



**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ
MANUEL FÉLIX LÓPEZ**

CARRERA INFORMÁTICA

**TESIS PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA
INFORMÁTICA**

TEMA:

**AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA
INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO
TECNOLÓGICO DE LA ESPAM MFL**

AUTORAS:

**MARÍA VICTORIA RIVERA CHÁVEZ
MARÍA FERNANDA ZAMBRANO BRAVO**

TUTOR:

LIC. ÍTALO BÉCQUER BRIONES VÉLIZ MG. SC.

CALCETA, ABRIL 2015

DERECHO DE AUTORÍA

María Victoria Rivera Chávez y María Fernanda Zambrano Bravo, declaran bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos los derechos de propiedad intelectual a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, según lo establecido por la Ley de Propiedad Intelectual y su reglamento.

.....
MARÍA V. RIVERA CHÁVEZ

.....
MARÍA F. ZAMBRANO BRAVO

CERTIFICACIÓN DE TUTOR

Ítalo Bécquer Briones Véliz, certifica haber tutelado la tesis **AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL**, que ha sido desarrollada por **María Victoria Rivera Chávez y María Fernanda Zambrano Bravo**, previa la obtención del título de Ingeniero Informático, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica de Manabí Manuel Félix López.

.....
LIC. ÍTALO BÉCQUER BRIONES VÉLIZ

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han **APROBADO** la tesis **AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL**, que ha sido propuesta, desarrollada y sustentada por **María Victoria Rivera Chávez y María Fernanda Zambrano Bravo**, previa la obtención del título de Ingeniero Informático, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

.....
ING. SERGIO A. INTRIAGO BRIONES

MIEMBRO

.....
ING. HIRAIIDA M. SANTANA CEDEÑO

MIEMBRO

.....
LIC. JOSÉ G. INTRIAGO CEDEÑO

PRESIDENTE

AGRADECIMIENTO

A la Escuela Superior Politécnica de Manabí Manuel Félix López que me dio la oportunidad de una educación superior de calidad y en la cual he forjado mis conocimientos profesionales día a día.

A nuestro querido tutor el Lcdo. Bécquer Briones Véliz que gracias a su ayuda constante nos enriqueció de muy buenos conocimientos para llevar a cabo este gran objetivo.

A la Directora de Carrera la Ing. Jessica Morales Carrillo que con su ayuda se pudo agilizar todos los trámites reglamentarios para cumplir con este gran objetivo.

LAS AUTORAS

DEDICATORIA

A Dios por permitirme cada día levantarme con vida y fortaleza para seguir adelante con este gran logro.

A mi padre el Señor Ángel Antonio Rivera Sánchez que con mucho amor siempre ha estado ahí cuidándome, protegiéndome y dándome fuerzas para cumplir este objetivo.

A mi madre la Sra. Ida Teresa Sánchez Palacios que de alguna u otra manera ha sido motivo de inspiración para poder lograr este gran objetivo de mi vida.

A mi madre la Sra. Mercedes Chávez Valencia por ser una amiga que sin importar nuestras diferencias de opiniones me ha demostrado su apoyo incondicional.

A mi novio Adrián Alcívar que siempre ha estado brindándome sus consejos su apoyo, su motivación constante, pero más que nada su amor.

A toda mi familia que ha sido pilar fundamental para cumplir mis objetivos.

.....
MARÍA V. RIVERA CHÁVEZ

DEDICATORIA

A Dios fuente de inspiración de mi espíritu para la conclusión de esta tesis.

A mis padres quienes me dieron vida, educación, apoyo y consejos hicieron todo en la vida para que yo pudiera lograr mis sueños, por motivarme y darme la mano cuando sentía que el camino se terminaba.

A mis hijos quienes fueron un gran apoyo emocional durante el tiempo en que escribía esta tesis.

A mis hermanos que siempre estuvieron listos para brindarme toda su ayuda.

.....
MARÍA F. ZAMBRANO BRAVO

CONTENIDO GENERAL

CARATULA.....	i
DERECHO DE AUTORÍA.....	ii
CERTIFICACIÓN DE TUTOR.....	iii
APROBACIÓN DEL TRIBUNAL.....	iv
AGRADECIMIENTO.....	v
DEDICATORIA.....	vi
DEDICATORIA.....	vii
CONTENIDO GENERAL.....	viii
RESUMEN.....	xviii
PALABRAS CLAVES.....	xviii
ABSTRACT.....	xix
KEY WORDS.....	xix
CÁPITULO I. ANTECEDENTES.....	1
1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA.....	1
1.2. JUSTIFICACIÓN.....	3
1.3. OBJETIVOS.....	5
1.3.1. OBJETIVO GENERAL.....	5
1.3.2. OBJETIVOS ESPECÍFICOS.....	5
1.4. IDEA A DEFENDER.....	5
CÁPITULO II. MARCO TEÓRICO.....	7
2.1. AUDITORIA.....	7
2.1.1. AUDITORIA INFORMÁTICA.....	7
2.1.2. CLASES DE AUDITORÍA INFORMÁTICA.....	8
2.1.2.1. AUDITORIA INTERNA.....	8
2.1.2.2. AUDITORIA EXTERNA.....	10
2.1.3. TIPOS DE AUDITORÍA INFORMÁTICA.....	11
2.1.3.1. AUDITORÍA DE EXPLOTACIÓN.....	11
2.1.3.2. AUDITORÍA INFORMÁTICA DE DESARROLLO DE PROYECTOS O APLICACIONES.....	12
2.1.3.3. AUDITORÍA INFORMÁTICA DE COMUNICACIONES Y REDES.....	13
2.1.3.4. AUDITORIA DE SISTEMAS.....	13

2.1.3.5.	AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA.....	14
2.1.4.	EL PROCESO DE LA AUDITORÍA INFORMÁTICA	15
2.1.4.1.	PLANEACIÓN DE LA AUDITORÍA INFORMÁTICA	16
2.1.4.2.	EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA.....	17
2.1.4.2.1.	TÉCNICAS DE AUDITORIA	18
2.1.4.3.	ANÁLISIS DE RESULTADOS	23
2.1.4.4.	COMUNICACIÓN DE RESULTADOS	23
2.1.4.5.	INFORME FINAL	23
2.1.4.5.1.	TIPOS DE INFORME DE AUDITORÍA	24
2.2.	CONTROL INTERNO	26
2.2.1.	CLASIFICACIÓN DEL CONTROL INTERNO.....	27
2.3.	AMBIENTE DE CONTROL	30
2.4.	LA CONSTITUCIÓN DEL ECUADOR.....	31
2.4.1.	LEYES.....	31
2.4.1.1.	LEY ORGÁNICA DE CONTRALORÍA GENERAL DEL ESTADO (LOCGE)	32
2.4.2.	NORMATIVAS LEGALES DEL ECUADOR.....	33
2.4.2.1.	NORMAS DE CONTROL INTERNO EN TECNOLOGÍAS DE INFORMACIÓN.....	33
2.4.2.2.	NORMAS ISO	35
2.4.3.	LOS SISTEMAS DE INFORMACIÓN	36
2.4.4.	TECNOLOGÍA DE LA INFORMACIÓN	36
2.4.4.1.	PROBLEMAS ÉTICOS EN LA UTILIZACIÓN DE LAS TECNOLOGÍAS INFORMÁTICAS EN LAS ORGANIZACIONES.....	37
2.4.4.2.	RIESGOS DE LAS TECNOLOGÍAS DE INFORMACIÓN.....	37
2.5.	METODOLOGÍAS DE AUDITORÍA	38
2.5.1.	CMM – MODELO DE MADUREZ	38
2.5.2.	RIESGO – CONFIANZA	39
	CÁPITULO III. DESARROLLO METODOLÓGICO	41
3.1.	ALCANCE	41
3.2.	RESTRICCIONES.....	42
3.3.	MÉTODO DE TRABAJO	43
3.3.1.	FASE I. PLANIFICACIÓN DE LA AUDITORÍA	43

3.3.1.1.	PLANIFICACIÓN PRELIMINAR	44
3.3.1.2.	PLANIFICACIÓN ESPECÍFICA	45
3.3.2.	FASE II. EJECUCIÓN DE LA AUDITORIA.....	46
3.3.3.	FASE III. ANÁLISIS DE LOS RESULTADOS.....	47
3.3.4.	FASE IV. COMUNICACIÓN DE RESULTADOS	48
CÁPITULO IV. RESULTADOS Y DISCUSIÓN.....		50
4.1.	IDENTIFICACIÓN DE LAS ÁREAS QUE CAREZCAN DE NORMATIVIDAD	50
4.1.1.	ANÁLISIS DE RESULTADOS DEL CUMPLIMIENTO DE NORMAS EN EL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL.....	50
4.1.1.1.	DOCUMENTACIÓN.....	51
4.1.1.2.	HARDWARE.....	52
4.1.1.3.	SOFTWARE.....	56
4.2.	RESULTADOS PORCENTUALES DE LA EVALUACIÓN DE LA NORMA DE CONTROL INTERNO	59
4.2.1.	MATRIZ RIESGO CONFIANZA GENERAL	59
4.2.2.	GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO POR INDIVIDUO Y COMPONENTE NORMA CONTROL INTERNO.....	60
4.2.3.	GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO DEL DEPARTAMENTO POR COMPONENTE NORMA CONTROL INTERNO	60
4.2.4.	GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO-CONFIANZA POR INDIVIDUO CONTROL INTERNO	61
4.2.5.	GRAFICO REPRESENTATIVO DEL PROMEDIO GENERAL PORCENTUAL DEL NIVEL DE RIESGO-CONFIANZA DEL DEPARTAMENTO NORMA CONTROL INTERNO	61
4.3.	DESCRIPCIÓN DE LOS GRÁFICOS	62
4.4.	ANÁLISIS DE LOS RIESGOS SEGÚN NORMA DE CONTROL INTERNO	63
4.5.	ANÁLISIS DE LOS RESULTADOS DE LAS TABULACIONES DE LAS ENCUESTAS REALIZADAS AL PERSONAL ADMINISTRATIVO Y LAS DIFERENTES CARRERAS DE LA ESPAM MFL	63
4.6.	ANÁLISIS DE RESULTADOS DEL CUMPLIMIENTO DE LA NORMA ISO 27000 EN EL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL	73
4.6.1.	INVENTARIO DE ACTIVO SEGÚN LA NORMA ISO 27000.....	73

4.6.2.	SEGURIDAD DE LOS RECURSOS HUMANOS SEGÚN LA NORMA ISO 27000	76
4.6.3.	SEGURIDAD FÍSICA DEL ENTORNO SEGÚN LA NORMA ISO 27000 79	
4.6.4.	GESTIÓN DE COMUNICACIÓN Y DE OPERACIÓN SEGÚN LA NORMA ISO	82
4.6.5.	CONTROL DE ACCESO SEGÚN NORMA ISO 27000	85
4.6.6.	CUMPLIMIENTO SEGÚN LA NORMA ISO 27000	88
4.7.	RESULTADOS PORCENTUALES DE LA EVALUACIÓN DE LA NORMA ISO 27000	90
4.7.1.	MATRIZ RIESGO CONFIANZA GENERAL NORMA ISO 27000	90
4.7.2.	GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO NORMA ISO 27000	90
4.7.3.	GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO NORMA ISO 27000 POR COMPONENTE	91
4.7.4.	GRAFICO REPRESENTATIVO DEL PROMEDIO GENERAL PORCENTUAL DEL NIVEL DE RIESGO POR INDIVIDUO NORMA ISO 27000 ...	91
4.7.5.	GRAFICO REPRESENTATIVO DEL PROMEDIO GENERAL PORCENTUAL DEL NIVEL DE RIESGO DEL DEPARTAMENTO NORMA ISO 27000	92
4.8.	DESCRIPCIÓN DE LOS GRÁFICOS	92
4.9.	ANÁLISIS DE LOS RIESGOS SEGÚN NORMA ISO 27000	94
4.10.	OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE CHECKLIST NORMA DE CONTROL INTERNO	98
4.11.	OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE CHECKLIST NORMA ISO 27000	98
4.12.	NIVEL DE MADUREZ DE LOS PROCESO ESTUDIADOS EN EL DEPARTAMENTO TECNOLÓGICO	101
4.12.1.	CRITERIOS DE EVALUACIÓN DE LOS PROCESOS ESTUDIADOS EN EL DEPARTAMENTO TECNOLÓGICO	101
CAPITULO V. CONCLUSIONES Y RECOMENDACIONES		104
5.1.	CONCLUSIONES	104
5.2.	RECOMENDACIONES	106
BIBLIOGRAFÍA		107
ANEXOS		113

CONTENIDO DE CUADROS

Cuadro 3.1. Determinación del Nivel de Riesgo-Confianza.....	45
Cuadro 4.1. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Jefe del Departamento Tecnológico	50
Cuadro 4.2. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Analista de Computo 1.....	51
Cuadro 4.3. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Jefe del Departamento Tecnológico	52
Cuadro 4.4. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Asistente de Computo 2.....	53
Cuadro 4.5. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Asistente de Computo 1.....	53
Cuadro 4.6. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Asistente de Computo 2.....	54
Cuadro 4.7. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Jefe del Departamento Tecnológico	55
Cuadro 4.8. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Analista de Computo.....	56
Cuadro 4.9. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Asistente de Computo 1.....	56
Cuadro 4.10. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Asistente de Computo 2.....	58
Cuadro 4.11. Matriz general porcentual del nivel de Riesgo-Confianza Control Interno	58
Cuadro 4.12. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico	72

Cuadro 4.13. Matriz de Riesgo – Confianza en el cumplimiento de la norma ISO 27000 al Analista de Computo	73
Cuadro 4.14. Matriz de Riesgo – Confianza en el cumplimiento de la norma ISO 27000 al Asistente de Computo 1	74
Cuadro 4.15. Matriz de Riesgo – Confianza en el cumplimiento de la norma ISO 27000 al Asistente de Computo 2	75
Cuadro 4.16. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico	76
Cuadro 4.17. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Analista de Computo	76
Cuadro 4.18. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 1	77
Cuadro 4.19. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 2	78
Cuadro 4.20. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico	79
Cuadro 4.21. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Analista de Cómputo	79
Cuadro 4.22. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 1	80
Cuadro 4.23. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 2	81
Cuadro 4.24. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico	82
Cuadro 4.25. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Analista de Cómputo	83
Cuadro 4.26. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Cómputo 1	83
Cuadro 4.27. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 2	84

Cuadro 4.28. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico	85
Cuadro 4.29. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Analista de Cómputo	85
Cuadro 4.30. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Cómputo 1	86
Cuadro 4.31. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 2	87
Cuadro 4.32. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico	88
Cuadro 4.33. Matriz general porcentual del nivel de Riesgo-Confianza Norma ISO 27000.....	89
Cuadro 4.34. Observaciones encontradas mediante la aplicación de ckecklist Control Interno	95
Cuadro 4.35. Observaciones encontradas mediante la aplicación de ckecklist Control Interno	97
Cuadro 4.36. Nivel de Madurez de los procesos estudiados en el Departamento Tecnológico.....	100
Cuadro 4.37. Criterios de evaluacion de los procesos estudiados en el Departamento Tecnológico.....	101

CONTENIDO DE TABLAS

Tabla 4.1. Promedio Riesgo General Control Interno del departamento tecnológico.....	
---	--

Tabla 4.2. Resultado de la encuesta realizadas al personal que labora en la institución PREGUNTA 1	63
Tabla 4.3. Resultado de la encuesta realizadas al personal que labora en la institución PREGUNTA 2	64
Tabla 4.4. Resultado de la encuesta realizadas al personal que labora en la institución PREGUNTA 2	65
Tabla 4.5. Resultado de la encuesta realizadas al personal que labora en la institución PREGUNTA 2	66
Tabla 4.6. Resultado de la encuesta realizadas al personal que labora en la institución PREGUNTA 2	67
Tabla 4.7. Resultado de la encuesta realizadas al personal que labora en la institución PREGUNTA 3	68
Tabla 4.8. Resultado de la encuesta realizadas al personal que labora en la institución PREGUNTA 3	69
Tabla 4.9. Resultado de la encuesta realizadas al personal que labora en la institución PREGUNTA 3	69
Tabla 4.10. Resultado de la encuesta realizadas al personal que labora en la institución PREGUNTA 3	70
Tabla 4.11. Promedio Riesgo General del departamento tecnológico.....	93

CONTENIDO DE FIGURAS

Figura 2.1. Pirámide de Procesos	15
Figura 2.2. Tipos de Informes de Auditoría	24
Figura 2.4. Niveles de Modelo de Madurez	38

CONTENIDO DE GRÁFICOS

Gráfico 4.1. Grafico Representativo general porcentual del nivel de Riesgo – Confianza por individuo y componente Norma Control Interno	59
Gráfico 4.2. Grafico Representativo general porcentual del nivel de Riesgo – Confianza del Departamento por Componente Control Interno.....	59
Gráfico 4.3. Grafico Representativo general porcentual del nivel de Riesgo – Confianza por Individuo Control Interno.....	60
Gráfico 4.4. Grafico Representativo del promedio general porcentual del nivel de riesgo Riesgo-Confianza del Departamento Norma Control Interno.....	60
Gráfico 4.7. Equipos Tecnológicos a cargo de custodios.....	64
Gráfico 4.8. Mantenimiento Preventivo a Equipos Tecnológicos.....	65
Gráfico 4.9. Tiempo de Mantenimiento Preventivo a Equipos Tecnológicos...	66
Gráfico 4.10. Tiempo de tardanza en el Mantenimiento Preventivo a Equipos Tecnológicos	66
Gráfico 4.11. Negativa a la realización del Mantenimiento Preventivo de los Equipos Tecnológicos	67
Gráfico 4.12. Mantenimiento Correctivo a Equipos Tecnológicos	68
Gráfico 4.13. Tiempo de Mantenimiento Correctivo a Equipos Tecnológicos..	69

Gráfico 4.14. Negativa a la realización del Mantenimiento Correctivo de los Equipos Tecnológicos	70
Gráfico 4.15. Solicitud de Mantenimiento Preventivo o Correctivo	71
Gráfico 4.16. Grafico Representativo general porcentual del nivel de riesgo Riesgo-Confianza por individuo Norma ISO 27000.....	89
Gráfico 4.17. Grafico Representativo general porcentual del nivel de riesgo Riesgo-Confianza Norma ISO 27000 por Componente.....	90
Gráfico 4.18. Grafico Representativo del promedio general porcentual del nivel de riesgo Riesgo-Confianza por individuo Norma ISO 27000.....	90
Gráfico 4.19. Grafico Representativo del promedio general porcentual del nivel de riesgo Riesgo-Confianza del Departamento Norma ISO 27000.....	91

RESUMEN

La aplicación de una auditoría al control y mantenimiento de la infraestructura tecnológica en el Departamento Tecnológico de la ESPAM MFL, permitió evaluar el nivel de cumplimiento de aplicaciones de buenas prácticas, estándares y normas de control interno de las TI de la Contraloría General del Estado Ecuatoriano con respecto a los procesos, políticas y procedimientos de los recursos tecnológicos (equipos de comunicación y redes, computación, software base) existentes en la entidad, para el efecto, se empleó la metodología determinada en las Normas Internacionales de Auditoría, dividida en tres fases: Planificación, envolvió un estudio completo de todos los elementos tanto internos como externos a la entidad, utilizando la evaluación de control interno en TI 410-09 y Norma ISO 27000 con la finalidad de determinar los hechos de mayor relevancia; en la fase de Ejecución se aplicaron los programas de auditoría, los que permitieron evidenciar los principales hallazgos ocasionados en la entidad y en la fase de Comunicación de Resultados se detallaron las conclusiones y recomendaciones mediante la presentación del Informe Final. En base a los resultados obtenidos de la evaluaciones, se determinó que el área auditada lleva lineamientos generales de control y mantenimiento en la infraestructura tecnológica, pero no aplica adecuadamente las normas mencionada anteriormente, evidenciando que el riesgo es alto y su confianza es bajo en sus procesos, por lo tanto, es conveniente la aplicación de dichas normativas que permitan tomar mayor organización y responsabilidad, minimizando los riesgos en la infraestructura tecnológica.

PALABRAS CLAVES

Auditoría, Infraestructura Tecnológica, Control y Mantenimiento, Hardware, Software.

ABSTRACT

The application of an audit control and maintenance of the technological infrastructure in the Technology Department of the ESPAM MFL, allowed us to evaluate the level of compliance application of best practices, standards and internal control standards of IT Comptroller General of the Ecuadorian State regarding the processes, policies and procedures of technological resources (communications and networking, computing, software base) existing in the state, for that purpose, the particular methodology was used in the International Standards Audit, divided into three phases: Planning, wrapped a complete internal and external to the entity using the evaluation of internal control in TI 410-09 and ISO 27000 in order to determine the facts further study of all elements relevance; at the stage of execution audit programs were applied, which revealed the main findings arising in the entity and the phase of Communicating Results conclusions and recommendations were detailed by submitting the Final Report. Based on the results of the evaluation, it was determined that the audited area carries general guidelines for control and maintenance the IT infrastructure, but not properly applied the standards mentioned above, showing that the risk is high and confidence is low in their processes, therefore, it is appropriate to apply these regulations to allow greater organization and take responsibility, minimizing risks in technological infrastructure.

KEY WORDS

Audit, Technology Infrastructure, Control and Maintenance, Hardware, Software

CÁPITULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

Actualmente todas las empresas a nivel mundial, están expuestas a nuevas amenazas que ponen en peligro los sistemas informáticos. Este tipo de problemática se da muy a menudo porque muchas de las organizaciones no cuentan con el personal capacitado en la aplicación de las prácticas efectivas para cumplir a cabalidad con la Ley.

Según la Contraloría General del Estado (2009), estas organizaciones deben contar con normas de control interno de las tecnologías de información, que estarán acoplados a un marco de trabajo que les permita hacer una buena planeación, evaluación y organización de sus diversos procesos tecnológicos, que se realizan a diario en la institución.

Ramírez y Álvarez (2009) refiere que la auditoría informática explica que siempre todo sistema tiene algo que mejorar, es decir, por muy bien que se realicen las cosas, una auditoría reflejará debilidades y puntos fuertes de la empresa, lo que en resumidas cuentas se transformarán en datos que siempre podrán ser obtenidos con el fin de perfeccionar, y sobre todo, teniendo en cuenta que estamos en un mundo cambiante donde las tecnologías de la información nunca paran de avanzar ofreciendo nuevas oportunidades para romper barreras de seguridad, o de optimizar la eficiencia de un sistema de información.

Los entes del estado están vinculados con la función de la entidad, para ello, están clasificados en entes estatales públicos, que son entes del Estado que cumplen una función privada; los públicos no estatales, que son privados y por su vinculación con la labor estatal son públicos; y privados que son no públicos, sin embargo están sometidos al controles extremos: normas de salubridad, seguridad e higiene.

Todas las Instituciones públicas son entes del Estado Ecuatoriano y deben contar con un Auditor Interno que es asignado por Contraloría, a su vez, es el que se encarga de verificar si se están cumpliendo estas normas de control interno, si los recursos de la institución están siendo utilizados adecuadamente y además estén alineados de acuerdo a los objetivos institucionales, de esta manera se podrá detectar cuáles son sus debilidades y los posibles riesgos que pueden tener las organizaciones sino cumplen con la normativa legal del país.

Por último las autoras de acuerdo a la investigación que ellas realizaron en la Institución, plasman que, en la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López (ESPAM MFL) según su organigrama estructural, cuenta con el departamento tecnológico, el mismo, que se encarga de administrar, controlar y mantener la infraestructura tecnológica, distribuyendo, así, todos sus equipos informáticos físicos y lógicos con ayuda del departamento de almacén, quién es el que les asigna la ubicación de los mismos en las diferentes áreas informatizadas de la entidad. Todas las funciones y procesos que se realizan en esta unidad tecnológica deben estar acorde con la aplicación de las prácticas efectivas y la adopción de normas de control interno en tecnologías de información de la Contraloría General del Estado, ya que la información y todos los recursos tecnológicos manejados por el Coordinador del departamento, son de vital importancia y por lo tanto tienen que ser controladas.

Es por este motivo que las autoras se plantean la siguiente interrogante:

¿Cómo evaluar la aplicación de las mejores prácticas y la adopción de normas de la Infraestructura Tecnológica en el Departamento Tecnológico de la ESPAM MFL?

1.2. JUSTIFICACIÓN

En la actualidad existe muy poca difusión y menor aceptación por parte de las empresas sobre la necesidad de contar con una función de auditoría en informática; es por esto que las necesidades relacionadas con la misma, obligan a las entidades aplicar políticas y procedimientos que aseguren el uso adecuado de los recursos tecnológicos que soportan a los objetivos de la institución. Los procesos, procedimientos y normas sobre las auditorías, analizados durante la investigación, permiten evaluar el grado de cumplimiento de los procedimientos, lineamientos y disposiciones establecidas para la actividad productiva (Acosta, *et al*, 2011).

De acuerdo a la información encontrada en la investigación, las autoras plasman que la situación actual acorde con el desarrollo tecnológico de la ESPAM MFL, en lo referente a como se manejan los diferentes procesos tales como: los procesos de instalaciones de equipos informáticos, mantenimientos correctivos y preventivos, entre otros procesos que realiza al departamento se maneja de manera informal y un tanto desordenada por lo que las autoras tuvieron como finalidad constatar si sus procesos y actividades son correctos y si se encuentran enmarcados y en conformidad con las practicas efectivas y generales de la organización, mediante una auditoría informática, siendo realizada y ejecutada por las autoras , las cuales deberán proponer recomendaciones efectivas, para que se puedan minimizar riesgos, reflejando debilidades y diferentes puntos fuertes del área a estudiar de la Institución.

La investigación también se la realizó con el motivo de vincularnos de manera beneficiosa con la universidad, según la LOES, 2010 (Ley Orgánica de Educación Superior) en el “Art. 8.- Literal f. Fomentar y ejecutar programas de investigación de carácter científico, tecnológico y pedagógico que coadyuven al mejoramiento y protección del ambiente además de promover el desarrollo sustentable Nacional” , al mismo tiempo, considerando el Manual de Sistemas de Investigación Institucional del Art.- 7. Reglamento de tesis de grado del manual de investigaciones.- La tesis de investigación laboral son realizadas por

el postulante(s) en centros académicos, de investigación, producción o servicio local, regional, nacional o internacional a fin a su formación profesional y consiste en estudiar alternativas de solución científica a un problema presentado en el centro patrocinado, cumpliendo así todas las normativas reglamentarias.

Por lo tanto las autoras pretenden realizar la Auditora Informática, con el fin de, verificar el nivel de cumplimiento de políticas, planes y procedimientos de la aplicación de buenas prácticas que emplea la ESPAM MFL en cuanto a tecnologías de información, mediante las normas ISO, normas de estándares de calidad y normas de control interno de tecnologías de información emitidas por la Contraloría General del Estado.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

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.

1.3.2. OBJETIVOS ESPECÍFICOS

- Verificar el grado de cumplimiento al mantenimiento y control de la infraestructura tecnológica de acuerdo a la Norma 410-09 de TI y Norma ISO 27000.
- Relevar riesgos de Tecnologías de Información.
- Identificar las áreas que carezcan de normatividad.
- Verificar el nivel de cumplimiento de políticas, planes y procedimientos que emplea el Departamento Tecnológico en cuanto al uso de los recursos tecnológicos.
- Emitir el informe de auditoría de la infraestructura tecnológica tomando en cuenta todos los hallazgos recopilados.

1.4. IDEA A DEFENDER

Al aplicar auditoría al control y mantenimiento de la infraestructura tecnológica del departamento tecnológico en la ESPAM MFL, se evaluará el cumplimiento

de las aplicaciones de las buenas prácticas, estándares y normas de control interno en Tecnologías de Información emitidas por la Contraloría General del Estado Ecuatoriano.

CÁPITULO II. MARCO TEÓRICO

2.1. AUDITORIA

Auditoría, en su sentido más general, se puede entender como la investigación, consulta, revisión, verificación, comprobación y obtención de evidencia, desde una posición de independencia, sobre la documentación e información de una organización, realizadas por un profesional, el auditor, designado para desempeñar tales funciones. (Nava, s.f).

Las observaciones de Ocampo, *et al*, (2010) revelan que así como existen normas y procedimientos específicos para la realización de auditorías contables, debe haber también normas y procedimientos para la realización de auditorías en informática como parte de una profesión. Pueden estar basadas en las experiencias de otras profesiones pero con algunas características propias y siempre guiándose por el concepto de que la auditoría debe ser más amplia que la simple detección de errores, y además la auditoría debe evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución.

2.1.1. AUDITORIA INFORMÁTICA

Según Piattini, *et al*, (2008) dice que la auditoría en informática se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional; por lo tanto, nada más se señalarán algunos aspectos básicos para su entendimiento.

La auditoría informática no sólo se centra en evaluar los equipos de cómputo con que cuenta la organización, sino que también se encarga de la evaluación de los sistemas de información, desde sus entradas, pasando por los procedimientos, archivos, información y las salidas de información (Herrera, 2013).

Las investigaciones de Ocampo, *et al*, (2010) demuestran que el auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas asistidas por ordenador. El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Los principales objetivos que constituyen a la auditoría informática son el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos (Carvajal, 2008).

2.1.2. CLASES DE AUDITORÍA INFORMÁTICA

La auditoría, como cualquier disciplina toma características diferentes de acuerdo al campo de acción en que se desenvuelven. Sin embargo, el objetivo final debe responder a la definición general de auditoría. (Whitten, 2010).

2.1.2.1. AUDITORIA INTERNA

Es la realizada con recursos materiales y personas que pertenecen a la empresa auditada.

La auditoría interna se puede concebir como una parte del control interno. La realizan personas dependientes de la organización con un grado de independencia suficiente para poder realizar el trabajo objetivamente; una vez acabado su cometido han de informar a la Dirección de todos los resultados

obtenidos. La característica principal de la auditoría interna es, por tanto, la dependencia de la organización y el destino de la información. Hay autores, que la definen como «el órgano asesor de la dirección que busca la manera de dotar a la empresa de una mayor eficiencia mediante el constante y progresivo perfeccionamiento de políticas, sistemas, métodos y procedimientos de la empresa. (Whitten, 2010).

Tello, (2008) define que en una empresa, los responsables de Informática escuchan, orientan e Informan sobre las posibilidades técnicas y los costes de tal Sistema. Con voz, pero a menudo sin voto, Informática trata de satisfacer lo más adecuadamente posible aquellas necesidades. La empresa necesita controlar su Informática y ésta necesita que su propia gestión esté sometida a los mismos procedimientos y estándares que el resto de aquella. La conjunción de ambas necesidades cristaliza en la figura del auditor interno informático.

La auditoría informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido o matiz "político" ajeno a la propia estrategia y política general de la empresa. La función auditora puede actuar de oficio, por iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente. (Alfonso, *et al*, 2012).

a) Principal ventaja de la auditoria interna:

- Debido a que el auditor permanece conoce las problemática, funciones, actividades, áreas y operaciones.
- Por otra parte el coste será menor puesto que los recursos solo son internos para organización, por lo tanto no representan ninguna erogación adicional.
- El informe que rinde el auditor, independientemente del resultado, es solo de carácter interno y por lo tanto no sale de la empresa, ya que únicamente le sirve a las autoridades de la institución.

- Puede llevar un programa concreto de evaluación en apoyo a las autoridades de la empresa, lo cual ayudara a sus dirigentes en la evaluación y la toma de decisiones. (Alfonso, *et al*, 2012).

b) Principal desventaja de la auditoria interna:

- Posible falta de objetividad de las personas que la llevan a cabo, puesto que pueden estar directamente implicados en el propio sistema de información, al laborar en la misma empresa donde realiza la auditoria, puede presentar presiones, compromisos y ciertos intereses al realizar la evaluación.
- Su veracidad, alcance y confiabilidad pueden ser limitados, debido a que puede haber injerencias por parte de las autoridades de la institución sobre la forma de evaluar y emitir informes.
- Se pueden presentar vicios de trabajo del auditor con relativa frecuencia, ya sea en las formas de utilizar las técnicas y herramientas para aplicar la auditoria, como en la forma de evaluar y emitir su informe sobre la misma. (Alfonso, *et al*, 2012).

2.1.2.2. AUDITORIA EXTERNA

Según Whitten, 2010 refiere que la definición de auditoría externa generalizada, es la siguiente: «El objetivo de un examen de los estados financieros de una compañía, por parte de un auditor independiente, es la expresión de una opinión sobre si los mismos reflejan razonablemente su situación patrimonial, los resultados de sus operaciones y los cambios en la situación financiera, de acuerdo con los principios de contabilidad generalmente aceptados y con la legislación vigente». Algunos autores, como J. L. Larrea y A. S. Suárez, califican la auditoría como externa por su condición de legalidad y porque el auditor es ajeno a la empresa; mientras que otros autores lo hacen por los efectos que ella produce frente a terceros (inscripción en el Registro Mercantil).

a) Principal ventaja de la auditoria externa

- Alto grado de objetividad que se consigue en comparación con los auditores internos, dado que es realizada por un personal ajeno a la empresa, puesto que no tendrá condicionantes de dependencia jerárquica o vinculaciones de otro tipo con la empresa (Whitten, 2010).
- En su realización, estas auditorías pueden estar apoyadas por una mayor experiencia por parte de los auditores externos, debido a que utiliza técnicas y herramientas que ya fueron probadas en otras empresas con características similares (Whitten, 2010).
- Sus dictámenes pueden ser válidos para las autoridades impositivas, y con ello pueden satisfacer requerimientos de carácter legal, siempre que sean realizadas por auditores de prestigio que tengan el reconocimiento público. (Whitten, 2010).

b) El principal inconveniente de la auditoria externa

- Dado por el alejamiento de la problemática de la empresa de quienes asumen la responsabilidad de llevar a cabo la auditoria. No obstante, la profesionalidad y experiencia de quienes de quienes asumen la auditoria deben superar estos inconvenientes para llevar a cabo un trabajo adecuado. (Whitten, 2010).
- Depende en absoluto de la cooperación que el auditor pueda obtener de parte de los auditados. (Whitten, 2010).
- Su evaluación, alcances y resultados pueden ser muy limitados. (Whitten, 2010).
- En algunos casos son sumamente costosas para la empresa, no solo en el aspecto numérico, sino por el tiempo y trabajo adicional que representan. (Whitten, 2010).

2.1.3. TIPOS DE AUDITORÍA INFORMÁTICA

2.1.3.1. AUDITORÍA DE EXPLOTACIÓN

La explotación informática se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, órdenes automatizadas para lanzar o modificar procesos industriales, etc. La explotación informática se puede considerar como una fábrica con ciertas peculiaridades que las distinguen de las reales (Carvajal, 2008).

Carvajal, (2008) refiere que la auditoría de explotación consiste en auditar las secciones que la componen y sus interrelaciones. La explotación informática se divide en tres grandes áreas:

- Planificación;
- Producción y
- Soporte Técnico.

2.1.3.2. AUDITORÍA INFORMÁTICA DE DESARROLLO DE PROYECTOS O APLICACIONES

Revisión del proceso completo de desarrollo de proyectos por parte de la empresa auditada. Según la Universidad Autónoma Ecuatoriana Hidalgo, (2011) expresa que el análisis se basa en cuatro aspectos fundamentales:

- Revisión de las metodologías utilizadas:

Se analizarán éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas

- Control Interno de las Aplicaciones:

Se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo: Estudio de Vialidad de la Aplicación, Definición Lógica de la Aplicación, Desarrollo Técnico de la Aplicación, Diseño de Programas, Métodos de Pruebas, Documentación, Equipo de Programación.

- Satisfacción de usuarios:

Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

- Control de Procesos y Ejecuciones de Programas Críticos:

Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran podría provocar graves y altos costos de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial informativo, etc.

2.1.3.3. AUDITORÍA INFORMÁTICA DE COMUNICACIONES Y REDES

Revisión de la topología de Red y determinación de posibles mejoras, análisis de caudales y grados de utilización (UAEH, 2011).

Carvajal, (2008) indica que en la auditoria de comunicaciones ha de verse:

- La gestión de red. Los equipos y su conectividad.
- La monitorización de las comunicaciones.
- La revisión de costes y la asignación formal de proveedores.
- Creación y aplicabilidad de estándares.

2.1.3.4. AUDITORIA DE SISTEMAS

Los sistemas de información son cada vez más complejos, integrados y relacionados. La administración efectiva de la Tecnología de la Información (TI) es un elemento crítico para la supervivencia y el éxito de las compañías, varias son las razones que producen esta alto nivel de criticidad, por ejemplo la dependencia que tienen las organizaciones de la información para su funcionamiento, el nivel de inversión que tienen en el área de TI, la potencialidad que tiene la TI para transformar las organizaciones, los riesgos y

amenazas que en la actualidad tiene la información, la economía globalizada que exige un alto nivel de competitividad, entre otras. La auditoría de sistemas es el conjunto de técnicas, actividades y procedimientos destinados a analizar, evaluar, supervisar y recomendar sobre cuestiones relacionadas con la planificación, el seguimiento, la eficacia, seguridad y adecuación de los sistemas de información en las empresas (Kuna, et al, 2010).

2.1.3.5. AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA.

Es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que la Universidad necesita tener en funcionamiento para poder llevar a cabo toda su actividad, tanto docente como de investigación o de gestión interna. (UOC, 2013).

El conjunto de hardware consta de elementos tan diversos como los aires acondicionados o los estabilizadores de corriente de las salas de máquinas, los sensores, las cámaras, los grandes ordenadores que hacen de servidores de aplicaciones, los elementos de red, como routers o cortafuegos, los ordenadores personales, las impresoras, los teléfonos, entre otros equipos. (UOC, 2013).

El conjunto de software va desde los sistemas operativos (un conjunto de programas de computación destinados a desempeñar una serie de funciones básicas esenciales para la gestión del equipo) hasta el software de sistemas (son aplicaciones de ámbito general necesarias para que funcionen las aplicaciones informáticas concretas de los servicios; por ejemplo, las bases de datos, los servidores de aplicaciones o las herramientas de ofimática. (UOC, 2013).

Las autoras definen a la infraestructura tecnológica como al conjunto de hardware y software que tiene una unidad informática en la cual abarcan todos los procesos, políticas y procedimientos que se realicen en ella para su debida utilización.

Para el mantenimiento y control de la infraestructura tecnológica se debe contar con un plan de Mantenimiento, y a la vez llevar de una manera organizada el control de todos los procedimientos en el área tecnológico.

Para evaluar estos procesos de mantenimiento y control el auditor debe comprender y analizar los planes de mantenimiento de la Infraestructura o plataforma Tecnología (hardware y software) implementado por el área informática de la unidad. (OLACEFs, 2011).

2.1.4. EL PROCESO DE LA AUDITORÍA INFORMÁTICA

Lara y Párraga, (2013) llegan a la conclusión que el proceso de la auditoría informática es similar al que se lleva a cabo a los de estados financieros, en el cual, los objetivos principales son: salvaguardar los activos, asegurar la integridad de los datos, la consecución de los objetivos gerenciales y, la utilización racional de los recursos, con eficiencia y eficacia, para lo que se realiza la recolección y evaluación de evidencias.

Para que una auditoría sea exitosa, debe tomar en cuenta muchos de los aspectos tratados en el punto anterior. A continuación se muestra un gráfico que muestra cómo actúan conjuntamente todos los componentes, tanto de la empresa como del auditor, para que se genere una auditoría efectiva y eficaz.



Figura 2.1. Pirámide de procesos

Fuente: Lara y Parraga, (2013)

Loor, A. y Espinoza, V., (2012), refiere que de acuerdo a las Normas Internacionales de Auditoría, el proceso de la auditoría comprende las siguientes fases (IAASB, 2009).

2.1.4.1. PLANEACIÓN DE LA AUDITORÍA INFORMÁTICA

Planeación de la auditoría, en función de los objetivos de la misma. Incluye el estudio general preliminar de la entidad, su misión, sus objetivos, sus funciones y sus características de desempeño (Blanco, L., 2011)

Según Martínez *et, al.* (2012). Define las siguientes etapas en la planeación de la auditoría:

✓ PLANIFICACIÓN PRELIMINAR.

El auditor se familiariza con las áreas a ser evaluadas, observando a simple vista los problemas que enfrentan, volviéndose parte de la empresa (ESPE, 2010).

Al terminar la revisión preliminar el auditor puede proceder a seguir una de las tres opciones:

- Diseñar la auditoría.
- Realizar una revisión detallada de los controles internos.
- Decidir no confiar en los controles internos (Loor, A. y Espinoza, V., 2012).

✓ PLANIFICACIÓN ESPECÍFICA

Escuela Superior Politécnica del Ejército, (2010), expresa que en esta fase el auditor logra planificar su área de trabajo, junto con la medición del control interno que efectúa y la elaboración de su programa de trabajo.

2.1.4.2. EJECUCIÓN DE LA AUDITORÍA INFORMÁTICA

Esta fase es la más extensa de la auditoría ya que debe efectuarse pruebas, procedimientos y prácticas de auditoría en detalle que contribuyan a la obtención de hallazgo, mismas que aportarán al auditor para la elaboración del informe. Para ello las auditoras trabajaron con:

✓ HALLAZGOS DE LA AUDITORÍA

Los hallazgos en la auditoría, se definen como asuntos que llaman la atención del auditor y que en su opinión, deben comunicarse a la entidad, ya que representan deficiencias importantes que podrían afectar en forma negativa, su capacidad para registrar, procesar, resumir y reportar información confiable y consistente, en relación con las aseveraciones efectuadas por la administración (Whitten, 2008).

✓ ELEMENTOS DE LOS HALLAZGOS DE LA AUDITORÍA

Según Piattini, (2008), la extensión mínima de cada hallazgo de auditoría dependerá de cómo éste debe ser informado, aunque por lo menos, el auditor debe identificar los siguientes elementos:

- Condición: Se refiere a la situación actual encontrada por el auditor al examinar un área, actividad, función u operación, entendida como “lo que es”.
- Criterio: Comprende la concepción de “lo que debe ser “, con lo cual el auditor mide la condición del hecho o situación.
- Efecto: Es el resultado adverso o potencial de la condición encontrada, generalmente representa la pérdida en términos monetarios originados por el incumplimiento para el logro de la meta, fines y objetivos institucionales.
- Causa: Es la razón básica (o las razones) por lo cual ocurrió la condición, o también el motivo del incumplimiento del criterio de la norma. Su identificación requiere de la habilidad y el buen juicio del auditor y, es indispensable para el

desarrollo de una recomendación constructiva que prevenga la recurrencia de la condición

✓ **EVIDENCIAS DE AUDITORÍA**

Lloor y Espinoza, (2012) expresa que la evidencia de una auditoría es el conjunto de hechos comprobados, suficientes, evidencia de competentes y pertinentes (relevantes) que sustentan las conclusiones de auditoría. Las evidencias de auditoría constituyen los elementos de prueba que obtiene el auditor sobre los hechos que examina y cuando éstas son suficientes y competentes, constituyen el respaldo del examen que sustenta el contenido de la auditoría.

✓ **PAPELES DE TRABAJO**

Los papeles de trabajo de la auditoría deberán mostrar los detalles de la evidencia, la forma de su obtención, las pruebas a que fue sometido y las conclusiones sobre su validez. Son propiedad absoluta del auditor condicionando su uso únicamente a los propósitos de su revisión y soporte de los resultados obtenidos. Además, los papeles de trabajo son archivos que guarda el auditor de los procedimientos aplicados, las pruebas realizadas y de la información obtenida. También buscan respaldar la efectividad y suficiencia del trabajo a más de servir de guía para auditorías futuras (Gallardo y Salazar, 2014).

2.1.4.2.1. TÉCNICAS DE AUDITORIA

De acuerdo con Piattini *et, al.* (2008), para la obtención de evidencias se pueden utilizar diversos tipos de técnicas, procedimientos y herramientas de auditoría, de los cuales destacan el análisis de datos, debido que para las organizaciones el conjunto de datos o información son de tal importancia, por lo que es necesario verificarlos y comprobarlos; utilizando diversas técnicas para el análisis de datos, entre las cuales los autores nombran las siguientes:

✓ **OBSERVACIÓN DIRECTA**

Es una técnica que permite captar con todos los sentidos de la realidad de la organización y puede ser de dos tipos. No participante, es aquella en que el auditor observa externamente el proceso sin interferir en ellos y, participante, es aquella en la que el auditor participa en los procesos de la unidad auditada, integrándose en el grupo y sus actividades. En cualquier caso, hay que definir el objetivo de la observación (cuál es el motivo de su realización), las variables de la observación (que queremos observar, planificación de la observación (que haremos durante la observación y transcripción de la observación (como se expresara la observación, por escrito, visualmente, etc.) (Barros y Cadena, 2012).

✓ **ENTREVISTA**

Es una técnica útil y arriesgada, ésta representa la inversión del territorio laboral de una persona, es lógico por lo tanto reacciones defensivas e incluso hostiles. Una forma de 'rebajar' la tensión, está en adoptar una postura amigable y de colaboración. El éxito de la entrevista, depende de los siguientes factores (repartidos por igual entre el auditor y el entrevistado): la experiencia y los conocimientos del auditor y la predisposición y los conocimientos del entrevistado (Barros y Cadena, 2012).

El tema de la entrevista ocupa un lugar muy destacado dentro de las técnicas aplicadas de recogida de datos ya que es una de las más utilizadas en las investigaciones, después de la técnica de la encuesta, técnica cuantitativa, la entrevista se diferencia de la encuesta en que es una técnica Cualitativa (Barros y Cadena, 2012).

✓ **ENCUESTAS**

La encuesta es una técnica de investigación realizada sobre una muestra poblacional de un colectivo más amplio que permitirá obtener datos de los sujetos encuestados en forma estadística; este instrumento utilizará un listado de preguntas cerradas a fin de recolectar los datos. (Gallardo y Salazar, 2014).

✓ **CHECKLIST.**

El checklist es una herramienta útil para ayudar a definir un problema y organizar las ideas, las autoras lo utilizarán al inicio de la resolución de los problemas de la auditoría informática, durante las fases de definición, medición y análisis del ciclo para mejorar su proceso en el departamento tecnológico (AUDISA, 2009).

Además como definición de problemas se utiliza para identificar información específica que se requiere para completar la descripción del problema. La forma de cómo utilizarlo es siguiendo los siguientes pasos:

- 1.- Las autoras deberán completar el checklist para la definición del problema.
- 2.- Una vez que se haya recogido suficiente información, se deberá responder las preguntas en la hoja para la definición de problemas.
- 3.- Se redactará y acordará una descripción efectiva del problema. Una descripción efectiva del problema debe ser:
 - Específica.- Que explique qué está mal y distinga la deficiencia de los otros problemas en la institución.
 - Observable.- Que describa la evidencia visible del problema.
 - Medible.- Que indique el alcance del problema en términos cuantificables.
 - Manejable.- Esto significa que:
 - a.- Se puede resolver dentro de la esfera de influencia del equipo.
 - b.- Se puede resolver en un tiempo razonable (AUDISA, 2009).

✓ **MATRIZ DE RIESGOS**

Una vez definidos los objetivos y el alcance del trabajo a realizar, se desarrollaron criterios de evaluación de riesgos de Tecnologías de Información, que es el aspecto en el que se va a centrar esta evaluación, para el Área de Informática.

Para la identificación de los riesgos, se entrevista a cada uno de los expertos, donde se analizan los problemas que afectan al departamento, se establece la Matriz de Ponderaciones y se determinan los riesgos más relevantes.

Para la valoración de los riesgos que se analizan, se definió una escala de valoración Cualitativa, que es la asignación de las características Alto, Moderado y Bajo a los diferentes riesgos encontrados.

Una matriz de riesgos muestra gráficamente tanto las amenazas a que están expuestos los sistemas computarizados y la información del departamento, como los objetos que comprenden el departamento informático.

Se describe a continuación los pasos para el desarrollo del método:

- Crear la matriz de amenazas (causas de riesgo) y de objetos del sistema a analizar.
- Categorizar los riesgos.

Luego de ponderar los riesgos existentes dentro del Departamento, trabajo realizado por el grupo de experto, se determinan lo que compondrá la Matriz de Control de Riesgos (Amenazas y Objetos). (Loor y Espinoza, 2012).

✓ **MODELOS DE MADUREZ**

El desarrollo de un modelo de madurez se enmarca dentro de las Ciencias del Diseño, donde la investigación se ejecuta a través del proceso de construcción y evaluación de artefactos (II/ISSN, 2013).

En general un modelo de madurez incluye niveles que representan el desarrollo del área o proceso en cuestión y elementos de medición que permitan determinar el nivel de madurez. De acuerdo al trabajo desarrollado por Montaña, (2008), se tiene que la aplicación de los modelos de madurez se presenta en las siguientes áreas de aplicación:

Modelos de Madurez para el Desarrollo de Software

Modelos de Madurez para el Desarrollo de las Capacidades

Modelos de Madurez para la Gestión de Proyectos

Modelos de Madurez de Habilidad de Cambio

Modelos de Madurez de Gestión del Conocimiento

✓ **TESTINGS DE VELOCIDAD DE INTERNET**

Este test sirve para medir tu velocidad real de conexión a Internet. A diferencia de los test provistos por los ISPs, los cuales solo miden la velocidad de Conexión a Internet desde sus servidores, este test mide el ancho de banda total Nacional e Internacional que usarás para navegar por Internet.

Para realizar esta medición de velocidad de internet podemos las autoras hicieron uso de estos dos servicios online:

- CNT
- OKLA

✓ **TABLAS DINÁMICAS**

Una tabla dinámica es una de las herramientas más poderosas de Excel, pero también es una de las características que más usuarios de Excel se sienten intimidados a utilizar. Si eres uno de ellos te estás perdiendo de utilizar una gran herramienta de Excel.

Las tablas dinámicas te permiten resumir y analizar fácilmente grandes cantidades de información con tan sólo arrastrar y soltar las diferentes columnas que formarán el reporte (Ortíz, M., 2011).

2.1.4.3. ANÁLISIS DE RESULTADOS

En esta fase se toman en consideración todo los resultados obtenidos posteriormente para ser analizados y poder concluir y recomendar a la máxima autoridad o jefe del departamento al que se esté auditando.

2.1.4.4. COMUNICACIÓN DE RESULTADOS

Las auditoras una vez que estudian y evalúan toda la información obtenida, adjuntan los hallazgos señalando la interpretación que se hace de ellos, en esta fase se desarrolla el informe de auditoría en la que se toma como base los programas de planificación, las hojas de hallazgos y los papales de trabajo que son el soporte documentado de las auditoras.

Los resultados obtenidos se proporcionan a la entidad auditada mediante el informe final de auditoría, que incorpora las recomendaciones a ser aplicadas y monitoreadas principalmente en su planificación estratégica, capacitación e indicadores de gestión.

2.1.4.5. INFORME FINAL

El informe de auditoría es una opinión formal, o renuncia de los mismos, expedido por un auditor interno o por un auditor externo independiente como resultado de una auditoria interna o externa o evaluación realizada sobre una entidad jurídica o sus subdivisiones (llamado "auditado"). El informe es presentado posteriormente a un "usuario" (por ejemplo, un individuo, un grupo de personas, una empresa, un gobierno, o incluso el público en general, entre otros) como un servicio de garantía para que el usuario pueda tomar

decisiones basadas en los resultados de la auditoría (Gallardo y Salazar, 2014).

2.1.4.5.1. TIPOS DE INFORME DE AUDITORÍA

Business Assurance and Audit, s.f., refiere que los informes de auditoría expresan la opinión de un profesional independiente sobre el contenido razonable y confiable de los estados financieros, sistema de control interno, etc. de una entidad. Su elaboración, pero sobre todo, su interpretación, resultan claves para poder interpretar, resultan claves para poder analizar el estado de una empresa.

Hay cuatro tipos comunes de los informes de auditoría, cada uno presenta una situación diferente encontrada durante el trabajo del auditor. Los cuatro informes son los siguientes:

- Informe de Auditoria sin Salvedades
- Informe de Auditoria con Salvedades
- Informe de Auditoria sin Opinión
- Informe de Auditoria Adverso/Rechazado

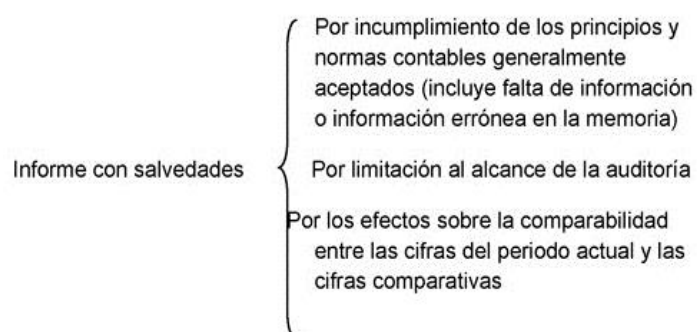


Figura 2.2. Tipos de Informes de Auditoría Informática

Fuente: Contraloría general del Estado

Las autoras pretenden hacer uso en la presente investigación el informe con salvedad, ya que pretenden evaluar las normas de control interno de la Contraloría General del Estado Ecuatoriano en la ESPAM MFL.

✓ INFORME CON SALVEDADES

Es usual y resulta lógico que el auditor recoja la salvedad o salvedades suficientemente explicadas y detalladas, ya que se causan, normalmente, por las diferencias de criterios o de interpretación que ante un mismo hecho o circunstancia, se producen entre los administradores o sus asesores y el propio auditor o firma de auditoría (Mira, s.f)

Opinión con salvedades. La opinión con salvedades supone la existencia de excepciones o discrepancias significativas en el cumplimiento de los principios, normas y criterios aplicables, sin llegar a justificar una opinión adversa o una abstención o denegación de opinión. Una opinión con salvedades puede responder a alguna de las circunstancias siguientes:

- Que existan limitaciones al alcance de la fiscalización.
- Que los estados financieros resulten erróneos o incompletos, por incumplimiento de principios y normas contables, aplicación no uniforme de los mismos o existencia de omisiones significativas de información.
- Que exista incertidumbre con respecto al contenido de las cuentas y los hechos con ellas relacionados, cuyo desarrollo final e incidencia cuantitativa no sean susceptibles de una estimación razonable Estas circunstancias deberán ser verificables, y recogerse explícitamente en el informe, de forma concisa, debidamente justificadas, y cuantificando en lo posible su incidencia. En cualquier caso, la opinión deberá mencionar la existencia de estas salvedades (CCOPCEE, s.f.).

Según Mira, s.f. expresa que las salvedades en el informe del auditor se refieren a cualquiera de las excepciones particulares que este se ve precisado a hacer a alguna de las afirmaciones genéricas del dictamen estándar, (dictamen normal o dictamen no calificado). Las afirmaciones genéricas del

dictamen normal sobre las cuales se efectúan las salvedades del auditor tienen relación con las normas de Auditoría de General Aceptación sobre la información. Es recomendable usar los términos "excepto por" o "salvo por" para expresar una excepción particular o salvedad que individualmente o en conjunto no afecte un área importante.

Orellana, 2008, refiere que las limitaciones en el alcance de las normas de auditoría son las siguientes:

- Cuando fue contratado como auditor externo en una fecha posterior a la de realización del inventario físico inicial o final de bienes, sin haber podido validar las existencias mediante procedimientos alternativos de auditoría.
- Cuando el ente no le permite al auditor solicitar confirmaciones escritas de terceros (clientes, abogados, etc.), sin haber podido validar su pertenencia e integridad mediante procedimientos alternativos de auditoría.
- Cuando el ente registra contablemente parte de las operaciones sin conservar la documentación de respaldo pertinente.

Cuando la Dirección del Ente se niega a suscribir la carta de gerencia o carta de confirmación escrita de los directivos del ente, en relación con explicaciones relevantes que no pueden ser confirmadas aplicando otros procedimientos de auditoría.

2.2. CONTROL INTERNO

El control interno será responsabilidad de cada institución del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos y tendrá como finalidad crear las condiciones para el ejercicio del control. (NCI, 2009).

El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos. Constituyen componentes del control interno el ambiente de control, la evaluación de riesgos, las actividades de control, los sistemas de información y comunicación y el seguimiento. (NCI, 2009).

El control interno está orientado a cumplir con el ordenamiento jurídico, técnico y administrativo, promover eficiencia y eficacia de las operaciones de la entidad y garantizar la confiabilidad y oportunidad de la información, así como la adopción de medidas oportunas para corregir las deficiencias de control. (NCI, 2009).

2.2.1. CLASIFICACIÓN DEL CONTROL INTERNO

Carvajal, (2008), manifiesta que los controles internos se clasifican en los siguientes:

- **Controles preventivos:** Para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- **Controles detectivos:** Cuando fallan los preventivos, para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.
- **Controles correctivos:** Facilitan la suelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.
- **Controles sobre captura de datos:** Sobre altas de movimientos, modificaciones de movimientos, consultas de movimientos, mantenimiento de los ficheros.

- **Controles de proceso de datos:** Normalmente se incluyen en los programas. Se diseñan para detectar o prevenir los siguientes tipos de errores: entrada de datos repetidos, procesamiento y actualización de ficheros o ficheros equivocados, entrada de datos ilógicos, pérdida o distorsión de datos durante el proceso.
- **Controles de supervisión: controles de la tecnología de la información (TI):** Son el conjunto de normas y procedimientos que deben existir en todo centro de proceso de datos para asegurar la confidencialidad, integridad y disponibilidad de los datos informatizados. Aseguran que los procedimientos programados dentro de un sistema informático se diseñen, implanten, mantengan y operen de forma adecuada y que solo se introduzcan cambios autorizados en los programas y en los datos. Dentro de las TI nos encontraremos con distintos tipos de controles.
- **Controles de mantenimiento:** Destinados a asegurar que las modificaciones de los procedimientos programados están adecuadamente diseñadas, probadas, aprobadas e implantadas.
- **Controles de seguridad de programas:** Destinado a garantizar que no se puedan efectuar cambios no autorizados en los procedimientos programados.
- **Controles de seguridad de ficheros de datos:** Destinados a asegurar que no se puedan efectuar modificaciones no autorizadas en los archivos de datos.
- **Controles de la operación informática:** Destinados a garantizar los procedimientos programados autorizados se apliquen de manera uniforme y se utilicen versiones correctas de los ficheros de datos.
- **Controles de conversión de ficheros:** Destinados a garantizar una completa y exacta conversión de los datos de un sistema antiguo a uno nuevo.

- **Controles de software sistema:** Destinados a asegurar que se implante un software de sistema apropiado y que se encuentre protegido contra modificaciones no autorizadas.
- **Controles de implantación:** Destinados a asegurar que los procedimientos programados para los nuevos sistemas son adecuados y están efectivamente implantados, y que el sistema esté diseñado para satisfacer las necesidades del usuario.
- **Controles de seguridad informática:** Este tipo de controles evitarán el riesgo de fraude o de que información confidencial o sensible llegue a personas no autorizadas dentro o fuera de la sociedad. Otro riesgo que evitaríamos con la seguridad física sería el posible daño o destrucción de las instalaciones informáticas como resultado de incendios, inundaciones o sabotajes que podrían interrumpir la ejecución de los procesos.
- **Controles de operaciones informáticas:** Los procedimientos de operaciones que cubren procesos diferidos o por lotes que se realizan en momentos específicos deben estar documentados, programados y mantenidos en forma adecuada. Las copias de seguridad de los programas y de los datos deben estar siempre disponibles para casos de emergencia. Las instalaciones informáticas de los usuarios finales deben ser apropiadas para las necesidades del negocio y controladas para maximizar la compatibilidad y apoyar eficazmente al usuario. Con todos estos controles podremos evitar fallos en los equipos y en el software o como mínimo tendremos capacidad para recuperarnos de ellos o sacar poco rendimiento de los sistemas informáticos.
- **Controles de supervisión: controles de los usuarios:** Son los procedimientos manuales tradicionales que se deben ejecutar sobre los documentos y transacciones antes y después de su proceso en el ordenador para comprobar el adecuado y continuo funcionamiento de los controles de las aplicaciones.

2.3.AMBIENTE DE CONTROL

El ambiente de control se determina por el conjunto de circunstancias que enmarcan el accionar de una entidad, organización o empresa, desde una perspectiva de control interno y que son determinantes para el cumplimiento de las metas y objetivos de la organización en que los principios y políticas actúan, sobre las conductas y los procedimientos organizacionales. (Barros y Cadena, 2012).

El sistema de control interno está relacionado directamente con las actividades operativas y de procedimiento dentro de la organización y, existen por razones empresariales fundamentales y, a que estos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y el cumplimiento de las leyes y normas vigentes.

El ambiente control se puede definir como un proceso, efectuado por el personal de una organización, diseñado para conseguir objetivos específicos. Los auditores deben considerar factores que influyen en la organización y que garantizan el éxito de sus procesos internos, siendo los más importantes los siguientes:

- La filosofía y el estilo de la dirección y gerencia.
- La estructura del plan organizacional, los reglamentos y los manuales de procedimientos.
- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los colaboradores de la organización, así como su adhesión a las políticas y objetivos establecidos.
- Las formas de asignación de responsabilidades, de administración y desarrollo del personal.

- El grado de documentación de políticas, decisiones y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

Cada uno de estos factores ayuda a que las organizaciones crezcan y cumplan sus principales objetivos, que permiten el éxito o fracaso de las mismas, siendo estos criterios:

- Eficacia y eficiencia de las operaciones.
- Fiabilidad de la información.
- Cumplimiento de las leyes y normas aplicables.

De acuerdo a estos factores, es necesario que los encargado realicen evaluaciones al ambiente de control en el Departamento Tecnológico de la ESPAM MFL, en el cual permita identificar los riesgos y definir los controles adecuados para que puedan contrarrestarlos ,es decir el núcleo principal de control son las personas que si no tienen integridad, valores éticos y competencias, el resto de procesos posiblemente no funcionarán, por lo cual, debe establecerse un adecuado ambiente de control sobre el que se desarrollan las operaciones de la organización a evaluarse.

2.4.LA CONSTITUCIÓN DEL ECUADOR

La Constitución Política es la norma jurídica fundamental del Estado, es decir, la “LEY SUPREMA” que sirve para reglar su organización y establecer las relaciones del Poder Público con las Funciones y Órganos del mismo y las de las personas y la sociedad con el Estado.

2.4.1. LEYES

Icaza, (2010) expresa que la ley es una norma escrita emanada del poder legislativo, por lo que es la norma por excelencia del ordenamiento jurídico y prima sobre las demás. Dentro de esta categoría podemos distinguir los diferentes tipos de leyes de acuerdo a su contenido y a su jerarquización constitucional, para lo cual podemos dividir las en:

- Leyes orgánicas
- Leyes estatutarias
- Leyes marco
- Leyes de facultades
- Leyes de convocatoria a Asamblea Nacional Constituyente y de convocatoria a Referendo
- Leyes aprobatorias
- Leyes ordinarias

2.4.1.1. LEY ORGÁNICA DE CONTRALORÍA GENERAL DEL ESTADO (LOGE)

Según la Ley Orgánica de la Contraloría General del Estado, (2004) en el Art. 1.- Objeto de la Ley.- La presente Ley tiene por objeto establecer y mantener, bajo la dirección de la Contraloría General del Estado, el sistema de control, fiscalización y auditoría del Estado, y regular su funcionamiento con la finalidad de examinar, verificar y evaluar el cumplimiento de la visión, misión y objetivos de las instituciones del Estado y la utilización de recursos, administración y custodia de bienes públicos.

➤ CONTRALORÍA GENERAL DEL ESTADO

Según la Constitución Ecuatoriana, (2008) dispone en sus artículos 204, 205 y 211, la Contraloría General del Estado es un organismo técnico dotado de personalidad jurídica y autonomía administrativa, financiera, presupuestaria y organizativa, dirigida y representada por el Contralor General del Estado, quien

desempeñará sus funciones durante cinco años.

Es en este contexto que la Contraloría General del Estado, como organismo técnico de control, cumple con las funciones a ella encomendadas ya sea efectuando auditorías de gestión, financieras, de carácter técnico o bien exámenes especiales de los recursos financieros, materiales y humanos, en base a un plan anual de actividades. (CE, 2008).

2.4.2. NORMATIVAS LEGALES DEL ECUADOR

La Constitución del Ecuador, (2008) en su artículo 18, numeral segundo menciona que todas las personas, en forma individual o colectiva, tienen derecho a acceder libremente a la información generada en instituciones públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley en caso de violación a los derechos humanos, ninguna institución pública negará la información.

2.4.2.1. NORMAS DE CONTROL INTERNO EN TECNOLOGÍAS DE INFORMACIÓN

Normas de Control Interno, (2009) estableció que La Ley Orgánica de la Contraloría General del Estado, dispone a este organismo, la regulación del funcionamiento del sistema de control, con la adaptación, expedición, aprobación y actualización de las Normas de Control Interno. A partir de este marco regulador, cada institución del Estado dictará las normas, políticas y manuales específicos que consideren necesarios para su gestión.

Según Contraloría General del Estado, (2003) dispuso que las Normas de Control Interno desarrolladas incluyen: normas generales y otras específicas relacionadas con la administración financiera gubernamental, talento humano, tecnología de la información y administración de proyectos y recogen la utilización del marco integrado de control interno emitido por el Comité de

Organizaciones que patrocina la Comisión Treadway (COSO), que plantea cinco componentes interrelacionados e integrados al proceso de administración, con la finalidad de ayudar a las entidades a lograr sus objetivos.

Las Normas de Control Interno son concordantes con el marco legal vigente y están diseñadas bajo principios administrativos, disposiciones legales y normativa técnica pertinente.

Mediante las Normas (410) de Control Interno de Tecnologías de Información, emitidas por la Contraloría General del Estado, las autoras solo evaluarán el grado de cumplimiento de la siguiente norma:

410-09 Mantenimiento y control de la infraestructura tecnológica.- La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades. Los temas a considerar son:

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios. (NCI, 2009).

2. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondencia bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias. (NCI, 2009).

3. Control y registro de las versiones del software que ingrese a producción. (NCI, 2009).

4. Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y de publicación. (NCI, 2009).

5. Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementaran medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura. (NCI, 2009).

6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad. (NCI, 2009).

7. Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables. (NCI, 2009).

8. El mantenimiento de los bienes que se encuentran en garantía será proporcionado por el proveedor, sin costo adicional para la entidad. (NCI, 2009).

Con esta norma 410-09 las autoras definen su alcance y establecen las restricciones debidas para la ejecución de esta tesis.

2.4.2.2. NORMAS ISO

ISO/IEC 27000. Las normas ISO/IEC 27000 constituyen una familia de estándares, desarrolladas por la International Organization for Standardization (ISO) y por la International Electrotechnical Commission (IEC). Esta familia de

estándares se publicó ante la necesidad de contar con una base para la gestión de la seguridad de la información, especificando los requisitos para establecer, implementar, controlar, mantener e innovar un Sistema de Gestión de Seguridad de la Información (SGSI). La serie ISO 27000 está formada por varias normas. Son consideradas como normas base: ISO 27001 e ISO 27002, mientras que las normas complementarias son principalmente: ISO 27003, ISO 27004, e ISO 27005 (ISO/IEC, 2012).

2.4.3. LOS SISTEMAS DE INFORMACIÓN

Yáñez, (2011) puntualiza que para adentrarse en el proceso de una auditoría a las tecnologías de la información y comunicaciones, es requisito imprescindible comprender los conceptos de sistemas, información y tecnologías de las comunicaciones. Al lograr una visión y conocimientos del entorno informático, el auditor juzgará, de manera suficiente, la naturaleza de la problemática y riesgos a los cuales se verá enfrentado al planificar y realizar la auditoría.

2.4.4. TECNOLOGÍA DE LA INFORMACIÓN

Con el acercamiento de las distancias se reordena el tiempo y el espacio, para generar nuevos procesos que transforman la sociedad; algunos lo llaman globalización, y refiere a ese proceso que, gracias a las tecnologías de información, abre canales de comunicación y atraviesa fronteras, modificando culturas e identidades, generando nuevas formas de democracia y de participación. (Castells, 2010).

De acuerdo a estas apreciaciones las autoras determinan tomar como referencia a la norma (410) de las Normas de Control Interno de la Contraloría General del Estado Ecuatoriano para así poder realizar el debido análisis a la institución y dar como resultado conclusiones y recomendaciones.

2.4.4.1. PROBLEMAS ÉTICOS EN LA UTILIZACIÓN DE LAS TECNOLOGÍAS INFORMÁTICAS EN LAS ORGANIZACIONES

Los problemas éticos han sido estudiados durante muchos años, se han realizado conferencias en el ámbito internacional en los problemas éticos de tecnología de información, interviniendo los Países Bajos, Reino Unido, EEUU, Italia, entre otros. La ética de la información está basada en la fundación filosófica de ética informática, esta ética informática es calificada como una disciplina filosófica. Según Christofolletti y Piassa, (2013) expresa que la popularización masiva de las computadoras personales, la expansión de dispositivos de comunicación móviles y el aumento de la oferta de internet en banda ancha son factores que ayudan a mantener un conjunto de transformaciones en la sociabilidad y en la comunicabilidad humana, que afectan directamente al Periodismo como actividad profesional, institución y modelo de producción de una forma específica de conocimiento.

Estos factores básicos igualmente permitieron al público -antes confinado al estado de receptor de la información- participar de modo colaborativo y activo en el proceso comunicacional; tales factores también causaron una avalancha entre los profesionales y organizaciones para adaptarse al nuevo y tumultuoso escenario (Christofolletti y Piassa, 2013).

Las últimas dos décadas han sido pródigas en estudios de investigación acerca de los impactos de las nuevas tecnologías en la técnica periodística, pero el conjunto de transformaciones también lanza rayos de luz a los debates éticos. Después de todo, si cambian los instrumentos, cambian las prácticas y, con ellas, se pueden cambiar los comportamientos, tanto en el ámbito general como en el profesional (Christofolletti y Piassa, 2013).

2.4.4.2. RIESGOS DE LAS TECNOLOGÍAS DE INFORMACIÓN

Entre los riesgos más comunes de las Tecnologías de Información son las siguientes, según refiere Vásquez, s.f.:

- Procesamiento de datos incorrecto por errores en la operación de los sistemas
- Ataques externos (hackers, virus)
- Accesos no autorizados a información sensible del negocio
- Fuga de información por mal uso de dispositivos externos (USB, telefonía)
- Falta de alineación de los objetivos de negocio con los recursos y proyectos de TI.
- Debilidad para garantizar la recuperación de la infraestructura de TI y continuidad del negocio.
- Ausencia de un marco regulatorio (gobierno de TI)

2.5.METODOLOGÍAS DE AUDITORÍA

2.5.1. CMM – MODELO DE MADUREZ

Quintuña, V. s.f., refiere a que el Modelo de Madurez de Capacidades es un modelo de referencia para la aplicación de conceptos de gestión de procesos y de mejora de calidad en el desarrollo y mantenimiento de software. Según este modelo, la madurez de los procesos de desarrollo de software en una organización pasa por 5 niveles: primero o inicial, en que los procesos son inmaduros, no han sido medidos ni controlados nunca; segundo o repetible, centrado en la administración de proyectos, tercero o definido, que se fija en el proceso de ingeniería, cuarto o gestionado (o controlado) en el cual se mejora la calidad del producto y del proceso y quinto u optimizado, llegados a este punto la mejora de los procesos es continuo. Esto se muestra en la **figura 2.4** a continuación:

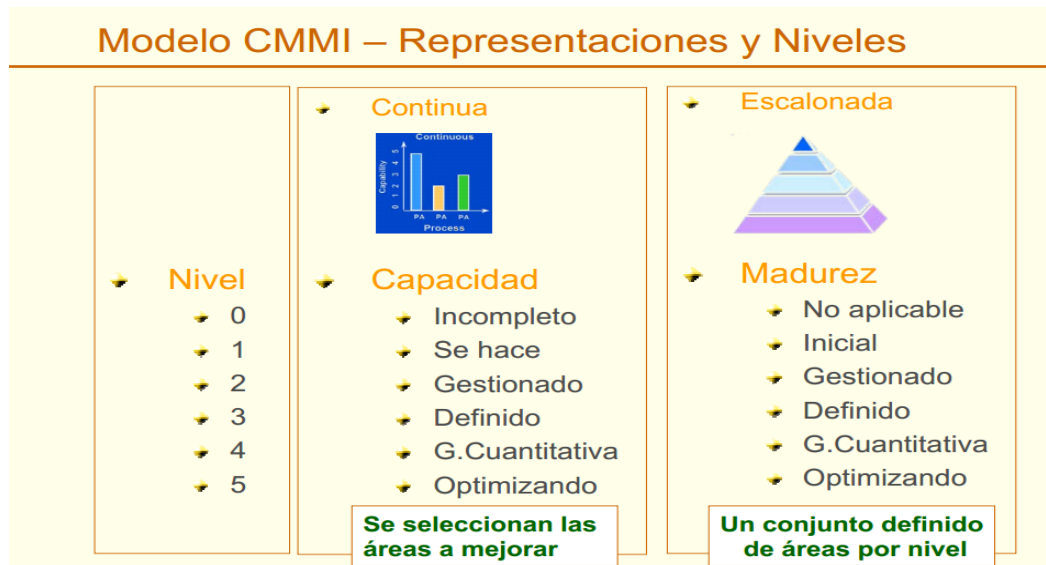


Figura 2.4. Niveles de Modelo de Madurez
Fuente: SEI_CMM Chacón 2004

2.5.2. RIESGO – CONFIANZA

En este contexto, las Entidades no pueden ser ajenas al tema de los riesgos y deben buscar cómo manejarlos partiendo de la base de su razón de ser y su compromiso con los clientes y partes interesadas; por esto se debe tener en cuenta que los riesgos no sólo son de carácter económico y están directamente relacionados con Entidades financieras o con lo que se ha denominado riesgos laborales, sino que hacen parte de cualquier gestión que se realice (Corral, 2009).

Política de Administración de Riesgos: Identifica las directrices para tratar y manejar los riesgos. Establece la posición de la dirección para la gestión de los riesgos y determina las acciones de control necesarias (Corral, 2009).

Mapa de Riesgos: Es una representación de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa. Incluye los controles y su seguimiento mediante las acciones determinadas y los responsables de las mismas (Corral, 2009).

La matriz Riesgo Confianza del Control Interno en Ecuador permite dar a conocer el impacto que tiene el riesgo en el departamento o entidad auditada. En el desarrollo metodológico de este trabajo se puede observar de qué

manera se puede realizar una Matriz Riesgo-Confianza y como determinar el nivel de riesgo en el cumplimiento de normas de control Interno e ISO 27000.

CÁPITULO III. DESARROLLO METODOLÓGICO

El trabajo de investigación realizado en el Departamento Tecnológico de la ESPAM MFL en la ciudad de Calceta, tuvo la duración de nueve meses. Para el inicio de la auditoría de control y mantenimiento de la infraestructura tecnológica del departamento tecnológico, fue necesario solicitar la autorización de inicio a la máxima autoridad, el Ing. Leonardo Félix López, Rector de la Escuela Superior Agropecuaria de Manabí “Manuel Félix López” ESPAM-MFL, por intermediación de la Ing. Jessica Morales Carillo, Directora de la Carrera Informática, la misma que puntualizaba el permiso para poder obtener la información necesaria para realizar la respectiva auditoría(**Anexo 1**).

Para el desarrollo del trabajo, las autoras utilizaron la metodología de auditoría basada en las aplicaciones de las buenas prácticas, estándares y normas de control Interno de la Contraloría General del Estado y la metodología de la Contraloría General del Estado Matriz Riesgo Confianza. Esta metodología de auditoría se dividió en cuatro fases: planificación, ejecución, análisis de los resultados y presentación de los resultados de la auditoría, mediante las cuales, las autoras llevaron a cabo la aplicación del trabajo.

A la vez con estas metodologías las autoras se permitieron incorporar el uso de la Norma Técnica ISO 27000 referente a Tecnología de la información (Técnicas de seguridad) y la Norma de Control Interno 410-09, relativo a Tecnología de Información (Control y Mantenimiento a la Infraestructura Tecnológica), la misma que está dirigida para las entidades y organismos del sector público del Ecuador, y que permitirá guiar a las autoras en el plan de auditoría.

3.1. ALCANCE

El alcance que tiene esta auditoría será sobre la evaluación del Control y Mantenimiento de la Infraestructura Tecnológica del Departamento Tecnológico y abarcará:

- Equipos de comunicación, equipos de computación e infraestructura de redes, Licenciamientos de software base.
- Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios son registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones son registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.
- Control y registro de las versiones del software que ingrese a producción.
- Se verificará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en la función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.
- Se verificará el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.
- El mantenimiento de los bienes que se encuentren en garantía.

3.2. RESTRICCIONES

- No abarcará al Departamento de Almacén en sus procesos y procedimientos adquisitivos, reposo y baja de recursos tecnológicos.
- Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y

normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.

- Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.
- Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementaran medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.

3.3. MÉTODO DE TRABAJO

3.3.1. FASE I. PLANIFICACIÓN DE LA AUDITORÍA

Cumpliendo con el método de trabajo, las autoras (las auditoras) establecieron relación directa con la entidad, para proceder a ejecutar la planificación estructurada del desarrollo de la investigación, inmediatamente realizaron el Plan de Auditoría para estar al corriente de la situación actual de la institución y así, las autoras lograron determinar el alcance y los objetivos tanto generales como específicos de la investigación.

Las autoras dividieron esta fase en dos subfases señaladas como planificación preliminar y planificación específica. En la planificación preliminar las autoras construyeron de manera formal la emisión de la orden de trabajo para llevar a cabo la investigación de campo dentro de la institución y así, adquirieron obtener toda la información relevante a la situación actual del Departamento Tecnológico que constituye a toda la universidad. En la planificación específica las autoras determinaron las diferentes estrategias a seguir para llevar a cabo el desarrollo de la auditoría mediante la aplicación de recursos métodos y técnicas.

Los diferentes resultados obtenidos se mostraran en el Capítulo de Resultados y Discusiones, se analizaran y se mostrarán con mayor detalle.

3.3.1.1. PLANIFICACIÓN PRELIMINAR

Una vez obtenido el permiso por parte del rector de la universidad ESPAM MFL, las auditoras(las autoras) procedieron a iniciar con los planes de auditoría, mediante la elaboración y aplicación de cuestionarios de observaciones iniciales a las personas que conforman el departamento tecnológico, los mismos que permitieron obtener una idea global de las actividades y operaciones, así como la identificación de procedimientos en el manejo de los recursos tecnológicos que se llevan a cabo en esta unidad.

Posteriormente de la recopilación de la información, a través de los cuestionarios de observación inicial, se realizó una matriz (**Anexo 13**) con las preguntas efectuadas y las personas encargadas con sus respectivas respuestas cada uno, esto permitió a las auditoras identificar datos, hechos e información relevante. Además de la obtención de la información también se evidenciaron los procedimientos del manejo y control de los equipos tecnológicos de la institución.

Una vez que se concluyó con la planificación preliminar, fue necesario elaborar el Memorando de Investigación Preliminar (**Anexo 17**), con el propósito de dar a conocer los resultados obtenidos en esta fase, dicho memorando está conformado por los antecedentes, el motivo de la auditoría, los objetivos de la auditoría, el alcance de la auditoría, conocimiento de la entidad, puntos de interés para la planificación específica y los componentes a ser examinados.

Explicando generalmente, esta etapa incluyó un análisis completo de todos los elementos internos y externos a la entidad, con la finalidad de determinar los eventos con la mayor relevancia para cumplir con la misión y objetivos estratégicos del Departamento Tecnológico.

3.3.1.2. PLANIFICACIÓN ESPECÍFICA

Los resultados obtenidos en la planificación preliminar fueron indispensables para definir los procedimientos a cumplir en la planificación específica, para lo cual, esta fase inicia con la realización del Programa Específico de Auditoría, el cual incluyó por cada componente en la fase de ejecución sus diferentes elementos los programas de auditoría.

Se aplicaron los diferentes cuestionarios a las personas que trabajan dentro del Departamento Tecnológico, la sucesión de las preguntas estuvieron realizadas en una matriz general (**Anexo 13**) con el fin de medir el nivel de cumplimiento de normas políticas y procedimientos dentro de las mismas y a su vez si el personal está informado de todo lo que rodea al Departamento Tecnológico.

Los procesos que se trabajaron en los diferentes cuestionarios están estructurados de la siguiente forma: poseen una ponderación de diez puntos para cada una de las preguntas y la calificación que las autoras le asignaron está basada dentro de un rango de puntuación (0 – 10), donde, 0 significa que dicho proceso no se cumple, 5 significa que el proceso se cumple en un 50% y 10 establece que los procedimientos se cumple en su totalidad, es decir en un 100%, dicho rango de puntuación está fundamentado en el criterio de las autoras de esta auditoría, en base a las respuestas y evidencias obtenidas por parte de cada uno de los entrevistados del Departamento Tecnológico.

Para dar sustento fiable a las diferentes afirmaciones las autoras solicitaron los diferentes documentos que debería tener el departamento tecnológico con respecto al control interno de la institución.

Una vez aplicados los cuestionarios de control interno, las autoras procedieron a realizar la matriz de determinación del riesgo – confianza por cada uno de los entrevistados en el Departamento Tecnológico, la misma que inicia con la siguiente fórmula definida en el Manual General de Auditoría.

$$CP = \frac{CT*100}{PT} \quad (3.1)$$

CP: Calificación Porcentual

PT: Ponderación Total

CT: Calificación Total

Para obtener la calificación porcentual (CP), se multiplicó la calificación total (CT) por 100 y se dividió para la ponderación total (PT).

La calificación porcentual, permitió identificar el grado de confianza y nivel de riesgo por cada componente examinado, asignando un tipo de color en cada nivel, de acuerdo a la siguiente tabla de calificación (Loor y Espinoza, 2014).

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES
15 – 50	BAJO	ALTO	ROJO
51 – 75	MODERADO	MODERADO	AMARILLO
76 - 95	ALTO	BAJO	VERDE

Cuadro 3.1. Determinación del Nivel de Confianza y del Riesgo

Este cuadro muestra la calificación porcentual, grado de confianza, nivel de riesgo y los diferentes colores con los cuales nos permite identificar cada rango. De 15% a 50% muestra un grado de confianza BAJO y un nivel de riesgo ALTO identificándose con el color ROJO; de 51% a 75% muestra un grado de confianza MODERADO y un nivel de riesgo ALTO identificándose con el color AMARILLO; de 76% a 95% un grado de confianza BAJO y un nivel de riesgo BAJO identificándose con el color verde.

3.3.2. FASE II. EJECUCIÓN DE LA AUDITORIA

La fase ejecución está ligada directamente a la fase de planificación ya que en la misma, las auditoras (las autoras) se familiarizaron con el entorno de la institución, recopilaron toda la información y además en ésta procedieron a aplicar todo lo realizado como lo son: los planes de trabajo, las planificaciones

tanto preliminar como específica, las mismas, que van a verificar directamente al Departamento Tecnológico.

El objetivo principal de aplicar el plan de trabajo y las planificaciones de la Auditoria fue determinar el nivel de cumplimiento y el nivel riesgo confianza que se maneja dentro del departamento tecnológico. Dentro de estas pruebas de cumplimiento por cada uno de los componentes evaluados se tuvo como objetivo comprobar, es decir que para dar respuesta a lo antepuesto, las autoras solicitaron mediante oficio (**Anexo 2**) toda la evidencia posible que se maneja el departamento.

El principal propósito de esta fase fue revisar, controlar, evaluar y comprobar los diferentes procesos que se llevaba en el área auditada, mediante la realización de cada una de las actividades plasmadas en las planificaciones tanto preliminares como específicas, para dar cumplimiento a los diferentes objetivos del control de la auditoria.

Las diferentes observaciones encontradas en la evaluación interna del departamento se registraron en hojas de resultados realizadas por las autoras y se analizaron de acuerdo a la norma de control interno nº 410-09 y la norma ISO 27000, con el fin de determinar si los procesos que se maneja dentro del Departamento Tecnológico ayudan a ofrecer un mejor servicio como departamento. Esto es, evaluar la confiabilidad de los controles utilizados para prevenir o detectar y corregir las causas de los riesgos y así mismo poder minimizarlos para que esto no llegue a efectuarse.

En la evaluación de una auditoria la evaluación del cumplimiento de las leyes y reglamentos es de fundamental importancia debido a que los organismos, programas, servicios, actividades y funciones se rigen generalmente por las leyes, ordenanzas, decretos y están sujetas a disposiciones legales y reglamentarias específicas.(Loor y Espinoza, 2014).

3.3.3. FASE III. ANÁLISIS DE LOS RESULTADOS

Una vez aplicado los planes de trabajo, las planificaciones tanto preliminar como específica y diferentes instrumentos y herramientas para obtener los diferentes resultados, se procedió a realizar los respectivos análisis de las evaluaciones tanto de la Norma de Control Interno como la Norma ISO 27000, permitiendo así tener un enfoque general del estado actual del departamento y finalmente hacer la respectiva comunicación de resultados que se mostrará en la siguiente fase.

3.3.4. FASE IV. COMUNICACIÓN DE RESULTADOS

Comunicación de resultados es la última fase de la Auditoria, la cual está directamente sujeta a las dos fases anteriores como lo son planificación ejecución y análisis de los resultados, en la misma se pudieron obtener los resultados pertinentes como lo es, el memorando de investigación preliminar (**Anexo 15**), el memorando de análisis inicial específico (**Anexo 19**) y el informe final de Auditoria (**Anexo 20**), para con ellos darse a conocer al Jefe del Departamento Tecnológico (**Anexo 21**) y este a su vez a la máxima autoridad quien es el rector(a) de ESPM MFL y a los demás interesados, las observaciones, conclusiones y recomendaciones sobre los riesgos encontrados mediante la evaluación de la Norma 410-09 que trata sobre el Control y Mantenimiento de la Infraestructura Tecnológica y la evaluación de la Norma ISO 27000.

Los memorandos tanto de investigación preliminar como de análisis inicial específico son documentos que describen procedimientos, archivos, relaciones de personal o factores de riesgo para la compañía y luego hacen sugerencias sobre cómo mejorar el área específica que está siendo auditada, es por este motivo que **MEMORANDO DE INVESTIGACIÓN PRELIMINAR** constan de: **1.** Antecedentes, **2.** Motivo de la Auditoria, **3.** Objetivo de la tesis, **4.** Alcance-Restricción de la Auditoria, **5.** Conocimiento de Entidad, **6.** Puntos de Interés de la Auditoria, **7.** Identificación de los componentes a ser examinados en la planificación específica. El **MEMORANDO DE ANÁLISIS INICIAL**

ESPECÍFICO consta de: **1.** Referencia de la Planificación Preliminar, **2.** Cuestionarios Iniciales, **3.** Resultado de la Evaluación del Control Interno, **4.** Evaluación y calificación de los riesgos de control interno, **5.** Resultado de las encuestas realizadas al personal administrativo y las diferentes carreras de la ESPAM MFL, **6.** Resultado de los testing realizado a cada una de las carreras de la ESPAM MFL, **7.** Resultado de la evaluación de la norma ISO 27000, **8.** Evaluación y calificación de los riesgos norma ISO 27000, **9.** Recursos a utilizarse.

El Informe final de Auditoria es un documento en el cual se muestran todos los resultados obtenidos en la Investigación, es decir es la realización de todo lo que se planeó en la Auditoria. Este Informe final consta de: Carta de Presentación, **Capítulo I** Información Introdutoria de la entidad, **Capítulo II** Resultado obtenidos en toda la investigación.

CÁPITULO IV. RESULTADOS Y DISCUSIÓN

En este capítulo las autoras detallan todo los resultados obtenidos que se plantearon en las diferentes fases del diseño metodológico de la Auditoria al control y mantenimiento de la infraestructura tecnológica del Departamento Tecnológico de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

En la planificación preliminar se realizó un proceso en el cual se inició con la emisión de la orden de trabajo, es decir, se elaboró una guía o también llamada **PLANIFICACIÓN PRELIMINAR (Anexo 9)** para la visita previa al Departamento Tecnológico y así las autoras lograran obtener información sobre la entidad a ser evaluada. Dentro la planificación específica se definió la estrategia a seguir en el trabajo de campo, realizando así los diferente cuestionarios y encuestas al Departamento Tecnológico para formarse una opinión de la situación actual del mismo y lograr evaluar el departamento teniendo incidencia en la eficiente utilización de los recursos métodos y técnicas para lograr así los objetivos generales y específicos que se plantearon en el **PLAN DE AUDITORIA (Anexo 8)**.

A continuación se muestran los resultados que las autoras obtuvieron al realizar los diferentes cuestionarios (documentación, hardware y software), aplicados al personal para poder constatar el nivel riesgo confianza y el nivel de concordancia de la información que se maneja dentro del Departamento Tecnológico.

4.1. IDENTIFICACIÓN DE LAS ÁREAS QUE CAREZCAN DE NORMATIVIDAD

4.1.1. ANÁLISIS DE RESULTADOS DEL CUMPLIMIENTO DE NORMAS EN EL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL

A continuación se muestran los resultados obtenidos mediante la aplicación de los cuestionarios de control interno y sus componentes son Documentación, Hardware y Software.

4.1.1.1. DOCUMENTACIÓN.

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza: CP: Calificación Porcentual PT: Ponderación Total CT: Calificación Total		$CP = \frac{CT * 100}{PT}$ $CP = \frac{170 * 100}{520}$ $CP = 32,69 \%$	
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES
15 – 50	BAJO	ALTO	ROJO
51 – 75	MODERADO	MODERADO	AMARILLO
76 - 95	ALTO	BAJO	VERDE
Nivel de confianza:		BAJO	32,69%
Nivel de riesgo:		ALTO	67,31%
<p>El cuestionario de control interno aplicado al Jefe del Departamento sobre la documentación que se maneja dentro del mismo está integrado por 52 preguntas, obtuvo la contestación de 24 respuestas positivas y 28 respuestas negativas; obteniendo la ponderación total de 520 puntos y la calificación total de 170 puntos, lo que representa una calificación porcentual del 32,69%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>			

Cuadro 4.1. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Jefe del Departamento Tecnológico

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual			
PT: Ponderación Total		$CP = \frac{155 * 100}{520}$	
CT: Calificación Total		$CP = 29,80 \%$	
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES
15 – 50	BAJO	ALTO	ROJO
51 – 75	MODERADO	MODERADO	AMARILLO
76 - 95	ALTO	BAJO	VERDE
Nivel de confianza:		BAJO	29,80%
Nivel de riesgo:		ALTO	70,20%
<p>El cuestionario de control interno aplicado al Analista de Computo 1 sobre la documentación que se maneja dentro del mismo está integrado por 52 preguntas, obtuvo la contestación de 17 respuestas positivas y 35 respuestas negativas; obteniendo la ponderación total de 520 puntos y la calificación total de 155 puntos, lo que representa una calificación porcentual del 29,80%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>			

Cuadro 4.2. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Analista de Computo

1

Elaborado por: Las autoras

En referencia al asistente de computo 1 y 2 las autoras intentaron realizarles las diferentes preguntas referente a la documentación que se llevaba o como se manejaba y obtuvieron como respuesta que no tenían idea sobre cómo se trabajaba internamente el departamento tecnológico.

4.1.1.2. HARDWARE

Consecutivamente las autoras procedieron a realizar las diferentes preguntas de **hardware** a los diferentes Asistentes de Cómputo y al Jefe del departamento tecnológico.

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual		$CP = \frac{160 * 100}{340}$	
PT: Ponderación Total		$CP = 47,06 \%$	
CT: Calificación Total			
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES
15 – 50	BAJO	ALTO	ROJO
51 – 75	MODERADO	MODERADO	AMARILLO
76 - 95	ALTO	BAJO	VERDE
Nivel de confianza:		BAJO	47,06%
Nivel de riesgo:		ALTO	52,94%
<p>El cuestionario de control interno aplicado al Jefe del Departamento sobre el Hardware que se maneja dentro del mismo está integrado por 34 preguntas, obtuvo la contestación de 22 respuestas positivas y 12 respuestas negativas; obteniendo la ponderación total de 340 puntos y la calificación total de 160 puntos, lo que representa una calificación porcentual del 47,06%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>			

Cuadro 4.3. Matriz de Riesgo – Confianza en el cumplimiento de normas de Contro Interno al Jefe del Departamento Tecnológico
Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA	
Determinación del riesgo confianza:	$CP = \frac{CT * 100}{PT}$
CP: Calificación Porcentual	$CP = \frac{165 * 100}{340}$
PT: Ponderación Total	$CP = 48,53 \%$
CT: Calificación Total	

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES	
15 – 50	BAJO	ALTO	ROJO	48,53%
51 – 75	MODERADO	MODERADO	AMARILLO	
76 - 95	ALTO	BAJO	VERDE	

Nivel de confianza:	BAJO	48,53%
Nivel de riesgo:	ALTO	51,47%

El cuestionario de control interno aplicado al Analista de Computo sobre el Hardware que se maneja dentro del mismo está integrado por 34 preguntas, obtuvo la contestación de 20 respuestas positivas y 14 respuestas negativas; obteniendo la ponderación total de 340 puntos y la calificación total de 165 puntos, lo que representa una calificación porcentual del 48,53%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.4. Matriz de Riesgo – Confianza en el cumplimiento de normas de Contro Interno al Asistente de Computo 2

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA				
Determinación del riesgo confianza:				
CP: Calificación Porcentual		$CP = \frac{CT * 100}{PT}$		
PT: Ponderación Total		$CP = \frac{160 * 100}{340}$		
CT: Calificación Total		$CP = 47,06 \%$		

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES	
15 – 50	BAJO	ALTO	ROJO	
51 – 75	MODERADO	MODERADO	AMARILLO	
76 - 95	ALTO	BAJO	VERDE	

Nivel de confianza:	BAJO	47,06%
Nivel de riesgo:	ALTO	52,94%

El cuestionario de control interno aplicado al Asistente de Computo 1 sobre el Hardware que se maneja dentro del mismo está integrado por 34 preguntas, obtuvo la contestación de 24 respuestas positivas y 10 respuestas negativas; obteniendo la ponderación total de 340 puntos y la calificación total de 165 puntos, lo que representa una calificación porcentual del 47,06%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.5. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Asistente de Computo 1

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA																	
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$															
CP: Calificación Porcentual PT: Ponderación Total CT: Calificación Total		$CP = \frac{85 * 100}{340}$															
		$CP = 25 \%$															
<table border="1"> <thead> <tr> <th>CALIFICACIÓN PORCENTUAL</th> <th>GRADO DE CONFIANZA</th> <th>NIVEL DE RIESGO</th> <th></th> </tr> </thead> <tbody> <tr> <td>15 – 50</td> <td>BAJO</td> <td>ALTO</td> <td rowspan="3">25%</td> </tr> <tr> <td>51 – 75</td> <td>MODERADO</td> <td>MODERADO</td> </tr> <tr> <td>76 - 95</td> <td>ALTO</td> <td>BAJO</td> </tr> </tbody> </table>				CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO		15 – 50	BAJO	ALTO	25%	51 – 75	MODERADO	MODERADO	76 - 95	ALTO	BAJO
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO															
15 – 50	BAJO	ALTO	25%														
51 – 75	MODERADO	MODERADO															
76 - 95	ALTO	BAJO															
Nivel de confianza:		BAJO	25%														
Nivel de riesgo:		ALTO	75%														
<p>El cuestionario de control interno aplicado al Asistente de Cómputo 2 sobre el Hardware que se maneja dentro del mismo está integrado por 34 preguntas, obtuvo la contestación de 10 respuestas positivas y 24 respuestas negativas; obteniendo la ponderación total de 340 puntos y la calificación total de 85 puntos, lo que representa una calificación porcentual del 25%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>																	

Cuadro 4.6. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Asistente de Computo 2

Elaborado por: Las autoras

4.1.1.3. SOFTWARE

Por último las autoras procedieron a realizar las diferentes preguntas de **software** a los diferentes Asistentes de Cómputo y al Jefe del departamento tecnológico

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza: CP: Calificación Porcentual PT: Ponderación Total CT: Calificación Total		$CP = \frac{CT * 100}{PT}$ $CP = \frac{55 * 100}{110}$ $CP = 50 \%$	
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES
15 – 50	BAJO	ALTO	ROJO
51 – 75	MODERADO	MODERADO	AMARILLO
76 - 95	ALTO	BAJO	VERDE
Nivel de confianza:		BAJO	50%
Nivel de riesgo:		ALTO	50%
<p>El cuestionario de control interno aplicado al Jefe del Departamento sobre el Software que se maneja dentro del mismo está integrado por 11 preguntas, obtuvo la contestación de 8 respuestas positivas y 3 respuestas negativas; obteniendo la ponderación total de 110 puntos y la calificación total de 55 puntos, lo que representa una calificación porcentual del 50%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>			

Cuadro 4.7. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Jefe del Departamento Tecnológico

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual		$CP = \frac{50 * 100}{110}$	
PT: Ponderación Total			
CT: Calificación Total		$CP = 45,45 \%$	
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES
15 – 50	BAJO	ALTO	ROJO
51 – 75	MODERADO	MODERADO	AMARILLO
76 - 95	ALTO	BAJO	VERDE
Nivel de confianza:	BAJO	45,45%	
Nivel de riesgo:	ALTO	54,55%	
<p>El cuestionario de control interno aplicado al Analista de Computo sobre el Software que se maneja dentro del mismo está integrado por 11 preguntas, obtuvo la contestación de 8 respuestas positivas y 3 respuestas negativas; obteniendo la ponderación total de 110 puntos y la calificación total de 50 puntos, lo que representa una calificación porcentual del 45,45%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>			

Cuadro 4.8. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Analista de Computo
Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA	
Determinación del riesgo confianza:	$CP = \frac{CT * 100}{PT}$
CP: Calificación Porcentual	$CP = \frac{60 * 100}{110}$
PT: Ponderación Total	
CT: Calificación Total	$CP = 54,55 \%$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES
15 – 50	BAJO	ALTO	ROJO
51 – 75	MODERADO	MODERADO	AMARILLO
76 - 95	ALTO	BAJO	VERDE

Nivel de confianza:	MODERADO	54,55%
Nivel de riesgo:	MODERADO	45,45%

El cuestionario de control interno aplicado al Asistente de Computo 1 sobre el Software que se maneja dentro del mismo está integrado por 11 preguntas, obtuvo la contestación de 7 respuestas positivas y 4 respuestas negativas; obteniendo la ponderación total de 110 puntos y la calificación total de 60 puntos, lo que representa una calificación porcentual del 54,55%, determinando un nivel de riesgo moderado y a su vez el grado de confianza moderado.

Cuadro 4.9. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Asistente de Computo 1

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual PT: Ponderación Total CT: Calificación Total		$CP = \frac{25 * 100}{110}$	
		$CP = 22,73 \%$	
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	22,73%
15 – 50	BAJO	ALTO	
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	
Nivel de confianza:	BAJO	22,73%	
Nivel de riesgo:	ALTO	77,27%	

El cuestionario de control interno aplicado al Asistente de Cómputo 2 sobre el Software que se maneja dentro del mismo está integrado por 11 preguntas, obtuvo la contestación de 4 respuestas positivas y 7 respuestas negativas; obteniendo la ponderación total de 110 puntos y la calificación total de 25 puntos, lo que representa una calificación porcentual del 22,73%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.10. Matriz de Riesgo – Confianza en el cumplimiento de normas de Control Interno al Asistente de Computo 2

Elaborado por: Las autoras

Como las autoras pudieron observar el Departamento Tecnológico de la Escuela Superior Politécnica Agropecuaria de Manabí ESPAM MFL, no cuenta con la información necesaria sobre cómo se debe manejar internamente, es decir que los diferentes asistentes y Jefe del departamento no tienen una asignación de trabajo específica, todos hacen todo y con respecto a si conocen de cómo se maneja internamente en lo legal el departamento no están al corriente de como se lo hace o como se lo lleva.

Otra de las observaciones es que al momento de hacer los diferentes cuestionarios habían temas en los cuales los asistentes e incluso el jefe estaba desinformado de cómo se llevaba ese control es por eso que el nivel de riesgo es extremadamente alto.

4.2. RESULTADOS PORCENTUALES DE LA EVALUACIÓN DE LA NORMA DE CONTROL INTERNO

4.2.1. MATRIZ RIESGO CONFIANZA GENERAL

MATRIZ RIESGO-CONFIANZA CONTROL INTERNO					
TEMA	JEFE DEL DEPARTAMENTO	ANALISTA COMPUTO	ASISTENTE COMPUTO 1	ASISTENTE COMPUTO 2	RIESGO PROMEDIO DEL DEPARTAMENTO TECNOLÓGICO
	RIESGO	RIESGO	RIESGO	RIESGO	
CONTROL INTERNO	56,75%	58,74%	66,13%	84,09%	66,43%
DOCUMENTACIÓN	67,31%	70,20%	100%	100%	84,38%
HARDWARE	52,94%	51,47%	52,94%	75%	58,09%
SOFTWARE	50%	54,55%	45,45%	77,27%	56,82%

Cuadro 4.11. Matriz general porcentual del nivel de Riesgo-Confianza Control Interno

Fuente: Checklist de Control Interno

4.2.2. GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO POR INDIVIDUO Y COMPONENTE NORMA CONTROL INTERNO

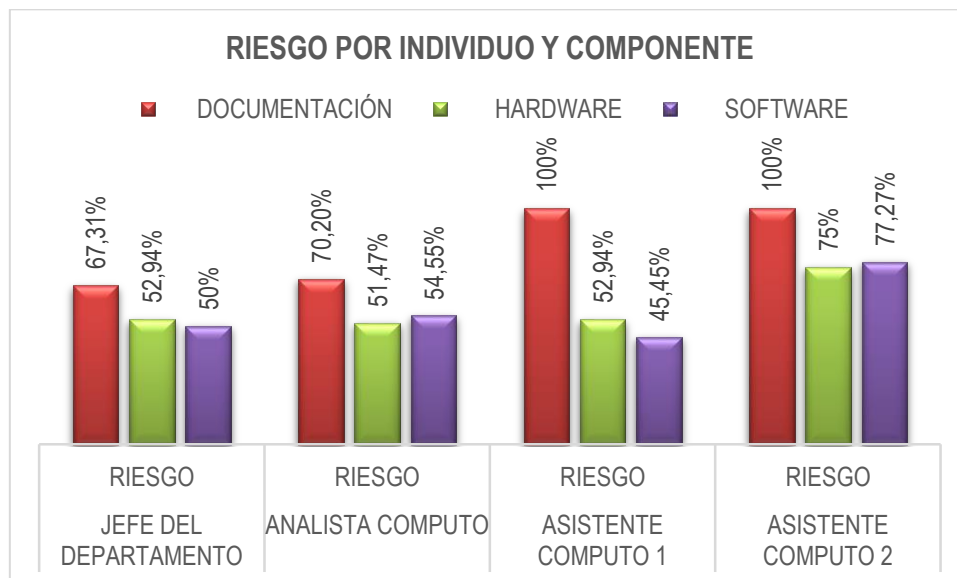


Gráfico 4.1. Grafico Representativo general porcentual del nivel de Riesgo-Confianza por individuo y componente Norma Control Interno.

Fuente: Cuestionarios de Control Interno

4.2.3. GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO DEL DEPARTAMENTO POR COMPONENTE NORMA CONTROL INTERNO

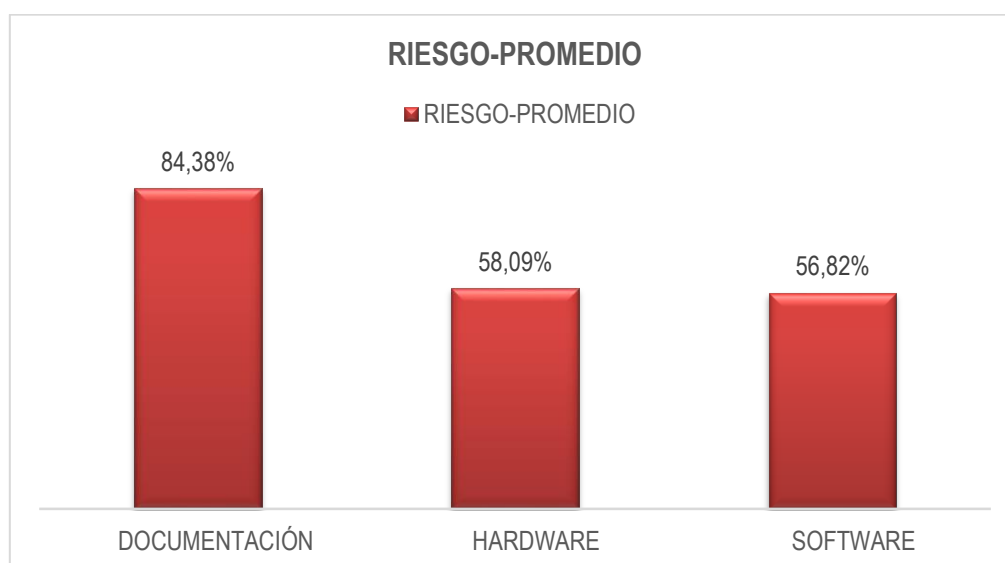


Gráfico 4.2. Grafico Representativo general porcentual del nivel de Riesgo-Confianza del Departamento Tecnológico por Componente Control Interno

Fuente: Cuestionarios de Control Interno

4.2.4. GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO-CONFIANZA POR INDIVIDUO CONTROL INTERNO

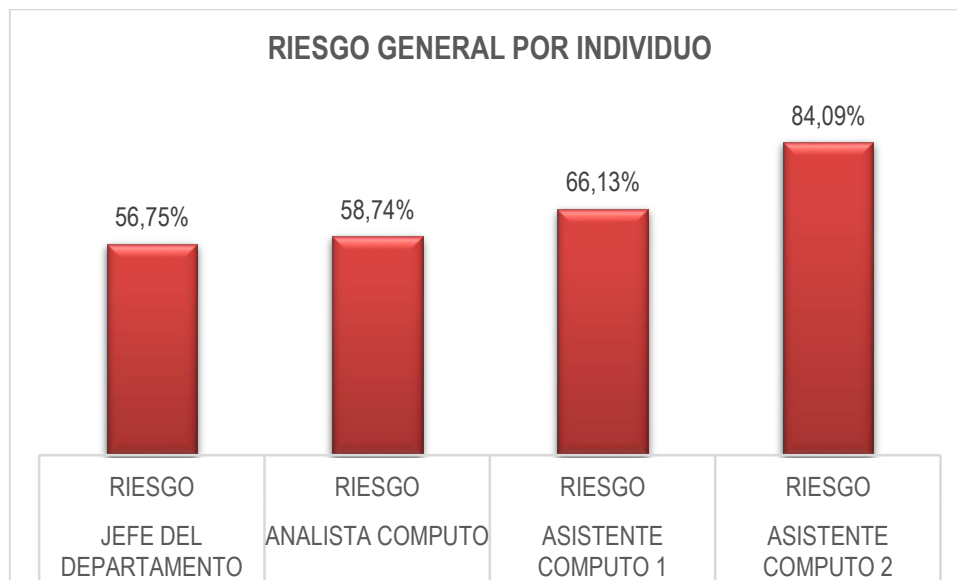


Gráfico 4.3. Grafico Representativo general porcentual del nivel de Riesgo-Confianza por individuo

Fuente: Cuestionarios de Control Interno

4.2.5. GRAFICO REPRESENTATIVO DEL PROMEDIO GENERAL PORCENTUAL DEL NIVEL DE RIESGO-CONFIANZA DEL DEPARTAMENTO NORMA CONTROL INTERNO

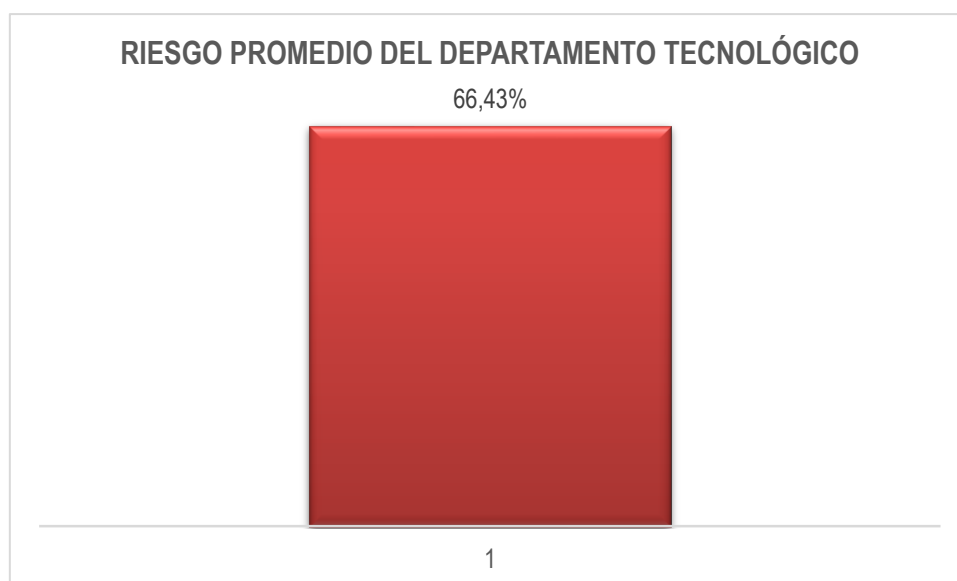


Gráfico 4.4. Grafico Representativo del promedio general porcentual del nivel de Riesgo-Confianza del Departamento Norma Control Interno

Fuente: Cuestionarios de Control Interno

4.3. DESCRIPCIÓN DE LOS GRÁFICOS

Dentro de los porcentajes de la matriz riesgo confianza se observa que el Departamento Tecnológico en la evaluación de las normas de Control Interno dio como resultado: sobre el componente Documentación el Jefe del Departamento tiene un nivel de riesgo de 67,31%, el Analista de Computo tiene un nivel de riesgo de 70,20%, el Asistente de Computo 1 tiene un nivel de riesgo de 100,00%, el Asistente de Computo 2 tiene un nivel de riesgo de 100,00% , y el riesgo promedio es de 84,38%; sobre el componente de Hardware el Jefe del Departamento tiene un nivel de riesgo es de 52,94%, el Analista de Computo tiene un nivel de riesgo es de 51,47%, el Asistente de Computo 1 tiene un nivel de riesgo es de 52,94%, el Analista de Computo 2 tiene un nivel riesgo es de 75,00%, y el riesgo promedio es de 58,09%; sobre el componente de Software el Jefe del Departamento tiene un nivel de riesgo es de 50%, el Analista de Computo tiene un nivel de riesgo de 54,55%, el Asistente de Computo 1 tiene un nivel de riesgo de 45,45%, el Asistente de Computo 2 tiene un nivel de riesgo es de 77,27%, y el riesgo promedio es de 56,82%.

De manera general el departamento tecnológico cuenta con unos porcentajes de nivel de riesgo por colaborador y por departamento como tal, el Jefe del Departamento tiene un nivel de riesgo de 56,75%, el Analista de Computo tiene un nivel de riesgo de 58,74%, el Asistente de Computo 1 tiene un nivel de riesgo de 66,13%, el Asistente de Computo 2 tiene un nivel de riesgo es de 84,09%. El riesgo promedio por departamento mediante la norma de control interno es de 66,43%.

Es así, que se evidencia que el componente con mayor nivel de riesgo es Documentación con un porcentaje de 84,38% y el componente con menor nivel de riesgo es Software con un porcentaje de 56,82%.

4.4. ANÁLISIS DE LOS RIESGOS SEGÚN NORMA DE CONTROL INTERNO

En base a los resultados obtenidos en la evaluación de riesgos según la Norma de Control Interno en Tecnologías de Información 410-09, referente al control y mantenimiento de la infraestructura tecnológica, el departamento tecnológico fue evaluado mediante los componentes de Documentación, Hardware y Software.

Para obtener la siguiente tabla, se evaluó a cada uno de las personas que laboran dentro del departamento tecnológico, donde dio como resultado un promedio de riesgo por individuo /componente y el riesgo promedio general del departamento, mostrado en la siguiente tabla:

COMPONENTES	RIESGOS
Documentación	84,38%
Hardware	58,09%
Software	56,82%
PROMEDIO RIESGO GENERAL DEL DEPARTAMENTO	66,43%

Tabla 4.1: Promedio Riesgo General Control Interno del departamento tecnológico

Fuente: Norma de Control Interno 410-09

Elaborado por: Las autoras

Se observa así, que el componente de Documentación, muestra un riesgo promedio de 84,38%, el componente de hardware un riesgo promedio de 58,09% y el componente de software un riesgo promedio de 56,82%, debido a que no se llevan a cabo en su totalidad los procedimientos, procesos, sistemas y acuerdos de servicios que serán registrados, evaluados y autorizados de forma previa a su implantación; la falta de bitácoras para su respectiva documentación; la inexistente actualización de todo tipo de manuales técnicos, planes estratégicos y planes operativos para la unidad tecnológica; la insuficiencia de mecanismos lógicos y físicos de seguridad para proteger los recursos tecnológicos; todo esto bajo la exigencia de la Norma de Control

Interno de tecnologías de información 410-09 referente al control y mantenimiento de la infraestructura tecnológica y el incumplimiento de los productos y servicios a entregar que lo dispone el registro oficial tecnológico de la ESPAM MFL.

4.5. ANÁLISIS DE RESULTADOS DE LAS TABULACIONES DE LAS ENCUESTAS REALIZADAS AL PERSONAL ADMINISTRATIVO Y LAS DIFERENTES CARRERAS DE LA ESPAM MFL.

Para la evaluación de las encuestas realizadas al personal que labora en la institución se solicitó al Departamento de Almacén el inventario en donde constaban todos los equipos tecnológicos de dicha institución, tomando como referencia los dos últimos años (2012-2013) para las evaluaciones pertinentes.

Se tomaron en cuenta las dos áreas de la institución:

En el Área Agroindustrial en donde se encuentra ubicado Rectorado, Vicerrectorado, Biblioteca, Talleres Agroindustriales, las carreras de Medio Ambiente, Agroindustrias, Turismo, Informática, y todas las áreas administrativas de esta área.

En el Área Agropecuaria en donde se encuentra ubicado la incubadora, las carreras de Agrícola, Pecuaria y Administración y todas las áreas administrativas de esta área.

A continuación, se muestran las preguntas realizadas en la encuesta elaborada para evaluar al departamento.

PREGUNTA 1. ¿CUANTOS EQUIPOS TECNOLÓGICOS TIENE A SU CARGO?

OPCIONES DE RESPUESTA	Nº DE EQUIPOS	%
Computadoras	210	54%
Impresoras	77	20%

UPS	52	13%
Otros	51	13%
TOTAL	390	100%

Tabla 4.2: Resultado de la encuesta realizadas al personal que labora en la institución **PREGUNTA 1**
Fuente: Custodios de Equipos Tecnológicos

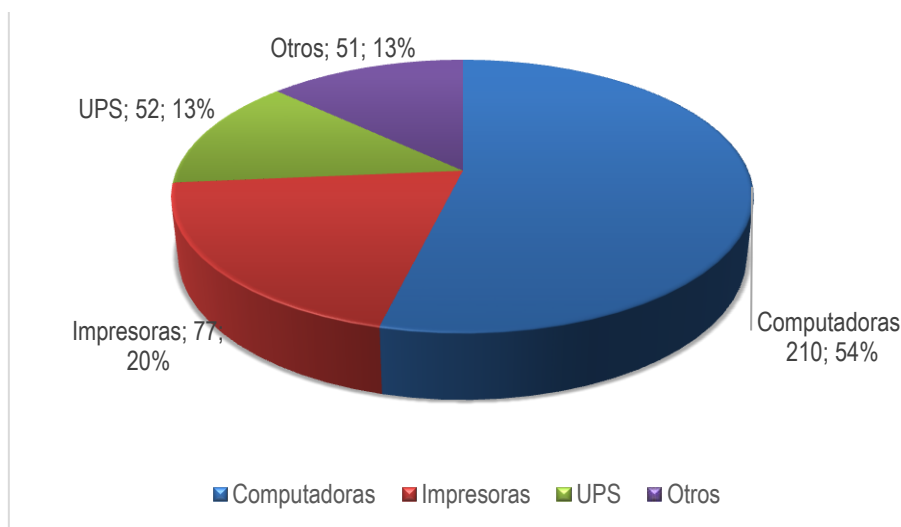


Gráfico 4.7. Equipos Tecnológicos a cargo de custodios
Fuente: Custodios de Equipos Tecnológicos

En las diferentes áreas administrativas y las diferentes carreras de la ESPAM MFL de las cincuenta y un (51) encuestas realizadas a los custodios de la institución, se obtuvieron como resultado que existen; 210 computadoras incluidas de escritorios y portátiles que constituye a un 54%, 77 Impresoras que constituyen a un 20%, 52 UPS que constituyen a un 13% y 51 en otros equipos que constituyen a un 13%, dando como resultado 390 equipos tecnológicos que equivale a un 100%.

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
SI	36	71%
NO	15	29%

PREGUNTA REALIZADO	2.	TOTAL	51	100%	¿LES HAN	MANTENIMIENTO PREVENTIVO A SUS EQUIPOS TECNOLÓGICOS?
---------------------------	-----------	--------------	-----------	-------------	-----------------	---

Tabla 4.3: Resultado de la encuesta realizadas al personal que labora en la institución **PREGUNTA 2**
Fuente: Custodios de Equipos Tecnológicos

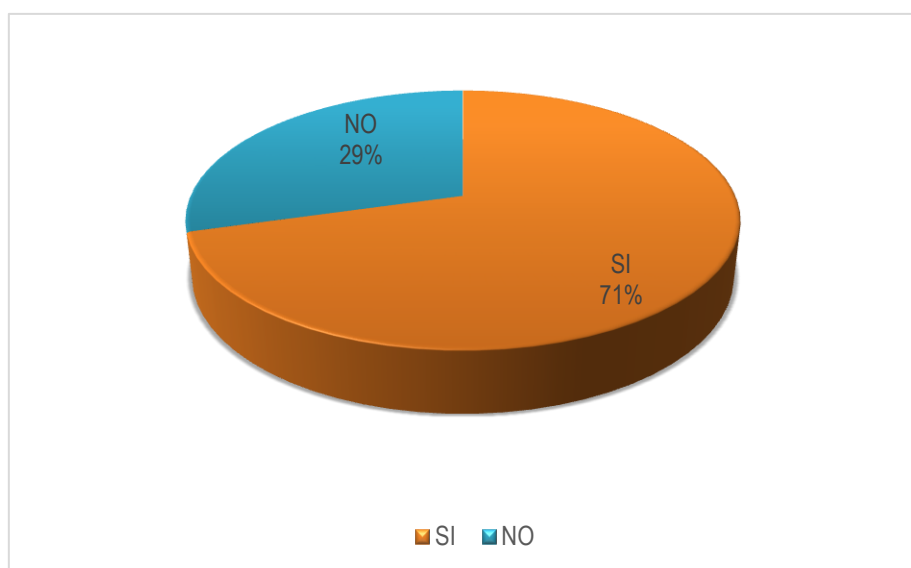


Gráfico 4.8. Mantenimiento Preventivo a Equipos Tecnológicos
Fuente: Custodios de Equipos Tecnológicos

En las diferentes áreas administrativas y las diferentes carreras de la ESPAM MFL de las cincuenta y un (51) encuestas realizadas a los custodios de la institución, se obtuvieron como resultado que; 36 custodios dieron como respuestas que **SI** les realizaban mantenimientos preventivos y constituye a un 71%, mientras que los otros 15 dieron como respuesta que **NO** se les realizaba mantenimientos a los equipos tecnológicos que tienen a su cargo con un porcentaje de 29%, dando como resultado un total de 51 respuestas que equivale a un 100%.

EN CASO DE QUE LA RESPUESTA SEA SI CADA QUE TIEMPO SE LO REALIZA:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
SEMANTAL	0	0%
TRIMESTRAL	16	45%
SEMESTRAL	13	36%
ANUAL	7	19%
TOTAL	36	100%

Tabla 4.4: Resultado de la encuesta realizadas al personal que labora en la institución **PREGUNTA 2**
Fuente: Custodios de Equipos Tecnológicos

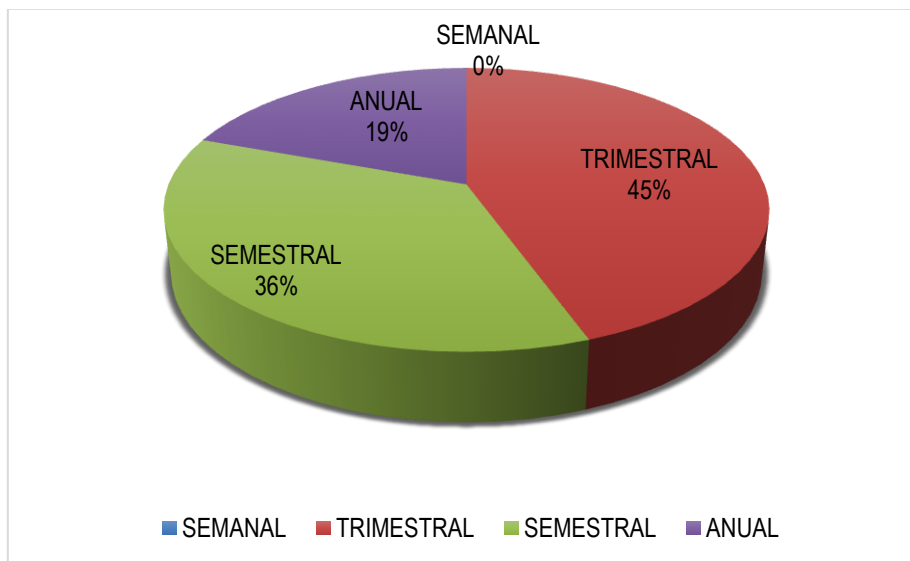


Gráfico 4.9. Tiempo de Mantenimiento Preventivo a Equipos Tecnológicos
Fuente: Custodios de Equipos Tecnológicos

EL TIEMPO EN QUE TARDA EL MANTENIMIENTO ES:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
MUCHO TIEMPO	4	11%
POCO TIEMPO	23	64%
LO ESPERADO PARA CONTINUAR ACTIVIDADES	9	25%
TOTAL	36	100%

Tabla 4.5: Resultado de la encuesta realizadas al personal que labora en la institución **PREGUNTA 2**

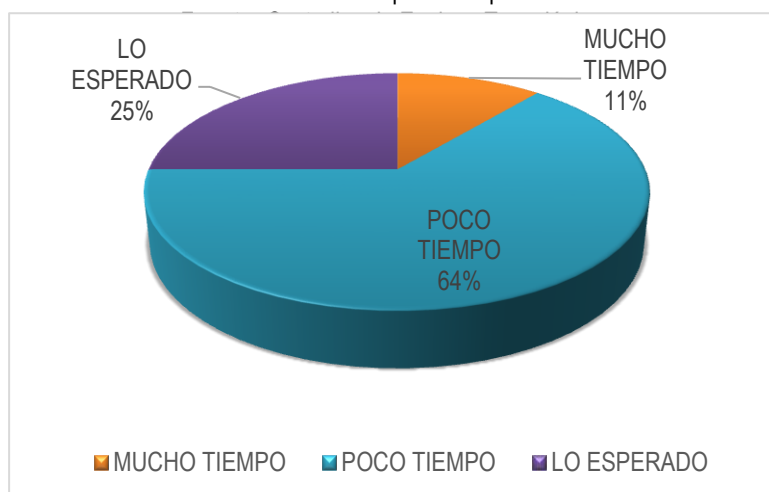


Gráfico 4.10. Tiempo de tardanza en el Mantenimiento Preventivo a Equipos Tecnológicos

Fuente: Custodios de Equipos Tecnológicos

EN CASO DE QUE LA RESPUESTA SEA NO:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
NUNCA	2	13%
CASI NUNCA	13	87%
TOTAL	15	100%

Tabla 4.6: Resultado de la encuesta realizadas al personal que labora en la institución **PREGUNTA 2**

Fuente: Custodios de Equipos Tecnológicos

**Gráfico 4.11.** Negativa a la realización del Mantenimiento Preventivo de los Equipos Tecnológicos

Fuente: Custodios de Equipos Tecnológicos

Como se puede observar mediante esta segunda pregunta las autoras de esta auditoria obtuvieron como resultado que el 71% de los encuestados corresponden al total de 36 encuestados, que son custodios de los equipos tecnológicos, y según los resultados SI les dan mantenimiento preventivo a los equipos; el tiempo que se lo realiza corresponde al 45% TRIMESTRAL, 36% SEMESTRAL y el 19% ANUAL; el tiempo en que tarda el mantenimiento corresponde al 11 % MUCHO TIEMPO, 64% POCO TIEMPO y 25% LO ESPERADO PARA CONTINUAR LAS ACTIVIDADES, mientras que el 29% de los encuestados que corresponden al total de 15 encuestados de los custodios

dicen que NO les dan mantenimiento preventivo a sus equipos, NUNCA el 13% y CASI NUNCA el 87%.

PREGUNTA 3. ¿LES HAN REALIZADO MANTENIMIENTO CORRECTIVO A SUS EQUIPOS TECNOLÓGICOS?

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
SI	42	82%
NO	9	18%
TOTAL	51	100%

Tabla 4.7: Resultado de la encuesta realizadas al personal que labora en la institución **PREGUNTA 3**
Fuente: Custodios de Equipos Tecnológicos

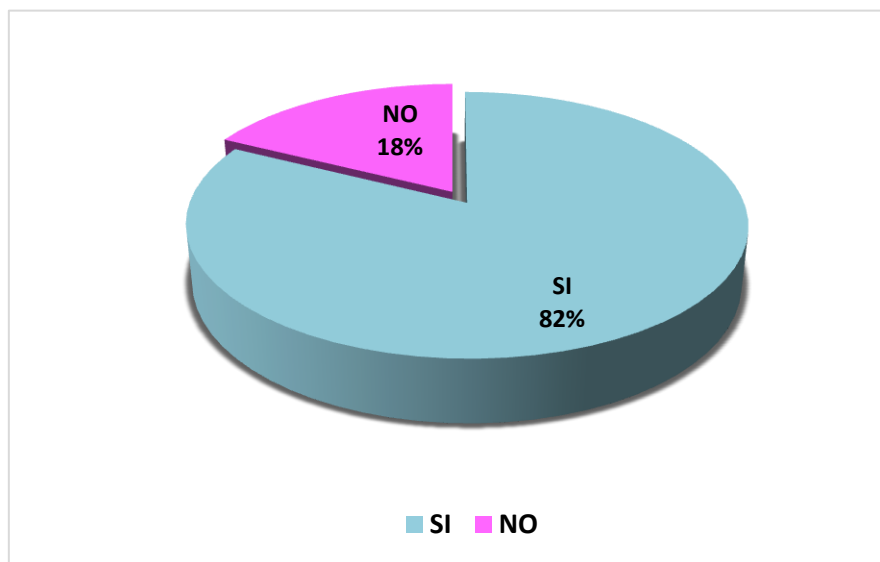


Gráfico 4.12. Mantenimiento Correctivo a Equipos Tecnológicos
Fuente: Custodios de Equipos Tecnológicos

En las diferentes áreas administrativas y las diferentes carreras de la ESPAM MFL de las cincuenta y un (51) encuestas realizadas a los custodios de la institución, se obtuvieron como resultado que; 42 custodios dieron como respuestas que **SI** les realizaban mantenimientos preventivos y constituye a un 82%, mientras que los otros 9 dieron como respuesta que **NO** se les realizaba mantenimientos a los equipos tecnológicos que tienen a su cargo, dando como resultado un 18%.

EN CASO DE QUE LA RESPUESTA SEA SI CADA QUE TIEMPO SE LO REALIZA:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
EN EL MISMO MOMENTO	14	33%
AL DÍA SIGUIENTE	9	22%
AL MES	1	2%
CUANDO EL TÉCNICO LO DISPONGA	18	43%
TOTAL	42	100%

Tabla 4.8: Resultado de la encuesta realizadas al personal que labora en la institución **PREGUNTA 3**
Fuente: Custodios de Equipos Tecnológicos

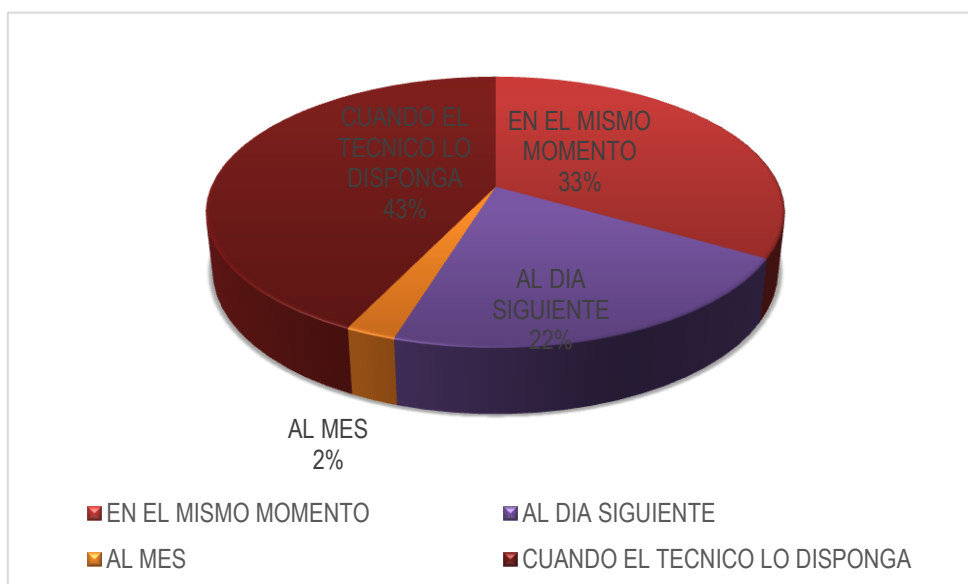


Gráfico 4.13. Tiempo de Mantenimiento Correctivo a Equipos Tecnológicos
Fuente: Custodios de Equipos Tecnológicos

EN CASO DE QUE LA RESPUESTA SEA NO:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
NUNCA	3	43%
CASI NUNCA	0	0%
CUANDO EL EQUIPO LO REQUIERA	6	57%
TOTAL	7	100%

Tabla 4.9: Resultado de la encuesta realizadas al personal que labora en la institución **PREGUNTA 3**
Fuente: Custodios de Equipos Tecnológicos

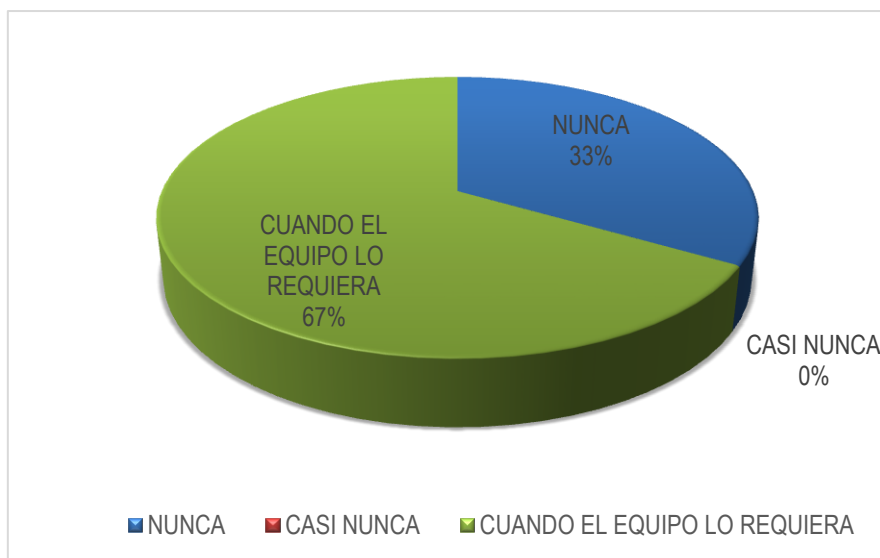


Gráfico 4.14. Negativa a la realización del Mantenimiento Correctivo de los Equipos Tecnológicos
Fuente: Custodios de Equipos Tecnológicos

Como se puede observar mediante esta tercera pregunta las autoras de esta auditoria obtuvieron como resultado que el 83% de los encuestados corresponden a el total de 40 encuestados, que son custodios de los equipos tecnológicos, y según los resultados SI les hacen mantenimiento correctivo a los equipos; el tiempo en que se lo realizan corresponde al 45% CUANDO EL TÉCNICO LO DISPONGA, un 32% EN EL MISMO MOMENTO, un 23% AL DÍA SIGUIENTE y un 0% al MES, mientras que el 17% correspondiente al total de 8 encuestados de los custodios NO les hacen mantenimiento correctivo a sus equipos, solamente cuando el equipo lo disponga que es el 50% y el 50% NUNCA.

PREGUNTA 4. ¿CÓMO SE REALIZA LA SOLICITUD DE MANTENIMIENTOS SEA PREVENTIVO O CORRECTIVO?

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
POR LLAMADA TELEFÓNICA	32	63%
POR CORREO ELECTRÓNICO	0	0%
POR OFICIO	14	27%

OTRO MEDIO	5	10%
TOTAL	51	100%

Tabla 4.10: Resultado de la encuesta realizadas al personal que labora en la institución **PREGUNTA 4**
Fuente: Custodios de Equipos Tecnológicos

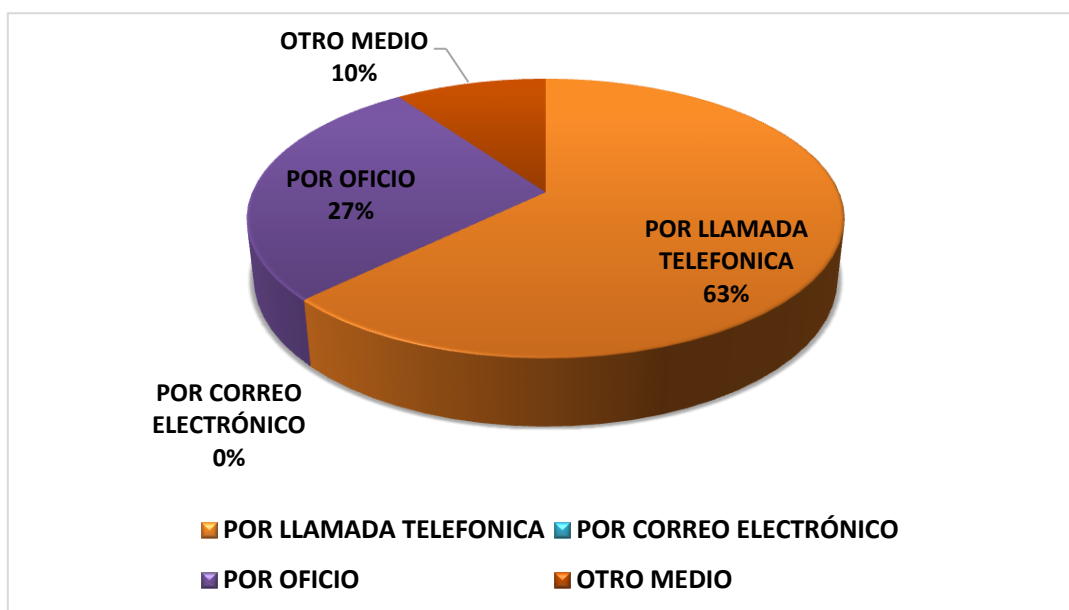


Gráfico 4.15. Solicitud de Mantenimiento Preventivo o Correctivo
Fuente: Custodios de Equipos Tecnológicos

Como resultado en esta pregunta se obtuvo que del total de 51 encuestados corresponden al 63% de los custodios de los equipos tecnológicos hacen la solicitud del mantenimiento ya sea preventivo o correctivo por medio de LLAMADA TELEFÓNICA, mientras el 27% corresponde POR OFICIO y un 10% lo hace POR OTRO MEDIO.

4.6. ANÁLISIS DE RESULTADOS DEL CUMPLIMIENTO DE LA NORMA ISO 27000 EN EL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL

A continuación se muestran los resultados obtenidos mediante la aplicación de los cuestionarios de la Norma ISO 27000 y sus componentes son Inventario de Activos, Seguridad de los Recursos Humanos, Seguridad Física del Entorno, Gestión de Comunicación y Operación, Control de Acceso, Cumplimiento.

4.6.1. INVENTARIO DE ACTIVO SEGÚN LA NORMA ISO 27000

MATRIZ DE RIESGO - CONFIANZA															
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$													
CP: Calificación Porcentual		$CP = \frac{30 * 100}{70}$													
PT: Ponderación Total		$CP = 42,86 \%$													
CT: Calificación Total															
<table border="1"> <thead> <tr> <th>CALIFICACIÓN PORCENTUAL</th> <th>GRADO DE CONFIANZA</th> <th>NIVEL DE RIESGO</th> </tr> </thead> <tbody> <tr> <td>15 – 50</td> <td>BAJO</td> <td>ALTO</td> </tr> <tr> <td>51 – 75</td> <td>MODERADO</td> <td>MODERADO</td> </tr> <tr> <td>76 - 95</td> <td>ALTO</td> <td>BAJO</td> </tr> </tbody> </table>			CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	15 – 50	BAJO	ALTO	51 – 75	MODERADO	MODERADO	76 - 95	ALTO	BAJO	42,86%
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO													
15 – 50	BAJO	ALTO													
51 – 75	MODERADO	MODERADO													
76 - 95	ALTO	BAJO													
Nivel de confianza:	BAJO	42,86%													
Nivel de riesgo:	ALTO	57,14%													
<p>El cuestionario de control interno aplicado al Jefe del Departamento sobre el Inventario de Activos según Norma ISO 27000 que se maneja dentro del mismo está integrado por 7 preguntas, obtuvo la contestación de 4 respuestas positivas y 3 respuestas negativas; obteniendo la ponderación total de 70 puntos y la calificación total de 30 puntos, lo que representa una calificación porcentual del 42,86%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>															

Cuadro 4.12. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual		$CP = \frac{0 * 100}{70}$	
PT: Ponderación Total		$CP = 0 \%$	
CT: Calificación Total			
0%			
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	
Nivel de confianza:		BAJO	0%
Nivel de riesgo:		ALTO	100 %
<p>El cuestionario de control interno aplicado al Asistente de Cómputo 1 sobre el Inventario de Activos según Norma ISO 27000 que se maneja dentro del mismo está integrado por 7 preguntas, obtuvo la contestación de 0 respuestas positivas y 7 respuestas negativas; obteniendo la ponderación total de 70 puntos y la calificación total de 0 puntos, lo que representa una calificación porcentual del 0%, determinando un nivel de riesgo alto al 100% y a su vez el grado de confianza 0 que está fuera de rango.</p>			

Cuadro 4.14. Matriz de Riesgo – Confianza en el cumplimiento de la norma ISO 27000 al Asistente de Computo 1

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA	
Determinación del riesgo confianza:	$CP = \frac{CT * 100}{PT}$
CP: Calificación Porcentual	$CP = \frac{10 * 100}{70}$
PT: Ponderación Total	$CP = 14,28 \%$
CT: Calificación Total	

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	14,28%
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	

Nivel de confianza:	BAJO	14,28%
Nivel de riesgo:	ALTO	85,71%

El cuestionario de control interno aplicado al Asistente de Cómputo 2 sobre el Inventario de Activos según Norma ISO 27000 que se maneja dentro del mismo está integrado por 7 preguntas, obtuvo la contestación de 2 respuestas positivas y 5 respuestas negativas; obteniendo la ponderación total de 70 puntos y la calificación total de 10 puntos, lo que representa una calificación porcentual del 14,28%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo que está fuera de rango.

Cuadro 4.15. Matriz de Riesgo – Confianza en el cumplimiento de la norma ISO 27000 al Asistente de Computo 2
Elaborado por: Las autoras

4.6.2. SEGURIDAD DE LOS RECURSOS HUMANOS SEGÚN LA NORMA ISO 27000

Consecutivamente las autoras procedieron a realizar las diferentes preguntas de **SEGURIDAD DE LOS RECURSOS HUMANOS SEGÚN LA NORMA ISO 27000** a los diferentes Asistentes de Cómputo y al Jefe del departamento tecnológico.

MATRIZ DE RIESGO - CONFIANZA	
Determinación del riesgo confianza:	$CP = \frac{CT * 100}{PT}$
CP: Calificación Porcentual PT: Ponderación Total CT: Calificación Total	$CP = \frac{55 * 100}{90}$
	$CP = 61,11 \%$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	
51 – 75	MODERADO	MODERADO	61,11%
76 - 95	ALTO	BAJO	

Nivel de confianza:	MODERADO	61,11%
Nivel de riesgo:	MODERADO	38,89%

El cuestionario de control interno aplicado al Jefe del Departamento sobre la Seguridad de Recursos Humanos según Norma ISO 27000 que se maneja dentro del mismo está integrado por 9 preguntas, obtuvo la contestación de 7 respuestas positivas y 2 respuestas negativas; obteniendo la ponderación total de 90 puntos y la calificación total de 55 puntos, lo que representa una calificación porcentual del 61,11%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.16. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual		$CP = \frac{40 * 100}{90}$	
PT: Ponderación Total		$CP = 44,44 \%$	
CT: Calificación Total			

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	44,44%
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	

Nivel de confianza:	BAJO	44,44%
Nivel de riesgo:	ALTO	55,56%

El cuestionario de control interno aplicado al Analista de Computo la Seguridad de Recursos Humanos según Norma ISO 27000 que se maneja dentro del mismo está integrado por 9 preguntas, obtuvo la contestación de 5 respuestas positivas y 4 respuestas negativas; obteniendo la ponderación total de 90 puntos y la calificación total de 40 puntos, lo que representa una calificación porcentual del 44,44%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.17. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Analista de Computo
Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual		$CP = \frac{35 * 100}{90}$	
PT: Ponderación Total		$CP = 38,89 \%$	
CT: Calificación Total			
38,89%			
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	
Nivel de confianza:	BAJO	38,89%	
Nivel de riesgo:	ALTO	61,11%	
El cuestionario de control interno aplicado al Asistente de Cómputo 1 sobre la Seguridad de Recursos Humanos según Norma ISO 27000 que se maneja dentro del mismo está integrado por 9 preguntas, obtuvo la contestación de 4 respuestas positivas y 5 respuestas negativas; obteniendo la ponderación total de 90 puntos y la calificación total de 35 puntos, lo que representa una calificación porcentual del 38,39%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.			

Cuadro 4.18. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 1
Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA																
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$														
CP: Calificación Porcentual		$CP = \frac{45 * 100}{90}$														
PT: Ponderación Total																
CT: Calificación Total		$CP = 50 \%$														
<table border="1"> <thead> <tr> <th>CALIFICACIÓN PORCENTUAL</th> <th>GRADO DE CONFIANZA</th> <th>NIVEL DE RIESGO</th> <th rowspan="4">50%</th> </tr> </thead> <tbody> <tr> <td>15 – 50</td> <td>BAJO</td> <td>ALTO</td> </tr> <tr> <td>51 – 75</td> <td>MODERADO</td> <td>MODERADO</td> </tr> <tr> <td>76 - 95</td> <td>ALTO</td> <td>BAJO</td> </tr> </tbody> </table>				CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	50%	15 – 50	BAJO	ALTO	51 – 75	MODERADO	MODERADO	76 - 95	ALTO	BAJO
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	50%													
15 – 50	BAJO	ALTO														
51 – 75	MODERADO	MODERADO														
76 - 95	ALTO	BAJO														
Nivel de confianza:		BAJO	50%													
Nivel de riesgo:		ALTO	50%													
<p>El cuestionario de control interno aplicado al Asistente de Cómputo 2 sobre la Seguridad de los Recursos Humanos según Norma ISO 27000 que se maneja dentro del mismo está integrado por 9 preguntas, obtuvo la contestación de 5 respuestas positivas y 4 respuestas negativas; obteniendo la ponderación total de 90 puntos y la calificación total de 45 puntos, lo que representa una calificación porcentual del 50%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>																

Cuadro 4.19. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 2

Elaborado por: Las autoras

4.6.3. SEGURIDAD FÍSICA DEL ENTORNO SEGÚN LA NORMA ISO 27000

Inmediatamente las autoras procedieron a realizar las diferentes preguntas de **SEGURIDAD FÍSICA DEL ENTORNO SEGÚN LA NORMA ISO 27000** a los diferentes Asistentes de Cómputo y al Jefe del departamento tecnológico

MATRIZ DE RIESGO - CONFIANZA														
Determinación del riesgo confianza: CP: Calificación Porcentual PT: Ponderación Total CT: Calificación Total		$CP = \frac{CT * 100}{PT}$ $CP = \frac{130 * 100}{300}$ $CP = 43,33 \%$												
<table border="1"> <thead> <tr> <th>CALIFICACIÓN PORCENTUAL</th> <th>GRADO DE CONFIANZA</th> <th>NIVEL DE RIESGO</th> </tr> </thead> <tbody> <tr> <td>15 – 50</td> <td>BAJO</td> <td>ALTO</td> </tr> <tr> <td>51 – 75</td> <td>MODERADO</td> <td>MODERADO</td> </tr> <tr> <td>76 - 95</td> <td>ALTO</td> <td>BAJO</td> </tr> </tbody> </table>	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	15 – 50	BAJO	ALTO	51 – 75	MODERADO	MODERADO	76 - 95	ALTO	BAJO		
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO												
15 – 50	BAJO	ALTO												
51 – 75	MODERADO	MODERADO												
76 - 95	ALTO	BAJO												
Nivel de confianza:	<table border="1"> <tr> <td>BAJO</td> <td>43,33%</td> </tr> </table>	BAJO	43,33%											
BAJO	43,33%													
Nivel de riesgo:	<table border="1"> <tr> <td>ALTO</td> <td>56,67%</td> </tr> </table>	ALTO	56,67%											
ALTO	56,67%													
<p>El cuestionario de control interno aplicado al Jefe del Departamento sobre la Seguridad Física del Entorno según Norma ISO 27000 que se maneja dentro del mismo está integrado por 30 preguntas, obtuvo la contestación de 22 respuestas positivas y 8 respuestas negativas; obteniendo la ponderación total de 300 puntos y la calificación total de 130 puntos, lo que representa una calificación porcentual del 43,33%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>														

Cuadro 4.20. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA	
Determinación del riesgo confianza: CP: Calificación Porcentual PT: Ponderación Total CT: Calificación Total	$CP = \frac{CT * 100}{PT}$ $CP = \frac{100 * 100}{300}$ $CP = 33,33 \%$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	33,33%
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	

Nivel de confianza:	BAJO	33,33%
Nivel de riesgo:	ALTO	66,67%

El cuestionario de control interno aplicado al Analista de Computo la Seguridad Física del Entorno según Norma ISO 27000 que se maneja dentro del mismo está integrado por 30 preguntas, obtuvo la contestación de 16 respuestas positivas y 14 respuestas negativas; obteniendo la ponderación total de 300 puntos y la calificación total de 100 puntos, lo que representa una calificación porcentual del 33,33%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.21. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Analista de Computo
Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:	$CP = \frac{CT * 100}{PT}$		
CP: Calificación Porcentual			
PT: Ponderación Total	$CP = \frac{135 * 100}{300}$		
CT: Calificación Total	$CP = 45 \%$		

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	45%
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	

Nivel de confianza:	BAJO	45%
Nivel de riesgo:	ALTO	55%

El cuestionario de control interno aplicado al Asistente de Cómputo 1 el sobre la Seguridad Física del Entorno según Norma ISO 27000 que se maneja dentro del mismo está integrado por 30 preguntas, obtuvo la contestación de 27 respuestas positivas y 3 respuestas negativas; obteniendo la ponderación total de 300 puntos y la calificación total de 135 puntos, lo que representa una calificación porcentual del 45%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.22. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 1
Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA														
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$												
CP: Calificación Porcentual														
PT: Ponderación Total		$CP = \frac{140 * 100}{300}$												
CT: Calificación Total		$CP = 46,67 \%$												
<table border="1"> <thead> <tr> <th>CALIFICACIÓN PORCENTUAL</th> <th>GRADO DE CONFIANZA</th> <th>NIVEL DE RIESGO</th> </tr> </thead> <tbody> <tr> <td>15 – 50</td> <td>BAJO</td> <td>ALTO</td> </tr> <tr> <td>51 – 75</td> <td>MODERADO</td> <td>MODERADO</td> </tr> <tr> <td>76 - 95</td> <td>ALTO</td> <td>BAJO</td> </tr> </tbody> </table>		CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	15 – 50	BAJO	ALTO	51 – 75	MODERADO	MODERADO	76 - 95	ALTO	BAJO	46,67%
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO												
15 – 50	BAJO	ALTO												
51 – 75	MODERADO	MODERADO												
76 - 95	ALTO	BAJO												
Nivel de confianza:	BAJO	46,67%												
Nivel de riesgo:	ALTO	53,33%												
<p>El cuestionario de control interno aplicado al Asistente de Cómputo 2 sobre la Seguridad Física del Entorno según Norma ISO 27000 que se maneja dentro del mismo está integrado por 30 preguntas, obtuvo la contestación de 18 respuestas positivas y 12 respuestas negativas; obteniendo la ponderación total de 300 puntos y la calificación total de 140 puntos, lo que representa una calificación porcentual del 46,67%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>														

Cuadro 4.23. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 2
Elaborado por: Las autoras

4.6.4. GESTIÓN DE COMUNICACIÓN Y DE OPERACIÓN SEGÚN LA NORMA ISO

Seguidamente las autoras procedieron a realizar las diferentes preguntas de **GESTIÓN DE COMUNICACIÓN Y DE OPERACIÓN SEGÚN LA NORMA ISO**

27000 a los diferentes Asistentes de Cómputo y al Jefe del departamento tecnológico

MATRIZ DE RIESGO - CONFIANZA															
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$													
CP: Calificación Porcentual		$CP = \frac{115 * 100}{170}$													
PT: Ponderación Total															
CT: Calificación Total		$CP = 67,65 \%$													
<table border="1"> <thead> <tr> <th>CALIFICACIÓN PORCENTUAL</th> <th>GRADO DE CONFIANZA</th> <th>NIVEL DE RIESGO</th> </tr> </thead> <tbody> <tr> <td>15 – 50</td> <td>BAJO</td> <td>ALTO</td> </tr> <tr> <td>51 – 75</td> <td>MODERADO</td> <td>MODERADO</td> </tr> <tr> <td>76 - 95</td> <td>ALTO</td> <td>BAJO</td> </tr> </tbody> </table>			CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	15 – 50	BAJO	ALTO	51 – 75	MODERADO	MODERADO	76 - 95	ALTO	BAJO	67,65%
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO													
15 – 50	BAJO	ALTO													
51 – 75	MODERADO	MODERADO													
76 - 95	ALTO	BAJO													
Nivel de confianza:	MODERADO	67,65%													
Nivel de riesgo:	MODERADO	32,35%													
<p>El cuestionario de control interno aplicado al Jefe del Departamento sobre la Gestión de Comunicación y Operación según Norma ISO 27000 que se maneja dentro del mismo está integrado por 17 preguntas, obtuvo la contestación de 13 respuestas positivas y 4 respuestas negativas; obteniendo la ponderación total de 170 puntos y la calificación total de 115 puntos, lo que representa una calificación porcentual del 67,65%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>															

Cuadro 4.24. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA	
Determinación del riesgo confianza:	$CP = \frac{CT * 100}{PT}$
CP: Calificación Porcentual	$CP = \frac{60 * 100}{170}$
PT: Ponderación Total	
CT: Calificación Total	$CP = 35,29 \%$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	35,29%
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	

Nivel de confianza:	BAJO	35,29%
Nivel de riesgo:	ALTO	64,71%

El cuestionario de control interno aplicado al Analista de Computo Zambrano la Gestión de Comunicación y Operación según Norma ISO 27000 que se maneja dentro del mismo está integrado por 17 preguntas, obtuvo la contestación de 7 respuestas positivas y 10 respuestas negativas; obteniendo la ponderación total de 170 puntos y la calificación total de 60 puntos, lo que representa una calificación porcentual del 35,29%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.25. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Analista de Computo
Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual		$CP = \frac{90 * 100}{170}$	
PT: Ponderación Total			
CT: Calificación Total		$CP = 52,94 \%$	

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	52,94%
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	

Nivel de confianza:	MODERADO	52,94%
Nivel de riesgo:	MODERADO	47,06%

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual		$CP = \frac{25 * 100}{60}$	
PT: Ponderación Total			
CT: Calificación Total		$CP = 41,67 \%$	
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	41,67%
15 – 50	BAJO	ALTO	
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	
Nivel de confianza:	BAJO	41,67%	
Nivel de riesgo:	ALTO	58,33%	
<p>El cuestionario de control interno aplicado al Jefe del Departamento sobre el Control de Acceso según Norma ISO 27000 que se maneja dentro del mismo está integrado por 6 preguntas, obtuvo la contestación de 5 respuestas positivas y 1 respuestas negativas; obteniendo la ponderación total de 60 puntos y la calificación total de 25 puntos, lo que representa una calificación porcentual del 41,67%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>			

Cuadro 4.28. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico

Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA	
Determinación del riesgo confianza:	$CP = \frac{CT * 100}{PT}$
CP: Calificación Porcentual	$CP = \frac{20 * 100}{60}$
PT: Ponderación Total	
CT: Calificación Total	$CP = 33,33 \%$

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	33,33%
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	

Nivel de confianza:	BAJO	33,33%
Nivel de riesgo:	ALTO	66,67%

El cuestionario de control interno aplicado al Analista de Computo sobre el Control de Acceso según Norma ISO 27000 que se maneja dentro del mismo está integrado por 6 preguntas, obtuvo la contestación de 2 respuestas positivas y 4 respuestas negativas; obteniendo la ponderación total de 60 puntos y la calificación total de 20 puntos, lo que representa una calificación porcentual del 33,33%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.29. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Analista de Computo
Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual		$CP = \frac{10 * 100}{60}$	
PT: Ponderación Total		$CP = 16,67 \%$	
CT: Calificación Total			

CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	
15 – 50	BAJO	ALTO	16,67%
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	

Nivel de confianza:	BAJO	16,67%
Nivel de riesgo:	ALTO	83,33%

El cuestionario de control interno aplicado al Asistente de Cómputo 1 sobre el Control de Acceso según Norma ISO 27000 que se maneja dentro del mismo está integrado por 6 preguntas, obtuvo la contestación de 2 respuestas positivas y 4 respuestas negativas; obteniendo la ponderación total de 60 puntos y la calificación total de 10 puntos, lo que representa una calificación porcentual del 16,67%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.

Cuadro 4.30. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 1
Elaborado por: Las autoras

MATRIZ DE RIESGO - CONFIANZA															
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$													
CP: Calificación Porcentual		$CP = \frac{15 * 100}{60}$													
PT: Ponderación Total		$CP = 25 \%$													
CT: Calificación Total															
<table border="1"> <thead> <tr> <th>CALIFICACIÓN PORCENTUAL</th> <th>GRADO DE CONFIANZA</th> <th>NIVEL DE RIESGO</th> </tr> </thead> <tbody> <tr> <td>15 – 50</td> <td>BAJO</td> <td>ALTO</td> </tr> <tr> <td>51 – 75</td> <td>MODERADO</td> <td>MODERADO</td> </tr> <tr> <td>76 - 95</td> <td>ALTO</td> <td>BAJO</td> </tr> </tbody> </table>			CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	15 – 50	BAJO	ALTO	51 – 75	MODERADO	MODERADO	76 - 95	ALTO	BAJO	25%
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO													
15 – 50	BAJO	ALTO													
51 – 75	MODERADO	MODERADO													
76 - 95	ALTO	BAJO													
Nivel de confianza:	BAJO	25%													
Nivel de riesgo:	ALTO	75%													
<p>El cuestionario de control interno aplicado al Asistente de Cómputo 2 sobre el Control de Acceso según Norma ISO 27000 que se maneja dentro del mismo está integrado por 6 preguntas, obtuvo la contestación de 4 respuestas positivas y 2 respuestas negativas; obteniendo la ponderación total de 60 puntos y la calificación total de 15 puntos, lo que representa una calificación porcentual del 25%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>															

Cuadro 4.31. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Asistente de Computo 2
Elaborado por: Las autoras

4.6.6. CUMPLIMIENTO SEGÚN LA NORMA ISO 27000

Por último las autoras procedieron a realizar las diferentes preguntas de **CUMPLIMIENTO SEGÚN LA NORMA ISO 27000** a los diferentes Asistentes de Cómputo y al Jefe del departamento tecnológico

MATRIZ DE RIESGO - CONFIANZA			
Determinación del riesgo confianza:		$CP = \frac{CT * 100}{PT}$	
CP: Calificación Porcentual		$CP = \frac{10 * 100}{20}$	
PT: Ponderación Total		$CP = 50 \%$	
CT: Calificación Total			
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	50%
15 – 50	BAJO	ALTO	
51 – 75	MODERADO	MODERADO	
76 - 95	ALTO	BAJO	
Nivel de confianza:	BAJO	50%	
Nivel de riesgo:	ALTO	50%	
<p>El cuestionario de control interno aplicado al Jefe del Departamento sobre el Cumplimiento según Norma ISO 27000 que se maneja dentro del mismo está integrado por 2 preguntas, obtuvo la contestación de 1 respuestas positivas y 1 respuestas negativas; obteniendo la ponderación total de 20 puntos y la calificación total de 10 puntos, lo que representa una calificación porcentual del 50%, determinando un nivel de riesgo alto y a su vez el grado de confianza bajo.</p>			

Cuadro 4.32. Matriz de Riesgo – Confianza en el cumplimiento de norma ISO 27000 al Jefe del Departamento Tecnológico

Elaborado por: Las autoras

En referencia al Analista de Cómputo y los Asistentes de Cómputo 1 y 2 las autoras le realizaron las diferentes preguntas referente al CUMPLIMIENTO SEGÚN LA NORMA ISO 27000 que se llevaba o como se manejaba y obtuvieron como respuesta un porcentaje que se encuentra fuera de los rangos de la tabla de la Contraloría General del Estado, es decir que no tenían conocimiento sobre el cumplimiento de todas las normas legales Ecuatorianas.

4.7. RESULTADOS PORCENTUALES DE LA EVALUACIÓN DE LA NORMA ISO 27000

4.7.1. MATRIZ RIESGO CONFIANZA GENERAL NORMA ISO 27000

MATRIZ CONFIANZA-RIESGO NORMA ISO 27000					
TEMA	JEFE DEL DEPARTAMENTO	ANALISTA DE COMPUTO	ASISTENTE DE COMPUTO 1	ASISTENTE DE COMPUTO 2	RIESGO PROMEDIO DEL DEPARTAMENTO TECNOLÓGICO
	RIESGO	RIESGO	RIESGO	RIESGO	
NORMA ISO 27000	48,90%	70,84%	74,42%	67,54%	65,42%
INVENTARIO DE ACTIVOS	57,14%	71,43%	100%	85,71%	78,57%
SEGURIDAD DE LOS RECURSOS HUMANOS	38,89%	55,56%	61,11%	50%	51,39%
SEGURIDAD FÍSICA DEL ENTORNO	56,67%	66,67%	55%	53,33%	57,92%
GESTIÓN DE COMUNICACIÓN Y OPERACIÓN	32,35%	64,71%	47,06%	41,18%	46,33%
CONTROL DE ACCESO	58,33%	66,67%	83,33%	75%	70,83%
CUMPLIMIENTO	50%	100%	100%	100%	87,50%

Cuadro 4.33. Matriz general porcentual del nivel de Riesgo-Confianza

Fuente: Checklist de Control Interno

4.7.2. GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO NORMA ISO 27000

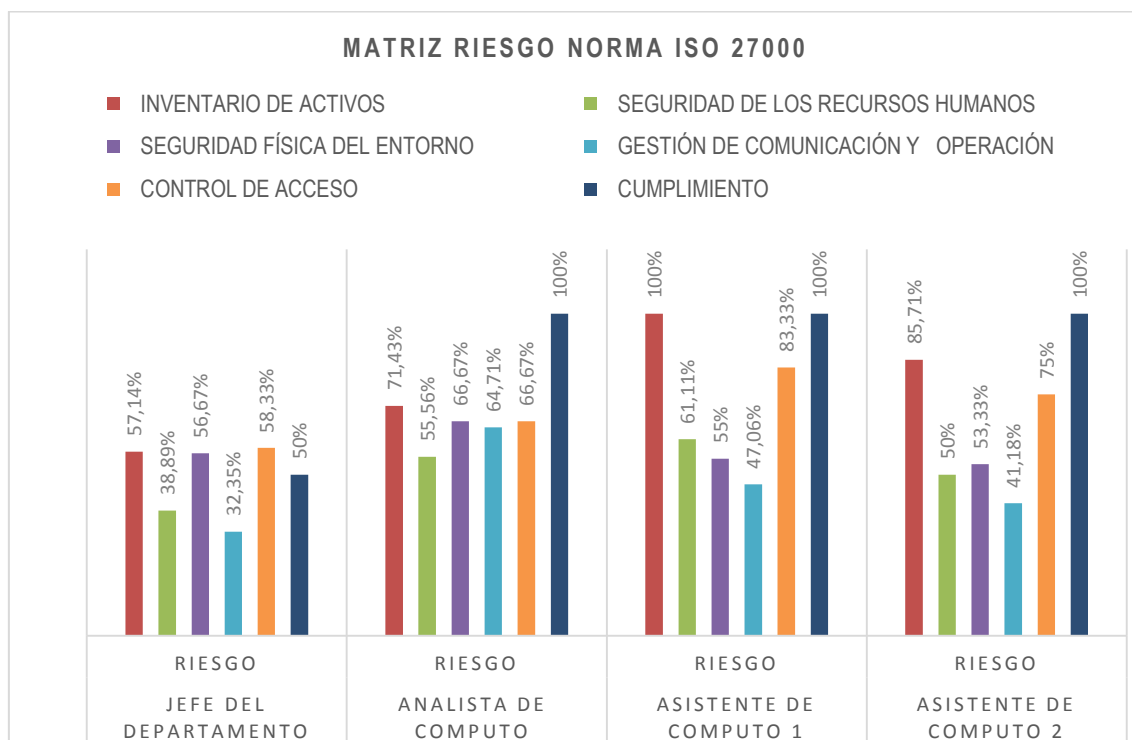


Gráfico 4.16. Gráfico Representativo general porcentual del nivel de Riesgo-Confianza por individuo Norma ISO 27000

Fuente: Cuestionarios de Control Interno

4.7.3. GRAFICO REPRESENTATIVO GENERAL PORCENTUAL DEL NIVEL DE RIESGO NORMA ISO 27000 POR COMPONENTE

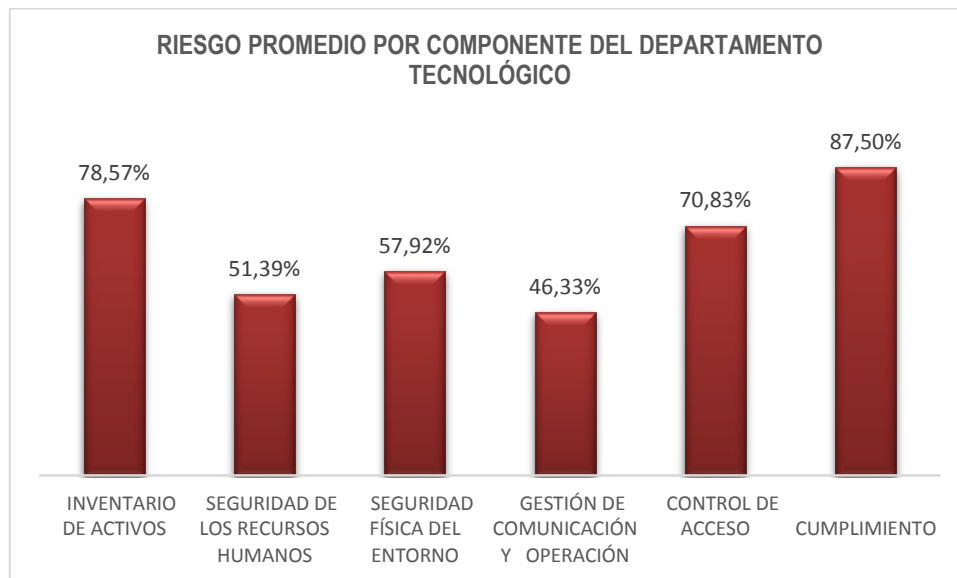


Gráfico 4.17. Grafico Representativo general porcentual del nivel de Riesgo-Confianza por Componente
Fuente: Cuestionarios de Control Interno

4.7.4. GRAFICO REPRESENTATIVO DEL PROMEDIO GENERAL PORCENTUAL DEL NIVEL DE RIESGO POR INDIVIDUO NORMA ISO 27000

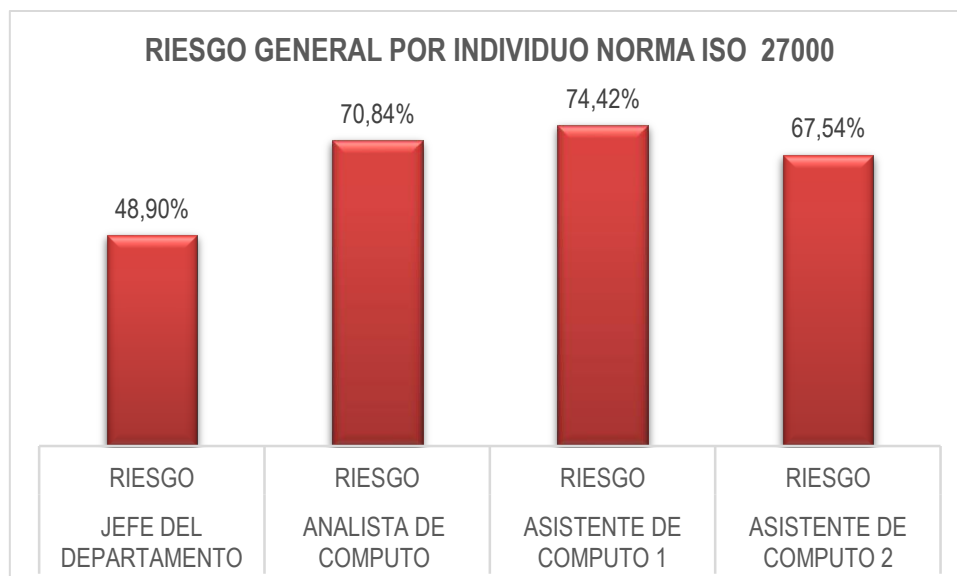


Gráfico 4.18. Grafico Representativo del promedio general porcentual del nivel de Riesgo-Confianza por Individuo Norma ISO 27000
Fuente: Cuestionarios de Control Interno

4.7.5. GRAFICO REPRESENTATIVO DEL PROMEDIO GENERAL PORCENTUAL DEL NIVEL DE RIESGO DEL DEPARTAMENTO NORMA ISO 27000

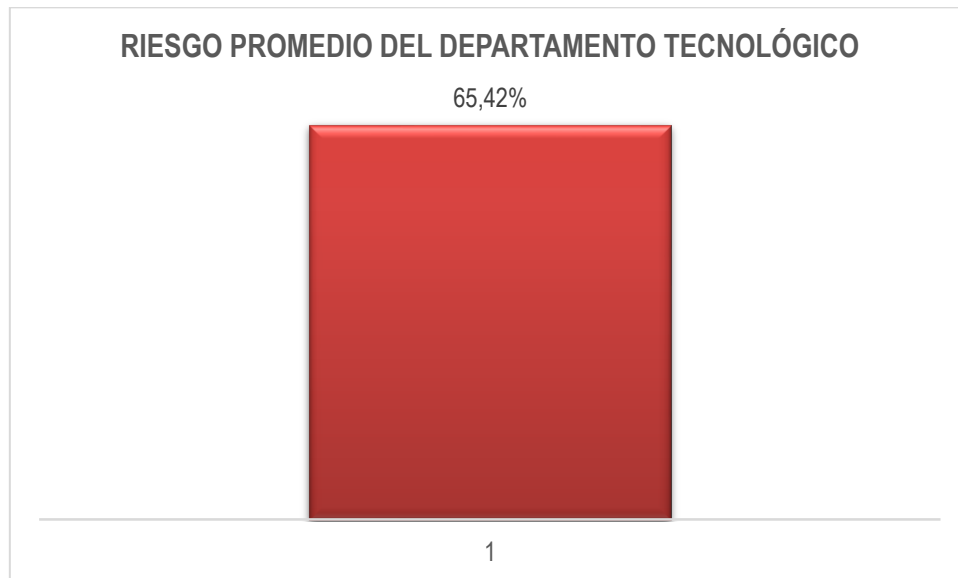


Gráfico 4.19. Grafico Representativo del promedio general porcentual del nivel de Riesgo-Confianza del Departamento Norma ISO 27000
Fuente: Cuestionarios de Control Interno

4.8. DESCRIPCIÓN DE LOS GRÁFICOS

Dentro de los porcentajes de la matriz riesgo confianza se observa que el Departamento dentro la evaluación de la norma ISO 27000 dio como resultado: sobre el componente Inventario de Activos del Jefe del Departamento tiene un nivel de riesgo de 57,14%, el Analista de Computo tiene un nivel riesgo es de 71,43%, el Asistente de Computo 1 tiene un nivel de riesgo es de 100,00% , el Asistente de Computo 2 tiene un nivel de riesgo es de 85,71% , y el nivel de riesgo promedio del departamento es de 78,57%; sobre el componente Seguridad de los Recursos Humanos el Jefe de Computo tiene un nivel de riesgo de 38,89%, el Analista de Computo tiene un nivel de riesgo de 55,56%, el Asistente de Computo 1 tiene un nivel de riesgo de 61,11%, el Analista de Computo 2 tiene un nivel de riesgo es de 50%, y el riesgo promedio del departamento es de 51,39%; sobre el componente Seguridad Física del Entorno el Jefe de Computo tiene un nivel de riesgo de 56,67%, el Analista de Computo tiene un nivel de riesgo de 66,67%, el Asistente de Computo 1 tiene un nivel de riesgo de 55%, el Asistente de Computo 2 tiene un nivel de riesgo

de 53,33%, y el riesgo promedio del departamento es de 57,92%; sobre el componente Gestión de Comunicación y Operación el Jefe de Computo tiene un nivel de riesgo de 32,35%, el Analista de Computo tiene un nivel de riesgo de 64,71%, el Asistente de Computo 1 tiene un nivel de riesgo de 47,06%, el Asistente de Computo 2 tiene un nivel de riesgo de 41,18%, y riesgo promedio del departamento es de 46,33%; sobre el componente Control de Acceso el Jefe de Computo tiene un nivel de riesgo es de 58,33%, el Analista de Computo tiene un nivel de riesgo de 66,67%, el Asistente de Computo 1 tiene un nivel de riesgo de 83,33%, el Asistente de Computo 2 tiene un nivel de riesgo de 75%, y el riesgo promedio del departamento es de 70,83%; sobre el componente Cumplimiento el Jefe de Computo tiene un nivel de riesgo es de 50%, el Analista de Computo tiene un nivel de riesgo de 100,00%, el Asistente de Computo 1 tiene un nivel de riesgo de 100,00%, el Asistente de Computo 2 tiene un nivel de riesgo de 100,00%, y riesgo promedio del departamento es de 87,50%.

De manera general el departamento tecnológico cuenta con unos porcentajes de riesgo por colaborador y por departamento como tal, el Jefe del Departamento tiene un nivel de riesgo promedio en la evaluación de la NORMA ISO 27000 de 48,90%, el Analista de Computo tiene un nivel de riesgo promedio en la evaluación de la NORMA ISO 27000 de 70,84%, el Asistente de Computo 1 tiene un nivel de riesgo promedio en software de 74,42%, el Asistente de Computo 2 tiene un nivel de riesgo promedio en la evaluación de la NORMA ISO 27000 de 67,54%. El riesgo promedio por departamento mediante la NORMA ISO 27000 es de 65,42%.

Es así, que se evidencia que el componente con mayor nivel de riesgo es de 87,50% que equivale al componente de cumplimiento y el componente con menor nivel de riesgo es el de Gestión de Comunicación y Operación con 46,33%.

4.9. ANÁLISIS DE LOS RIESGOS SEGÚN NORMA ISO 27000

En base a los resultados obtenidos en la evaluación de riesgos según la Norma ISO 27000, el departamento tecnológico fue evaluado mediante los componentes de Inventario de Activos, Seguridad de los Recursos Humanos, Seguridad Física y del Entorno, Gestión de Comunicación y Operación, Control de Acceso y Cumplimiento.

Para obtener la siguiente tabla, se evaluó a cada uno de las personas que laboran dentro del departamento tecnológico, donde dio como resultado un promedio de riesgo por individuo /componente y el riesgo promedio general del departamento, mostrado en la siguiente tabla:

COMPONENTES	RIESGOS
Inventario de Activos	78,57%
Seguridad de los Recursos Humanos	51,39%
Seguridad Física y del Entorno	57,92%
Gestión de Comunicación y Operación	46,33%
Control de Acceso	70,83%
Cumplimiento	87,50%
PROMEDIO RIESGO GENERAL DEL DEPARTAMENTO	65,42%

Tabla 4.11. Promedio Riesgo General del departamento tecnológico

Fuente: Norma ISO 27000

Elaborado por: Las autoras

Procediendo al análisis, se observa, que el componente de Inventario de Activos, muestra un riesgo promedio de 78,57%, debido a que no se cumple en su totalidad el control de inventario de Activos Tecnológicos, como lo dispone la Norma ISO 27000.

El componente de Seguridad de los Recursos Humanos, con un riesgo promedio de 51,39%, no cumple con todas las disposiciones que exige la Norma ISO 27000, como lo es de tener un Manual de Funciones y Responsabilidades actualizados, y no hacen la respectiva formalidad de la devolución de los activos tecnológicos.

En el componente de Seguridad Física y del Entorno, con un riesgo promedio de 57,92%, como lo dispone la Norma ISO 27000, acerca de los perímetros de la seguridad física del entorno, la protección contra amenazas externas y ambientales de los equipos tecnológicos, seguridad de cableados, ubicación y protección de los equipos tecnológicos, áreas seguras, seguridad de los equipos fuera de las instalaciones y seguridad en la reutilización de los equipos, no se está cumpliendo en su totalidad como lo exige la ley.

En el componente de Gestión de Comunicación y Operación, con un riesgo promedio de 46,33%, es debido a que solo se lleva en partes la respectiva documentación de los procedimientos de operación, gestión del cambio, distribución de funciones, separación de áreas, realización de proyecciones de los requerimientos de capacidad futura, control contra códigos maliciosos, respaldo de la información, controles a las redes, seguridad de los servicios de la red, registros de auditoría, como lo dispone la Norma ISO 27000.

En el componente de Control de Acceso, con un riesgo promedio de 70,83%, se debe a que no se cumple a cabalidad las políticas de control de acceso, registros de usuarios, políticas de uso de los servicios de red, identificación de los equipos en las redes, control de conexiones a las redes, control de accesos remotos como lo dispone la Norma ISO 27000.

En el componente de Cumplimiento, con un riesgo promedio de 87,50%, la Norma ISO 27000 refiere a la Identificación de la legislación aplicable: Inventario de todas las Normas legales que utiliza la institución, y controles de auditorías de los sistemas de información, que el departamento tecnológico debe cumplir porque así lo exige esta Norma, y no se está llevando a cabo.

ESPAM MFL	
ANÁLISIS MEDIANTE LA NORMA 410 DE CONTROL INTERNO	
Objetivo/Ámbito: El presente análisis es con la finalidad de dar conocer la verificación del nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.	
Área auditada: Departamento Tecnológico de la ESPAM MFL	
Personal Auditado: Jefe del Departamento, Analista de Computo, Asistente de Computo 1 y Asistente de Computo 2	
DOCUMENTACIÓN	
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:	
La Institución cuenta con un organigrama	
El departamento tecnológico no cuenta con un organigrama actualizado, existe uno como Jefatura de Cómputo, y debido a esta observación las auditoras proponen un organigrama para el área auditada.	
El Manual de Funciones y Responsabilidades no está actualizado porque consta como Jefatura de Computo, y según la Norma de Control Interno de TI 410-09, refiere a que todos los Manuales técnicos, funciones, políticas y procedimientos deben ser actualizados	
No tienen delimitadas las funciones y responsabilidades en el departamento, por esta razón en la actualidad no existe la debida asignación de funciones como lo dispone la Norma de Control Interno de TI 410-09.	
La Planificación de Mantenimientos de Equipos de Redes, Computación y Software Base, está como Jefatura de Computo, no tiene fecha de cuando fue elaborada, debería ser actualizada para el departamento tecnológico como lo dispone la Norma de Control TI 410-09.	
Los diferentes mantenimientos (preventivo, correctivo) en la institución, no se los realiza con la debida autorización del Jefe del Departamento	
La solicitud de los diferentes mantenimientos (preventivo, correctivo) que brinda el departamento tecnológico se lo realiza de manera verbal o por medio de vía telefónica.	
Actualmente se hacen los mantenimientos preventivos cada 3 meses y los correctivos cuando el equipo tecnológico lo requiera, aunque no tienen una Planificación de Mantenimientos Programados.	
No cuenta con Políticas y Procedimientos el Departamento Tecnológico.	
No se lleva un control de los equipos en garantía.	
El departamento tecnológico no lleva un control de inventarios de los equipos de computación y software a excepción de los equipos de comunicación y redes, que se llevan en un 30% en archivos Excel.	
No se dispone de ningún tipo de bitácoras para el registro de fallas de los equipos.	
Se poseen registros individuales de los equipos tecnológicos en el Departamento de Almacén, aunque también debería llevarlos el departamento tecnológico como lo refiere la Norma de Control Interno de TI 410-09.	
No se realizan revisiones periódicas de los equipos computación y software base.	
Se realizan revisiones cada semana a los equipos de las redes.	
No aplican metodologías para planificar las revisiones de los equipos tecnológicos en general.	
El Departamento no cuenta con un Plan de Contingencia.	
El departamento tecnológico realiza el respaldo de la información de los equipos formateados en dispositivos externos, pero no son registrados ni almacenados para su conservación, una vez devuelta la información al equipo formateado, se elimina la información respaldada.	
No existen controles de acceso a las computadoras del personal administrativo.	
Si existen controles de acceso a las redes inalámbricas de la institución.	
Si existen controles de acceso a los servidores.	
No se llevan registros estadísticos del uso de la red.	
El departamento tecnológico administra las contraseñas de admisión de las redes.	

Las contraseñas de admisión son abiertas en un 50% debido a que sus usuarios son estudiantes de las diferentes áreas en la institución.
Se han realizado auditorías al departamento tecnológico por parte de la Contraloría General del Estado, sin embargo no se han aplicado las recomendaciones pertinentes de dichas evaluaciones.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma de Control Interno que emite la Contraloría General del Estado Ecuatoriano.
HARDWARE
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
El departamento no cuenta con un servicio de mantenimiento para todos los equipos tecnológicos en general.
El mantenimiento de los equipos tecnológicos se lo realiza cada 3 meses o cuando hay algún problema o falla.
Existe un plan de mantenimiento para los equipos tecnológicos como Jefatura de Cómputo.
No cuentan con un control y registro de los mantenimientos realizados.
Los equipos tecnológicos que tienen garantía, el proveedor realiza el mantenimiento fuera de la institución y se llevan éstos con discos duros.
No se tienen criterios de evaluación de rendimiento de los equipos de computación, solamente se hace el criterio de evaluación de funcionalidad de los equipos.
La administración de las bases de datos y los servidores lo lleva la Carrera de Informática y no el Departamento Tecnológico, como la Carrera Informática es de área Educativa y no de área administrativa como lo es el departamento tecnológico, entonces la administración de las bases de datos y servidores incluyendo la producción de software debería ser llevados por éste, reformando su estructura de acuerdo al organigrama propuesto por las auditoras y con personal capacitado para llevar el control de dicha administración.
El registro de los equipos de computación, no los lleva el departamento tecnológico, esto lo hace el departamento de Almacén, sin embargo debería llevarlo también el departamento porque esto lo dispone la Norma de Control Interno TI 410-09
No se tienen acceso remoto a las redes.
No se tiene un registro de los puntos de acceso que existen en la institución.
La seguridad de las redes inalámbricas es WPA WPA2 dentro de la institución.
No se realiza la relevación de los costos en mantenimientos de equipos en general de los últimos años.
No se evidencian los tiempos de mantenimiento.
No se realiza el seguimiento de los controles de los componentes de los equipos tecnológicos de la institución.
No se realiza el seguimiento a los controles de equipos que ya fueron cambiados por garantía.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma de Control Interno que emite la Contraloría General del Estado Ecuatoriano.
SOFTWARE
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
Se realiza el mantenimiento del software base dentro de la Institución, solamente cuando este lo requiera y que su versión sea compatible con el equipo.
Se evalúa el funcionamiento del software base en el momento que se instala y cada año después de instalado, sin embargo no se llevan registros de su funcionamiento.
No se actualiza el software base, solo cuando lo requiere el usuario o la nueva versión sea compatible con el equipo.
Las licenciaturas del software base son actualizadas cada año.
El tipo de licenciaturas que tiene la Universidad es institucional, no estudiantil.
No existen procedimientos para hacer las diferentes actualizaciones.
No todos los equipos de computación tienen instalados los antivirus.
Los programas instalados en los equipos tecnológicos, para las actividades de la institución son paquete Office, Antivirus, PDF, WinRAR.

NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma de Control Interno que emite la Contraloría General del Estado Ecuatoriano.

4.10. OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE CHECKLIST NORMA DE CONTROL INTERNO

Cuadro 4.34. Observaciones encontradas mediante la aplicación de checklist Control Interno

Elaborado: por las autoras

4.11. OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE CHECKLIST NORMA ISO 27000

ESPAM MFL ANÁLISIS MEDIANTE LA NORMA ISO 27000
Objetivo/Ámbito: El presente análisis es con la finalidad de dar conocer la verificación del nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.
Área auditada: Departamento Tecnológico de la ESPAM MFL
Personal Auditado: Jefe del Departamento, Analista de Computo, Asistente de Computo 1 y Asistente de Computo 2
INVENTARIO DE ACTIVOS
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
<p>En consideración a la Norma ISO 27000 con respecto a la Gestión de activos, en el punto de Inventario de activos, refiere que se debe inventariar los activos primarios en formatos físicos y/o electrónicos, también los activos de soporte de Hardware, Software y Redes, debe tener un plan estratégico, y que los activos tengan asignados un responsable del activo, lo que el departamento tecnológico no cumple con lo siguiente:</p>
<p>No tiene un Plan Estratégico</p>
<p>No llevan el control de inventario de hardware y software con sus respectivos formatos como lo estipula la norma ISO 27000.</p>
<p>Del inventario de comunicación y redes solo se lleva el 30 % de su totalidad, en forma electrónico (digital), mostrando evidencia en archivos Excel, quien lleva el control del inventario de activos tecnológicos (hardware, software, redes) en su totalidad, es el departamento de almacén.</p>
<p>Con respecto a los custodios asignados a los equipos tecnológicos, si se hace la respectiva asignación, lo que no se hace es la debida formalidad del cambio inmediato cuando éste termina su contrato de trabajo en el área asignada o en la entidad como lo estipula la Norma ISO 27000. (Inventario desactualizado por parte de Almacén)</p>
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
SEGURIDAD DE LOS RECURSOS HUMANOS
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CUESTIONARIOS:
<p>Mediante la siguiente observación dentro del Departamento tecnológico, se socializan los procedimientos de mantenimiento preventivo, correctivo de los bienes: Hardware, Software y equipos de comunicación de redes, con respecto a trabajos técnicos, y en cuánto a la documentación que se deja como constancia en las hojas de registros e informes que evidencien la realización de los mantenimientos no se está llevando a cabo como lo dispone la Norma ISO 27000.</p>
<p>Se responsabiliza a cada custodio por el mal uso y destrucción de los equipos tecnológicos asignados y entregados al responsable, este proceso lo realiza el Departamento de Almacén y no el Departamento Tecnológico.</p>

Con respecto a las responsabilidades del Departamento, no existe una planificación ni procedimientos para la distribución de tareas.
El personal que labora en el departamento tecnológico, desconoce los objetivos establecidos para el departamento y también si éstos han sido definidos por escrito.
Como lo estipula la Norma ISO 27000 sobre el proceso de devolución de los activos tecnológicos en la terminación del contrato de trabajo, no se cumple con la totalidad de dicho proceso, ya que cuando se termina el contrato del custodio del equipo, las actas de entrega no se las realiza en el tiempo debido y con la formalidad respectiva que debe hacerse, y solo se reporta al Departamento de Almacén, hasta que se haga el trámite correspondiente. Además el departamento tecnológico también debería llevar estas actas de entrega como lo dispone la Norma ISO 27000 en referencia al Inventario de activos.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
SEGURIDAD FÍSICA DEL ENTORNO
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
De acuerdo a las observaciones pertinentes y según la norma ISO 27000 con respecto a la protección contra amenazas externas y ambientales, la ubicación de los equipos de repuestos y soportes deben estar a una distancia prudente para evitar daños en caso de desastre que afecten las instalaciones principales, la cual el Departamento tecnológico no cuenta con estas áreas de protección de equipos tecnológicos, incluso el departamento no tiene una estructura física adecuada para resguardar la seguridad de sus equipos en caso de algún desastre.
El 20% de las áreas en la universidad no tienen ubicado los equipos contra incendios.
El área de mantenimiento a las instalaciones eléctricas, al sistema de climatización y ductos de ventilación, no lo realiza el Departamento Tecnológico porque le compete al Departamento de Construcción.
Existen cámaras de seguridad para minimizar el riesgo de robos de equipos tecnológicos, sin embargo no se puede determinar si existe el debido control que permita verificar el funcionamiento de las mismas.
Todas las áreas de la institución tienen protección contra descargas eléctricas, y disponen de filtros protectores en el suministro de energía y en las líneas de comunicación, y quien lleva todas estas actividades es el departamento de Construcción.
El 87% de los equipos tecnológicos no tienen ups, esto se pudo determinar mediante las encuestas realizadas a los custodios de equipos a su cargo.
El 30% de las áreas con cableado de red en la institución no se protege contra la intersección o daño.
El 20% de las áreas de la institución no hacen la respectiva separación del cableado de la red con el cableado de energía.
No se pudo verificar si se separa el cableado de la red con el cableado de energía en el Data Center, ya que las políticas de acceso no permitieron la debida constatación de la separación del cableado.
Se realiza la identificación y rotulación del cableado de red de acuerdo a las normas locales (RTE INEN 098) e internacionales (ISO) en un 30%.
El departamento tecnológico dispone del 20% de documentación, el 80% en diseños/planos y de la distribución de conexiones de datos de redes inalámbricas y alámbricas.
De acuerdo a las especificaciones y recomendaciones del proveedor, el departamento tecnológico les da mantenimientos periódicos a los equipos y dispositivos tecnológicos.
El personal que labora en el departamento tecnológico, está calificado y autorizado para ser los únicos que den los servicios de mantenimientos a los equipos tecnológicos de la institución. Esto se evidencia con sus hojas de vida de cada uno de los individuos.
No se lleva ni se conservan los registros de los mantenimientos preventivos, correctivos o de fallas con causas no determinadas.
No se establecen controles de mantenimientos programados en el departamento, no hay un cronograma de actividades, ni un plan de mantenimiento actual, solamente existe un plan de mantenimiento cuando el departamento tenía el nombre de Jefatura de Cómputo pero no es aplicado en la actualidad.

No se custodian los equipos y medios que se encuentran fuera de las instalaciones de la institución, pero si se hacen firmar actas de responsabilidad y entrega del equipo a la persona que llevará este fuera de la entidad.
La institución No establece una cobertura adecuada del seguro (robo, incendio o mal uso del equipo) para proteger los equipos que se encuentran fuera de las instalaciones de la institución.
En la institución existen controles de acceso a las redes inalámbricas, cuando detectan muchas personas accediendo a las redes, ellos hacen el cambio inmediato de las contraseñas.
Se llevan controles de acceso a los servidores
No se realiza el correctivo para la evaluación de los dispositivos deteriorados que contengan información sensible antes de enviar a reparación.
Se utiliza la Técnica de formateo para borrar, destruir o sobrescribir la información sensible de un equipo reutilizado, pero esto no asegura el borrado seguro de la información.
Los retiros de los equipos tecnológicos o cualquier información de éste, se lo realiza con la previa autorización del custodio.
Existen personas autorizadas con su identificación respectiva para el retiro de los activos de la institución.
El registro de los equipos o activos que se retiran o se devuelven en la institución lo hace el Departamento de Almacén.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
GESTIÓN DE COMUNICACIÓN Y DE OPERACIÓN
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
No se documenta el proceso de respaldo y restauración de la información.
No se documentan las instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas.
No se documentan los procedimientos para el reinicio y recuperación del sistema en caso de fallas.
No se planifica el proceso de cambio y no se realiza la prueba correspondiente.
No se establecen responsables y procedimientos formales de control de cambios de procesos en los equipos y software.
No se aprueban de manera formal los cambios propuestos.
No está actualizado el Manual de Funciones y Responsabilidades del Departamento Tecnológico, existe uno como Jefatura de Cómputo.
No se realizan proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos como lo dispone la Norma ISO referente a la Gestión de Capacidad.
Se instalan y actualizan cada 6 meses el software de antivirus contra código malicioso.
Se mantienen los sistemas operativos actualizados con parches y actualizaciones disponibles, dependiendo de la máquina si soporta la versión actual.
No existen procedimientos de respaldo de información en el Departamento Tecnológico antes del mantenimiento.
La Norma ISO 27000 dispone en los controles de redes, que se debe separar el área de redes con el área de operaciones, y el departamento tecnológico no está cumpliendo con esta disposición.
No se designan responsabilidades para la asistencia de equipos remotos.
Se realizan diseños antes de la implementación de una red, en un 80% muestran evidencia.
No revisan alertas o fallas del sistema operativo
Realizan cambios de configuración de los controles de seguridad del sistema operativo
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
CONTROL DE ACCESO
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
Se identifican y se documentan los equipos que se encuentran en las redes, pero no en su totalidad.

Se tiene documentada la identificación de los equipos que están permitidos, según la red que corresponda.
No se implementan procedimientos para controlar la instalación de software en sistemas operativos
No se lleva un control y registro de auditoría de las actualizaciones de software que se realizan.
No se tienen restricciones de cambios de paquetes de software.
No se lleva un control de versiones para todas las actualizaciones de software.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
CUMPLIMIENTO
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
Con los resultados obtenidos en los checklist, y de acuerdo a la Norma ISO 27000 referente al cumplimiento de la legislación aplicable en la institución, el personal que labora en el departamento tecnológico, no está considerando todas las normas y leyes más generales en cuanto a gestión de datos e información electrónica como lo estipula la Norma.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000

Cuadro 4.35. Observaciones encontradas mediante la aplicación de checklist Norma ISO 27000

Elaborado: por las autoras

4.12. NIVEL DE MADUREZ DE LOS PROCESOS ESTUDIADOS EN EL DEPARTAMENTO TECNOLÓGICO

COMPONENTES	CONFIANZA PROMEDIO DEL DEPARTAMENTO	ESTADO DE NIVEL DE MADUREZ DE LOS PROCESOS	NIVEL DE MADUREZ DEL DE LOS PROCESOS	NIVEL DE MADUREZ DEL DEPARTAMENTO TECNOLÓGICO
Cumplimiento	12,50%	Inicial	1	ESTADO INICIAL NIVEL 2
Documentación	15,62%	Inicial	1	
Inventario de Activos	21,43%	Inicial	1	
Control de Acceso	29,17%	Inicial	1	
Hardware	41,91%	Gestionado	2	
Seguridad Física del Entorno	42,08%	Gestionado	2	
Software	43,18%	Gestionado	2	
Seguridad de los Recursos Humanos	48,61%	Gestionado	2	
Comunicación y operación	53,68%	Gestionado	2	

Cuadro 4.36. Nivel de Madurez de los procesos estudiados en el Departamento Tecnológico

Fuente: Modelo de Madurez CMMI

Elaborado por: Las autoras

4.12.1. CRITERIOS DE EVALUACIÓN DE LOS PROCESOS ESTUDIADOS EN EL DEPARTAMENTO TECNOLÓGICO

NIVEL DE MADUREZ	DESCRIPCIÓN DEL NIVEL DE MADUREZ	CUMPLIMIENTO DE LAS NORMAS CONTROL INTERNO de TI 410-09 E ISO 27000
1	El componente de Cumplimiento de acuerdo a su nivel de confianza 12,50% se encuentra en el estado de madurez Inicial, debido a que se cumplen parcialmente con las normas de ley en sistemas de información y también el personal no conoce en su totalidad las leyes tanto nacionales como internacionales para la aplicación de la misma. El riesgo es de un 87,50% para el departamento tecnológico.	Se está cumpliendo parcialmente con la Norma ISO 27000 referente a Cumplimiento.
1	El componente de documentación de acuerdo a su nivel de confianza 15,62% se encuentra en el estado de madurez Inicial, debido a que hay políticas, manual de funciones y responsabilidades y un plan de mantenimiento sin actualizar. Este es un componente que no está aplicando la totalidad de la normativa de ley, y la cual refleja un impacto de riesgo de 84,38% para el departamento.	Se aplica parcialmente la Norma de Control Interno de Tecnologías de Información 410-09 que refiere al Control y mantenimiento de la infraestructura tecnológica
1	El componente de Inventario de Activos de acuerdo a su nivel de confianza 21,43% se encuentra en el estado de madurez Inicial, debido a que se lleva parcialmente el Control de Inventario de activos tecnológicos en Redes y Telecomunicaciones y el proceso de devolución de activos no se lo realiza formalmente, El riesgo es alto y corresponde a un 78,57% para el departamento tecnológico.	Se está cumpliendo parcialmente con la Norma ISO 27000 referente a Gestión de Activos.
1	El componente de Control de Acceso de acuerdo a su nivel de confianza 29,17% se encuentra en el estado de madurez Inicial, debida a que se tiene parcialmente documentada la identificación de los equipos permitidos en la red. El riesgo corresponde a un 70,83% para el departamento tecnológico.	Se está cumpliendo parcialmente con la Norma ISO 27000 referente a Control de Acceso.
2	El componente de Hardware de acuerdo a su nivel de confianza 41,91% se encuentra en estado de madurez Gestionado, ya que sus actividades dentro de este componente como mantenimientos preventivos, correctivos, implementaciones de redes se realizan de manera total, con un patron regular aunque estas no se documentan de manera adecuada, lo que implica que sus procesos sean desorganizados. El impacto de riesgo por no cumplir totalmente la normativa es de 58,09% en el departamento tecnológico.	Se aplica la Norma de Control Interno de Tecnologías de Información 410-09, teniendo un patrón regular.
2	El componente de Seguridad Física del Entorno de acuerdo a su nivel de confianza 42,08% tienen un estado de madurez Gestionado, sus actividades dentro de estos componentes como el formateo seguro de la información, la custodia de los equipos tecnológicos fuera de la institución, la protección del cableado de red, identificación y rotulación del cableado de red se hacen de manera regular sin una documentación adecuada, llevando al departamento a obtener un riesgo de 57,92% .	Se cumple con un patrón regular la Norma ISO 27000 referente a Seguridad Física del Entorno.
2	El componente de Software de acuerdo a su nivel de confianza 43,18% se encuentra en estado de madurez Gestionado, ya que sus actividades como actualizaciones de software base, actualizaciones de licenciaturas de software e instalación de programas en los equipos tecnológicos se realizan de manera total aunque estas no se documentan de manera adecuada, y al igual que Hardware, implica que sus procesos son	Se aplica un patrón regular a la Norma de Control Interno de Tecnologías de Información 410-09.

	desorganizados. El impacto de riesgo por no cumplir totalmente la normativa es de 56,82% (Software) en el departamento tecnológico.	
2	El componente de Seguridad de los Recursos Humanos de acuerdo a su nivel de confianza 48,61% tienen un estado de madurez Gestionado, sus actividades dentro de estos componentes se hacen de manera parcial sin una documentación adecuada, como por ejemplo no tener una planificación y procedimientos para la distribución de tareas, llevando al departamento a resultados pobres en el control y mantenimiento de la infraestructura tecnológica, causando a la vez un riesgo de 51,39%.	Se cumple un patrón regular a la Norma ISO 27000 referente a la Seguridad de los Recursos Humanos
2	El componente de Comunicación y Operación de acuerdo a su nivel de confianza 53,68% tiene un estado de madurez Inicial, sus actividades dentro de este componente se hacen de manera parcial como el proceso de respaldo y restauración de la información, las instrucciones para el manejo de los errores en la ejecución de tareas, todo esto sin una documentación adecuada, causando un riesgo de 46,32% en el departamento tecnológico.	Se sigue un patrón regular a la Norma ISO 27000 referente a Comunicación y Operación.

Cuadro 4.46. Criterios de evaluación de los procesos estudiados en el Departamento Tecnológico

Fuente: Modelo de Madurez CMMI

Elaborado por: Las autoras

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Una vez finalizada la investigación de Auditoria al control y mantenimiento de la Infraestructura Tecnológica del Departamento Tecnológico de la ESPAM MFL se concluye de la siguiente manera:

- Al alinear las metodologías que se utilizaron en las diferentes fases de la auditoria se logró familiarizarse con la situación actual del departamento.
- 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.
- Mediante la aplicación de las técnicas se pudo notar que los procesos que se manejan internamente no se encuentran documentado (registro 70%, políticas no actualizadas, bitácoras 100%, métodos 100%, plan de contingencia 100%, entre otros).
- Al momento de aplicar los diferentes cuestionarios habían temas en los cuales los asistentes e incluso el jefe del departamento tecnológico estaba desinformado de cómo se llevaba ese control, es por eso, que el nivel de riesgo es extremadamente alto.
- A través de la matriz de Riesgo-Confianza del Manual de Contraloría General del Estado se determinó que el nivel de riesgo de la Norma Control Interno de TI 410-09 Infraestructura Tecnológica es 66,43% y el nivel de riesgo de la Norma ISO 27000 es 65,42%

- Durante la evaluación y el análisis de las Norma 410-09 de Control Interno y la Norma ISO 27000, se logró identificar las debilidades obteniendo observaciones y recomendaciones para ser emitidas en el informe final

5.2. RECOMENDACIONES

Finalizada la investigación de Auditoría al control y mantenimiento de la Infraestructura Tecnológica del Departamento Tecnológico de la ESPAM MFL lo siguiente:

- De acuerdo con lo planteado y el proyecto realizado es responsabilidad del Departamento Tecnológico aplicar y poner en marcha las recomendaciones emitidas de ésta Auditoría Informática.
- Hacer cumplir lo que exige la misión del departamento tecnológico que se lo encuentra en el registro oficial(anexo 7)
- Al Jefe del Departamento Tecnológico, socializar con el personal que labora dentro del departamento los procesos, políticas planes y procedimientos y toda información que esté vinculada directamente a la Institución.
- Al Jefe del Departamento Tecnológico, para el mejoramiento de los procesos debe estrictamente poner en práctica lo que dispone la Norma de TI 410-09 Infraestructura Tecnológica y la Norma ISO 27000.
- Que se cumplan con obligatoriedad las recomendaciones de la auditoría interna a la ESPAM MFL DR5-0020-2010 realizada por la Contraloría General, donde se manifiesta que se conforme un Comité Técnico, donde existe ausencia de actas de entrega-recepción de documentos, bienes e información electrónica.

BIBLIOGRAFÍA

- Acosta, D.; González, A. y Díaz, O. 2011. Proceso de auditoría de la calidad para la actividad productiva. Universidad de las ciencias informáticas (UCI). La Habana, Cuba. Vol. 32. N° 2. p 97.
- Acuerdo N° 039 CG. 2009. Normas de Control Interno para las entidades, organismos del sector público y personas jurídica de derecho privado que dispongan de recursos públicos. San Francisco de Quito, EC. 16 de nov.
- Acuerdo N° 166. 2013. Esquema gubernamental de seguridad de la información (EGSI). San Francisco de Quito, EC. 19 de sept
- Alfonso, Y; Blanco, B; Loy, L. 2012. Auditoría con Informática a Sistemas Contables. CU. Revista de Arquitectura e Ingeniería. Vol.6. p. 3-4.
- AUDISA (Auditoría Informática S.A). 2009. Qué es un checklist- para qué sirve. (En línea). ES. Consultado el 22 de Dic. 2014. Formato HTML. Disponible en:
<https://audisa.wordpress.com/2007/11/02/checklist-¿que-es¿para-que-sirve.html>
- Aymara, A. 2010. Auditoría Informática y Gestión de Tecnologías De Información y Comunicación (TICs). Venezuela. Universidad Centroccidental Lisandro Alvarado. Vol. 13. p. 3-4.
- Azuaje, M y Leal, S. 2011. Tres tipos penales informáticos. Venezuela. VE. Cuestiones Jurídicas. Vol. V. p. 5- 15.
- BAA (Business Assurance and Audit), s.f. Informes de Auditoría. Empresa de Auditores. P. 4.
- Barros, G; Cadena, A. 2012. Auditoría informática de la cooperativa de ahorro y crédito "Alianza del Valle" Ltda.". (En línea) EC. Consultado el 18 de Oct. 2013. Formato PDF. Disponible en:
<http://repositorio.espe.edu.ec/bitstream/21000/5197/1/T-ESPE-0330.pdf>
- Blanco, L. 2011. Auditoría a Sitios Web. Facultad de Economía de la Universidad de La Habana. Calle L No. 353, Vedado, La Habana, Cuba.
- Carvajal, J. 2008. Auditoría informática en la unidad educativa particular francés de la ciudad de esmeraldas en el año lectivo 2006 – 2007. (En línea). EC. Consultado el 10 de Nov. 2014. Formato PDF. Disponible en:
<http://www.pucese.edu.ec/websistemas/index.php/repositorio-de-trabajos-de-grado/category/63.pdf>

- Castells, M. 2010. La Sociedad red: una Visión Global. Edición Especial. Madrid. Revista Venezolana de Información, Tecnología y Conocimiento. p 139.
- Castromán, J y Porto, N. 2005. Responsabilidad Social y Control Interno. BR. BRA. Revista Universo Contábil. Vol. 1. p. 93-96.
- CCOPCEE (Comisión de Coordinación de los Órganos Públicos del Estado Español). s.f. Principios y Normas de Auditoría del Sector Público. (En línea) ES. Consultado el 1 de Jun. 2014. Disponible en: <http://www.acuentascanarias.org/documentos/normasaudpublico.pdf>
- CE (Constitución del Ecuador). 2008. Art. 204, 205 y 211. La Contraloría General del Estado. EC. p. 1.
- CGE (Contraloría General del Estado), 2003. Manual General de Auditoría Gubernamental de las Entidades y Organismo del Sector Público y para las Firmas privadas de auditorías contratadas. Acuerdo 012-CG-2003, RO 107 19 de Jun de 2003
- CGE (Contraloría General del Estado), 2010. Examen especial a las operaciones administrativas financieras de la Escuela Superior Agropecuaria de Manabí Manuel Félix López ESPAM MFL (DR5-0020-2010). Pág. 12.
- Christofolletti, R. y Piassa, D. 2013. Tecnología y Zonas de Tensión Ética para Periodistas. Santiago, CH. Cuadernos de Información. p 32.
- Corral, F. 2009. Evaluación del Sistema de Control Interno. Universidad Andina Simón Bolívar. Quito-Ecuador. p. 39.
- ESPAM-MFL (Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López). 2013. Reseña Histórica de la ESPAM MFL. (En línea) EC. Consultado el 24 de Nov. 2013. Formato HTML. Disponible en: <http://www.espam.edu.ec/universidad/index.php?id=historia>
- _____. 2012. Manual del Sistema de Investigación Institucional. 2ed. Calceta-Manabí, EC. p 19
- ESPE (Escuela Superior Politécnica del Ejército). 2010. Planificación de Auditoría. (En línea).EC. Consultado el 20 de Oct. 2014. Formato PDF. Disponible en: <http://ai.espe.edu.ec/wp-content/uploads/2012/07/Manual-de-Auditoría-Gubernamental-Cap-V.pdf>
- Espinoza, M. 2007. Auditoría Informática para los Departamentos Financiero, Tesorería, Proveeduría, Agencia Norte y Agencia Sur de la Empresa Municipal de Agua Potable y Alcantarillado de Ambato. Ecuador-Ambato.

- Gallardo, V. y Salazar, T. 2014. "Auditoría de gestión a la dirección de investigación de la universidad técnica de Cotopaxi. Tesis. Ing. Contabilidad y Auditoría. Unidad Académica de Ciencias Administrativas y Humanísticas. Cotopaxi-Latacunga, EC. p 17
- García, F. 2005. El análisis de la realidad social: Métodos y técnicas de investigación, Madrid, Alianza Universidad Textos.
- Govindan, M. 2007. Control Interno, Auditoría y Seguridad Informática. Tomo II – IV. España.
- Herrera, A. 2013. Tecnologías de la información y las organizaciones inteligentes en la sociedad del conocimiento. (En línea). MX. Consultado el 14 de Ag. 2014. Formato PDF. Disponible en: <http://cdigital.uv.mx/bitstream/123456789/34417/1/herreraelizondoazuena.pdf>
- Icaza, D. 2010. El cuasicontrato administrativo. Revista Jurídica. Facultad de Derecho. Universidad Católica de Santiago de Guayaquil. Ecuador. Consultado el 03 de Febrero del 2014. Disponible en: http://www.revistajuridicaonline.com/images/stories/revistasjuridicas/derecho-publico-tomo-2/77a100_el_cuasi.pdf
- II/ISSN (Ingeniería Industrial/ISSN 1815-5936). 2013. Bases para crear un modelo de madurez para Arquitecturas Orientadas a Servicios Vol. XXXIV. No. 3. p. 308.
- ISO/IEC. 2012. Normas ISO 27000. (En línea) MX. Consultado el 14 de Dic. 2014. Formato PDF. Disponible en: <http://dspace.ucuenca.edu.ec/jspui/bitstream/123456789/652/1/ts205.pdf>
- Jugdev, K. y Thomas, J. 2002. "Project management maturity models: the silver bullets of competitive advantage", Project Management Journal, Vol. 33 pp.4-14.
- Kuna, H.; Caballero, S.; Rambo, A.; Meinel, E.; Steinhilber, A.; Pautsch, G.; García-Martínez, R. y Villatoro, F. 2010. Avances en procedimientos de la explotación de información para la identificación de datos faltantes, con ruido e inconsistentes. Red de Universidades con Carreras en Informática (RedUNCI). Málaga, ES, p 137.
- Lara, A y Párraga, F. 2013. Auditoría Informática Ingeniería de Software Bases de Datos Información Genética. Ecuador. Disponible en: <http://repositorio.espe.edu.ec/handle/21000/6587>
- Ley N° 22. 2010. Ley Orgánica de Educación Superior. Publicado en el Registro Oficial No. 298. Quito, EC. 12 de Oct

- Loor, A y Espinoza, V. 2014. Auditoría de seguridad física y lógica a los recursos de tecnología de información en la carrera informática de la ESPAM MFL. Tesis. Ing. Informática. ESPAM MFL. Calceta-Manabí, EC. p 34
- LOCGE (Ley Orgánica de Contraloría General del Estado). 2004. Art. 1.- Objeto de Ley. EC. p. 1
- LOES (Ley Orgánica de Educación Superior). 2010. Art. 8.- Objeto de Ley. EC. p. 1
- Martínez, A; Blanco, B; Loy M. 2012. Auditoría con Informática a Sistemas Contables. Revista de Arquitectura e Ingeniería, Vol. 6, N° 2. p 1-14.
- Mira, J. s.f. Informes de Auditoría. (En línea). EC. Consultado el 4 de Sept. 2014. Formato PDF. Disponible en: <http://www.miramegias.com/auditoria/files/present/ut05s.pdf>
- Montaño, O. 2008. "Modelo que identifica los elementos que contribuyen a elevar el grado de madurez en la pequeña empresa (PEM) del sector manufacturero" Tesis de Doctorado, Facultad de Ingeniería, Universidad Nacional Autónoma de México.
- Nava, J. s.f. Apuntes de Auditoría Informática. (En línea) EC. Consultado el 14 Mayo 2014. Formato PDF. Disponible en: <http://www.escet.urjc.es/~ai/T1Apuntes.pdf>
- NCI (Normas de Control Interno). 2010. Acuerdo de la Contraloría General del Estado. Registro Oficial 39. Suplemento 87. De 14-dic-2009 Estado: Vigente.
- Ocampo, C; Trejos, O; Solarte, G. 2010. Las técnicas forenses y la auditoria. Colombia. COL. Scientia et technica. Vol. XVI. 108-113.
- OLACEFs (Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores). 2011. Manual de Auditoría Gestión en Tecnologías. (En línea). ES. Consultado el 12 Oct. 2014. Formato PDF. Disponible en: <http://bibliotecavirtual.olacefs.com/gsd/collect/guasyman/archives/HASH0155.dir/ManualAuditoriaGestionTICs.pdf>
- Orellana, P. 2008. Informes de Auditoría. (En línea). CO. Consultado el 4 de Julio del 2014. Formato PDF. Disponible en: <http://www.cpcese.org.ar/file/1315432920.pdf>

- Ortíz, M. 2011. Tablas Dinámicas. (En línea). MX. Consultado el 10 de Dic. 2014. Formato HTML. Disponible en: <http://exceltotal.com/tablas-dinamicas-en-excel.html>
- PLOPDP (Proyecto de Ley Orgánica de Protección de Datos Personales).2013. Resolución no. 007-DN-DINARDAP. 2013. Capítulo III. De la información, su publicidad y protección. EC. p 10
- Quintuña, V. s.f. Auditoría Informática a Telecomunicaciones Supertel. (En línea) EC. Consultado el 18 de Sept. 2014. Formato PDF. Disponible en: <http://dspace.ucuenca.edu.ec/jspui/bitstream/123456789/652/1/ts205.pdf>
- Piattini, M; Del Peso, E.; Del Peso, M. 2008. Auditoria de Tecnologías y Sistemas de Información. 4ed. Madrid, ES. RA-MAI. Vol. 1378. p 38.
- Ramírez, J y Álvarez, E. 2009. Auditoría a la Gestión de las Tecnologías y Sistemas de Información. Perú. Universidad Nacional Mayor de San Marcos. Vol. 6. p. 99-102.
- Silva, N y Espina, J. 2006. Ética Informática en la Sociedad de la Información. Venezuela. VE. Revista Venezolana de Gerencia. Vol. 11. p. 559-579.
- Tello, E. 2008. Las tecnologías de la información y comunicaciones (TIC) y la brecha digital. México. Revista de Universidad y Sociedad del Conocimiento. Vol. 4 n. ° 2.
- UOC (Universitat Oberta de Catalunya). 2013. Infraestructura Tecnológica. (En línea) ES. Consultado el 10 de Mayo 2014. Formato HTML. Disponible en: http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html
- Vásquez, R. s.f. Gestión Integral de Riesgos de Tecnologías de Información. (En línea). Consultado el 22 de Mayo 2014. Formato PDF. Disponible en: <http://www.share-pdf.com/ae5edbbca89945a7bfef43d893ad5fa6/6%20Gestion%20Integral%20de%20Riesgos%20TI.pdf>
- Villardefrancos, M y Rivera, Z. 2006. La auditoría como proceso de control: concepto y tipología. Cuba. Ciencias de la Información. Vol.37. p. 53-59.
- Viloria, N. 2004. Una aproximación a un enfoque holístico en auditoría. Venezuela. VE. Actualidad Contable Faces. Vol.7. p. 85-94.
- Yañez, C. 2011. Enfoque Metodológico de la Auditoría a las Tecnologías de Información y Comunicación. Seudónimo 6. Chile. Pág. 17-26. Disponible en: http://www.olacefs.com/Olacefs/ShowProperty/BEA%20Repository/Olacefs/uploaded/content/article/20120829_1.pdf

Whitten, J. 2008. Análisis y Diseño de Sistemas de Información. 2 ed. Editorial McGraw Hill Interamericana. Argentina. Buenos Aires.

_____ 2010. La auditoría, concepto, clases y evolución. 12 ed. Editorial McGraw Hill Interamericana. Colombia.

ANEXOS

ANEXO 1
CARTA DE AUTORIZACIÓN

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ
MANUEL FÉLIX LÓPEZ**

REPÚBLICA DEL ECUADOR



CARRERA DE INFORMÁTICA

Oficio N° ESPAM MFL - CI - 2014- 179-OF
Calceta, 16 de junio de 2014

Ingeniero
Leonardo Félix López
RECTOR ESPAM MFL
En su despacho.-

De mi consideración:

Por medio del presente reciba un cordial y afectuoso saludo de quienes conformamos la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM - MFL.

Nuestra institución dentro de su malla curricular contempla la realización de tesis de tercer nivel que tienen que efectuar todos los estudiantes con la finalidad de obtener el título de Ingeniero en Informática y, dentro de estas, las Instituciones públicas o privadas.

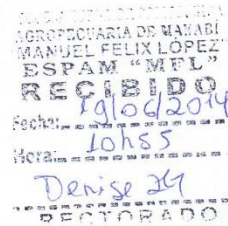
Con estos antecedentes, solicito a usted de la manera más cordial y por su digno intermedio a quien corresponda, brinde la información requerida para la elaboración de la tesis titulada "AUDITORÍA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ" en la dependencia que acertadamente usted dirige; por parte de los señores: **RIVERA CHÁVEZ MARÍA VICTORIA** y **ZAMBRANO BRAVO MARÍA FERNANDA**, estudiantes de décimo semestre de la Carrera de Informática ESPAM – MFL, para tal efecto es necesario contar con el apoyo requerido brindándole las facilidades pertinentes.

Esperando favorable acogida a la presente quedo de usted agradecida

Atentamente,

Ing. Jessica Morales Carrillo
DIRECTORA CARRERA DE INFORMÁTICA ESPAM – MFL

JM/jb



WWW.ESPAM.EDU.EC

1/1

ANEXO 2

**OFICIO DE SOLICITUD DE INFORMACIÓN AL JEFE DEL DEPARTAMENTO
TECNOLÓGICO**

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ
MANUEL FÉLIX LÓPEZ**

REPÚBLICA DEL ECUADOR



Oficio N° ESPAM MFL - CI – 2014- 217-OF
Calceta, 11 de agosto de 2014

Ingeniero
Geovanny García Montes
COORDINADOR DE CÓMPUTO ESPAM MFL
En su despacho.-

De mi consideración:

Por medio del presente reciba un cordial y afectuoso saludo de quienes conformamos la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM - MFL.

Nuestra institución dentro de su malla curricular contempla la realización de tesis de tercer nivel que tienen que efectuar todos los estudiantes con la finalidad de obtener el título de Ingeniero en Informática y, dentro de estas, las Instituciones públicas o privadas.

Con estos antecedentes, solicito a usted de la manera más cordial se brinde la información requerida para la elaboración de la tesis titulada "AUDITORÍA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ" en la dependencia que acertadamente usted dirige; por parte de los señores: **RIVERA CHÁVEZ MARÍA VICTORIA** y **ZAMBRANO BRAVO MARÍA FERNANDA**, estudiantes de décimo semestre de la Carrera de Informática ESPAM – MFL, para tal efecto es necesario contar con el apoyo requerido brindándole las facilidades pertinentes.

Esperando favorable acogida a la presente quedo de usted agradecida

Atentamente,


Ing. Jéssica Morales Carrillo
DIRECTORA CARRERA DE INFORMÁTICA ESPAM – MFL

JM/jb

Recibido
12/08/2014
09:30



1 / 1

ANEXO 3

**OFICIO DE SOLICITUD DE INFORMACIÓN AL JEFE DE TALENTO
HUMANO**

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ
MANUEL FÉLIX LÓPEZ**

REPÚBLICA DEL ECUADOR



Oficio N° ESPAM MFL - CI – 2014- 218-OF
Calceta, 11 de agosto de 2014

Ingeniero
Fabián Álava Rade
DIRECTOS DE TALENTOS HUMANOS ESPAM MFL
En su despacho.-

De mi consideración:

Por medio del presente reciba un cordial y afectuoso saludo de quienes conformamos la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM - MFL.

Nuestra institución dentro de su malla curricular contempla la realización de tesis de tercer nivel que tienen que efectuar todos los estudiantes con la finalidad de obtener el título de Ingeniero en Informática y, dentro de estas, las Instituciones públicas o privadas.

Con estos antecedentes, solicito a usted de la manera más cordial se brinde la información requerida para la elaboración de la tesis titulada "AUDITORÍA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ" en la dependencia que acertadamente usted dirige; por parte de los señores: **RIVERA CHÁVEZ MARÍA VICTORIA** y **ZAMBRANO BRAVO MARÍA FERNANDA**, estudiantes de décimo semestre de la Carrera de Informática ESPAM – MFL, para tal efecto es necesario contar con el apoyo requerido brindándole las facilidades pertinentes.

Esperando favorable acogida a la presente quedo de usted agradecida

Atentamente,


Ing. Jéssica Morales Carrillo
DIRECTORA CARRERA DE INFORMÁTICA ESPAM – MFL

JM/jb



19/08/2014
16:57
DUBEN 6002

1/1

WWW.ESPAM.EDU.EC

ANEXO 4

**OFICIO DE SOLICITUD DE INFORMACIÓN AL COORDINADOR DEL DATA
CENTER ESPAM MFL**

**ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ
MANUEL FÉLIX LÓPEZ**

REPÚBLICA DEL ECUADOR



Oficio N° ESPAM MFL - CI – 2014- 221-OF

Calceta, 11 de agosto de 2014

Ingeniero
César Moreira Zambrano
COORDINADOR DEL DATAR CENTER ESPAM – MFL
En su despacho.-

De mi consideración:

Por medio del presente reciba un cordial y afectuoso saludo de quienes conformamos la Carrera de Informática de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López ESPAM - MFL.

Nuestra institución dentro de su malla curricular contempla la realización de tesis de tercer nivel que tienen que efectuar todos los estudiantes con la finalidad de obtener el título de Ingeniero en Informática y, dentro de estas, las Instituciones públicas o privadas.

Con estos antecedentes, solicito a usted de la manera más cordial se brinde la información requerida; y además nos ayude con las políticas de Acceso al Datar Center; dicha información será para la elaboración de la tesis titulada "AUDITORÍA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ"; por parte de las señoras: **RIVERA CHÁVEZ MARÍA VICTORIA** y **ZAMBRANO BRAVO MARÍA FERNANDA**, estudiantes de décimo semestre de la Carrera de Informática ESPAM – MFL, para tal efecto es necesario contar con el apoyo requerido brindándole las facilidades pertinentes.

Esperando favorable acogida a la presente quedo de usted agradecida

Atentamente,

Ing. Jéssica Morales Carrillo
DIRECTORA CARRERA DE INFORMÁTICA ESPAM – MFL

JM/jb

Resto
19-08-14
17:15 PM

1 / 1

WWW.ESPAM.EDU.EC

ANEXO 5

**OFICIO DE SOLICITUD DE INFORMACIÓN AL JEFE DE ALMACÉN ESPAM
MFL**

Calceta, 19 de agosto del 2014

Ingeniero
Héctor John Macías Moreira
JEFE DEL DEPARTAMENTO DE ALMACÉN
En su despacho.-

De nuestras consideraciones:

Quienes estamos realizando la tesis titulada: **“AUDITORÍA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA AL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL”**, Srta. María Victoria Rivera Chávez y Sra. María Fernanda Zambrano Bravo, les desean un cordial saludo y a su vez éxitos en sus labores cotidianas.

Por medio de la presente, le solicitamos que nos otorgue el inventario de activos de todos los equipos tecnológicos (computación, redes y software), con motivo de hacer la respectiva verificación en las diferentes áreas en las que han sido instalados dichos recursos informáticos dentro de la institución.


Agradeciendo de antemano la atención que se sirve prestar al presente a fin de que se me otorgue lo anteriormente solicitado.

Sin más por el momento, quedamos de usted a sus apreciables órdenes.

Atentamente,


M. Victoria Rivera Chávez


M. Fernanda Zambrano Bravo

RECIBIDO
19/08/14
16 N 42


ANEXO 6

**OFICIO DE SOLICITUD DE LA ÚLTIMA AUDITORÍA REALIZADA A LA
ESPAM MFL A CONTRALORÍA GENERAL DEL ESTADO ECUATORIANO**

Portoviejo, 10 de septiembre del 2014



Econ.

Jack Ochoa Murillo Duvalieur

**DELEGADO PROVINCIAL DE LA CONTRALORIA GENERAL
DEL ESTADO**

Ciudad.-

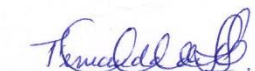
De mis consideraciones

Srtas. **MARIA VICTORIA RIVERA CHAVEZ Y MARIA FERNANDA ZAMBRANO BRAVO**, estudiantes egresadas de la Universidad **ESPAM MFL**, le solicitamos muy respetuosamente se nos conceda una copia de un informe de auditoria realizada a dicha Universidad, ya que estamos desarrollando una tesis titulada **Auditoria al Control y Mantenimiento de la Infraestructura Tecnológica del Departamento Tecnológico de la ESPAM MFL**.

Por su amable atención quedamos muy agradecidas.

Atentamente,


MARIA RIVERA CHAVEZ
C.C. 1312850421


MARIA ZAMBRANO BRAVO
C.C. 1310050115

632344 Ext 5006

ANEXO 7
REGISTRO OFICIAL N° 318

19. Informes de actividades académicas y administrativas;
20. Informes de la documentación interna y externa del Área Académica

3.2.5 TECNOLÓGICO

- a. **Misión.-** Proveer y administrar los servicios informáticos, comunicaciones e implantación de la infraestructura tecnológica necesaria para coadyuvar al desarrollo tecnológico de la Escuela.
- b. **Productos y servicios:**
 1. Plan de desarrollo informático;
 2. Informe de la ejecución del plan informático;
 3. Plan de mantenimiento preventivo, correctivo y predictivo de SOFTWARE y HARDWARE;
 4. Informe de ejecución de SOFTWARE y HARDWARE; y,
 5. Asesora en la adquisición de equipos y paquetes informáticos;
 6. Informe de configuración de sistemas de redes y comunicaciones;

Disposiciones Generales:

El portafolio de productos de la Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López" -ESPAM MFL, podrá ser reformado (incorporar, fusionar o transferir) de acuerdo a las necesidades institucionales.

El presente Estatuto Orgánico de Gestión Organizacional por Procesos entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en la ciudad de Calceta, 16 de enero del 2012.

CERTIFICACIÓN

La suscrita Secretaria General-Procuradora de la Escuela Superior Politécnica Agropecuaria de Manabí, Manuel Félix López, ESPAM MFL, certifica: que el presente Estatuto Orgánico de Gestión Organizacional por Procesos, fue discutido y aprobado por el Honorable Consejo Politécnico en dos sesiones extraordinarias de fechas: 11 y 16 de enero del 2012.

Calceta, 17 de enero del 2012.

LO CERTIFICO

f.) Mg P.E.S Lya Villafuerte Vélez, Secretaria General, ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ.



SUSCRÍBASE

Al Registro Oficial Físico y Web

Av. 12 de Octubre N° 16-90 y Pasaje Nicolás Jiménez / Edificio NAIDER
Teléfonos: Dirección: 2501 629 / 2502 835
Oficinas centrales y sucursales: 2234 540
Estación Nacional: Maicóns 201 y 10 de Agosto / Teléfono: 2433 951
Distribución (Alameda): 2430 110
Barral Guayaquil: Malecón N° 1606 y Av. 10 de Agosto / Teléfono: 2432 400

www.registroficial.gob.ec

facebook

EL REGISTRO OFICIAL no se responsabiliza por los errores ortográficos, gramaticales, de fondo y/o de forma que contengan los documentos publicados, dichos documentos remitidos por las diferentes instituciones para su promulgación, son transcritos fielmente a sus originales, los mismos que se encuentran archivados y son nuestro respaldo.

ANEXO 8
PLAN DE AUDITORÍA

DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL

PLAN DE AUDITORÍA

DEPENDENCIA:

Departamento Tecnológico de la ESPAM MFL

OBJETIVOS:

- a. Verificar el grado de cumplimiento al mantenimiento y control de la infraestructura tecnológica de acuerdo a la visión del departamento tecnológico.
- b. Relevar riesgos de Tecnologías de Información.
- c. Identificar las áreas que carezcan de normatividad.
- d. Verificar el nivel de cumplimiento de políticas, planes y procedimientos que emplea el Departamento Tecnológico en cuanto al uso de los recursos tecnológicos.
- e. Emitir el informe de auditoría de la infraestructura tecnológica tomando en cuenta todos los hallazgos recopilados.

El proceso de Auditoría al Mantenimiento y Control de la Infraestructura Tecnológica se realizará en el Departamento Tecnológico, en las áreas de Planeación, Centro de datos, Dirección de Carrera Informática, Inventario, Mantenimiento, Secretaría, Redes, la misma que ha proporcionado total apertura en las diferentes áreas. La evaluación comprende:

- a. **Evaluación de la dirección del departamento tecnológico en lo que corresponde a:**

ALCANCE:

- Los procesos que se llevan a cabo.
- Estructura Orgánica y Funcional.
- Normas, políticas y procedimientos.
- Planes de trabajo.
- Controles.
- Estándares.
- Estudio de viabilidad
- Convenios que se tiene con otras instalaciones.
- Fechas de instalación y planes de instalación de sistemas y equipos.
- Contratos vigentes de compra y servicio de mantenimiento.
- Contrato de Seguros.

b. Evaluación de los software base

- Evaluación de los diferentes sistemas de operación (procedimientos, documentación, organización de archivos, controles, utilización de los sistemas, licencia de software base).
- Seguridad física y lógica de los sistemas, su confidencialidad y respaldos.
- Descripción general del software base existente.
- Diagramas de Descripción
- Manual de procedimientos, instalación y mantenimiento.
- Descripción genérica
- Fechas de instalación del software base.
- Procedimientos y políticas en caso de desastres.

c. Evaluación de los equipos de computación y

ALCANCE:	<p>de redes</p> <ul style="list-style-type: none">• Número de equipos, localización y las características (equipos instalados y por instalarse).• Configuración de equipos y capacidades actuales y máximas.• Planes de expansión.• Ubicación general de los equipos.• Políticas de operación.• Políticas de uso de los equipos.• Planes de mantenimiento preventivo y/o correctivo de los equipos.• Estándares utilizados en la infraestructura de los equipos de redes.• Contratos de seguros de los equipos informáticos.
-----------------	---

DOCUMENTOS A SOLICITAR:

a) Información General:

- Solicitar documentos sobre los equipos, así como el número de ellos, localización y características.
- Estructura del ambiente de procesamiento de los sistemas de computación, sistemas de redes y software base.
- Listado valorado de activos con que cuenta el departamento tecnológico.
- Controles gerenciales y manual de funciones de usuarios (segregación de funciones).
- Estructura del departamento tecnológico, expedientes de personal del mismo, y a nivel de usuarios.
- Manuales, políticas y procedimientos de operaciones.
- Manuales de mantenimiento de los sistemas de información (Soporte Técnico).
- Documentación sobre el mantenimiento y control de la infraestructura tecnológica (equipos de computación, redes y software base).

b) Seguridad

- Solicitar las políticas de respaldo interno.
- Seguridad en los ambientes de los sistemas de control en la infraestructura tecnológica.
- Inventario y ubicación de los extintores e extinguidores, detectores de humos, adecuación de instalaciones.
- Accesos lógicos y físicos en el departamento tecnológico, así como en su ambiente computacional y redes.

<p>DOCUMENTOS A SOLICITAR:</p>	<p>c) Integridad, confidencialidad y disponibilidad de los sistemas de información.</p> <ul style="list-style-type: none"> ▪ La utilización y almacenamiento de los códigos fuentes, licencia de los sistemas utilizados. ▪ Obtener los planes de contingencia y pruebas de controles de usuarios. <p>d) Mantenimiento y Control de los equipos de computación, redes y software base.</p> <ul style="list-style-type: none"> ▪ Manuales y guías sobre los soportes de las redes, software base, hardware y computacional. ▪ Principales operaciones de los sistemas de información.
<p>DOCUMENTO DE REFERENCIA</p>	<p>Se tomará como documento de referencia: Norma ISO/IEC 27000, Normas de Control Interno 410-09</p>

ANEXO 9

PROGRAMA GENERAL PARA LA PLANIFICACIÓN PRELIMINAR

DEPARTAMENTO TECNOLÓGICO ESPAM MFL			
AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ			
PROGRAMA GENERAL PARA LA PLANIFICACIÓN PRELIMINAR			
N°	OBJETIVOS:	REFERENCIA	REALIZADO POR
	<p>Objetivos</p> <p>Comprender la situación actual del Departamento Tecnológico, mediante la aplicación de técnicas de auditoría.</p> <p>Identificar globalmente las actividades que se ejecutan en el Departamento Tecnológico, para el desarrollo de la auditoría.</p>		
	PROCEDIMIENTOS:		
1	Dialogar con el Jefe del Departamento Tecnológico.	P.T. 01	Las autoras.
2	Obtener la base legal de la entidad.	P.T. 03	Las autoras.
3	Obtener el organigrama estructural y funcional.	P.T. 03	Las autoras.
5	Verificar si la entidad ha elaborado y aprobado un plan estratégico.	P.T. 03	Las autoras.
6	Observar si el Departamento Tecnológico preparó el plan operativo anual.	P.T. 03	Las autoras.
7	Verificar si existen manuales, políticas y procedimientos de operaciones.	P.T. 03	Las autoras.
8	Verificar el plan de mantenimiento preventivo correctivo y predictivo de software y hardware	P.T. 03	
9	Verificar si existen planes de contingencia.	P.T. 03	Las autoras.
	Conocer la estructura de los laboratorios, aulas y		

11	oficinas donde existan equipos tecnológicos dentro de la entidad.	P.T. 04	Las autoras.
12	Solicitar información sobre los recursos tecnológicos disponibles, como documentos sobre los equipos, licencias de software base, seguros, número de ellos, características, entre otros.	P.T. 03	Las autoras.
13	Solicitar el inventario y la ubicación de los extintores y extinguidores, detectores de humo y adecuación de instalaciones	P.T. 03	Las autoras.
14	Solicitar la documentación del uso y almacenamiento de los códigos fuentes, licencias de los sistemas utilizados	P.T. 03	Las autoras.
15	Análisis y evaluación de información obtenida	P.T. 04	Las autoras.
16	Verificar el proceso de evaluación	P.T. 03	Las autoras.
17	Dialogar con el Jefe del Departamento Tecnológico sobre los resultados de la planificación preliminar.	P.T. 05	Las autoras.
18	Definir actividades y procedimientos que se llevaran a cabo en la fase de ejecución	P.T. 05	Las autoras.
19	Realizar el Memorando de la Planificación Preliminar.	P.T. 05	Las autoras.

Elaborado por: Las autoras

ANEXO 10
CUESTIONARIO DE CONTROL INTERNO PRELIMINARES

ESPAM MFL
CUESTIONARIO DE CONTROL INTERNO
Componente: Organización de la Documentación

ÁREA AUDITADA: Departamento Tecnológico		FECHA:		
		PERSONA AUDITADA:		
PREGUNTAS	SI	NO	N/A	OBSERVACIONES
1) ¿Cuenta con un organigrama la institución?				
2) ¿Cuenta con un organigrama el Departamento Tecnológico?				
3) ¿Cuenta con Manual de Funciones y Responsabilidades el Departamento Tecnológico?				
4) ¿Cuántas personas conforman el Departamento Tecnológico?				
5) ¿Cada quien conoce sus funciones y responsabilidades en el Departamento Tecnológico?				
6) ¿Cómo están designadas sus funciones?				
7) ¿Cuenta con una Planificación de Mantenimientos de Equipos de Redes, Computación y Software Base?				
8) ¿Quién autoriza el servicio de mantenimiento a los equipos?				
9) ¿A quién reportan una vez realizado el mantenimiento de los equipos?				
10) ¿Cómo reportan la finalización del mantenimiento de los equipos?				
11) La solicitud de mantenimiento de los equipos en general ¿De qué manera se lo realiza?				
12) La solicitud de software base ¿De qué manera se lo realiza?				
13) ¿Tiene actualmente mantenimientos programados?				
14) ¿Qué clase de mantenimientos programados tiene?				

15) ¿Cuenta con Políticas y Procedimientos el Departamento Tecnológico?				
16) ¿Qué políticas de mantenimiento y formateos tienen para los equipos de redes?				
17) ¿Qué políticas de mantenimiento tienen para los equipos de computación?				
18) ¿Cuáles son los proveedores que tiene la institución?				
19) ¿Se lleva un control de los equipos en garantía?				
20) Cuando finaliza la garantía ¿Los equipos se integran algún programa de mantenimiento?				
21) ¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos de redes?				
22) ¿Se cuenta con un control de inventarios de todos los equipos que integran la institución?				
23) ¿Con qué frecuencia se revisa el inventario?				
24) ¿Se posee bitácoras de fallas detectadas en los equipos de redes?				
25) ¿Se posee bitácoras de fallas detectadas en los equipos de computación?				
26) ¿Se posee bitácoras de fallas detectadas en el software base?				
27) ¿Las bitácoras son llenadas por personal especializado?				
28) ¿Señala la bitácora la detección de la falla?				
29) ¿Señala la bitácora la fecha de corrección de la falla detectada?				
30) ¿Señala la bitácora la fecha de revisión en que el equipo funcione correctamente?				
31) ¿La bitácora hace referencia a hojas de servicio, en donde se detalla la falla, y las causas que la originaron, así como las refacciones utilizadas?				

32) ¿Se poseen registros individuales de los equipos?				
33) ¿Se realizan revisiones periódicas de los equipos de redes, computación y software base?				
34) ¿Cada qué tiempo se hacen estas revisiones (semanal, mensual, trimestral, anual)?				
35) ¿Mediante que metodologías planifican las revisiones de los equipos?				
36) ¿El departamento tecnológico tiene un plan de Contingencia?				
37) ¿Qué métodos de contingencia se utilizan en los mantenimientos de equipos?				
38) ¿Qué métodos de contingencia se utilizan en los formateos de los equipos en general?				
39) ¿Hacen respaldo de la información de los equipos formateados?				
40) ¿Cómo administran y guardan estos respaldos de información?				
41) ¿Existen controles de acceso a las computadoras del personal administrativo?				
42) ¿Existen controles de acceso a las redes inalámbricas de la institución?				
43) ¿Existen controles de acceso a los servidores?				
44) ¿Se llevan registros estadísticos del uso de la red?				
45) ¿Tienen algún acuerdo de servicio para el mantenimiento de las redes?				
46) ¿Quién administra las contraseñas de admisión?				
47) ¿Son abiertas las contraseñas de admisión?				
48) ¿Cada que tiempo expiran las contraseñas de admisión?				
49) ¿Se mantiene información acerca de las compañías de servicios?				
50) ¿En qué categoría se encuentran estas compañías?				

51) ¿Se ha auditado el departamento tecnológico antes?				
52) ¿Se tomaron en cuenta las conclusiones y recomendaciones sugeridas por el auditor?				

ESPAM MFL CUESTIONARIO DE CONTROL INTERNO Componente: Hardware				
ÁREA AUDITADA: Departamento Tecnológico	FECHA:			
	PERSONA AUDITADA:			
PREGUNTAS	SI	NO	N/A	OBSERVACIONES
1) ¿Se cuenta con un servicio de mantenimiento para todos los equipos en general?				
2) ¿Qué tipo de servicio de mantenimiento de equipos maneja el departamento tecnológico?				
3) ¿Con qué frecuencia se realiza el mantenimiento a los equipos de redes?				
4) ¿Con qué frecuencia se realiza el mantenimiento de equipos de computación?				
5) ¿Cuentan con un control y registro de los mantenimientos?				
6) ¿Tiene equipos con garantía de los proveedores?				
7) ¿Qué clase de garantías tienen los equipos de redes?				
8) ¿Qué clase de garantía tienen los equipos de computación?				
9) ¿El proveedor de los equipos en general realiza el mantenimiento fuera o dentro de la institución?				

10) Los equipos en garantía cuando el proveedor los lleva a realizar el mantenimiento ¿éstos van con discos duros?				
11) ¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos de redes?				
12) ¿Se tienen criterios de evaluación de los equipos de computación?				
13) ¿Qué es lo mínimo que debe tener un equipo cuando lo entregan?				
14) ¿El Departamento Tecnológico administra las bases de datos?				
15) ¿Con cuántos servidores cuenta la institución?				
16) ¿Cuántos equipos de redes hay en cada área de la institución?				
17) ¿Cuántos equipos de computación hay en cada área de la institución?				
18) En la institución ¿cuántos tipos de redes existen?				
19) ¿Qué tipo de diagramas de topologías de redes utilizan?				
20) ¿Existen accesos remotos habilitados a las redes?				
21) ¿Qué protocolos y estándares utiliza la institución para la implementación de las redes?				
22) Los medios de transmisión utilizados en las topologías de redes cuántos son por:				
Cobre				
Par Trenzado				
Fibra Óptica				

Radio				
Microondas				
VPN's				
Otros				
23) ¿Cuántas redes inalámbricas existen?				
24) ¿Cuántos puntos de acceso existen?				
25) ¿Cómo se administran las contraseñas de las redes inalámbricas?				
26) ¿Tienen seguridad las redes inalámbricas implementadas?				
27) ¿Qué tipo de seguridad tienen?				
28) ¿Qué protocolos utilizan para la seguridad de la implementación de las redes inalámbricas?				
29) ¿Qué métodos de seguridad se utilizan para la implementación de las redes inalámbricas?				
30) ¿Qué tipo de servicio externo hay para las redes implementadas en la institución?				
31) ¿Se realiza la relevación de los costos en mantenimientos de equipos en general de los últimos años?				
32) ¿Se evidencian los tiempos de mantenimiento?				
33) ¿Se realiza el seguimiento de los controles de los componentes de los equipos en general de la institución?				
34) ¿Se realiza el seguimiento a los controles de equipos que ya fueron cambiados por garantía?				

Componente: Organización de la Documentación				
ÁREA AUDITADA: Departamento Tecnológico	FECHA:			
	PERSONA AUDITADA:			
PREGUNTAS	SI	NO	N/A	OBSERVACIONES
1) ¿Qué es software base para el Departamento Tecnológico?				
2) ¿Con qué frecuencia se realiza el mantenimiento del software base?				
3) ¿Qué clase de garantía tiene el software base?				
4) ¿Se evalúa el funcionamiento del software base?				
5) ¿Cada que tiempos se actualiza el software base?				
6) ¿Qué tipos de licencias tiene la institución?				
7) ¿Cuenta la institución con licencias de estudiantes?				
8) ¿Existen licenciamientos vigentes?				
9) ¿Cuáles son los procedimientos para hacer sus actualizaciones?				
10) ¿Todos los equipos de computación tiene instalados los antivirus?				
11) ¿Con qué programas informáticos cuenta la institución para sus actividades?				

ANEXO 11
CUESTIONARIO DE LA NORMA ISO 27000 PRELIMINARES

ESPAM MFL CUESTIONARIO DE CONTROL INTERNO Componente: INVENTARIO DE ACTIVO SG. NORMA ISO 27000 Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.				
ÁREA AUDITADA: Departamento Tecnológico	FECHA:			
	PERSONA AUDITADA:			
PREGUNTAS	REF	SI	NO	OBSERVACIONES
1) ¿Cuentan con un Plan Estratégico?				
2) ¿Se llevan los inventarios de los activos en formatos físicos?				
3) ¿Se llevan el inventario de los activos en formatos electrónicos?				
4) ¿Llevar los inventarios de los activos de soporte de hardware:				
a) Equipos Móviles (Smartphone, tablets, celular, computadoras portátiles, etc.)				
b) Equipos fijos (servidores, computadoras de escritorio, portátiles, etc.)				
c) Periféricos de entrada (teclado, ratón, escáneres, cámara digital, cámara web, etc.)				
d) Periféricos de salida (monitor, audífonos, impresoras, proyector, etc.)				
e) Periféricos y dispositivos de almacenamiento (disco duro portátil, disco flexible, grabador de discos, CD, DVD, Blu-Ray, Memoria USB, etc.)				
f) Periféricos de Comunicaciones (Tarjetas USB y tarjeta PCMCIA para redes inalámbricas: WiFi, Bluetooth, GPRS, HSDPA; tarjeta USB para redes inalámbricas/inalámbricas de datos y telefonía, etc.)				

g) Tableros (de transferencia (bypass) de la unidad de energía (UPS); transferencia de salidas de energía, de transferencia automática de energía, etc.)				
h) Sistemas de control de acceso, de aire acondicionado, automático de extinción de incendios, etc.)				
5) ¿Llevan los inventarios de los activos de soporte de software?				
a) Sistemas Operativos				
b) Software de servicio, mantenimiento, administración de : servidores, sistema de redes de datos, sistemas de almacenamiento, telefonía, sistemas de UPS, etc.				
c) Paquetes de software o software base (suite de ofimática, navegador de internet, mensajería instantánea, etc.)				
6) ¿Llevan los inventarios de los activos de soporte de redes?				
a) Cable de Comunicaciones (Interfaces: RJ-45, RJ-11, etc; Interfaz: RS232, USB, etc.; Panel de conexión, toma de red o puntos, etc.)				
b) Switches				
c) Router, Firewall, Controlador de red inalámbrica, etc.				
d) Sistema de detección/prevención de intrusos (IDS/IPS), firewall de aplicaciones web, etc.				
7) ¿Existen activos o grupos de activos que no tienen custodios asignados?				

ESPAM MFL CUESTIONARIO DE CONTROL INTERNO Componente: SEGURIDAD DE LOS RECURSOS HUMANOS SG. NORMA ISO 27000 Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.				
ÁREA AUDITADA: Departamento Tecnológico	FECHA:			
	PERSONA AUDITADA:			
PREGUNTAS	REF	SI	NO	OBSERVACIONES

1) ¿Se socializan los procedimientos de mantenimiento preventivo, correctivo de los bienes: Hardware, Software y equipos de comunicación?				
2) ¿se responsabiliza al personal del mal uso y destrucción de los equipos tecnológicos asignados a su cargo?				
3) ¿El departamento tecnológico tiene delimitadas con claridad sus responsabilidades?				
4) ¿Se han establecido objetivos para el departamento tecnológico?				
5) ¿Se han definido por escrito los objetivos del departamento tecnológico?				
6) ¿El número de empleados que trabaja en el departamento de informática son los adecuados a las necesidades de este?				
7) ¿Existen conflictos en el departamento tecnológico por la carga de trabajo?				
8) La falta de cumplimiento de sus funciones es debido a:				
a) falta de personal				
b) personal no capacitado carga de trabajo excesivas				
c) por que realiza otras actividades				
d) otras razones				
9) ¿Se realiza la devolución de los activos de equipos tecnológicos del personal que finaliza su contrato de trabajo por escrito?				

ESPAM MFL CUESTIONARIO DE CONTROL INTERNO Componente: SEGURIDAD FÍSICA DEL ENTORNO SG. NORMA ISO 27000 Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.				
ÁREA AUDITADA: Departamento Tecnológico	FECHA:			
	PERSONA AUDITADA:			
PREGUNTAS	REF	SI	NO	OBSERVACIONES
1) ¿Se ubican los equipos de repuestos y soportes a una distancia prudente para evitar daños en caso de desastre que afecten las instalaciones principales?				
2) ¿se suministra y se ubica el equipo apropiado contra incendios?				
3) ¿Se realizan mantenimientos de las instalaciones eléctricas y ups?				
4) ¿Se realizan mantenimientos en los sistemas y climatización y ductos de ventilación?				
5) ¿Se adoptan controles para minimizar el riesgo de amenazas físicas, potenciales como robo, incendio, entre otras interferencias a las comunicaciones?				
6) ¿Se diseña y se aplica la protección física para trabajar en las áreas seguras?				
7) ¿Se ubican o se protegen los equipos para reducir el riesgo debido a amenazas o peligros del entorno?				
8) ¿Se monitorean las condiciones ambientales de temperatura y humedad?				
9) ¿Se tiene protección contra descargas eléctricas en las edificaciones de la institución?				
10) ¿Se disponen de filtros protectores en el suministro de energía y en las líneas de comunicación?				
11) ¿Están los equipos tecnológicos protegidos contra fallas de suministro de energía?				

12) ¿Se protege el cableado de la red contra la intersección o daño?				
13) ¿Se separan los cables de energía de los cables de red?				
14) ¿Se separan los cables de energía de los cables de red en el Data Center?				
15) ¿Se llevan las normas locales e internacionales para la implementación de las redes?				
16) ¿Se dispone de documentación, diseños/planos, y la distribución de conexiones de datos de redes inalámbricas y alámbricas?				
17) ¿Se brindan mantenimientos periódicos a los equipos y dispositivos tecnológicos de acuerdo a las especificaciones y recomendaciones del proveedor?				
18) ¿Los mantenimientos de los equipos tecnológicos únicamente los realiza el personal calificado y autorizado?				
19) ¿Se conservan los registros de los mantenimientos preventivos, correctivos o fallas relevantes o sospechosas?				
20) ¿Se establecen controles de mantenimientos programados?				
21) ¿Se llevan un registro de los mantenimientos preventivos y correctivos?				
22) ¿Se custodian los equipos y medios que se encuentran fuera de las instalaciones de la institución?				
23) ¿Se establece una cobertura adecuada de seguro para proteger los equipos que se encuentran fuera de las instalaciones de la institución?				
24) ¿Existen controles de acceso a las redes inalámbricas de la institución?				
25) ¿Existen controles de acceso a los servidores?				

26) ¿Se evalúan los dispositivos deteriorados que contengan información sensible antes de enviar a reparación?				
27) ¿Que técnicas utilizan para borrar, destruir o sobrescribir la información sensible de un equipo reutilizado?				
28) ¿Se tiene autorización previa para el retiro de cualquier equipo información o software				
29) ¿Se identifican a las personas autorizadas para el retiro de los activos de la institución?				
30) ¿Se lleva un registro cuando el equipo o activo se ha retirado o cuando se ha devuelto				

ESPAM MFL CUESTIONARIO DE CONTROL INTERNO Componente: GESTIÓN DE COMUNICACIÓN Y DE OPERACIÓN SG. NORMA ISO 27000 Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.				
ÁREA AUDITADA: Departamento Tecnológico	FECHA:			
	PERSONA AUDITADA:			
PREGUNTAS	REF	SI	NO	OBSERVACIONES
1) ¿Se documenta el proceso de respaldo y restauración de la información?				
2) ¿Se documentan las instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas?				
3) ¿Se documentan los procedimientos para el reinicio y recuperación del sistema en caso de fallas?				
4) ¿Se planifica el proceso de cambio y se realiza la prueba correspondiente?				

5) ¿Se establecen responsables y procedimientos formales de control de cambios en los equipos y software?				
6) ¿Se aprueban de manera formal los cambios propuestos?				
7) ¿Existen distribución de funciones y responsabilidades en el Departamento Tecnológico?				
8) ¿Se realizan gestiones de capacidad futura para asegurar el desempeño requerido de los servicios y sistemas informáticos?				
9) ¿Se prohíbe el uso de software no autorizado por la institución?				
10) ¿Se instalan y actualizan periódicamente software de antivirus contra código malicioso?				
11) ¿Se mantienen los sistemas operativos actualizados con las últimas versiones?				
12) ¿Existen políticas de respaldo de información el Departamento Tecnológico antes del mantenimiento?				
13) ¿Separan el área de redes con el área de mantenimiento?				
14) ¿Designan procedimientos y responsabilidades para la asistencia de equipos remotos?				
15) ¿Se realizan diseños antes de la implementación de una red?				
16) ¿Revisan alertas o fallas del sistema operativo?				
17) ¿Realizan cambios de configuración de los controles de seguridad del sistema operativo?				

ESPAM MFL

CUESTIONARIO DE CONTROL INTERNO

Componente: CONTROL DE ACCESO SG. NORMA ISO 27000

Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.

ÁREA AUDITADA: Departamento Tecnológico	FECHA:			
	PERSONA AUDITADA:			
PREGUNTAS	REF	SI	NO	OBSERVACIONES
1) ¿Se identifican y se documentan los equipos que se encuentran en las redes?				
2) ¿Se tiene documentada la identificación de los equipos que están permitidos, según la red que corresponda?				
3) ¿Se implementan procedimientos para controlar la instalación de software en sistemas operativos?				
4) ¿Se lleva un registro de auditoría de las actualizaciones de software que se realizan?				
5) ¿Se tienen restricciones de cambios de paquetes de software?				
6) ¿Se lleva un control de versiones para todas las actualizaciones de software?				

<p align="center">ESPAM MFL CUESTIONARIO DE CONTROL INTERNO Componente: CUMPLIMIENTO SG. NORMA ISO 27000 Objetivo/Ámbito: El presente checklist es con la finalidad de conocer y verificar el nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.</p>				
ÁREA AUDITADA: Departamento Tecnológico	FECHA:			
	PERSONA AUDITADA:			
PREGUNTAS	REF	SI	NO	OBSERVACIONES
1) ¿Se tienen inventariadas todas las normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y toda información que utilice la institución?				
2) ¿Se tiene conocimiento de todas las normas y leyes generales relacionadas a la gestión de datos e información electrónica?				

ANEXO 12
VERIFICACIÓN DE LA ÉTICA DEL CABLEADO DE RED



ANEXO 13

**MATRIZ GENERAL DE LOS CUESTIONARIOS DE CONTROL INTERNO
PRELIMINARES**

ESPAM MFL
CUESTIONARIO DE CONTROL INTERNO
Componente: Hardware

ÁREA AUDITADA: Departamento Te	FECHA: 12-08-2014						FECHA: 12-08-2014						FECHA: 12-08-2014						FECHA: 12-08-2014						
	PERSONA AUDITADA: Ing. Geovanny						PERSONA AUDITADA: Ing. Patricio						PERSONA AUDITADA: Ing. Juse Castro						PERSONA AUDITADA: Ing. Manuel M						
	RESPUESTAS		CUMPLIMI		OBSERVACION		RESPUESTAS		CUMPLIMI		OBSERVACION		RESPUESTAS		CUMPLIMIE		OBSERVACION		RESPUESTAS		CUMPLIMIEN		OBSERVACION		
S	N	N/A	PO ND.	CALIF.		S	N	N/A	PO ND.	CALIF.		S	N	N/A	PO ND.	CALIF.		S	N	N/A	PON D.	CALIF.			
1) ¿Se cuenta con un servicio de mantenimiento para todos los equipos en general?	x			10	0	solo la universidad	x					solo cubre la garantía de seguros de la	x						x			10	10		
2) ¿Qué tipo de servicio de mantenimiento de equipos maneja el departamento	x			10	5	preventivo, correctivo, adoptivo						no entiende la pregunta	x						Preventivo, Correctivo	x			10	5	preventivo, correctivo
3) ¿Con qué frecuencia se realiza el mantenimiento a los equipos de redes?	x			10	2,5	solo cuando hay problema se lo realiza	x					semanal	x						Cuando hay algún inconveniente	x			10	5	3 meses o cuando se lo necesita
4) ¿Con qué frecuencia se realiza el mantenimiento de equipos de computación?	x			10	2,5	cada 3 ms o cuando hay problemas		x					x						Cuando hay algún inconveniente	x			10	5	6 meses o cuando se lo requiera
5) ¿Cuentan con un control y registro de los mantenimientos?	x			10	0		x						x							x			10	0	
6) ¿Tiene equipos con garantía de los proveedores?	x			10	5	todas por 1 año	x					almacen lleva las garantías, solicitar evidencias	x							x			10	10	todas por 1 año
7) ¿Qué clase de garantías tienen los equipos de redes?	x			10	5	Lo sabe el Ing. Patricio Z.	x					por daño de fábrica, pero no todos los equipos	x						Por daño de fábrica	x			10	10	por defecto
8) ¿Qué clase de garantía tienen los equipos de computación?	x			10	5	daño de fábrica	x					por daño de fábrica	x						Por daño de fábrica	x			10	10	daño de fábrica
9) ¿El proveedor de los equipos en general realiza el mantenimiento fuera o dentro de la institución?	x			10	0	cuando es falla mayor s lo envía al proveedor	x					se envía al proveedor, pero en el caso de las impresoras vienen a la institución	x						No se lo realiza dentro de la institución	x			10	0	

10) Los equipos en garantía cuando el proveedor los lleva a realizar el mantenimiento ¿éstos van con discos duros?	x		10	2,5	solamente la parte dañada se llevan para el mantenimiento	x				todos van completos	x				Van Completos	x		10	5	completos
11) ¿Se tienen criterios de evaluación para determinar el rendimiento de los equipos de redes?	x		10	0	funcionalidad solamente	x				solo de funcionalidad	x					x		10	0	funcionalidad solamente
12) ¿Se tienen criterios de evaluación de los equipos de computación?	x		10	0		x				almacen lo lleva	x					x		10	0	funcionalidad
13) ¿Qué es lo mínimo que debe tener un equipo cuando lo entregan?	x		10	5	office, PDF, encarta, traductor	x				teclado, parlantes, monitor, case, mouse	x				Teclado, mouse, monitor, case	x		10	5	de acuerdo a las necesidades del departamento
14) ¿El Departamento Tecnológico administra las bases de datos?	x		10	0	Lo administra Informática	x				lo administra informática	x					x		10	0	
15) ¿Con cuántos servidores cuenta la institución?	x		10	5	4 o 5 lo sabe el Ing. César Moreira	x				8 servidores internos, lo maneja el Ing. César se llevan registro, evidencia para 19-08-	x				No recuerda la cantidad	x		10	5	8 servidores
16) ¿Cuántos equipos de redes hay en cada área de la institución?	x		10	2,5	Bastantes, sin registros	x				lo lleva el almacén	x				Algunos, no recuerda la cantidad	x		10	5	Bastantes, sin registros
17) ¿Cuántos equipos de computación hay en cada área de la institución?	x		10	2,5	Bastantes, sin registros	x				inalámbrica guiada y no guiada	x				Lo lleva el almacén la cantidad de	x		10	5	Bastantes, sin registros
18) En la institución ¿cuántos tipos de redes existen?	x		10	5	LAN, wireless	x				estrella extendida, anillo	x				2 inalámbrico y por cable	x		10	10	2 tipos
19) ¿Qué tipo de diagramas de topologías de redes utilizan?	x		10	5	Anillo, estrella, estrella extendida	x				acceso remoto solo a los	x				Estrella	x		10	10	Anillo, estrella, estrella extendida
20) ¿Existen accesos remotos habilitados a las redes?	x		10	5	El Ing. Patricio Zambrano	x				IPv4	x				Desconoce	x		10	10	
21) ¿Qué protocolos y estándares utiliza la institución para la implementación de las	x		10	5	TCP/IP, WPA2	x									IPv4	x		10	10	ip v4
22) Los medios de transmisión utilizados en las topologías de redes cuántos son	x		10	2,5	Lo lleva el Ing. Patricio Zambrano											x		10	5	

33) ¿Se realiza el seguimiento de los controles de los componentes de los equipos en general de la institución?	x		10	0		x				solo el funcionamiento	x				Se revisa y si es para cambiar se lo hace	x		10	0
34) ¿Se realiza el seguimiento a los controles de equipos que ya fueron cambiados por garantía?	x		10	0	lo lleva el almacén	x				no hay control físico, lo lleva el almacén	x					x		10	5 sin evidencia

ESPAM MFL
CUESTIONARIO DE CONTROL INTERNO
Componente: Software

ÁREA AUDITADA: Departamento T	FECHA: 12-08-2014						FECHA: 12-08-2014						FECHA: 12-08-2014						FECHA: 12-08-2014																	
	PERSONA AUDITADA: Ing. Patricia												PERSONA AUDITADA: Ing. José Carlos												PERSONA AUDITADA: Ing. Manuel M											
	RESPUESTAS						CUMPLIMIENTO						OBSERVACION						RESPUESTAS						CUMPLIMIENTO						OBSERVACION					
PREGUNTAS	S	N	N/A	PON.	CALIF.	OBSERVACION	S	N	N/A	PON.	CALIF.	OBSERVACION	S	N	N/A	PON.	CALIF.	OBSERVACION	S	N	N/A	PON.	CALIF.	OBSERVACION												
	1) ¿Qué es software base para el Departamento Tecnológico?	x			10		5	Office, windows 7 y 8, pero más al 7	x						sistemas operativos windows 7 u 8 solamente	x						Office, antivirus, reproductor	x				10	10	Office, antivirus, archivo pdf, driver winrar							
2) ¿Con que frecuencia se realiza el mantenimiento del software base?	x			10	0	solo cuando hay fallas	x					cuando hay problemas	x					Cuando se lo requiera.	x			10	0	solo cuando lo amerita												
3) ¿Qué clase de garantía tiene el software base?	x			10	5	un año por fábrica	x					licencias	x					Por defecto de fábrica	x			10	10	solo office que son con licencias												
4) ¿Se evalúa el funcionamiento del software?	x			10	2,5	por año pero no se lleva	x					solo cuando se instala	x						x			10	0													
5) ¿Cada que tiempos se actualiza el software base?	x			10	5	cada año	x						x					Cuando viene una	x			10	0	solo cuando existe												
6) ¿Qué tipos de licencias tiene la institución?	x			10	5	solo para la institucion	x					licencias corporativas	x						x			10	5	microsoft licencias												
7) ¿Cuenta la institución con licencias de estudiantes?	x			10	0		x					se facilita para los	x						x			10	0													
8) ¿Existen licenciamientos vigentes?	x			10	5	solo de antivirus no hay licencias.	x						x						x			10	10													
9) ¿Cuáles son los procedimientos para hacer sus actualizaciones?	x						x					solo por llamadas telefónicas	x						x			10	0	por medio del internet												
10) ¿Todos los equipos de computación tiene instalados los antivirus?	x						x					pero no todos los equipos	x						x			10	10													
11) ¿Con qué programas informáticos cuenta la institución para sus actividades?	x					office, encarta, pdf, traductor	x					office, PDF, winrar	x					Office, antivirus, PDF	x			10	5	office, encarta, pdf, traductor												

ANEXO 14
ENCUESTA REALIZADA AL PERSONAL QUE LABORA EN LA ESPAM
MFL

ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ
ENCUESTA DE CONTROL INTERNO A LOS CUSTODIOS DE LOS EQUIPOS TECNOLÓGICOS
Calceta-Bolívar-Manabí

1.- ¿CUÁNTOS EQUIPOS TECNOLÓGICOS TIENE A SU CARGO?

COMPUTADORAS 20
IMPRESORAS 0
UPS 0

ENTRE OTROS (Especifique): _____

1. ¿Qué es el mantenimiento preventivo?

Es el conjunto de intervenciones realizadas de forma periódica en una maquina o instalación, con la finalidad de optimizar su funcionamiento y evitar daños imprevistos.

2.- ¿LES HAN REALIZADO MANTENIMIENTO PREVENTIVO A SUS EQUIPOS TECNOLÓGICOS?

SI NO

En caso de que la respuesta sea SI cada que tiempo se lo realiza:

Semanal Semestral
Trimestral Anual

El tiempo en que tarda el mantenimiento es:

Mucho tiempo Poco tiempo
Lo esperado para continuar con sus actividades

En caso de que la repuesta sea NO:

Nunca Casi Nunca

¿Qué es el mantenimiento correctivo?

Es el que se realiza luego que ocurra una falla o avería en el equipo que por su naturaleza no pueden planificarse en el tiempo, presenta costos por reparación y repuestos no presupuestadas, pues implica el cambio de algunas piezas del equipo.

3.- ¿LES HAN REALIZADO MANTENIMIENTO CORRECTIVO A SUS EQUIPOS TECNOLÓGICOS?

SI NO

En caso de que la respuesta sea SI el tiempo que toma para la entrega es:

En el mismo momento Al mes
Al día siguiente Cuando el técnico lo disponga

En caso de que la repuesta sea NO:

Nunca Casi Nunca
Cuando el equipo lo requiera

4.- ¿CÓMO SE REALIZA LA SOLICITUD DE MANTENIMIENTO SEA PREVENTIVO O CORRECTIVO?

- POR LLAMADA TELEFÓNICA
 POR CORREO ELECTRÓNICO
 POR OFICIO
 OTRO MEDIO

ANEXO 15
CD QUE CONTIENE EL INVENTARIO DE LOS EQUIPOS TECNOLÓGICOS

ANEXO 16

VERIFICACIÓN DEL MANTENIMIENTO DE LOS EQUIPOS TECNOLÓGICOS



ANEXO 17

MEMORANDO DE PLANIFICACIÓN PRELIMINAR

AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL

MEMORANDO DE INVESTIGACIÓN PRELIMINAR

1. ANTECEDENTES

El departamento tecnológico es el responsable del proceso de control y del proceso de mantenimiento de la infraestructura tecnológica de la ESPAM MFL, y se centra especialmente en asegurar que los servicios cumplan con los niveles acordados, y que, todas las actividades del día a día dedicadas a estos dos procesos, aseguren que los servicios brindados se están prestando con normalidad y cumplan con las normativas de ley y buenas prácticas en tecnologías de información.

La misión del departamento es proveer y administrar los servicios informáticos, comunicaciones e implantación de la infraestructura tecnológica necesaria para coadyuvar al desarrollo tecnológico de la Escuela.

1.1. PRODUCTOS Y SERVICIOS

- Plan de desarrollo informático.
- Informe de la ejecución del plan informático.
- Plan de mantenimiento preventivo y correctivo de software y hardware.
- Informe de ejecución de software y hardware.
- Asesoría en la adquisición de equipos y paquetes informáticos.
- Informe de configuración de sistema de redes y telecomunicaciones.

OBSERVACIÓN:

En el Manual de Funciones se muestra un organigrama como Jefatura de Computo, en el cual se pudo observar que no existe concordancia alguna con el orgánico institucional, por lo que se llegó a la conclusión de proponer un

nuevo orgánico funcional para el departamento tecnológico realizado por las autoras.

2. MOTIVO DE LA AUDITORÍA

La Auditoría al Control y Mantenimiento de la Infraestructura Tecnológica del Departamento Tecnológico de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, se llevó a efecto como propuesta de tema de tesis que las autoras plantearon, la misma que tuvo autorización del ingeniero Leonardo Félix López, Rector de la ESPAM MFL, mediante el oficio N°: ESPAM MFL –CI – 2014 – 179 – OF, y la autorización del tribunal de tesis mediante el oficio S/N. de fecha 16 de mayo de 2014.

3. OBJETIVOS DE LA TESIS

- Verificar el grado de cumplimiento al mantenimiento y control de la infraestructura tecnológica de acuerdo a la Norma de TI 410-09 y la Norma ISO 27000.
- Relevar riesgos de Tecnologías de Información.
- Identificar las áreas que carezcan de normatividad.
- Verificar el nivel de cumplimiento de políticas, planes y procedimientos que emplea el Departamento Tecnológico en cuanto al uso de los recursos tecnológicos.
- Emitir el informe de auditoría de la infraestructura tecnológica tomando en cuenta todos los hallazgos recopilados.

4. ALCANCE DEL EXAMEN

El alcance que tiene esta auditoría será sobre la evaluación del Control y Mantenimiento de la Infraestructura Tecnológica del Departamento Tecnológico y abarcará:

- Equipos de comunicación, equipos de computación e infraestructura de redes, Licenciamientos de software base.

- Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios son registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones son registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.
- Control y registro de las versiones del software que ingrese a producción.
- Se verificará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en la función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.
- Se verificará el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.
- El mantenimiento de los bienes que se encuentren en garantía.

5. RESTRICCIÓN

- No abarcará al Departamento de Almacén en sus procesos y procedimientos adquisitivos, reposo y baja de recursos tecnológicos.
- Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.

- Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.
- Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementaran medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.

6. CONOCIMIENTO DE LA ENTIDAD

6.1. BASE LEGAL

El Departamento Tecnológico es un Departamento dependiente de la Dirección de la máxima autoridad, encargada de la supervisión de todas las actividades informáticas y generales que se realizan en la institución, cuya misión es proveer y administrar los servicios informáticos, comunicaciones e implantación de la infraestructura tecnológica necesaria para coadyuvar al desarrollo tecnológico de la Escuela.

Atendiendo lo dispuesto la suscrita Secretaria General-Procuradora de la Escuela Superior Politécnica Agropecuaria de Manabí, Manuel Félix López, ESPAM MFL, certifica: que el presente Estatuto Orgánico de Gestión Organizacional por Procesos, fue discutido y aprobado por el Honorable Consejo Politécnico en dos sesiones extraordinarias de fechas: 11 y 16 de enero del 2012.

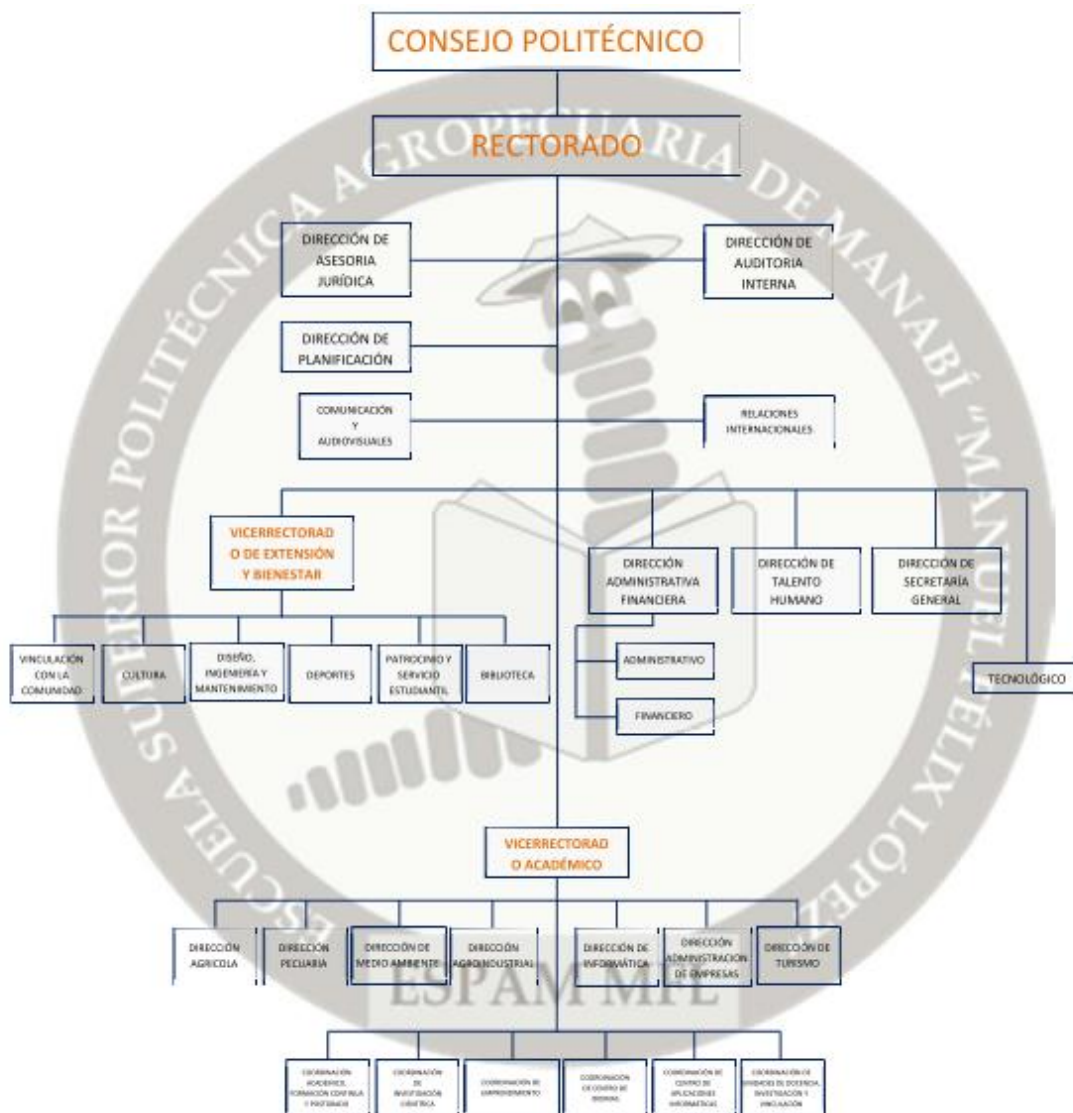
Con fecha del 17 de enero del 2012 lo certifica la Mg P.E.S Lya Villafuerte Vélez, Secretaria General, **ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ.**

6.2. DISPOSICIONES LEGALES

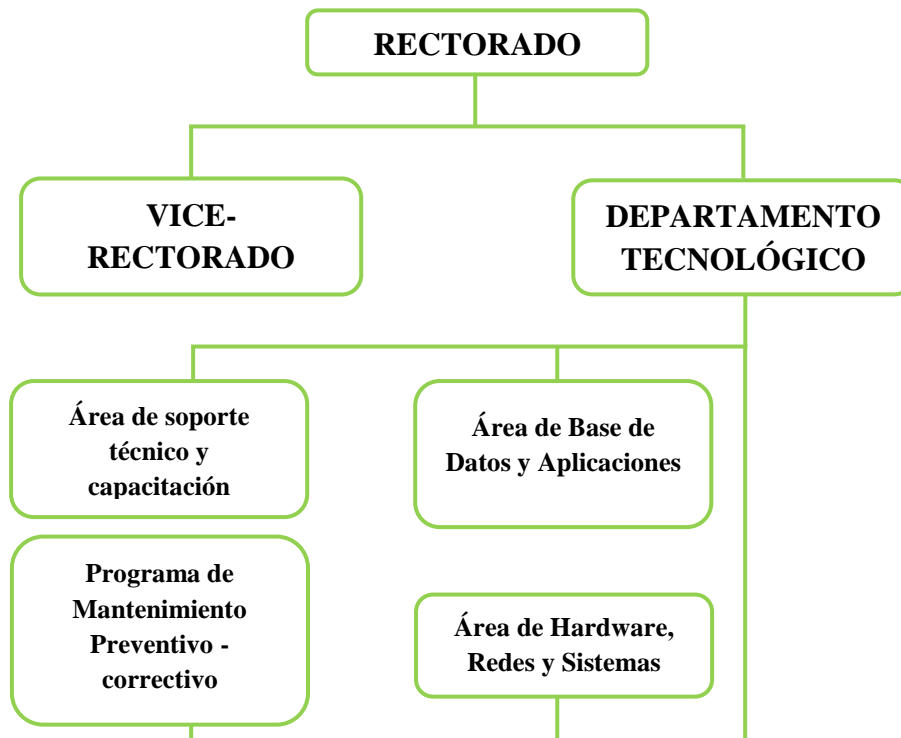
- Ley de Educación Superior.
- Estatuto de la ESCUELA SUPERIOR POLITÉCNICA DE MANABÍ
- Plan de Desarrollo de la Politécnica.
- Normas de control interno - Normas de control interno para el área de sistemas de información computarizados. Norma 410 de Tecnologías de información.

6.3. ESTRUCTURA ORGÁNICA.

a) ESTRUCTURA ORGÁNICA DE LA ESPAM MFL



b) ESTRUCTURA ORGÁNICA DEL DEPARTAMENTO



6.4. PERSONAL LABORAL

PERSONAL QUE INTEGRA EL DEPARTAMENTO TECNOLÓGICO	
NOMBRE	OCUPACIÓN
ING. GEOVANNY GARCÍA	JEFE DEL DEPARTAMENTO TECNOLÓGICO
ING. PATRICIO ZAMBRANO	ANALISTA DE CÓMPUTO
ING. JUAN CARLOS MUÑOZ	ASISTENTE DE CÓMPUTO 1
ING. MANUEL DE JESÚS MACÍAS	ASISTENTE DE CÓMPUTO 2

6.5. DE ACUERDO CON LA MISIÓN DE LA ESPAM MFL , LOS REQUERIMIENTOS INFORMÁTICOS DE LA INSTITUCIÓN SON:

- Disponer de una cantidad óptima de computadoras y servicios informáticos.
Destinar al máximo las computadoras a actividades docentes, administrativas, servicios y fines productivos.
- Mantener un aprovechamiento óptimo de las computadoras y servicios.

6.6. . OBJETIVOS

a) DE ACUERDO CON LOS REQUERIMIENTOS LOS OBJETIVOS GENERALES

- Mantener un sistema óptimo de atención y capacitación permanentes para el usuario (estudiante, docente, empleado), apoyado por un servicio técnico.
- Mantener un sistema óptimo de procesos de información, sostenido adecuadamente por una base de datos institucionales, un conjunto de aplicaciones y un conjunto de protocolos y normas.
- Mantener un conjunto de herramientas informáticas, organizado como una red de hardware y software de sistemas.

b) OBJETIVOS DE MANTENIMIENTO

- Ampliar la vida útil y mantener en óptimo estado los equipos tecnológicos.
- Tener en perfectas condiciones de operatividad en los equipos tecnológicos.
- Disminuir costos, aumentar la eficiencia y eficacia en el soporte tecnológico de los equipos.
- Realizar y mantener el inventario actualizado de los equipos tecnológicos.

6.7. POLÍTICAS

Los recursos informáticos centrales son administrados por el Jefe del departamento. Los recursos informáticos del Campus son administrados por el asistente, bajo las directivas establecidas por el Departamento Tecnológico.

La designación y asignación de nombres de dominio, identificadores de red y direcciones es competencia exclusiva del Departamento Tecnológico.

La representación digital de la información institucional y la especificación de las reglas de nomenclatura es de competencia y responsabilidad exclusivas del Departamento Tecnológico.

El sistema informático es un solo conjunto de recursos organizados en una red de control centralizado y arquitectura distribuida, permitiendo la coexistencia coordinada y regulada de sistemas informáticos propios de las unidades de gestión.

Todo recurso informático de o en la Universidad será asignado a un responsable directo, parte de una cadena de mando o responsabilidad.

Toda herramienta desarrollada dentro de la institución será de arquitectura abierta, con código fuente y documentación públicamente disponibles, sin perjuicio del reconocimiento de autoría individual y de equipo.

Se respetarán plenamente los derechos de propiedad intelectual, licenciamiento y autoría de cualquier recurso informático.

Se garantizará la seguridad de la información individual y colectiva, regulando el acceso de acuerdo a la propiedad y la necesidad institucionales.

Toda contratación, instalación y adquisición de recursos informáticos deberá gestionarse a través del Departamento Tecnológico, la cual establecerá mecanismos expeditivos, bajo los criterios de costo/beneficio, planificación anual/semestral indicada en el POA.

La cantidad y calidad de los recursos disponibles se fijará anualmente y revisará semestralmente constituyendo del Nivel de Servicios acordado, documentándose de manera accesible su uso y acceso.

El recurso humano especializado es el valor más importante del sistema informático y como tal debe ser estimulado con especializaciones y cursos en medida justa y proporcional a su contribución.

6.8. MISIÓN

Proveer y administrar los servicios informáticos, comunicaciones e implantación de la infraestructura tecnológica necesaria para coadyuvar al desarrollo tecnológico de la Escuela.

a) PRODUCTOS Y SERVICIOS

- Plan de desarrollo informático.
- Informe de la ejecución del plan informático.
- Plan de mantenimiento preventivo y correctivo de software y hardware.
- Informe de ejecución de software y hardware.
- Asesoría en la adquisición de equipos y paquetes informáticos.
- Informe de configuración de sistema de redes y telecomunicaciones.

6.9. DESCRIPCIÓN ESTRUCTURAL DEL DEPARTAMENTO TECNOLÓGICO

El departamento Tecnológico, se encuentra ubicada en el Campus Politécnico, km 2.7 vía Calceta – El Morro – El Limón, Manabí, Ecuador, actualmente cuenta con una Jefe del Departamento Tecnológico, el que posee como dependencia a Mantenimiento preventivo-Correctivo de HARDWARE, Mantenimiento preventivo-correctivo de software, Mantenimiento preventivo-correctivo de redes y telecomunicaciones y al Data-Center, el departamento internamente cuenta con un organigrama estructural definido legalmente y por ende con un manual de funciones pero con el nombre anterior de JEFATURA DE COMPUTO, los cuales se han tomado como referencia para realizar sus objetivos, organigrama y misión del departamento.

La edificación del departamento tecnológico que poseen actualmente se encuentra ubicada a lado de las oficinas de FEPAM, es un lugar pequeño que laboran temporalmente hasta su pronta reubicación.

6.10. FUNCIONES Y ACTIVIDADES QUE REALIZA EL DEPARTAMENTO TECNOLÓGICO

FUNCIONES	
GENERALES	ESPECÍFICAS
a) Planificar, dirigir, organizar, evaluar y coordinar las actividades informáticas de la Universidad, de acuerdo con el Plan Estratégico y el Plan Operativo vigentes.	a) Supervisar las actividades de los asistentes del Centro de Cómputo
b) Planificar, implementar, dirigir y supervisar los sistemas relacionadas en las áreas académicas y administrativas	b) Comunicar al Centro de Cómputo con las Direcciones Departamentales y de Carrera
c) Asegurar la provisión de servicios directos para el usuario (directivos, docentes, estudiantes, empleados), incluyendo el análisis y evaluación de requerimientos	c) Dar a conocer las necesidades anuales de equipos informáticos (Hardware y Software)
d) Asegurar la provisión de procesos y aplicaciones de acceso al sistema de información y la base de datos institucionales.	d) Evaluar regularmente los indicadores de gestión del Centro de Cómputo.
e) Asegurar la provisión de infraestructura informática y telemática organizada en una red interconectada con acceso a Internet.	

Es función del **Área de Soporte Técnico y Capacitación**: Asegurar la provisión de servicios directos para el usuario, incluyendo el análisis y evaluación de requerimientos.

Es función del **Área de Base de Datos y Aplicaciones**: Asegurar la provisión de procesos y aplicaciones de acceso al sistema de información y la base de datos institucionales.

Es función del **Área de Hardware, Redes y Sistemas**: Asegurar la provisión de infraestructura informática y telemática organizada en una red interconectada con acceso a Internet.

Son funciones del **Área de Capacitación**: Diseñar, desarrollar y distribuir módulos de capacitación en tecnología de información para los distintos niveles de usuario en todas las modalidades que sean apropiadas.

Son funciones del Área de diseño Web: (a) Diseñar, desarrollar y mantener los canales de comunicación, incluyendo el portal web. (b) Desarrollar, diseñar y producir materiales de comunicación audiovisual en medio digital.

Son funciones del **Programa de Mantenimiento Preventivo - correctivo**: Revisar periódicamente los equipos informáticos incorporados al plan de mantenimiento, efectuando las acciones técnicas necesarias a nivel de hardware, software y redes y telecomunicaciones, para reducir la probabilidad de falla y aumentar el grado de utilización de los equipos. Y atender, diagnosticar y resolver los requerimientos originados en fallas de los equipos informáticos, tanto a nivel de hardware como de software y como de redes y telecomunicaciones.

6.10.1. FUNCIONES ESPECÍFICAS DE LOS CARGOS

Son funciones del Jefe de Tecnología: Planificar, dirigir, organizar, evaluar y coordinar las actividades informáticas del Departamento Tecnológico. Los asistentes en las áreas reportan al Jefe del departamento.

Es función del asistente del Área de Soporte Técnico y Capacitación: Asegurar la provisión de servicios directos para el usuario, incluyendo el análisis y evaluación de requerimientos.

Es función del asistente del Área de Base de Datos y Aplicaciones: Asegurar la provisión de procesos y aplicaciones de acceso al sistema de información y la base de datos institucionales.

Es función del asistente del Área de Hardware, Redes y Sistemas: Asegurar la provisión de infraestructura informática y telemática organizada en una red interconectada.

6.10.2. ACTIVIDADES QUE SE REALIZARÁN EN EL DEPARTAMENTO TECNOLÓGICO

- Instalar y supervisar las redes y cableado estructurado informático de la institución.

- Evaluar y reparar los equipos, periféricos, cableados y conexiones afines a los equipos de cómputo de la institución.
- Instalar, supervisar y realizar mantenimiento de los sistemas de seguridad física para los equipos de la institución.
- Administrar las redes existentes en la institución, así como la sala de servidores, esto incluye los permisos de acceso a los sistemas por parte de los servidores y redes externas a la institución, Servidores de correo y base de datos institucionales.
- Brindar asistencia técnica ante problemas eventuales de software y hardware.
- Coordinar y supervisar la renovación en la tecnología informática utilizada en la institución.
- Coordinar con los proveedores la atención a los equipos bajo garantía.
- Participar en el programa de adquisición de equipos institucional
- Elaborar, coordinar y supervisar el programa de mantenimiento preventivo y correctivo de los equipos informáticos de la institución.
- Administrar el stock de herramientas, accesorios, cables y repuestos que son utilizados para cumplir con su servicio
- Registrar en una base de datos las características y ubicación de los equipos asignados.
- Participar en la elaboración de la normatividad informática de la institución.
- Administrar una biblioteca que incluya el control de los manuales de hardware y software, libros especializados, licencias y diskettes, cintas, CDs y similares de todo el software y hardware adquirido por la institución.

7. PUNTOS DE INTERÉS PARA LA AUDITORÍA

Determinar el control y mantenimiento de la infraestructura tecnológica mediante la aplicación de normas de control interno y la norma ISO 27000.

Se tomó como referencia los dos últimos años (2012-2013) para las evaluaciones pertinentes.

8. IDENTIFICACIÓN DE LOS COMPONENTES A SER EXAMINADOS EN LA PLANIFICACIÓN ESPECÍFICA

Los componentes a evaluar son:

- DOCUMENTACIÓN
- HARDWARE
- SOFTWARE
- INVENTARIO DE ACTIVOS
- SEGURIDAD DE LOS RECURSOS HUMANOS
- SEGURIDAD FÍSICA DEL ENTORNO
- GESTIÓN DE COMUNICACIÓN Y OPERACIÓN
- CONTROL DE ACCESO
- CUMPLIMIENTO

ANEXO 18
PROGRAMA ESPECÍFICO DE AUDITORÍA

DEPARTAMENTO TECNOLÓGICO ESPAM MFL			
AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ			
PROGRAMA GENERAL PARA LA PLANIFICACIÓN ESPECIFICA			
N°	OBJETIVOS:	REFERENCIA	ELABORADO POR:
	<p>Evaluar el cumplimiento de las normas control interno a la entidad, verificando sus puntos fuertes y débiles.</p> <p>Determinar el nivel de riesgo y confianza de las normas de control interno del Departamento Tecnológico</p> <p>Evaluar el cumplimiento de la norma ISO a la entidad, verificando sus puntos fuertes y débiles.</p> <p>Determinar el nivel de riesgo y confianza de las normas de ISO del Departamento Tecnológico</p>		
PROCEDIMIENTOS			
	<p>Desarrollar cuestionarios de control interno para los componentes determinados en la planificación preliminar (Documentación, Hardware y Software).</p>		
1	<p>Aplicar cuestionarios de la norma de control interno, a los responsables del Departamento Tecnológico y sus colaboradores.</p>	P.T. 06	Las autoras
	<p>Evaluar el cumplimiento de la norma de control interno.</p>	P.T. 06	Las autoras
	<p>Elaborar las matrices de riesgo confianza por cada componente de la norma de control interno y para los responsables y sus colaboradores.</p>	P.T. 07	Las autoras
	<p>Elaborar las matrices de riesgo confianza de la norma de control interno de todos los involucrados al departamento de manera general.</p>	P.T. 08	Las autoras
2	<p>Elaborar hallazgos de auditoría, según la evaluación de la norma de Control Interno.</p>	P.T. 09	Las autoras



	<p>Desarrollar cuestionarios de control interno para los componentes determinados en la planificación preliminar (Inventario de Activos, Seguridad de Recursos Humanos, Gestión de Comunicación y Operación, Seguridad Física del Entorno, Control de Acceso, Cumplimiento).</p>		
1	<p>Aplicar cuestionarios de los componentes de la norma ISO 27000, a los responsables del Departamento Tecnológico y sus colaboradores.</p>	P.T. 10	Las autoras
	<p>Evaluar el cumplimiento de los componentes de la norma ISO 27000.</p>	P.T. 10	Las autoras
2	<p>Elaborar las matrices de riesgo confianza por cada componente de la norma ISO 27000 y para los responsables y sus colaboradores.</p>	P.T. 11	Las autoras
3	<p>Elaborar las matrices de riesgo confianza de la norma ISO 27000 de todos los involucrados de manera general.</p>	P.T. 12	Las autoras
4	<p>Elaborar hallazgos de auditoría, según la evaluación de la norma ISO 27000.</p>	P.T. 13	Las autoras
5	<p>Dialogar con el Jefe del Departamento Tecnológico sobre los resultados de la planificación preliminar.</p>	P.T. 13	Las autoras
6	<p>Preparar un Memorando de Planificación Específica con el resultado del trabajo, las conclusiones alcanzadas y los comentarios acerca de la solidez y/o debilidades de la norma de control interno que requieren tomar una acción inmediata o puedan ser puntos apropiados para el informe final con sus conclusiones y recomendaciones.</p>	P.T. 14	Las autoras

ANEXO 19
MEMORANDO DE ANÁLISIS INICIAL ESPECÍFICO DIRIGIDO AL JEFE DEL
DEPARTAMENTO TECNOLÓGICO

AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ

MEMORANDO DE ANÁLISIS INICIAL ESPECÍFICO

1. REFERENCIA DE LA PLANIFICACIÓN PRELIMINAR

La planificación preliminar a la Carrera Informática de la ESPAM MFL, de la ciudad de Calceta, se entregó el 16 de Diciembre de 2014 en la que se estableció el enfoque de la auditoria para la planificación específica; como se observó que en la planificación preliminar, mediante respuesta de oficios la entidad no cuenta con lineamientos generales respecto al control y mantenimiento de la infraestructura tecnológica.

2. CUESTIONARIOS INICIALES

Se aplicaron los diferentes cuestionarios a las personas que trabajan dentro del Departamento Tecnológico, la sucesión de preguntas están realizadas en una matriz general con el fin de medir el nivel de cumplimiento de normas políticas y procedimientos dentro de las mismas y a su vez si el personal está informado de todo lo que rodea al Departamento Tecnológico.

Los procesos que se trabajaron en los diferentes cuestionarios están estructurados de la siguiente forma: poseen una ponderación de diez puntos para cada una de las preguntas y la calificación que las autoras le asignaron está basada dentro de un rango de puntuación (0 – 10), donde, 0 significa que dicho proceso no se cumple, 5 significa que el proceso se cumple en un 50% y 10 establece que los procedimientos se cumple en su totalidad, es decir en un 100%, dicho rango de puntuación está fundamentado en el criterio de las autoras de esta auditoría, en base a las respuestas y evidencias obtenidas por parte de cada uno de los entrevistados del Departamento Tecnológico.

Una vez aplicados los cuestionarios de control interno, las autoras procedieron a realizar la matriz de determinación del riesgo – confianza por cada uno de los entrevistados en el Departamento Tecnológico, la misma que inicia con la siguiente fórmula definida en el Manual General de Auditoría.

$$CP = \frac{CT*100}{PT}$$

CP: Calificación Porcentual

PT: Ponderación Total

CT: Calificación Total

Para obtener la calificación porcentual (CP), se multiplicó la calificación total (CT) por 100 y se dividió para la ponderación total (PT).

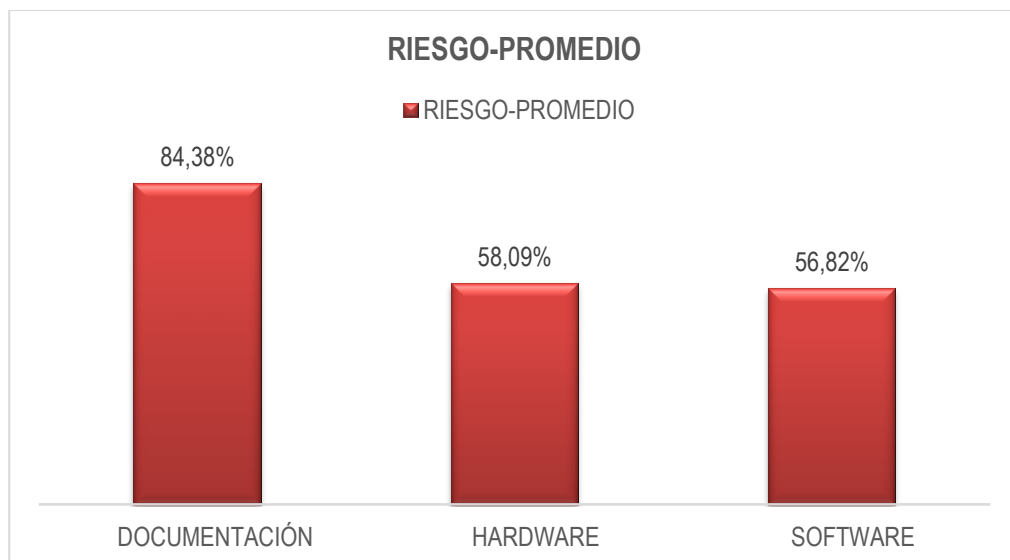
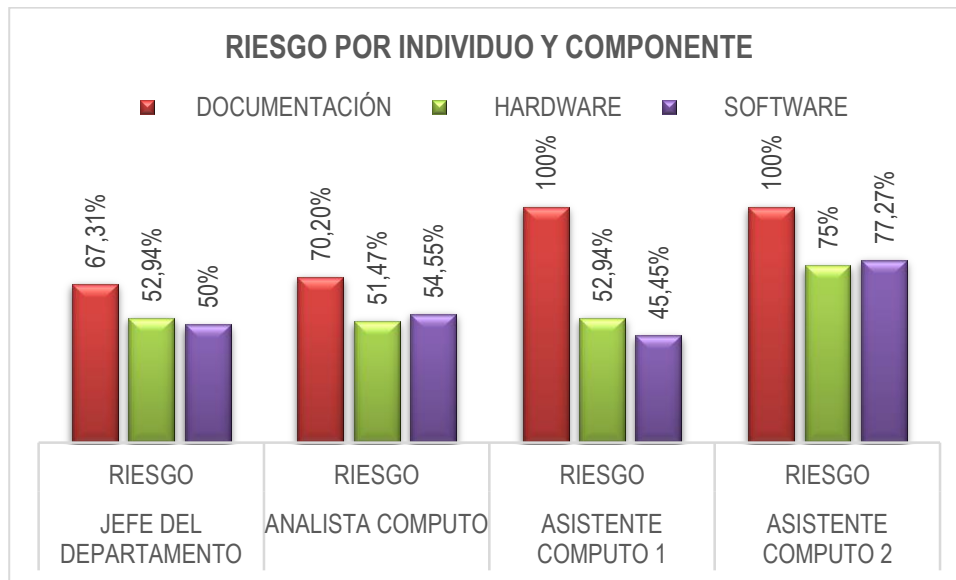
La calificación porcentual, permitió identificar el grado de confianza y nivel de riesgo por cada componente examinado, asignando un tipo de color en cada nivel, de acuerdo a la siguiente tabla de calificación (Loor y Espinoza, 2014).

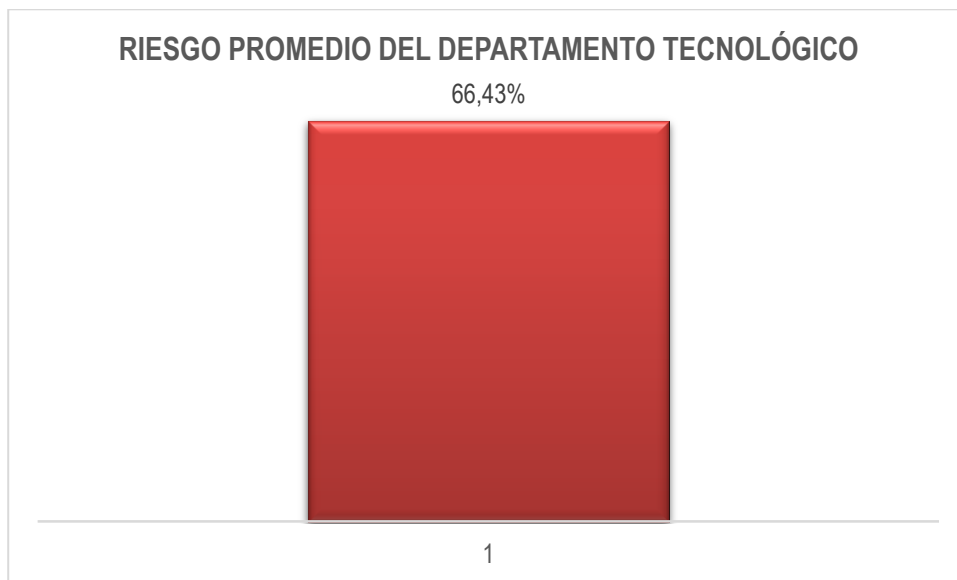
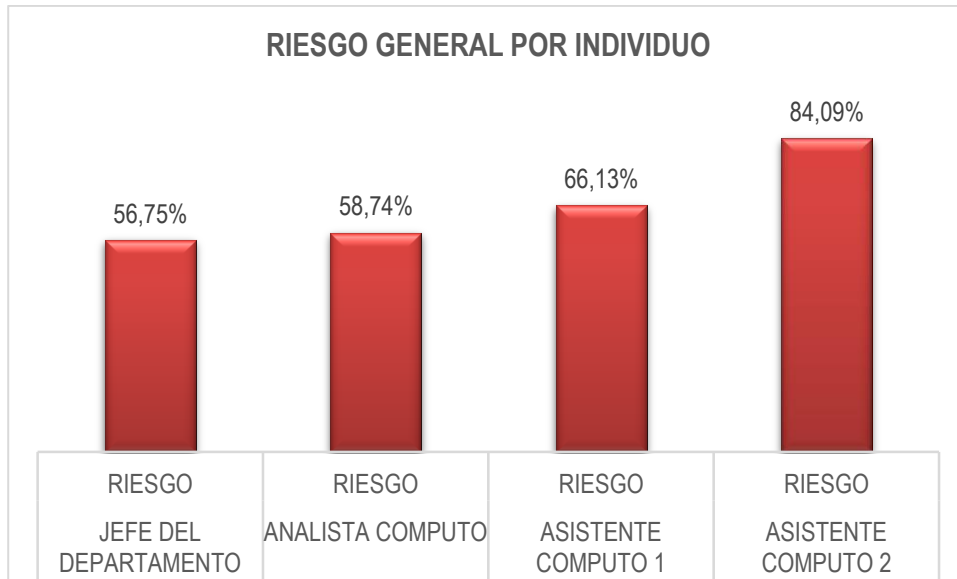
CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLORES
15 – 50	BAJO	ALTO	ROJO
51 – 75	MODERADO	MODERADO	AMARILLO
76 - 95	ALTO	BAJO	VERDE

Este cuadro muestra la calificación porcentual, grado de confianza, nivel de riesgo y los diferentes colores con los cuales nos permite identificar cada rango. De 15% a 50% muestra un grado de confianza BAJO y un nivel de riesgo ALTO identificándose con el color ROJO; de 51% a 75% muestra un grado de confianza MODERADO y un nivel de riesgo ALTO identificándose con el color AMARILLO; de 76% a 95% un grado de confianza BAJO y un nivel de riesgo BAJO identificándose con el color verde.

3. RESULTADO DE LA EVALUACIÓN DE CONTROL INTERNO

MATRIZ RIESGO-CONFIANZA CONTROL INTERNO					
TEMA	JEFE DEL DEPARTAMENTO	ANALISTA COMPUTO	ASISTENTE COMPUTO 1	ASISTENTE COMPUTO 2	RIESGO PROMEDIO DEL DEPARTAMENTO TECNOLÓGICO
	RIESGO	RIESGO	RIESGO	RIESGO	
CONTROL INTERNO	56,75%	58,74%	66,13%	84,09%	66,43%
DOCUMENTACIÓN	67,31%	70,20%	100%	100%	84,38%
HARDWARE	52,94%	51,47%	52,94%	75%	58,09%
SOFTWARE	50%	54,55%	45,45%	77,27%	56,82%





3.1. DESCRIPCIÓN DE LOS GRÁFICOS

Dentro de los porcentajes de la matriz riesgo confianza se observa que el Departamento Tecnológico en la evaluación de las normas de Control Interno dio como resultado: sobre el componente Documentación el Jefe del Departamento tiene un nivel de riesgo de 67,31%, el Analista de Computo tiene un nivel de riesgo de 70,20%, el Asistente de Computo 1 tiene un nivel de riesgo de 100,00% , el Asistente de Computo 2 tiene un nivel de riesgo de 100,00% , y el riesgo promedio es de 84,38%; sobre el componente de Hardware el Jefe del Departamento tiene un nivel de riesgo es de 52,94%, el Analista de Computo tiene un nivel de riesgo es de 51,47%, el Asistente de

Computo 1 tiene un nivel de riesgo es de 52,94%, el Analista de Computo 2 tiene un nivel riesgo es de 75,00%, y el riesgo promedio es de 58,09%; sobre el componente de Software el Jefe del Departamento tiene un nivel de riesgo es de 50%, el Analista de Computo tiene un nivel de riesgo de 54,55%, el Asistente de Computo 1 tiene un nivel de riesgo de 45,45%, el Asistente de Computo 2 tiene un nivel de riesgo es de 77,27%, y el riesgo promedio es de 56,82%.

De manera general el departamento tecnológico cuenta con unos porcentajes de nivel de confianza y el riesgo por colaborador y por departamento como tal, el Jefe del Departamento tiene un nivel de riesgo de 56,75%, el Analista de Computo tiene un nivel de riesgo de 58,74%, el Asistente de Computo 1 tiene un nivel de riesgo de 66,13%, el Asistente de Computo 2 tiene un nivel de riesgo es de 84,09%. El riesgo promedio por departamento mediante la norma de control interno es de 66,43%.

Es así, que se evidencia que el componente con mayor nivel de riesgo es Documentación con un porcentaje de 84,38% y el componente con menor nivel de riesgo es Software con un porcentaje de 56,82%.

3.2. ANÁLISIS DE LOS RIESGOS SEGÚN NORMA DE CONTROL INTERNO

En base a los resultados obtenidos en la evaluación de riesgos según la Norma de Control Interno en Tecnologías de Información 410-09, referente al control y mantenimiento de la infraestructura tecnológica, el departamento tecnológico fue evaluado mediante los componentes de Documentación, Hardware y Software.

Para obtener la siguiente tabla, se evaluó a cada uno de las personas que laboran dentro del departamento tecnológico, donde dio como resultado un promedio de riesgo por individuo /componente y el riesgo promedio general del departamento, mostrado en la siguiente tabla:

COMPONENTES	RIESGOS
Documentación	84,38%
Hardware	58,09%
Software	56,82%
PROMEDIO RIESGO GENERAL DEL DEPARTAMENTO	66,43%

Se observa así, que el componente de Documentación, muestra un riesgo promedio de 84,38%, el componente de hardware un riesgo promedio de 58,09% y el componente de software un riesgo promedio de 56,82%, debido a que no se llevan a cabo en su totalidad los procedimientos, procesos, sistemas y acuerdos de servicios que serán registrados, evaluados y autorizados de forma previa a su implantación; la falta de bitácoras para su respectiva documentación; la inexistente actualización de todo tipo de manuales técnicos, planes estratégicos y planes operativos para la unidad tecnológica; la insuficiencia de mecanismos lógicos y físicos de seguridad para proteger los recursos tecnológicos; todo esto bajo la exigencia de la Norma de Control Interno de tecnologías de información 410-09 referente al control y mantenimiento de la infraestructura tecnológica y el incumplimiento de los productos y servicios a entregar que lo dispone el registro oficial tecnológico de la Espam Mfl.

4. EVALUACIÓN Y CALIFICACIÓN DE LOS RIESGOS DE CONTROL INTERNO

De conformidad a la evaluación del control interno a los componentes seleccionados los resultados son los siguientes:

COMPONENTE	JEFE DEL DEPARTAMENTO				ANALISTA DE COMPUTO				ASISTENTE DE COMPUTO 1				ASISTENTE DE COMPUTO 2			
	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR
CONTROL INTERNO	43,25%	BAJO	ALTO	ROJO	41,26%	BAJO	ALTO	ROJO	33,87%	BAJO	ALTO	ROJO	15,91%	BAJO	ALTO	ROJO
DOCUMENTACIÓN	32,69%	BAJO	ALTO	ROJO	29,80%	BAJO	ALTO	ROJO	0,00%	BAJO	ALTO	ROJO	0,00%	BAJO	ALTO	ROJO
HARDWARE	47,06%	BAJO	ALTO	ROJO	48,53%	BAJO	ALTO	ROJO	47,06%	BAJO	ALTO	ROJO	25,00%	BAJO	ALTO	ROJO
SOFTWARE	50%	BAJO	ALTO	ROJO	45,45%	BAJO	ALTO	ROJO	54,55%	MODERADO	MODERADO	AMARILLO	22,73%	BAJO	ALTO	ROJO

5. RESULTADO DE LAS ENCUESTAS REALIZADAS AL PERSONAL ADMINISTRATIVO Y LAS DIFERENTES CARRERAS DE LA ESPAM MFL

Para la evaluación de las encuestas realizadas al personal que labora en la institución se solicitó al Departamento de Almacén el inventario en donde constaban todos los equipos tecnológicos de dicha institución, tomando como referencia los dos últimos años (2012-2013) para las evaluaciones pertinentes.

Se tomaron en cuenta las dos áreas de la institución:

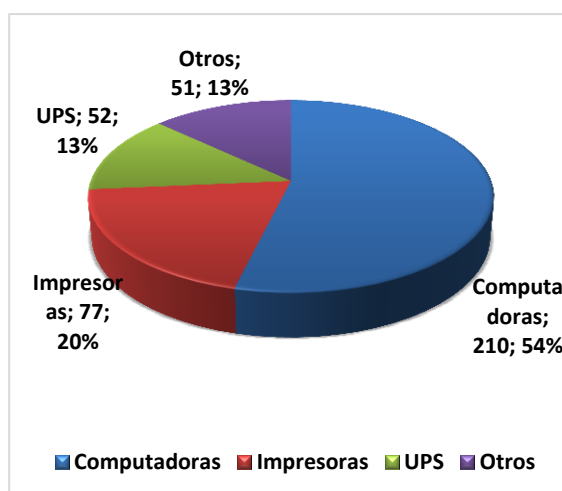
En el Área Agroindustrial en donde se encuentra ubicado Rectorado, Vicerrectorado, Biblioteca, Talleres Agroindustriales, las carreras de Medio Ambiente, Agroindustrias, Turismo, Informática, y todas las áreas administrativas de esta área.

En el Área Agropecuaria en donde se encuentra ubicado la incubadora, las carreras de Agrícola, Pecuaria y Administración y todas las áreas administrativas de esta área.

A continuación se muestran las preguntas realizadas en la encuesta elaborada para evaluar al departamento.

PREGUNTA 1. ¿CUANTOS EQUIPOS TECNOLÓGICOS TIENE A SU CARGO?

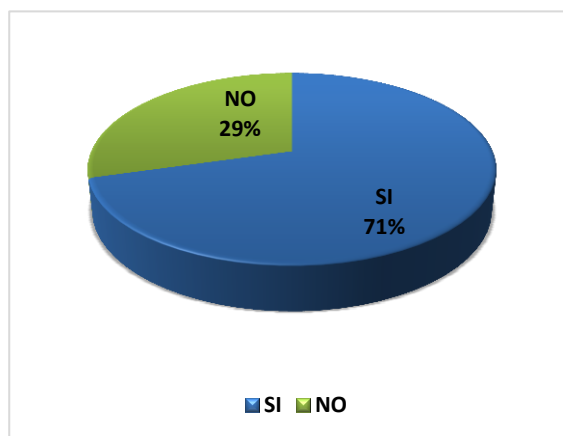
OPCIONES DE RESPUESTA	Nº DE EQUIPOS	%
Computadoras	210	54%
Impresoras	77	20%
UPS	52	13%
Otros	51	13%
TOTAL	390	100%



En las diferentes áreas administrativas y las diferentes carreras de la ESPAM MFL de las cincuenta y un (51) encuestas realizadas a los custodios de la institución, se obtuvieron como resultado que existen; 210 computadoras incluidas de escritorios y portátiles que constituye a un 54%, 77 Impresoras que constituyen a un 20%, 52 UPS que constituyen a un 13% y 51 en otros equipos que constituyen a un 13%, dando como resultado 390 equipos tecnológicos que equivale a un 100%.

PREGUNTA 2. ¿LES HAN REALIZADO MANTENIMIENTO PREVENTIVO A SUS EQUIPOS TECNOLÓGICOS?

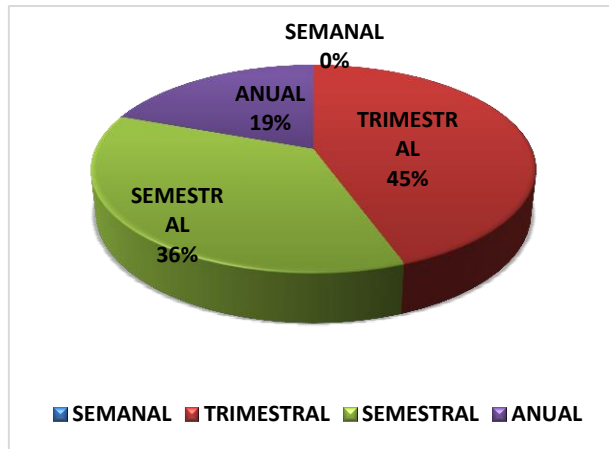
OPCIONES DE RESPUESTAS	N° DE RESPUESTAS	%
SI	36	71%
NO	15	29%
TOTAL	51	100%



En las diferentes áreas administrativas y las diferentes carreras de la ESPAM MFL de las cincuenta y un (51) encuestas realizadas a los custodios de la institución, se obtuvieron como resultado que; 36 custodios dieron como respuestas que **SI** les realizaban mantenimientos preventivos y constituye a un 71%, mientras que los otros 15 dieron como respuesta que **NO** se les realizaba mantenimientos a los equipos tecnológicos que tienen a su cargo con un porcentaje de 29% , dando como resultado un total de 51 respuestas que equivale a un 100%.

EN CASO DE QUE LA RESPUESTA SEA SI CADA QUE TIEMPO SE LO REALIZA:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
SEMANTAL	0	0%
TRIMESTRAL	16	45%
SEMESTRAL	13	36%
ANUAL	7	19%
TOTAL	36	100%



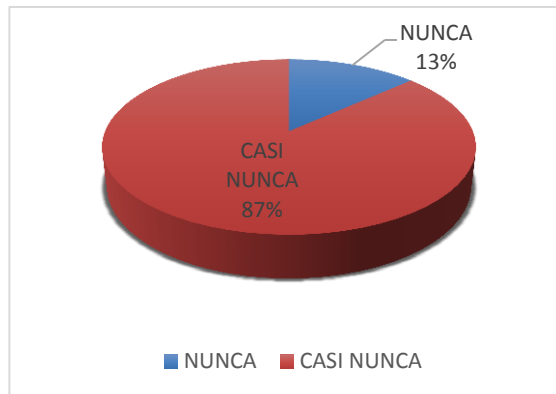
EL TIEMPO EN QUE TARDA EL MANTENIMIENTO ES:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
MUCHO TIEMPO	4	11%
POCO TIEMPO	23	64%
LO ESPERADO PARA CONTINUAR ACTIVIDADES	9	25%
TOTAL	36	100%



EN CASO DE QUE LA RESPUESTA SEA NO:

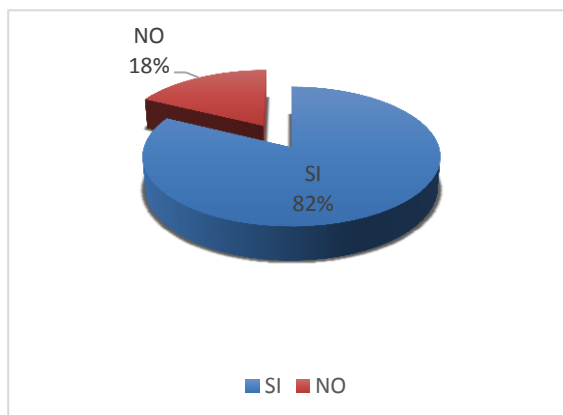
OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
NUNCA	2	13%
CASI NUNCA	13	87%
TOTAL	15	100%



Como se puede observar mediante esta segunda pregunta las autoras de esta auditoria obtuvieron como resultado que el 71% de los encuestados corresponden al total de 36 encuestados, que son custodios de los equipos tecnológicos, y según los resultados SI les dan mantenimiento preventivo a los equipos; el tiempo que se lo realiza corresponde al 45% TRIMESTRAL, 36% SEMESTRAL y el 19% ANUAL; el tiempo en que tarda el mantenimiento corresponde al 11 % MUCHO TIEMPO, 64% POCO TIEMPO y 25% LO ESPERADO PARA CONTINUAR LAS ACTIVIDADES, mientras que el 29% de los encuestados que corresponden al total de 15 encuestados de los custodios dicen que NO les dan mantenimiento preventivo a sus equipos, NUNCA el 13% y CASI NUNCA el 87%.

PREGUNTA 3. ¿LES HAN REALIZADO MANTENIMIENTO CORRECTIVO A SUS EQUIPOS TECNOLÓGICOS?

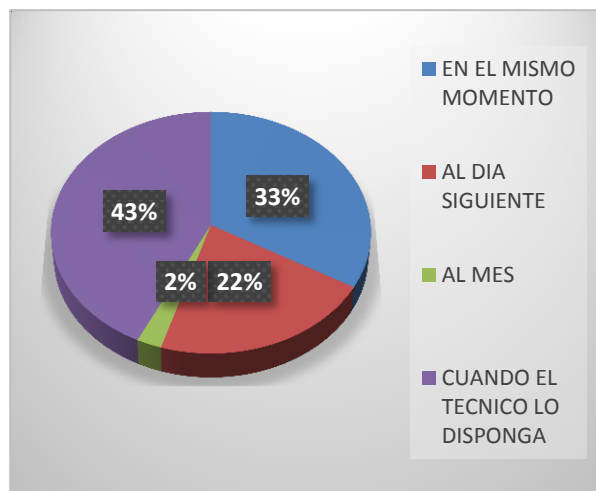
OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
SI	42	82%
NO	9	18%
TOTAL	51	100%



En las diferentes áreas administrativas y las diferentes carreras de la ESPAM MFL de las cincuenta y un (51) encuestas realizadas a los custodios de la institución, se obtuvieron como resultado que; 42 custodios dieron como respuestas que **SI** les realizaban mantenimientos preventivos y constituye a un 82%, mientras que los otros 9 dieron como respuesta que **NO** se les realizaba mantenimientos a los equipos tecnológicos que tienen a su cargo, dando como resultado un 18%.

EN CASO DE QUE LA RESPUESTA SEA SI CADA QUE TIEMPO SE LO REALIZA:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
EN EL MISMO MOMENTO	14	33%
AL DÍA SIGUIENTE	9	22%
AL MES	1	2%
CUANDO EL TÉCNICO LO DISPONGA	18	43%
TOTAL	42	100%



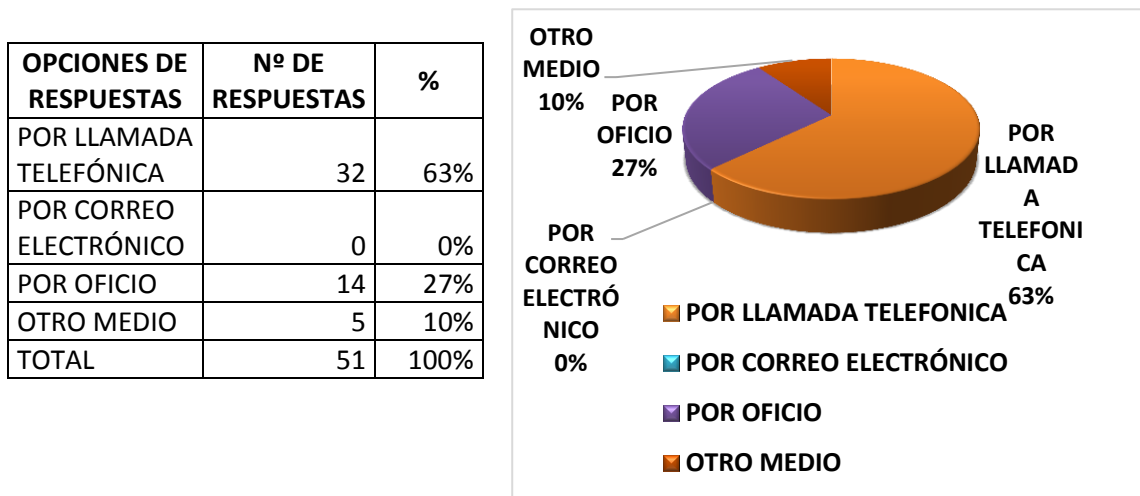
EN CASO DE QUE LA RESPUESTA SEA NO:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
NUNCA	3	33%
CASI NUNCA	0	0%
CUANDO EL EQUIPO LO REQUIERA	6	67%
TOTAL	9	100%



Como resultado se obtuvo en esta tercera pregunta del total de 51 encuestados, el 82% corresponden a el total de 42 encuestados de los custodios de los equipos tecnológicos y al que SI les hacen mantenimiento correctivo a los mismos, y el tiempo que toma la entrega corresponde al 43% que es CUANDO EL TÉCNICO LO DISPONGA, un 33% es EN EL MISMO MOMENTO y el 22% AL DIA SIGUIENTE y el 2% AL MES, mientras que el 18% correspondiente al total de 9 encuestados de los custodios, NO les hacen mantenimiento correctivo a sus equipos, solamente cuando el equipo lo disponga que es el 67% y el 33% NUNCA.

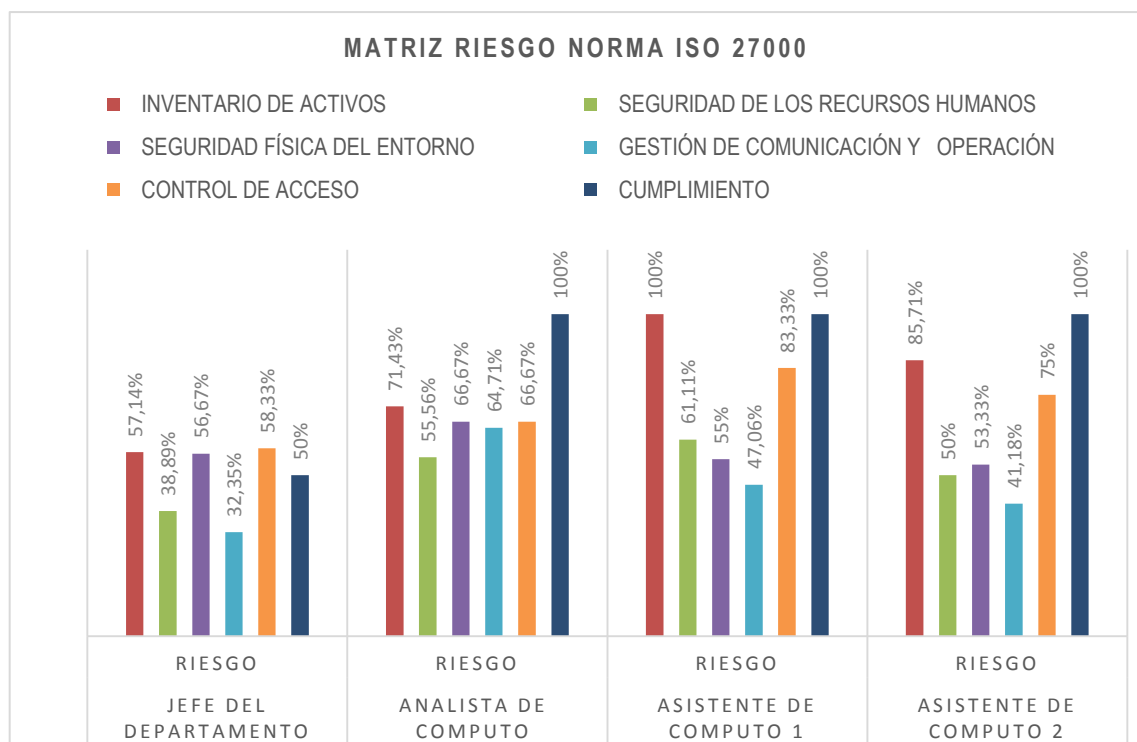
PREGUNTA 4: ¿CÓMO SE REALIZA LA SOLICITUD DE MANTENIMIENTO SEA PREVENTIVO O CORRECTIVO?



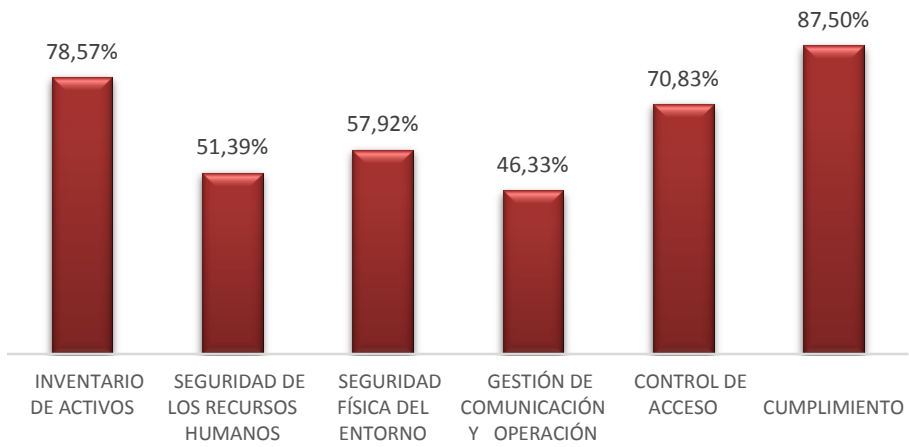
Como resultado en esta cuarta pregunta se obtuvo que del total de 51 encuestados, el 63% corresponden a los custodios de los equipos tecnológicos hacen la solicitud del mantenimiento ya sea preventivo o correctivo por medio de LLAMADA TELEFÓNICA, mientras el 27% corresponde POR OFICIO y un 10% lo hace POR OTRO MEDIO.

6. RESULTADO DE LA EVALUACIÓN DE LA NORMA ISO 27000

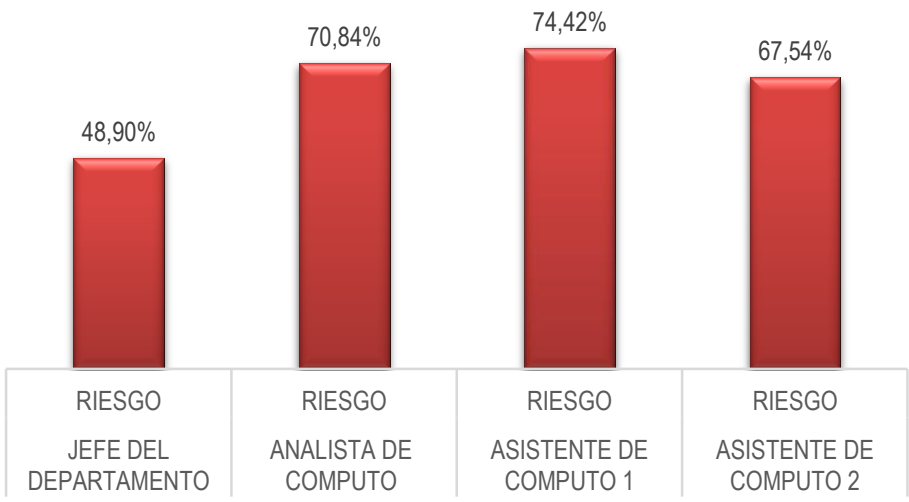
MATRIZ CONFIANZA-RIESGO NORMA ISO 27000					
TEMA	JEFE DEL DEPARTAMENTO	ANALISTA DE COMPUTO	ASISTENTE DE COMPUTO 1	ASISTENTE DE COMPUTO 2	RIESGO PROMEDIO DEL DEPARTAMENTO TECNOLÓGICO
	RIESGO	RIESGO	RIESGO	RIESGO	
NORMA ISO 27000	48,90%	70,84%	74,42%	67,54%	65,42%
INVENTARIO DE ACTIVOS	57,14%	71,43%	100%	85,71%	78,57%
SEGURIDAD DE LOS RECURSOS HUMANOS	38,89%	55,56%	61,11%	50%	51,39%
SEGURIDAD FÍSICA DEL ENTORNO	56,67%	66,67%	55%	53,33%	57,92%
GESTIÓN DE COMUNICACIÓN Y OPERACIÓN	32,35%	64,71%	47,06%	41,18%	46,33%
CONTROL DE ACCESO	58,33%	66,67%	83,33%	75%	70,83%
CUMPLIMIENTO	50%	100%	100%	100%	87,50%



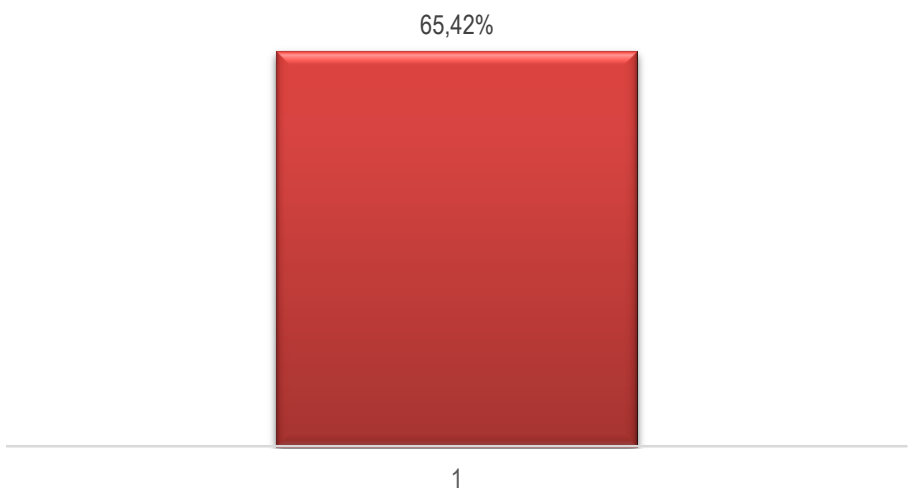
RIESGO PROMEDIO POR COMPONENTE DEL DEPARTAMENTO TECNOLÓGICO



RIESGO GENERAL POR INDIVIDUO NORMA ISO 27000



RIESGO PROMEDIO DEL DEPARTAMENTO TECNOLÓGICO



6.1. DESCRIPCIÓN DE LOS GRÁFICOS

Dentro de los porcentajes de la matriz riesgo confianza se observa que el Departamento dentro la evaluación de la norma ISO 27000 dio como resultado: sobre el componente Inventario de Activos del Jefe del Departamento tiene un nivel de riesgo de 57,14%, el Analista de Computo tiene un nivel riesgo es de 71,43%, el Asistente de Computo 1 tiene un nivel de riesgo es de 100,00% , el Asistente de Computo 2 tiene un nivel de riesgo es de 85,71% , y el nivel de riesgo promedio del departamento es de 78,57%; sobre el componente Seguridad de los Recursos Humanos el Jefe de Computo tiene un nivel de riesgo de 38,89%, el Analista de Computo tiene un nivel de riesgo de 55,56%, el Asistente de Computo 1 tiene un nivel de riesgo de 61,11%, el Analista de Computo 2 tiene un nivel de riesgo es de 50%, y el riesgo promedio del departamento es de 51,39%; sobre el componente Seguridad Física del Entorno el Jefe de Computo tiene un nivel de riesgo de 56,67%, el Analista de Computo tiene un nivel de riesgo de 66,67%, el Asistente de Computo 1 tiene un nivel de riesgo de 55%, el Asistente de Computo 2 tiene un nivel de riesgo de 53,33%, y el riesgo promedio del departamento es de 57,92%; sobre el componente Gestión de Comunicación y Operación el Jefe de Computo tiene un nivel de riesgo de 32,35%, el Analista de Computo tiene un nivel de riesgo de 64,71%, el Asistente de Computo 1 tiene un nivel de riesgo de 47,06%, el Asistente de Computo 2 tiene un nivel de riesgo de 41,18%, y riesgo promedio del departamento es de 46,33%; sobre el componente Control de Acceso el Jefe de Computo tiene un nivel de riesgo es de 58,33%, el Analista de Computo tiene un nivel de riesgo de 66,67%, el Asistente de Computo 1 tiene un nivel de riesgo de 83,33%, el Asistente de Computo 2 tiene un nivel de riesgo de 75%, y el riesgo promedio del departamento es de 70,83%; sobre el componente Cumplimiento el Jefe de Computo tiene un nivel de riesgo es de 50%, el Analista de Computo tiene un nivel de riesgo de 100,00%, el Asistente de Computo 1 tiene un nivel de riesgo de 100,00%, el Asistente de Computo 2 tiene un nivel de riesgo de 100,00%, y riesgo promedio del departamento es de 87,50%.

De manera general el departamento tecnológico cuenta con unos porcentajes de riesgo por colaborador y por departamento como tal, el Jefe del Departamento tiene un nivel de riesgo promedio en la evaluación de la NORMA ISO 27000 de 48,90%, el Analista de Computo tiene un nivel de riesgo promedio en la evaluación de la NORMA ISO 27000 de 70,84%, el Asistente de Computo 1 tiene un nivel de riesgo promedio en software de 74,42%, el Asistente de Computo 2 tiene un nivel de riesgo promedio en la evaluación de la NORMA ISO 27000 de 67,54%. El riesgo promedio por departamento mediante la NORMA ISO 27000 es de 65,42%.

Es así, que se evidencia que el componente con mayor nivel de riesgo es de 87,50% que equivale al componente de cumplimiento y el componente con menor nivel de riesgo es el de Gestión de Comunicación y Operación con 46,33%.

6.2. ANÁLISIS DE LOS RIESGOS SEGÚN NORMA ISO 27000

En base a los resultados obtenidos en la evaluación de riesgos según la Norma ISO 27000, el departamento tecnológico fue evaluado mediante los componentes de Inventario de Activos, Seguridad de los Recursos Humanos, Seguridad Física y del Entorno, Gestión de Comunicación y Operación, Control de Acceso y Cumplimiento.

Para obtener la siguiente tabla, se evaluó a cada uno de las personas que laboran dentro del departamento tecnológico, donde dio como resultado un promedio de riesgo por individuo /componente y el riesgo promedio general del departamento, mostrado en la siguiente tabla:

COMPONENTES	RIESGOS
Inventario de Activos	78,57%
Seguridad de los Recursos Humanos	51,39%
Seguridad Física y del Entorno	57,92%
Gestión de Comunicación y Operación	46,33%
Control de Acceso	70,83%
Cumplimiento	57,14%
PROMEDIO RIESGO GENERAL DEL DEPARTAMENTO	65,42%

Procediendo al análisis, se observa, que el componente de Inventario de Activos, muestra un riesgo promedio de 78,57%, debido a que no se cumple en su totalidad el control de inventario de Activos Tecnológicos, como lo dispone la Norma ISO 27000.

El componente de Seguridad de los Recursos Humanos, con un riesgo promedio de 51,39%, no cumple con todas las disposiciones que exige la Norma ISO 27000, como lo es de tener un Manual de Funciones y Responsabilidades actualizados, y no hacen la respectiva formalidad de la devolución de los activos tecnológicos.

En el componente de Seguridad Física y del Entorno, con un riesgo promedio de 57,92%, como lo dispone la Norma ISO 27000, acerca de los perímetros de de la seguridad física del entorno, la protección contra amenazas externas y ambientales de los equipos tecnológicos, seguridad de cableados, ubicación y protección de los equipos tecnológicos, áreas seguras, seguridad de los equipos fuera de las instalaciones y seguridad en la reutilización de los equipos, no se está cumpliendo en su totalidad como lo exige la ley.

En el componente de Gestión de Comunicación y Operación, con un riesgo promedio de 46,33%, es debido a que solo se lleva en partes la respectiva documentación de los procedimientos de operación, gestión del cambio, distribución de funciones, separación de áreas, realización de proyecciones de los requerimientos de capacidad futura, control contra códigos maliciosos, respaldo de la información, controles a las redes, seguridad de los servicios de la red, registros de auditoria, como lo dispone la Norma ISO 27000.

En el componente de Control de Acceso, con un riesgo promedio de 70,83%, se debe a que no se cumple a cabalidad las políticas de control de acceso, registros de usuarios, políticas de uso de los servicios de red, identificación de los equipos en la redes, control de conexiones a las redes, control de accesos remotos como lo dispone la Norma ISO 27000.

En el componente de Cumplimiento, con un riesgo promedio de 87,50%, la Norma ISO 27000 refiere a la Identificación de la legislación aplicable: Inventario de todas las Normas legales que utiliza la institución, y controles de auditorías de los sistemas de información, que el departamento tecnológico debe cumplir porque así lo exige esta Norma, y no se está llevando a cabo.

7. EVALUACIÓN Y CALIFICACIÓN DE LOS RIESGOS NORMA ISO 27000

COMPONENTE	JEFE DEL DEPARTAMENTO				ANALISTA DE COMPUTO				ASISTENTE DE COMPUTO 1				ASISTENTE DE COMPUTO 2			
	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR
NORMA ISO 27000	51,10%	MODERADO	MODERADO	AMARILLO	29,16%	BAJO	ALTO	ROJO	25,67%	BAJO	ALTO	ROJO	32,46%	BAJO	ALTO	ROJO
INVENTARIO DE ACTIVOS	42,86%	BAJO	ALTO	ROJO	28,57%	BAJO	ALTO	ROJO	0,00%	Fuera de Rango	Fuera de Rango	sin color	14,29%	Fuera de Rango	Fuera de Rango	sin color
SEGURIDAD DE LOS RECURSOS HUMANOS	61,11%	MODERADO	MODERADO	AMARILLO	44,44%	BAJO	ALTO	ROJO	39,00%	BAJO	ALTO	ROJO	50,00%	BAJO	ALTO	ROJO
SEGURIDAD FÍSICA DEL ENTORNO	43,33%	BAJO	ALTO	ROJO	33,33%	BAJO	ALTO	ROJO	45,00%	BAJO	ALTO	AMARILLO	46,67%	BAJO	ALTO	ROJO
GESTIÓN DE COMUNICACIÓN Y OPERACIÓN	67,61%	MODERADO	MODERADO	AMARILLO	35,29%	BAJO	ALTO	ROJO	53,00%	MODERADO	MODERADO	AMARILLO	58,82%	MODERADO	MODERADO	AMARILLO
CONTROL DE ACCESO	41,67%	BAJO	ALTO	ROJO	33,33%	BAJO	ALTO	ROJO	17,00%	BAJO	ALTO	ROJO	25,00%	BAJO	ALTO	ROJO
CUMPLIMIENTO	50,00%	BAJO	ALTO	ROJO	0,00%	Fuera de Rango	Fuera de Rango	sin color	0,00%	Fuera de Rango	Fuera de Rango	sin color	0,00%	Fuera de Rango	Fuera de Rango	sin color

7. OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE CHECKLIST NORMA DE CONTROL INTERNO

<p>ESPAM MFL ANÁLISIS MEDIANTE LA NORMA 410 DE CONTROL INTERNO</p>
<p>Objetivo/Ámbito: El presente análisis es con la finalidad de dar conocer la verificación del nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.</p>
<p>Área auditada: Departamento Tecnológico de la ESPAM MFL</p>
<p>Personal Auditado: Jefe del Departamento, Analista de Computo, Asistente de Computo 1 y Asistente de Computo 2</p>
<p>DOCUMENTACIÓN</p>
<p>OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:</p>
<p>La Institución cuenta con un organigrama</p>
<p>El departamento tecnológico no cuenta con un organigrama actualizado, existe uno como Jefatura de Cómputo, y debido a esta observación las auditoras proponen un organigrama para el área auditada.</p>
<p>El Manual de Funciones y Responsabilidades no está actualizado porque consta como Jefatura de Computo, y según la Norma de Control Interno de TI 410-09, refiere a que todos los Manuales técnicos, funciones, políticas y procedimientos deben ser actualizados</p>
<p>No tienen delimitadas las funciones y responsabilidades en el departamento, por esta razón en la actualidad no existe la debida asignación de funciones como lo dispone la Norma de Control Interno de TI 410-09.</p>
<p>La Planificación de Mantenimientos de Equipos de Redes, Computación y Software Base, está como Jefatura de Computo, no tiene fecha de cuando fue elaborada, debería ser actualizada para el departamento tecnológico como lo dispone la Norma de Control TI 410-09.</p>
<p>Los diferentes mantenimientos (preventivo, correctivo) en la institución, no se los realiza con la debida autorización del Jefe del Departamento</p>
<p>La solicitud de los diferentes mantenimientos (preventivo, correctivo) que brinda el departamento tecnológico se lo realiza de manera verbal o por medio de vía telefónica.</p>
<p>Actualmente se hacen los mantenimientos preventivos cada 3 meses y los correctivos cuando el equipo tecnológico lo requiera, aunque no tienen una Planificación de Mantenimientos Programados.</p>
<p>No cuenta con Políticas y Procedimientos el Departamento Tecnológico.</p>
<p>No se lleva un control de los equipos en garantía.</p>
<p>El departamento tecnológico no lleva un control de inventarios de los equipos de computación y software a excepción de los equipos de comunicación y redes, que se llevan en un 30% en archivos Excel.</p>
<p>No se dispone de ningún tipo de bitácoras para el registro de fallas de los equipos.</p>
<p>Se poseen registros individuales de los equipos tecnológicos en el Departamento de Almacén, aunque también debería llevarlos el departamento tecnológico como lo refiere la Norma de</p>

Control Interno de TI 410-09.
No se realizan revisiones periódicas de los equipos computación y software base.
Se realizan revisiones cada semana a los equipos de las redes.
No aplican metodologías para planificar las revisiones de los equipos tecnológicos en general.
El Departamento no cuenta con un Plan de Contingencia.
El departamento tecnológico realiza el respaldo de la información de los equipos formateados en dispositivos externos, pero no son registrados ni almacenados para su conservación, una vez devuelta la información al equipo formateado, se elimina la información respaldada.
No existen controles de acceso a las computadoras del personal administrativo.
Si existen controles de acceso a las redes inalámbricas de la institución.
Si existen controles de acceso a los servidores.
No se llevan registros estadísticos del uso de la red.
El departamento tecnológico administra las contraseñas de admisión de las redes.
Las contraseñas de admisión son abiertas en un 50% debido a que sus usuarios son estudiantes de las diferentes áreas en la institución.
Se han realizado auditorías al departamento tecnológico por parte de la Contraloría General del Estado, sin embargo no se han aplicado las recomendaciones pertinentes de dichas evaluaciones.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma de Control Interno que emite la Contraloría General del Estado Ecuatoriano.
HARDWARE
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
El departamento no cuenta con un servicio de mantenimiento para todos los equipos tecnológicos en general.
El mantenimiento de los equipos tecnológicos se lo realiza cada 3 meses o cuando hay algún problema o falla.
Existe un plan de mantenimiento para los equipos tecnológicos como Jefatura de Cómputo.
No cuentan con un control y registro de los mantenimientos realizados.
Los equipos tecnológicos que tienen garantía, el proveedor realiza el mantenimiento fuera de la institución y se llevan éstos con discos duros.
No se tienen criterios de evaluación de rendimiento de los equipos de computación, solamente se hace el criterio de evaluación de funcionalidad de los equipos.

<p>La administración de las bases de datos y los servidores lo lleva la Carrera de Informática y no el Departamento Tecnológico, como la Carrera Informática es de área Educativa y no de área administrativa como lo es el departamento tecnológico, entonces la administración de las bases de datos y servidores incluyendo la producción de software debería ser llevados por éste, reformando su estructura de acuerdo al organigrama propuesto por las auditoras y con personal capacitado para llevar el control de dicha administración.</p>
<p>El registro de los equipos de computación, no los lleva el departamento tecnológico, esto lo hace el departamento de Almacén, sin embargo debería llevarlo también el departamento porque esto lo dispone la Norma de Control Interno TI 410-09</p>
<p>No se tienen acceso remoto a las redes.</p>
<p>No se tiene un registro de los puntos de acceso que existen en la institución.</p>
<p>La seguridad de las redes inalámbricas es WPA WPA2 dentro de la institución.</p>
<p>No se realiza la relevación de los costos en mantenimientos de equipos en general de los últimos años.</p>
<p>No se evidencian los tiempos de mantenimiento.</p>
<p>No se realiza el seguimiento de los controles de los componentes de los equipos tecnológicos de la institución.</p>
<p>No se realiza el seguimiento a los controles de equipos que ya fueron cambiados por garantía.</p>
<p>NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma de Control Interno que emite la Contraloría General del Estado Ecuatoriano.</p>
<p style="text-align: center;">SOFTWARE</p>
<p>OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:</p>
<p>Se realiza el mantenimiento del software base dentro de la Institución, solamente cuando este lo requiera y que su versión sea compatible con el equipo.</p>
<p>Se evalúa el funcionamiento del software base en el momento que se instala y cada año después de instalado, sin embargo no se llevan registros de su funcionamiento.</p>
<p>No se actualiza el software base, solo cuando lo requiere el usuario o la nueva versión sea compatible con el equipo.</p>
<p>Las licenciaturas del software base son actualizadas cada año.</p>
<p>El tipo de licenciaturas que tiene la Universidad es institucional, no estudiantil.</p>
<p>No existen procedimientos para hacer las diferentes actualizaciones.</p>
<p>No todos los equipos de computación tienen instalados los antivirus.</p>
<p>Los programas instalados en los equipos tecnológicos, para las actividades de la institución son paquete Office, Antivirus, PDF, WinRAR.</p>
<p>NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma de Control Interno que emite la Contraloría General del Estado Ecuatoriano.</p>

8. OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE CHECKLIST NORMA ISO 27000

ESPAM MFL ANÁLISIS MEDIANTE LA NORMA ISO 27000
Objetivo/Ámbito: El presente análisis es con la finalidad de dar conocer la verificación del nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.
Área auditada: Departamento Tecnológico de la ESPAM MFL
Personal Auditado: Jefe del Departamento, Analista de Computo, Asistente de Computo 1 y Asistente de Computo 2
INVENTARIO DE ACTIVOS
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
<p>En consideración a la Norma ISO 27000 con respecto a la Gestión de activos, en el punto de Inventario de activos, refiere que se debe inventariar los activos primarios en formatos físicos y/o electrónicos, también los activos de soporte de Hardware, Software y Redes, debe tener un plan estratégico, y que los activos tengan asignados un responsable del activo, lo que el departamento tecnológico no cumple con lo siguiente:</p>
<p>No tiene un Plan Estratégico</p>
<p>No llevan el control de inventario de hardware y software con sus respectivos formatos como lo estipula la norma ISO 27000.</p>
<p>Del inventario de comunicación y redes solo se lleva el 30 % de su totalidad, en forma electrónico (digital), mostrando evidencia en archivos Excel, quien lleva el control del inventario de activos tecnológicos (hardware, software, redes) en su totalidad, es el departamento de almacén.</p>
<p>Con respecto a los custodios asignados a los equipos tecnológicos, si se hace la respectiva asignación, lo que no se hace es la debida formalidad del cambio inmediato cuando éste termina su contrato de trabajo en el área asignada o en la entidad como lo estipula la Norma ISO 27000. (Inventario desactualizado por parte de Almacén)</p>
<p>NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000</p>
SEGURIDAD DE LOS RECURSOS HUMANOS
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CUESTIONARIOS:
<p>Mediante la siguiente observación dentro del Departamento tecnológico, se socializan los procedimientos de mantenimiento preventivo, correctivo de los bienes: Hardware, Software y equipos de comunicación de redes, con respecto a trabajos técnicos, y en cuánto a la documentación que se deja como constancia en las hojas de registros e informes que evidencien la realización de los mantenimientos no se está llevando a cabo como lo dispone la Norma ISO 27000.</p>
<p>Se responsabiliza a cada custodio por el mal uso y destrucción de los equipos tecnológicos asignados y entregados al responsable, este proceso lo realiza el Departamento de Almacén y no el Departamento Tecnológico.</p>
<p>Con respecto a las responsabilidades del Departamento, no existe una planificación ni procedimientos para la distribución de tareas.</p>
<p>El personal que labora en el departamento tecnológico, desconoce los objetivos establecidos para el departamento y también si éstos han sido definidos por escrito.</p>

Como lo estipula la Norma ISO 27000 sobre el proceso de devolución de los activos tecnológicos en la terminación del contrato de trabajo, no se cumple con la totalidad de dicho proceso, ya que cuando se termina el contrato del custodio del equipo, las actas de entrega no se las realiza en el tiempo debido y con la formalidad respectiva que debe hacerse, y solo se reporta al Departamento de Almacén, hasta que se haga el trámite correspondiente. Además el departamento tecnológico también debería llevar estas actas de entrega como lo dispone la Norma ISO 27000 en referencia al Inventario de activos.

NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000

SEGURIDAD FÍSICA DEL ENTORNO

OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:

De acuerdo a las observaciones pertinentes y según la norma ISO 27000 con respecto a la protección contra amenazas externas y ambientales, la ubicación de los equipos de repuestos y soportes deben estar a una distancia prudente para evitar daños en caso de desastre que afecten las instalaciones principales, la cual el Departamento tecnológico no cuenta con estas áreas de protección de equipos tecnológicos, incluso el departamento no tiene una estructura física adecuada para resguardar la seguridad de sus equipos en caso de algún desastre.

El 20% de las áreas en la universidad no tienen ubicado los equipos contra incendios.

El área de mantenimiento a las instalaciones eléctricas, al sistema de climatización y ductos de ventilación, no lo realiza el Departamento Tecnológico porque le compete al Departamento de Construcción.

Existen cámaras de seguridad para minimizar el riesgo de robos de equipos tecnológicos, sin embargo no se puede determinar si existe el debido control que permita verificar el funcionamiento de las mismas.

Todas las áreas de la institución tienen protección contra descargas eléctricas, y disponen de filtros protectores en el suministro de energía y en las líneas de comunicación, y quien lleva todas estas actividades es el departamento de Construcción.

El 87% de los equipos tecnológicos no tienen ups, esto se pudo determinar mediante las encuestas realizadas a los custodios de equipos a su cargo.

El 30% de las áreas con cableado de red en la institución no se protege contra la intersección o daño.

El 20% de las áreas de la institución no hacen la respectiva separación del cableado de la red con el cableado de energía.

No se pudo verificar si se separa el cableado de la red con el cableado de energía en el Data Center, ya que las políticas de acceso no permitieron la debida constatación de la separación del cableado.

Se realiza la identificación y rotulación del cableado de red de acuerdo a las normas locales (RTE INEN 098) e internacionales (ISO) en un 30%.

El departamento tecnológico dispone del 20% de documentación, el 80% en diseños/planos y de la distribución de conexiones de datos de redes inalámbricas y alámbricas.

De acuerdo a las especificaciones y recomendaciones del proveedor, el departamento tecnológico les da mantenimientos periódicos a los equipos y dispositivos tecnológicos.

El personal que labora en el departamento tecnológico, está calificado y autorizado para ser los únicos que den los servicios de mantenimientos a los equipos tecnológicos de la institución. Esto se evidencia con sus hojas de vida de cada uno de los individuos.

No se lleva ni se conservan los registros de los mantenimientos preventivos, correctivos o de fallas con causas no determinadas.

No se establecen controles de mantenimientos programados en el departamento, no hay un cronograma de actividades, ni un plan de mantenimiento actual, solamente existe un plan de mantenimiento cuando el departamento tenía el nombre de Jefatura de Cómputo pero no es aplicado en la actualidad.
No se custodian los equipos y medios que se encuentran fuera de las instalaciones de la institución, pero si se hacen firmar actas de responsabilidad y entrega del equipo a la persona que llevará este fuera de la entidad.
La institución No establece una cobertura adecuada del seguro (robo, incendio o mal uso del equipo) para proteger los equipos que se encuentran fuera de las instalaciones de la institución.
En la institución existen controles de acceso a las redes inalámbricas, cuando detectan muchas personas accediendo a las redes, ellos hacen el cambio inmediato de las contraseñas.
Se llevan controles de acceso a los servidores
No se realiza el correctivo para la evaluación de los dispositivos deteriorados que contengan información sensible antes de enviar a reparación.
Se utiliza la Técnica de formateo para borrar, destruir o sobrescribir la información sensible de un equipo reutilizado, pero esto no asegura el borrado seguro de la información.
Los retiros de los equipos tecnológicos o cualquier información de éste, se lo realiza con la previa autorización del custodio.
Existen personas autorizadas con su identificación respectiva para el retiro de los activos de la institución.
El registro de los equipos o activos que se retiran o se devuelven en la institución lo hace el Departamento de Almacén.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
GESTIÓN DE COMUNICACIÓN Y DE OPERACIÓN
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
No se documenta el proceso de respaldo y restauración de la información.
No se documentan las instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas.
No se documentan los procedimientos para el reinicio y recuperación del sistema en caso de fallas.
No se planifica el proceso de cambio y no se realiza la prueba correspondiente.
No se establecen responsables y procedimientos formales de control de cambios de procesos en los equipos y software.
No se aprueban de manera formal los cambios propuestos.
No está actualizado el Manual de Funciones y Responsabilidades del Departamento Tecnológico, existe uno como Jefatura de Cómputo.
No se realizan proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos como lo dispone la Norma ISO referente a la Gestión de Capacidad.
Se instalan y actualizan cada 6 meses el software de antivirus contra código malicioso.
Se mantienen los sistemas operativos actualizados con parches y actualizaciones disponibles, dependiendo de la máquina si soporta la versión actual.
No existen procedimientos de respaldo de información en el Departamento Tecnológico antes del mantenimiento.
La Norma ISO 27000 dispone en los controles de redes, que se debe separar el área de redes con el área de operaciones, y el departamento tecnológico no está cumpliendo con esta disposición.

No se designan responsabilidades para la asistencia de equipos remotos.
Se realizan diseños antes de la implementación de una red, en un 80% muestran evidencia.
No revisan alertas o fallas del sistema operativo
Realizan cambios de configuración de los controles de seguridad del sistema operativo
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
CONTROL DE ACCESO
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
Se identifican y se documentan los equipos que se encuentran en las redes, pero no en su totalidad.
Se tiene documentada la identificación de los equipos que están permitidos, según la red que corresponda.
No se implementan procedimientos para controlar la instalación de software en sistemas operativos
No se lleva un control y registro de auditoría de las actualizaciones de software que se realizan.
No se tienen restricciones de cambios de paquetes de software.
No se lleva un control de versiones para todas las actualizaciones de software.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
CUMPLIMIENTO
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
Con los resultados obtenidos en los checklist, y de acuerdo a la Norma ISO 27000 referente al cumplimiento de la legislación aplicable en la institución, el personal que labora en el departamento tecnológico, no está considerando todas las normas y leyes más generales en cuanto a gestión de datos e información electrónica como lo estipula la Norma.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000

9. NIVEL DE MADUREZ DE LOS PROCESO ESTUDIADOS EN EL DEPARTAMENTO TECNOLÓGICO

COMPONENTES	CONFIANZA PROMEDIO DEL DEPARTAMENTO	ESTADO DE NIVEL DE MADUREZ DE LOS PROCESOS	NIVEL DE MADUREZ DEL DE LOS PROCESOS	NIVEL DE MADUREZ DEL DEPARTAMENTO TECNOLÓGICO
Cumplimiento	12,50%	Inicial	1	ESTADO INICIAL NIVEL 1,5
Documentación	15,62%	Inicial	1	
Inventario de Activos	21,43%	Inicial	1	
Control de Acceso	29,17%	Inicial	1	
Hardware	41,91%	Gestionado	2	
Seguridad Física del Entorno	42,08%	Gestionado	2	
Software	43,18%	Gestionado	2	
Seguridad de los Recursos Humanos	48,61%	Gestionado	2	
Comunicación y operación	53,68%	Gestionado	2	

10. CRITERIOS DE EVALUACIÓN DE LOS PROCESOS ESTUDIADOS EN EL DEPARTAMENTO TECNOLÓGICO

NIVEL DE MADUREZ	DESCRIPCIÓN DEL NIVEL DE MADUREZ	CUMPLIMIENTO DE LAS NORMAS CONTROL INTERNO de TI 410-09 E ISO 27000
1	El componente de Cumplimiento de acuerdo a su nivel de confianza 12,50% se encuentra en el estado de madurez Inicial, debido a que se cumplen parcialmente con las normas de ley en sistemas de información y también el personal no conoce en su totalidad las leyes tanto nacionales como internacionales para la aplicación de la misma. El riesgo es de un 87,50% para el departamento tecnológico.	Se está cumpliendo parcialmente con la Norma ISO 27000 referente a Cumplimiento.
1	El componente de documentación de acuerdo a su nivel de confianza 15,62% se encuentra en el estado de madurez Inicial, debido a que hay políticas, manual de funciones y responsabilidades y un plan de mantenimiento sin actualizar. Este es un componente que no está aplicando la totalidad de la normativa de ley, y la cual refleja un impacto de riesgo de 84,38% para el departamento.	Se aplica parcialmente la Norma de Control Interno de Tecnologías de Información 410-09 que refiere al Control y mantenimiento de la infraestructura tecnológica
1	El componente de Inventario de Activos de acuerdo a su nivel de confianza 21,43% se encuentra en el estado de madurez Inicial, debido a que se lleva parcialmente el Control de Inventario de activos tecnológicos en Redes y Telecomunicaciones y el proceso de devolución de activos no se lo realiza formalmente, El riesgo es alto y corresponde a un 78,57% para el departamento tecnológico.	Se está cumpliendo parcialmente con la Norma ISO 27000 referente a Gestión de Activos.
1	El componente de Control de Acceso de acuerdo a su nivel de confianza 29,17% se encuentra en el estado de madurez Inicial, debida a que se tiene parcialmente documentada la identificación de los equipos permitidos en la red. El riesgo corresponde a un 70,83% para el departamento tecnológico.	Se está cumpliendo parcialmente con la Norma ISO 27000 referente a Control de Acceso.

2	<p>El componente de Hardware de acuerdo a su nivel de confianza 41,91% se encuentra en estado de madurez Gestionado, ya que sus actividades dentro de este componente como mantenimientos preventivos, correctivos, implementaciones de redes se realizan de manera total, con un patron regular aunque estas no se documentan de manera adecuada, lo que implica que sus procesos sean desorganizados. El impacto de riesgo por no cumplir totalmente la normativa es de 58,09% en el departamento tecnológico.</p>	<p>Se aplica la Norma de Control Interno de Tecnologías de Información 410-09, teniendo un patrón regular.</p>
2	<p>El componente de Seguridad Física del Entorno de acuerdo a su nivel de confianza 42,08% tienen un estado de madurez Gestionado, sus actividades dentro de estos componentes como el formateo seguro de la información, la custodia de los equipos tecnológicos fuera de la institución, la protección del cableado de red, identificación y rotulación del cableado de red se hacen de manera regular sin una documentación adecuada, llevando al departamento a obtener un riesgo de 57,92% .</p>	<p>Se cumple con un patrón regular la Norma ISO 27000 referente a Seguridad Física del Entorno.</p>
2	<p>El componente de Software de acuerdo a su nivel de confianza 43,18% se encuentra en estado de madurez Gestionado, ya que sus actividades como actualizaciones de software base, actualizaciones de licenciatras de software e instalación de programas en los equipos tecnológicos se realizan de manera total aunque estas no se documentan de manera adecuada, y al igual que Hardware, implica que sus procesos son desorganizados. El impacto de riesgo por no cumplir totalmente la normativa es de 56,82% (Software) en el departamento tecnológico.</p>	<p>Se aplica un patrón regular a la Norma de Control Interno de Tecnologías de Información 410-09.</p>
2	<p>El componente de Seguridad de los Recursos Humanos de acuerdo a su nivel de confianza 48,61% tienen un estado de madurez Gestionado, sus actividades dentro de estos componentes se hacen de manera parcial sin una documentación adecuada, como por ejemplo no tener una planificación y procedimientos para la distribución de tareas, llevando al departamento a resultados pobres en el control y mantenimiento de la infraestructura tecnológica, causando a la vez un riesgo de 51,39%.</p>	<p>Se cumple un patrón regular a la Norma ISO 27000 referente a la Seguridad de los Recursos Humanos</p>

2	El componente de Comunicación y Operación de acuerdo a su nivel de confianza 53,68% tiene un estado de madurez Inicial, sus actividades dentro de este componente se hacen de manera parcial como el proceso de respaldo y restauración de la información, las instrucciones para el manejo de los errores en la ejecución de tareas, todo esto sin una documentación adecuada, causando un riesgo de 46,32% en el departamento tecnológico.	Se sigue un patrón regular a la Norma ISO 27000 referente a Comunicación y Operación.
----------	--	---

11. RECURSOS A UTILIZARSE

7.1 MATERIALES

En el transcurso de la auditoría se utilizaron los siguientes materiales:

CANTIDAD	DETALLE
2	Computadoras
3	Resma de papel A4
1	Tinta para la impresora
3	Libreta de notas
4	2 esferos negros y 2 esferos azules
2	Lápiz mecánicos
3	Borrador
10	Carpetas
6	Resaltador
2	Corrector

8.1. FINANCIEROS

NOMBRES Y APELLIDOS	TIEMPO/ DÍAS	SUBSISTENCIA	MOVILIZACIÓN	COMIDA	TOTAL
Victoria Rivera	270	\$ 150,00	\$ 50,00	\$ 50,00	\$ 250
Fernanda Zambrano	270	\$ 150,00	\$ 50,00	\$ 50,00	\$ 250
TOTAL		\$ 300,00	\$ 100,00	\$100,00	\$ 500

ANEXO 20
INFORME FINAL DE AUDITORIA DIRIGIDO A LA MÁXIMA AUTORIDAD
(RECTOR(a) DE LA ESPAM MFL)

INFORME FINAL

**AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA
INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO
TECNOLÓGICO DE LA ESPAM MFL**

CARTA DE PRESENTACIÓN

Calceta, 03 de marzo de 2015

Econ. Miriam Félix López

**RECTORA DE LA ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA
DE MANABÍ MANUEL FÉLIX LÓPEZ**

Ciudad.-

De mi consideración:

Se ha realizado la AUDITORIA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL, por el período comprendido entre el 02 de Junio de 2014 hasta el 03 de Marzo de 2014.

Nuestra acción de control se efectuó de acuerdo con las Normas de Control Interno emitidas por la Contraloría General del Estado y la Norma ISO 27000. Estas normas requieren que la auditoría sea planificada y ejecutada para obtener certeza razonable de que la información y la documentación examinada no contienen exposiciones erróneas de carácter significativo, igualmente que las operaciones a las cuales corresponden, se hayan ejecutado de conformidad con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables.

Debido a la naturaleza de la acción de control efectuada, los resultados se encuentran expresados en las conclusiones y recomendaciones que constan en el presente informe. Una adecuada implantación de aquello, permitirá mejorar los procedimientos internos del departamento tecnológicos de la entidad.

Atentamente,

Victoria Rivera Chávez

Fernanda Zambrano Bravo

CAPÍTULO I

INFORMACIÓN INTRODUCTORIA

MOTIVO DE LA AUDITORÍA

La Auditoría al Control y Mantenimiento de la Infraestructura Tecnológica del Departamento Tecnológico de la ESPAM MFL, se llevó a efecto como propuesta de tema de tesis que las autoras plantearon, la misma que tuvo autorización del ingeniero Leonardo Félix López, Rector de la ESPAM MFL, mediante el oficio N°: ESPAM MFL –CI – 2014 – 179 – OF, y la autorización del tribunal de tesis mediante el oficio S/N. de fecha 16 de mayo de 2014.

OBJETIVOS DE LA AUDITORÍA

- Comprender la situación actual del Departamento Tecnológico, mediante la aplicación de técnicas de auditoría.
- Identificar globalmente las actividades que se ejecutan en el Departamento Tecnológico, para el desarrollo de la auditoría.
- Evaluar el cumplimiento de las normas control interno a la entidad, verificando sus puntos fuertes y débiles.
- Determinar el nivel de riesgo y confianza de las normas de control interno del Departamento Tecnológico.
- Evaluar el cumplimiento de la norma ISO a la entidad, verificando sus puntos fuertes y débiles.

- Determinar el nivel de riesgo y confianza de las normas de ISO del Departamento Tecnológico.

ALCANCE DEL EXAMEN

El alcance que tiene esta auditoría será sobre la evaluación del Control y Mantenimiento de la Infraestructura Tecnológica del Departamento Tecnológico y abarcará:

- Equipos de comunicación, equipos de computación e infraestructura de redes, Licenciamientos de software base.
- Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.
- Control y registro de las versiones del software que ingrese a producción.
- Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en la función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.
- Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.

- El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

RESTRICCIÓN

- No abarcará al Departamento de Almacén en sus procesos y procedimientos adquisitivos, reposo y baja de recursos tecnológicos.
- Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.
- Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.
- Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementaran medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.

CONOCIMIENTO DE LA ENTIDAD

BASE LEGAL

El Departamento Tecnológico es un Departamento dependiente de la Dirección de la máxima autoridad, encargada de la supervisión de todas las actividades informáticas y generales que se realizan en la institución, cuya misión es proveer y administrar los servicios informáticos, comunicaciones e implantación de la infraestructura tecnológica necesaria para coadyuvar al desarrollo tecnológico de la Escuela.

Atendiendo lo dispuesto la suscrita Secretaria General-Procuradora de la Escuela Superior Politécnica Agropecuaria de Manabí, Manuel Félix López, ESPAM MFL, certifica: que el presente Estatuto Orgánico de Gestión Organizacional por Procesos, fue discutido y aprobado por el Honorable Consejo Politécnico en dos sesiones extraordinarias de fechas: 11 y 16 de enero del 2012.

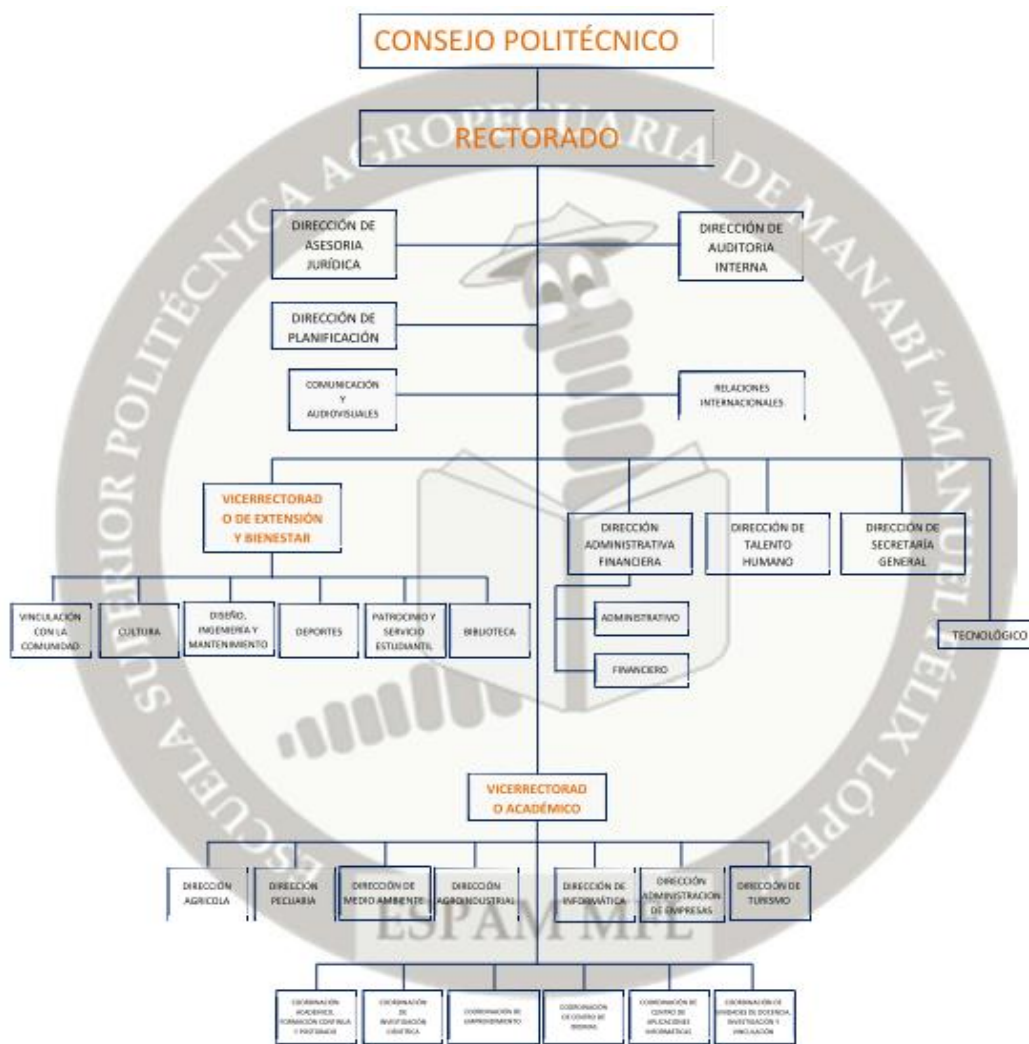
Con fecha del 17 de enero del 2012 lo certifica la Mg P.E.S Lya Villafuerte Vélez, Secretaria General, **ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DE MANABÍ MANUEL FÉLIX LÓPEZ.**

DISPOSICIONES LEGALES

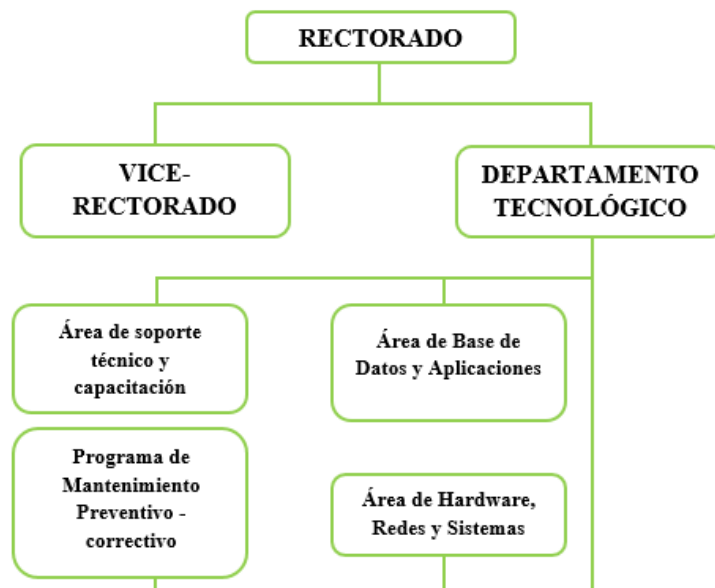
- Ley de Educación Superior.
- Estatuto de la ESCUELA SUPERIOR POLITÉCNICA DE MANABÍ
- Plan de Desarrollo de la Politécnica.
- Normas de control interno - Normas de control interno para el área de sistemas de información computarizados. Norma 410 de Tecnologías de información.

ESTRUCTURA ORGÁNICA

c) ESTRUCTURA ORGÁNICA DE LA ESPAM MFL



d) ESTRUCTURA ORGÁNICA DEL DEPARTAMENTO



PERSONAL LABORAL

PERSONAL QUE INTEGRA EL DEPARTAMENTO TECNOLÓGICO	
NOMBRE	OCUPACIÓN
ING. GEOVANNY GARCÍA	JEFE DEL DEPARTAMENTO TECNOLÓGICO
ING. PATRICIO ZAMBRANO	ANALISTA DE CÓMPUTO
ING. JUAN CARLOS MUÑOZ	ASISTENTE DE CÓMPUTO 1
ING. MANUEL DE JESÚS MACÍAS	ASISTENTE DE CÓMPUTO 2

DE ACUERDO CON LA MISIÓN DE LA ESPAM MFL , LOS REQUERIMIENTOS INFORMÁTICOS DE LA INSTITUCIÓN SON:

- Disponer de una cantidad óptima de computadoras y servicios informáticos.
Destinar al máximo las computadoras a actividades docentes, administrativas, servicios y fines productivos.
- Mantener un aprovechamiento óptimo de las computadoras y servicios.

OBJETIVOS

a) OBJETIVOS GENERALES

- Mantener un sistema óptimo de atención y capacitación permanentes para el usuario (estudiante, docente, empleado), apoyado por un servicio técnico.

- Mantener un sistema óptimo de procesos de información, sostenido adecuadamente por una base de datos institucionales, un conjunto de aplicaciones y un conjunto de protocolos y normas.
- Mantener un conjunto de herramientas informáticas, organizado como una red de hardware y software de sistemas.

b) OBJETIVOS DE MANTENIMIENTO

- Ampliar la vida útil y mantener en óptimo estado los equipos tecnológicos.
- Tener en perfectas condiciones de operatividad en los equipos tecnológicos.
- Disminuir costos, aumentar la eficiencia y eficacia en el soporte tecnológico de los equipos.
- Realizar y mantener el inventario actualizado de los equipos tecnológicos

POLÍTICAS

Los recursos informáticos centrales son administrados por el Jefe del departamento. Los recursos informáticos del Campus son administrados por el asistente, bajo las directivas establecidas por el Departamento Tecnológico.

La designación y asignación de nombres de dominio, identificadores de red y direcciones es competencia exclusiva del Departamento Tecnológico.

La representación digital de la información institucional y la especificación de las reglas de nomenclatura es de competencia y responsabilidad exclusivas del Departamento Tecnológico.

El sistema informático es un solo conjunto de recursos organizados en una red de control centralizado y arquitectura distribuida, permitiendo la coexistencia coordinada y regulada de sistemas informáticos propios de las unidades de gestión.

Todo recurso informático de o en la Universidad será asignado a un responsable directo, parte de una cadena de mando o responsabilidad.

Toda herramienta desarrollada dentro de la institución será de arquitectura abierta, con código fuente y documentación públicamente disponibles, sin perjuicio del reconocimiento de autoría individual y de equipo.

Se respetarán plenamente los derechos de propiedad intelectual, licenciamiento y autoría de cualquier recurso informático.

Se garantizará la seguridad de la información individual y colectiva, regulando el acceso de acuerdo a la propiedad y la necesidad institucionales.

Toda contratación, instalación y adquisición de recursos informáticos deberá gestionarse a través del Departamento Tecnológico, la cual establecerá mecanismos expeditivos, bajo los criterios de costo/beneficio, planificación anual/semestral indicada en el POA.

La cantidad y calidad de los recursos disponibles se fijará anualmente y revisará semestralmente constituyendo del Nivel de Servicios acordado, documentándose de manera accesible su uso y acceso.

El recurso humano especializado es el valor más importante del sistema informático y como tal debe ser estimulado con especializaciones y cursos en medida justa y proporcional a su contribución.

PUNTOS DE INTERÉS A SER EVALUADOS EN EL SIGUIENTE CAPITULO

Determinar el control y mantenimiento de la infraestructura tecnológica mediante la aplicación de normas de control interno y la norma ISO 27000.

Se tomó como referencia los dos últimos años (2012-2013) para las evaluaciones pertinentes.

Mostrar los resultados de la evaluación de Control Interno que comprende los componentes de documentación hardware y software con sus respectivos porcentajes tanto de confianza como de riesgo del departamento y por cada individuo que trabaja en el área auditada.

Mostrar los gráficos de los resultados de la evaluación de control interno.

Realizar la descripción respectiva de los cuadros y gráficos que muestran los porcentajes de riesgo como de confianza.

Mostrar la evaluación y calificación de los riesgos de Control Interno.

Mostrar los resultados de las encuestas realizadas al personal administrativo y de las diferentes carreras de la ESPAM MFL.

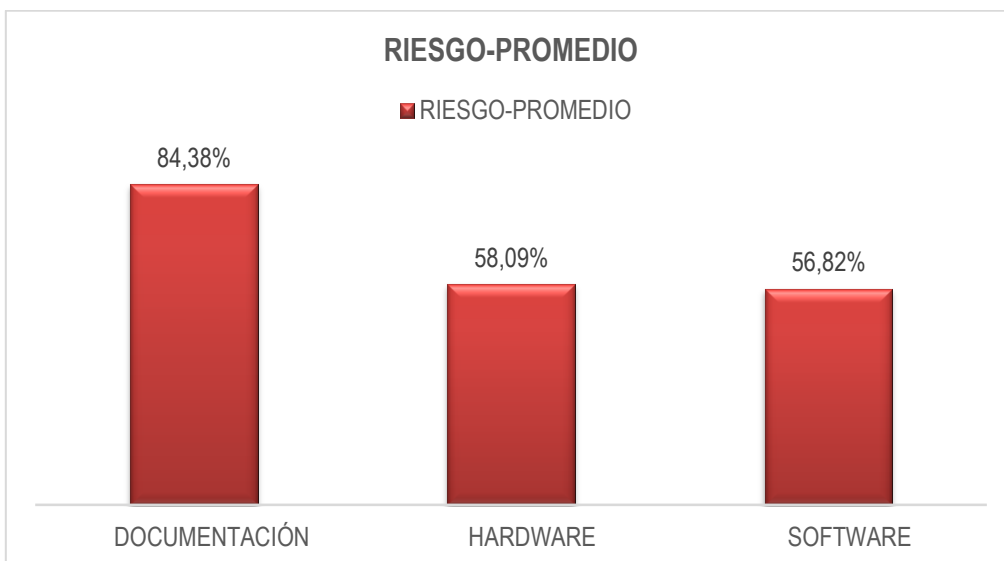
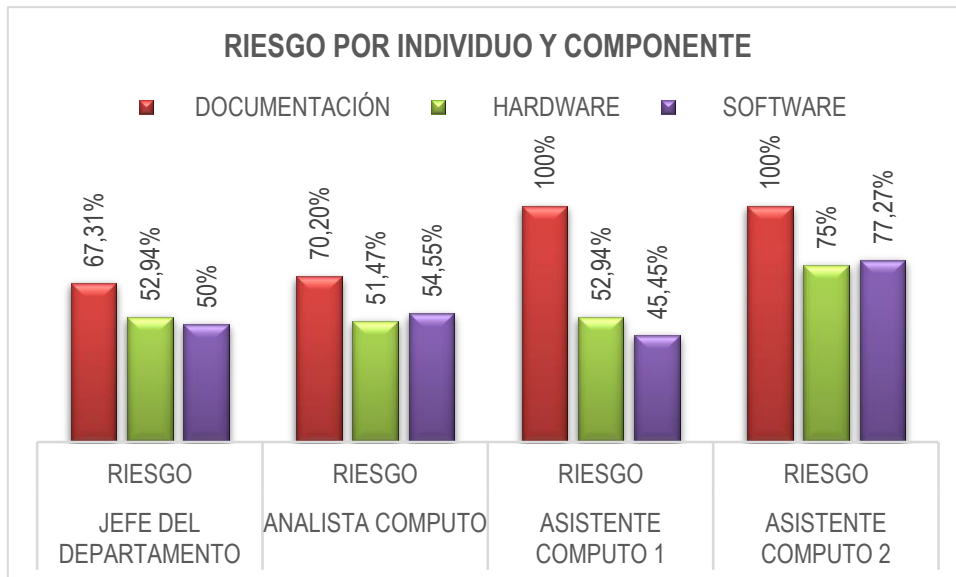
Mostrar el resultado de los testing realizado a cada una de las carreras de la ESPAM MFL.

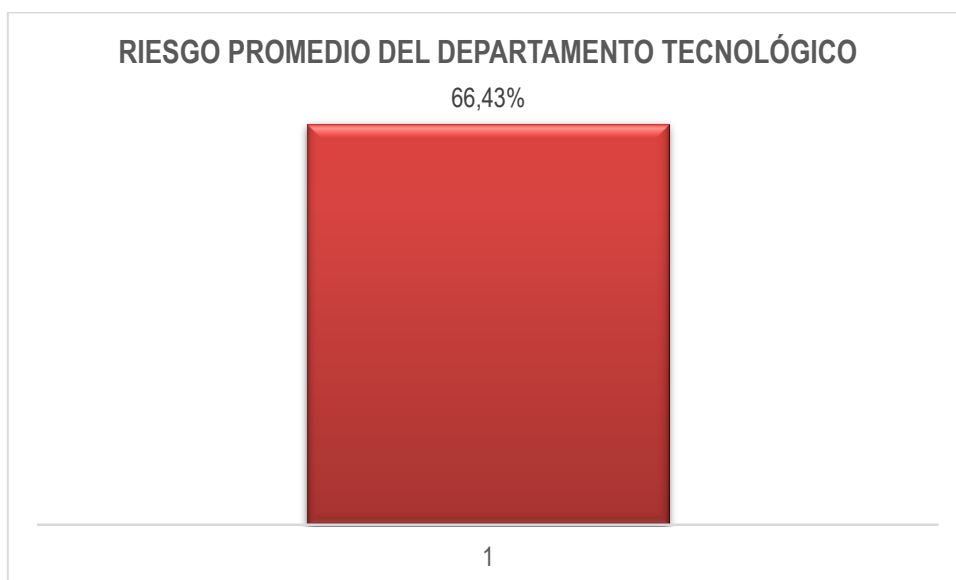
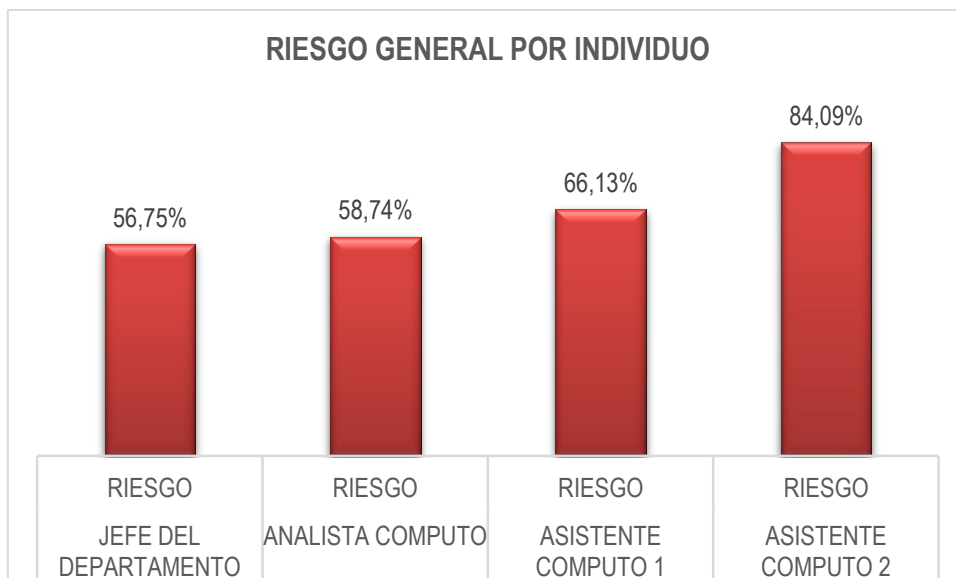
- INVENTARIO DE ACTIVOS
- SEGURIDAD DE LOS RECURSOS HUMANOS
- SEGURIDAD FÍSICA DEL ENTORNO
- GESTIÓN DE COMUNICACIÓN Y OPERACIÓN
- CONTROL DE ACCESO
- CUMPLIMIENTO

CAPÍTULO II

RESULTADO DE LA EVALUACIÓN DE CONTROL INTERNO

MATRIZ RIESGO-CONFIANZA CONTROL INTERNO					
TEMA	JEFE DEL DEPARTAMENTO	ANALISTA COMPUTO	ASISTENTE COMPUTO 1	ASISTENTE COMPUTO 2	RIESGO PROMEDIO DEL DEPARTAMENTO TECNOLÓGICO
	RIESGO	RIESGO	RIESGO	RIESGO	
CONTROL INTERNO	56,75%	58,74%	66,13%	84,09%	66,43%
DOCUMENTACIÓN	67,31%	70,20%	100%	100%	84,38%
HARDWARE	52,94%	51,47%	52,94%	75%	58,09%
SOFTWARE	50%	54,55%	45,45%	77,27%	56,82%





DESCRIPCIÓN DE LOS GRÁFICOS

Dentro de los porcentajes de la matriz riesgo confianza se observa que el Departamento Tecnológico en la evaluación de las normas de Control Interno como resultado: sobre el componente Documentación el Jefe del Departamento tiene un nivel de riesgo de 67,31%, el Analista de Computo tiene un nivel de riesgo de 70,20%, el Asistente de Computo 1 tiene un nivel de riesgo de 100,00%, el Asistente de Computo 2 tiene un nivel de riesgo de 100,00% , y el riesgo promedio es de 84,38%; sobre el componente de

Hardware el Jefe del Departamento tiene un nivel de riesgo es de 52,94%, el Analista de Computo tiene un nivel de riesgo es de 51,47%, el Asistente de Computo 1 tiene un nivel de riesgo es de 52,94%, el Analista de Computo 2 tiene un nivel riesgo es de 75,00%, y el riesgo promedio es de 58,09%; sobre el componente de Software el Jefe del Departamento tiene un nivel de riesgo es de 50%, el Analista de Computo tiene un nivel de riesgo de 54,55%, el Asistente de Computo 1 tiene un nivel de riesgo de 45,45%, el Asistente de Computo 2 tiene un nivel de riesgo es de 77,27%, y el riesgo promedio es de 56,82%.

De manera general el departamento tecnológico cuenta con un porcentaje de nivel de riesgo por colaborador y por departamento como tal, el Jefe del Departamento tiene un nivel de riesgo de 56,75%, el Analista de Computo tiene un nivel de riesgo de 58,74%, el Asistente de Computo 1 tiene un nivel de riesgo de 66,13%, el Asistente de Computo 2 tiene un nivel de riesgo es de 84,09%. El riesgo promedio por departamento mediante la norma de control interno es de 66,43%.

Es así, que se evidencia que el componente con mayor nivel de riesgo es Documentación con un porcentaje de 84,38% y el componente con menor nivel de riesgo es Software con un porcentaje de 56,82%.

ANÁLISIS DE LOS RIESGOS SEGÚN NORMA DE CONTROL INTERNO

En base a los resultados obtenidos en la evaluación de riesgos según la Norma de Control Interno en Tecnologías de Información 410-09, referente al control y mantenimiento de la infraestructura tecnológica, el departamento tecnológico fue evaluado mediante los componentes de Documentación, Hardware y Software.

Para obtener la siguiente tabla, se evaluó a cada uno de las personas que laboran dentro del departamento tecnológico, donde dio como resultado un

promedio de riesgo por individuo /componente y el riesgo promedio general del departamento, mostrado en la siguiente tabla:

COMPONENTES	RIESGOS
Documentación	84,38%
Hardware	58,09%
Software	56,82%
PROMEDIO RIESGO GENERAL DEL DEPARTAMENTO	66,43%

Se observa así, que el componente de Documentación, muestra un riesgo promedio de 84,38%, el componente de hardware un riesgo promedio de 58,09% y el componente de software un riesgo promedio de 56,82%, debido a que no se llevan a cabo en su totalidad los procedimientos, procesos, sistemas y acuerdos de servicios que serán registrados, evaluados y autorizados de forma previa a su implantación; la falta de bitácoras para su respectiva documentación; la inexistente actualización de todo tipo de manuales técnicos, planes estratégicos y planes operativos para la unidad tecnológica; la insuficiencia de mecanismos lógicos y físicos de seguridad para proteger los recursos tecnológicos; todo esto bajo la exigencia de la Norma de Control Interno de tecnologías de información 410-09 referente al control y mantenimiento de la infraestructura tecnológica y el incumplimiento de los productos y servicios a entregar que lo dispone el registro oficial tecnológico de la Espam Mfl.

EVALUACIÓN Y CALIFICACIÓN DE LOS RIESGOS DE CONTROL INTERNO

De conformidad a la evaluación del control interno a los componentes seleccionados los resultados son los siguientes:

COMPONENTE	JEFE DEL DEPARTAMENTO				ANALISTA DE COMPUTO				ASISTENTE DE COMPUTO 1				ASISTENTE DE COMPUTO 2			
	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR
CONTROL INTERNO	43,25%	BAJO	ALTO	ROJO	41,26%	BAJO	ALTO	ROJO	33,87%	BAJO	ALTO	ROJO	15,91%	BAJO	ALTO	ROJO
DOCUMENTACIÓN	32,69%	BAJO	ALTO	ROJO	29,80%	BAJO	ALTO	ROJO	0,00%	BAJO	ALTO	ROJO	0,00%	BAJO	ALTO	ROJO
HARDWARE	47,06%	BAJO	ALTO	ROJO	48,53%	BAJO	ALTO	ROJO	47,06%	BAJO	ALTO	ROJO	25,00%	BAJO	ALTO	ROJO
SOFTWARE	50%	BAJO	ALTO	ROJO	45,45%	BAJO	ALTO	ROJO	54,55%	MODERADO	MODERADO	AMARILLO	22,73%	BAJO	ALTO	ROJO

RESULTADO DE LAS ENCUESTAS REALIZADAS AL PERSONAL ADMINISTRATIVO Y LAS DIFERENTES CARRERAS DE LA ESPAM MFL

Para la evaluación de las encuestas realizadas al personal que labora en la institución se solicitó al Departamento de Almacén el inventario en donde constaban todos los equipos tecnológicos de dicha institución, tomando como referencia los dos últimos años (2012-2013) para las evaluaciones pertinentes.

Se tomaron en cuenta las dos áreas de la institución:

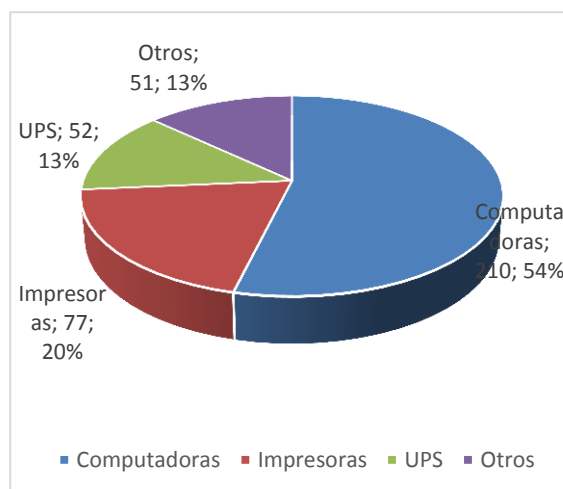
En el Área Agroindustrial en donde se encuentra ubicado Rectorado, Vicerrectorado, Biblioteca, Talleres Agroindustriales, las carreras de Medio Ambiente, Agroindustrias, Turismo, Informática, y todas las áreas administrativas de esta área.

En el Área Agropecuaria en donde se encuentra ubicado la incubadora, las carreras de Agrícola, Pecuaria y Administración y todas las áreas administrativas de esta área.

A continuación se muestran las preguntas realizadas en la encuesta elaborada para evaluar al departamento.

PREGUNTA 1. ¿CUANTOS EQUIPOS TECNOLÓGICOS TIENE A SU CARGO?

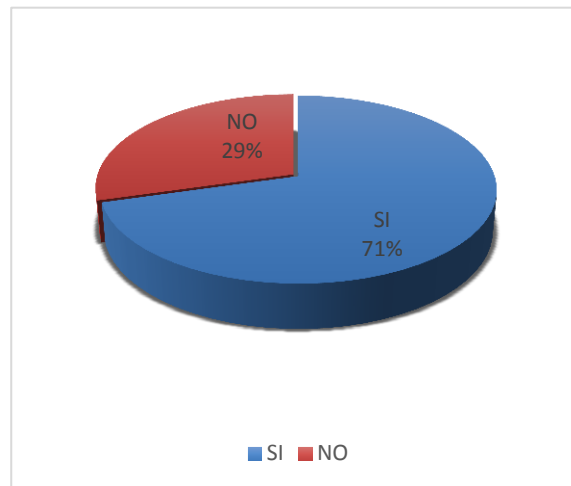
OPCIONES DE RESPUESTA	Nº DE EQUIPOS	%
Computadoras	210	54%
Impresoras	77	20%
UPS	52	13%
Otros	51	13%
TOTAL	390	100%



En las diferentes áreas administrativas y las diferentes carreras de la ESPAM MFL de las cuarenta y cinco (51) encuestas realizadas a los custodios de la institución, se obtuvieron como resultado que existen; 210 computadoras incluidas de escritorios y portátiles que constituye a un 54%, 77 Impresoras que constituyen a un 20%, 52 UPS que constituyen a un 13% y 51 en otros equipos que constituyen a un 13 %, dando como resultado 390 equipos tecnológicos que equivale a un 100%.

PREGUNTA 2. ¿LES HAN REALIZADO MANTENIMIENTO PREVENTIVO A SUS EQUIPOS TECNOLÓGICOS?

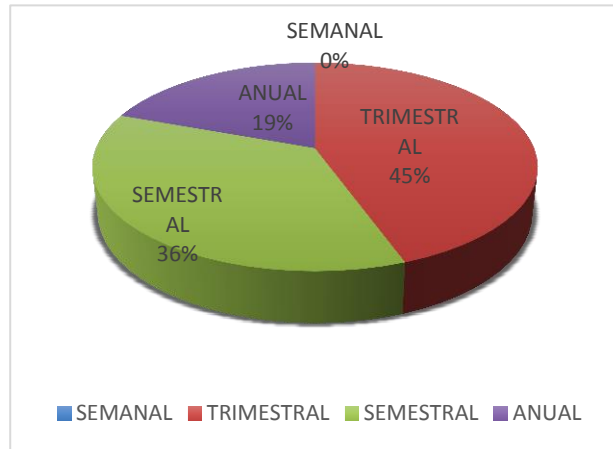
OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
SI	36	71%
NO	15	29%
TOTAL	51	100%



En las diferentes áreas administrativas y las diferentes carreras de la ESPAM MFL de las cuarenta y cinco (51) encuestas realizadas a los custodios de la institución, se obtuvieron como resultado que; 36 custodios dieron como respuestas que **SI** les realizaban mantenimientos preventivos y constituye a un 71%, mientras que los otros 15 dieron como respuesta que **NO** se les realizaba mantenimientos a los equipos tecnológicos que tienen a su cargo con un porcentaje de 29% , dando como resultado un total de 51 respuestas que equivale a un 100%.

EN CASO DE QUE LA RESPUESTA SEA SI CADA QUE TIEMPO SE LO REALIZA:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
SEMANTAL	0	0%
TRIMESTRAL	16	45%
SEMESTRAL	13	36%
ANUAL	7	19%
TOTAL	36	100%



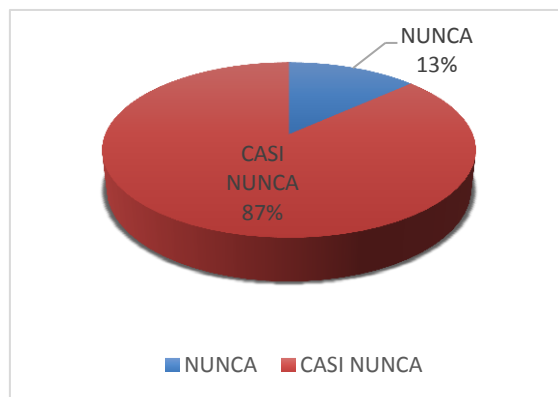
EL TIEMPO EN QUE TARDA EL MANTENIMIENTO ES

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
MUCHO TIEMPO	4	11%
POCO TIEMPO	23	64%
LO ESPERADO PARA CONTINUAR ACTIVIDADES	9	25%
TOTAL	36	100%



EN CASO DE QUE LA RESPUESTA SEA NO:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
NUNCA	2	13%
CASI NUNCA	13	87%
TOTAL	15	100%

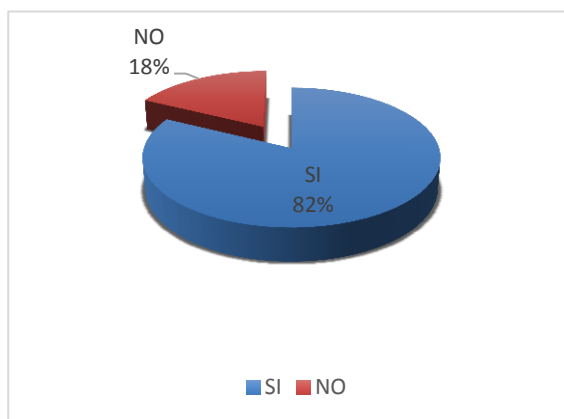


Como se puede observar mediante esta segunda pregunta las autoras de esta auditoria obtuvieron como resultado que el 71% de los encuestados corresponden al total de 36 encuestados, que son custodios de los equipos tecnológicos, y según los resultados SI les dan mantenimiento preventivo a los

equipos; el tiempo que se lo realiza corresponde al 45% TRIMESTRAL, 36% SEMESTRAL y el 19% ANUAL; el tiempo en que tarda el mantenimiento corresponde al 11 % MUCHO TIEMPO, 64% POCO TIEMPO y 25% LO ESPERADO PARA CONTINUAR LAS ACTIVIDADES, mientras que el 29% de los encuestados que corresponden al total de 15 encuestados de los custodios dicen que NO les dan mantenimiento preventivo a sus equipos, NUNCA el 13% y CASI NUNCA el 87%.

PREGUNTA 3. ¿LES HAN REALIZADO MANTENIMIENTO CORRECTIVO A SUS EQUIPOS TECNOLÓGICOS?

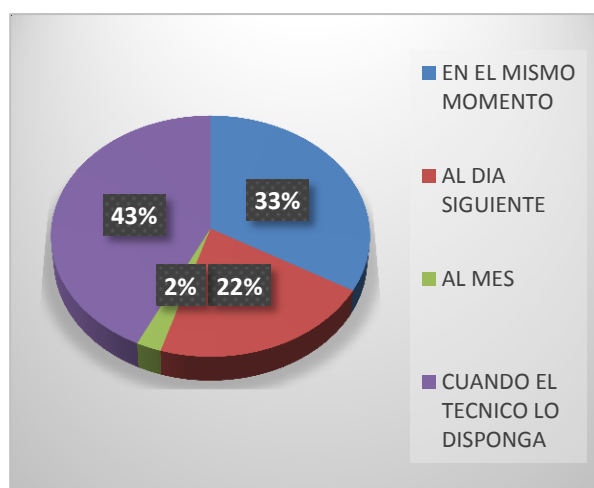
OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
SI	42	82%
NO	9	18%
TOTAL	51	100%



En las diferentes áreas administrativas y las diferentes carreras de la ESPAM MFL de las cuarenta y cinco (51) encuestas realizadas a los custodios de la institución, se obtuvieron como resultado que; 42 custodios dieron como respuestas que **SI** les realizaban mantenimientos preventivos y constituye a un 82%, mientras que los otros 9 dieron como respuesta que **NO** se les realizaba mantenimientos a los equipos tecnológicos que tienen a su cargo, dando como resultado un total de 48 respuestas que equivale a un 18%.

EN CASO DE QUE LA RESPUESTA SEA SI CADA QUE TIEMPO SE LO REALIZA:

OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
EN EL MISMO MOMENTO	14	33%
AL DÍA SIGUIENTE	9	22%
AL MES	1	2%
CUANDO EL TÉCNICO LO DISPONGA	18	43%
TOTAL	40	100%



EN CASO DE QUE LA RESPUESTA SEA NO:

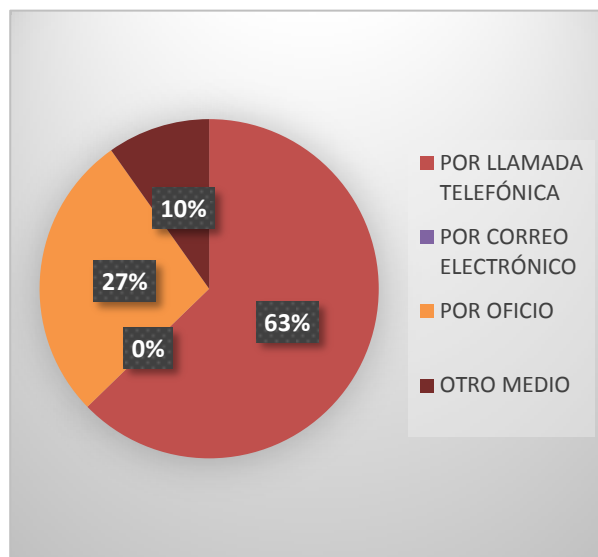
OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
NUNCA	3	33%
CASI NUNCA	0	0%
CUANDO EL EQUIPO LO REQUIERA	6	67%
TOTAL	7	100%



Como resultado se obtuvo en esta tercera pregunta del total de 51 encuestados, el 82% corresponden a el total de 42 encuestados de los custodios de los equipos tecnológicos y al que SI les hacen mantenimiento correctivo a los mismos, y el tiempo que toma la entrega corresponde al 43% que es CUANDO EL TÉCNICO LO DISPONGA, un 33% es EN EL MISMO MOMENTO y el 22% AL DIA SIGUIENTE y el 2% AL MES, mientras que el 18% correspondiente al total de 9 encuestados de los custodios, NO les hacen mantenimiento correctivo a sus equipos, solamente cuando el equipo lo disponga que es el 67% y el 33% NUNCA.

PREGUNTA 4: ¿CÓMO SE REALIZA LA SOLICITUD DE MANTENIMIENTO SEA PREVENTIVO O CORRECTIVO?

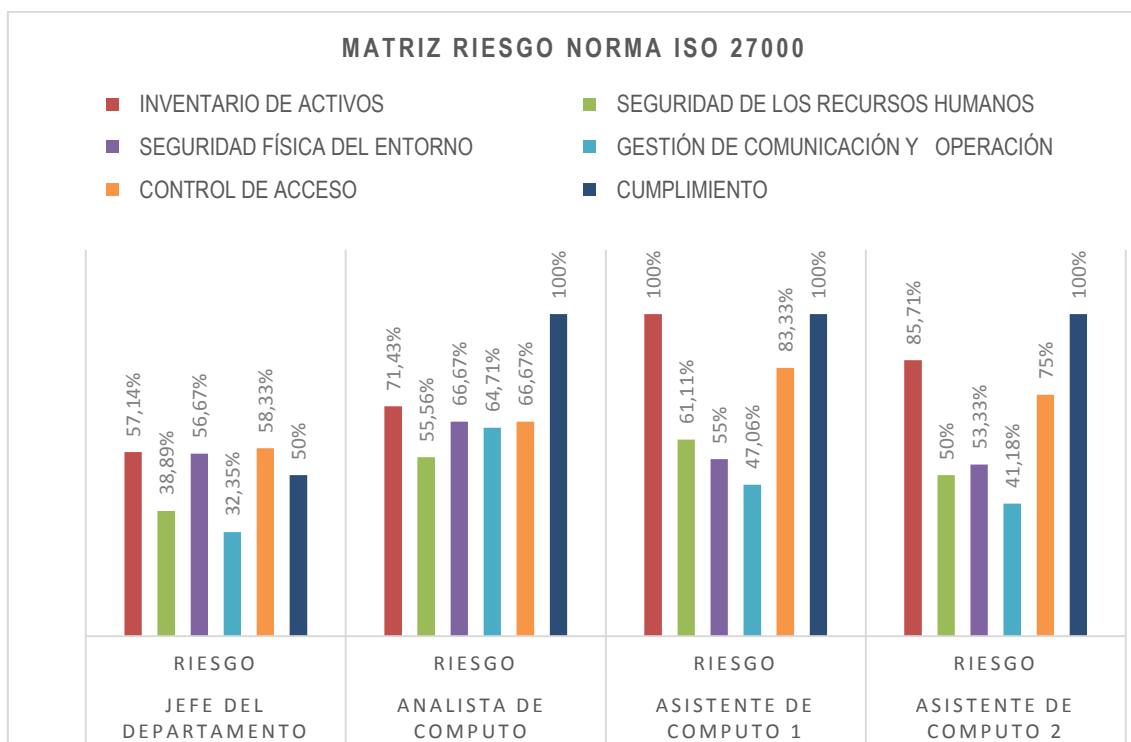
OPCIONES DE RESPUESTAS	Nº DE RESPUESTAS	%
POR LLAMADA TELEFÓNICA	32	63%
POR CORREO ELECTRÓNICO	0	0%
POR OFICIO	14	27%
OTRO MEDIO	5	10%
TOTAL	51	100%



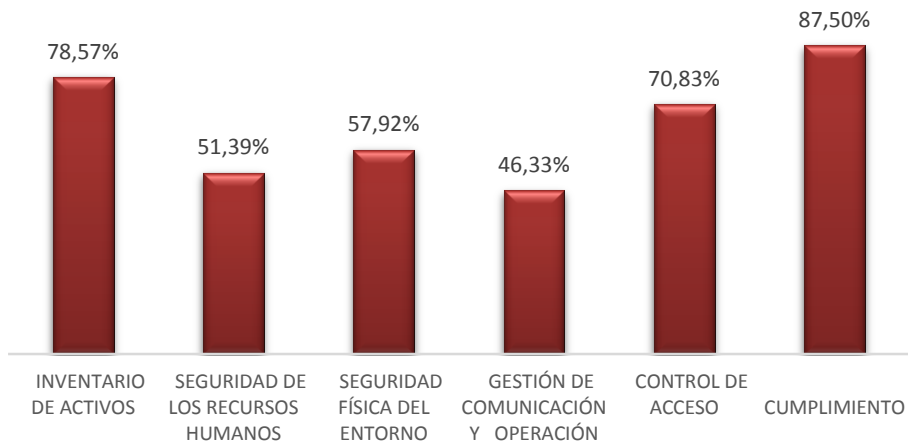
Como resultado en esta cuarta pregunta se obtuvo que del total de 51 encuestados, el 63% corresponden a los custodios de los equipos tecnológicos hacen la solicitud del mantenimiento ya sea preventivo o correctivo por medio de LLAMADA TELEFÓNICA, mientras el 27% corresponde POR OFICIO y un 10% lo hace POR OTRO MEDIO.

RESULTADO DE LA EVALUACIÓN DE LA NORMA ISO 27000

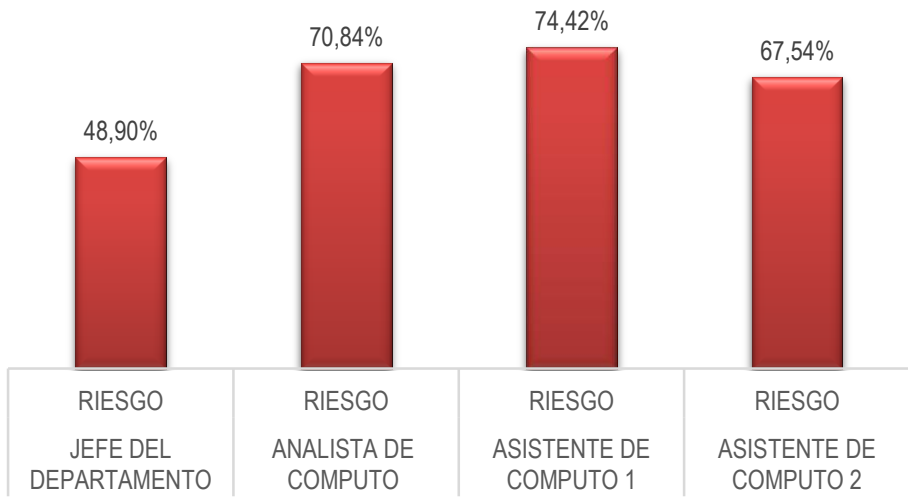
MATRIZ CONFIANZA-RIESGO NORMA ISO 27000					
TEMA	JEFE DEL DEPARTAMENTO	ANALISTA DE COMPUTO	ASISTENTE DE COMPUTO 1	ASISTENTE DE COMPUTO 2	RIESGO PROMEDIO DEL DEPARTAMENTO TECNOLÓGICO
	RIESGO	RIESGO	RIESGO	RIESGO	
NORMA ISO 27000	48,90%	70,84%	74,42%	67,54%	65,42%
INVENTARIO DE ACTIVOS	57,14%	71,43%	100%	85,71%	78,57%
SEGURIDAD DE LOS RECURSOS HUMANOS	38,89%	55,56%	61,11%	50%	51,39%
SEGURIDAD FÍSICA DEL ENTORNO	56,67%	66,67%	55%	53,33%	57,92%
GESTIÓN DE COMUNICACIÓN Y OPERACIÓN	32,35%	64,71%	47,06%	41,18%	46,33%
CONTROL DE ACCESO	58,33%	66,67%	83,33%	75%	70,83%
CUMPLIMIENTO	50%	100%	100%	100%	87,50%



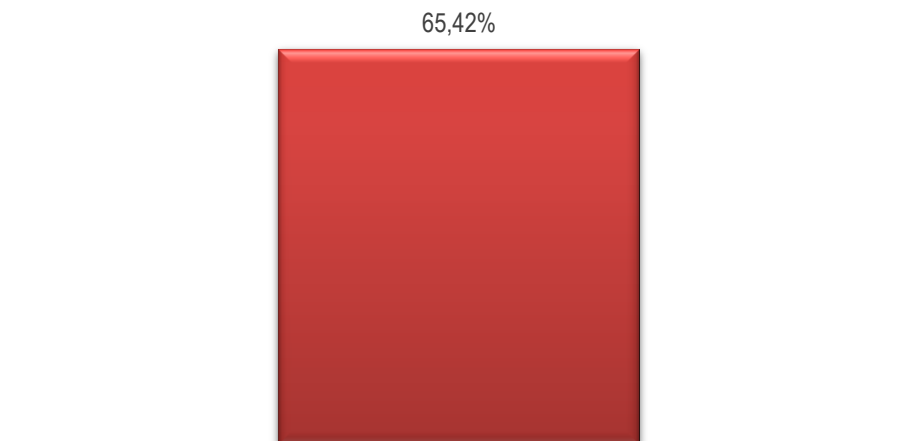
RIESGO PROMEDIO POR COMPONENTE DEL DEPARTAMENTO TECNOLÓGICO



RIESGO GENERAL POR INDIVIDUO NORMA ISO 27000



RIESGO PROMEDIO DEL DEPARTAMENTO TECNOLÓGICO



DESCRIPCIÓN DE LOS GRÁFICOS

Dentro de los porcentajes de la matriz riesgo confianza se observa que el Departamento dentro la evaluación de la norma ISO 27000 dio como resultado: sobre el componente Inventario de Activos del Jefe del Departamento tiene un nivel de riesgo de 57,14%, el Analista de Computo tiene un nivel riesgo es de 71,43%, el Asistente de Computo 1 tiene un nivel de riesgo es de 100,00% , el Asistente de Computo 2 tiene un nivel de riesgo es de 85,71% , y el nivel de riesgo promedio del departamento es de 78,57%; sobre el componente Seguridad de los Recursos Humanos el Jefe de Computo tiene un nivel de riesgo de 38,89%, el Analista de Computo tiene un nivel de riesgo de 55,56%, el Asistente de Computo 1 tiene un nivel de riesgo de 61,11%, el Analista de Computo 2 tiene un nivel de riesgo es de 50%, y el riesgo promedio del departamento es de 51,39%; sobre el componente Seguridad Física del Entorno el Jefe de Computo tiene un nivel de riesgo de 56,67%, el Analista de Computo tiene un nivel de riesgo de 66,67%, el Asistente de Computo 1 tiene un nivel de riesgo de 55%, el Asistente de Computo 2 tiene un nivel de riesgo de 53,33%, y el riesgo promedio del departamento es de 57,92%; sobre el componente Gestión de Comunicación y Operación el Jefe de Computo tiene un nivel de riesgo de 32,35%, el Analista de Computo tiene un nivel de riesgo de 64,71%, el Asistente de Computo 1 tiene un nivel de riesgo de 47,06%, el Asistente de Computo 2 tiene un nivel de riesgo de 41,18%, y riesgo promedio del departamento es de 46,33%; sobre el componente Control de Acceso el Jefe de Computo tiene un nivel de riesgo es de 58,33%, el Analista de Computo tiene un nivel de riesgo de 66,67%, el Asistente de Computo 1 tiene un nivel de riesgo de 83,33%, el Asistente de Computo 2 tiene un nivel de riesgo de 75%, y el riesgo promedio del departamento es de 70,83%; sobre el componente Cumplimiento el Jefe de Computo tiene un nivel de riesgo es de 50%, el Analista de Computo tiene un nivel de riesgo de 100,00%, el Asistente de Computo 1 tiene un nivel de riesgo de 100,00%, el Asistente de Computo 2 tiene un nivel de riesgo de 100,00%, y riesgo promedio del departamento es de 87,50%.

De manera general el departamento tecnológico cuenta con unos porcentajes de riesgo por colaborador y por departamento como tal, el Jefe del Departamento tiene un nivel de riesgo promedio en la evaluación de la NORMA ISO 27000 de 48,90%, el Analista de Computo tiene un nivel de riesgo promedio en la evaluación de la NORMA ISO 27000 de 70,84%, el Asistente de Computo 1 tiene un nivel de riesgo promedio en software de 74,42%, el Asistente de Computo 2 tiene un nivel de riesgo promedio en la evaluación de la NORMA ISO 27000 de 67,54%. El riesgo promedio por departamento mediante la NORMA ISO 27000 es de 65,42%.

Es así, que se evidencia que el componente con mayor nivel de riesgo es de 87,50% que equivale al componente de cumplimiento y el componente con menor nivel de riesgo es el de Gestión de Comunicación y Operación con 46,33%.

11.2. ANÁLISIS DE LOS RIESGOS SEGÚN NORMA ISO 27000

En base a los resultados obtenidos en la evaluación de riesgos según la Norma ISO 27000, el departamento tecnológico fue evaluado mediante los componentes de Inventario de Activos, Seguridad de los Recursos Humanos, Seguridad Física y del Entorno, Gestión de Comunicación y Operación, Control de Acceso y Cumplimiento.

Para obtener la siguiente tabla, se evaluó a cada uno de las personas que laboran dentro del departamento tecnológico, donde dio como resultado un promedio de riesgo por individuo /componente y el riesgo promedio general del departamento, mostrado en la siguiente tabla:

COMPONENTES	RIESGOS
Inventario de Activos	78,57%
Seguridad de los Recursos Humanos	51,39%
Seguridad Física y del Entorno	57,92%
Gestión de Comunicación y Operación	46,33%
Control de Acceso	70,83%
Cumplimiento	57,14%
PROMEDIO RIESGO GENERAL DEL DEPARTAMENTO	65,42%

Procediendo al análisis, se observa, que el componente de Inventario de Activos, muestra un riesgo promedio de 78,57%, debido a que no se cumple en su totalidad el control de inventario de Activos Tecnológicos, como lo dispone la Norma ISO 27000.

El componente de Seguridad de los Recursos Humanos, con un riesgo promedio de 51,39%, no cumple con todas las disposiciones que exige la Norma ISO 27000, como lo es de tener un Manual de Funciones y Responsabilidades actualizados, y no hacen la respectiva formalidad de la devolución de los activos tecnológicos.

En el componente de Seguridad Física y del Entorno, con un riesgo promedio de 57,92%, como lo dispone la Norma ISO 27000, acerca de los perímetros de de la seguridad física del entorno, la protección contra amenazas externas y ambientales de los equipos tecnológicos, seguridad de cableados, ubicación y protección de los equipos tecnológicos, áreas seguras, seguridad de los equipos fuera de las instalaciones y seguridad en la reutilización de los equipos, no se está cumpliendo en su totalidad como lo exige la ley.

En el componente de Gestión de Comunicación y Operación, con un riesgo promedio de 46,33%, es debido a que solo se lleva en partes la respectiva documentación de los procedimientos de operación, gestión del cambio, distribución de funciones, separación de áreas, realización de proyecciones de los requerimientos de capacidad futura, control contra códigos maliciosos, respaldo de la información, controles a las redes, seguridad de los servicios de la red, registros de auditoria, como lo dispone la Norma ISO 27000.

En el componente de Control de Acceso, con un riesgo promedio de 70,83%, se debe a que no se cumple a cabalidad las políticas de control de acceso, registros de usuarios, políticas de uso de los servicios de red, identificación de los equipos en la redes, control de conexiones a las redes, control de accesos remotos como lo dispone la Norma ISO 27000.

En el componente de Cumplimiento, con un riesgo promedio de 87,50%, la Norma ISO 27000 refiere a la Identificación de la legislación aplicable: Inventario de todas las Normas legales que utiliza la institución, y controles de auditorías de los sistemas de información, que el departamento tecnológico debe cumplir porque así lo exige esta Norma, y no se está llevando a cabo.

12. EVALUACIÓN Y CALIFICACIÓN DE LOS RIESGOS NORMA ISO 27000

COMPONENTE	JEFE DEL DEPARTAMENTO				ANALISTA DE COMPUTO				ASISTENTE DE COMPUTO 1				ASISTENTE DE COMPUTO 2			
	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR	CALIFICACIÓN PORCENTUAL	GRADO DE CONFIANZA	NIVEL DE RIESGO	COLOR
NORMA ISO 27000	51,10%	MODERADO	MODERADO	AMARILLO	29,16%	BAJO	ALTO	ROJO	25,67%	BAJO	ALTO	ROJO	32,46%	BAJO	ALTO	ROJO
INVENTARIO DE ACTIVOS	42,86%	BAJO	ALTO	ROJO	28,57%	BAJO	ALTO	ROJO	0,00%	Fuera de Rango	Fuera de Rango	sin color	14,29%	Fuera de Rango	Fuera de Rango	sin color
SEGURIDAD DE LOS RECURSOS HUMANOS	61,11%	MODERADO	MODERADO	AMARILLO	44,44%	BAJO	ALTO	ROJO	39,00%	BAJO	ALTO	ROJO	50,00%	BAJO	ALTO	ROJO
SEGURIDAD FÍSICA DEL ENTORNO	43,33%	BAJO	ALTO	ROJO	33,33%	BAJO	ALTO	ROJO	45,00%	BAJO	ALTO	AMARILLO	46,67%	BAJO	ALTO	ROJO
GESTIÓN DE COMUNICACIÓN Y OPERACIÓN	67,61%	MODERADO	MODERADO	AMARILLO	35,29%	BAJO	ALTO	ROJO	53,00%	MODERADO	MODERADO	AMARILLO	58,82%	MODERADO	MODERADO	AMARILLO
CONTROL DE ACCESO	41,67%	BAJO	ALTO	ROJO	33,33%	BAJO	ALTO	ROJO	17,00%	BAJO	ALTO	ROJO	25,00%	BAJO	ALTO	ROJO
CUMPLIMIENTO	50,00%	BAJO	ALTO	ROJO	0,00%	Fuera de Rango	Fuera de Rango	sin color	0,00%	Fuera de Rango	Fuera de Rango	sin color	0,00%	Fuera de Rango	Fuera de Rango	sin color

OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE CHECKLIST NORMA DE CONTROL INTERNO

<p>ESPAM MFL ANÁLISIS MEDIANTE LA NORMA 410 DE CONTROL INTERNO</p>
<p>Objetivo/Ámbito: El presente análisis es con la finalidad de dar conocer la verificación del nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.</p>
<p>Área auditada: Departamento Tecnológico de la ESPAM MFL</p>
<p>Personal Auditado: Jefe del Departamento, Analista de Computo, Asistente de Computo 1 y Asistente de Computo 2</p>
<p>DOCUMENTACIÓN</p>
<p>OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:</p>
<p>La Institución cuenta con un organigrama</p>
<p>El departamento tecnológico no cuenta con un organigrama actualizado, existe uno como Jefatura de Cómputo, y debido a esta observación las auditoras proponen un organigrama para el área auditada.</p>
<p>El Manual de Funciones y Responsabilidades no está actualizado porque consta como Jefatura de Computo, y según la Norma de Control Interno de TI 410-09, refiere a que todos los Manuales técnicos, funciones, políticas y procedimientos deben ser actualizados</p>
<p>No tienen delimitadas las funciones y responsabilidades en el departamento, por esta razón en la actualidad no existe la debida asignación de funciones como lo dispone la Norma de Control Interno de TI 410-09.</p>
<p>La Planificación de Mantenimientos de Equipos de Redes, Computación y Software Base, está como Jefatura de Computo, no tiene fecha de cuando fue elaborada, debería ser actualizada para el departamento tecnológico como lo dispone la Norma de Control TI 410-09.</p>
<p>Los diferentes mantenimientos (preventivo, correctivo) en la institución, no se los realiza con la debida autorización del Jefe del Departamento</p>
<p>La solicitud de los diferentes mantenimientos (preventivo, correctivo) que brinda el departamento tecnológico se lo realiza de manera verbal o por medio de vía telefónica.</p>
<p>Actualmente se hacen los mantenimientos preventivos cada 3 meses y los correctivos cuando el equipo tecnológico lo requiera, aunque no tienen una Planificación de Mantenimientos Programados.</p>
<p>No cuenta con Políticas y Procedimientos el Departamento Tecnológico.</p>
<p>No se lleva un control de los equipos en garantía.</p>
<p>El departamento tecnológico no lleva un control de inventarios de los equipos de computación y software a excepción de los equipos de comunicación y redes, que se llevan en un 30% en archivos Excel.</p>
<p>No se dispone de ningún tipo de bitácoras para el registro de fallas de los equipos.</p>

Se poseen registros individuales de los equipos tecnológicos en el Departamento de Almacén, aunque también debería llevarlos el departamento tecnológico como lo refiere la Norma de Control Interno de TI 410-09.
No se realizan revisiones periódicas de los equipos computación y software base.
Se realizan revisiones cada semana a los equipos de las redes.
No aplican metodologías para planificar las revisiones de los equipos tecnológicos en general.
El Departamento no cuenta con un Plan de Contingencia.
El departamento tecnológico realiza el respaldo de la información de los equipos formateados en dispositivos externos, pero no son registrados ni almacenados para su conservación, una vez devuelta la información al equipo formateado, se elimina la información respaldada.
No existen controles de acceso a las computadoras del personal administrativo.
Si existen controles de acceso a las redes inalámbricas de la institución.
Si existen controles de acceso a los servidores.
No se llevan registros estadísticos del uso de la red.
El departamento tecnológico administra las contraseñas de admisión de las redes.
Las contraseñas de admisión son abiertas en un 50% debido a que sus usuarios son estudiantes de las diferentes áreas en la institución.
Se han realizado auditorías al departamento tecnológico por parte de la Contraloría General del Estado, sin embargo no se han aplicado las recomendaciones pertinentes de dichas evaluaciones.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma de Control Interno que emite la Contraloría General del Estado Ecuatoriano.
HARDWARE
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
El departamento no cuenta con un servicio de mantenimiento para todos los equipos tecnológicos en general.
El mantenimiento de los equipos tecnológicos se lo realiza cada 3 meses o cuando hay algún problema o falla.
Existe un plan de mantenimiento para los equipos tecnológicos como Jefatura de Cómputo.
No cuentan con un control y registro de los mantenimientos realizados.
Los equipos tecnológicos que tienen garantía, el proveedor realiza el mantenimiento fuera de la institución y se llevan éstos con discos duros.
No se tienen criterios de evaluación de rendimiento de los equipos de computación, solamente se hace el criterio de evaluación de funcionalidad de los equipos.

La administración de las bases de datos y los servidores lo lleva la Carrera de Informática y no el Departamento Tecnológico, como la Carrera Informática es de área Educativa y no de área administrativa como lo es el departamento tecnológico, entonces la administración de las bases de datos y servidores incluyendo la producción de software debería ser llevados por éste, reformando su estructura de acuerdo al organigrama propuesto por las auditoras y con personal capacitado para llevar el control de dicha administración.
El registro de los equipos de computación, no los lleva el departamento tecnológico, esto lo hace el departamento de Almacén, sin embargo debería llevarlo también el departamento porque esto lo dispone la Norma de Control Interno TI 410-09
No se tienen acceso remoto a las redes.
No se tiene un registro de los puntos de acceso que existen en la institución.
La seguridad de las redes inalámbricas es WPA WPA2 dentro de la institución.
No se realiza la relevación de los costos en mantenimientos de equipos en general de los últimos años.
No se evidencian los tiempos de mantenimiento.
No se realiza el seguimiento de los controles de los componentes de los equipos tecnológicos de la institución.
No se realiza el seguimiento a los controles de equipos que ya fueron cambiados por garantía.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma de Control Interno que emite la Contraloría General del Estado Ecuatoriano.
SOFTWARE
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
Se realiza el mantenimiento del software base dentro de la Institución, solamente cuando este lo requiera y que su versión sea compatible con el equipo.
Se evalúa el funcionamiento del software base en el momento que se instala y cada año después de instalado, sin embargo no se llevan registros de su funcionamiento.
No se actualiza el software base, solo cuando lo requiere el usuario o la nueva versión sea compatible con el equipo.
Las licenciaturas del software base son actualizadas cada año.
El tipo de licenciaturas que tiene la Universidad es institucional, no estudiantil.
No existen procedimientos para hacer las diferentes actualizaciones.
No todos los equipos de computación tienen instalados los antivirus.
Los programas instalados en los equipos tecnológicos, para las actividades de la institución son paquete Office, Antivirus, PDF, WinRAR.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma de Control Interno que emite la Contraloría General del Estado Ecuatoriano.

OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE CHECKLIST NORMA ISO 27000

ESPAM MFL ANÁLISIS MEDIANTE LA NORMA ISO 27000
Objetivo/Ámbito: El presente análisis es con la finalidad de dar conocer la verificación del nivel de cumplimiento de procedimientos de control y mantenimiento de los bienes o activos tecnológicos de la institución.
Área auditada: Departamento Tecnológico de la ESPAM MFL
Personal Auditado: Jefe del Departamento, Analista de Computo, Asistente de Computo 1 y Asistente de Computo 2
INVENTARIO DE ACTIVOS
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
En consideración a la Norma ISO 27000 con respecto a la Gestión de activos, en el punto de Inventario de activos, refiere que se debe inventariar los activos primarios en formatos físicos y/o electrónicos, también los activos de soporte de Hardware, Software y Redes, debe tener un plan estratégico, y que los activos tengan asignados un responsable del activo, lo que el departamento tecnológico no cumple con lo siguiente:
No tiene un Plan Estratégico
No llevan el control de inventario de hardware y software con sus respectivos formatos como lo estipula la norma ISO 27000.
Del inventario de comunicación y redes solo se lleva el 30 % de su totalidad, en forma electrónico (digital), mostrando evidencia en archivos Excel, quien lleva el control del inventario de activos tecnológicos (hardware, software, redes) en su totalidad, es el departamento de almacén.
Con respecto a los custodios asignados a los equipos tecnológicos, si se hace la respectiva asignación, lo que no se hace es la debida formalidad del cambio inmediato cuando éste termina su contrato de trabajo en el área asignada o en la entidad como lo estipula la Norma ISO 27000. (Inventario desactualizado por parte de Almacén)
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
SEGURIDAD DE LOS RECURSOS HUMANOS
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CUESTIONARIOS:
Mediante la siguiente observación dentro del Departamento tecnológico, se socializan los procedimientos de mantenimiento preventivo, correctivo de los bienes: Hardware, Software y equipos de comunicación de redes, con respecto a trabajos técnicos, y en cuánto a la documentación que se deja como constancia en las hojas de registros e informes que evidencien la realización de los mantenimientos no se está llevando a cabo como lo dispone la Norma ISO 27000.
Se responsabiliza a cada custodio por el mal uso y destrucción de los equipos tecnológicos asignados y entregados al responsable, este proceso lo realiza el Departamento de Almacén y no el Departamento Tecnológico.
Con respecto a las responsabilidades del Departamento, no existe una planificación ni procedimientos para la distribución de tareas.

El personal que labora en el departamento tecnológico, desconoce los objetivos establecidos para el departamento y también si éstos han sido definidos por escrito.
Como lo estipula la Norma ISO 27000 sobre el proceso de devolución de los activos tecnológicos en la terminación del contrato de trabajo, no se cumple con la totalidad de dicho proceso, ya que cuando se termina el contrato del custodio del equipo, las actas de entrega no se las realiza en el tiempo debido y con la formalidad respectiva que debe hacerse, y solo se reporta al Departamento de Almacén, hasta que se haga el trámite correspondiente. Además el departamento tecnológico también debería llevar estas actas de entrega como lo dispone la Norma ISO 27000 en referencia al Inventario de activos.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
SEGURIDAD FÍSICA DEL ENTORNO
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
De acuerdo a las observaciones pertinentes y según la norma ISO 27000 con respecto a la protección contra amenazas externas y ambientales, la ubicación de los equipos de repuestos y soportes deben estar a una distancia prudente para evitar daños en caso de desastre que afecten las instalaciones principales, la cual el Departamento tecnológico no cuenta con estas áreas de protección de equipos tecnológicos, incluso el departamento no tiene una estructura física adecuada para resguardar la seguridad de sus equipos en caso de algún desastre.
El 20% de las áreas en la universidad no tienen ubicado los equipos contra incendios.
El área de mantenimiento a las instalaciones eléctricas, al sistema de climatización y ductos de ventilación, no lo realiza el Departamento Tecnológico porque le compete al Departamento de Construcción.
Existen cámaras de seguridad para minimizar el riesgo de robos de equipos tecnológicos, sin embargo no se puede determinar si existe el debido control que permita verificar el funcionamiento de las mismas.
Todas las áreas de la institución tienen protección contra descargas eléctricas, y disponen de filtros protectores en el suministro de energía y en las líneas de comunicación, y quien lleva todas estas actividades es el departamento de Construcción.
El 87% de los equipos tecnológicos no tienen ups, esto se pudo determinar mediante las encuestas realizadas a los custodios de equipos a su cargo.
El 30% de las áreas con cableado de red en la institución no se protege contra la intersección o daño.
El 20% de las áreas de la institución no hacen la respectiva separación del cableado de la red con el cableado de energía.
No se pudo verificar si se separa el cableado de la red con el cableado de energía en el Data Center, ya que las políticas de acceso no permitieron la debida constatación de la separación del cableado.
Se realiza la identificación y rotulación del cableado de red de acuerdo a las normas locales (RTE INEN 098) e internacionales (ISO) en un 30%.
El departamento tecnológico dispone del 20% de documentación, el 80% en diseños/planos y de la distribución de conexiones de datos de redes inalámbricas y alámbricas.
De acuerdo a las especificaciones y recomendaciones del proveedor, el departamento tecnológico les da mantenimientos periódicos a los equipos y dispositivos tecnológicos.
El personal que labora en el departamento tecnológico, está calificado y autorizado para ser los únicos que den los servicios de mantenimientos a los equipos tecnológicos de la institución. Esto se evidencia con sus hojas de vida de cada uno de los individuos.

No se lleva ni se conservan los registros de los mantenimientos preventivos, correctivos o de fallas con causas no determinadas.
No se establecen controles de mantenimientos programados en el departamento, no hay un cronograma de actividades, ni un plan de mantenimiento actual, solamente existe un plan de mantenimiento cuando el departamento tenía el nombre de Jefatura de Cómputo pero no es aplicado en la actualidad.
No se custodian los equipos y medios que se encuentran fuera de las instalaciones de la institución, pero si se hacen firmar actas de responsabilidad y entrega del equipo a la persona que llevará este fuera de la entidad.
La institución No establece una cobertura adecuada del seguro (robo, incendio o mal uso del equipo) para proteger los equipos que se encuentran fuera de las instalaciones de la institución.
En la institución existen controles de acceso a las redes inalámbricas, cuando detectan muchas personas accediendo a las redes, ellos hacen el cambio inmediato de las contraseñas.
Se llevan controles de acceso a los servidores
No se realiza el correctivo para la evaluación de los dispositivos deteriorados que contengan información sensible antes de enviar a reparación.
Se utiliza la Técnica de formateo para borrar, destruir o sobrescribir la información sensible de un equipo reutilizado, pero esto no asegura el borrado seguro de la información.
Los retiros de los equipos tecnológicos o cualquier información de éste, se lo realiza con la previa autorización del custodio.
Existen personas autorizadas con su identificación respectiva para el retiro de los activos de la institución.
El registro de los equipos o activos que se retiran o se devuelven en la institución lo hace el Departamento de Almacén.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
GESTIÓN DE COMUNICACIÓN Y DE OPERACIÓN
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
No se documenta el proceso de respaldo y restauración de la información.
No se documentan las instrucciones para el manejo de errores y otras condiciones que pueden surgir mediante ejecución de tareas.
No se documentan los procedimientos para el reinicio y recuperación del sistema en caso de fallas.
No se planifica el proceso de cambio y no se realiza la prueba correspondiente.
No se establecen responsables y procedimientos formales de control de cambios de procesos en los equipos y software.
No se aprueban de manera formal los cambios propuestos.
No está actualizado el Manual de Funciones y Responsabilidades del Departamento Tecnológico, existe uno como Jefatura de Cómputo.
No se realizan proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos como lo dispone la Norma ISO referente a la Gestión de Capacidad.
Se instalan y actualizan cada 6 meses el software de antivirus contra código malicioso.
Se mantienen los sistemas operativos actualizados con parches y actualizaciones disponibles, dependiendo de la máquina si soporta la versión actual.
No existen procedimientos de respaldo de información en el Departamento Tecnológico antes del mantenimiento.

La Norma ISO 27000 dispone en los controles de redes, que se debe separar el área de redes con el área de operaciones, y el departamento tecnológico no está cumpliendo con esta disposición.
No se designan responsabilidades para la asistencia de equipos remotos.
Se realizan diseños antes de la implementación de una red, en un 80% muestran evidencia.
No revisan alertas o fallas del sistema operativo
Realizan cambios de configuración de los controles de seguridad del sistema operativo
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
CONTROL DE ACCESO
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
Se identifican y se documentan los equipos que se encuentran en las redes, pero no en su totalidad.
Se tiene documentada la identificación de los equipos que están permitidos, según la red que corresponda.
No se implementan procedimientos para controlar la instalación de software en sistemas operativos
No se lleva un control y registro de auditoría de las actualizaciones de software que se realizan.
No se tienen restricciones de cambios de paquetes de software.
No se lleva un control de versiones para todas las actualizaciones de software.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000
CUMPLIMIENTO
OBSERVACIONES ENCONTRADAS MEDIANTE LA APLICACIÓN DE LOS CHECKLIST:
Con los resultados obtenidos en los checklist, y de acuerdo a la Norma ISO 27000 referente al cumplimiento de la legislación aplicable en la institución, el personal que labora en el departamento tecnológico, no está considerando todas las normas y leyes más generales en cuanto a gestión de datos e información electrónica como lo estipula la Norma.
NOTA: Todos estos puntos deben cumplirse de manera obligatoria porque lo exige la norma ISO 27000

NIVEL DE MADUREZ DE LOS PROCESO ESTUDIADOS EN EL DEPARTAMENTO TECNOLÓGICO

COMPONENTES	CONFIANZA PROMEDIO DEL DEPARTAMENTO	ESTADO DE NIVEL DE MADUREZ DE LOS PROCESOS	NIVEL DE MADUREZ DEL DE LOS PROCESOS	NIVEL DE MADUREZ DEL DEPARTAMENTO TECNOLÓGICO
Cumplimiento	12,50%	Inicial	1	ESTADO INICIAL NIVEL 1,5
Documentación	15,62%	Inicial	1	
Inventario de Activos	21,43%	Inicial	1	
Control de Acceso	29,17%	Inicial	1	
Hardware	41,91%	Gestionado	2	
Seguridad Física del Entorno	42,08%	Gestionado	2	
Software	43,18%	Gestionado	2	

Seguridad de los Recursos Humanos	48,61%	Gestionado	2	
Comunicación y operación	53,68%	Gestionado	2	

CRITERIOS DE EVALUACIÓN DE LOS PROCESOS ESTUDIADOS EN EL DEPARTAMENTO TECNOLÓGICO

NIVEL DE MADUREZ	DESCRIPCIÓN DEL NIVEL DE MADUREZ	CUMPLIMIENTO DE LAS NORMAS CONTROL INTERNO de TI 410-09 E ISO 27000
1	El componente de Cumplimiento de acuerdo a su nivel de confianza 12,50% se encuentra en el estado de madurez Inicial, debido a que se cumplen parcialmente con las normas de ley en sistemas de información y también el personal no conoce en su totalidad las leyes tanto nacionales como internacionales para la aplicación de la misma. El riesgo es de un 87,50% para el departamento tecnológico.	Se está cumpliendo parcialmente con la Norma ISO 27000 referente a Cumplimiento.
1	El componente de documentación de acuerdo a su nivel de confianza 15,62% se encuentra en el estado de madurez Inicial, debido a que hay políticas, manual de funciones y responsabilidades y un plan de mantenimiento sin actualizar. Este es un componente que no está aplicando la totalidad de la normativa de ley, y la cual refleja un impacto de riesgo de 84,38% para el departamento.	Se aplica parcialmente la Norma de Control Interno de Tecnologías de Información 410-09 que refiere al Control y mantenimiento de la infraestructura tecnológica
1	El componente de Inventario de Activos de acuerdo a su nivel de confianza 21,43% se encuentra en el estado de madurez Inicial, debido a que se lleva parcialmente el Control de Inventario de activos tecnológicos en Redes y Telecomunicaciones y el proceso de devolución de activos no se lo realiza formalmente, El riesgo es alto y corresponde a un 78,57% para el departamento tecnológico.	Se está cumpliendo parcialmente con la Norma ISO 27000 referente a Gestión de Activos.

1	<p>El componente de Control de Acceso de acuerdo a su nivel de confianza 29,17% se encuentra en el estado de madurez Inicial, debida a que se tiene parcialmente documentada la identificación de los equipos permitidos en la red. El riesgo corresponde a un 70,83% para el departamento tecnológico.</p>	<p>Se está cumpliendo parcialmente con la Norma ISO 27000 referente a Control de Acceso.</p>
2	<p>El componente de Hardware de acuerdo a su nivel de confianza 41,91% se encuentra en estado de madurez Gestionado, ya que sus actividades dentro de este componente como mantenimientos preventivos, correctivos, implementaciones de redes se realizan de manera total, con un patron regular aunque estas no se documentan de manera adecuada, lo que implica que sus procesos sean desorganizados. El impacto de riesgo por no cumplir totalmente la normativa es de 58,09% en el departamento tecnológico.</p>	<p>Se aplica la Norma de Control Interno de Tecnologías de Información 410-09, teniendo un patrón regular.</p>
2	<p>El componente de Seguridad Física del Entorno de acuerdo a su nivel de confianza 42,08% tienen un estado de madurez Gestionado, sus actividades dentro de estos componentes como el formateo seguro de la información, la custodia de los equipos tecnológicos fuera de la institución, la protección del cableado de red, identificación y rotulación del cableado de red se hacen de manera regular sin una documentación adecuada, llevando al departamento a obtener un riesgo de 57,92% .</p>	<p>Se cumple con un patrón regular la Norma ISO 27000 referente a Seguridad Física del Entorno.</p>
2	<p>El componente de Software de acuerdo a su nivel de confianza 43,18% se encuentra en estado de madurez Gestionado, ya que sus actividades como actualizaciones de software base, actualizaciones de licenciaturas de software e instalación de programas en los equipos tecnológicos se realizan de manera total aunque estas no se documentan de manera adecuada, y al igual que Hardware, implica que sus procesos son desorganizados. El impacto de riesgo por no cumplir totalmente la normativa es de 56,82% (Software) en el departamento tecnológico.</p>	<p>Se aplica un patrón regular a la Norma de Control Interno de Tecnologías de Información 410-09.</p>

2	El componente de Seguridad de los Recursos Humanos de acuerdo a su nivel de confianza 48,61% tienen un estado de madurez Gestionado, sus actividades dentro de estos componentes se hacen de manera parcial sin una documentación adecuada, como por ejemplo no tener una planificación y procedimientos para la distribución de tareas, llevando al departamento a resultados pobres en el control y mantenimiento de la infraestructura tecnológica, causando a la vez un riesgo de 51,39%.	Se cumple un patrón regular a la Norma ISO 27000 referente a la Seguridad de los Recursos Humanos
2	El componente de Comunicación y Operación de acuerdo a su nivel de confianza 53,68% tiene un estado de madurez Inicial, sus actividades dentro de este componente se hacen de manera parcial como el proceso de respaldo y restauración de la información, las instrucciones para el manejo de los errores en la ejecución de tareas, todo esto sin una documentación adecuada, causando un riesgo de 46,32% en el departamento tecnológico.	Se sigue un patrón regular a la Norma ISO 27000 referente a Comunicación y Operación.

CONCLUSIONES Y RECOMENDACIONES

COMO CONCLUSIONES LAS AUDITORAS EXPRESAN:

- ✚ El departamento tecnológico no cuenta con documentación de los procesos que se realizan dentro de éste.
- ✚ Cuentan con un manual de funciones y organizaciones, un Plan de Mantenimiento y un organigrama funcional desactualizado.
- ✚ No tiene un plan de Contingencias.
- ✚ No se evidenció que llevan el Control de inventarios de los activos tecnológicos.
- ✚ Se evidenció que el departamento tecnológico no está cumpliendo con la debida normativa de Control Interno en lo referente al control y mantenimiento de la infraestructura tecnológica.

- ✚ El número de personal que labora no es el adecuado para brindar un buen servicio a la institución.
- ✚ El departamento no cuenta con registros de ningún tipo de inventario.
- ✚ El personal que labora no tiene conocimiento sobre el marco legal que afecta al departamento tecnológico.
- ✚ El inventario solicitado a Almacén esta desactualizado por lo que hay custodios que ya no tienen equipos tecnológicos a su cargo.
- ✚ Mediante la Norma de Control Interno y Norma ISO 27000 se evaluó el proceso de control y el proceso de mantenimiento, determinando que tienen un alto riesgo que afecta el desempeño del departamento.
- ✚ En algunas áreas de la institución al momento de implementar las redes, el cableado no se lo ha realizado con estética y no se han tenido en cuenta los estándares que exige la Norma ISO 27000.
- ✚ En algunas áreas de la institución no existen extintores q permitan proteger los equipos ante cualquier fenómeno.
- ✚ El departamento no le realiza ningún tipo de mantenimiento a las redes y telecomunicaciones de la institución.
- ✚ La carrera de administración no tiene puntos de red.
- ✚ Mediante los cuestionarios realizados al departamento tecnológico se pudo evaluar y constatar que el mismo no cuenta con información suficiente (Planes, políticas, procedimientos, bitácoras, entre otros) de cómo se debe manejar internamente el departamento tecnológico.

COMO RECOMENDACIÓN A LA MÁXIMA AUTORIDAD:

- ✚ Que la Carrera Informática se desvincule totalmente del Departamento Tecnológico, ya que esto ocasiona una mala organización en los procesos del departamento y además se asignan responsabilidades que no le corresponden a la carrera por ser esta académica y no administrativa.
- ✚ Que el Departamento ponga en práctica el Manual de Funciones y el Plan de mantenimiento.
- ✚ Que realicen un plan de Contingencia.
- ✚ Que el Data Center pertenezca al departamento Tecnológico, desvinculándose así de la carrera de Informática.
- ✚ Que se cumplan con obligatoriedad las recomendaciones de la auditoría interna a la ESPAM MFL DR5-0020-2010 realizada por la Contraloría General, donde se manifiesta que se conforme un Comité Técnico, donde existe ausencia de actas de entrega-recepción de documentos, bienes e información electrónica.
- ✚ Que el Departamento Tecnológico lleve un control de inventarios de todos los equipos tecnológicos con sus respectivos custodios.
- ✚ Que el Departamento Tecnológico lleve un control de inventarios de toda la normativa que afectan directamente al departamento.
- ✚ Que el jefe del departamento capacite a su personal de cómo se trabaja internamente en el departamento.
- ✚ Que se realicen bitácoras para el registro del mantenimiento correctivo y predictivo de los equipos tecnológicos

- ✚ Que elaboren un cronograma de mantenimiento de los equipos tecnológicos.
 - ✚ Que se reestructure el organigrama funcional aplicando buenas prácticas.
 - ✚ Que reeduzcan los cableados que no están protegido ante daños.
 - ✚ Que se tengan extintores en todas las áreas de la institución.
 - ✚ Que se realice mantenimientos planificados, programados y periódicamente a las redes y telecomunicaciones de la institución.
- Que la carrera de administración se le implemente puntos de red.
 - Que se tomen en cuenta el informe final de esta tesis donde encontrarán los riesgos en que se encuentra el departamento de manera general y por componente y se reúnan para corregir y que sus funciones estén como lo exige la contraloría y la norma iso 27000.

ANEXO 21
OFICIO DE ENTREGA DE RESULTADOS AL JEFE DEL DEPARTAMENTO
TECNOLÓGICO

ACTA DE ENTREGA-RECEPCION POR AVANCES DE TESIS

ACTA DE ENTREGA-RECEPCION DE LOS AVANCES DE LA TESIS TITULADA AUDITORÍA AL CONTROL Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL DEPARTAMENTO TECNOLÓGICO DE LA ESPAM MFL, AL ING. GEOVANNY GARCÍA MONTES JEFE DEL DEPARTAMENTO TECNOLÓGICO.

En la ciudad de Calceta, a los quince días del mes de enero del dos mil quince, las suscritas: señorita María Victoria Rivera Chávez y la señora María Fernanda Zambrano Bravo, quienes entregan los avances al: señor Ing. Geovanny García Montes quien recibe los avances, en la ESPAM MFL, ubicada en el sitio El Limón, con el objeto de realizar la diligencia de entrega – recepción correspondiente.

Al efecto con la presencia de las personas mencionadas anteriormente se procede con la constatación física y entrega-recepción de los avances de la tesis sujetos de control administrativo.


Se deja constancia que el señor Ing. Geovanny García, se encargará de velar por el buen uso, conservación, administración, utilización, así como que las condiciones sean adecuadas y no se encuentren en riesgo de deterioro de los avances antes mencionados y confiados a su guarda.

En consecuencia, por la demostración que antecede y de conformidad la señorita María Victoria Rivera Chávez y la señora María Fernanda Zambrano Bravo, entregan a satisfacción al señor Ing. Geovanny García Montes, quien recibe a satisfacción los avances de la tesis sujetos de control administrativo.

Para Constancia de lo actuado y en fe de conformidad y aceptación, suscriben la presente acta entrega-recepción en tres ejemplares de igual tenor y efecto las personas que intervienen en esta diligencia.


SRTA. M. VICTORIA RIVERA CH.
C.C.
ENTREGUÉ CONFORME


SRA. M. FERNANDA ZAMBRANO B.
C.C. 1310050115
ENTREGUE CONFORME


SR. ING. GEOVANNY GARCÍA MONTES
RECIBÍ CONFORME
JEFE DEL DEPARTAMENTO
TECNOLÓGICO

