ Administración de contraseñas de usuario.
  - ✓ Verificación de usos de usuario, contraseñas y niveles de seguridad.
  - ✓ Concientización a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

- Mantener un archivo de auditoría o logs, donde sean registradas todas las operaciones realizadas por los usuarios; en caso de sospecha de falla en la seguridad este

archivo podrá ser consultado para conocer el autor y los daños causados por operaciones irregulares.

- Instituir estrategias para verificar el cumplimiento de las pautas establecidas, relacionadas con control de acceso, creación de usuarios, administración de privilegios, autenticación de usuarios, uso controlado de utilitarios del software.

- Una buena administración de la seguridad permitirá mayor control de las actividades de los usuarios sobre el sistema.

Respecto A Administrar Riesgos Ti

Hallazgo 1

- No existen planes eficaces de mitigación de riesgos cuando se presentan fallas en la realización de los procesos del área.

Recomendación

- Definir, implementar, probar y mantener un proceso para administrar la continuidad del servicio que incluya elementos como: prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal

- Los planes de contingencia deben cumplir, como mínimo con los siguientes requisitos:

- Haber superado las pruebas necesarias para confirmar su eficacia y eficiencia.

- Cubrir por lo menos los siguientes aspectos: identificación de eventos que pueden afectar la operación, actividades a realizar cuando se presentan fallas, alternativas de operación y regreso a la actividad.

- Efectuar semestralmente un diagnóstico sobre la situación de los sistemas que incluya análisis de riesgos y su variación en los niveles.

- Observar los protocolos y procedimientos establecidos para la protección de la información y garantizar la preservación de la información de los bienes del área.

Respecto A Administrar Cambios

Hallazgos

- No existe una política formal que permita el análisis, implementación y seguimiento de cambios requeridos.

- No existen procesos de revisión para garantizar la implantación completa y el correcto funcionamiento de las actualizaciones

- No se tiene documentación física de los equipos rotulados.

Recomendaciones

- Implementar un proceso de actualizaciones de software en el cual se analicen los cambios que la institución necesita que se realicen al software; este procedimiento tiene como objetivo identificar los que necesita el software para cumplir

con todos los requisitos de funcionalidad y eficiencia de la institución.

- El proceso de actualizaciones se deberá especificar aspectos como:

    - ✓ Evaluar, priorizar y autorizar cambios
    - ✓ Llevar un control de cambios.
    - ✓ Garantizar que el cambio quede bien implantado.
    - ✓ Revisión y Aprobación.

Respecto A Planes De Continuidad

Hallazgos

- No existen planes de trabajo como también plan de contingencia efectivos donde se consideren requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de los servicios.

- Al presentarse una falla en el software los empleados tienen como plan de contingencia (informal) que continuar con todos los registros en hojas de cálculo o de forma manual, mientras se restablece el servicio.

- No se llevan a cabo investigaciones de los bienes adquiridos.

Recomendaciones

- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total la prestación del servicio.

- El plan de contingencia es una herramienta que ayudará a que los procesos críticos de la institución continúen funcionando a pesar de una posible falla en los sistemas computarizados; es decir, un plan que permite a la organización seguir prestando servicio a los usuarios.
- Crear un plan de trabajo para el desarrollo efectivo del área.

Respecto A Plan De Seguridad

Hallazgo 1

- Las computadoras encargadas de realizar el registro de los bienes no cuentan con contraseñas para su ingreso al sistema operativo esto hace que la información esté vulnerable a robos de información relevante del área.

- No cuentan con extinguidores para seguridad ante un incendio.

- Existen equipos informáticos que no cuentan con el registro adecuado por tanto están expuestos a hurtos y clonaciones.

Recomendación

- Crear contraseñas para cada computadora en funcionamiento del área, solo tengan acceso a las computadoras el personal encargado.

- Establecer periodos de caducidad de las contraseñas con la finalidad de fomentar al personal encargado de la operatividad del acceso a la información y de la modificación constante de las contraseñas de ingreso para mejorar la seguridad de los datos.

- Solicitar pedido de 2 extinguidores para la seguridad del área ante incendios.

Hallazgo 2

- No existen permisos de acceso de usuario al sistema, todos los operarios pueden acceder a las funciones de otros empleados por ejemplo el personal odontológico puede ingresar a las funciones e historias de clínicas de medicina general y viceversa.

Recomendaciones

- Establecer procedimientos de cuentas de usuario en donde se deben identificar los datos a los que ciertos operarios deben tener acceso, los datos que se deben negar a otros y que datos deberían ser compartidos a todos los empleados; estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados).

La política de administración de permisos debe establecer grupos para los empleados encargados de los módulos de Info-Salud y los respectivos derechos de acceso con el fin de restringir o permitir el acceso de los operarios a archivos para visualización de contenidos o modificación; incrementando así la privacidad de los usuarios y usos inadecuados de la información personal de los pacientes.

- Falta de un plan de trabajo

El área no cuenta con un plan de trabajo para el desarrollo eficiente y eficaz del área.

Recomendación

Realizar un plan trabajo anualmente para tener un mejor desarrollo de los procesos del área.

- Realizar un plan estratégico para la mejora de la información.

No cuentan con un plan estratégico que pueda mejorar las funciones del área.

Recomendación

Desarrollar un plan estratégico para el mejor manejo de registro de información.

- Falta de personal adecuado para los procedimientos del área

No cuenta con el suficiente personal para el desarrollo del registro de los bienes y realizar un trabajo eficiente brindando seguridad en la información.

Recomendación

Contratar personal para el cumplimiento de cada proceso que realiza el área.

- No cuenta con las medidas de preventivas ante desastres naturales.

El área no cuenta con un extintor para protección ante un incendio los equipos están vulnerables.

Recomendación

Realizar un informe sugiriendo la adquisición de 2 extinguidores para el bien del área.

- No cuenta con un plan de contingencia

Actualmente no cuenta con un plan de contingencia posibilitando riesgos en los procedimientos del área.

Recomendación

Realizar un plan de contingencia informando la situación actual en la que se encuentra el área.

- No se cuenta con una metodología de trabajo para el desarrollo de las actividades del área y políticas.

Recomendación

Establecer una metodología que permita alinear los procesos que realiza el área de patrimonio.

- No tienen un control interno de calidad

El área no cuenta con un control de los procedimientos y políticas que realiza el área, por tanto el desarrollo es muy complejo.

Recomendación

Realizar técnicas con instrumentos de recolección de datos para establecer una mejor normativa para el beneficio del área y cumpliendo con los procedimientos y políticas del área.

- Existen equipos informáticos que no cuentan con código patrimonial.

  Al realizar el proceso de evaluación en el área y durante la entrevista que existen equipos informáticos que no están registrados en el software que cuenta el área, por tanto se le toma como un bien rotulado.

  Recomendación

  Realizar a menudo un control de registro de los bienes adquiridos.

- Inexistencia y falta de uso de los manuales de las políticas del área.

  No cuentan con manuales de repositorio físico donde se registran los bienes que son de altas y bajas.

  Recomendación

  Realizar un manual de repositorio para los bienes que son de altas y bajas.

- No cuentan con un respaldo de información en caso de pérdida.

No cuentan con un backup de los datos que maneja, no cuentan con discos duros externos o usb donde puedan guardar la información.

Recomendación

Realizar backups, se recomienda sacar respaldos por la seguridad del manejo de información. Esto lo tienen que hacer semanalmente.

- no cuenta con inventario actualizado.

No cuentan con un inventario actualizado, el inventario es del año 2014, y los inventarios lo tienen que hacer cada 6 meses.

Recomendación

Realizar inventarios cada 6 meses para el mejor registro de información de los equipos informáticos.

- no cuentan con los aparatos adecuados para el registro e inventariado de los equipos informáticos.

No cuentan con equipos modernos que puedan mejorar la labor del personal en el momento de realizar los procesos de registro e inventarios de los equipos informáticos, un ejemplo es el detector de códigos barras de los equipos.

Recomendación

Adquirir equipos modernos para mejorar la labor del personal y realizando una mejor labor para las áreas.

No se cuenta con pruebas que permiten evaluar la efectividad y eficiencia de la integración de las aplicaciones.

No existen pruebas que puedan evaluar la efectividad de las aplicaciones.

Recomendación

Realizar pruebas que puedan medir la efectividad de las aplicaciones.

- No existe un proceso definido de adquisición de los equipos informáticos.

- No cuentan con un manual de repositorio de altas y bajas de los bienes informáticos.

- Las soluciones informáticas no están alineadas con la estrategia de negocio del área.

- No cuentan con una buena seguridad en el manejo de información.

- No cuentan con el software que emite el ministerio de economía y finanzas (SIGA).

  Cuentan con un sistema antiguo.
  Recomendación

  Adquirir el nuevo sistema SIGA que envía el MEF.

- Falta alinear los procedimientos y objetivos del área.

Los procedimientos no se encuentran alineados a una metodología que permita establecer un orden.

Recomendación

Alinear los procedimientos mediante metodologías que logran establecer las normativas de desarrollo de las políticas.

- existen equipos informáticos que se encuentran en un ambiente inapropiado.

  No cuentan con ambiente apropiado para ubicación de los equipos informáticos.

Recomendación

Ubicar en un lugar apropiado los equipos informáticos.

- No existen registros de software intangibles.

  No existe una documentación que mencione que el área toda al software como un bien intangible.

Recomendación

Realizar una documentación del software y registrarlos como bien intangible.

- El cronograma de actividades esta desactualizado.

El cronograma de actividades se encuentra desactivo, el ultimo cronograma de actividades es del año 2014.

Recomendación

Realizar un cronograma de actividades desarrollos los procesos que realiza el área.

- No cuentan con un rol de trabajo.

No cuentan con un rol de trabajo para cada personal del área.

Recomendación

Establecer roles para el persona y lograr un mejor funcionamiento del área.

- No cuentan con un manual de entradas y salidas de bienes.

No cuentan con un manual físico donde se muestra las entradas y salidas de bienes.

Recomendación

Desarrollar un manual físico de entradas y salidas de los bienes adquiridos

- Mala ejecución de las herramientas

La herramienta office no cuenta con licencia de activación.

Recomendación

Adquirir licencias para activar está y mejorar el uso de dichas.

- No se evidencia las ejecuciones de los procesos

No existen evidencias de desarrollo de los procedimientos y políticas del área.

Recomendación

Realizar acciones de control mediante técnicos e instrumentos y verificar los procedimientos.

Hallazgos de la oficina general de tecnologías de información, sistemas y estadística (OGTISE).

Descripción de la situación según su categoría

Ofimática: en la OGTISE se encuentran implementadas cuatro impresoras multifuncionales y seis computadoras, las impresoras con su software debidamente instalados y las computadoras cuenta con un paquete completo de ofimática instalada, con licencia falsa en su versión de Microsoft Office 2013. Y se sabe que esta versión no es la más actual ya que en diciembre del 2018 salió al mercado la versión Microsoft Office 2019, quedando dos versiones retrasadas la versión 2013.

- Se sabe por norma de organización del estado que, todo ordenador debería contar con la licencia pagada al proveedor si es el caso, para evitar sanciones en posibles auditorias por parte del organismo de control pertinente.

- La oficina cuenta con un respaldo de información de documentos, colgados en la nube utilizando un servidor gratuito conocido como mega.nz.

- No existe un calendario de mantenimiento ofimático.

Dirección: Se dividen en las siguientes fases:

- **Planificación:** esta oficina cuenta con un plan estratégico y operativo de sistemas de información presentado, que sugiere mejoras en el tramite documentario, mejoras en la atención de solicitudes de soporte, implementación de un portal de reclamaciones web, mejoramiento de velocidad para la red interna, creación de un sistema integrado con módulo de registro de información para de cada área de la Universidad Nacional de Ucayali, diseño e implementación de un portal web en base a las normas de transparencia y la creación de un sistema de seguimiento de atenciones para el área de soporte técnico.

- **Organización y Coordinación:** por parte de la organización se determinó las funciones a cada responsable de área y a sus respectivos apoyos según el plan estratégico y operativo, a su vez se estableció plazos para rendir informe o entrega según corresponda. Existen procedimientos para la adquisición de bienes y servicios. Se fijaron prioridades como la instalación de los 500 antivirus con licencia para las computadoras de toda la entidad de las cuales no se sabe dónde fueron instaladas ya que no hay registro de que facultades están instaladas.

- **Control:** todo lo acordado en el plan estratégico y operativo es monitoreado por el director de la oficina, así mismo por las altas direcciones que dependen de nuestra información para poder realizar sus funciones. No se está evaluando el rendimiento de cada empleado, en base a los estándares establecidos.

1. **Explotación:** verificar la adecuación de las funciones que sirven de apoyo a las tecnologías de información.

- Se lleva un control de la producción por persona, con metas y plazos establecidos por el director de la oficina.

- De los sistemas desarrollados y ejecutados no existe registro de anomalías o errores en la información debido a la mala codificación.

- Existe un responsable en caso de fallas presentadas en los sistemas implementados por parte de la OGTISE.

- Se realizan validaciones de los proyectos implementados por la oficina y test de calidad durante el tiempo que sea necesarios dependiendo de las circunstancias que se presenten.

- Falta planes de sistemas información.

- No existen programas de capacitación y actualización al personal.

- Inexistencia y falta de uso de los manuales operación.
- No existe un plan de actualización de versiones en su panel de control, de los sistemas implementados.

- El plan de trabajo se encuentra desactualizado.

2. **Desarrollo:** verificar las metodologías utilizadas, revisar el cumplimiento del proceso completado de desarrollo de proyectos.

- No existe documento que contenga las funciones de competencia del área de desarrollo, tampoco está aprobado por la dirección.

- El área de desarrollo y ejecución de software no lleva su control presupuestario.

- Existe un ingeniero de sistemas encargado de del área de desarrollo y un practicante para la administración web.

- Cuenta con un sistema de matrícula web desarrollado en java, con base de datos Oracle 11G, con metodología propuesta por la ONGEI y que se encuentra en funcionamiento.

- Existe un software de módulo de seguimiento de notas desarrollado en power vinder versión 10 con base de datos Oracle, y se están realizando capacitaciones a los docentes, con metodología propuesta por la ONGEI se encuentra funcionando en algunas facultades.

- Cuenta con un sistema de Biblioteca desarrollado en java, con base de datos SQL Server 2008, con metodología RUP esta implementado y en funcionamiento, pero a su vez requiere actualización.

- Se cuenta con un sistema web de carnetisación, desarrollado en java con base de datos SQL Server 2008, con metodología RUB y se encuentra en funcionamiento.

- Hasta el momento solo se está desarrollando un sistema de libro de reclamaciones electrónico, un sistema de seguimiento de atenciones para el área de soporte técnico. Todos desarrollados en java, con base de datos SQL Server. Todas estas establecidas por las normas de SUNEDU y Transparencia.

- Cuenta con un hosting y dominio de alquiler, con su Cpanel y su entorno integrado de desarrollo en mysql, html y html5, css, php 7entre otros.

- Existe un sitio web implementado en el hosting y dominio de alquiler donde se instaló el cliente de joomla en su versión 3.0.0 y no es la versión más actual.

- Presenta inconsistencia de compatibilidad al realizar actualización dentro del administrador joomla del sitio, por contar con la versión 3.0.0 ya que la versión más actual es la 3.9.6 contiene nuevos módulos y son más interactivos.

- El sitio web de la UNU no cuenta con información completa, segura y actualizada, la interfaz gráfica que se muestra en el sitio no es interactiva y mucho menos dinámica.

3. **Mantenimiento:** evaluar el mantenimiento correctivo y preventivo del software.

- No existe contrato de mantenimiento de software.
- incumplimiento en el cronograma de copias de seguridad de equipos de cómputo de usuarios y servidores

- No existe programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo.

- No existe plan logístico para dar soporte al producto de software.

- El sistema de matrícula web y el módulo de seguimiento de notas cuenta con modularidad para conseguir procesos con un mínimo acoplamiento y una máxima relación. Establecidas por norma ISO 12207.

- El sistema de matrícula web y el módulo de seguimiento de notas cuenta con responsabilidad, porque establece

responsables para cada proceso, facilitando la aplicación del estándar en proyectos. Establecidas por norma ISO 12207.

- La documentación de diseño no reflejan los elementos del software.

- Falta de presupuesto para mantenimiento.

- Los sistemas implementados cuentan con metodologías de desarrollo, pero existe ausencia de ellas en cuanto al mantenimiento.

- Se brinda mantenimiento de software de matrícula web, y son mantenimientos constantes por que presenta muchas fallas de registro y entre otros errores propios del sistema. Por otra parte el sistema seguimiento de notas está en proceso de implementación pero el cronograma de actividades está desactualizada.

- Por la parte de soporte técnico se brinda mantenimiento a todos los equipos de cómputo, impresoras y otros de manera efectiva. Pero no se cuenta con un plan de mantenimiento preventivo a todos los equipos de la oficina y entidad, porque realizan actividades del diario o por orden de prioridades.

4. **Base de datos:** administración de la Base de Datos, brindar servicios de apoyo en aspectos de organización y métodos mediante la definición, implementación y actualización de Base de Datos y/o procedimientos administrativos con la finalidad de contribuir a la eficiencia.

- Cuenta con un SGBD como el SQL Server 2008 para la base de datos del sistema siaf, siga y seace, en todos sus módulos.

- El sistema de matrícula web esta implementado con un SGBD Oracle versión 11G, cuenta hasta con la séptima normalización, manteniendo los estándares de llaves y claves que se establece por norma en el estado, basándonos en el modelo del siga académico.

- El módulo de seguimiento de notas esta implementado con un SGBD con su SGBD Oracle, cuenta hasta con la séptima normalización, manteniendo los estándares de llaves y claves que estable por normal en el estado basándonos en el modelo del siga académico.

- El sistema de carnetisación esta implementado con un SGBD SQL Server 2008, cuenta hasta con la tercera normalización establecido en los estándares de la ISO 25012, que se refiere al modelo de calidad de datos.

- El SGBD está instalado en un potente servidor que tiene como sistema operativo al Windows Server 2008.
- No se realiza mantenimiento a la base de datos para verificar su estado.

5. **Calidad:** evaluar la capacidad de realizar trabajo específico y verificar los procesos aplicables del programa de calidad que han sido desarrollados y documentados.

- El sistema de matrícula web y el módulo de seguimiento de notas no refleja lo establecido en la documentación.

- Los sitios web cuentan con un pésimo diseño de interacción para con el usuario.

- En el sitio web la búsqueda de información se dificulta por que no está debidamente categorizada y existe mucho relleno visual.

- Se realizan pruebas de testeo en periodos establecidos para solucionar posibles fallas no contempladas por los desarrolladores.

- No existe orden de prioridades para atenciones en el área de soporte técnico.

6. **Seguridad:** verificar la adecuación de las medidas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos. Revisión de las políticas y normas de seguridad física. Verificar la seguridad del personal, seguridad de datos, hardware, software e instalaciones.

   - Cuenta con el anti virus NOD ESET, se adquirió 500 licencias activas de un año, para uso en los servidores y computadoras, existentes en todo el campus universitario.

   - No se ha normalizado los privilegios de usuarios para las computadoras de la OGTISE, todos las computadoras están con un usuario que es administrador, de ser vulnerado pueden realizar modificaciones o cambios mal intencionados.

   - Se realizan copias de seguridad y de restauración de datos en las seis computadoras y los cuatro servidores pertenecientes a la OGTISE.

- El sistema web de matrícula y el módulo de seguimiento de notas cuentan con los estándares acceso, privilegios y control de usuarios.

- Periódicamente se está realizando cambios de contraseña del administrado de web para evitar posibles ataques o manipulaciones males intencionados.

- El sitio web desarrollado en joomla, está implementado con seguridad en permisos a los grupos y tipos de usuarios establecidos por la configuración del administrador web.

- No existe una vigilancia estricta del área de informática por personal de seguridad dedicado a este sector.

- Existe material altamente inflamable.

- No existe detectores de incendio y extintores automáticos.

- No existe un puesto o cargo específico para la función de seguridad informática.

- La infraestructura es relativamente adecuada, se cuenta con ventiladores, módulos de escritorio, stands, con aire acondicionado pero no todos funcionan adecuadamente, uno de ellos escurre agua por falta de mantenimiento.

- No existe salidas de emergencia, solo una principal.

- No existe un plan de vulnerabilidad, frente a riesgos físicos y no físicos, incluyendo el riesgo informático.

- Se cuenta con seis potentes computadoras, con procesador Intel i5-6700 con 2.9Ghz, 8 Gb ram, Disco

duro de 1 Tera, Pantalla led 17”, kit de mouse, teclado y estabilizador.

7. **Sistemas de Redes:** verificar la adecuación de las medidas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos.

   - Existe un ancho de banda de 80 megas pero con contrato corporativo que garantiza el 90 % en descarga y el 80 % en subida, se puede decir que se cuenta con un buen acceso a internet.

   - El sistema de cableado estructurada no es la correcta según las normas CISCO.

   - Falta un diseño de reestructuración de la red cableada interna de la OGTISE, partiendo de la sala de servidores.

   - Se cuenta con tipo de red LAN, de topología jerárquica hasta la dirección y estrella para las áreas según organigrama.

   - Existe una tecnología llamada PaloAlto Networks que es un firewall potente que observa y analiza todo el tráfico de red, pero aún no se le da el interés necesario para garantizar un mejor control de la red.

   - Falta aplicar por completo el uso de cables UTP categoría 6 establecidos por la norma ANSI.ISO.IEEE descrito en el estándar EIA/TIA-568B. Porque aún se usa cables UTP categoría 5.

- Se cuenta con implementación de fibra óptica en todo el campus universitario pero sin embargo la conexión de red es lenta.

- Se cuenta con protocolos LAN de comunicación para la red local y para la red wifi su modo de seguridad es WPA2/WPA mixe modem pero ya están para cambiarlos.

- Bloqueo de acceso a internet para algunos usuarios que sus funciones son netamente de oficina, habilitación de servidores proxy para acceso de red mediante puertas de enlace.

- No existe un inventario de equipos y software asociados a las redes de datos.

- Falta más puntos de red para conexión cableada a más colaboradores, dentro de la oficina de dirección y soporte técnico.

- La transmisión de información y su uso compartido está protegido por las credenciales de red que el sistema operativo nos proporciona.

8. **Aplicaciones:** verificar la adecuación de los estándares de funcionamiento y procedimiento del área de informática.

    - No cuenta con ninguna aplicación en funcionamiento.

    - Existe un aplicación web de sistema de monitoreo del servicio de transporte de la UNU, que se quedó sin funcionamiento por que no designaron presupuesto para el pago del alquiler de hosting y dominio.

- No existe un plan de desarrollo de aplicaciones propuestos por la OGTISE, no asignaron presupuesto para la creación de nuevas aplicaciones.

Conclusión General

Durante el desarrollo de la Auditoria, se logró realizar una auditoria con lo cual llegamos a ver que hay un déficit en la documentación (inventarios, manual de procedimientos) así como también la inexistencia de documentos importantes para el desarrollo del manejo de información del software y el hardware.

Observaciones

- Actualmente el área de patrimonio y la oficina no cuenta con un plan de trabajo.

- Actualmente el inventario del área de patrimonio y la oficina se encuentra desactualizado.

- El área de patrimonio no cuenta con el personal suficiente para el mejor manejo de información del registro de software y hardware.

- El área de patrimonio como la oficina de sistemas no cuenta con un plan de contingencia.

Recomendaciones

- Desarrollar un plan de trabajo para la mejor del registro de los bienes del área de patrimonio y oficina general de tecnologías de información, sistemas y estadística (OGTISE).

- Contratar más personal en el área de patrimonio para el registro de software y hardware.

- Desarrollar un plan de contingencia

- Actualizar el inventario de registros.

- Actualizar el cronograma de mantenimiento de computadoras de la oficina general de tecnologías de información, sistemas y estadística (OGTISE).

Fecha del informe de la auditoria informática

Planeamiento de ejecución del informe

Fechas: 16-08-2019

Identificación y firma del auditor

Nombres y Apellidos: Marcos Alexis Bautista Ushiñahua

Cargo: Auditor Informático

Firma

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

Se logró identificar el nivel de relación de la Auditoria Informática con metodología COBIT 4.5 con el registro de software y hardware la cual es r = 0.74 con lo cual se comprueba que el índice de relación tiende a la unidad por la tanto es una correlación positiva considerable.

6.1. CONCLUSIONES

- Se analizó los procedimientos y riesgos relativos del área de patrimonio, desarrollando la metodología COBIT 4.5.

- Se Desarrolló un plan de auditoria basado en la metodología COBIT 4.5 definiendo los métodos, técnicas, procedimientos, plan de pruebas para la evaluación de los procedimientos del área de patrimonio de la Universidad Nacional de Ucayali.

- Se logró identificar el grado de relación entre la auditoria informática con metodología COBIT 4.5 con el software, la cual es 0.38 indicando que existe un grado de Correlación positiva media y con respecto al hardware es r= 0.82 indicando que existe un grado de Correlación positiva muy fuerte.

- Se logró identificar el grado de relación entre la auditoria informática con metodología COBIT 4.5 con el Manejo de información de software y hardware la cual es r = 0.71 indicando que existe un grado de Correlación positiva considerable.

- Se elaboró un informe final de la auditoria informática con los hallazgos y recomendaciones para que el área de patrimonio establezca el plan de mejoramiento y el sistema de control adecuado.

6.2. RECOMENDACIONES

- Hacer un análisis de los procedimientos y riesgos relativos del área de patrimonio, desarrollando la metodología COBIT 4.5.

- Para la realización de la auditoria se debe tener en cuenta que cualquier falla o riesgo afecta al área y también puede afectar a otras áreas. Por ello se recomienda poner mucho énfasis en el desarrollado de relación entre la auditoria informática y el procesamiento de adquisición de

bienes de equipos informáticos y software, como La actualización y la calidad del producto.

- Recomendamos estar siempre en constante comunicación con el ente mayor (rector de la Universidad Nacional de Ucayali) para ver los posibles riesgos y fallas que puedan ocurrir en el área, desarrollando un plan de contingencia ante cualquier falla que pueda ocurrir.

- Recomendamos adquirir un software para el mejor control de información del software y hardware adquiridos mediante las comprar que se realizan para la mejora de la institución.

REFERENCIAS BIBLIOGRÁFICAS

Albán Gramonte, A. M. (2016). *Auditoría del sistema de seguridad de información en el hospital III José Cayetano Heredia - castilla; 2016.* PIURA.

Alcalde Garcia, E. (1994). *Clasificación del sotfware.*

Alfaro Paredes, E. A. (2016). *Metodología Para La Auditoría Integral De La Gestión De La Tecnología De Información.* Lima.

Ampuero Chang, C. E. (2016). *Diseño De Un Sistema D2e Gestión De Seguridad De Información Para Una Compañía De Seguros.* lima.

Avilés Freire, V. A. (2016). *Implementación De Una Auditoría Informática Al Sistema De Matriculación De Estudiantes (Sais) De La Universidad Agraria Del Ecuador.* GUAYAQUIL.

Baquero, K. (2012). *COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas).* medellín-colombia.

Barrantes, R. (2008). *Investigación. Un camino al conocimiento.* San José, Costa Rica: Universidad Estatal a Distancia.

Becerra Arévalo, N. P. (2017). *Auditoría Informática Basada En Norma Iso 27004 Para El Control Del Parque Tecnológico De Uniandes Puyo.* Abanto.

Berelson, B. (1971). *Teoria de Analisis.* Chicago.

Briones Véliz, Í. B. (2015). *Auditoria Al Control Y Mantenimiento De La Infraestructura Tecnológica Del Departamento Tecnológico De La Espam Mfl.* junin.

Carrasco Díaz, S. (2010). *Metodologia de la investigación cientifica.* Lima: San Marcos.

Castellano Casas, R. (2001). *definición de siftware.*

CRUZ, I. U. (2009). *definicion de excel.*

Donoso Yáñez, J. (2018). *concepto de informe, literatura peruana .* santiago-chile.

Fernández García, M. (2007). *Glosario de terminos de auditoria informatica.*

Fernando Zavaleta Henriquez. (2015). *auditoria informatica al departamento de informatica del hospital de belen de trujillo.* trujillo.

Flores Rubio, L. A. (2015). *propuesta metodologica de auditoria informatica para realizar la auditoria informatica en el sector financiero.* trujillo.

Gabriela Acosta, J. M. (2016). *Auditoría informática para la optimización del funcionamiento de los sistemas y equipos informáticos de la facultad de ingeniería en sistemas, electrónica e industrial de la universidad Ambato - Ecuador.* abanto-ecuador.

Garcia. (1975). *control de gestion.*

Giopp, A. M. (2005). *Gestión por procesos y creación de valor público: un enfoque analítico.* Santo Domingo: INTEC.

Gomez , V. M. (2014).

Henriquez Zavaleta, F. (2015). *Auditoria Informática al departamento de informática del hospital de belén de Trujillo.* trujillo.

Hernández, R., & Fernández, C. &. (2010). *diseño de investigación.*

IBM. (2017). *IBM SPSS Statistics, Software libre.*

Jamrich parsons, J. (2004). *Definicíon del software.*

juan cherre, A. (2017). *Definición de Hardware.* Proyecto Escuela Virtual - Macro.

juan, r. (2008). *defiinición de encuesta.*

Marcillo Barros, G. F. (2012). *Auditoría Informática De La Cooperativa De Ahorro Y Crédito "Alianza Del Valle" Ltda. Aplicando Cobit 4.0.* SANGOLQUÍ.

Medina, R. (2017). *Definición de observación.*

Mondragon Barrera, M. A. (2014). USO DE LA CORRELACIÓN DE SPEARMAN EN UN ESTUDIO DE INTERVENCIÓN EN FISIOTERAPIA. *Información Cientifica*, 98-104.

Nazareno Vivero, G. (2016). *Auditoría Informática En El Área Administrativa De La Pontificia Universidad Católica Del Ecuador Sede Esmeraldas.* esmeraldas.

Porto, J. P. (2008). *definicion de hardware.* la real academia española.

Ramirez Reyes, G. (2015). *Metodología para auditoría informática en entidades públicas.* lambayeque.

Ramos Arca, C. C. (2015). *Propuesta De Un Plan De Auditoria Informática Para El "Sistema De Información En Salud" Y El "Aplicativo Para El Registro De Formatos Sis" En Los Establecimientos De Salud De La Unidad Ejecutora 400 En La Región Piura En El Año 2015.* piura.

real academia española, e. (2009). *definicion de adquisicion.* españa: real academia española.

Rivera Chávez, M. V., & Zambrano Bravo, M. (2016). *Auditoria Al Control Y Mantenimiento De La Infraestructura Tecnológica Del Departamento Tecnológico De La Espam Mfl.* calcetas.

Rodriguez Quitnuña, V. K. (2017). *Auditoría Informática a la Superintendencia de Telecomunicaciones.* Cuenca-Ecuador.

Samillan, G. R. (2016). *Auditoría Informática Usando Las Normas Cobit En El Centro De Sistemas De Información Del Hospital Regional Docente Las Mercedes De Chiclayo – 2016.* lambayaque.

Santillana González, J. R. (2002). *Auditoria informatica, conceptos previos.* Thomson.

Serrano, G. P. (2000). *Modelos de investigación cualitativa en educación social y animación sociocultural: aplicaciones prácticas.* Narcea Ediciones.

Sobeyda Monica, R. M., & Bonilla Díaz, J. A. (2015). *Auditoria al sistema de información ALPWIN 2.0 En el rubro de cuentas por cobrar del módulo de ventas de la compañía Syscompsa S.A.* Guayaquil.

Sosa, R., & Rodríguez , R. (1990). *técnicas de recolección de datos.*

Soto Sánchez, E. A. (2018). *Definición de Hardware.* hidalgo.

Tamara Oppenheime, e. (2017). *manejo de informacion.* bogota-colombioa.

Tansley, A. G. (1939). *concepto de anális - enfoque sistemas de la információn.* londres.

Torres, C. A. (2006). *Metodología de la investigación: para administración, economía, humanidades y ciencias sociales.* Pearson Educación.

Urbizagastegui Aguilar, S. A. (2016). *Auditoria de seguridad informática aplicada a la Municipalidad Distrital de Santa María.* huacho.

Valencia, J. R. (2002). *Estudio de sistemas y procedimientos administrativos.* Mexico: International Thomson Editores.

vea bayarre, h. (2004). *denominación de un informe final.* ciudad de la habana.

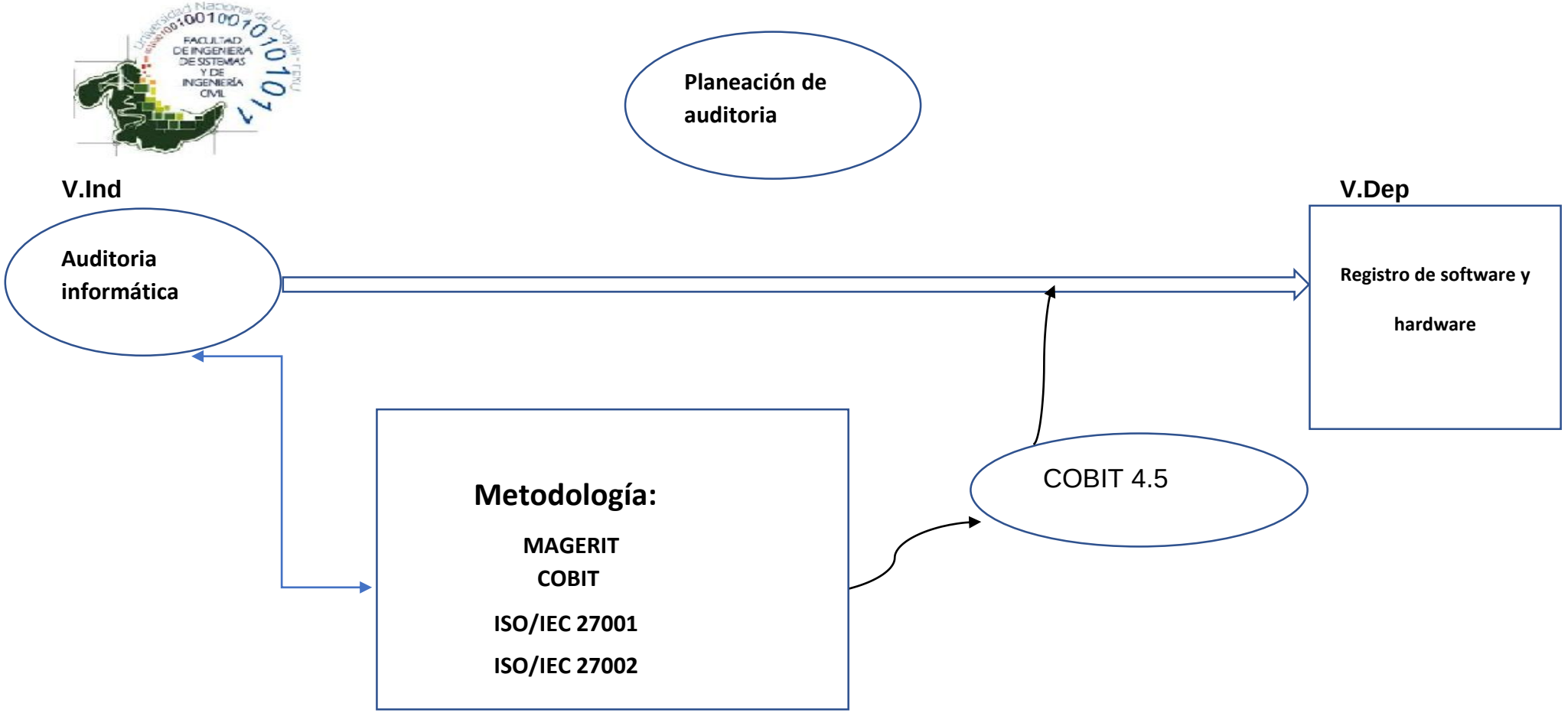
Winslow Taylor, F. (1895). *contabilidad analitica- concepto de control de la informacion .* filadelfia.

ANEXOS

Anexo 1: *Mapa de identificación de problemas*

“AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI ”			
SINTOMAS	**CAUSA**	**CONSECUENCIAS**	**PRONOSTICOS**
Se presenta inconvenientes al adquirir información del uso de los sistemas y equipos informáticos	Existe poca información en cuanto a los equipos y sistemas informáticos un control escaso para ese servicio todo producto informático para por el área de inventario llega con una información muy pobre a lo que quiere realmente saber	Pérdida de tiempo, retraso en el servicio que se requiere realizar.	Realizar una aplicación que realice las preguntas internamente, y que cuente con todo lo necesario para realizar la matrícula y en tiempo real.
Para realizar trabajos relacionadas a las áreas los productos están siendo usados de manera incorrecta.	Existen equipos que están votados sin saber el fin con los que compraron no son usados y si lo hacen lo están usando inadecuadamente.	El no usar los equipos apropiadamente hace que haya fallas muy complejas en la facultad.	El control de información detallada del porque estarán los sistemas y equipos en la facultad
Cuando se desea saber la condición de los equipos informáticos tenemos que ir a buscar información en las oficina administrativa y eso causa perdida de tiempo	Se tiene la información de los equipos informáticos dispersa es tan en forma desordenada.	Mayores tiempos en la obtención de información, utilizando tiempos que se utilizarían para otras actividades.	Contar con toda la información en un solo lugar, y que este al día todo lo relacionado al equipo y saber el fin de porque se compró y el sistema que se implantara dentro de la facultad.
Se presenta una cantidad de inconvenientes al conocer el fin de los equipos informáticos del porque los adquirieron y no les dan usos.	Para realizar cualquier servicio de los equipos informáticos debemos tener en cuenta que con qué fin compraron esos equipos y el permiso correspondiente	Genera conflictos con las personas encargadas de la información con las personas que realizaron la obtención de los sistemas y equipos informáticos.	Lograr tener una optimización apropiada de cada sistema y equipo informático.
Deficiencias en el registro de software y hardware			

Anexo 2: *Mapa de variables*



***Anexo 3**: hoja de ruta de variables*



Dimensiones	Indicaciones
Informe preliminar o de datos	- Elaboración de una ficha Técnica. - Informe de la Situación actual del área en cuanto al manejo de datos. - Recolección de información o datos
Análisis de la situación actual	- Tratamiento de la documentación. - Análisis previos.
Control y gestión de la información	- Verificación - Planificación - Control detallado de la información
Informe final	- Observaciones - Conclusiones

Dimensiones	Indicadores
Manejo de información de software y hardware.	- Usuario encargado de la recepción de software y hardware - Fabricante que brinda los software y hardware - Recolección de información
fines de la adquisición	- Inventariado de los hardware y software del área. - Propósito de adquisición
Software	- Seguridad - Actualización - Tipo de uso
Hardware	- Mantenimiento - Reparación

Anexo 4: *Matriz de consistencia sistémica*

AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017

PROBLEMA	OBJETIVOS	MARCO TEÓRICO	HIPÓTESIS	VARIABLES/ DIMENSIONES/ INDICADORES	Población Muestra
General ¿Cómo la Auditoria Informática con metodología COBIT 4.5 podrá mejorar el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017?. **Específicos** ¿Cómo se analiza los procesos y riesgos relativos que se llevan a cabo en el área de patrimonio de la Universidad Nacional de Ucayali?. ¿Cómo el plan de auditoria basado en la metodología COBIT 4.5 podrá definir los métodos, técnicas, procedimientos, plan de pruebas para la evaluación de los procesos del área de patrimonio de la Universidad Nacional de Ucayali?. ¿En qué medida la auditoria informática con metodología COBIT 4.5 se relaciona con el software y hardware del área de patrimonio de la universidad nacional de Ucayali?. ¿Cómo la auditoria informática con metodología COBIT 4.5, se relaciona con el manejo con el manejo de información de software y hardware del área de patrimonio de la Universidad Nacional de Ucayali?. ¿Cómo reportar los hallazgos de la auditoria y recomendaciones para que el área de patrimonio establezca el plan de mejoramiento y el sistema de control adecuado?.	***General*** Realizar una auditoria informática con metodología COBIT 4.5 para el registro de software y hardware del área de patrimonio de la Universidad Nacional de Ucayali: 2017. .**Específicos** Analizar los procesos y riesgos relativos del área de patrimonio, desarrollando la metodología COBIT 4.5. Desarrollar un plan de auditoria basado en la metodología COBIT 4.5 definiendo los métodos, técnicas, procedimientos, plan de pruebas para la evaluación de los procedimientos del área de patrimonio de la Universidad Nacional de Ucayali. Establecer el nivel de relación entre la auditoria informática con metodología COBIT 4.5 con el software y hardware del área de patrimonio de la universidad nacional de Ucayali. Establecer el nivel de relación entre la auditoria informática con metodología COBIT 4.5, con el manejo de información de software y hardware del área de patrimonio de la Universidad Nacional de Ucayali. Elaborar un informe final de auditoria con los hallazgos y recomendaciones para que el área de patrimonio establezca el plan de mejoramiento y el sistema de control adecuado.	2.1. Antecedentes de la investigación 2.1.1. Tesis Internacionales 2.1.2. Tesis nacionales 2.2. Definición de términos Básicos 2.2.1. Auditoria 2.2.2.COBIT 4.5 2.2.3. Registro de software y hardware	***General*** La Auditoria Informática con metodología COBIT 4.5 mejora el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017. **Específicos:** El análisis de los procedimientos y riesgos relativos del área de patrimonio, se desarrolla con la metodología COBIT 4.5. El desarrollo de un plan de auditoria basado en la metodología COBIT 4.5 define los métodos, técnicas, procedimientos, plan de pruebas para la evaluación de los procedimientos del área de patrimonio de la Universidad Nacional de Ucayali. La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el software del área de patrimonio de la Universidad Nacional de Ucayali. La Auditoria Informática con metodología COBIT 4.5 se relaciona directamente, con el Manejo de información de software y hardware del área de patrimonio de la universidad Nacional de Ucayali. El informe final de auditoria nos reporta los hallazgos y recomendaciones para que el área de patrimonio establezca el plan de mejoramiento y el sistema de control adecuado.	**Variables:** **Variable independiente:** Auditoria informática. **Dimensiones:** – Informe preliminar o de datos – Análisis de la situación actual – Control y gestión de la información – Informe final **Variable dependiente:** Registro de software y hardware. **Dimensiones:** **2 Manejo de información de software y hardware.** **3 Fines de la adquisición** **4 Software** **5 Hardware** **Metodología de Investigación** **Según Barrantes (2008)** • **Tipo de investigación: Aplicada** • **Nivel de investigación: Descriptiva** • **Alcance temporal: Estudios transversales** • **Carácter de medida: Cuantitativo** • **Concepción: Ideográfica** • **Orientación: Comprobación** **Metodología de desarrollo de software:** **COBIT 4.5**	Población **Personas del Área de patrimonio de la universidad nacional de Ucayali y el área de** Muestra **8 Personas del** Área de patrimonio junto con el área de informática de la universidad nacional de Ucayali**. Muestra igual a la población** **Fuentes:** Primarias Secundarias **Técnica:** Cuestionario Observación **Instrumento:** Internet Libros Referencias Bibliografías Encuesta Ficha de observación Diseño de investigación. **Descriptivo correlacional** 

Anexo 5: *Base de datos del Alfa de Cronbach de la variable 1*

Auditoria informática																					Variable 1
	Informe preliminar o de datos						Análisis de la situación actual				Control y gestión de la información						Informe final				
Codigo	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
1	2	1	1	1	1	1	1	1	1	1	2	2	1	3	3	2	1	1	2	2	30
2	3	2	1	2	2	1	3	3	3	2	2	2	2	2	3	2	3	3	2	2	45
3	3	3	2	2	3	2	1	1	3	2	3	2	2	2	1	3	3	2	2	3	45
4	2	1	1	3	2	3	1	1	1	1	1	1	1	1	2	2	2	1	2	2	31
5	3	2	1	2	3	2	2	2	1	1	2	2	3	1	2	3	2	3	2	3	42
6	1	2	1	1	1	2	1	1	2	1	1	2	1	2	3	2	1	3	1	1	30
Varianza	0.5556	0.4722	0.1388889	0.4722	0.6667	0.4722	0.5833	0.5833	0.8056	0.2222	0.4722	0.1389	0.5556	0.4722	0.5556	0.2222	0.6667	0.8056	0.1389	0.4722	47.8055556
S.Varianza	9.4722																				

Fuente: Elaboración Propia

Anexo 6: *Base de datos del Alfa de Cronbach de la variable 2*

Registro de software y hardware																					
	Manejo de información de software y hardware						Fines de la adquisición				Software						Hardware				
Codigo	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Variable 2
1	3	2	3	1	2	3	3	3	1	3	2	1	3	3	2	3	3	2	1	3	47
2	3	3	3	1	2	3	1	3	2	3	3	3	3	3	3	2	2	1	3	3	50
3	2	3	1	3	1	1	1	1	1	1	1	2	2	1	2	2	1	2	1	1	30
4	2	2	2	3	2	3	1	2	3	3	2	3	2	3	2	2	3	1	2	3	46
5	2	3	1	1	1	1	2	2	1	1	1	3	2	2	1	2	1	1	2	3	33
6	3	1	1	1	2	2	2	2	1	2	1	2	1	1	1	3	2	3	2	2	35
Varianza	0.25	0.5556	0.8056	0.8889	0.2222	0.8056	0.56	0.47	0.58	0.81	0.56	0.56	0.47	0.81	0.47	0.22	0.67	0.56	0.47	0.58	59.80556
S.Varianza	11.3056																				

Fuente: Elaboración Propia

Anexo 7: *Confiabilidad De La Variable Auditoria Informática*

CONFIABILIDAD

ANÁLISIS ESTADÍSTICO ALFA DE CRONBACH

Variable: Auditoria informática

$$\alpha = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum V_i}{\sum V_T}\right)$$

$$\alpha = \left(\frac{20}{19}\right).\left(1 - \frac{9.4722}{47.8056}\right)$$

$$\alpha = 0.84$$

ALFA DE CRONBACH	Ítems
0,84	20

Fuente: Salida del SPSS V24

Interpretación: El estadístico ALFA DE CRONBACH, aplicado al instrumento de investigación, arrojó 0,84. Por ende el instrumento tiene un grado de confiabilidad **MUY ALTA**, para la investigación, por el resultado que se obtuvo.

Pucallpa; 13 de julio del 2017

Marco Antonio Díaz Apac
Lic. Especialidad de Matemática
Doctor en Administración de la Educación

Anexo 8: *Confiabilidad de la variable Registro de Software y Hardware*

CONFIABILIDAD

ANÁLISIS ESTADÍSTICO ALFA DE CRONBACH

Variable: Registro de software y hardware

$$\alpha = \left(\frac{k}{k-1}\right)\left(1 - \frac{\sum V_i}{\sum V_T}\right)$$

$$\alpha = \left(\frac{20}{19}\right).\left(1 - \frac{11.3056}{59.8056}\right)$$

$$\alpha = 0.85$$

ALFA DE CRONBACH	Items
0,85	20

Fuente: Salida del SPSS V24

Interpretación: El estadístico ALFA DE CRONBACH, aplicado al instrumento de investigación, arrojó 0,85. Por ende el instrumento tiene un grado de confiabilidad **MUY ALTA**, para la investigación, por el resultado que se obtuvo.

Pucallpa; 13 de julio del 2017

Marco Antonio Díaz Apac
Lic. Especialidad de Matemática
Doctor en Administración de la Educación

Anexo 9: *Oficio N° 001-2007*

Pucallpa, 12 de julio del 2017

OFICIO Nº 001 – 2017

Señor: Ing. Mg. Diana Margarita Diaz Estrada

Presente.-

ASUNTO: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO

Tengo el alto honor de dirigirme a Ud. para saludarle muy cordialmente y hacer de su conocimiento que soy alumno del IX Ciclo de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Ucayali, y estoy desarrollando el proyecto de tesis: **"AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT PARA EL REGISTRO DE SOFTWARES Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017".**

Por tal motivo, recurro a Ud. para solicitar su opinión profesional para validar los instrumentos de mi investigación.

Para lo cual acompaño:

1. Matriz de consistencia
2. Matriz de recolección de datos
3. Ficha de opinión de expertos
4. Instrumento de investigación

Agradezco por anticipado su aceptación a la presente, quedando de Ud. muy reconocido.

Atentamente

Bautista Ushiñahua marcos

Anexo 10: *Validación de los Instrumentos, por los expertos*

VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Apellidos y Nombres del Experto: DIAZ ESTRADA, DIANA MARGARITA

1.2 Cargo e Institución donde labora: Responsable Oficina Informatica - UNU - FIS.

1.3 Nombre del instrumento motivo de Evaluación: Cuestionario

1.4 Autor del Instrumento: Marcos Alexis Bautista Ushiñahua

INDICADORES	CRITERIOS	Deficiente 0 –20 %	Regular 21– 40 %	Bueno 41–60 %	Muy bueno 61–80 %	Excelente 81–100 %
1. CLARIDAD	Esta formulada con lenguaje apropiado		X			
2. OBJETIVIDAD	Est expresa ado en conductas observables			X		
3. ACTUALIDAD	Adecuado el alcance de ciencia y tecnología			X		
4. ORGANIZACIÓN	Existe un a organización lógica			X		
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad		X			
6. INTENCIONALIDAD	Adecu par ado a valorar aspectos del sistema de evaluación y desarrollo de capacidades cognosciti vas			X		
7. CONSISTENCIA	Basados en aspectos Teóricos – científicos de la Tecnol			X		

	ogía Educativa					
8. COHERENCIA	Entre los indicadores y las dimensiones		X			
9. METODOLOGIA	La estrategia responde al propósito del diagnostico.			X		
10. OPORTUNIDAD	El instrumento ha sido aplicado en el momento oportuno o más adecuado.			X		

II. OPINIÓN DE APLICABILIDAD:

Seria recomendable agregar el termino Software y Hardware como "Recursos Informaticos".

III. PROMEDIO DE VALORACIÓN: [ ]

Pucallpa,....12 de julio del 2017

VALIDACIÓN DEL INSTRUMENTO

ITEMS	PREGUNTA	APRECIACIÓN		OBSERVACIONES
		SI	NO	
1	¿El instrumento responde al planteamiento del problema?	X		
2	¿El instrumento responde a los objetivos del problema?	X		
3	¿Las dimensiones que se han tomado en cuanta son adecuadas para la realización del instrumento?	X		
4	¿El instrumento responde a la operacionalización de las variables?	X		
5	¿La estructura que presenta el instrumento es de forma clara y precisa?	X		
6	¿Los ítems están redactados en forma clara y precisa?	X		
7	¿El número de ítems es el adecuado?		X	
8	¿Los ítems del instrumento son validos?	X		
9	¿Se debe incrementar el número de ítems?	X		
10	¿Se debe eliminar algunos ítems?		X	

Aportes y/o sugerencias:

Ampliar numero de ítems para poner en contexto a las entrevistadas.

Nombre y Firma

Fecha: 12/07/2017

VALIDACIÓN DE EXPERTOS

I. DATOS GENERALES

Nombre:
DIANA M. DIAZ ESTRADA

Especialidad:
Ing. Sistemas

Fecha:
12/09/2017

II. OBSERVACIONES EN CUENTA A:

1. FORMA:
ADECUADA

2. CONTENIDO:
CORRECTO PERO SE RECOMIENDA AÑADIR MAS ITEMS.

3. ESTRUCTURA:
ADECUADA

III. APORTES Y/O SUGERENCIAS:

Replantear nombre del Proyecto de Tesis para abarcar Recursos Informaticos.

Luego, de revisado el documento procede a su aprobación.

SI [X] NO [ ]

Nombre y Firma

Fecha: 12/09/2017

Pucallpa, 12 de julio del 2017

OFICIO Nº 001 – 2017

Señor: CESAR NILTON AYRA APAC

Presente.-

ASUNTO: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO

Tengo el alto honor de dirigirme a Ud. para saludarle muy cordialmente y hacer de su conocimiento que soy alumno del IX Ciclo de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Ucayali, y estoy desarrollando el proyecto de tesis: **"AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT PARA EL REGISTRO DE SOFTWARES Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017".**

Por tal motivo, recurro a Ud. para solicitar su opinión profesional para validar los instrumentos de mi investigación.

Para lo cual acompaño:

1. Matriz de consistencia
2. Matriz de recolección de datos
3. Ficha de opinión de expertos
4. Instrumento de investigación

Agradezco por anticipado su aceptación a la presente, quedando de Ud. muy reconocido.

Atentamente

Bautista Ushiñahua marcos

VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Apellidos y Nombres del Experto: CESAR NIXON AYRA APAC

1.2 Cargo e Institución donde labora: PROYECTO DE INVESTIGACION

1.3 Nombre del instrumento motivo de Evaluación: CUESTIONARIO

1.4 Autor del Instrumento: Marcos Alexis Bautista Ushiñahua

INDICADORES	CRITERIOS	Deficiente 0 –20 %	Regular 21– 40 %	Bueno 41–60 %	Muy bueno 61–80 %	Excelente 81–100 %
1. CLARIDAD	Esta formulada con lenguaje apropiado		X			
2. OBJETIVIDAD	Est expresa ado en conductas observables			X		
3. ACTUALIDAD	Adecuado el alcance de ciencia y tecnología			X		
4. ORGANIZACIÓN	Existe una organización lógica			X		
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad			X		
6. INTENCIONALIDAD	Adecuado para valorar aspectos del sistema de evaluación y desarrollo de capacidades cognositivas			X		
7. CONSISTENCIA	Basados en aspectos Teóricos – científicos de la Tecnol			X		

	ogía Educativa					
8. COHERENCIA	Entre los indices, indicadores y las dimensiones		X			
9. METODOLOGIA	La estrategia responde al propósito del diagnostico.			X		
10. OPORTUNIDAD	El instrumento ha sido aplicado en el momento oportuno o más adecuado.			X		

II. OPINIÓN DE APLICABILIDAD:

.....

.....

III. PROMEDIO DE VALORACIÓN: 50%

Pucallpa,....12 de julio del 2017

VALIDACIÓN DEL INSTRUMENTO

ITEMS	PREGUNTA	APRECIACIÓN		OBSERVACIONES
		SI	NO	
1	¿El instrumento responde al planteamiento del problema?	X		
2	¿El instrumento responde a los objetivos del problema?	X		
3	¿Las dimensiones que se han tomado en cuanta son adecuadas para la realización del instrumento?	X		
4	¿El instrumento responde a la operacionalización de las variables?	X		
5	¿La estructura que presenta el instrumento es de forma clara y precisa?	X		
6	¿Los ítems están redactados en forma clara y precisa?	X		
7	¿El número de ítems es el adecuado?	X		
8	¿Los ítems del instrumento son validos?	X		
9	¿Se debe incrementar el número de ítems?	X		
10	¿Se debe eliminar algunos ítems?		X	

Aportes y/o sugerencias:

.....NINGUNA.....

.....

Nombre y Firma

Fecha:...../...../.....

VALIDACIÓN DE EXPERTOS

I. DATOS GENERALES

Nombre: CESAR NILTON AYBAR APAC

Especialidad: INGENIERIA DE SISTEMAS

Fecha: 12/07/2012

II. OBSERVACIONES EN CUENTA A:

1. FORMA:

NINGUNA

2. CONTENIDO:

NINGUNA

3. ESTRUCTURA:

AUMENTAR ITEMS.

III. APORTES Y/O SUGERENCIAS:

Luego, de revisado el documento procede a su aprobación.

SI [X] NO [ ]

Nombre y Firma

Fecha: ../...../.....

Pucallpa, 12 de julio del 2017

OFICIO Nº 001 – 2017

Señor:..... AGURTO CHERRE CESAR AUGUSTO .....

Presente.-

ASUNTO: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO

Tengo el alto honor de dirigirme a Ud. para saludarle muy cordialmente y hacer de su conocimiento que soy alumno del IX Ciclo de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Ucayali, y estoy desarrollando el proyecto de tesis: **"AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT PARA EL REGISTRO DE SOFTWARES Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017".**

Por tal motivo, recurro a Ud. para solicitar su opinión profesional para validar los instrumentos de mi investigación.

Para lo cual acompaño:

1. Matriz de consistencia
2. Matriz de recolección de datos
3. Ficha de opinión de expertos
4. Instrumento de investigación

Agradezco por anticipado su aceptación a la presente, quedando de Ud. muy reconocido.

Atentamente

Bautista Ushiñahua marcos

VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Apellidos y Nombres del Experto: CESAR AUGUSTO AGUNTO CHERRE

1.2 Cargo e Institución donde labora: OFICINA DE PRACTICAS PRE PROFESIONALES DE I.J.

1.3 Nombre del instrumento motivo de Evaluación: CUESTIONARIO

1.4 Autor del Instrumento: Marcos Alexis Bautista Ushiñahua

INDICADORES	CRITERIOS	Deficiente 0 –20 %	Regular 21– 40 %	Bueno 41–60 %	Muy bueno 61–80 %	Excelente 81–100 %
1. CLARIDAD	Esta formulada con lenguaje apropiado			X		
2. OBJETIVIDAD	Est expresa ado en conductas observables			X		
3. ACTUALIDAD	Adecuado el alcance de ciencia y tecnología			X		
4. ORGANIZACIÓN	Existe un a organización lógica			X		
5. SUFICIENCIA	Comprende los aspectos de cantidad y calidad			X		
6. INTENCIONALIDAD	Adecu par ado a valorar aspectos del sistema de evaluación y desarrollo de capacidades cognosciti vas				X	
7. CONSISTENCIA	Basados en aspectos Teóricos – científicos de la Tecnol				X	

	ogía Educativa					
8. COHERENCIA	Entre los indices, indicadores y las dimensiones					X
9. METODOLOGIA	La estrategia responde al propósito del diagnostico.					X
10. OPORTUNIDAD	El instrumento ha sido aplicado en el momento oportuno o más adecuado.				X	

II. OPINIÓN DE APLICABILIDAD:

.....

.....

III. PROMEDIO DE VALORACIÓN: 60%

Pucallpa,....12 de julio del 2017

VALIDACIÓN DEL INSTRUMENTO

ITEMS	PREGUNTA	APRECIACIÓN		OBSERVACIONES
		SI	NO	
1	¿El instrumento responde al planteamiento del problema?	X		
2	¿El instrumento responde a los objetivos del problema?	X		
3	¿Las dimensiones que se han tomado en cuanta son adecuadas para la realización del instrumento?	X		
4	¿El instrumento responde a la operacionalización de las variables?	X		
5	¿La estructura que presenta el instrumento es de forma clara y precisa?	X		
6	¿Los ítems están redactados en forma clara y precisa?	X		
7	¿El número de ítems es el adecuado?	X		
8	¿Los ítems del instrumento son validos?	X		
9	¿Se debe incrementar el número de ítems?	X		
10	¿Se debe eliminar algunos ítems?	X		

Aportes y/o sugerencias:

.....

.....

Cesar Augusto Agusto Chec
INGENIERO DE SISTEMAS
C.I.P. N° 1[illegible]

Nombre y Firma

Fecha: 12.07.17

***Anexo 11**: Arquitectura de equipos informáticos (Vigentes)*

Equipos de cómputos y software

Área de patrimonio

Equipos	Componentes	Software
Core i7	Procesador 4 Ghz. 8 gb de RAM, disco duro de 1 tb Pertenece: José Moncada	Windows 10 y sistema de inventario
Core i5	Procesador 4 Ghz. 8 gb de RAM, disco duro de 1 tb. Pertenece: José Moncada	Windows 10 y office
Core i7	Procesador 4 Ghz. 8 gb de RAM, disco duro de 1 tb. Pertenece: José Moncada	Windows 10 y sistema de tramite documentario
Core i3	Procesador 4 Ghz. 8 gb de RAM, disco duro de 1 tb Pertenece: José Moncada	Windows 10 y siga
Core i7	Procesador 4 Ghz. 4 gb de RAM, disco duro de 1 tb Pertenece: José Moncada	Windows 10 y siga
Core i7	Procesador 4 Ghz. 8 gb de RAM, disco duro de 1 tb Pertenece: José Moncada	Windows 10
Core i5	Procesador 4 Ghz. 8 gb de RAM, disco duro de 1 tb. Pertenece: José Moncada	Windows 10
Core i7	Procesador 4 Ghz. 8 gb de RAM, disco duro de 1 tb	Windows 10

Fuente: Elaboración propia

Anexo 12: *Recursos Humanos y materiales*

RECURSOS HUMANOS

a) Encuestas
   - ✓ Encuestador
   - ✓ Digitador
   - ✓ Encuestados
   - ✓ Asesor

MATERIALES

- ✓ Hoja papel bond A4
- ✓ Lapiceros
- ✓ Tinta a color y blanco y negro
- ✓ Laptop HP
- ✓ Impresora
- ✓ Folder

Anexo 13: *Encuesta para medir la variable Auditoria Informática*

ENCUESTA, PARA MEDIR LA VARIABLE AUDITORÍA INFORMÁTICA, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar El Instrumento ENCUESTA, para medir la Variable Auditoría Informática en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

AUDITORIA INFORMÁTICA

PG.	Informe preliminar	Malo	Regular	Bueno
1	¿Cómo calificaría usted la elaboración de una ficha técnica para realización de una auditoria informática en el área de patrimonio?			
2	¿Cómo cree que es el rendimiento de las adquisiciones de las TI?			
3	¿Qué le parece el manejo de información en el área de patrimonio?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo define la falta de información del área de patrimonio de las TI?			
6	¿Qué le parece la forma de recopilación de la información?			
PG.	**Análisis de la situación actual**			
7	¿Cómo calificas el proceso de datos de la información?			
8	¿Qué le parece la forma de manejo de información escasa dentro del área?			
9	¿Qué calificación daría usted al posible riesgo de pérdidas de información del área?			

10	¿Cómo califica usted la falta de interés de las adquisiciones dentro del área?			
PG.	**Control y gestión de la información**			
11	¿Cómo califica el rendimiento de la seguridad de datos?			
12	¿Qué le parece la implantación de la auditoria informática para el mejor control de seguridad y manejo de la información?			
13	¿Cómo califica usted el plan de trabajo del área para minimización de riesgos en la perdida de datos informáticos?			
14	¿Qué le parece a usted la utilización de una metodología capaz de mejorar el desarrollo de información del área?			
15	¿Usted como personal administrativo cómo calificaría el estado de la seguridad de información?			
16	¿Cómo observa usted que se está dando el uso de las tecnologías de información?			
PG.	**Observaciones**			
17	¿De acuerdo con la investigación como califica las falencias encontradas en el manejo de información?			
18	¿Cómo califica el hallazgo de riesgos en las TI?			
19	¿Cómo califica el estudio que se realizó del manejo de información?			
20	¿Qué le parece a usted la metodología que se realizará para solución del problema encontrado en el área?			

Anexo 14: *Encuesta para medir la variable Registro de Software y Hardware*

ENCUESTA, PARA MEDIR LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar el Instrumento ENCUESTA, para medir la Variable Registro de Software y Hardware en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

REGISTRO DE SOFTWARE Y HARDWARE

PG.	Manejo de información de software y hardware	Malo	Regular	Bueno
1	¿Cuál es el nivel de capacidad que tiene el personal en el manejo de información de los equipos informáticos?			
2	¿Qué le parece la falta de capacitación del personal en las actualizaciones y versiones?			
3	¿Cómo califica la calidad del producto adquirido?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo califica usted la falta de información de los software y hardware, con qué fin fueron comprados?			
6	¿Qué le parece a usted la falta de un plan de contingencia ante un problema o riesgo?			
PG.	**Fines de la adquisición**			
7	¿Cómo calificas el proceso de datos de la información de los equipos informáticos?			
8	¿Cómo califica usted el manejo de la información del software y el hardware del área?			

9	¿Qué le parece a usted la calidad de los equipos informáticos que fueron adquiridos?			
10	¿Cuál es el nivel de mejora al adquirir software y hardware de última generación?			
PG.	**Software**			
11	¿Qué le parece la seguridad del software adquiridos, en cuanto a los datos guardados?			
12	¿Cómo califica usted el nivel de seguridad de información del software?			
13	¿Qué le parece las versiones que brindan los proveedores para la actualización de diversos software?			
14	¿Cómo califica la actualización de los programas antiguos a las nuevas versiones?			
15	¿Qué le parece el uso establecido para el software, Función de dicha?			
16	¿Cómo califica usted el uso de programas que bloquean páginas prohibidas?			
PG.	**Hardware**			
17	¿Cómo califica el servicio de mantenimiento al hardware (PC, impresoras, discos duros, laptops, etc?			
18	¿Qué le parece el tiempo que establecen para dar mantenimiento a las pcs?			
19	¿Cómo califica el nivel de solución de las fallas ocurridas?			
20	¿Qué le parece la reparación de los equipos informáticos ante riesgos y tiempo de uso?			

Anexo 15: *modelo de Informe de auditoría informática*

1. **Identificación del informe**

   Auditoria informática

2. **Identificación del cliente**

   El área de patrimonio

3. **Identificación de la entidad auditada**

   Universidad Nacional de Ucayali

4. **Objetivo General**

   Determinar el nivel de relación entre la Auditoria Informática con metodología COBIT 4.5, con el registro de software y Hardware del área de patrimonio de la universidad Nacional de Ucayali, 2017

5. **Hallazgos potenciales**

   - Falta de licencias de software
   - Falta de software de aplicaciones actualizados
   - Falta de manejo de información de software y hardware
   - Deficiencia en el registro de software y hardware

6. **Conclusión General**

   Durante el desarrollo de la Auditoria, se logró establecer el nivel de relación que existe entre la auditoria informática lo cual llegamos a ver que hay un déficit en la documentación (inventarios, manual de procedimientos) así como también la inexistencia de documentos importantes para el desarrollo del manejo de información del software y el hardware.

7. Recomendación

El área de patrimonio de la universidad nacional de Ucayali realice una mejora en el manejo de información de software y hardware verificando los datos establecidos por la norma establecida, plasmando la idea que se requiere para una mejor labor en el área.

8. Fecha del informe de la auditoria informática

Planeamiento de ejecución del informe

Fechas: 16-08-2019

9. Identificación y firma del auditor

Nombres y Apellidos: Marcos Alexis Bautista Ushiñahua

Cargo: Auditor Informático

Firma

Anexo 16: *Ficha Técnica*

FICHA TÉCNICA DE EQUIPOS DE CÓMPUTO

ENCARGADO: _____

FECHA:	SALA:	EQUIPO #:

HARDWARE				
PROCESADOR	Marca-Velocidad:			
MEMORIA RAM	Capacidad y Numero de Módulos:			
DISCO DURO	Marca:	serial:	Tipo IDE__ SATA__	
UNIDAD DE CD-DVD	Marca:	Modelo:	Tipo IDE__ SATA__	
PUERTOS	DIMM	SIMM	USB	
MONITOR	Marca y serial :		Tipo CRT_____ LCD_____	
TARJETA DE RED	Integrada: ____	Inalámbrica: ____	placa de red :	dirección de red:
TARJETA DE VIDEO	integrada _____ _____		placa de video : placa de sonido :	
TECLADO	Marca:		Estado:	
MOUSE	Marca y serial :		Estado:	
FUENTE DE PODER	Marca:		Modelo:	
MARCA DEL CASE	tipo y serial		tipo de computadora :	
BOARD	Marca-Referencia:		tipo y ancho de bus :	

SOFTWARE			
SISTEMA OPERATIVO Service pack			
PARTICIONES DISCO DURO	No PARTICIONES 1___ 2___ Mas ___		
MICROSOFT OFFICE	SI ____ NO____	Versión:	
NAVEGADOR(ES)	Nombre(s):	Versión:	
ADOBE READER	SI ____ NO____	Versión:	
COMPRESOR DE ARCHIVOS	SI ____ NO____	Nombre:	Versión:
ANTIVIRUS			
DEEP FREEZE	Nombre:	Versión:	
UTILIDADES DE GRABACIÓN	Nombre:	Versión:	
OTRO SOFTWARE	Nombre:	Versión:	

OBSERVACIONES: _____

Anexo 17: *Informe Mantenimiento Preventivo/Correctivo del Campus universitario*

UNIVERSIDAD NACIONAL DE UCAYALI

OFICINA GENERAL DE SISTEMAS E INFORMATICA

AREA DE SOPORTE TECNICO

"Año de la Consolidación Económica y Social del Perú"

INFORME Nº 047-2010-OGSeI-AST-UNU

PARA **:** Ing. Jorge trigueros
Jefe de la Oficina General de Sistemas e Informática

ASUNTO **:** Mantenimiento Preventivo/Correctivo del Campus Universitario

REF **:** MEMORANDO N° 138-2010-UNU-R

FECHA: Pucallpa, 25 de julio del 2018

Mediante el presente me es grato dirigirme a usted, para informarle lo siguiente:

En relación al proyecto plan operativo institucional "POI", organización y ejecución del plan de mantenimiento de hardware y software, surge la necesidad de brindar un mejor servicio a todo el personal y poder ofrecerles un buen desarrollo laboral. En la mayoría de las ocasiones el problema que presenta los equipos es resuelto a la falta de revisiones periódicas que detecten a tiempo las fallas técnicas que se puedan encontrar en niveles informáticos. La ejecución de este plan de mantenimiento ayudara a un mejor control con respecto a todas las necesidades

preventivas y correctivas que puedan presentarse ante los equipos de cómputo, siendo estos el motor principal de la calidad de trabajo.

El mantenimiento preventivo consiste en una profesional atención periódica de limpieza, verificación y afinación de los distintos elementos integrantes de un equipo de cómputo. Estos elementos son:

- Las unidades de entrada / salida (teclado, mouse, monitor, impresoras, scanner, etc.).
- Las unidades de almacenamiento (disco duro, unidades de disquete, unidades de CD-ROM, unidades de DVD-ROM, zips, etc.)
- Software en términos de configuración, instalación y optimización.

Es importante notar que un gran porcentaje de los problemas que se presentan en el trabajo cotidiano, se debe a la falta de un programa específico de mantenimiento de los equipos, de tal manera que la mayoría de los problemas se resuelven con el mismo procedimiento del mantenimiento preventivo. Lo importante de esto es que mediante una programación anticipada de los servicios de mantenimiento, se previenen las molestas demoras generadas por una falla inesperada. Con un adecuado programa de mantenimiento es posible mantener en buen estado los equipos, ayudando a prevenir y/o a reparar fallas.

Básicamente consiste en la limpieza física Interna y Externa del equipo de cómputo incluye técnicas que se aplican a las PC`s para darle un periodo de vida útil más largo y libre de fallas. Así mismo los procedimientos que se deben aplicar para el cuidado de las maquinas del medio ambiente, como dispositivos para protección de las sobre cargas eléctricas, contra las altas temperaturas y o las excesivas vibraciones.

El Servicio Correctivo de un equipo de cómputo se realiza eventualmente o cuando una falla técnica lo requiera para solucionar problemas operativos de software o hardware; cambio o instalación de nuevos componentes de hardware y cuando la presencia de un Virus afecta el desempeño de la computadora.

Las ventajas del plan de mantenimiento preventivo y correctivo son:

* Confiabilidad, los equipos operan en mejores condiciones de seguridad, ya que se conoce su estado, y sus condiciones de funcionamiento.
* Disminución del tiempo muerto, tiempo de parada de equipos.
* Mayor duración, de los equipos e instalaciones.
* Uniformidad en la carga de trabajo para el personal de Mantenimiento debido a una programación de actividades.
* Menor costo de las reparaciones.

Es por ello que presento la organización de acuerdo al POI, para la ejecución del plan de mantenimiento preventivo de hardware y software; durante el año

CRONOGRAMA DE EJECUCION											
ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
	1				1				1		

se realizan tres mantenimientos a todo el parque informático de la UNU.

Es todo cuanto informo para su conocimiento y demás fines.

Atentamente,

Sr. WARREN KLAUS ROJAS GARCÍA

Técnico del Área de Soporte

c.c.
Archivo
O.G.S.e.I

Anexo 18: *inventario de equipos del área de informática*

COMPUTADORAS	Descripción del Activo	Marca	Modelo	Serie
FORES-001	PLACA	GIGABYTE	H81M-H	f7a27000970
	PROCESADOR	INTEL	CORE i7 3.6Ghz	mc539194a2297
	MEMORIA	KINGSTON	KVR13N9S8/4	saulq211249
	DISCO DURO	WB	1TB	WCC6Y7PNDJHY
	LECTORA	LG	GH24NSD1	509hifz089091
	CASE	LANDBYTE	ATX-600W	su241114200730
FORES-002	PLACA	GIGABYTE	H81M-H	F6A32303695
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC539194A2054
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211245
	DISCO DURO	WB	1TB	WCC6Y6DR4KCS
	LECTORA	LG	GH24NSD1	509HIJD088756
	CASE	LANDBYTE	ATX-600W	SU241114200665
FORES-003	PLACA	GIGABYTE	H81M-H	F6A32303687
	PROCESADOR	INTEL	CORE i7 3.6Ghz	3E539177A0507
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211247
	DISCO DURO	WB	1TB	WCC6Y7VEF1RT
	LECTORA	LG	GH24NSD1	509HIRU088758
	CASE	LANDBYTE	ATX-600W	SU241114200702
FORES-004	PLACA	GIGABYTE	H81M-H	F6A32303114
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC539194A2043
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211256
	DISCO DURO	WB	1TB	WCC6Y1CEFVDK
	LECTORA	LG	GH24NSD1	509HIBN088757
	CASE	LANDBYTE	ATX-600W	SU241114200600
FORES-005	PLACA	GIGABYTE	H81M-H	F6A32303231
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC539194A0024
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211248
	DISCO DURO	WB	1TB	WCC6Y3NFSUK2
	LECTORA	LG	GH24NSD1	509HIVY088759
	CASE	LANDBYTE	ATX-600W	SU241114200614
FORES-006	PLACA	GIGABYTE	H81M-H	F6A32303699
	PROCESADOR	INTEL	CORE i7 3.6Ghz	3E539177A1855
	MEMORIA	KINGSTON	KVR13N9S8/4	saulq211242
	DISCO DURO	WB	1TB	WCC6Y0ZYYTCD
	LECTORA	LG	GH24NSD1	509hipe088760
	CASE	LANDBYTE	ATX-600W	su241114200606
FORES-007	PLACA	GIGABYTE	H81M-H	f6a32303239
	PROCESADOR	INTEL	CORE i7 3.6Ghz	mc538219a3381
	MEMORIA	KINGSTON	KVR13N9S8/4	saulq211259
	DISCO DURO	WB	1TB	wcc6y6dr4d6d
	LECTORA	LG	GH24NSD1	509hins088751
	CASE	LANDBYTE	ATX-600W	su241114200587
FORES-008	PLACA	GIGABYTE	H81M-H	f6a32303675
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC538219A3366
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211243
	DISCO DURO	WB	1TB	WCC6Y3CTU3H3

	LECTORA	LG	GH24NSD1	509HIAC088752
	CASE	LANDBYTE	ATX-600W	SU241114200757
FORES-009	PLACA	GIGABYTE	H81M-H	F6A32303138
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC538219A4600
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211236
	DISCO DURO	WB	1TB	WCC6Y7VEF103
	LECTORA	LG	GH24NSD1	509HIWM088753
	CASE	LANDBYTE	ATX-600W	SU241114200723
FORES-010	PLACA	GIGABYTE	H81M-H	F6A32303683
	PROCESADOR	INTEL	CORE i7 3.6Ghz	3E539177A1609
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211262
	DISCO DURO	WB	1TB	WCC6Y7PND39D
	LECTORA	LG	GH24NSD1	509HIXT088754
	CASE	LANDBYTE	ATX-600W	SU241114200635
FORES-011	PLACA	GIGABYTE	H81M-H	F6A32303229
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC539194A2104
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211261
	DISCO DURO	WB	1TB	WCC6Y1CEFNCU
	LECTORA	LG	GH24NSD1	509HIFZ088755
	CASE	LANDBYTE	ATX-600W	SU241114200698
FORES-012	PLACA	GIGABYTE	H81M-H	F7A14800997
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC539194A1366
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211240
	DISCO DURO	WB	1TB	WCC6Y0ZYYUXU
	LECTORA	LG	GH24NSD1	509HIMA088771
	CASE	LANDBYTE	ATX-600W	SU241114200689
FORES-013	PLACA	GIGABYTE	H81M-H	F7A14800340
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC539194A2508
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211258
	DISCO DURO	WB	1TB	WCC6Y0JEU1P4
	LECTORA	LG	GH24NSD1	509HIEJ088772
	CASE	LANDBYTE	ATX-600W	SU241114200645
FORES-014	PLACA	GIGABYTE	H81M-H	F7A14801432
	PROCESADOR	INTEL	CORE i7 3.6Ghz	3E539060A0422
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211257
	DISCO DURO	WB	1TB	WCC6Y3CTUEUU
	LECTORA	LG	GH24NSD1	509HIKK088773
	CASE	LANDBYTE	ATX-600W	SU241114200585
FORES-015	PLACA	GIGABYTE	H81M-H	F7A14801475
	PROCESADOR	INTEL	CORE i7 3.6Ghz	3E539177A1693
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211246
	DISCO DURO	WB	1TB	WCC6Y0ZYYYTJ
	LECTORA	LG	GH24NSD1	509HIUL088774
	CASE	LANDBYTE	ATX-600W	SU241114200573
FORES-016	PLACA	GIGABYTE	H81M-H	F7A14800900
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC539194A2130
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211253
	DISCO DURO	WB	1TB	WCC6Y7PND3PS
	LECTORA	LG	GH24NSD1	509HIAC088776

	CASE	LANDBYTE	ATX-600W	SU241114200579
FORES-017	PLACA	GIGABYTE	H81M-H	F7A14801205
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC539194A2147
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211238
	DISCO DURO	WB	1TB	WCC6Y0ZYYLRX
	LECTORA	LG	GH24NSD1	509HIWM088777
	CASE	LANDBYTE	ATX-600W	SU241114200572
FORES-018	PLACA	GIGABYTE	H81M-H	F7A14801424
	PROCESADOR	INTEL	CORE i7 3.6Ghz	MC539194A0218
	MEMORIA	KINGSTON	KVR13N9S8/4	SAULQ211263
	DISCO DURO	WB	1TB	WCC6Y0ZYY90F
	LECTORA	LG	GH24NSD1	509HIXT088778
	CASE	LANDBYTE	ATX-600W	SU241114200589
FORES-019	PLACA	GIGABYTE	H81M-H	f7a14801481
	PROCESADOR	INTEL	CORE i7 3.6Ghz	mc539194a0166
	MEMORIA	KINGSTON	KVR13N9S8/4	saulq211255
	DISCO DURO	WB	1TB	wcc6y4rau8h9
	LECTORA	LG	GH24NSD1	509hifz088779
	CASE	LANDBYTE	ATX-600W	su241114200745
FORES-020	PLACA	GIGABYTE	H81M-H	f7a14801301
	PROCESADOR	INTEL	CORE i7 3.6Ghz	mc539194a1370
	MEMORIA	KINGSTON	KVR13N9S8/4	saulq211087
	DISCO DURO	WB	1TB	wcc6y7tkkchc
	LECTORA	LG	GH24NSD1	509hins088775
	CASE	LANDBYTE	ATX-600W	su241114200631
FORES-021	PLACA	GIGABYTE	H81M-H	f7a14801665
	PROCESADOR	INTEL	CORE i7 3.6Ghz	mc539194a1990
	MEMORIA	KINGSTON	KVR13N9S8/4	saulq211241
	DISCO DURO	WB	1TB	wcc6y3nfsksz
	LECTORA	LG	GH24NSD1	509hijd088780
	CASE	LANDBYTE	ATX-600W	su241114200596
FORES-022	PLACA	GIGABYTE	H81M-H	f7a05703629
	PROCESADOR	INTEL	CORE i7 3.6Ghz	mc538219a2783
	MEMORIA	KINGSTON	KVR13N9S8/4	saulq211082
	DISCO DURO	WB	1TB	wcc6y4ay6ay7
	LECTORA	LG	GH24NSD1	509hisw089150
	CASE	LANDBYTE	ATX-600W	su241114200647
FORES-023	PLACA	GIGABYTE	H81M-H	f7a05703186
	PROCESADOR	INTEL	CORE i7 3.6Ghz	mc539194a2347
	MEMORIA	KINGSTON	KVR13N9S8/4	saulq211071
	DISCO DURO	WB	1TB	wcc6y4xk9hj3
	LECTORA	LG	GH24NSD1	509hizf089149
	CASE	LANDBYTE	ATX-600W	SU241114200662
FORES-024	PLACA	GIGABYTE	H81M-H	f7a05703649
	PROCESADOR	INTEL	CORE i7 3.6Ghz	mc538219a3777
	MEMORIA	KINGSTON	KVR13N9S8/4	saulq211260
	DISCO DURO	WB	1TB	wcc6y4rau6jf
	LECTORA	LG	GH24NSD1	509hiqp089148
	CASE	LANDBYTE	ATX-600W	SU241114200820

FORES-025	**PLACA**	**GIGABYTE**	**H81M-H**	**f7a05703101**
	PROCESADOR	**INTEL**	**CORE i7 3.6Ghz**	**3e539177a1499**
	MEMORIA	**KINGSTON**	**KVR13N9S8/4**	**saulq211073**
	DISCO DURO	WB	1TB	wcc6y4ay61c3
	LECTORA	**LG**	**GH24NSD1**	**509hicx089147**
	CASE	**LANDBYTE**	**ATX-600W**	**su241114200833**

Anexo 19: *Análisis y evaluación de riesgos*

N°	Descripción	Impacto	Probabilidad
R1	Pérdida de información de software y hardware	5	3
R2	Funcionamiento inadecuado del personal	4	3
R3	Indisponibilidad de los equipos de computo	4	4
R4	Funcionamiento inadecuado del almacenamiento de datos	3	2
R5	Falta de un plan de trabajo	3	3
R6	Desactualización del inventario de software y hardware	2	2
R7	Retraso de las actividades del área	5	3
R8	Incumplimiento en el reporte de la información	4	3
R9	Uso indebido de la información del software y hardware	3	2
R10	Inadecuada utilización de los equipos informáticos	3	3
R11	Desconocimiento de los avances del Plan Estratégico	3	2
R12	Accesos no autorizados a las instalaciones del área tecnológica	3	3

EVALUACIÓN Y MEDIDAS DE RESPUESTA					
PROBABILIDAD	**IMPACTO**				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)					
Improbable (2)		R7	R4, R10		
Posible (3)			R6, R11	R2, R9	R1, R5, R8
Probable (4)				R3	
Casi Seguro (5)					

RESULTADO MATRIZ DE RIESGOS

Una vez se tiene la matriz de riesgos aplicada a cada uno de los procesos se indica las acciones que pueden realizarse para el tratamiento de los riesgos de acuerdo a la siguiente tabla donde se indica por cada color, el tratamiento que se puede aplicar en cada caso.

B	Zona de riesgo Baja: Asumir el riesgo
M	Zona de riesgo Moderada: Asumir el riesgo, reducir el riesgo
A	Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir
E	Zona de riesgo Extremo: Reducir el riesgo, evitar, compartir o transferir

Anexo 20: *Carta de presentación al área de patrimonio*



UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL
"AÑO DE LA LUCHA CONTRA LA CORRUPCION E IMPUNIDAD"

Pucallpa, 22 de Julio 2019

CARTA No. 092/2019-UNU-FIS e IC-D

Señor:
CPCC HUGO PANDURO SAJAMI
JEFE DE LA OFICINA GENERAL DE ADMINISTRACION
Presente

Estimado Señor:

A través de la presente carta presento al joven BAUTISTA USHIÑAHUA MARCOS ELEXIS estudiante de la Facultad de Ingeniería de Sistemas e Ingeniería Civil, Carrera Profesional de Ingeniería de Sistemas, de esta Casa Superior de Estudios.

Para el curso TESIS, desarrollándose en la oficina de Patrimonio, siendo requisito indispensable que lo realice, para obtener experiencia en la formación de su carrera profesional.

No dudando de su apoyo, quedo de usted, reiterándole las muestras de mi mayor consideración.

05 AGO 2019
C694

Anexo 21: *Check List al jefe de soporte técnico*

Verificación	**Condiciones**		
	Si	**No**	**No Aplica**
1. *¿Existe un plan de contingencia documentado?			
2. *¿Se identificó un responsable del mantenimiento e implementación del plan de contingencia?			
3. *Se identificaron y evaluaron los riesgos potenciales en lo referido a: • Ubicación • Infraestructura • Back up y protección de información • Seguridad de la información (hardware, software, datos, redes) • Protección de base espejada			
4. Impacto en el área de informática • *¿Se identificaron las funciones críticas del área de informática? • *¿Se cuantificó el valor de la información? • *¿Se valoraron las pérdidas financieras para el negocio de la interrupción de la continuidad de los sistemas? • *¿Se determinó el impacto en los clientes y proveedores de la interrupción? • *¿Se determinaron los tiempos de inoperatividad permitidos para cada una de las funciones del negocio (críticas y no críticas)?			

Verificación	Condiciones		
	Si	No	No Aplica
1. *¿Existe un plan de contingencia documentado?			
5. Estrategias de Recupero • *¿Se determinaron los riesgos y los niveles aceptables para los mismos? • *¿Se identificaron los recursos mínimos necesarios para el funcionamiento del negocio? • *¿Se establecieron sitios alternativos de almacenaje y procesamiento? • *¿Se evaluó la eficacia de los controles preventivos? • *¿Están documentados los procedimientos de implementación para las estrategias de recupero?			
6. *¿Se identificaron las capacidades de procesamiento mínimas requeridas para las acciones de recuperación?			
7. *¿Se identificaron los procedimientos técnicos de recuperación y la secuencia de ejecución de los mismos?			
8. Servicios técnicos, comunicaciones, redes y soporte • ¿Se cuenta con proveedores alternativos para el servicio de comunicaciones? • *¿Se cuenta con un respaldo de la información y los programas en una ubicación física diferente? • *¿Se seleccionaron las políticas, procedimientos y tecnologías de backup?			
9. *¿Se capacitó al personal en los procedimientos de emergencia?			

Verificación	Condiciones		
	Si	No	No Aplica
1. *¿Existe un plan de contingencia documentado?			
10. *¿Se realizan, de manera frecuente y aleatoria, simulacros de recupero?			
11. *¿Se testea la capacidad del centro de cómputos alternativo?			
12. *¿Se evaluaron los resultados de las pruebas y simulacros de recupero, internas y del centro de cómputos alternativo?			
13. Actualizaciones • *¿Se mantiene el plan de contingencia actualizado frente a los cambios ocurridos en el negocio? • ¿Se evalúan nuevas tecnologías y opciones de recuperación que mejoren la relación costo beneficio para el negocio?			
14. *¿Es razonable la relación costo beneficio del plan de contingencia implementado para el negocio?			
15. Software • *¿Existe una copia del software original para reinstalar fuera de la organización? • *¿Se cuenta con una estimación del tiempo que llevará la reinstalación para dejar el software operacional?			

Verificación	Condiciones		
	Si	No	No Aplica
1. *¿Existe un plan de contingencia documentado?			
16. Hardware • *¿Disponemos de un inventario del hardware de la organización? • *¿Está actualizado? • *¿Se identificaron los componentes esenciales de hardware? • *¿Son reparables internamente los componentes esenciales del hardware? • *¿Hay dependencia hacia un tercero para realizar reparaciones? • *¿Existen componentes de hardware que no sean reparables?			

Nota:

Las preguntas indicadas con * *(asterisco)* son de carácter invalidante, si aplican, para la aceptación del Plan de Contingencia del área de patrimonio.

***Anexo 22**: Checklist Aplicada Al jefe del área de patrimonio*

PREGUNTA	SI	NO	NO APLICA	OBSERVACIONES
DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
APO1.4.Definir un Plan Estratégico de TI				
¿Se cuenta con un plan estratégico dentro del área de patrimonio?				
¿Cree usted que al realizar un plan estratégico se podrá minimizar los riesgos encontrados?				
¿Actualmente cuentan con un plan de contingencia?				
APO1.5. Planes tácticos				
¿Cree usted que al tener un plan táctico se logrará mejorar los objetivos trazados?				
¿Es consciente usted de los problemas que pueden causar si no se cuenta con un plan táctico para la solución de dichas?				
¿Cree usted que por la falta de un plan estratégico es el motivo de la deficiencia de información del manejo de software y hardware?				
APO7.1.Mantener la dotación de personal suficiente y adecuado				
¿Actualmente cuenta con el suficiente personal para el desarrollo de las funciones del área?				
¿Cree usted que por la falta de personal es el motivo de la deficiencia de las labores para lograr los objetivos propuestos?				
¿Se capacita al personal constantemente?				
APO 7.3. Mantener las habilidades y competencias del personal				
¿Existe personal capaz de desarrollar los objetivos y actividades bajo presión?				
¿Actualmente cuenta con personal calificado para el desarrollo de las actividades del área?				

¿El personal cuenta con la experiencia necesaria para la mejora de la eficiencia de los procesos y actividades?				
APO 7.4. Evaluar el desempeño laboral de los empleados				
¿Cuenta con el personal adecuado para realizar los registros de información de software y hardware?				
APO 7.6. Gestionar personal contratado				
¿Es suficiente con el personal que tiene para las actividades de registro de información de software y hardware?				
DOMINIO: ADQUIRIR E IMPLEMENTAR				
AI 1.2. Reporte de análisis de riesgos				
¿En el área de patrimonio se realiza un análisis de riesgos?				
¿Cuentan con un informe de análisis de riesgos?				
¿Cree usted que con el desarrollo de la auditoria informática se podrá identificar los riesgos que puedan existir en el área?				
AI 5.1. Control de adquisición				
¿Actualmente cuenta con un inventario de las adquisiciones realizadas por el área?				
¿Cuenta con un repositorio de adquisiciones para el área?				
¿Se realiza un control detallado del bien a adquirir, si tiene garantía, si tiene manual de usuario, etc?				
DOMINIO: MONITOREAR Y EVALUAR				
MEA 1.1. Establecer un enfoque de la supervisión				
¿Se comunica a todo el personal del área de patrimonio sobre los objetivos y requisitos				

empresariales que realiza el área?				
¿Existe un proceso de control de cambios y de gestión en la supervisión y la presentación de informes?				
MEA 1.4. Analizar e informar sobre el rendimiento				
¿Se documenta las incidencias y problemas para contar como guía para la mejora de la deficiencia del registro software y hardware del área?				
¿Se realizó un informe de las incidencias de la deficiencia del manejo de información del software y hardware?				
MEA 2.1. Supervisar el control interno				
¿Anteriormente realizaron una auditoria en el área?				
MEA 2.2. Revisar la efectividad de los controles sobre los procesos de negocio				
¿Se cuenta con un registro de información física para el control de los equipos informáticos?				
MEA 2.7. Estudiar las iniciativas de aseguramiento				
¿Se realiza un análisis y un informe sobre el rendimiento de los equipos informáticos distribuidos?				
¿Se realiza una evaluación de los procesos bajo la revisión de los controles y hallazgos de riesgos en el área?				
¿Cada bien informático adquirido cuenta con una garantía?				
DOMINIO: SERVICIO Y SOPORTE				
DSS 2.2. Registrar, clasificar y priorizar peticiones e incidentes				
¿Se cuenta con un registro de clasificación y priorización de peticiones de servicios e incidentes para la mejora del registro de software y hardware?				
DSS 6.1. Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos				

¿Existe documentación y supervisión de actividades de control de los procesos del área, en este caso del registro de software y hardware?				
DSS 6.6. Asegurar los activos de información				
¿Existen políticas de clasificación de datos y procedimientos para proteger los activos de información del registro de software y hardware?				
¿Se restringe el acceso a la información a personal externas del área?				

Anexo 23: *Checklist Aplicada al jefe de la general de tecnologías de información, sistemas y estadística.*

PREGUNTA	SI	NO	NO APLICA	OBSERVACIONES
DOMINIO ALINEAR, PLANIFICAR Y ORGANIZAR (APO)				
APO1.4.Definir un Plan Estratégico de TI				
¿Se cuenta con un plan estratégico dentro del área de informática?				
¿Cree usted que al realizar un plan estratégico se podrá minimizar los riesgos encontrados?				
¿Actualmente cuentan con un plan de contingencia?				
APO1.5. Planes tácticos				
¿Cuenta con un plan de trabajo?				
¿Es consciente usted de los problemas que pueden causar si no se cuenta con un plan táctico para la solución de dichas?				
¿Cree usted que por la falta de un plan estratégico es el motivo de la deficiencia de información del manejo de software y hardware?				
APO7.1.Mantener la dotación de personal suficiente y adecuado				
¿Actualmente cuenta con el suficiente personal para el desarrollo de las funciones del área?				
¿Cree usted que por la falta de personal es el motivo de la deficiencia de las labores para lograr los objetivos propuestos?				
¿Se capacita al personal constantemente?				
APO 7.3. Mantener las habilidades y competencias del personal				

¿Existe personal capaz de desarrollar los objetivos y actividades bajo presión?				
¿Actualmente cuenta con personal calificado para el desarrollo de las actividades del área?				
¿El personal cuenta con la experiencia necesaria para la mejora de la eficiencia de los procesos y actividades?				
APO 7.6. Gestionar el personal contratado				
¿Se cuenta con el personal adecuado para el manejo de las TI?				
¿Existe una coordinación entre los miembros del área de informática para desarrollar las actividades del manejo de información?				
¿Cree usted que es suficiente la cantidad de personal con lo que cuenta?				
DOMINIO: ADQUIRIR E IMPLEMENTAR				
AI 1.2. Reporte de análisis de riesgos				
¿En el área de informática de realiza un análisis de riesgos?				
¿Cuentan con un informe de análisis de riesgos?				
¿Cree usted que con el desarrollo de la auditoria informática se podrá identificar los riesgos que puedan existir en el área?				
AI 1.5. Control de adquisición				
¿Actualmente cuenta con un inventario de los equipos informáticos entregados al área?				
¿Cuenta con un repositorio de los equipos informáticos para el área?				
¿Se realiza un control detallado del bien entregado para su reparación, si tiene garantía, si tiene manual de usuario, si es factible arreglarlo, etc?				
DOMINIO: MONITOREAR Y EVALUAR				
MEA 1.1. Establecer un enfoque de la supervisión				

¿Se comunica a todo el personal del área de patrimonio sobre los objetivos y requisitos que establece el gobierno en el funcionamiento de las actividades a desarrollar?				
¿Existe un proceso de control de cambios y de gestión en la supervisión y la presentación de informes de los equipos informáticos, para dar de baja o equipos que se pueden repotenciar?				
MEA 1.4. Analizar e informar sobre el rendimiento				
¿Se documenta las incidencias y problemas para contar como guía para la mejora de la deficiencia del registro software y hardware del área?				
¿Se realizó un informe de las incidencias de la deficiencia del manejo de información del software y hardware?				
MEA 2.7. Estudiar las iniciativas de aseguramiento				
¿Se realiza un análisis y un informe sobre el rendimiento de los equipos informáticos?				
¿Se realiza una evaluación de los procesos bajo la revisión de los controles y hallazgos de riesgos en el área?				
¿Cada bien informático adquirido cuenta con una garantía?				

Anexo 24: *Acta de reunión de registro*

ACTA DE REUNIÓN CON EL JEFE DE PATRIMONIO Y DE INFORMATICA			
Motivo: Entrevista para el desarrollo de la investigación		Acta No: 01	
Citada por: BACH. Marcos Alexis Bautista Ushiñahua		**Hora inicio:** 10:00 AM Fin: 12:00 AM	
Fecha: 23 DE JULIO DEL 2019		**Lugar:** Área de patrimonio y área de informática	
PARTICIPANTES			
Nº	NOMBRES Y APELLIDOS	CARGO	TELÉFONO
1	CPC. Sergio Cárdenas	Jefe del área de patrimonio	
2	BACH. Jorge Trigueros bellido	Jefe del área de informática	
3	TEC.Warren Klaus Rojas	Responsable del área de soporte técnico	
PRESENTACIÓN Se llevó a cabo la presentación de cada uno de los Jefes de las áreas que participarán y/o atenderán como designados las visitas de Auditoria como facilitadores y articuladores de la información requerida para su desarrollo. Luego se explicó por parte del auditor el contenido del plan de trabajo, en cuanto a: Metodología de seguimiento y el término previsto para la ejecución de la Auditoria.			
PUNTOS DE DISCUSIÓN			
1	Deficiencia del registro de software y hardware de las áreas		
2	Falta de personal para el desarrollo de los procesos del área		
3	Inventario desactualizado de los equipos de computo		
4	Falta de un plan de trabajo		
5	Permisos para acceder a información requerida		
6	Informe del tiempo que durará la investigación		

7	Problemática de las áreas
8	Seguridad de la información de los equipo informáticos
9	Tiempo del desarrollo de la auditoria
10	Análisis de los riesgos
11	Entrevistas a los interesados
12	Creación de un plan auditoria

DESARROLLO DE LA REUNIÓN

1. Realizar la entrevista con las personas los jefes de las áreas
2. Dar a conocer nuestro plan de trabajo
3. Recopilación de información necesaria para el desarrollo de auditoria
4. Encuestas a cada personal de las áreas a auditar
5. Brindar reportes de la auditoria

OBJETIVOS DE LA REUNIÍÓN

1. Brindar conocimiento de lo que se va realizar durante la auditoria
2. Recopilar información para el desarrollo de la auditoria
3. Planificar los pasos de desarrollo durante las entrevistas
4. Desarrollar los reportes correspondientes de la auditoria
5. Realizar un informe preliminar de la auditoria.

OBSERVACIONES

1. Al momento de realizar la entrevista se tuvo problemas con las asistencias de todos los interesados de la auditoria.
2. El ambiente era el inadecuado para las entrevistas
3. Las entrevistas fueron un poco cortas por el entorno laboral de los interesados.

---	---	---
Auditor:	jefe del área de patrimonio	jefe del área Informática
Marcos Alexis bautista u.	CPc. Sergio C.	Ing. Jorge trigueros

Anexo 25: *Cuestionario 1*

Encuesta al personal del área de patrimonio para medir la variable Auditoria Informática

ENCUESTA, PARA MEDIR LA VARIABLE AUDITORÍA INFORMÁTICA, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar El Instrumento ENCUESTA, para medir la Variable Auditoría Informática en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

AUDITORIA INFORMÁTICA

PG.	Informe preliminar	Malo	Regular	Bueno
1	¿Cómo calificaría usted la elaboración de una ficha técnica para realización de una auditoria informática en el área de patrimonio?			
2	¿Cómo cree que es el rendimiento de las adquisiciones de las TI?			
3	¿Qué le parece el manejo de información en el área de patrimonio?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo define la falta de información del área de patrimonio de las TI?			
6	¿Qué le parece la forma de recopilación de la información?			

PG.	Análisis de la situación actual			
7	¿Cómo calificas el proceso de datos de la información?			
8	¿Qué le parece la forma de manejo de información escasa dentro del área?			
9	¿Qué calificación daría usted al posible riesgo de pérdidas de información del área?			
10	¿Cómo califica usted la falta de interés de las adquisiciones dentro del área			
PG.	**Control y gestión de la información**			
11	¿Cómo califica el rendimiento de la seguridad de datos?			
12	¿Qué le parece la implantación de la auditoria informática para el mejor control de seguridad y manejo de la información?			
13	¿Cómo califica usted el plan de trabajo del área para minimización de riesgos en la perdida de datos informáticos?			
14	¿Qué le parece a usted la utilización de una metodología capaz de mejorar el desarrollo de información del área?			
15	¿Usted como personal administrativo cómo calificaría el estado de la seguridad de información?			
16	¿Cómo observa usted que se está dando el uso de las tecnologías de información?			
PG.	**Observaciones**			
17	¿De acuerdo con la investigación como califica las falencias encontradas en el manejo de información?			
18	¿Cómo califica el hallazgo de riesgos en las TI?			
19	¿Cómo califica el estudio que se realizó del manejo de información?			
20	¿Qué le parece a usted la metodología que se realizara para solución del problema encontrado en el área?			

Encuesta al personal del área de patrimonio para medir la variable Registro de Software y Hardware

ENCUESTA, PARA MEDIR LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar el Instrumento ENCUESTA, para medir la Variable Registro de Software y Hardware en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

REGISTRO DE SOFTWARE Y HARDWARE

PG.	Manejo de información de software y hardware	Malo	Regular	Bueno
1	¿Cuál es el nivel de capacidad que tiene el personal en el manejo de información de los equipos informáticos?			
2	¿Qué le parece la falta de capacitación del personal en las actualizaciones y versiones?			
3	¿Cómo califica la calidad del producto adquirido?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo califica usted la falta de información de los software y hardware, con qué fin fueron comprados?			
6	¿Qué le parece a usted la falta de un plan de contingencia ante un problema o riesgo?			
PG.	**Fines de la adquisición**			
7	¿Cómo calificas el proceso de datos de la información de los equipos informáticos?			
8	¿Cómo califica usted el manejo de la información del software y el hardware			

	del área?			
9	¿Qué le parece a usted la calidad de los equipos informáticos que fueron adquiridos?			
10	¿Cuál es el nivel de mejora al adquirir software y hardware de última generación?			
PG.	**Software**			
11	¿Qué le parece la seguridad del software adquiridos, en cuanto a los datos guardados?			
12	¿Cómo califica usted el nivel de seguridad de información del software?			
13	¿Qué le parece las versiones que brindan los proveedores para la actualización de diversos software?			
14	¿Cómo califica la actualización de los programas antiguos a las nuevas versiones?			
15	¿Qué le parece el uso establecido para el software, Función de dicha?			
16	¿Cómo califica usted el uso de programas que bloquean páginas prohibidas?			
PG.	**Hardware**			
17	¿Cómo califica el servicio de mantenimiento al hardware (PC, impresoras, discos duros, laptops, etc?			
18	¿Qué le parece el tiempo que establecen para dar mantenimiento a las pcs?			
19	¿Cómo califica el nivel de solución de las fallas ocurridas?			
20	¿Qué le parece la reparación de los equipos informáticos ante riesgos y tiempo de uso?			

Anexo 26: *Cuestionario 2*

ENCUESTA, PARA MEDIR LA VARIABLE AUDITORÍA INFORMÁTICA, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar El Instrumento ENCUESTA, para medir la Variable Auditoría Informática en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

AUDITORIA INFORMÁTICA

PG.	Informe preliminar	Malo	Regular	Bueno
1	¿Cómo calificaría usted la elaboración de una ficha técnica para realización de una auditoria informática en el área de patrimonio?			
2	¿Cómo cree que es el rendimiento de las adquisiciones de las TI?			
3	¿Qué le parece el manejo de información en el área de patrimonio?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo define la falta de información del área de patrimonio de las TI?			
6	¿Qué le parece la forma de recopilación de la información?			
PG.	**Análisis de la situación actual**			
7	¿Cómo calificas el proceso de datos de la información?			
8	¿Qué le parece la forma de manejo de información escasa dentro del área?			

9	¿Qué calificación daría usted al posible riesgo de pérdidas de información del área?			
10	¿Cómo califica usted la falta de interés de las adquisiciones dentro del área			
PG.	**Control y gestión de la información**			
11	¿Cómo califica el rendimiento de la seguridad de datos?			
12	¿Qué le parece la implantación de la auditoria informática para el mejor control de seguridad y manejo de la información?			
13	¿Cómo califica usted el plan de trabajo del área para minimización de riesgos en la perdida de datos informáticos?			
14	¿Qué le parece a usted la utilización de una metodología capaz de mejorar el desarrollo de información del área?			
15	¿Usted como personal administrativo cómo calificaría el estado de la seguridad de información?			
16	¿Cómo observa usted que se está dando el uso de las tecnologías de información?			
PG.	**Observaciones**			
17	¿De acuerdo con la investigación como califica las falencias encontradas en el manejo de información?			
18	¿Cómo califica el hallazgo de riesgos en las TI?			
19	¿Cómo califica el estudio que se realizó del manejo de información?			
20	¿Qué le parece a usted la metodología que se realizara para solución del problema encontrado en el área?			

ENCUESTA, PARA MEDIR LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar el Instrumento ENCUESTA, para medir la Variable Registro de Software y Hardware en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

REGISTRO DE SOFTWARE Y HARDWARE

PG.	Manejo de información de software y hardware	Malo	Regular	Bueno
1	¿Cuál es el nivel de capacidad que tiene el personal en el manejo de información de los equipos informáticos?			
2	¿Qué le parece la falta de capacitación del personal en las actualizaciones y versiones?			
3	¿Cómo califica la calidad del producto adquirido?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo califica usted la falta de información de los software y hardware, con qué fin fueron comprados?			
6	¿Qué le parece a usted la falta de un plan de contingencia ante un problema o riesgo?			
PG.	**Fines de la adquisición**			
7	¿Cómo calificas el proceso de datos de la información de los equipos informáticos?			
8	¿Cómo califica usted el manejo de la información del software y el hardware del área?			
9	¿Qué le parece a usted la calidad de los equipos informáticos que fueron adquiridos?			

10	¿Cuál es el nivel de mejora al adquirir software y hardware de última generación?			
PG.	**Software**			
11	¿Qué le parece la seguridad del software adquiridos, en cuanto a los datos guardados?			
12	¿Cómo califica usted el nivel de seguridad de información del software?			
13	¿Qué le parece las versiones que brindan los proveedores para la actualización de diversos software?			
14	¿Cómo califica la actualización de los programas antiguos a las nuevas versiones?			
15	¿Qué le parece el uso establecido para el software, Función de dicha?			
16	¿Cómo califica usted el uso de programas que bloquean páginas prohibidas?			
PG.	**Hardware**			
17	¿Cómo califica el servicio de mantenimiento al hardware (PC, impresoras, discos duros, laptops, etc?			
18	¿Qué le parece el tiempo que establecen para dar mantenimiento a las pcs?			
19	¿Cómo califica el nivel de solución de las fallas ocurridas?			
20	¿Qué le parece la reparación de los equipos informáticos ante riesgos y tiempo de uso?			

Anexo 27: *Cuestionario 3*

ENCUESTA, PARA MEDIR LA VARIABLE AUDITORÍA INFORMÁTICA, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar El Instrumento ENCUESTA, para medir la Variable Auditoría Informática en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

AUDITORÍA INFORMÁTICA

PG.	Informe preliminar	Malo	Regular	Bueno
1	¿Cómo calificaría usted la elaboración de una ficha técnica para realización de una auditoria informática en el área de patrimonio?			
2	¿Cómo cree que es el rendimiento de las adquisiciones de las TI?			
3	¿Qué le parece el manejo de información en el área de patrimonio?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo define la falta de información del área de patrimonio de las TI?			
6	¿Qué le parece la forma de recopilación de la información?			
PG.	**Análisis de la situación actual**			
7	¿Cómo calificas el proceso de datos de la información?			
8	¿Qué le parece la forma de manejo de información escasa dentro del área?			

9	¿Qué calificación daría usted al posible riesgo de pérdidas de información del área?			
10	¿Cómo califica usted la falta de interés de las adquisiciones dentro del área			
PG.	**Control y gestión de la información**			
11	¿Cómo califica el rendimiento de la seguridad de datos?			
12	¿Qué le parece la implantación de la auditoria informática para el mejor control de seguridad y manejo de la información?			
13	¿Cómo califica usted el plan de trabajo del área para minimización de riesgos en la perdida de datos informáticos?			
14	¿Qué le parece a usted la utilización de una metodología capaz de mejorar el desarrollo de información del área?			
15	¿Usted como personal administrativo cómo calificaría el estado de la seguridad de información?			
16	¿Cómo observa usted que se está dando el uso de las tecnologías de información?			
PG.	**Observaciones**			
17	¿De acuerdo con la investigación como califica las falencias encontradas en el manejo de información?			
18	¿Cómo califica el hallazgo de riesgos en las TI?			
19	¿Cómo califica el estudio que se realizó del manejo de información?			
20	¿Qué le parece a usted la metodología que se realizara para solución del problema encontrado en el área?			

ENCUESTA, PARA MEDIR LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar el Instrumento ENCUESTA, para medir la Variable Registro de Software y Hardware en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

REGISTRO DE SOFTWARE Y HARDWARE

PG.	Manejo de información de software y hardware	Malo	Regular	Bueno
1	¿Cuál es el nivel de capacidad que tiene el personal en el manejo de información de los equipos informáticos?			
2	¿Qué le parece la falta de capacitación del personal en las actualizaciones y versiones?			
3	¿Cómo califica la calidad del producto adquirido?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo califica usted la falta de información de los software y hardware, con qué fin fueron comprados?			
6	¿Qué le parece a usted la falta de un plan de contingencia ante un problema o riesgo?			
PG.	**Fines de la adquisición**			
7	¿Cómo calificas el proceso de datos de la información de los equipos informáticos?			
8	¿Cómo califica usted el manejo de la información del software y el hardware del área?			
9	¿Qué le parece a usted la calidad de los equipos informáticos que fueron adquiridos?			

10	¿Cuál es el nivel de mejora al adquirir software y hardware de última generación?			
PG.	**Software**			
11	¿Qué le parece la seguridad del software adquiridos, en cuanto a los datos guardados?			
12	¿Cómo califica usted el nivel de seguridad de información del software?			
13	¿Qué le parece las versiones que brindan los proveedores para la actualización de diversos software?			
14	¿Cómo califica la actualización de los programas antiguos a las nuevas versiones?			
15	¿Qué le parece el uso establecido para el software, Función de dicha?			
16	¿Cómo califica usted el uso de programas que bloquean páginas prohibidas?			
PG.	**Hardware**			
17	¿Cómo califica el servicio de mantenimiento al hardware (PC, impresoras, discos duros, laptops, etc?			
18	¿Qué le parece el tiempo que establecen para dar mantenimiento a las pcs?			
19	¿Cómo califica el nivel de solución de las fallas ocurridas?			
20	¿Qué le parece la reparación de los equipos informáticos ante riesgos y tiempo de uso?			

Anexo 28: *Cuestionario 4*

ENCUESTA, PARA MEDIR LA VARIABLE AUDITORÍA INFORMÁTICA, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar El Instrumento ENCUESTA, para medir la Variable Auditoría Informática en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

AUDITORÍA INFORMÁTICA

PG.	Informe preliminar	Malo	Regular	Bueno
1	¿Cómo calificaría usted la elaboración de una ficha técnica para realización de una auditoria informática en el área de patrimonio?			
2	¿Cómo cree que es el rendimiento de las adquisiciones de las TI?			
3	¿Qué le parece el manejo de información en el área de patrimonio?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo define la falta de información del área de patrimonio de las TI?			
6	¿Qué le parece la forma de recopilación de la información?			
PG.	**Análisis de la situación actual**			
7	¿Cómo calificas el proceso de datos de la información?			
8	¿Qué le parece la forma de manejo de información escasa dentro del área?			

9	¿Qué calificación daría usted al posible riesgo de pérdidas de información del área?			
10	¿Cómo califica usted la falta de interés de las adquisiciones dentro del área			
PG.	**Control y gestión de la información**			
11	¿Cómo califica el rendimiento de la seguridad de datos?			
12	¿Qué le parece la implantación de la auditoria informática para el mejor control de seguridad y manejo de la información?			
13	¿Cómo califica usted el plan de trabajo del área para minimización de riesgos en la perdida de datos informáticos?			
14	¿Qué le parece a usted la utilización de una metodología capaz de mejorar el desarrollo de información del área?			
15	¿Usted como personal administrativo cómo calificaría el estado de la seguridad de información?			
16	¿Cómo observa usted que se está dando el uso de las tecnologías de información?			
PG.	**Observaciones**			
17	¿De acuerdo con la investigación como califica las falencias encontradas en el manejo de información?			
18	¿Cómo califica el hallazgo de riesgos en las TI?			
19	¿Cómo califica el estudio que se realizó del manejo de información?			
20	¿Qué le parece a usted la metodología que se realizara para solución del problema encontrado en el área?			

ENCUESTA, PARA MEDIR LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar el Instrumento ENCUESTA, para medir la Variable Registro de Software y Hardware en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

REGISTRO DE SOFTWARE Y HARDWARE

PG.	Manejo de información de software y hardware	Malo	Regular	Bueno
1	¿Cuál es el nivel de capacidad que tiene el personal en el manejo de información de los equipos informáticos?			
2	¿Qué le parece la falta de capacitación del personal en las actualizaciones y versiones?			
3	¿Cómo califica la calidad del producto adquirido?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo califica usted la falta de información de los software y hardware, con qué fin fueron comprados?			
6	¿Qué le parece a usted la falta de un plan de contingencia ante un problema o riesgo?			
PG.	**Fines de la adquisición**			
7	¿Cómo calificas el proceso de datos de la información de los equipos informáticos?			
8	¿Cómo califica usted el manejo de la información del software y el hardware del área?			
9	¿Qué le parece a usted la calidad de los equipos informáticos que fueron adquiridos?			

10	¿Cuál es el nivel de mejora al adquirir software y hardware de última generación?			
PG.	**Software**			
11	¿Qué le parece la seguridad del software adquiridos, en cuanto a los datos guardados?			
12	¿Cómo califica usted el nivel de seguridad de información del software?			
13	¿Qué le parece las versiones que brindan los proveedores para la actualización de diversos software?			
14	¿Cómo califica la actualización de los programas antiguos a las nuevas versiones?			
15	¿Qué le parece el uso establecido para el software, Función de dicha?			
16	¿Cómo califica usted el uso de programas que bloquean páginas prohibidas?			
PG.	**Hardware**			
17	¿Cómo califica el servicio de mantenimiento al hardware (PC, impresoras, discos duros, laptops, etc?			
18	¿Qué le parece el tiempo que establecen para dar mantenimiento a las pcs?			
19	¿Cómo califica el nivel de solución de las fallas ocurridas?			
20	¿Qué le parece la reparación de los equipos informáticos ante riesgos y tiempo de uso?			

Anexo 29: *Cuestionario 5*

Encuesta Al Personal Del Área De Informática Para Medir La Variable Auditoria Informática

ENCUESTA, PARA MEDIR LA VARIABLE AUDITORÍA INFORMÁTICA, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar El Instrumento ENCUESTA, para medir la Variable Auditoría Informática en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

AUDITORÍA INFORMÁTICA

PG.	Informe preliminar	Malo	Regular	Bueno
1	¿Cómo calificaría usted la elaboración de una ficha técnica para realización de una auditoria informática en el área de patrimonio?			
2	¿Cómo cree que es el rendimiento de las adquisiciones de las TI?			
3	¿Qué le parece el manejo de información en el área de patrimonio?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo define la falta de información del área de patrimonio de las TI?			
6	¿Qué le parece la forma de recopilación de la información?			

PG.	Análisis de la situación actual			
7	¿Cómo calificas el proceso de datos de la información?			
8	¿Qué le parece la forma de manejo de información escasa dentro del área?			
9	¿Qué calificación daría usted al posible riesgo de pérdidas de información del área?			
10	¿Cómo califica usted la falta de interés de las adquisiciones dentro del área			
PG.	**Control y gestión de la información**			
11	¿Cómo califica el rendimiento de la seguridad de datos?			
12	¿Qué le parece la implantación de la auditoria informática para el mejor control de seguridad y manejo de la información?			
13	¿Cómo califica usted el plan de trabajo del área para minimización de riesgos en la perdida de datos informáticos?			
14	¿Qué le parece a usted la utilización de una metodología capaz de mejorar el desarrollo de información del área?			
15	¿Usted como personal administrativo cómo calificaría el estado de la seguridad de información?			
16	¿Cómo observa usted que se está dando el uso de las tecnologías de información?			
PG.	**Observaciones**			
17	¿De acuerdo con la investigación como califica las falencias encontradas en el manejo de información?			
18	¿Cómo califica el hallazgo de riesgos en las TI?			
19	¿Cómo califica el estudio que se realizó del manejo de información?			
20	¿Qué le parece a usted la metodología que se realizara para solución del problema encontrado en el área?			

ENCUESTA, PARA MEDIR LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar el Instrumento ENCUESTA, para medir la Variable Registro de Software y Hardware en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

REGISTRO DE SOFTWARE Y HARDWARE

PG.	**Manejo de información de software y hardware**	Malo	Regular	Bueno
1	¿Cuál es el nivel de capacidad que tiene el personal en el manejo de información de los equipos informáticos?			
2	¿Qué le parece la falta de capacitación del personal en las actualizaciones y versiones?			
3	¿Cómo califica la calidad del producto adquirido?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo califica usted la falta de información de los software y hardware, con qué fin fueron comprados?			
6	¿Qué le parece a usted la falta de un plan de contingencia ante un problema o riesgo?			
PG.	**Fines de la adquisición**			
7	¿Cómo calificas el proceso de datos de la información de los equipos informáticos?			

8	¿Cómo califica usted el manejo de la información del software y el hardware del área?			
9	¿Qué le parece a usted la calidad de los equipos informáticos que fueron adquiridos?			
10	¿Cuál es el nivel de mejora al adquirir software y hardware de última generación?			
PG.	**Software**			
11	¿Qué le parece la seguridad del software adquiridos, en cuanto a los datos guardados?			
12	¿Cómo califica usted el nivel de seguridad de información del software?			
13	¿Qué le parece las versiones que brindan los proveedores para la actualización de diversos software?			
14	¿Cómo califica la actualización de los programas antiguos a las nuevas versiones?			
15	¿Qué le parece el uso establecido para el software, Función de dicha?			
16	¿Cómo califica usted el uso de programas que bloquean páginas prohibidas?			
PG.	**Hardware**			
17	¿Cómo califica el servicio de mantenimiento al hardware (PC, impresoras, discos duros, laptops, etc?			
18	¿Qué le parece el tiempo que establecen para dar mantenimiento a las pcs?			
19	¿Cómo califica el nivel de solución de las fallas ocurridas?			
20	¿Qué le parece la reparación de los equipos informáticos ante riesgos y tiempo de uso?			

***Anexo 30**: Cuestionario 6*

ENCUESTA, PARA MEDIR LA VARIABLE AUDITORÍA INFORMÁTICA, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar El Instrumento ENCUESTA, para medir la Variable Auditoría Informática en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

AUDITORÍA INFORMÁTICA

PG.	Informe preliminar	Malo	Regular	Bueno
1	¿Cómo calificaría usted la elaboración de una ficha técnica para realización de una auditoria informática en el área de patrimonio?			
2	¿Cómo cree que es el rendimiento de las adquisiciones de las TI?			
3	¿Qué le parece el manejo de información en el área de patrimonio?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo define la falta de información del área de patrimonio de las TI?			
6	¿Qué le parece la forma de recopilación de la información?			
PG.	**Análisis de la situación actual**			
7	¿Cómo calificas el proceso de datos de la información?			

8	¿Qué le parece la forma de manejo de información escasa dentro del área?			
9	¿Qué calificación daría usted al posible riesgo de pérdidas de información del área?			
10	¿Cómo califica usted la falta de interés de las adquisiciones dentro del área			
PG.	**Control y gestión de la información**			
11	¿Cómo califica el rendimiento de la seguridad de datos?			
12	¿Qué le parece la implantación de la auditoria informática para el mejor control de seguridad y manejo de la información?			
13	¿Cómo califica usted el plan de trabajo del área para minimización de riesgos en la perdida de datos informáticos?			
14	¿Qué le parece a usted la utilización de una metodología capaz de mejorar el desarrollo de información del área?			
15	¿Usted como personal administrativo cómo calificaría el estado de la seguridad de información?			
16	¿Cómo observa usted que se está dando el uso de las tecnologías de información?			
PG.	**Observaciones**			
17	¿De acuerdo con la investigación como califica las falencias encontradas en el manejo de información?			
18	¿Cómo califica el hallazgo de riesgos en las TI?			
19	¿Cómo califica el estudio que se realizó del manejo de información?			
20	¿Qué le parece a usted la metodología que se realizara para solución del problema encontrado en el área?			

ENCUESTA, PARA MEDIR LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar el Instrumento ENCUESTA, para medir la Variable Registro de Software y Hardware en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

REGISTRO DE SOFTWARE Y HARDWARE

PG.	Manejo de información de software y hardware	Malo	Regular	Bueno
1	¿Cuál es el nivel de capacidad que tiene el personal en el manejo de información de los equipos informáticos?			
2	¿Qué le parece la falta de capacitación del personal en las actualizaciones y versiones?			
3	¿Cómo califica la calidad del producto adquirido?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo califica usted la falta de información de los software y hardware, con qué fin fueron comprados?			
6	¿Qué le parece a usted la falta de un plan de contingencia ante un problema o riesgo?			
PG.	**Fines de la adquisición**			
7	¿Cómo calificas el proceso de datos de la información de los equipos informáticos?			
8	¿Cómo califica usted el manejo de la información del software y el hardware del área?			
9	¿Qué le parece a usted la calidad de los equipos informáticos que fueron adquiridos?			

10	¿Cuál es el nivel de mejora al adquirir software y hardware de última generación?			
PG.	**Software**			
11	¿Qué le parece la seguridad del software adquiridos, en cuanto a los datos guardados?			
12	¿Cómo califica usted el nivel de seguridad de información del software?			
13	¿Qué le parece las versiones que brindan los proveedores para la actualización de diversos software?			
14	¿Cómo califica la actualización de los programas antiguos a las nuevas versiones?			
15	¿Qué le parece el uso establecido para el software, Función de dicha?			
16	¿Cómo califica usted el uso de programas que bloquean páginas prohibidas?			
PG.	**Hardware**			
17	¿Cómo califica el servicio de mantenimiento al hardware (PC, impresoras, discos duros, laptops, etc?			
18	¿Qué le parece el tiempo que establecen para dar mantenimiento a las pcs?			
19	¿Cómo califica el nivel de solución de las fallas ocurridas?			
20	¿Qué le parece la reparación de los equipos informáticos ante riesgos y tiempo de uso?			

Anexo 31: *Cuestionario 7*

ENCUESTA, PARA MEDIR LA VARIABLE AUDITORÍA INFORMÁTICA, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar El Instrumento ENCUESTA, para medir la Variable Auditoría Informática en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

AUDITORÍA INFORMÁTICA

PG.	Informe preliminar	Malo	Regular	Bueno
1	¿Cómo calificaría usted la elaboración de una ficha técnica para realización de una auditoria informática en el área de patrimonio?			
2	¿Cómo cree que es el rendimiento de las adquisiciones de las TI?			
3	¿Qué le parece el manejo de información en el área de patrimonio?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo define la falta de información del área de patrimonio de las TI?			
6	¿Qué le parece la forma de recopilación de la información?			
PG.	**Análisis de la situación actual**			
7	¿Cómo calificas el proceso de datos de la información?			
8	¿Qué le parece la forma de manejo de información escasa dentro del área?			

9	¿Qué calificación daría usted al posible riesgo de pérdidas de información del área?			
10	¿Cómo califica usted la falta de interés de las adquisiciones dentro del área			
PG.	**Control y gestión de la información**			
11	¿Cómo califica el rendimiento de la seguridad de datos?			
12	¿Qué le parece la implantación de la auditoria informática para el mejor control de seguridad y manejo de la información?			
13	¿Cómo califica usted el plan de trabajo del área para minimización de riesgos en la perdida de datos informáticos?			
14	¿Qué le parece a usted la utilización de una metodología capaz de mejorar el desarrollo de información del área?			
15	¿Usted como personal administrativo cómo calificaría el estado de la seguridad de información?			
16	¿Cómo observa usted que se está dando el uso de las tecnologías de información?			
PG.	**Observaciones**			
17	¿De acuerdo con la investigación como califica las falencias encontradas en el manejo de información?			
18	¿Cómo califica el hallazgo de riesgos en las TI?			
19	¿Cómo califica el estudio que se realizó del manejo de información?			
20	¿Qué le parece a usted la metodología que se realizara para solución del problema encontrado en el área?			

ENCUESTA, PARA MEDIR LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar el Instrumento ENCUESTA, para medir la Variable Registro de Software y Hardware en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

REGISTRO DE SOFTWARE Y HARDWARE

PG.	Manejo de información de software y hardware	Malo	Regular	Bueno
1	¿Cuál es el nivel de capacidad que tiene el personal en el manejo de información de los equipos informáticos?			
2	¿Qué le parece la falta de capacitación del personal en las actualizaciones y versiones?			
3	¿Cómo califica la calidad del producto adquirido?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo califica usted la falta de información de los software y hardware, con qué fin fueron comprados?			
6	¿Qué le parece a usted la falta de un plan de contingencia ante un problema o riesgo?			
PG.	**Fines de la adquisición**			
7	¿Cómo calificas el proceso de datos de la información de los equipos informáticos?			
8	¿Cómo califica usted el manejo de la información del software y el hardware del área?			
9	¿Qué le parece a usted la calidad de los equipos informáticos que fueron adquiridos?			
10	¿Cuál es el nivel de mejora al adquirir software y hardware de última generación?			

PG.	Software			
11	¿Qué le parece la seguridad del software adquiridos, en cuanto a los datos guardados?			
12	¿Cómo califica usted el nivel de seguridad de información del software?			
13	¿Qué le parece las versiones que brindan los proveedores para la actualización de diversos software?			
14	¿Cómo califica la actualización de los programas antiguos a las nuevas versiones?			
15	¿Qué le parece el uso establecido para el software, Función de dicha?			
16	¿Cómo califica usted el uso de programas que bloquean páginas prohibidas?			
PG.	**Hardware**			
17	¿Cómo califica el servicio de mantenimiento al hardware (PC, impresoras, discos duros, laptops, etc?			
18	¿Qué le parece el tiempo que establecen para dar mantenimiento a las pcs?			
19	¿Cómo califica el nivel de solución de las fallas ocurridas?			
20	¿Qué le parece la reparación de los equipos informáticos ante riesgos y tiempo de uso?			

Anexo 32: *Cuestionario 8*

ENCUESTA, PARA MEDIR LA VARIABLE AUDITORÍA INFORMÁTICA, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar El Instrumento ENCUESTA, para medir la Variable Auditoría Informática en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

AUDITORIA INFORMÁTICA

PG.	Informe preliminar	Malo	Regular	Bueno
1	¿Cómo calificaría usted la elaboración de una ficha técnica para realización de una auditoria informática en el área de patrimonio?			
2	¿Cómo cree que es el rendimiento de las adquisiciones de las TI?			
3	¿Qué le parece el manejo de información en el área de patrimonio?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo define la falta de información del área de patrimonio de las TI?			
6	¿Qué le parece la forma de recopilación de la información?			
PG.	**Análisis de la situación actual**			
7	¿Cómo calificas el proceso de datos de la información?			
8	¿Qué le parece la forma de manejo de información escasa dentro del área?			
9	¿Qué calificación daría usted al posible riesgo de pérdidas de información			

	del área?			
10	¿Cómo califica usted la falta de interés de las adquisiciones dentro del área			
PG.	**Control y gestión de la información**			
11	¿Cómo califica el rendimiento de la seguridad de datos?			
12	¿Qué le parece la implantación de la auditoria informática para el mejor control de seguridad y manejo de la información?			
13	¿Cómo califica usted el plan de trabajo del área para minimización de riesgos en la perdida de datos informáticos?			
14	¿Qué le parece a usted la utilización de una metodología capaz de mejorar el desarrollo de información del área?			
15	¿Usted como personal administrativo cómo calificaría el estado de la seguridad de información?			
16	¿Cómo observa usted que se está dando el uso de las tecnologías de información?			
PG.	**Observaciones**			
17	¿De acuerdo con la investigación como califica las falencias encontradas en el manejo de información?			
18	¿Cómo califica el hallazgo de riesgos en las TI?			
19	¿Cómo califica el estudio que se realizó del manejo de información?			
20	¿Qué le parece a usted la metodología que se realizara para solución del problema encontrado en el área?			

ENCUESTA, PARA MEDIR LA VARIABLE REGISTRO DE SOFTWARE Y HARDWARE, EN LA TESIS

Titulado: "**AUDITORÍA INFORMÁTICA CON METODOLOGÍA COBIT 4.5 PARA EL REGISTRO DE SOFTWARE Y HARDWARE DEL AREA DE PATRIMONIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI: 2017**"

OBJETIVO: Validar el Instrumento ENCUESTA, para medir la Variable Registro de Software y Hardware en Área de patrimonio de la Universidad Nacional de Ucayali: 2017"

INTRUCCIONES

- Al contestar, hágalo con la mayor objetividad y sinceridad.
- Este cuestionario es anónimo. No lo firme ni escriba ninguna identificación.
- Señale con una X el número de su preferencia dentro del cuadro ().
- No deje ninguna pregunta sin contestar.

Las respuestas que comprenden:

1	2	3
Malo	Regular	Bueno

REGISTRO DE SOFTWARE Y HARDWARE

PG.	Manejo de información de software y hardware	Malo	Regular	Bueno
1	¿Cuál es el nivel de capacidad que tiene el personal en el manejo de información de los equipos informáticos?			
2	¿Qué le parece la falta de capacitación del personal en las actualizaciones y versiones?			
3	¿Cómo califica la calidad del producto adquirido?			
4	¿Qué le parece la factibilidad del producto adquirido?			
5	¿Cómo califica usted la falta de información de los software y hardware, con qué fin fueron comprados?			
6	¿Qué le parece a usted la falta de un plan de contingencia ante un problema o riesgo?			
PG.	**Fines de la adquisición**			
7	¿Cómo calificas el proceso de datos de la información de los equipos informáticos?			
8	¿Cómo califica usted el manejo de la información del software y el hardware del área?			
9	¿Qué le parece a usted la calidad de los equipos informáticos que fueron adquiridos?			

10	¿Cuál es el nivel de mejora al adquirir software y hardware de última generación?			
PG.	**Software**			
11	¿Qué le parece la seguridad del software adquiridos, en cuanto a los datos guardados?			
12	¿Cómo califica usted el nivel de seguridad de información del software?			
13	¿Qué le parece las versiones que brindan los proveedores para la actualización de diversos software?			
14	¿Cómo califica la actualización de los programas antiguos a las nuevas versiones?			
15	¿Qué le parece el uso establecido para el software, Función de dicha?			
16	¿Cómo califica usted el uso de programas que bloquean páginas prohibidas?			
PG.	**Hardware**			
17	¿Cómo califica el servicio de mantenimiento al hardware (PC, impresoras, discos duros, laptops, etc?			
18	¿Qué le parece el tiempo que establecen para dar mantenimiento a las pcs?			
19	¿Cómo califica el nivel de solución de las fallas ocurridas?			
20	¿Qué le parece la reparación de los equipos informáticos ante riesgos y tiempo de uso?			