UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ESCUELA DE SISTEMAS

TESIS DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

Tema:

Plan de Auditoría Informática para el Departamento de Sistemas Informáticos en el Municipio del Cantón Ventanas

Autor:

Reinaldo Simón Ramírez Contreras

Director:

Ing. Raúl Ramos

Lector:

Lcdo. Holger Neira

Los Ríos – Babahoyo 2015

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ESCUELA DE SISTEMAS

TESIS DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

Tema:

Plan de Auditoría Informática para el Departamento de Sistemas Informáticos en el Municipio del Cantón Ventanas

Autor:

Reinaldo Simón Ramírez Contreras

Los Ríos - Babahoyo - 2015

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ESCUELA DE SISTEMAS

DECLARACIÓN DE AUDITORÍA

Ante las Autoridades de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo declaro que el contenido de la investigación cuyo título es **"**Plan de Auditoría Informática para el Departamento de Sistemas Informáticos en el Municipio del Cantón Ventanas", presentado como requisito para la obtención del título de Ingeniero en Sistemas es original, de mi autoría y total responsabilidad.

Atentamente,

Reinaldo Simón Ramírez Contreras

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ESCUELA DE SISTEMAS

DEDICATORIA

Esta tesis se lo dedico a mis padres quienes con mucho esfuerzo y sacrificio me han apoyado incondicional en mi preparación profesional, me han guiado y motivado para no darme por vencido y alcanzar mis metas, que con sacrificio, esfuerzo, y trabajo, he luchado día tras día para alcanzar esta meta propuesta.

También agradeciendo a mis estimados profesores: el Ingeniero Raúl Ramos y al Ingeniero Miguel Zúñiga por su dedicación y apoyo en el aprendizaje para de esta manera lograr desarrollar mis conocimientos, como ser un profesional útil para la sociedad, de esta manera cumplir mis logros de poder ingresar al mundo profesional de tecnologías de Informáticas.

UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ESCUELA DE SISTEMAS

AGRADECIMIENTO

Agradezco a Dios por darme la sabiduría y el conocimiento necesario para la realización de este proyecto de Tesis, por ser mi base de inspiración y apoyo espiritual, para superar cualquier problema, ante la adversidad y obstáculos durante el transcurso de mi carrera de sistemas.

A pesar de los grandes obstáculos para la realización de este proyecto el amor y el poder de mi corazón con la fe de Dios han hecho posible mantenerme firme para luchar contra la adversidad el egoísmo y la duda que se han presentado en el camino con ganas de obtener el conocimiento cada día ante las nuevas competencias y con el objetivo de cumplir cada una de mis metas que me he propuesto.

INDICE DE CONTENIDOS

INTRODUCCIÓN.....1
I. OBJETIVOS.....2
1.1 Objetivo general.....2
1.2 Objetivos Especificos.....2
II MARCO REFERENCIAL.....3
2.1 Antecedentes investigativos.....3
2.1.2 Unidad de Sistemas Informaticos.....4
2.1.3 Misión.....4
2.2. MARCO TEÓRICO.....5
2.2.1. Concepto de Auditoria.....5
2.2.1.2 Tipos de Auditoria.....6
2.2.1.2.1 Auditoría Informática.....6
2.2.1.2.2 Auditoría Seguridad.....6
2.2.1.2.3 Norma ISO 27001.....7
2.2.1.2.4 Función de la Norma ISO 27001.....7
2.2.1.2.5 Confidencialidad de la Información.....7
2.2.1.2.6 Integridad de la Información.....8
2.2.1.2.7 Disponibilidad de la Información.....8
2.2.1.2.8 Beneficios de la Norma ISO 27001.....8
2.2.1.2.9 Certificación en Seguridad Informática.....9
2.2.1.3. Seleccionar la Norma.....9
2.2.1.3.1 Comunicar.....9
2.2.1.3.2 Utilizar La Información.....9
2.2.1.3.3 Sistemas de Gestión de Seguridad de la Información SGSI.....10
2.2.1.3.4 Responsabilidades de la Dirección Informática.....10
2.2.1.3.5 Auditorías Internas a los Sistemas.....10
2.2.1.3.6 Revisiones de seguridad por la dirección informática.....10
2.2.1.3.7 Mejorar la Seguridad.....11
2.2.1.3.8 Planificar.....11
2.2.1.3.9 Que Hacer.....11
2.2.1.4. Chequear.....11

2.2.1.4. 1 Actuar.....11
2.2.1.4.2 Importancia de la Auditoria.....12
2.2.1.4.3 Investigación Preliminar.....12
2.2.1.4.4 Herramientas de auditoria.....12
2.2.1.4.5 Cuestionario.....12
2.2.1.4.6 Entrevistas.....13
2.2.1.4.7 Auditor Externo.....13
2.2.1.4.8 Evidencias.....14
2.2.1.4.9 Resultados de la Auditoria informáticas.....14
2.2.1.5. Informes.....14
2.2.1.5.1 Procedimientos Avanzados de Auditoria.....14
2.2.1.5.2 Sinopsis de la Metodología Magerit.....14
2.2.1.5.3 Consideraciones Importante de la Institución.....15
2.2.1.5.4 Síntomas de seguridad de Tecnologías de Información.....15
2.2.2.5.5 Síntomas de desarrollo de Planes de Contingencia.....16
2.2.2.5.6 Plan de Control en la Unidad de Sistemas.....16
2.2.1.5.7 Fase de Planificación.....16
2.2.1.5.8 Alcance del Plan.....17
2.2.1.5.9 Estructura Tecnológica.....18
2.2.1.6. Area Informática.....18
2.2.1.6.1 Recursos Informáticos.....18
2.2.1.6.2 Hardware.....19
2.2.1.6.3 Software.....19
2.2.1.6.4 Recursos Humanos.....19
2.2.1.6.5 Administración.....19
2.2.1.6.6 Análisis de Normas de Control Interno.....20
2.2.1.6.7 Análisis de Políticas de Seguridad.....20
2.2.1.6.8. Modelo de Trabajo.....21
2.2.1.6.9 Análisis de Metodología.....21
2.2.1.7. Análisis de Riesgos.....22
2.2.1.7.1 Identificar Activos.....24
2.2.1.7.2 Recursos Tecnológicos.....24

2.2.1.7.3 Inventarios de Hardware y Software....24
2.2.1.7.4 Información....25
2.2.1.7.5 Tipos de Información....25
2.2.1.7.6 Información Manual....25
2.2.1.7.7 Información Electrónica....25
2.2.1.8.8 Identificar Riesgos....25
2.2.1.7.9 Análisis de Amenazas....26
2.2.1.8. Identificar Amenazas....28
2.2.1.8.1 Amenazas Lógicas....28
2.2.1.8.2 Virus....28
2.2.1.8.3 Amenazas Ambientales....29
2.2.1.8.4 Incendios....29
2.2.1.8.5 Inundaciones....29
2.2.1.8.6 Terremotos....29
2.2.1.8.7 Amenazas Físicas....29
2.2.1.8.8 Agentes Internos....29
2.2.1.8.9 Agentes Externos....30
2.2.1.9. Hacker....30
2.2.1.9.1 Cracker....30
2.2.1.9.2 Lamer....30
2.2.1.9.3 Análisis de Vulnerabilidades....30
2.2.1.9.4 Identificar Vulnerabilidades....32
2.2.1.9.5 Vulnerabilidades de Acesos....32
2.2.1.9.6 Vulnerabilidades por Fallas....33
2.2.1.9.7 Vulnerabilidades por falta de Capacitaciones....33
2.2.1.9.8. Análisis de Impactos....33
2.2.1.9.9 Análisis del Tratamiento con el Riesgo....34
2.2.2. Fase de Ejecución....34
2.2.2.1 Lista de Chequeo....36
2.2.2.2 Personal Participante....36
2.2.2.3 Recursos Materiales....37
2.2.2.4 Evaluación de Riesgos....38

2.2.2.5 Evaluación de Amenazas....40
2.2.2.6 Evaluación de Vulnerabilidades....42
2.2.2.7 Fase de Monitorización....43
2.2.2.8 Pasos para Controlar Riesgos....44
2.2.2.9 Control de Riesgos Administrativos....44
2.2.2.3 Control Operativos de Amenazas....45
2.2.3.1 Controles Técnicos de Vulnerabilidades....46
2.2.3.2 Fase de Mejora....47
2.2.3.3 Gobierno Autónomo Descentralizado del Cantón Ventanas....47
2.2.3.4 Misión Institucional....48
2.2.3.5 Visión Institucional....48
2.2.3.6 Revisión por la Dirección....50
2.2.3.7 Revisión de Normas de Control Interno....50
2.2.3.8 Comités informáticos....50
2.2.3.9 Monitoreo y Evaluación de la Unidad Informática....50
2.2.4. Seguridad de Tecnología de Información:....51
2.2.4.1 Políticas y Procedimientos....51
2.2.4.2 Controles sobre Sistemas de Información....51
2.2.4.3 Adquisiciones de Infraestructura Tecnológica....51
2.2.4.4. Capacitación Informática....52
2.2.4.5 Organización Informática....52
2.2.4.6 Segregación de Funciones....52
2.2.4.7 Planeamiento Informático Estratégico de Tecnología....52
2.2.4.8 Modelo de Información Organizacional....52
2.2.4.9 Administración de Proyectos Tecnológicos....52
2.2.5 Desarrollo y Adquisición de Software Aplicativo....53
2.2.5.1 Mantenimiento y control de la Infraestructura Tecnológica....53
2.2.5.2 Administración de Soporte de Tecnología....53
2.2.5.3 Sitios web y servicios de Internet....53
2.2.5.4 Firmas electrónicas....53
2.2.5.5 Canales de comunicación abierta....53
2.2.5.6 Planes de Contingencias....54

2.2.5.7 Revisión de Políticas de Seguridad 54
2.2.5.8 Reglamentos Generales 55
2.2.5.9 Responsabilidades de la Dirección Informática 56
2.2.6. Análisis de la Unidad de Sistemas Informáticos 56
2.2.6.1 Estructura Organizacional de Trabajo 56
2.2.6.2 Equipo Directivo 57
2.2.6.3 Equipo de Sistemas y Asistencia Técnica 57
2.2.6.4 Tecnologías de la Información y Comunicación 57
2.2.6.5 Información 58
2.2.6.6 Sistemas Informáticos utilizados 58
2.2.6.7 Áreas de trabajo 59
2.2.6.8 Organización Actual de la Unidad de Sistemas 59
2.2.6.9 Plataforma Tecnológica 59
2.2.7. Entornos de Áreas de Trabajo 60
2.2.7.1 Recursos Informáticos 60
2.2.7.2 Personal de Trabajo y Suministro 60
2.2.7.3 Area de Sistemas y Soporte Técnico 60
2.3 Postura Teórica 61
2.4 Hipótesis 62
2.4.1 Hipótesis general de Trabajo 62
2.4.2 Hipótesis general de Nula 62
2.4.3 Hipótesis específicas 62
2.4.4 Variables 62
2.4.5 Variable Independiente 62
2.4.6 Variable Dependiente 62
III. RESULTADOS DE LA INVESTIGACIÓN 63
3.1 Descripción de resultados 63
3.1.2 Metodología de la Investigación 63
3.1.3 Técnicas e Instrumentos 64
3.1.4 Instrumentos 65
3.2. Interpretación y discusión de resultados 65
3.2.1 Población 67

3.2.2 Muestra 68
IV. CONCLUSIONES 79
V. RECOMENDACIONES 80
VI. PROPUESTA DE INTERVENCIÓN.....82
6.1 Titulo de la Propuesta 82
6.1.1 Marco de la Propuesta 82
6.2.1 Metodología de Desarrollo Utilizada 82
6.2 Objetivo de la Propuesta.....83
6.2.1 Objetivo General.....83
6.2.2 Objetivos Específicos 83
6.2.1 Análisis Previo.....83
6.2.1.2 Normas del Auditor 83
6.2.1.3 Normas de Presentación de Informes.....84
6.2.1.4 Plan de control de seguridad en la Unidad de Sistemas 85
6.2.1.5 Controles Generales.....86
6.2.1.6 Controles Específicos 86
6.2.1.7 Descripción de Componentes del Plan.....86
6.2.1.8 Análisis de Foda en la Unidad de Sistemas 86
6.2.1.9 Imagen de Sistema de Información.....88
6.2.2. Servidor Informático.....89
6.2.2.1 Funciones de un Firewall.....89
6.2.2.2 Servidor de Archivo.....90
6.2.2.3 Diagrama de Servidor de Archivos.....90
6.2.2.4 Departamento de sistema en la Institución.....91
6.2.2.5 Unidad de sistemas informáticos.....92
6.3. Justificación.....94
6.3.1 Equipo Directivo de Sistemas 94
6.3.2 Equipo de Sistemas, control y Soporte de Seguridad 95
6.3.3 Identificación de Recursos Humanos.....96
6.3.4 Fase de Planeamiento 98
6.3.5 Fase de revisión.....99
6.3.6. Fase de verificación 101

6.3.7 Factibilidad de la propuesta 103
6.3.8 Factibilidad Administrativa 103
6.3.9 Factibilidad Operativa 103
6.4. Factibilidad Técnica 103
6.4.1 Factibilidad Económica 103
6.3.3 Fase de Ejecución 104
6.4.4 Controles de Riesgos Administrativo 104
6.4.5 Control de Riesgos Operacional de Amenazas 105
6.4.6 Control Técnicos de Vulnerabilidades 105
6.4.7 Fase de Monitoreo 109
6.4.8 Acciones Preventivas 109
6.4.9. Acciones Correctivas del plan 111
6.5 Actividades correctivas del plan 112
6.6. Evaluación de la Propuesta 115
6.6.1 Escenario de Evaluación de Riesgos 115
6.6.2 Indicadores de Riesgos 115
6.6.3 Mejora continua del Plan 124
6.6.4 Tratamiento del Riesgo 124
6.6.4.1 Medidas de prevención del Plan 127
6.6.4.2 Identificaciones de Riesgos fallas Eléctricas 127
6.6.4.3 Identificaciones de Riesgos fallas de Hardware 129
6.6.4.4 Identificaciones de Riesgos fallas de Software 131
6.6.4.5 Identificaciones de Riesgos de Virus 133
6.6.4.6 Identificaciones Riesgos de Accesos de Agentes Cibernéticos 135
6.6.4.7 Identificaciones de Riesgo falta de Integración 137
6.6.4.8 Identificaciones de Riesgo falta de Respaldo 139
6.6.4.9 Identificaciones de riesgos de Catástrofes Naturales 141
6.6.5 Medidas correctivas del Plan 143
6.6.5.1 Utilización del plan de control 149
6.6.5.2 Coordinación de los equipos de control 149
6.6.5.3 Equipos directivos del área de sistemas 149
6.6.5.4 Equipos de Sistemas, Control, Soporte y Seguridad 149

6.6.5.5 Pasos para prevenir Amenazas e incidentes en el Plan 150
VII. BIBLIOGRAFÍA.....152
PAGINAS WEB.....153
VIII. ANEXOS.....156
Anexo Nº.1. Formulario de encuesta a Usuarios 157
Anexo Nº.2. Formulario de Entrevistas a Directivos.....159
Anexo Nº.3 Galería de imágenes.....162

INDICE DE FIGURAS

FIGURA	CONTENIDO	PAGINA
1	Diagrama de Administración	4
2	Estructura Tecnológica	17
3	Plan de Control	22
4	Identificación de Activos	24
5	Identificación de Riesgos	26
6	Identificación de Amenazas	28
7	Identificación de Vulnerabilidades	32
8	Estructura Organizacional del GAD Municipal Ventanas	49
9	Imagen de Sistemas de Información	88
10	Servidor Informático	89
11	Diagrama de Firewall	89
12	Servidor de Archivos	90
13	Unidad de Sistemas	91

INDICE DE TABLAS

TABLA	CONTENIDO	PAGINA
1	Personal Administrativo	21
2	Análisis de Riesgos	23
3	Análisis de Amenazas	27
4	Análisis de Vulnerabilidades	31
5	Análisis de Impacto	34
6	Análisis de tratamiento con el riesgos	34
7	Cronograma de Actividades de Auditoria	35
8	Lista de Chequeo	36
9	Personal Participante	37
10	Recursos Materiales.	37
11	Clasificación del Riesgo	38
12	Evaluación de Riesgo de Activo	39
13	Evaluación de Amenazas	40
14	Evaluación de Vulnerabilidades	42
15	Pasos para controlar Riesgos	44
16	Controlar Riesgo de Activos	44
17	Controles Operativos de Amenazas	45
18	Controles de Vulnerabilidades.	46
19	Pregunta a empleados	65
20	Nombramiento de empleados	67
21	Pregunta 1 aplicada a los Empleados	69
22	Pregunta 2 aplicada a los Empleados	70

23	Pregunta 3 aplicada a los Empleados	71
24	Pregunta 4 aplicada a los Empleados	72
25	Pregunta 5 aplicada a los ciudadanos	73
26	Pregunta 6 aplicada a los Empleados	74
27	Pregunta 7 aplicada a los Empleados	75
28	Pregunta 8 aplicada a los Empleados	76
29	Pregunta 9 aplicada a los Empleados	77
30	Pregunta 10 aplicada a los Empleados	78
31	Atribuciones y Responsabilidades	92
32	Equipo Administrativo	96
33	Interrogación	97
34	Planeamiento	98
35	Acciones de Control	99
36	Verificación	101
37	Validación	102
38	Verificación de Riesgos Administrativos	106
39	Verificación de Riesgos Operativos	107
40	Verificación de Riesgos Técnicos	108
41	Monitoreo de Sistemas de Información	110
42	Control de Riesgos Administrativos	112
43	Control Operacional de Amenazas	113
44	Control Técnicos de Vulnerabilidades	114
45	Indicadores Riesgos de seguridad.	115
46	Indicadores de nivel de Riesgos	115
47	Probabilidades de Riesgos	116
48	Matriz de porcentajes de Riesgos	117

49	Escenario de evaluación de Riesgos de seguridad	119
50	Escenario evaluación de Amenazas	120
51	Escenario de evaluación de vulnerabilidades	121
52	Tratamiento del Riesgo	124
53	Mitigación del Riesgo	125
54	Medidas correctivas del Plan	143

INDICE DE GRAFICO

GRAFICO	CONTENIDO	PAGINA
1	Encuesta 1 aplicada a los Empleados	69
2	Encuesta 2 aplicada a los Empleados	70
3	Encuesta 3 aplicada a los Usuarios	71
4	Encuesta 4 aplicada a los Empleados	72
5	Encuesta 5 aplicada a los Usuarios	73
6	Encuesta 6 aplicada a los Empleados	74
7	Encuesta 7 aplicada a los Usuarios	75
8	Encuesta 8 aplicada a los Empleados	76
9	Encuesta 9 aplicada a los Empleados	77
10	Encuesta 10 aplicada a los Empleados	78
11	Porcentaje de amenazas de acuerdo a los Riesgos	117
12	Porcentaje máximos de Riesgos	122
13	Porcentajes mínimos de Riesgos	123
14	Diagrama de fallas Eléctricas	128
15	Diagrama de fallas de Hardware	130
16	Diagrama de fallas de Software	132

17	Diagrama de prevención de Virus	134
18	Diagrama de prevención de Accesos	136
19	Diagrama de fallas de Integración	138
20	Diagrama de falta de Respaldos	140
21	Diagrama de prevención de Catástrofes	142

RESUMEN EJECUTIVO

El Plan de Auditoria informática determina la gran importancia que tienen las administraciones de Sistemas de Información y equipos de cómputo dentro de las Instituciones Públicas para verificar los riesgos informáticos en los procesos administrativos llevando a cabo procedimientos basados en controles de seguridad de tecnologías de información para salvaguardar los activos y recursos informáticos mediante supervisiones basadas en el cumplimiento de normas, políticas y estándares establecidos de Auditorias informáticas para proteger la integridad, confiabilidad y seguridad las áreas informanticas custodiando la Información institucional ante amenazas, fraudes, sabotajes y accesos no autorizados aplicando mecanismos de prevención de emergencias ante amenazas humanas y desastres naturales.

.

SUMMARIZE EXECUTIVE

The Plan of computer Audit determines the great importance that you/they have the administrations of systems of information and computation teams inside the public institutions to verify the computer risks in the administrative processes carrying out procedures based on controls of security of technologies of information to safeguard the assets and computer resources by means of supervisions based on the execution of norms, political and established entandares of computer Audits to protect the integrity, dependability and security the areas informanticas guarding the institutional Information before threats, frauds, sabotages and not authorized accesses applying mechanisms of prevention of emergencies before human threats and natural disasters.

INTRODUCCIÓN

El Plan de Auditoría informática es una actividad dirigida a analizar, evaluar y mejorar los controles de seguridad de los departamentos informáticos mediante supervisiones de las áreas de procesamiento de datos, la utilización de recursos Tecnológicos que intervienen para establecer la eficiencia y efectividad en relación al costo y al tiempo de los sistemas y equipos de cómputo en una organización.

Las evaluaciones de las estructuras informáticas en las administraciones públicas permiten priorizar los controles de seguridad basados en procedimientos de auditoria aplicados a los recursos informático de hardware y software relacionados con la administración de activos a través de evaluaciones a las administraciones de tecnologías informáticas controlando la seguridad de los recursos informáticos utilizando técnicas e instrumentos de investigación para el alcance de los objetivos coordinando las actividades relacionadas con el personal administrativo, la disposición de materiales informáticos a cargo de autoridades y usuarios de la entidad basados en los cumplimientos normativos de la institución a cargo de las funciones del auditor para analizar la utilización y protección de

recursos asignados por dicha entidad con la finalidad fortalecer la seguridad y corregir debilidades de las áreas informáticas.

I. OBJETIVOS.

1.1. Objetivo General

Desarrollar una Auditoria Informática que permita realizar el análisis y evaluación de la unidad de Sistemas en el Gobierno Autónomo Descentralizado de la Municipalidad del Cantón de Ventanas para llevar un control de seguridad de los activos y recursos informáticos.

1.2. Objetivos Específicos

1. Recoger y evidenciar si la Unidad de Sistemas en el Gobierno Autónomo Descentralizado de la Municipalidad del Cantón Ventanas mantiene los controles de seguridad e integridad de la información conforme a las metas institucionales y si utiliza adecuadamente los bienes y recursos de acuerdo a las normativas establecidas de auditoría informática.

2. Diagnosticar los problemas administrativos informáticos de la Unidad de Sistemas en el Gobierno Autónomo Descentralizado Municipal del Cantón de Ventanas.

3. Aplicar Normativas de auditoría a los procesos informáticos en la unidad de

sistemas del Gobierno Autónomo Descentralizado de la Municipalidad del Cantón de Ventanas.

II MARCO REFERENCIAL

2.1 ANTECEDENTES INVESTIGATIVOS

El Gobierno Autónomo Descentralizado del Cantón Ventanas es una Institución Publica que durante varios años ha venido promoviendo el desarrollo de proyectos que fortalezcan las unidades informáticas para tratar de apoyar los servicios informáticos y soporte de Tecnologías, estos proyectos en la actualidad se encuentran enfase de planificación a cargo de la unidad de Sistemas, el exhaustivo análisis de proyectos de investigación en la institución han permitido tomar en consideración la gran importancia que tienen la administración de las áreas y recursos informáticos para la gestión de actividades relacionadas con el funcionamiento, comunicación y seguridad de los activos.

Las unidades de tecnologías de la información son indispensables para las gestiones informáticas de las instituciones permiten establecer sistemas de información y equipos informáticos para simplificar los procesos manuales e interactuar con los procesos lógicos, almacenar procesar y proveer información.

En la actualidad la información es uno de los activos más importantes para los tramites y transacciones públicas a cargos de usuarios y empleados de las instituciones, la evolución de las tecnologías, en la actualidad, las conductas morales e intereses personales están expuestas a riesgos, amenazas y vulnerabilidades las mismas que deben ser supervisadas para salvaguardar la confidencialidad, integridad y disponibilidad de los datos administrados por sistemas computacionales en áreas informáticas.

Tomando en consideración la base de conocimientos de la entidad e investigaciones de auditorías informáticas se han llevado a cabo los análisis y evaluaciones que tendrá dicha auditoria para garantizar los controles de Auditoria informática en la institución Municipal.

2.1.2 UNIDAD DE SISTEMAS INFORMÁTICOS

La unidad de sistemas informáticos en el Gobierno Autónomo Descentralizado Municipal del Cantón Ventanas está orientada a asegurar el funcionamiento óptimo de la infraestructura tecnológica institucional con eficiencia de las tareas de procesamiento de datos e información de usuarios y ciudadanos.

La organización actual del área de sistemas se encuentra conformada por los recursos de hardware (componentes y dispositivos de comunicación de las áreas de trabajo) y software (sistemas de información e integración, programas de Windows, base de datos) servicios asistencia técnica de mantenimiento preventivo y correctivo de los recursos informáticos, proporcionando apoyo a los departamentos administrativos de la institución Municipal.

Figura 1. Diagrama de Administración[1]

2.1.3 MISIÓN

Contar con áreas de planificación y seguridad informática, base de datos, soporte técnico, mantenimiento e implementación de redes de comunicación[2].

2.2. MARCO TEÓRICO

2.2.1. CONCEPTO DE AUDITORÍA

La palabra Auditoria se deriva del latín Auditórius que proveniente del Auditor quien tiene la virtud de oír es un proceso por el cual se emplean normas de auditoria con procedimientos de carácter razonables en ámbitos profesionales para realizar supervisiones mediante exámenes aplicados a las organizaciones con la finalidad detectar y corregir errores en las actividades administrativas, técnicas e industriales(Hernández E. , 1997).

Las actividades de supervisión son solicitadas por las máximas Autoridades como necesidades para controlar las operaciones de los negocios asignadas a equipos de Auditores con tareas organizadas para realizar investigaciones en ambientes técnicos y administrativos de las empresas con el fin de examinar las administraciones de activos y recursos que poseen las áreas de negocios basados en el cumplimiento de códigos normativos para su ejecución, las evaluaciones se dan con la finalidad de obtener evidencias informadas basadas en cumplimiento de normas institucionales aplicadas a ambientes críticos de la administración de bienes, con la finalidad de verificar los riesgos que presentan las organizaciones dictaminando los hechos, observados a fin de emitir informes presentados a las gerencias para corregir errores mediante opiniones de los auditores que permitan dar soluciones a las organizaciones.

Los procedimiento de auditoria están basadas en los ámbitos de profesionales asignados a las instituciones las mismas que son supervisadas de acuerdo al tamaño la organización a auditar con características específicas, es decir el tipo de auditoria aplicada a cada modelo de negocio empresas e instituciones asignados a supervisores con niveles de dependencia para proteger los activos mejorar las gestiones de las entidades evaluadas por especialistas encargados de ejecutar tareas y actividades internas analizadas y dictaminadas por auditores de las organizaciones a través de informes finales que establezcan conclusiones y recomendaciones a las organizaciones(Foddy, 1994).

2.2.1.2 TIPOS DE AUDITORÍA

2.2.1.2.1 AUDITORÍA INFORMÁTICA

Las auditorías informáticas se basan en exámenes aplicados a recursos y herramientas del computador, supervisados por grupos de trabajos de profesionales con conocimientos informáticos asignados por las instituciones, encargados de evaluar y evidenciar los procesos técnicos relacionados con los equipos informáticos en ámbitos de administración de componentes de hardware y software basados en controles de eficiencia y seguridad de los recursos informáticos en las áreas de trabajo mediante planificaciones y procedimientos para supervisar los recursos tecnológicos desde su función hasta la administración de soportes técnicos(Echenique, Auditoria en Informática, 2013).

2.2.1.2.2 AUDITORÍA DE SEGURIDAD INFORMÁTICA

Las auditorías de seguridad son las más utilizada en actualidad por las empresas en entornos administrativos y organizacionales mediante contratos servicios de supervisiones, realizadas por auditores con conocimientos de seguridad de recursos humanos, materiales, financieros e informáticos utilizados en las áreas internas con las finalidades de tomar medidas correctivas de los riesgos de pérdidas y fraudes en las instituciones.

La seguridad física: Se encargada de examinar las presencia de amenazas de agentes no autorizados así como las posibilidades de desastres que puedan ocurrir empleando medidas de prevención y utilización de dispositivos físicos y recursos humanos bajo custodia de vigilancia.

La seguridad lógica: Se encarga de examinar las amenazas potenciales de acceso vulnerables de los equipos informáticos a través de claves y herramientas de seguridad asignadas a los programas y sistemas del computador(Gómez Vieites, 2012).

2.2.1.2.3 NORMA ISO 27001

La ISO/IEC 27001 son normas desarrolladas por las Organizaciones internacionales de estandarización (ISO) con cede en Ginebra Suiza a través de Comisiones Internacionales de Electrotécnicas (IEC)[3]establecen comité técnicos de desarrollo de estándares de seguridad en países Europeos y Americanos, certificando a las organizaciones Gubernamentales o no Gubernamentales que administren Sistemas de gestión de información e innovación de tecnologías en los ámbitos administrativos técnicos e industriales[4].

La ISO/IEC 27001 son normas de aplicaciones de buenas particas de administración de la seguridad de la información publicadas como estándar[5] en Octubre del 2005 la cual permite la gestión de seguridad de la informaciones mediante certificaciones a las empresas que implementan sistemas de gestión de seguridad, controles de integridad, confiabilidad y disponibilidad de la información durante las fases de evaluaciones y supervisiones de auditoria para mejorar los sistemas de gestión de seguridad (Ruiz, 2013).

2.2.1.2.4 FUNCIÓN DE LA NORMA ISO 27001

Las norma ISO 27001 especifica los requerimientos necesarios para establecer, implantar y mejora la seguridad de los Sistemas de Información administrados por las instituciones, con medidas de confidencialidad, integridad y disponibilidad para el uso protegido de la información libre de divulgaciones de manera secreta, protegida y disponibles para organizaciones que cumplan con los estándares internacionales ISO 27001 de seguridad informática (Ruiz, 2013).

2.2.1.2.5 CONFIDENCIALIDAD DE LA INFORMACIÓN

Comprenderán el cumplimiento de responsabilidad de los usuarios encargado de administrar la información mediante controles acceso a la información y compromiso con la institución de no realizar actividades que puedan generar acciones ilícitas, divulgaciones y accesos a personas ajenas a la institución (Ruiz, 2013).

2.2.1.2.6 INTEGRIDAD DE LA INFORMACIÓN

Comprenden las medidas de responsabilidad de los usuarios de los sistemas sujetos a conductas de honestidad sobre el manejo, uso y protección de la información de manera intangible (Ruiz, 2013).

2.2.1.2.7 DISPONIBILIDAD DE LA INFORMACIÓN

Comprenderá las medidas para proporcionar información durante el tiempo que duran las tareas y actividades del personal informático con el propósito de que el usuario no altere, utilice y comunique información confidencial de la institución (Ruiz, 2013).

2.2.1.2.8 BENEFICIOS DE LA NORMA ISO 27001

Las normas ISO/IEC 27001 permiten garantizar los controles internos para mantener la confiabilidad, integridad y disponibilidad de la información con la aplicación de sistemas de administración de seguridad de las informaciones de las organizaciones proporcionando los siguientes beneficios.

- Verifica que se cumplan y respeten las normas de control interno
- Proporciona niveles de seguridad en las gestiones administrativas
- Verifica los riesgos y vulnerabilidades de la información contenidas en los sistemas informáticos de las organizaciones que estén identificados y evaluados durante las gestiones administrativas de almacenamiento y procesamiento de datos de manera segura.
- Exige el compromiso de los Directivos y Autoridades en gestionar la seguridad de la información.
- Ayudan al proceso de supervisiones internas de acuerdo al rendimiento y mejora de actividades administrativas (Ruiz, 2013).

2.2.1.2.9 CERTIFICACIÓNES EN SEGURIDAD INFORMÁTICA

Las certificaciones ISO/IEC 27001 son acreditaciones a las organizaciones que cumplan con los controles efectivos de seguridad en base al cumplimiento de normas de gestión de seguridad de la información certificadas por la Organización de estandarización de las asociaciones de normalización AENOR creadas para el cumplimiento de estándares coordinadas con las normas y políticas internas de las organizaciones relacionados con los estándares internacionales de gestión de la seguridad de la información ISO/IEC 27001 de aplicación de buenas prácticas institucionales[6].

2.2.1.3 SELECCIONAR LA NORMA

Las obtenciones de las normas están disponibles en los portales web de la ISO 27001 contenidas en documento donde se explican los pasos para utilizar los mecanismos de aplicación de la norma de gestión de seguridad de la información[7].

2.2.1.3.1 COMUNICAR LA APLICACÍON DE EVALUACIONES

Notificar a los empleados de la entidades de las evaluaciones que se realizaran de acuerdo a los resultados obtenidos que implican las certificaciones de buenas prácticas de gestión de seguridad de la información como bases de profesionalismo de actividades y tareas realizadas durante el tiempo de trabajos, conocimientos sobre controles de seguridad para las certificaciones de acuerdo al cumplimiento de las normas ISO 27001 (Ruiz, 2013).

2.2.1.3.2 UTILIZAR LA INFORMACIÓN

Aplicar los conocimientos de estándares de seguridad disponiendo de capacitaciones, talleres y seminarios para adoptar mecanismos de uso y protección de la información que sean certificables de acuerdo a los sistemas de gestión de seguridad de la información dentro de cualquier institución (Ruiz, 2013).

2.2.1.3.3 SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI

Los sistemas de Administración de seguridad de la información abarcan todas las herramientas y mecanismos referentes a seguridad informática relacionada con la aplicación de normas y políticas de seguridad (Ruiz, 2013).

2.2.1.3.4 RESPONSABILIDADES DE LA DIRECCIÓN INFORMÁTICA

Las direcciones informáticas son capacitadas, preparadas e informadas para las evaluaciones de acuerdo al cumplimiento de las normas de control interno que sirven de base para gestionar el manejo de la información de manera segura, el uso y cuidado de los activos informáticos que sirvan de ayuda para la toma de decisiones de las Autoridades (Ruiz, 2013).

2.2.1.3.5 AUDITORÍAS INTERNAS A LOS SISTEMAS

Las supervisiones internas comprenden los análisis de riesgos amenazas y vulnerabilidades que representan los recursos informáticos ante acciones fraudulentas y potenciales basados en el cumplimientos de la normas institucionales aplicadas por el auditor externo, enfocadas al cumplimiento de actividades y obligaciones de acuerdo a las normas internas tomando acciones preventivas y correctivas (Ruiz, 2013).

2.2.1.3.6 REVISIONES DE GESTIÓN DE SEGURIDAD POR LA DIRECION INFORMÁTICA

Las revisiones se dan por parte de las direcciones enfocadas al cumplimiento de las normas y políticas aplicados a personales administrativos verificando los hechos y sucesos encontrados que sean mejorados e implementados. Los comités directivos forman parte importante de los cumplimientos de mecanismos de administración de seguridad de las informaciones mediante reuniones planificadas con el personal de trabajo verificando las medidas correctivas de amenazas y debilidades detectadas durante la fase de evaluación (Ruiz, 2013).

2.2.1.3.7 MEJORAR LA SEGURIDAD

Los análisis continuos de los Sistemas de información permiten controlar que no se produzcan riesgos y errores de seguridad aplicando medidas preventivas basadas en mecanismos de fortalecimiento de seguridad tomando medidas correctivas.

2.2.1.3.8 PLANIFICAR

Las fases de planificación comprenden las metas y objetivos de seguridad

- Establecer políticas de seguridad
- Determinar el alcance de los objetivos
- Valoración de activos
- Análisis de los riesgos
- Seleccionar los controles de seguridad ISO 27001

2.2.1.3.9 QUE HACER

- Definir e implementar el plan de administración de riesgos
- Establecer indicadores de seguridad
- Implementar el plan de gestión de seguridad

2.2.1.4. CHEQUEAR

- Supervisiones por parte de directivos
- Proceso de monitoreo
- Revisar los niveles de riesgos
- Auditar al SGSI

2.2.1.4.1 ACTUAR

- Implementar mejoras
- utilizar medidas preventivas y correctivas
- Comunicar Acciones y resultados (Ruiz, 2013)

2.2.1.4.2 IMPORTANCIAS DE LAS AUDITORÍAS

El propósito de las Auditorias informática es aplicar evaluaciones a los procesos administrativos e informáticos solicitados por las Autoridades mediante contratos de servicios de Auditoria asignados a grupos de supervisores con funciones para monitorear las actividades administrativas e informáticas basadas en las funcionalidades de las áreas de trabajo, para realizar análisis de la exactitud y veracidad de las evidencias obtenidas proporcionado informes a los directivos y autoridades de las organizaciones en base a criterios personales de responsabilidades de las administraciones, de bienes y recursos con niveles de seguridad e integridad de los procesos administrativos relacionados con la utilización de los recursos informáticos a fin de prevenir riesgos informáticos en las instituciones[8].

2.2.1.4.3 INVESTIGACIÓN PRELIMINAR

La investigación preliminar permiten a los auditores obtener informaciones relevantes de las administraciones asignadas, con visiones generales para la comprensión de los procesos de negocios, gestiones de recursos humanos, materiales y económicos vinculados con las tecnologías informáticas para obtener evidencias recopiladas de documentos, materiales y actividades de trabajos obtenidas a través de encuestas y entrevistas formuladas a los directivos y empleados mediante opiniones razonables redactadas en informes presentados a las autoridades de las organizaciones[9].

.2.2.1.4.4 HERAMIENTAS DE AUDITORÍA

2.2.1.4.5 CUESTIONARIO

Constituye la elaboración de formularios de preguntas dirigidas a los empleados de la organización en base a investigaciones de las áreas administrativas recursos humanos, materiales, sistemas y equipos de cómputo utilizados por las organizaciones con previos análisis cualitativos y cuantitativos para la elaboraciones de preguntas que contengan temas específicos de las actividades

observadas y planificadas previo a la aplicaciones de preguntas dirigidas a los empleados de las organizaciones para recolectar informaciones de hechos y sucesos para las comprobaciones de los resultados:

- ✓ Realizar varias preguntas repetidas de manera manual
- ✓ Las preguntas deben aplicarse por un grupo de personas que van a realizar la auditoria.
- ✓ Las preguntas deben ser aplicadas a varios usuarios para la comprobación de los resultados.

2.2.1.4.6 ENTREVISTAS

Las preguntas verbales aplicadas a los directivos internos de la organizaciones sirven de base para recolectar opiniones sobre las funciones y administraciones de los negocios ejecutadas de manera secuenciales basadas en recursos humanos, materiales, económicos e informáticos que describan las actividades de trabajo así como la administración de bienes y recursos tecnológicos como bases fundamentales de evidencias para el desarrollo de la auditoria.

2.2.1.4.7 AUDITOR EXTERNO

El auditor experto elabora de manera profesional varias veces los cuestionarios previos a la función de análisis de preguntas aplicadas al ente auditado para verificar los resultados basados en síntesis de preguntas que sirvan para evidenciar si dichas preguntas aplicadas presenta riesgos de mostrar resultados verdaderos o falsos revisando la presencia de errores comprobatorios antes y después de la aplicación preguntas emitidas por parte del auditor y del personal auditado utilizando un rango de puntuación de 1 a 5 manera calificativa(Elkin Nacor Muñoz, 2013)[10].

Log: El logo es un historial de cambios y modificaciones en los recursos informáticos es decir los sistemas poseen una serie de cambios para registrar almacenar y procesar la información en el caso que lo amerite el log se encarga de controlar los cambios informáticos que se puedan dar en un determinado periodo establecido por la entidad[11].

2.2.1.4.8 EVIDENCIAS

El análisis de evidencias es una manera de comprobar los resultados de hechos y sucesos observados durante las etapas de desarrollo de investigaciones aplicadas a las organizaciones, enfocadas a la realidad objetiva de los ambientes organizacionales de las empresas (Echenique, Auditoria en Informática, 2013).

2.2.1.4.9 RESULTADOS DE LA AUDITORÍA INFORMÁTICA

2.2.1.5. INFORMES

Son los resultados de los trabajos de las auditorías realizadas, informaciones recolectadas de encuestas y entrevistas donde se muestran las evidencias observadas durante las fases de evaluaciones basadas en fortalezas y debilidades que presentan las instituciones para emitir opiniones y recomendaciones[12].

2.2.1.5.1 PROCEDIMIENTOS AVANZADOS DE AUDITORÍA INFORMÁTICA

Técnicas Informáticas: Se refieren técnicas de Auditoría que conforman herramientas informáticas con el objetivo de realizar eficientemente pruebas de Auditoría. Las técnicas de auditoria permiten tener ideas globales de la entidad y de los procesos técnicos de administración de activos durante las actividades en áreas de trabajo[13].

2.2.1.5.2 SINOPSIS DE LA METODOLOGÍA MAGERIT

Magerit es la Metodología de Análisis y Gestión de Riesgos en los Sistemas de información para las administraciones Públicas (MAP) creadas por el Consejo de Administración Electrónica (CSAE) la utilización de la Metodología pertenece al Ministerio de Administración Publica en España[14].

La metodología se utiliza con la finalidad de controlar los riesgos en los medios electrónicos e informáticos utilizando medidas preventivas para las salvaguardas de Activos (Miguel Angel Amutio Gómez, 2012).

2.2.1.5.3 CONSIDERACIONES IMPORTANTES DE LA INSTITUCIÓN

Para la aplicación del plan de auditoria informática en la unidad de Sistemas de la institución Municipal se tuvo fundamentalmente conocimientos generales de la organización recopilando datos generales sobre la administración de recursos informáticos basada en los siguientes pasos.

- De acuerdo a la propuesta de Auditoria es necesario realizar una solicitud dirigida a los directivos del área informática una vez firmada y aprobada por los directivo se procede al desarrollo de la auditoria.
- Entrevista con el director de la área informática y de sistemas:
  La entrevista se debe realizar de manera organizada con preguntas claras, lógicas y precisas aplicadas personales encargadas de administrar y ejecutar el plan de auditoria.

Una vez aprobada la solicitud de autorización se designara a una persona (auditor) encargada de evaluar y desarrollar el plan de auditoria informática.

Investigar la forma de trabajo del área de informática así como el personal encargado de administrar los sistemas y recursos informáticos.

La recopilación de datos e información obtenidas son fundamentales para conocer la situación actual de los recursos informáticos utilizados en el departamento de informática.

2.2.1.5.4 Síntomas de Seguridad de tecnología de información

La unidad de sistemas presenta deficiencia en cuanto a medidas de seguridad ante los riesgos de amenazas a la integridad de la información en áreas donde se procesa la información.

2.2.1.5.5 Síntomas de desarrollo de Planes de contingencias

La unidad de sistemas presenta vulnerabilidad en cuanto a contingencias de tecnologías de la información incidentes y acciones en caso de emergencia.

2.2.1.5.6 PLAN DE CONTROL EN LA UNIDAD DE SISTEMAS

2.2.1.5.7 FASE DE PLANIFICACIÓN

La planificación se lleva a cabo mediante los análisis de actividades técnicas y administrativas, determinando los procedimientos de supervisiones aplicados a los recursos informáticos en la unidad de Sistemas del Gobierno Autónomo Descentralizado Municipal del Cantón Ventanas estableciendo los análisis continuos basados en normas, políticas y estándares de seguridad que determinan las fases de ejecución de evaluaciones, monitoreo, control y la mejora continua de seguridad basado en los siguientes aspectos[15].

Análisis de la organización: Modelo de trabajo en función de actividades técnicas administrativas, responsabilidades de cumplimiento de normas y políticas internas para administración de bienes y recursos tecnológicos en la institución.

Asignación de funciones: Cumplimiento de responsabilidades de las áreas informáticas, actividades y experiencia para la administración de recursos tecnológicos con reglamentos internos basados en capacidades y rendimientos de los usuarios.

Análisis de políticas de seguridad: Establecimiento de reglamentos para administración y asignación de recursos informáticos, humanos, materiales y económicos de manera organizada sujetos a responsabilidades de la institución.

Análisis de normas internas: describe el cumplimiento de responsabilidades de las áreas directivas supervisadas por los jefes departamentales reportados a las autoridades de la institución.

Monitoreo: Seguimiento de actividades, acciones y operaciones de de las áreas informáticas con responsabilidades de trabajos técnicos y administrativos e implementación de dispositivos de vigilancia.

Controles de seguridad: Comprobación de mecanismos de protección basada en la salvaguarda de activos y recursos en las áreas informáticas con reportes de amenazas, acciones preventivas y correctivas de incidentes.

Soporte de tecnologías: Procedimientos sobre la administración de datos y seguridad en la recepción, procesamiento, almacenamiento y distribución de la información.

Controles de información: Responsabilidades sobre el manejo de la información manual y automatizada en actividades administrativas con niveles de confiabilidad, integridad y disponibilidad de los servicios información.

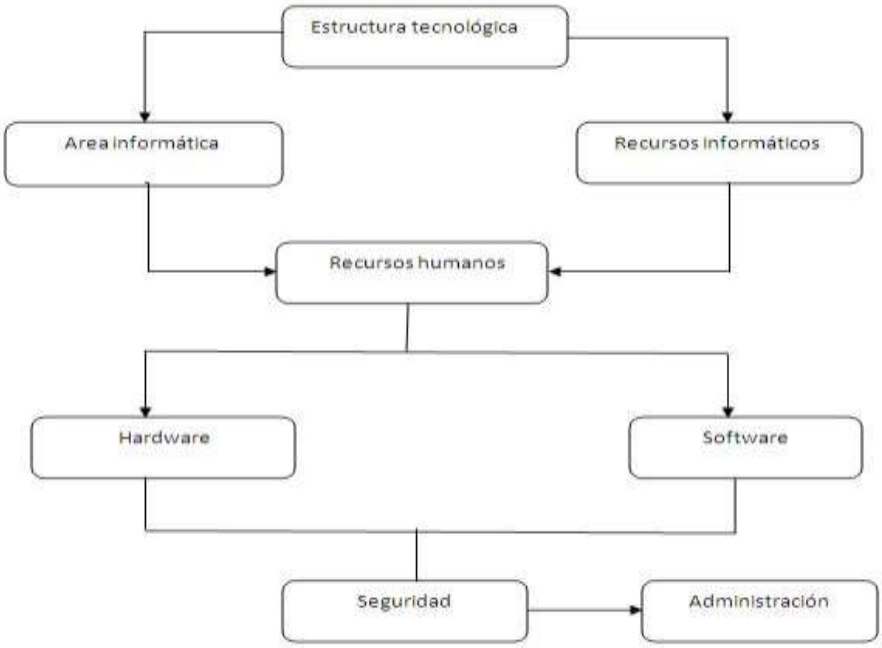
Contingencias: medidas y planes de emergencia ante posibles incidencias de desastres naturales.

Capacitación: Niveles de conocimientos administrativos y técnicos para la atribución de funciones de los usuarios.

2.2.1.5.8 ALCANCE DEL PLAN

El plan de auditoria determina los análisis y evaluaciones mediante controles de salvaguardar de activos y recursos informáticos a cargo de la Unidad de Sistemas en la Municipalidad del Cantón Ventanas.

Figura 2. Estructura Tecnológica



2.2.1.5.9 ESTRUCTURA TECNÓLOGICA

La estructura tecnológica es el conjunto de elementos materiales y equipos tecnológicos necesarios para la construcción y funcionamiento de áreas informática en ámbitos empresariales, sociales e industriales.

Dentro de las organizaciones se evalúan las infraestructuras informáticas como la base de soportes para el funcionamiento de las áreas y departamentos de las instituciones relacionados con los medios físicos y tecnológicos de acuerdo a las condiciones que conforman las áreas es decir paredes, instalaciones, dispositivos eléctricos correspondientes al mejoramiento de materiales tecnológicos que conforman las áreas informáticas.[16].

2.2.1.6. ÁREA INFORMÁTICA

El area informática comprende las condiciones de ambiente de entornos de trabajo para las administraciones de actividades de los usuarios, aunque es imprescindible establecer una perfecta comodidad debido a factores organizacionales y ambientales, se pueden coordinar las necesidades fundamentales (espacio, ventilación, abastecimiento de recursos materiales) de las áreas informáticas.

2.2.1.6.1 RECURSOS INFORMÁTICOS

Los recursos informáticos son un conjunto de bienes materiales designados en las áreas administrativas determinadas para grupos de trabajos, mediante la supervisión de materiales y equipos de cómputo para realizar actividades de trabajo mobiliario, distribución de equipos, adecuación de áreas para los equipo de cómputo, cantidad abastecimiento de equipos de cómputo, componentes y dispositivos adicionales que sean reemplazados al ocurrir un daño, la existencia de lugares específicos para guardar datos, herramientas, mantenimiento y seguridad para proteger los bienes, que hacen relación con el dañado de recursos ,sobre quien recae la responsabilidad de los bienes y equipos, capacidad de recuperación ante desastres[17].

2.2.1.6.2 HARDWARE

Es el conjunto de componentes tangibles que conforman los equipos de cómputo de las áreas de informáticas contienen dispositivos, monitores, escritorios, mouse, teclado, parlantes, reguladores e impresoras necesarias para las actividades de trabajo para ello se evalúan las actividades de accesos físicos, soporte de mantenimiento preventivo y correctivo ante posibles fallas e interferencias[18].

2.2.1.6.3 SOFTWARE

Es la parte intangible del computador conformada por el conjunto de programas (sistemas operativos, aplicaciones) que integran el hardware mediante instrucciones que son ejecutados por los usuarios de manera automática o por instrucciones programadas por el usuario, para ello se evalúan las actividades de soporte de mantenimiento preventivo ante posibles amenazas virtuales por filtraciones de virus, amenazas humanas que puedan causar daños[19].

2.2.1.6.4 RECURSOS HUMANOS

Se considera el conjunto de personas disponibles para realizar tareas y resolver problemas, responsables de las asignaciones y funciones de recursos materiales y sistemas cómputo así como los análisis de actividades administrativas y técnicas dentro de las organizaciones.

Las evaluaciones del talento humano dentro de las instituciones es una parte fundamental para verificar las funciones de desempeño del personal de acuerdo a las capacitaciones en niveles de conocimiento de funciones asignadas para emitir opiniones en aspectos de uso y seguridad de los bienes y recursos otorgados por las instituciones.

2.2.1.6.5 ADMINISTRACIÓN

Las administraciones son atribuciones otorgadas a jefes directivos institucionales con atribuciones de dirigir, organizar y asignar cargos administrativos en las instituciones, generalmente las administraciones están

basadas en las utilizaciones de recursos informáticos, humanos, materiales e información fundamentales para realizar actividades de trabajo, asegurando que las administraciones se den bajo reglamentos institucionales así como la disposición de políticas para la administrar las recursos informáticos a través de mecanismos que permitan proveer informaciones para salvaguardar los activos la seguridad de los equipos de cómputo y responsabilidades del área directiva, para controlar la gestión de actividades administrativas de manera adecuada.

2.2.1.6.6 ANÁLISIS DE NORMAS DE CONTROL INTERNO

Los procesos de ámbitos integrales dirigidos por las máximas Autoridades asignados como reglamentos para realizar supervisiones técnicas y administrativas, dirigidas a funcionarios y empleados de la entidad para la protección de bienes y recursos del sector público son normas establecidas por los comités de auditoría reportadas a autoridades que conforman el control interno mediante evaluaciones por parte de auditores internos para controlar los riesgos que se puedan suscitarse por medio del seguimiento y vigilancia de las gestiones de activos y recursos informáticos dando cumplimiento a los ordenamientos institucionales para garantizar la confiabilidad y seguridad de los recursos administrativos y tecnológicos adoptando medidas correctivas de deficiencias institucionales(039-CG Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Disponga de Recursos Públicos.).

2.2.1.6.7 ANÁLISIS DE POLÍTICAS DE SEGURIDAD

El análisis de políticas de seguridad determina la identificación de reglamentos establecidos por la unidad de Sistemas, dirigidos a los empleados y usuarios en ambientes administrativos y técnicos para la protección de bienes y recursos e informaciones con niveles confiables y seguros de la administración de las áreas informática ante los riesgos de amenazas y vulnerabilidades de los activos informáticos.

2.2.1.6.8 MODELO DE TRABAJO

La administración de la unidad de sistema se basa en la asignación de funciones y responsabilidades del personal técnico y operativo de acuerdo a las necesidades de la institución Municipal ante cualquier evento e incidentes contra la seguridad de las áreas informáticas y reaccionar ante riesgos bajo un modelo de gestión administrativa quienes serán los encargados de especificar la coordinación y aplicación de actividades para controlar la seguridad de la información en la unidad informática como responsables de (sistemas, estructura tecnológica y desarrollo de proyectos) mediante actividades seguridad informática.

Tabla 1. Personal Administrativo

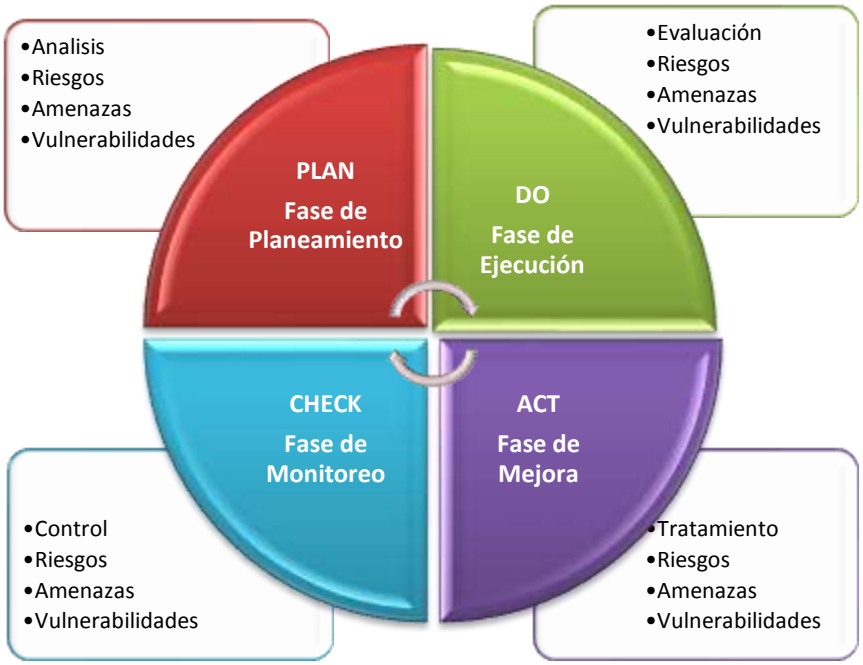
Unidad de Sistemas		
Nombre	**Departamento**	**Cargo**
Ingeniero	Sistemas	Director
Técnico	Mantenimiento	Jefe

Elaborado por: Reinaldo Ramírez

2.2.1.6.9 ANÁLISIS DE METODOLOGÍA

La identificación de metodología para el análisis de los riesgos, amenazas y vulnerabilidades de recursos informáticos en las administraciones de servicios Públicos (MAGERIT)[20] se aplica a la unidad de Sistemas conformada por mecanismos y reglas técnicas para la seguridad informática de forma responsable mediante un modelo de normas políticas y estándares para reducir los riesgos que presentan los recursos informáticos examinando las debilidades estableciendo medidas de prevención ante amenazas y situaciones actuales de la organización para recopilar evidencias que sean redactadas en informes estableciendo conclusiones y recomendaciones para el tratamiento de riesgos de administración y protección de recursos informáticos mediante soluciones que mejoren la administración actual(Miguel Angel Amutio Gómez, 2012).

Figura 3. Plan de Control Do Check At



21

Elaborado por: Reinaldo Ramírez

2.2.1.7. ANÁLISIS DE RIESGOS

El Análisis de Riesgos informáticos en la unidad de Sistemas es la manera de comprobar la identificación de activos informáticos que están expuestos a vulnerabilidades y amenazas así como la posibilidad del impacto de riesgos mediante controles para detectar, prevenir reducir y mitigar los riesgos que puedan causar daños o perdidas en la institución estableciendo controles de confidencialidad, integridad y disponibilidad de activos y recursos como necesidad de salvaguarda[22].

- ¿Qué representa la información para una institución?
- ¿Cómo afectaría la economía por interferencias de los servicios informáticos?

El análisis de riesgos en la Unidad de Sistemas del Gobierno Autónomo Descentralizado permite identificar las principales causas para evidenciar los principales tipos de riesgos observados para el estableciendo sugerencias.

Tabla2. Análisis de Riesgos

ANALISIS DE RIESGOS			
ACTIVIDAD	**DESCRIPCIÓN**	**OBSERVACIONES**	**SUGERENCIAS**
Planeamiento	Comité informático	Normas internas	Director
Funciones	Unidad de sistemas	Políticas de seguridad	Empleados y Usuarios
Procedimientos	Comité de Seguridad Informática	Estándares de Seguridad	Área Informática

Elaborado por: Reinaldo Ramírez

Planeamiento: El análisis del comité informático permite verificar el cumplimiento de normas internas en la etapa de planeamiento en base a supervisiones del Auditor.

Funciones: El Análisis de la unidad de sistemas permite verificar el cumplimiento de políticas de seguridad de acuerdo a las funciones de los usuarios y empleados

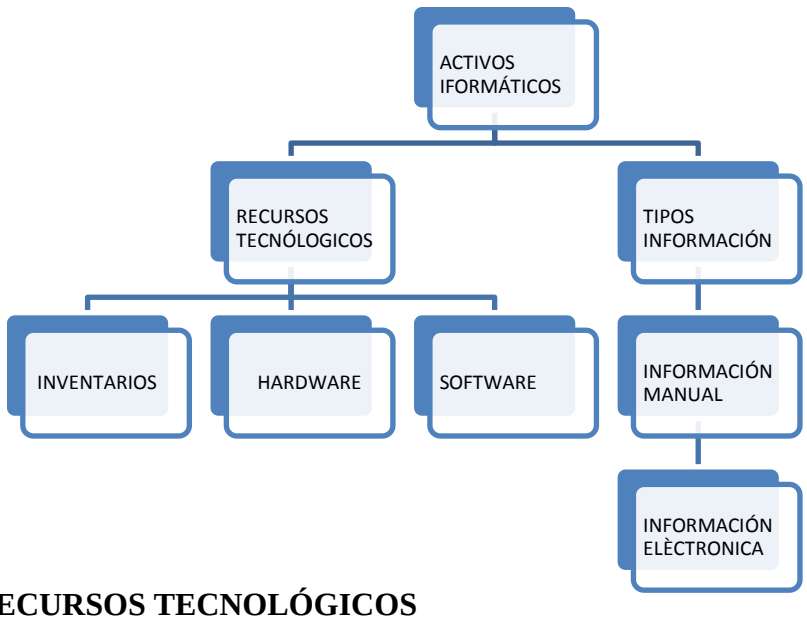
Procedimientos: El análisis del comité de seguridad permite verificar el cumplimiento de estándares en las áreas de Sistemas.

2.2.1.7.1 IDENTIFICAR ACTIVOS

Para las administraciones de recursos de información se determina la identificación de riesgos relacionados con la administración de activos involucrados con los procesos de los usuarios. En la actualidad la información es considerada los activos más importantes para la gestión de actividades de una organización relacionadas con las metas de la institución[23]:

- Inventarios de Hardware
- Inventarios de software
- Información Manual
- Información Electrónica

Figura 4. Identificación Activos



2.2.1.7.2 RECURSOS TECNOLÓGICOS

2.2.1.7.3 INVENTARIOS DE HARDWARE Y SOFTWARE

Inventarios de Hardware: Describen las características de componentes y equipos de cómputo de la unidad de sistemas marca, modelo, serie sistemas, operativos, instalaciones, uso y ubicación de dispositivos, monitores, mouse teclado, parlantes reguladores e impresoras necesarias para las actividades de trabajo[24].

Inventarios de Software: Describe las características de programas (sistemas operativos, aplicaciones) módulos, funciones, lenguajes de programación, fechas de creación y modificación software[25].

2.2.1.7.4 INFORMACIÓN

La información es un conjunto de datos recopilados, redactados en documentos que pueden ser digitalizados almacenados y procesados con el propósito de servir de base para realizar actividades y transacciones administrativas operacionales, económicas y financieras sirven de base para prestar servicios de gestión recepción, distribución de bienes y recursos en una organización.

2.2.1.7.5 TIPOS DE INFORMACIÓN

2.2.1.7.6 INFORMACIÓN MANUAL

Es la información que se utiliza para realizar trámites técnicos y administrativos en las instituciones como actas solicitudes y manuales técnicos que contienen informaciones públicas y privadas.

Informaciones públicas: es la información disponible y accesible para usuarios y empleados de las entidades.

Informaciones privadas: es la información secreta protegida de manera confidencial para las funciones administrativas técnicas y operativas.

2.2.1.7.7 INFORMACIÓN ELECTRÓNICA

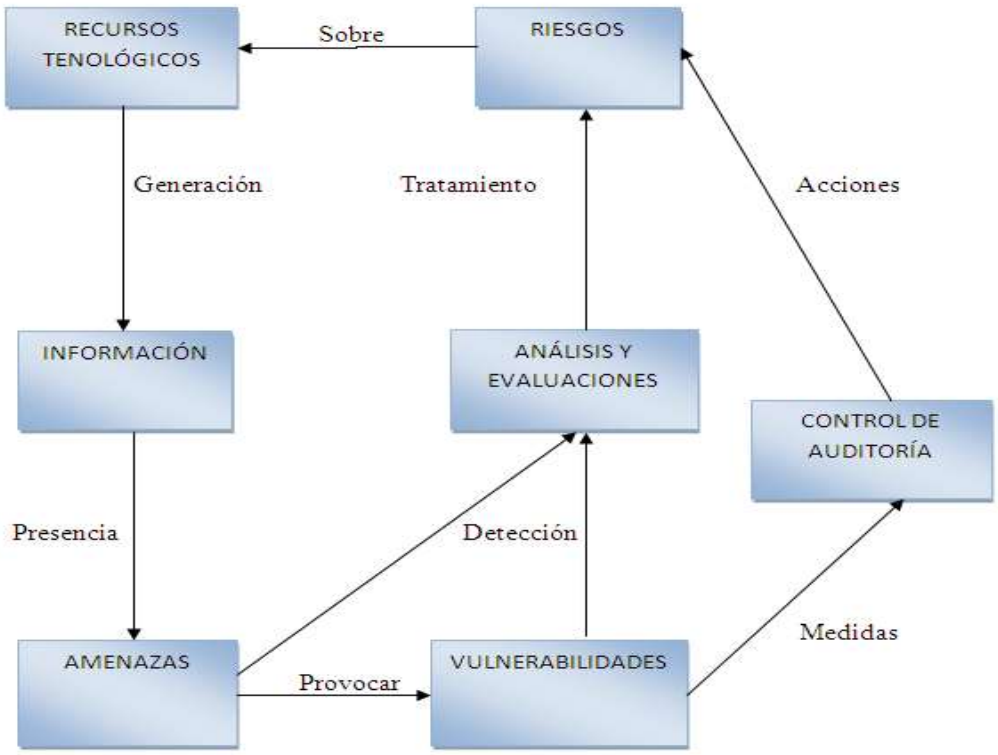
Es la Información que es compartida por medios electrónicos la mayor parte de los trámites en la actualidad se los realiza por medio de correos electrónicos para facilitar la comunicación y traslados de información entre organizaciones.[26]

2.2.1.7.8 IDENTIFICAR RIESGOS

Los riesgos de los sistemas de información se basan en los mecanismos de seguridad, mediante indicadores de gestión de seguridad en las áreas informáticas con la administración de herramientas de seguridad relacionados a

los recursos informáticos a través de controles de vulnerabilidades y probabilidades de amenazas relacionados con la información(SENA, 2013).

Figura 5. Identificación de Riesgos



Elaborado por: Reinaldo Ramírez

2.2.1.7.9 ANÁLISIS DE AMENAZAS

Las consecuencias negativas sobre los recursos informáticos por los avances tecnológicos se tornan vulnerables ante acciones de agentes maliciosos en el ámbito informático, presencia de incidentes por errores técnicos de los usuarios, pérdidas económicas, cabe aclarar que los riesgos informáticos dependen de las actividades propias e impropias de las organizaciones así como las medidas preventivas de accesos a la información vinculados con los empleados y los recursos utilizados, mediante instrucciones y capacitaciones para identificar intrusos relacionados con los controles internos de la organización(SENA, 2013).

El análisis de Amenazas en la unidad de sistemas permite identificar las principales causas para evidenciar los diferentes tipos de amenazas observadas para el estableciendo sugerencias(SENA, 2013).

Tabla 3. Análisis de Amenazas

ANALISIS DE AMENAZAS			
ANALISIS	**DESCRIPCIONES**	**OBSERVACIONES**	**SUGERENCIAS**
Estructura Tecnológica	Normas internas	cumplimiento de normas	Mantener responsabilidades de la seguridad
Tecnología de la Información	Políticas de seguridad	Administración de Accesos físicos y lógicos	Establecer mecanismos y herramientas para la gestión de seguridad de la información
Contingencias	Estándares de Seguridad	Planes de contingencias	Establecer medidas de Emergencia ante Desastres
Canales de comunicación		Comunicación personal y electrónica	Establecer mecanismos de comunicación y salvaguarda de (Redes Locales)

Cumplimiento de normas: El análisis de la estructura tecnológica permite verificar el cumplimiento de normas internas para controlar la seguridad de las tecnologías de la información y comunicación

Administración de Accesos físicos y lógicos: El análisis de las Tecnologías de la información permite verificar el cumplimiento de políticas de seguridad para establecer mecanismos y herramientas que gestionen la seguridad de la información.

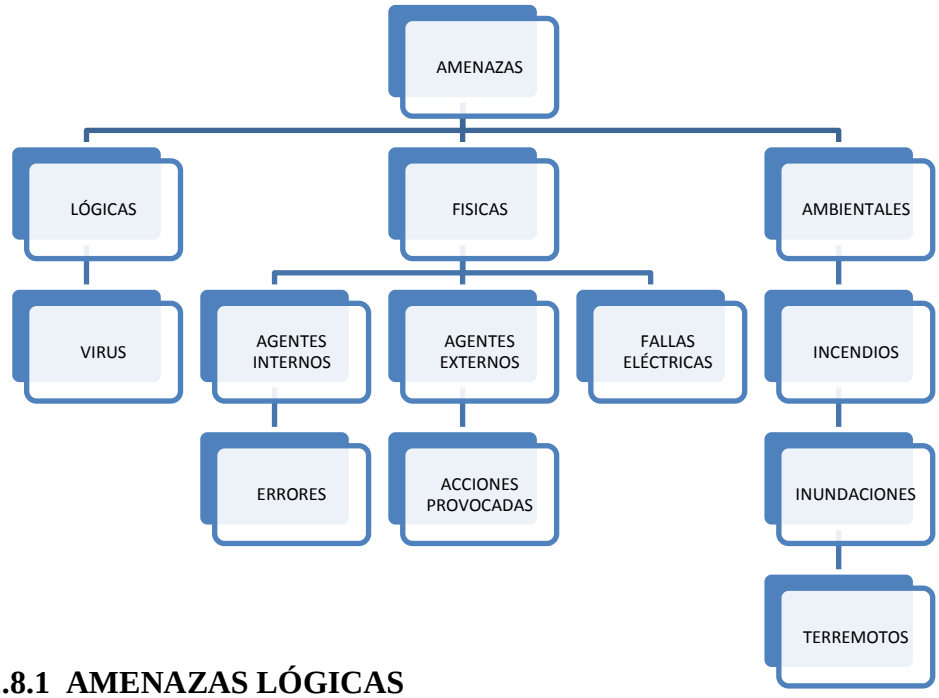
Planes de Contingencias: El Análisis de Contingencias permite verificar el cumplimiento estándares de seguridad para establecer medidas de emergencia ante desastres.

Comunicación personal y electrónica: El análisis de canales de Comunicación abierta permite verificar los mecanismos de comunicación de redes locales en las áreas informáticas.

2.2.1.8 IDENTIFICAR AMENAZAS

Las amenazas pueden surgir de incidentes y acciones provocadas o no provocadas ante posibles fenómenos naturales y amenazas que pueden ser de tipo físico o lógico considerando las acciones que pueden generar efectos negativos en las unidades informáticas expuestas a riesgos de fallas eléctricas, accesos no autorizados a áreas y recursos informáticos filtraciones de virus administraciones inadecuadas de activos y desastres ambientales(terremotos, inundaciones, incendios) las amenazas más comunes se muestran a continuación (SENA, 2013).

Figura.6Identificación de Amenazas



2.2.1.8.1 AMENAZAS LÓGICAS

2.2.1.8.2 Virus: Conocidos en el medio informático como amenazas potenciales de códigos maliciosos que circulan en la Web interrumpen actividades informáticas mediante ejecuciones de códigos secretos que provocan interferencias a equipos de cómputo, simulan la apariencia de sistemas, datos, programas y archivos contaminados impiden las operaciones informáticas[27].

2.2.1.8.3 AMENAZAS AMBIENTALES

Las condiciones ambientales de impactos de la naturaleza sobre el ser humano, causan pérdidas materiales y económicas en ambientes de trabajo. Las consecuencias de desastres en ocasiones se dan muchas veces por negligencias personales en la utilización materiales y productos de fácil combustión en otras ocasiones por falta de análisis ante posibles eventos imprevistos sobre las infraestructuras informáticas basados en medidas de emergencia(Quiroz, 2010).

2.2.1.8.4 Incendios: Los desastres provocados muchas veces por combustión de productos tóxicos e condiciones de altas temperaturas por cortocircuitos que provocan incendios, perdidas de materiales, en otras casaciones se dan por causas imprevista provocas intencionalmente por negligencia de personas en condiciones de trabajo que afectan a las organizaciones causando pérdidas materiales y económicas de recursos humanos(Quiroz, 2010).

2.2.1.8.5 Inundaciones: Fenómenos naturales causados por acumulación de agua en determinadas áreas, precipitaciones de lluvias de gran intensidad descongelación, de capas de hielo por altas temperaturas, despliegue de grandes masas de agua que inundan áreas e infraestructuras materiales en el medio ambiente provocando pérdidas humanas y materiales(Quiroz, 2010).

2.2.1.8.6 Terremotos: Fenómenos naturales causados por movimientos telúricos de la capas de la corteza terrestres ocasionados por las reacciones de la naturaleza a causa de grandes impactos sobre los seres humanados causando pérdidas materiales, destrucciones de áreas edificaciones e infraestructuras terrestres[28].

2.2.1.8.7 AMENAZAS FÍSICAS

2.2.1.8.8 Agentes Internos: Personal interno responsable de acciones como modificaciones e instalaciones en las áreas de trabajo con previa autorización de actividades de acceso a áreas informáticas y equipos de cómputo.

2.2.1.8 Agentes Externos:

2.2.1.9. Hacker: Agentes curiosos de avanzados conocimientos en informática dedicados a investigaciones para a detectar debilidades en la red, atacar a los accesos a la información e interrumpen la seguridad de las organizaciones con acciones personales con fines de lucro para las manipulaciones de programas sistemas y redes de comunicación[29].

2.2.1.9.1 Cracker: Personas de amplios conocimientos de programación en informática poseen capacidades para manipular, modificar programas y equipos de software realizar falsificaciones de copias de productos originales también conocidos como atacantes a los accesos de seguridad de los de sistemas en líneas dedicados a la elaboración de programas gratuitos a través de las páginas de internet.

2.2.1.9.2 Lamer: Personas que carecen de conocimientos técnicos por problemas de aprendizaje (novatos) aprenden de conocimientos de otras personas es decir se caracterizan por las manipulaciones de objetos que ya han sido creados por otros desarrolladores e investigadores utilizados para beneficios personales, individuos caracterizados por la reproducción de materiales manipulados, con actos de apoderase de objetos ajenos para adultéralos[30].

2.2.1.9.3 ANÁLISIS DE VULNERABILIDADES

Las incapacidades de reaccionar ante algún evento depende de los proceso de administraciones informáticas por factores económicos la falta de recursos de seguridad pueden representar debilidades en las organizaciones.

Determinando cuáles son las debilidades que se dan en las áreas de administración de recursos informáticos como actividades de la institución.

El análisis de vulnerabilidades en la unidad de sistemas del Gobierno Autónomo Descentralizado permite identificar las principales causas que permite evidenciar los diferentes tipos de vulnerabilidades observadas para el estableciendo sugerencias.

Tabla 4. Análisis de Vulnerabilidades

ANÁLISIS VULNERABILIDADES			
ACTIVIDAD	**DESCRIPCIONES**	**OBSERVACIONES**	**SUGERENCIAS**
Capacitación informática	Normas internas	Conocimiento y responsabilidades	Recibir capacitaciones en medidas de seguridad
Monitoreo y evaluación	Políticas de seguridad	Supervisión	Verificar el cumplimiento de políticas para salvaguardar la integridad de activos y recursos
Accesos a Sitios web y Redes Sociales		Restricciones	Evitar el Uso de redes sociales en horas laborables
Infraestructura Tecnológica	Estándares de Seguridad	Administración de Seguridad informática	Disponer de mecanismos y herramientas (SGSI, Criptografía, autentificación)
Soporte de Tecnología		Equipamiento	Abastecimiento de equipos tecnológicos(Dispositivos de monitoreo y aplicaciones)

Conocimiento y Responsabilidades: El análisis de capacitación informática permite verificar el cumplimiento de normas internas en base a capacitaciones de medidas de seguridad.

Supervisión: El Análisis mediante el monitoreo permite verificar el cumplimiento de políticas para salvaguardar la integridad de Activos y recursos.

Restricciones: El análisis de accesos a sitios web y redes sociales permite verificar el cumplimiento de políticas de seguridad mediante restricciones de acceso en las horas laborables.

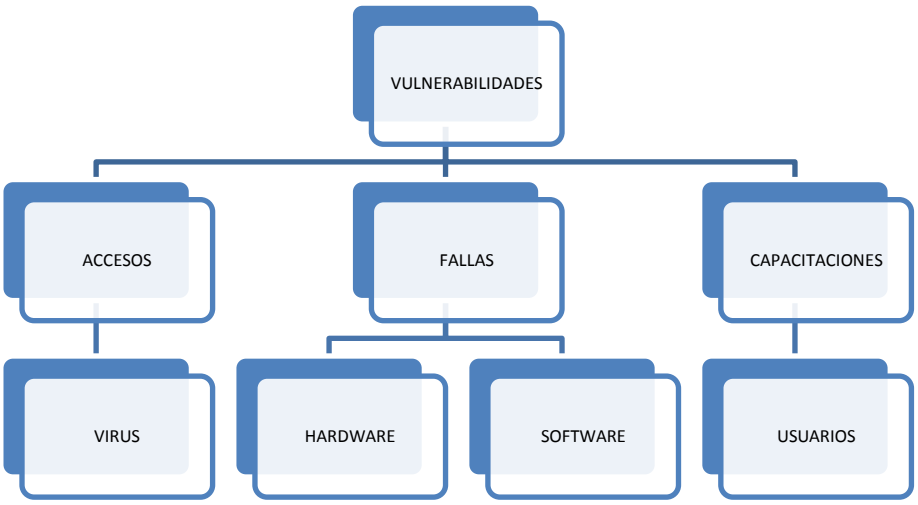
Administración de seguridad: El Análisis de la infraestructura tecnológica permite verificar el cumplimiento de estándares de seguridad para la administración de seguridad informática.

Equipamiento: El análisis de Soporte de tecnologías permite verificar el cumplimiento de estándares para el abastecimiento de equipos tecnológicos.

2.2.9.4 IDENTIFICAR VULNERABILIDADES

Las finalidades de los estudios de vulnerabilidades son detectar y verificar las diferentes amenazas que puedan generar debilidades que puedan afectar a la información y a los recursos informáticos que se pretende proteger mostrados en la siguiente figura donde se describen los tipos de vulnerabilidades más comunes en áreas de cómputo.

Figura 7.Identificación de Vulnerabilidades



Elaborado por: Reinaldo Ramírez

2.2.1.9.5 VULNERABILIDAD DE ACCESOS

La mayor probabilidad de amenazas en áreas informáticas se dan por uso de la web descargas de archivos, documentos, videos e imágenes de sitios web, compartición de redes sociales y dispositivos de almacenamiento externo durante las actividades de trabajo de las organizaciones la filtración de virus en los equipos de cómputo se da muchas veces por descuidos de actualizaciones del firewall es decir el escudo protector de Windows y simplemente la expiración de actualizaciones de antivirus en ambientes de trabajo.

2.2.9.6 VULNERABILIDAD POR FALLAS

Falla en los Sistemas: Los sistemas de información en los ambientes de institucionales muchas veces presentan inconvenientes de instalaciones de programas manipulaciones inadecuadas de herramientas de software que dificultan accesos y registros datos, interferencias eléctricas e ingreso de virus que dificultan las operaciones de trabajo en otras situaciones se dan por falta de integración de sistemas y redes de comunicación por lo general la falta de utilización de manuales de usuario pueden presentan muchas dificultades para la administración de recursos tecnológicos basados en capacitaciones por parte de especialistas en informática para administra sistemas.

Fallas en los Equipos: los equipos de cómputo en el mundo actual sufren interferencias por factores dados en los ambientes de trabajo y actividades personales cortes eléctricos, ingresos de virus, falta de soportes técnicos y sobrecargas de trabajo y riesgos de deterioro ante posibles incidentes sobre los recursos de hardware así como las necesidades de soporte de mantenimiento preventivo y correctivo para reparar daños y retornar las actividades de trabajo.

2.2.1.9.7 VULNERABILIDAD POR FALTA DE CAPACITACIONES

Se considera como el nivel entrenamiento de personas que requiere una esmerada capacitación para enfrentar los cambios tecnológicos acceso a las investigaciones y propuestas de especialistas (SENA, 2013).

2.2.1.9.8 ANÁLISIS DE IMPACTOS

Los impactos sobre los activos y recursos informáticos de la institución pueden representarse en pérdidas económicas de productos, para identificar la cantidad de pérdidas anuales, los riesgos se calculan mediante el producto de dos valores es decir el impacto (I) por la frecuencia (F) la cantidad de daños que se puedan presentarse en la unidad de sistemas como necesidades de control de riesgo económicos. El análisis de impactos se puede distinguir en la siguiente tabla[31]:

Tabla 5 .Análisis de Impactos

Unidad de Sistemas	Integridad Datos		Confidencialidad	Disponibilidad	Riesgo.
	Modifica	Destrucción			
Recursos	Información				
Impacto	I	I	I	I	I
Frecuencia	F	F	F	F	F
Costo	($)	($)	($)	($)	($)

Elaborado por: Reinaldo Ramírez

2.2.9.9 ANÁLISIS DE TRATAMIENTO DEL RIESGO

El tratamiento del riesgo es la acción llevada a cabo para controlar el riesgo identificando cada una de las amenazas en la unidad de sistemas determinando la implantación de mecanismos y herramientas para aceptar, transferir, eliminar y reducir riesgos[32].

Tabla 6. Análisis de Tratamiento con los Riesgos

Tratamiento del Riesgo en la Unidad de Sistemas				
Accesos Físicos y Lógicos	Aceptar	Transferir	Reducir	Eliminar

2.2.2. FASE DE EJECUCIÓN

La ejecución del Plan estratégico contempla la organización de cronogramas de actividades para el desarrollo de la auditoria en un periodo determinado, para dirigir los procesos y documentos necesarios para llevar acabo los objetivos a alcanzar, asignar recursos humanos y materiales necesarios para supervisar las áreas y activos informáticos, recopilando datos para verificarlos y evaluarlos.

Tabla 7. Cronograma de Actividades de Auditoria

Actividades	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Planificación	**2014**	**2014**	**2014**	**2014**	**2014**	**2014**	**2014**	**2014**	**2014**	**2014**	**2014**	**2014**
Análisis												
Contrato												
Encuestas												
Entrevistas												
Evaluación												
Control												
Tratamiento												
Conclusiones												
Recomendaciones												
Informes												
Tiempo Total												**12 meces**

Elaborado por: Reinaldo Ramírez

2.2.1. LISTA DE CHEQUEO

Las listas de chequeo permiten considerar la coordinación de preguntas redactadas y emitidas por parte del supervisor informático con la finalidad de obtener resultados coherentes y correctos verificando las ventajas y desventajas de elaborar preguntas bien fundamentadas y analizadas para luego ser emitidas.

Las listas de chequeo se las realizan de manera calificativa de acuerdo a los resultados obtenidos de la realidad.

Tabla8. Lista de Chequeo

UNIDAD DE SISTEMAS **LISTA DE CHEQUEO**				
Auditor	RSRC	**Día**	**Mes**	**Año**

DESCRIPCIÓN				
		Cumple		
N^{O}	**Variable / Indicadores**	**Si**	**No**	**Observaciones**
1	**Preguntas**			
2				
3				

2.2.2.2 PERSONAL PARTICIPANTE

Un punto importante es el apoyo de autoridades y directivos contando con un grupo especializado para la participación del personal técnico y administrativo auditado para obtener información de las actividades de trabajo estableciendo las metas y objetivos de la investigación(Elkin Nacor Muñoz, 2013).

Personal Administrativo: Permiten obtener gran parte de informaciones documentadas en forma manual (archivos, documentos y solicitudes)

Proporcionando informaciones sobre las organizaciones de actividades realizadas mediante planes de trabajo.

Personal Técnico: Son personales con conocimientos en administraciones de sistemas de información y comunicación (base de datos archivos, registros, consultas y reportes) proporcionando información sobre funcionamiento y procesamiento de la información materiales y equipos tecnológicos utilizados con las siguientes características del personal.

Tabla 9. Personal Participante

Personal Participante	**Descripción**
Directivos	
Asistente Técnico	
Usuarios	
Empleados	

2.2.2.3 RECURSOS MATERIALES

Es importante señalar la utilización de requerimientos materiales para llevar a cabo la investigación y comprobar la existencia de los mismos que servirán para los objetos de estudio.

Tabla 10. Recursos Materiales

Recursos Materiales	**Descripción**
Computadores	
Impresoras	
Dispositivos	
Informaciones Manuales y Digitales	
Internet	
Sistemas de Información	
Inventarios de hardware y software	

2.2.2.4 EVALUACIÓN DE RIESGOS

La evaluación de riesgos en la unidad de sistemas permite identificar las principales causas para evidenciar los diferentes tipos de riesgos para el estableciendo sugerencias.

Los riesgos de amenazas y vulnerabilidades serán evaluados y representados mediante una tabla de clasificación de riesgos presentado en la siguiente explicaciones[33].

R1 representara el nivel de riesgo inicial B con la posibilidad de riesgo bajo y un impacto indicador L Leve color Verde

R2 representara el nivel de riesgo inicial M con la posibilidad de riesgo medio y un impacto indicador M moderado color Amarillo

R3 representara el nivel de riesgo inicial A con la posibilidad de riesgo muy alta y un impacto indicador C catastrófico color Rojo

Tabla 11.Clasificación de Riesgos

Cuadro de evaluación de riesgos amenazas y vulnerabilidades					
Unidad de Sistemas					
Nivel	**Variable**	**Indicador**	**Variable**	**Impacto**	**Color**
R3	A	Alta	C	Catastrófico	
R2	M	Media	M	Moderado	
R1	B	Baja	L	Leve	

Elaborado por: Reinaldo Ramírez

DESCRIPCIÓN DE ACTIVOS	VALOR	CALIFICATIVOS	CONTROL DE RIESGOS
	1	Correcto.	Amenazas
	2	Aceptable	Vulnerabilidades
	3	Mejorable.	Confidencialidad
	4	Deficiente.	Integridad
	5	Muy deficiente	Disponibilidad

Tabla12. Evaluación de Riesgos de Activos

EVALUACIÓN DE RIESGOS			
REVISIÓN	**DESCRIPCIONES**	**OBSERVACIONES**	**SUGERENCIAS**
Recursos tecnológicos	Instructivos de Operación	Manuales operativos	Administrar los sistemas y aplicaciones utilizando los manuales del usuario
Autentificación	Accesos Lógicos	Contraseñas	Autentificar y actualizar claves personales
Administración de Activos	Hardware	Inventarios	Mantener un registro de inventarios
	Software		
Cifrado de claves	Seguridad Lógica y Confidencial	Restricción y refrendación de claves y archivos confidenciales	Cifrar los accesos a la información confidencial
Seguridad Física	Seguridad en los equipos informáticos	Administración de equipos	Establecer dispositivos de vigilancia
Seguridad Lógica	Seguridad en los Sistemas	Administración de claves	Establecer mecanismos de Cifrado
Recuperación de información	Procedimientos de respaldos	Respaldos programas e información	Respaldar la información en lugares seguros y recuperables ante emergencia

Elaborado por: Reinaldo Ramírez

Manuales operativos: La evaluación de administración del manual de usuario permiten comprobar la utilización de Manuales de Usuario para administrar Sistemas y Aplicaciones en las áreas informáticas.

Autentificación: La evaluación de claves de accesos de los usuarios permite comprobar las restricciones y refrendaciones de claves de accesos verificando la autentificación de claves del usuario.

Inventarios de hardware y software: La evaluación de administración de activos permite verificar la existencia de inventarios de acuerdo a las caracterizas, diseño costo y adquisición de productos informáticos en las áreas de trabajo.

Administración de equipos: La evaluación de seguridad física permite comprobar la seguridad en los equipos informáticos para la aplicación de dispositivos de seguridad.

Administración de sistemas: La evaluación de la administración de claves permite comprobar el uso de cifrado de claves.

Respaldos de programas e información: La evaluación de recuperación de información permite comprobar los respaldos de información en lugares seguros.

2.2.2.5 EVALUACIÓN DE AMENAZAS

La evaluación de amenazas en la unidad de sistemas permite identificar las principales causas para evidenciar los diferentes tipos de amenazas evaluadas para el estableciendo sugerencias.

Tabla 13. Evaluación de Amenazas

EVALUACIÓN DE AMENAZAS			
ACTIVIDAD	**DESCRIPCIÓNES**	**OBSERVACIONES**	**SUGERENCIAS**
Agentes internos	Errores Técnicos	Labores de trabajo informáticas	Supervisar el cumplimiento de responsabilidades
Agentes Externos	Corrupción	Entrada y salida del personal	Aplicar Restricciones y accesos Autorizados
	Espionaje		
Agentes		Interferencias	Aplicar y actualizar escudos

Cibernéticos	Virus		protectores firewall antivirus
Medidas de prevención	Consumo de bebidas ingreso de materiales tóxicos	Áreas y equipos informáticos	Aplicación de restricciones
Salvaguarda	Confidencialidad Integridad , Disponibilidad	Información manual y electrónica	Establecer controles de modificación y eliminación de información
Instalaciones	Fallas eléctricas	conexiones cableado y energía	Verificar conexiones eléctricas
Medidas de emergencia	Incendios	Respaldos de Información	Mantener Archivadores Lugares seguros
	Inundaciones	Respaldos de Sistemas	Mantener respaldos de sistemas y programas
	Terremotos	Seguridad en los Equipos	Mantener los equipos en lugares seguros

Elaborado por: Reinaldo Ramírez

Agentes internos: La evaluación de labores de trabajo permite comprobar las posibilidades errores técnicos y cumplimiento de responsabilidades de labores de trabajo personal interno en la institución.

Agentes Externos: La evaluación de entrada y salida del personal permite comprobar las posibilidades amenazas de corrupción y espionaje de accesos de personas ajenas a la institución

Agentes cibernéticos: La evaluación de interferencias permite verificar las protecciones y actualizaciones de programas contra virus en los equipos informáticos.

Medidas de prevención: La evaluación de áreas y equipos informáticos permite comprobar las restricciones para los ingresos de materiales, bebidas y productos tóxicos en áreas de trabajo.

Salvaguarda: La evaluación de administración de información permite comprobar los controles de confidencialidad integridad y disponibilidad de la información.

Instalaciones: La evaluación de conexiones de cableado permite comprobar las posibilidades de fallas eléctricas en las áreas informáticas.

Medidas de emergencia: La evaluación de respaldos permite comprobar si existen mecanismos de respaldos de programas información y seguridad de equipos informáticos ante incendios inundaciones y terremotos.

2.2.2.6 EVALUACIÓN DE VULNERABILIDAES

La evaluación de vulnerabilidades en la unidad de sistemas del Gobierno autónomo descentralizado permite identificar las principales causas que permite evidenciar los diferentes tipos de vulnerabilidades evaluadas para el estableciendo sugerencias.

Tabla 14. Evaluación de Vulnerabilidades

EVALUACIÓN DE VULNERABILIDADES			
ACTIVIDAD	**DESCRIPCIÓN**	**OBSERVACIONES**	**SUGERENCIAS**
Capacitaciones	Técnicas	Conocimientos técnicos	Recibir capacitaciones en tecnologías
Soporte técnico	Fallas en hardware	Mantenimientos Preventivos	Establecer reparos
		Mantenimientos correctivos	Establecer respaldos
	Fallas en software		
Accesos	Agentes internos y Externos	Accesos Físicos y Lógicos	Controlar los accesos Autorizados
Seguridad Lógica	Filtración de virus	Escudo de protección de virus	Mantener instalaciones y actualizaciones de antivirus
Comunicación	Fallas de integración	Redes de comunicación	Establecer canales de comunicación redes

Capacitaciones: La evaluación de conocimientos técnicos permite comprobar las técnicas de capacitaciones para administrar recursos tecnologías.

Mantenimientos Preventivos y correctivos: La evaluación de soporte técnico permite verificar la vulnerabilidad de fallas de hardware y software comprobando los mantenimientos preventivos y correctivos.

Accesos físicos y lógicos: La evaluación de accesos físicos permite evidenciar la vulnerabilidad de accesos de agentes externos e internos comprobando los accesos autorizados.

Escudos de protección de virus: La evaluación de seguridad lógica permite evidenciar las vulnerabilidades de filtración de virus en los equipos tecnológicos comprobando las actualizaciones de antivirus

Redes de comunicación: La evaluación de comunicación permite evidenciar las faltas de integración comprobando los canales de comunicación de redes locales.

2.2.2.7 FASE DE MONITORIZACIÓN

Las necesidades de monitorear las áreas informáticas se llevan a cabo para controlar la gestión de seguridad de la información basados en actividades de supervisión de manera continua por ejemplo: la detección de amenazas de los recursos informáticos asignados a los empleados de mantener la confidencialidad, integridad y disponibilidad de la información ante eventos imprevisto de presencia de acciones y amenazas de agentes externos y el efecto sobre los activos y recursos tecnológicos de la institución.

Se tomara en cuenta la auditoria externa para la comprobación de hechos y sucesos también se tomara en cuenta el proceso certificable si se cumplen con las normas y estándares establecidos.

2.2.2.8 PASOS PARA CONTROLAR RIESGOS

Dependiendo del análisis de la unidad de sistemas se establecen controles relevantes que identificara las categorías en las que se mantendrán los controles (I) Implantado, (P) en proceso de implantación, (N) o no Existentes[34].

Tabla. 15 Control de Riesgos

Auditoria Externa	**Estado de control en la Unidad de Sistemas**		
Descripción	**Implantado**	**Proceso de implantación**	**No existe**
Indicadores	I	P	N

2.2.2.9 CONTROLES DE RIESGOS ADMINISTRATIVOS

La finalidad del control de riesgos es analizar el cumplimiento de medidas de protección mediante la ejecución de actividades ante las amenazas y vulnerabilidades basadas en normas, políticas y estándares aplicados a la institución[35].

El control de riesgos en la unidad de sistemas permite controlar las principales causas de riesgos observados para el estableciendo sugerencias.

Tabla 16. Control de Riesgo de Activos

RIESGOS			
DESCRIPCION	**CONTROL**	**OBSERVACIONES**	**SUGERENCIAS**
Normas internas	Supervisiones	Planificaciones	Realizar una correcta planificación de Auditoria
Políticas de seguridad	Accesos físicos y lógicos	Acceso a los equipos y sistemas	Verificar accesos de usuario y administrador
	Hardware y software	Inventarios	Verificar la existencia de inventarios de equipos y sistemas
Estándares de Seguridad	Monitoreo	Comunicación	Tomar acciones preventivas para fortalecer la seguridad
	Mecanismos	Acciones de seguridad	Establecer Medidas correctivas para mejorar la seguridad

Planificaciones: El control de supervisiones de normas internas permite realizar una correcta planificación de actividades de Auditoria externa.

Accesos a los equipos: El control de accesos físicos permite comprobar el cumplimiento de políticas de seguridad para verificar los Accesos a los equipos mediante el usuario o administrador.

Acceso a los sistemas: El control de acceso lógico permite comprobar el cumplimiento de políticas para verificar los accesos a los sistemas mediante la verificación de autenticidad y cifrado de claves personales.

Comunicación: El control mediante el monitoreo permite comprobar los estándares de seguridad para tomar acciones preventivas.

Acciones de seguridad: El control de mecanismos de seguridad permite comprobar los estándares para actuar estableciendo medidas de seguridad.

2.2.3. CONTROLES OPERATIVOS DE AMENAZAS

Estos controles permiten observar si existen procedimientos de seguridad ante amenazas desastres e incidentes relacionados con las medidas de seguridad y planes respaldos de información[36].

El control de Amenazas en la unidad de sistemas del permite controlar las principales causas de amenazas observadas para el estableciendo sugerencias.

Tabla 17. Control de operativos de Amenazas

AMENAZAS			
DESCRIPCION	**CONTROL**	**OBSERVACIONES**	**SUGERENCIAS**
Normas internas	Accesos físicos y lógicos	Restricciones	Establecer restricciones a accesos no autorizados
Políticas de seguridad	Instalaciones	Conexiones eléctricas y	Establecer conexiones seguras y programas de seguridad
Estándares de Seguridad	Contingencias	Medidas de emergencia	Establecer la utilización de herramientas de emergencia y seguridad
	Desastres	Mecanismos Respaldos	Establecer Mecanismos de respaldos

Restricciones: El control de accesos físicos y lógicos permite comprobar el cumplimiento de normas internas para los accesos autorizados a áreas y recursos informáticos.

Medidas de emergencia: El control de planes de contingencias permite comprobar el cumplimiento de políticas para establecer herramientas de emergencia ante desastres.

Mecanismos de respaldos: El control de Desastres permite comprobar el cumplimiento de estándares de seguridad para establecer mecanismos de respaldos.

2.2.3.1 CONTROLES TÉCNICOS DE VULNERABILIDAES

Los controles técnicos permiten verificar los mecanismos de seguridad de recursos de hardware y software para asegurar el cumplimiento de normas políticas y estándares de seguridad[37].

El control de Vulnerabilidades en la unidad de sistemas permite controlar las principales causas de vulnerabilidades observadas para el estableciendo sugerencias.

Tabla 18. Control de Vulnerabilidades

VULNERABILIDADES			
DESCRIPCIÓN	**CONTROL**	**OBSERVACIONES**	**SUGERENCIAS**
Normas internas	Talleres y Seminarios	Capacitaciones	Recibir capacitaciones en seguridad y emergencias informáticas
Políticas de seguridad	Hardware y Software	Soporte técnico	Establece r Técnicas de mantenimiento
	Firewall	Actualizaciones de Seguridad	Actualizar el Firewall para evitar riesgos y amenazas
Estándares de Seguridad	Software	Herramientas de seguridad	Establecer Sistemas de seguridad

Capacitaciones: El control de talleres y seminarios de capacitación permite comprobar el cumplimiento de normas internas verificando el cumplimiento de disposiciones normativas.

Soporte de Técnico: El control de hardware permite comprobar el cumplimiento de políticas de seguridad para las actividades de manteamiento preventivo y correctivo.

Actualizaciones de Seguridad: El control de Actualizaciones de firewall permite comprobar el cumplimiento de políticas de seguridad para evitar riesgo y amenazas.

Herramientas de seguridad: El control se software y software permite comprobar el cumplimiento de los estándares de seguridad para establecer sistemas de seguridad.

2.2.3.2 FASE DE MEJORA

Comprende la etapa de tomar medidas de seguridad sobre los riesgos identificados mediante verificaciones del cumplimiento de los objetivos antes mencionados, en la etapa de puesta en marcha los controles de seguridad se tomaran medidas preventivas y correctivas orientadas a la solución de los problemas detectados mediante mecanismo establecidos.
Las mejoras continuas de seguridad se verificaran en informes que establecen el alcance de los objetivos estableciendo conclusiones y recomendaciones documentadas y comunicadas a las unidades de auditoria.

2.2.3.3 GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN VENTANAS.

La Constitución de la República del Ecuador señala que los Gobiernos Autónomos Descentralizados son ejercidos por los Gobiernos Provinciales, Municipales, Parroquiales Rurales, Distritos Metropolitanos, y las circunscripciones territoriales de comunas, comunidades, pueblos y nacionalidades indígenas, Afro Ecuatorianas y montubias;

Reestructurar el Orgánico Funcional que norme de manera clara y objetiva los procedimientos de la administración del Gobierno Municipal, los niveles jerárquicos, delegación, coordinación, control y las funciones específicas de cada Unidad Administrativa; de acuerdo a las competencias exclusivas y las que determine la ley, señaladas en el artículo 264 de la Constitución de la República del Ecuador.

Las funciones del Gobierno Autónomo Descentralizado Municipal del Cantón Ventanas esta dado bajo un marco de políticas públicas de planificaciones nacionales y regionales[38].

Participación social: la elaboración y aplicación de políticas públicas para dar seguimiento a la elaboración de proyectos garantizando los accesos a bienes y servicios.

Viabilidad Económica: promover un marco de planificaciones Cantonales mediante actividades económicas públicas y privadas de competitividad y beneficio social.

Cooperación Internacional: proveer la cooperación internacional a través del Estado Ecuatoriano para el fortalecimiento de la infraestructura de desarrollo social económico y productivo de planificación y responsabilidad Municipal[39].

2.2.3.4 MISIÓN INSTITUCIONAL

Asegurar el desarrollo social, económico y ambiental de la población con la participación de actores sociales, mediante la conservación ambiental de transparencia moral, ética institucional de sus servidores descartando los actos de corrupción de la institución al margen de la ley para el bienestar de colectividad, defensa y protección de intereses locales[40].

2.2.3.5 VISIÓN INSTITUCIONAL

Consolidar la Institución en el desarrollo social, económico y productivo, servicios públicos, seguridad ciudadana, impulsar el micro emprendimiento apoyando a todas las áreas para las competencias en beneficio a la comunidad Ventanéense[41].

FIGURA 8. ESTRUCTURA ORGANIZACIONAL DEL GAD MUNICIPAL VENTANAS

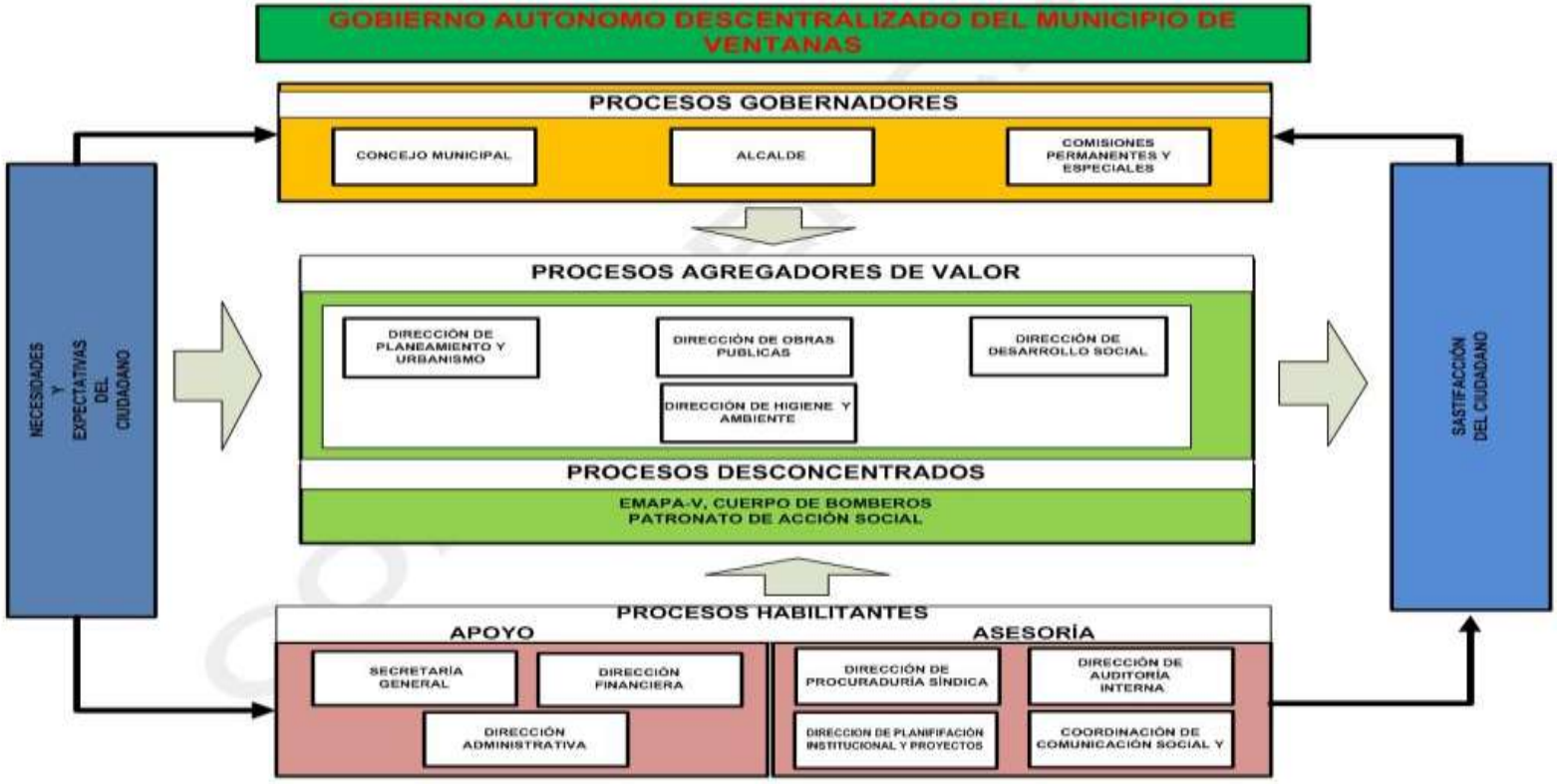


Figura8. Fuente: GAD Municipal de Ventanas

42

www.ventanas.gob.ec

2.2.3.6 REVISIONES POR LA DIRECCIÓN

Las revisiones por parte de la dirección deben recopilar las evidencias suficientes según la propuesta para la toma de decisiones sobre los estudios de riesgos y procedimientos para los controles de seguridad estableciendo indicadores de riesgos.

2.2.3.7 RESVISIÓN DE NORMAS DE CONTROL INTERNO

2.2.3.8 Comités informáticos

El departamento de informática contara con un comité informático legalmente establecido y definido en función del tamaño y complejidad de la entidad.

Los comités de informática de las entidades contemplaran la organización de grupos de consultoría de gestiones para la toma de decisiones.

2.2.3.9 Monitoreo y Evaluación de la Unidad Informática

El departamento de informática definirá una metodología legalizada establecida que permita monitorear las contribuciones y acciones realizadas por el departamento de informática.

2.2.4 Seguridad de Tecnología de Información

La Unidad de Sistema establecerá mecanismos de seguridad de recursos informáticos y sistemas de información para la gestión de procesos de vigilancia tomando medidas preventivas y correctivas en base a los riesgos que puedan presentarse durante las etapas de ejecución trabajos internos.

Protección de activos y recursos físicos de las áreas informáticas contra perdidas estableciendo procedimientos formales de obtención periódica de respaldos

2.2.4.1 Políticas y Procedimientos

La unidad de sistemas establecerá estándares y reglamentos para las actividades de las tecnologías de la información en la organización vigentes de acuerdo a las tareas de responsabilidades de las ejecuciones de procesos informáticos en base al cumplimiento normativo según las sanciones administrativas.

2.2.4.2 Controles sobre sistemas de información

La unidad informática definirá mecanismos para los controles de seguridad, integridad, confiabilidad y accesibilidad de la información, para las administraciones de calidad de acuerdo a los niveles de acceso a la información y administración de datos.

La utilización de los sistemas de información responsabilizara a las unidades de tecnologías de las actividades realizadas por la administración en las áreas informáticas de la institución.

2.2.4.3 Adquisiciones de Infraestructura Tecnológica

La Unidad de sistemas realizara planificaciones en base a las capacidades para responder ante los riesgos tecnológicos con versiones y actualizaciones considerando los requerimientos de trabajos para los almacenamientos de información en caso de contingencias de recursos tecnológicos.

2.2.4.4 Capacitación informática

La unidad de tecnologías definirá proyectos de capacitaciones del personal de informática con capacitación técnica a los usuarios que administran los servicios de información.

2.2.4.5 Organización Informática

La unidad de sistemas establecerá Infraestructuras tecnológicas para las atribuciones de desempeño de las gestiones administrativas contemplando regulaciones en temas tecnológicos

2.2.4.6 Segregación de Funciones

La unidad de sistemas definirá las Atribuciones de responsabilidades, por medio de procedimientos de producto y recursos informáticos asignados a usuarios y empleados como partes de la administración información.

2.2.4.7 Planeamiento Informático Estratégico de Tecnología

La unidad de Sistemas establecerá desarrollos de proyectos informáticos de tecnologías legalizados por las autoridades relacionados a las políticas públicas e institucionales.

2.2.4.8 Modelo de Información Organizacional

La unidad de sistemas establecerá servicios de información y comunicación mantendrá un modelo definido para la compartición de datos e información con integridad, disponibilidad y seguridad de la información.

2.2.4.9 Administración de Proyectos Tecnológicos

La Unidad de tecnologías establecerá mecanismos que faciliten las administraciones de proyectos informáticos utilizados en la unidad tecnológica estableciendo objetivos para los alcances de proyectos institucionales, mediante

cronogramas de actividades, recursos humanos y económicos con pruebas y capacitaciones.

2.2.5. Desarrollo y Adquisición de Software Aplicativo

La Unidad de Sistemas establera lineamientos con procedimientos que regulen los procesos de desarrollo para adquisición de software aplicativos con sus respectivas licencias de uso.

2.2.5.1 Mantenimiento y control de la Infraestructura Tecnológica

La Unidad de Sistemas implementara planes de soporte técnico preventivos y correctivos de las plataformas informáticas por medio de supervisiones periódicas de vigilancia ante posibles acciones institucionales con controles de seguridad ante de riegos de vulnerabilidades como mecanismos de seguridad.

2.2.5.2 Administración de Soporte de Tecnología

La unidad de sistemas establecerá niveles operativos que agiliten la adecuada gestión de operaciones de plataformas tecnológicas que fortalezcan la seguridad e intangibilidad de los activos e información para un buen servicio informático disponiendo de procedimientos legalizados que permitan administrar las informaciones con librerías sistemas de respaldos y recuperación de datos.

2.2.5.3 Sitios web y servicios de internet Intranet

El departamento de informática definirá las normas y restricciones procedimientos de instructivos de servicios de internet, correos electrónicos dentro de la entidad.

2.2.5.4 Firmas electrónicas

La entidad se ajustara a los procedimientos de operaciones implementando técnicas para el uso de firmas electrónicas de acuerdo a la ley del comercio electrónico.

2.2.5.5 Canales de comunicación abierta

La unidad informática establecerá redes de comunicación que permitan enviar y recibir información de modo seguro preciso y oportuno, a los destinatarios integrados con la institución a través políticas de control interno, que permitan integrar a los funcionarios y funcionarias de la institución sobre controles administrativos de acuerdo a sus funciones en las diferentes áreas.

2.2.5.6 Planes de Contingencias

La Unidad de sistemas establecerá el desarrollarlo de planes de emergencias ante posibles riesgos de tecnologías informáticas mediante simulacros de contingencias con responsabilidades de la salvaguarda física y lógica, de las informaciones internas como medidas de protección para la recuperación de activos institucionales(039-CG Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Disponga de Recursos Públicos.).

2.2.5.7 REVISIÓN DE POLÍTICAS DE SEGURIDAD

Comprende la revisión de reglas establecidas por autoridades de la institución mediante unos actos jurídicos enfocados a las administraciones de las tecnologías de información y comunicación orientadas a los usuarios que administran recursos informáticos proporcionados por unidades de sistemas y tecnologías utilizados en instituciones para el cumplimiento de seguridad.

Las políticas serán administradas por los directivos de las áreas administrativas e informáticas de forma general para verificar el cumplimiento mediante revisiones y actualizaciones basadas en recomendaciones y sugerencias(Gómez Vieites, 2012).

2.2.5.8 REGLAMENTOS GENERALES

El cumplimiento de las reglas obligatorias son coordinaciones por los directivos conjuntamente con los comités informáticos y empleados de las instituciones responsables de las administraciones de recursos de hardware y software con controles de seguridad y calidad de la información para el desempeño administrativo bajo custodia, tomando medidas preventivas y correctivas para que se cumplan.

Las gestiones de las tecnologías de información en las áreas administrativas son ordenamientos estandarizados en base al desarrollo de actividades y administración informática proporcionando mecanismos de seguridad y efectividad de la información para las organizaciones.

Los comités informáticos estarán integrados a los directivos de las aéreas informáticas y al personal administrativo en base al cumplimiento de las normas institucionales de administración de tecnologías e informática con las siguientes atribuciones y responsabilidades.

- Establecimiento de infraestructuras tecnológicas
- Establecimiento de redes servidores e integración de sistemas
- Monitorear el funcionamiento de las áreas informáticas y sistemas de información mediante la implementación de cámaras de seguridad
- Dar seguimiento a las actividades administrativas mediante un plan de auditorías informáticas mediante las unidades de auditoria interna de la institución verificando el cumplimiento de las normas de control interno.
- Fortalecer las infraestructuras tecnológicas e informáticas
- Controlar los niveles de servicio otorgado por los usuarios
- Verificar el cumplimiento de las políticas establecidas por la institución.

2.2.5.9 RESPONSABILIDADES DE LA DIRECCIÓN INFORMÁTICA

Las responsabilidades de las normas de seguridad son cargos signados por los comités directivos de las áreas informáticas como bases de cumplimiento normativo dirigidos a empleados de las áreas informáticas sobre las atribuciones de responsabilidades y asignación de funciones sujetos a revisiones de salvaguarda de informaciones ante amenazas actos de divulgaciones confidenciales utilizadas por agentes potenciales en las redes de comunicación (internet, email, aplicaciones web, sistemas, redes y servidores) utilizando estándares de seguridad informática[43].

2.2.6. ANÁLISIS DE LA UNIDAD DE SISTEMAS INFORMÁTICOS

El objetivo del análisis informático es identificar los factores administrativos expuestos amenazas e interferencias, que puedan afectar generalmente a la información y actividades de procesamiento de datos.

El análisis de amenazas en los procesos de registro de la información puede ser detectado o no para ello se pretende estimar evaluaciones a la institución teniendo en cuenta las posibilidades de que puedan surgir problemas durante la fase de desarrollo.

2.2.6.1 ESTRUCTURA ORGANIZACIONAL DE EQUIPOS DE TRABAJO

La unidad de sistemas tiene definida sus funciones de acuerdo a las atribuciones de cargos con responsabilidades organizadas dentro de la institución para realizar las labores administrativas y técnicas.

2.2.6.2 EQUIPO DIRECTIVO

Encargados de coordinar adecuadamente las actividades de las áreas informáticas con reglamentos de responsabilidades de la administración, custodia de los activos y recursos de las áreas informáticas para aportar soluciones de inconvenientes de cada equipo asignado bajo ordenanzas de Actividades Municipales para la gestión de documentos, proveer de servicios a los ciudadanos del Cantón Ventanas encargado de la unidad.

- Director coordinador de la Unidad.

2.2.6.3 EQUIPO DE SISTEMAS Y ASISTENCIA TÉCNICA

Encargados de prestar servicios de Asistencia técnica a los equipos de cómputo con actividades de mantenimientos preventivos y correctivos de fallas que puedan ocurrir, tomando medidas preventivas de filtración de amenazas e incidentes que puedan ocurrir por fallas ante eventos imprevistos ocurridos en los equipos con la aplicación de medidas correctivas encargados de la unidad.

2.2.6.4 TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Las Tecnologías de información son un grupo componentes de hardware y software destinados a la gestión de datos e información organizada para facilitar las necesidades de personas, actividades, datos y comunicación de recursos materiales e informático que interactúan mediante procesos manuales y automatizados[44].

Los sistemas de información permiten almacenar, manipular, administrar, controlar, procesar, trasmitir y recibir datos para satisfacer las necesidades de los usuarios, abarca todo lo que es equipos de cómputo y personas para gestionar la transmisión de datos.

Usuarios: son personas que interactúan con los sistemas para registrar, procesar y almacenar información de manera responsable con controles de autenticidad y accesibilidad de manera segura.

Equipos técnicos: comprende el uso responsable de hardware y software utilizado materiales y documentos manuales relacionado con otros elementos que conforman las actividades de soporte a la comunicación e información(Galdámez).

2.2.6.5 INFORMACIÓN

La información es un conjunto de datos recopilados, redactados en documentos que pueden ser digitalizados, almacenados y procesados con el propósito de servir de base para realizar tareas, actividades, transacciones administrativas, operacionales, económicas y financieras sirven de base para prestar servicios de gestión recepción, distribución de bienes y recursos en una organización.

Información Manual: Es la información utilizada para los procesos administrativos de las unidades informáticas esta información puede ser información técnica para los controles técnicos información estratégica para los procesos estratégicos información financiera para los controles financieros y contables,

Información Electrónica: Es el tipo de información compartida por medios electrónicos las mismas que pueden contener datos públicos y confidenciales que son compartidas por medio de correos electrónicos[45].

2.2.6.6 SISTEMAS INFORMÁTICOS UTILIZADOS

Control Municipal: Plan /gestión de predios urbanos y rurales para el control de registros de la propiedad con avalúos y catastros de solares.

Gestión integral: Sistema de información catastral en línea para gestión de información de catastros del Cantón Ventanas.

2.2.6.7 ÁREAS DE TRABAJO

La gestión de actividades en los departamentos informáticos son análisis de procesamiento de la información de acuerdo a las normas institucionales referentes al uso de tecnologías informáticas con los siguientes aspectos.

- Soportes técnicos en administraciones informáticas a equipos Municipales para ayudar a los controles de calidad de acuerdo a los procesos administrativos para gestionar la seguridad de la información a cargos de los funcionarios y empleados a futuro se pretende contar con un sistema de gestión de seguridad para los gobiernos Municipales.
- Implementar proyectos y recursos tecnológicos mediante la evaluación de sistemas informáticos como parte de la propuesta.

2.2.6.8 ORGANIZACIÓN ACTUAL DE LA UNIDAD DE SISTEMAS

2.2.6.9 PLATAFORMA TÉCNOLOGICA

La infraestructura informática es el soporte principal de cualquier organización permite la administración de actividades mediante la implementación de equipamientos de recursos tecnológicos que agiliten las gestiones de la institución de manera inmediata con requerimientos y exigencias del mundo actual con los siguientes aspectos.

La organización actual del área de sistemas se encuentra conformada por los recursos de hardware (componentes y dispositivos de comunicación de las áreas de trabajo) y software (sistemas de información e integración, programas de Windows, base de datos) y asistencia técnica (servicios de mantenimiento preventivo y correctivo de los recursos informáticos) administrados por personales del área de sistemas.

2.2.7. ENTORNOS DE ÁREAS TRABAJO

Se deben considerar las siguientes condiciones

- Ubicación de los recursos informáticos
- Espacio amplio y acondicionado
- Personal capacitado

2.2.7. 1 RECURSOS INFORMÁTICOS

- Sistemas de información
- Equipos de cómputo
- Respaldo de información

2.2.7.2 PERSONAL DE TRABAJO Y SUMINISTROS

- Servicios de asistencia técnica
- Costo y Duración

Establecida la planificación estratégica se realizaran respaldos de la información en interferencias de seguridad se desarrollaran todos los pasos basados en mecanismos con tareas para fortalecer los procesos de seguridad en a un determinado plazo.

2.2.7.3 AREA DE SISTEMAS Y SOPORTE TÉCNICO

Atribuciones y Responsabilidades

- Términos de referencia y especificaciones técnicas.
- Dar soporte técnico a todas las áreas administrativas con mantenimientos preventivos y correctivos (equipos, impresoras)
- Asistencia técnica presencial a los recursos de informáticos de la institución Municipal. Medidas técnicas de uso de aplicaciones puntuales. Ayuda a los usuarios en utilización de nuevo hardware para su eficiente aprovechamiento.

2.3 POSTURA TEÓRICA

En el campo de la eficiencia y seguridad de los sistemas de información muchas organizaciones e instituciones públicas pueden tener dificultades por el desconocimiento de los avances tecnológicos basadas en las vulnerabilidades que pueden presentarse en los sistemas en relación al ámbito administrativo, que actualmente nos ofrece una nueva estrategia de cómo administrar nuestras organizaciones e instituciones que utilicen sistemas de información, poniendo en práctica todas las herramientas que se requieren para, brindar servicios de calidad, si bien es cierto el trabajo investigativo se lo realizo en la unidad de Sistemas del Gobierno Autónomo Descentralizado de la Municipalidad del Cantón Ventanas en donde hemos encontrado una problemática debido al desconocimiento de los controles de seguridad en el uso adecuado de los activos y recursos informáticos para una buena administración, por este motivo, según los contenidos se explicaran los requerimientos de seguridad que requiera el investigador porque en la actualidad tenemos instancias públicas y privadas.

En base a la investigación realizada para el desarrollo del proyecto, el libro que más se ajusta al tema de investigación de Auditoria Informática es la del Autor José Antonio Echenique García (2003). Auditoría en Informática. México edición de McGraw-Hill ubicado en la Biblioteca General de la Universidad Técnica de Babahoyo.

La edición de McGraw-Hill especifica la coordinación de procedimientos basados en los análisis investigativos para el desarrollo de la auditoria informática, por medio planificaciones que indican los pasos de evaluaciones de las áreas, recursos humanos y tecnológicos de las organizaciones describiendo los requerimiento e instrumentos necesarios que el auditor debe aplicar para la ejecución de la auditoria bajo los conocimientos informáticos adquiridos de la entidad a auditar(Echenique, Auditoria en Informática, 2013).

2.4 HIPÓTESIS

2.4.1 Hipótesis General de Trabajo

El Plan de Auditoría Informática en la Unidad de Sistemas de la Municipalidad del Cantón Ventanas mejorara el control de seguridad de los activos y recursos informáticos

2.4.3 Hipótesis Específicas

- La aplicación de la auditoria informática permitirá controlar la seguridad de la Unidad de Sistemas en el Gobierno Autónomo Descentralizado Municipal del Cantón de Ventanas.

- El diagnóstico de la seguridad informática en la unidad de sistemas estará acorde a las necesidades de la aplicación del plan de auditoria.

- Las Normas internas de auditoría informática permitirán realizar un control de seguridad en la Unidad de Sistemas del Gobierno Autónomo Descentralizado del Cantón de Municipalidad del Cantón Ventanas.

2.4.4 Variables

2.4.5 Variable Independiente:

Plan de Auditoria informática

2.4.6 Variable Dependiente:

Control de seguridad de los activos y recursos.

III. RESULTADOS DE LA INVESTIGACIÓN

3.1 DESCRIPCIÓN DE LOS RESULTADOS

3.1.2. METODOLOGÍA DE LA INVESTIGACIÓN

Para lograr los alcances de los objetivos se utilizó los siguientes tipos de investigaciones.

De campo: Con el objetivo de realizar un análisis completo se recopilo toda la información y los instrumentos necesarios para el desarrollo de la auditoria, para lo cual se realizó una investigación de campo en el lugar de los hechos, es decir en la unidad de sistemas de GAD Municipal del Cantón Ventanas, realizando encuestas y entrevistas al personal administrativo como también a la ciudadanía, y de esta manera se llegó a un acuerdo como se realizó la auditoria, y también cuál es su contenido.

Documental: La investigación se baso en el análisis y estudio realizado de revisiones de varias fuentes bibliográficas sitios web, es decir mediante documentos e informaciones obtenidos a través de fuentes bibliográficas (sitios web, libros, revistas), (artículos periódicos) y (en archivos, etc.). En tipo de investigación el cual permitió, realizar el análisis del desarrollo de la auditoria.

Preliminar: La investigación permitió tener una idea global del departamento y percibir las estructuras fundamentales de la organización para recopilar información mediante una visión general del departamento por medio de observaciones, entrevistas, solicitudes, documentos así como el programa detallado de la investigación observando el estado general del departamento, su organización, área de informática y equipos de cómputo.

La planeación de la auditoria comprendió el plan y alcance del trabajo con una vista al organismo, área de informática y los equipos de cómputo solicitando documentos que sirvan de información y revisarlos(Autor: Muñoz, [2010].).

Descriptiva: Es la etapa del trabajo de investigación científica que permite ordenar los resultados de observaciones, características, factores, procedimientos de variables, fenómenos y hechos.

3.1.3 Técnicas e Instrumentos

Es el método de investigación mediante pruebas para obtener información y comprobación necesaria para emitir opiniones.

Estudio General: Es la revisión general del área para conocer la situación actual del departamento de informática.

Análisis: Es el método por el cual se realizo un estudio y diagnóstico de los problemas existentes y las posibles soluciones.

Observación: Es una técnica de investigación que permitió examinar y tener una visión de los hechos y problemas existentes como opera el sistema y organización actual.

Inspección: Es el examen físico de funciones y revisión de documentos sistemas, equipos y materiales mediante la comprobación.

Confirmación: Es la comprobación de los hechos y operaciones observadas.

Checklist: El Auditor experto emplea listas de chequeo mediante rangos de niveles calificativos y comprobatorios aplicados a la entidad.

Checklist de rango: Contiene preguntas formuladas por el auditor dentro de un rango establecido (ejemplo de 1 a 5 determinado categoría positiva negativa y errónea) con las siguientes calificaciones[46].

1. Correcto.
2. Aceptable.
3. Mejorable.
4. Deficiente.
5. Muy deficiente.

3.1.4 Instrumentos

- Cuestionario
- Guía de entrevista

Encuesta: En base a las necesidades de un Plan de control de Seguridad y evaluación de la Unidad de Sistemas se realizo varias preguntas dirigidas a empleados de la institución Municipal del Cantón Ventanas.

3.2. INTERPRETACIÓN Y DISCUSIÓN DE LOS RESULTADOS

La interpretación de los resultados se basada en la encuestas aplicadas al personal administrativo a la Municipalidad del Cantón Ventanas.

Para la realización de muestra se utilizaron 200 empleados encuestados

Tabla 19. Pregunta a empleados

PREGUNTAS A EMPLEADOS	RESPUESTAS
1. ¿Considera usted que es adecuada la seguridad de activos y recursos en la Unidad de Sistemas de la Municipalidad de Ventanas?	Si ( ) No ( )
Porqué	
2. ¿Admite que el proceso actual de seguridad informática es vulnerable?	Si ( ) No ( )
Porqué	
3. ¿Usted Piensa que con la aplicación de una Auditoria informática se garantizara los controles seguridad de la información?	Si ( ) No ( )
Porqué	

4. ¿Considera usted que con la nueva propuesta se controlara de mejor manera la gestión de información?	Si ( ) No ( )
5. ¿En la actualidad considera que la seguridad de la información en la institución Municipal es eficaz?	Si ( ) No ( )
6. ¿Considera Usted que la aplicación evaluaciones informáticas son de vital importancia para los procesos administrativos?	Si ( ) No ( )
7. ¿Existen mecanismo de emergencias ante posibles desastres naturales para recuperación de la información?	Si ( ) No ( )
Porqué	
8. ¿Se han realizado capacitaciones de seguridad ante amenazas físicas y lógicas en el departamento de Avalúos y catastros del GAD Municipal?	Si ( ) No ( )
Porqué	
9. ¿Opina usted que la falta de Auditoria Informática en el departamento de Informática ofrece muchas desventajas para la administración de información de los ciudadanos de la ciudad de Ventanas?	Si ( ) No ( )
Porqué	
10. ¿Apoya la idea de aplicar controles de acuerdo a los estándares seguridad para mantener la integridad y seguridad de la información de los ciudadanos para evitar el fraude y sabotajes de documentos?	Si ( ) No ( )

Fuente elaborada por: Reinaldo Ramírez

3.2.1 Población

La población es un conglomerado de personas indispensables para obtener los resultados de una muestra estadística en base a investigaciones.

Por lo general esta investigación está conformada por la población de usuarios y empleados de las áreas y departamentos del Gobierno Autónomo Descentralizado de la Municipalidad de Ventanas.
Una muestra estadística nos permitirá calcular el número de empleados Encuestados con la siguiente formula.

$$n = \frac{N * Z^2 * p * q}{e^2 * (N-1) + (Z^2 * p * q)}$$

SIMBOLOGÍA

n=Tamaño de la muestra

N= Tamaño de la Población **(200)** Empleados

e=Error **(0.05)**

p= Probabilidad de éxito **(0.50)**

q= Probabilidad de fracaso **(0.50)**

z=Nivel de confianza para un grado de 95%**(1.96)**

Tabla 19. Nombramientos de empleados del GAD

GOBIERNO MUNICIPAL DEL CANTÓN VENTANAS	
CARGOS	**CANTIDAD**
TITULARES	150
CONTRATADOS	50
TOTAL	200

3.2.2 MUESTRA

$$n = \frac{N * Z^2 * p * q}{e^2 * (N-1) + (Z^2 * p * q)}$$

$$\mathbf{n=} \frac{200 * (1{,}96)^2 * (0{,}50) * (0{,}50)}{(0{,}05)^2 * (200-1) + ((1.96)^2 * (0{,}50) * (0{,}50))}$$

$$\mathbf{n=} \frac{200 * (3{,}8416) * (0{,}50) * (0{,}50)}{(0{,}0025) * (199) + ((3.8416) * (0{,}50) * (0{,}50))}$$

$$\mathbf{n=} \frac{192{,}08}{(4.975) + (0{,}9604)}$$

$$\mathbf{n=} \frac{192{,}08}{5{,}9354}$$

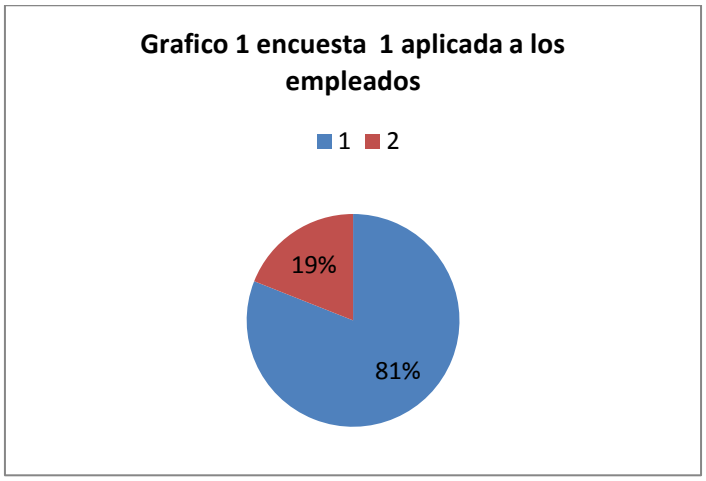
n=32

PREGUNTA # 1

¿Considera usted que es adecuada la seguridad de activos y recursos informáticos en la Unidad de Sistemas?

Tabla. 21 Pregunta 1aplicada a los empleados

Respuesta	Frecuencia	%
SI	**26**	**81 %**
NO	**6**	**19%**
TOTAL	**32**	**100%**



Fuente elaborada por: Reinaldo Ramírez

Análisis # 1

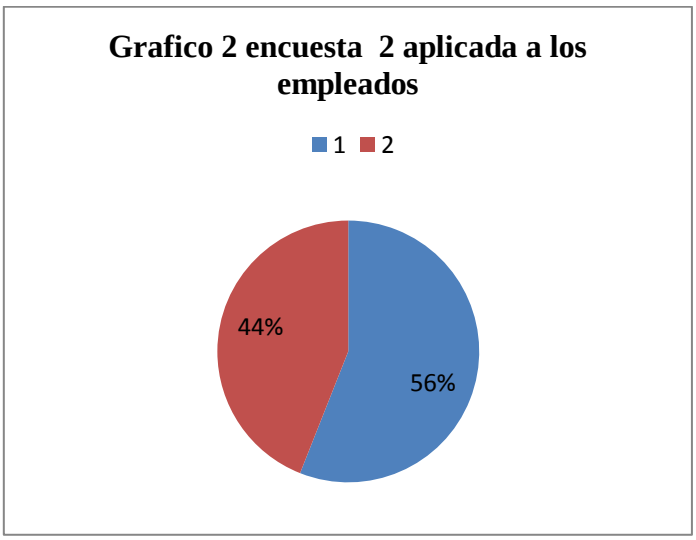
El 81 % de los empleados consideraron que si es de gran importancia la gestión de seguridad de información en la Unidad de Sistemas, mientras que el 19 % de los empleados opinan que no es de gran importancia la seguridad; por tanto se considera que existe un gran número de empleados que están de acuerdo con esta propuesta.

PREGUNTA # 2

¿Admite que el proceso actual de seguridad informática es vulnerable?

Tabla. 22 Pregunta 2 aplicada a los empleados

Respuesta	Frecuencia	%
SI	18	56 %
NO	14	44%
TOTAL	32	100%



Fuente elaborada por: Reinaldo Ramírez

Análisis # 2

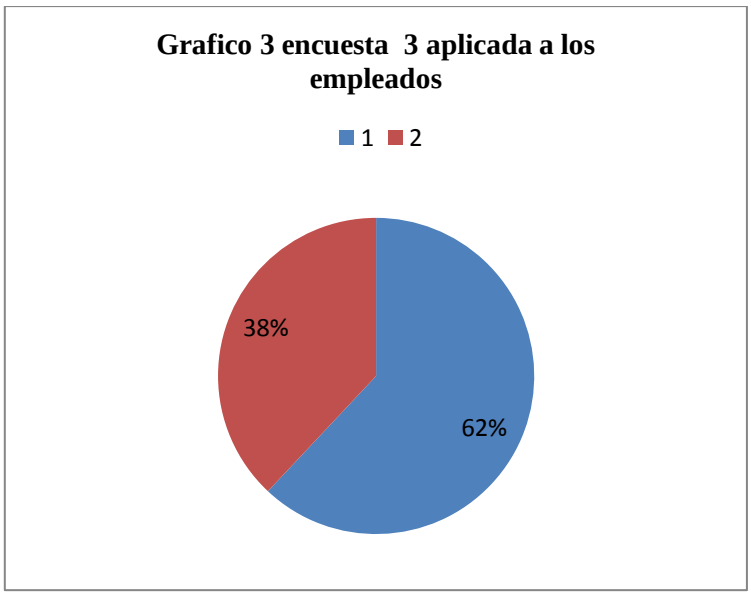
El 56 % de los empleados admitieron que el proceso actual de seguridad es vulnerable sin embargo solo el 44 % reconoce que el proceso de seguridad no vulnerable es por ello que se debe tomar en consideración la opinión de los empleados, y mejorar los procesos de gestión de seguridad.

PREGUNTA # 3

¿Usted Piensa que con la aplicación de una Auditoria informática se garantizara los controles de seguridad de la información?

Tabla. 23 Pregunta 3 a aplicada los empleados

RESPUESTA	Frecuencia	%
SI	20	62 %
NO	12	38%
TOTAL	32	100%



Fuente elaborada por: Reinaldo Ramírez

Análisis # 3

El 62 % de los empleados admitieron que con la aplicación de una Auditoria se garantizara la seguridad de la información, mientras que el 38 % opinan que no.

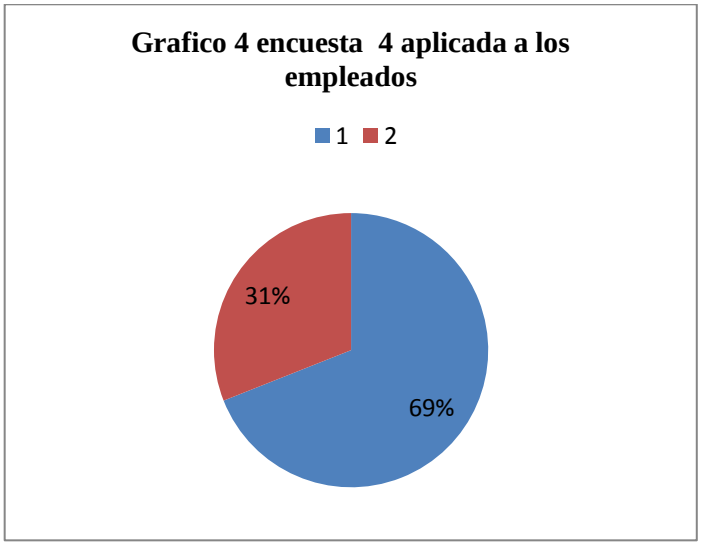
PREGUNTA # 4

¿Considera usted que con la nueva propuesta se controlara de mejor manera la gestión de activos y recursos?

Tabla. 24 Pregunta 4 aplicada a los empleados

Respuesta	Frecuencia	%
SI	22	69 %
NO	10	31%
TOTAL	32	100%

Grafico4encuesta 4 aplicada a los empleados



Fuente elaborada por: Reinaldo Ramírez

Análisis # 4

El 69% de los empleados sí consideraron que con la nueva propuesta se controlara de mejor manera la gestión de información de la ciudadanía, sin embargo el 31% considera que el sistema actual controla mejor su actividad.

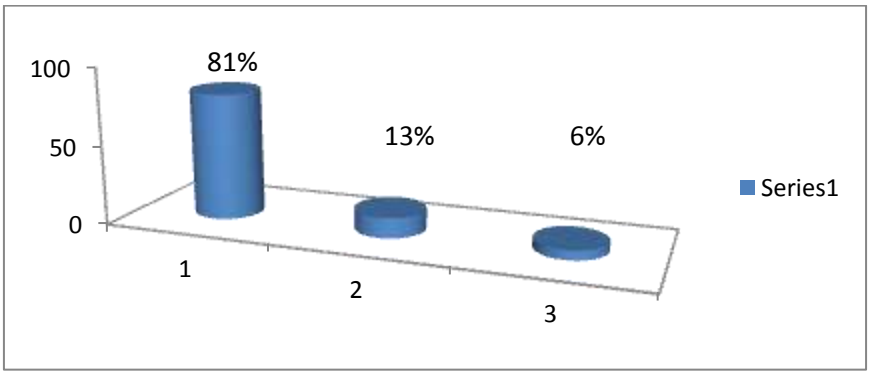
PREGUNTA # 5

¿En la actualidad considera que la seguridad de la información en la institución Municipal es eficaz?

Tabla. 25 Pregunta 5 aplicada a los ciudadanos

Respuesta	Frecuencia	%
Aceptable	**26**	**81%**
Regular	**2**	**13%**
Deficiente	**4**	**6%**
Total	**32**	**100%**

Grafico5encuesta 5 aplicada a los Ciudadanos



Fuente elaborada por: Reinaldo Ramírez

Análisis # 5

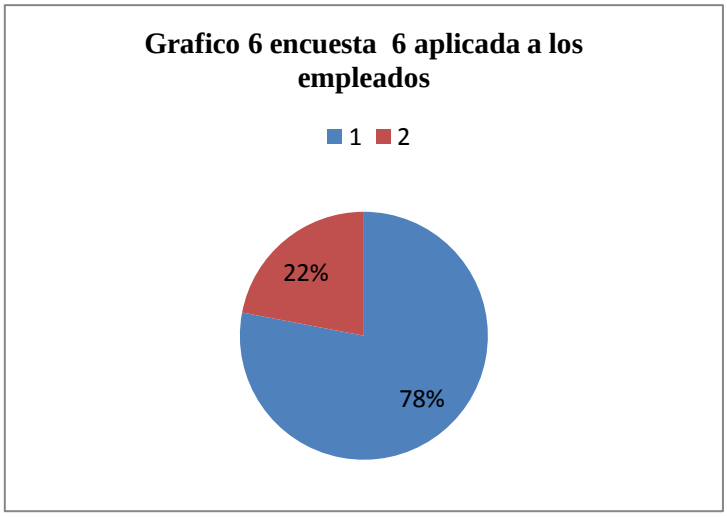
El 81% de los empleados afirmaron que la seguridad de la información en la institución Municipal es aceptable, mientras que el 13 % piensan que la atención es regular y tan solo el 6 % de los ciudadanos consideran que la atención es deficiente.

PREGUNTA # 6

¿Considera Usted que la aplicación supervisiones de áreas y recursos informáticos son de vital importancia para los procesos administrativos?

Tabla.26 Pregunta 6 aplicada a los empleados

RESPUESTA	Frecuencia	%
SI	25	78 %
NO	7	22%
TOTAL	32	100%



Fuente elaborada por: Reinaldo Ramírez

Análisis # 6

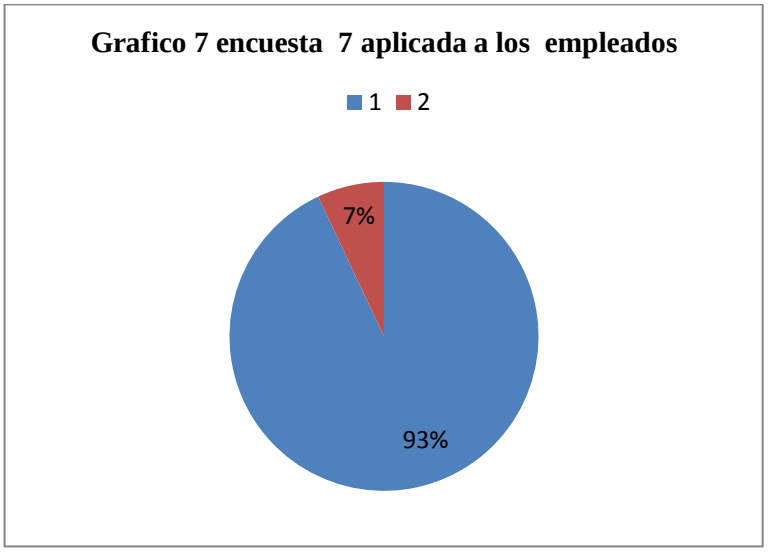
El 78 % de los empleados consideraron que la aplicación supervisiones de seguridad de los sistemas de información si son de vital importancia, para la seguridad sin embargo el 22 % de los empleados opinan que las normas de seguridad no son de vital importancia en la actualidad.

PREGUNTA # 7

¿Existe mecanismo de emergencias ante posibles desastres para recuperación de la información?

Tabla. 27 Pregunta 7 aplicada a los empleados

Respuesta	Frecuencia	%
SI	2	7 %
NO	30	93%
TOTAL	32	100%



Fuente elaborada por: Reinaldo Ramírez

Análisis # 7

El 7 % de los empleados consideraron que si existe mecanismo de emergencia ante desastres para la recuperación de información, sin embargo el 93 % consideran que no se existen mecanismos ante posibles desastres naturales.

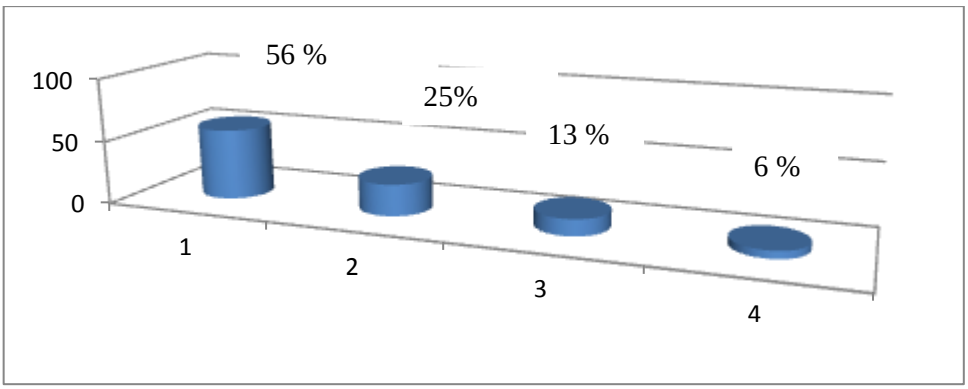
PREGUNTA # 8

¿Se han realizado capacitaciones de seguridad informático en la institución Municipal?

Tabla. 28 Pregunta 8 aplicada a los empleados

Respuesta	Frecuencia	%
Algunas Veces	**18**	**56 %**
Siempre	**8**	**25%**
Casi siempre	**4**	**13 %**
Nunca	**2**	**6 %**
TOTAL	**32**	**100%**

Grafico 8 encuesta 8 aplicada a los empleados



Fuente elaborada por: Reinaldo Ramírez

Análisis # 8

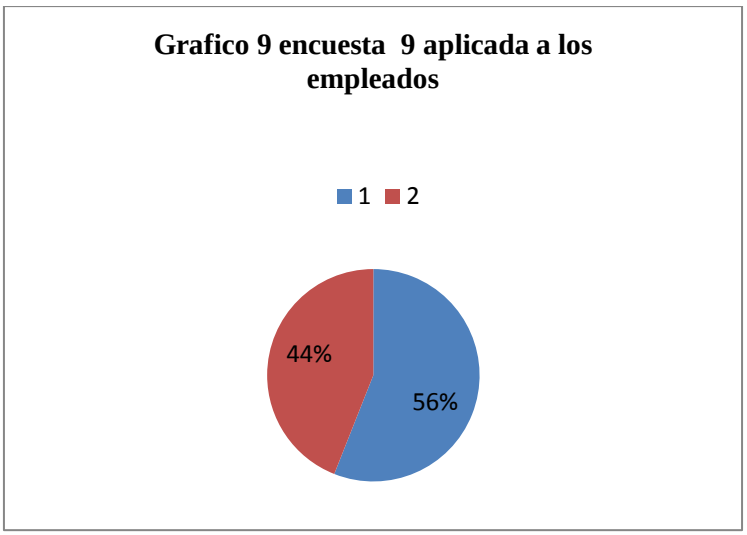
El 25% de los empleados admitieron que alguna vez se han realizados capacitaciones en seguridad mientras el 13% opinan que casi siempre, el 6% algunas veces, y el 56% opinan que no se han realizados capacitaciones.

PREGUNTA # 9

¿Opina usted que la falta de Auditoria Informática muchas desventajas para la administración de Activos y recursos de información?

Tabla. 29 Pregunta 9 aplicada a los empleados

Respuesta	Frecuencia	%
SI	18	56%
NO	14	44%
TOTAL	32	100%



Fuente elaborada por: Reinaldo Ramírez

Análisis # 9

El 56% de los empleados consideraron que la no existencia de una Auditoria Informática en la unidad de sistemas presenta muchas desventajas a los ciudadanos, mientras que el 44% de los empleados consideran que no existen desventajas para los empleados.

PREGUNTA # 10

¿Apoya la idea de aplicar controles seguridad para mantener la integridad y seguridad de la información de los ciudadanos para evitar el fraude y sabotaje de documentos?

Tabla. 30 Pregunta 10 aplicada a los empleados

Respuesta	Frecuencia	%
SI	**30**	**93 %**
NO	**2**	**7%**
TOTAL	**32**	**100%**

Fuente elaborada por: Reinaldo Ramírez

Análisis # 10

El 93% de los empleados si apoyaron a la idea aplicar estándares para mantener la integridad y seguridad de la información de los ciudadanos para evitar el fraude y sabotaje de documento, mientras que el 7% de los empleados no apoyan.

IV. CONCLUSIONES

Como conclusión de la encuesta aplicada a los empleados de la Municipalidad del Cantón Ventanas se basó en la interpretación de los resultados fundamentales que implicaron los conocimientos de la administración de recursos informáticos en las áreas de trabajo basadas en el cumplimiento de normas, políticas y estándares institucionales para fortalecer la gestión de activos de manera segura y confiable.

La auditoría informática ha permitido examinar las principales debilidades y amenazas que presentan los activos informáticos en la unidad de sistemas así como la aplicación de estándares que permitan controlar los procesos de seguridad en base cumpliendo con las normas nacionales de auditoría interna para mejorar la calidad e integridad de la información.

Las normas nacionales de auditoría interna o normas de la contraloría general del estado son medidas de cumplimiento de actividades y administración de los sistemas de información utilizados dentro de la institución Municipal aplicadas según el artículo 410 por la ley orgánica de régimen Municipal.

V. RECOMENDACIONES

- Es importante la implementación de políticas y herramientas de seguridad a cargos de usuarios y empleados dentro de las áreas administrativas y tecnológicas.

- Se recomienda poner en práctica el cumplimiento de normas institucionales, además contribuir al desarrollo de proyectos y herramientas informáticas bien estructuradas mediante los análisis técnicos y administrativos para disminuir las vulnerabilidades y salvaguardar la información ante riesgos que presenta el mundo actual.

- Contratar servicios de auditorías externas para una gestión de calidad y seguridad basadas en controles de las áreas informáticas y exámenes aplicados a las tecnologías de información así como el establecimiento de medidas recomendadas por los auditores externos e internos de las instituciones para asegurar la calidad y seguridad de la información institucional.

- Examinar los recursos informáticos utilizando medidas preventivas y correctivas para reducir los riesgos contratando servicios de seguridad para proteger los ambientes administrativos y los acceso no autorizados que pueden repercutir daños, perdidas económicas en las instituciones.

- Implementar dispositivos y sistemas de seguridad (servicios de vigilancia, alarmas, cámaras de seguridad) considerando todas las medidas preventivas como medidas correctivas mediante servicios de auditoría para evaluar los riesgos que presentan las instituciones en el

ámbito administrativos para gestionar la seguridad de las tecnologías de la información con la implementación de dispositivos de identificación de seguridad (huella digital, firma digital, criptografía).

- Recibir capacitaciones en seguridad informática a través de seminarios y talleres para mejorar los procesos de seguridad de los sistemas de información.

- Los directivos del departamento de sistemas deben participar y coordinar estrategias para hacer más útil la eficacia de seguridad a fin de realizar auditorías de sistemas de información que estén acorde a los estándares internacionales de la calidad y seguridad de la información y comunicación.

- Implementar Data Center externos a la institución para almacenar la información en lugares seguros para recuperar la información en caso de desastres naturales.

- Contratar profesionales capacitados en seguridad informática que provea soluciones de sistema y mantenimiento necesario para las áreas informatices.

- Los administradores de sistemas de información y comunicación deben contar con controles generales de hardware (manual de equipos informáticos) y operativos de software (manual del sistema o de usuario).

- Las claves de los usuarios internos deberán ser actualizadas en un periodo establecido por la institución para evitar pérdidas y espionaje de acceso.

- Desarrollar planes de contingencias ante posibles desastres y amenazas que puedan ocurrir.

VI PROPUESTA DE INTERVENCIÓN

6.1 TÍTULO DE LA PROPUESTA

"Plan de Auditoría para la Unidad de Sistemas en la Municipalidad del Cantón Ventanas".

6.1.1 MARCO DE LA PROPUESTA

6.2.1 METODOLOGÍA DE DESARROLLO UTILIZADA

La metodología utilizada para la elaboración de la Auditoria Informática es de carácter investigativo permitiendo plantear los procedimientos para fundamentar la base del conocimiento para el desarrollo de la auditoria a través de los análisis de las áreas de trabajo utilizado técnicas y herramientas, para conocer las actividades técnicas y administración recursos informáticos.

La metodología (MAGERIT versión 3.0) a permitido realizar el análisis y gestión de Riesgos de amenazas y vulnerabilidad de recursos informáticos en la administración de los servicios Públicos de la institución Municipal promoviendo el uso de mecanismos y herramientas de seguridad informática y reglas técnicas para la administración de sistemas de forma responsable mediante un modelo de normas políticas y estándares para reducir los riesgos que presentan los recursos informáticos considerado las medidas de prevención ante las probabilidades de impactos y perdidas económicas que se presentan ante algún evento de desastres de situaciones actuales de la institución redactadas, estableciendo sugerencias y acciones que deben tomarse empleando medidas preventivas y correctivas de acuerdo alas necesidades de seguridad orientada a la Unidad de Sistemas Informáticos de la del GAD Municipal del Cantón Ventanas para la reducción de riesgos y llevar una correcta administración y protección de recursos técnicos e informáticos mediante soluciones(Miguel Angel Amutio Gómez, 2012)[47].

6.2. OBJETIVOS DE LA PROPUESTA

6.2.1 Objetivo General

Garantizar los controles de seguridad en la Unidad de Sistemas en Gobierno Autónomo Descentralizado Municipal del Cantón Ventanas mediante la elaboración un plan de control de seguridad de los activos y recursos informáticos.

6.2.2 Objetivos Específicos

- Mejorar los niveles de seguridad informática en condiciones vulnerables de la organización en caso de acciones que interfieran las gestiones de la institución.

- Proporcionar las bases para llevar un control de riesgos de vulnerabilidades mediante la protección y salvaguarda de activos ante cualquier interferencia minimizando los costos de inversión.

- Dar a conocer los resultados por medio de informes que contemplen conclusiones y recomendaciones a la institución

6.2.1. ANÁLISIS PREVIO

6.2.1.2 NORMAS DEL AUDITOR

El objetivo del Auditor ha sido identificar y valorar los riesgos de incorrección de materiales detectando las vulnerabilidades que puedan presentar las administraciones informáticas por medio del conocimiento de la entidad en entornos de trabajo mediante controles internos, con la finalidad de proporcionar una base para el diseño y la implementación de respuestas a los riesgos valorados de incorrección.

Responsabilidades y Funciones: la finalidad de la Auditoria informática ha permitido examinar y expresar sugerencias razonables en los diferentes aspectos en situaciones técnicas.

Funciones del auditor: Se ha establecido aspecto importantes para conseguir la máxima eficacia y rentabilidad de los medios informáticos de la entidad auditada presentando recomendaciones y reforzamiento de la unidad informática mediante soluciones según los problemas detectados siempre y cuando no violen los principios de auditoría mediante reportes.

- Recomendar actuaciones Adecuadas para el auditado deben ser coherentes y con bases científicas para incidir en la toma de decisiones.

- Prestar servicios de acuerdo a las posibilidades de la ciencia utilización de medios, condiciones técnicas de acuerdo a la calidad del servicio para recabar información sobre aspectos o incidencias de acuerdo a su capacidad profesional para dictaminar y reforzar la calidad y factibilidad de la auditoria.

- Actuar con cierto grado de humildad evitando presentar información privilegiada sobre nuevas tecnologías y métodos.

- Mantener el grado de confianza con el auditado en base a su actividad sin alarde científico[48].

6.2.1.3 NORMAS DE LA PRESENTACIÓN DE INFORMES

- Es el resultado del informe final se lo realiza mediante el conocimiento para el dictamen.
- Realizar un informe por escrito y firmado al finalizar la evaluación de las auditorías realizadas.
- Los informes deberán ser claros y precisos con el propósito de lograr los alcances y resultados de la auditoria mediante la opinión del auditor.
- Los reportes deberán incluir conclusiones y recomendaciones[49].

6.2.1.4 PLAN DE CONTROL DE SEGURIDAD EN LA UNIDAD DE SISTEMAS

La finalidad del plan de control es verificar el cumplimiento de normas, políticas y estándares para fortalecer la seguridad ante acciones de posibles amenazas de los recursos y activos a salvaguardar considerados vulnerables ante interferencia y de posibles catástrofes a través de evaluaciones de manera secuencial llevadas a cabo estableciendo acciones de controles seguros.

El plan de control de seguridad requiere de una planificación adecuada revisión de cumplimiento de normas políticas y estándares para ejecutar las evaluaciones y posteriormente monitorear las actividades tomando controles y acciones preventivas y correctivas que permite proteger la administración de recursos informáticos en base a el conjunto de requerimientos y procedimientos de gestiones de la institución de manera segura ante interferencias imprevistas de los sistemas de información y recursos informáticos.

El control de seguridad tiene como objetivo servir de guía para utilización de herramientas y mecanismo de protección orientada a las administraciones informáticas así como la minimización de amenazas que generan consecuencias ante incidentes y posibles catástrofes naturales aun determinado plazo y aun costo aceptable.

En actualidad la seguridad de la información dentro de una organización no basta con el uso de normas y políticas internas para proteger los activos se requiere una serie de actividades, herramientas y recursos humanos para reducir amenazas que van evolucionado junto con las tecnologías de hacer concienciación de responsabilidades, así como supervisiones periódicas por las unidades de auditoria interna para la implementación de sistemas de seguridad relacionados con los estándares para certificar que el cumplimiento de controles de seguridad de manera responsable en un tiempo y plazo estimado.

6.2.1.5 CONTROLES GENERALES

Servir de información general para los controles informáticos de acuerdo a los requerimientos necesarios para reducir los riesgos de amenazas y vulnerabilidades en la administración de tecnologías informáticas en la institución Municipal.

6.2.1.6 CONTROLES ESPECÍFICOS

- Establecer planificaciones para controlar los riesgos, amenazas y vulnerabilidades detectadas.
- Establecer el monitoreo y revisión de riesgos
- Establecer acciones preventivas y correctivas

6.2.1.7 DESCRIPCIÓN DE COMPONENTES DEL PLAN

Un plan de control de seguridad es un conjunto de medidas y requerimientos de controles para las organizaciones a través de actividades informáticos a cargo de los usuarios sobre la protección de activos y recursos informáticos vulnerables para reducir el impacto de los costos y perdidas materiales caso de desastres.

- Controles de Riesgos Administrativos
- Controles de Operativos de Amenazas
- Controles de Técnicos de Vulnerabilidades

6.2.1.8 ANÁLISIS DE FODA EN LA UNIDAD DE SISTEMAS

El proyecto de investigación está enfocado al estudio de fortalezas y debilidades del departamento de informatica vinculado con la administración de Sistemas de información del Gobierno Municipal del Catón Ventanas

En el estudio de FODA de la unidad de sistemas se ha elaborado contemplada la necesidad de la institución de acuerdo a los siguientes puntos.

Fortalezas

- Los equipos de trabajo de la unidad de sistemas tienen una buena coordinación por parte de los recursos informáticos.

- Se ajustaran a los procesos informáticos de acuerdo a las funciones y atribuciones asignadas dentro de la institución.

Oportunidades

- La unidad de sistemas facilita la participación de proyectos de mejoramiento y gestión propuestos por la institución.
- Tener acceso a informaciones públicas precedidas por la institución.
- Estudiar las actividades de uso de tecnologías informáticas de hardware y software

Debilidades

- Capacitación en el uso de tecnologías
- Comunicación
- Seguridad

Con la accesoria de los comités directivos para la administración de seguridad de las tecnologías de la información.

Amenazas Naturales

- Terremoto
- incendios
- Inundación
- Tsunami

Amenazas Humanas

- Incidentes
- Acciones
- Errores

Amenazas Maliciosos

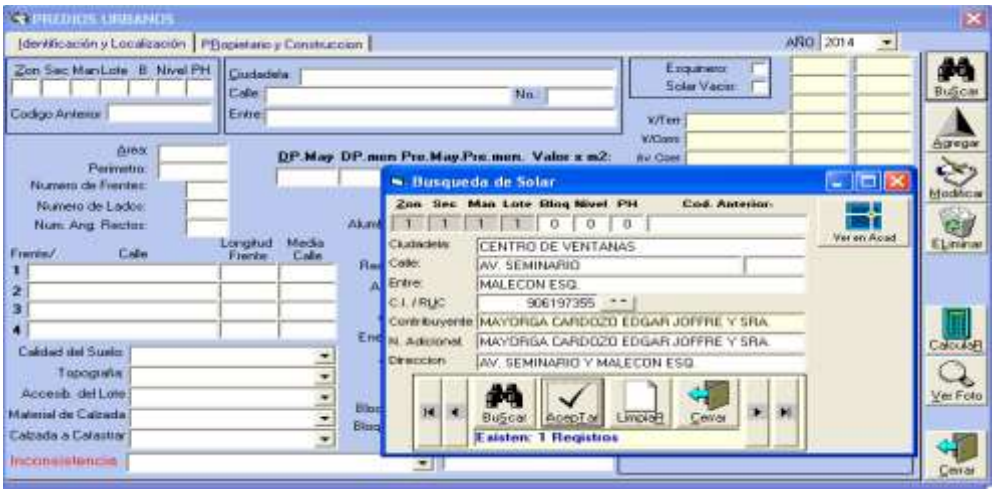
- Robo
- Sabotaje
- Virus

Amenazas seguridad

- Herramientas
- Dispositivos
- Sistemas de seguridad

6.2.1.9 IMAGEN DE SISTEMA DE INFORMACIÓN

Figura 9. Sistema de Control Municipal



Fuente: Municipio de ventanas

6.2.2. SERVIDOR INFORMÁTICO

Los servidores son ordenadores que realizan actividades asignadas por los usuarios para distribuir información a otras áreas de negocio de manera compartida, en otras palabras los servidores son computadores matrices conectados a otros computadores a través de la red encargados de asignar y distribuir información de manera cliente servidor es decir los servidores facilitan la comunicación y trasportes de información desde un computador matriz a otros equipos de usuario para proveer de información de manera rápida[50].

Figura10. Servidor informático

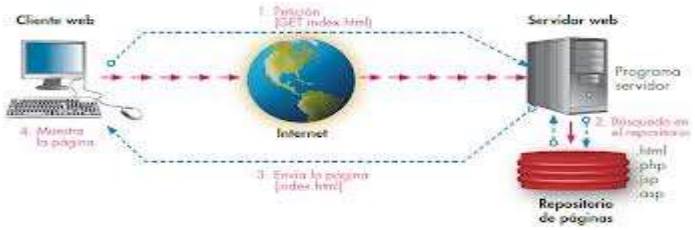
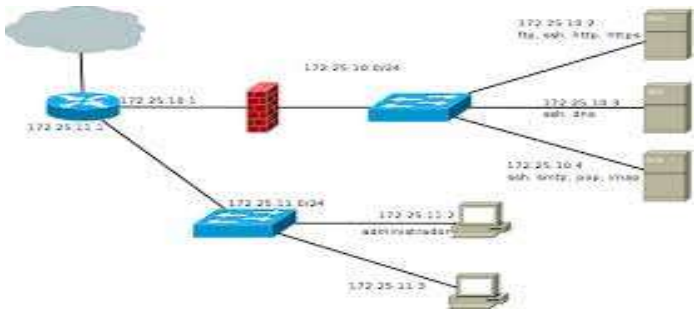


Figura 11. Diagrama de firewall

6.2.2.1 Funciones de un Firewall



El firewall es considerado un escudo protector que impide los accesos no autorizados de las redes locales a través de la web con las características para detectar agentes maliciosos que puedan vulnerar las comunicaciones de redes privadas de las empresas[51].

6.2.2.2 SERVIDOR DE ARCHIVO

Los servidores de archivo básicamente se caracterizan por almacenar todo tipo de archivos que son distribuidos a otros clientes para los accesos a archivos a través de los ordenadores, es decir un servidor está almacenado en una máquina permite compartir archivos con otras computadores locales para proveer información a otros usuarios en las instituciones.

Los servidores de archivos proporcionan protocolos utilizados dentro de los servidores tales como:

- FTP (Multiplataforma)
- SMB (Windows)
- NFS (Unix)

6.2.2.3 DIAGRAMA DE SERVIDOR DE ARCHIVOS

A continuación se muestra en el gráfico de representación de las funcionalidades y de utilización de un servidor de archivo.

Equipos de Administración conectados a un mismo servidor

Figura 12. Servidor de archivos

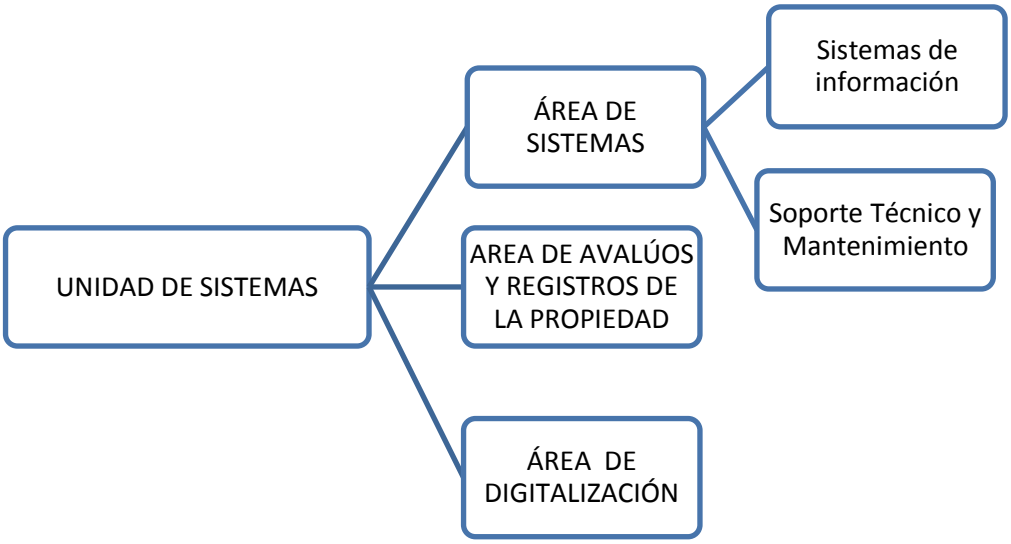
Un servidor permite proveer información a otros computadores en forma simultánea, en el departamento de avalúos y catastros los servidores proveen información a otros equipos de cómputo del area de cobro de impuestos para compartir información de los usuarios[52].

6.2.2.4 DEPARTAMENTO DE SISTEMAS EN LA INSTITUCIÓN

El área de sistemas está conformada por el conjunto de programas sistemas y componentes de hardware (servidores de base de datos)

Software (sistemas operativos, documentos de office, Word, Excel, Base Datos y materiales administrativos) servicios de mantenimiento preventivo y correctivo de recursos informáticos de la unidad de avalúos y catastros de GAD Municipal ventanas.

Figura 13 Unidad de Sistemas



Fuente elaborada por: Reinaldo Ramírez

6.2.2.5 UNIDAD DE SISTEMAS INFORMÁTICOS

Esta unidad esta destinada a mantener el funcionamiento óptimo de la infraestructura tecnológica institucional, haciendo eficientes la seguridad de tareas de procesamiento de datos y de información con las siguientes especificaciones[53].

Tabla 31. Atribuciones y Responsabilidades

ÁREAS	Atribuciones y Responsabilidades
Area de Hardware	Presentar informes mensuales de evaluación técnica y operativa de las áreas informáticas
	Poner en práctica las normas de Seguridad de la Información (ISO 27001)
	Establecer procedimientos técnicos basados en metodologías sobre la seguridad de sistemas informáticos.
	Desarrollar políticas de gestión tecnológica.
	Presentar informes de implementaciones y administraciones y mantenimiento de aplicaciones y sistemas informáticos.
	Establecer especificaciones técnicas para la compra de equipos.
	Desarrollar proyectos Informáticos

Area de Software	adquisición de software.
	Presentar informes de identificación de usuario y contraseña.
	Presentar informes de cumplimiento de procesos.
	Presentar informes de revisiones de software.
	Presentar informes de instalación de antivirus.
	Realizar mantenimientos preventivos y correctivos de hardware y software.
	Realizar soportes técnicos de manera presencial y telefónica de información del Gobierno Municipal.
	Presentar informes de administración de activos informáticos
	Presentar reportes de actualización de antivirus.
	Presentar informes del desarrollo y ejecución de proyectos de infraestructura tecnológica servidores y redes de comunicación.
	Presentar informes de la administración y acceso a sitios web e internet.

Elaborado por: Reinaldo Ramírez

6.3. JUSTIFICACIÓN

- Salvaguardar el activo Municipal para mantener la integridad de los datos, de acuerdo a los objetivos establecidos, controlando la seguridad de manera eficiente protegiendo los recursos informáticos.

- Disminuir los inconvenientes causados por falta de controles generales y operativos de sistemas y equipos al adquirir alguna información.

- Mantener los niveles de seguridad de la información, para que sea accesible solo al personal autorizado.

- Mantener los niveles de confianza de protección de activos y recursos a utilizados usuarios y empleados de la institución

6.3.1 EQUIPO DIRECTIVO DEL ÁREA DE SISTEMAS

La función principal de la área directiva será minimizar los posibles riesgos de la información mediante supervisiones periódicas para detectar vulnerabilidades de la información y administración, el comité informático será los encargado de la toma de decisiones ante posibles acciones e incidentes vinculados a la dirección manteniendo informados a todos los miembros y empleados del área administrativa con las tareas principales.

- Estudio de la situación actual.
- Decisiones de poner en marcha los controles de seguridad.
- Realizar procesos de supervisiones de actividades administrativas y manejo de recursos informáticos.
- Monitoreo de cumplimientos de normas y políticas internas.

6.3.2 EQUIPOS DE SISTEMAS, CONTROL, SOPORTE DE SEGURIDAD

El equipo de sistemas tomara la responsabilidad del control de la infraestructura tecnológica necesaria para el soporte y seguridad de los recursos informáticos relacionados con la administración de sistemas de información.

El trabajo de los equipos incluye componentes de computadores herramientas y dispositivos de seguridad para el monitoreo y recuperación de las actividades de soporte de servicios de administración y comunicación.

Este equipo es responsable de todo lo relacionado con asistencia técnica con acciones preventivas y correctivas con las siguientes actividades.

- Mantenimiento de equipos de cómputo
- Soporte de hardware y software.

6.3.3 IDENTIFICACIÓN DE LOS RECURSOS HUMANOS

La identificación del talento humano encargado de administrar las áreas informáticas de acuerdo a las funciones y atribuciones de responsabilidades para responder ante los riegos amenazas y vulnerabilidades que presente los recursos informáticos.

Tabla. 32 Equipo Administrativo

PROBLEMA:	**SEGURIDAD FISICA**		
PRODUCTO:	**RECURSOS HUMANOS**	PDCA No.:	**1**
No. DE PARTE	**1**	FECHA APERTURA	**03/O3/2014**
CLIENTE:	**UNIDAD DE SISTEMAS**	FECHA CIERRE	**05/11/2014**

EQUIPO DE RESOLUCIÓN DE PROBLEMA

Nombre	Puesto	Departamento
Ing. Cesar Vara	Jefe de la Unidad	Unidad de sistemas
Sr. Israel Conforme	Soporte Técnico	Área de Mantenimiento

Elaborado: por Reinaldo Ramírez

Tabla. 33 Interrogación

PDCA PASO 1: PLANEAR
(FORMULACIÓN DEL PROBLEMA) (¿QUÉ?)

PDCA No.	03/O3/2014	FECHA	05/11/2014

¿Qué es lo que se ha encontrado (esquema eventual)?
Falta de controles de seguridad
¿Quién lo ha detectado? :
Auditor externo
¿Dónde se ha encontrado? :
Área de sistemas
¿Cuándo se presentó (referencia, turno,…)? :
¿Cómo se ha detectado? :
Mediante una investigación preliminar
¿Cuántas veces se ha encontrado (por día, por semana, por mes,…)? :
1
¿Por qué se ha constatado (Pb ya se había encontrado,…)? :
entrevista al director de la unidad de sistemas
¿Cuál es el objetivo que se quiere alcanzar y cuándo (plazo)?
Certificar a la institución

Elaborado Por Reinaldo Ramírez

6.3.4 FASE DE PLANEAMIENTO

En la fase de planificación se definirá los mecanismos para reaccionar ante incidentes que se den por acciones que ocasionen disturbios, daños y pérdidas de recursos de cualquier área vulnerable.

La fase de planificación es la etapa previa a la revision de seguridad de la unidad de sistemas es importante señalar la coordinación y aplicación de normas, herramientas y políticas que son parte de los controles de seguridad.

Tabla 34. Planeamiento

	PDCA PASO 1: PLANEAR (CAUSAS POTENCIALES) (¿POR QUÉ?)		**Producto : Unidad de Sistemas** **Fecha :** 03/03/2014 **PDCA No.**:	
Problema : Controles de seguridad				
1st WHY?	**2nd WHY?**	**3rd WHY?**	**4th WHY?**	**5th WHY?**
Accesos físicos y lógicos	Normas internas	Políticas	Estándares	Contingencia
Autentificaciones	Comité de seguridad	Instructivos de Operación	Soporte de Seguridad	Medidas de Emergencia
Restricciones	Monitoreo	Reglamentos	Sistemas y equipos	Materiales de emergencia
Vigilancia		Restricciones	Certificación	Respaldo

6.3.5 FASE DE REVISIÓN

La fase de revisión es la etapa previa a la comprobación de seguridad de los sistemas es importante señalar la coordinación y aplicación de los diferentes normas, herramientas y políticas que son parte de los controles de seguridad decisión del equipo director de ejecutar el Plan debido al alcance de los daño

PDCA PASO 3: VERIFICAR
TABLA 35. ACCIONES DE CONTROL

PDCA No. :	**NORMAS Y ESTANDARES**	FECHA:	**03/03/ 2014**

	Turno	**RIESGOS**	total	Observaciones	Responsable de la inspección:	Fecha:
1a Revisión	1o	Comité de seguridad	0	Sistemas de seguridad	Auditor Externo	03/03/ 2014
	2o		0	Instructivos de operación		
	3o	Estándares de seguridad	1	Dispositivo de seguridad		
	Todas las acciones propuestas han sido terminadas			SI ✓ / NO		
	Si es no explicar:					

POLITICAS

	Turno	**AMENAZAS**	total	Observaciones	Responsable de la inspección:	Fecha:
2da Revisión	1o	Accesos lógicos	0	Autentificación y cifrado	Auditor Externo	03/03/2014
	2o	Accesos Físicos	0	Dispositivos de Vigilancia		
	3o		0			

	Todas las acciones propuestas han sido terminadas	SI	✓
		NO	
Si es no explicar:			

POLITICAS

3a Revisión	Turno	VULNERABILIDADES	total	Observaciones	Responsable de la inspección:	Fecha:
	1o	Capacitación	1	Mecanismos de emergencia	Auditor Externo	03/03/2014
	2o	Contingencias	0	Mecanismos de respaldo		
	3o		1			

	Todas las acciones propuestas han sido terminadas	SI	✓
		NO	
Si es no explicar:			

	Las medidas propuestas han sido comprobadas exitosamente	Si	✓
		No	
Si es no explicar			

Área / Puesto	Nombre	Firma	Fecha
Director de Sistemas	Ing. Cesar Vara		05/08/2014
Asistente Técnico	Sr. Israel Conforme		05/08/2014
Administrador de Sistemas	Ing. Cesar Vara		05/08/2014

6.3.6 FASE DE VERIFICACIÓN

La fase de verificación es la etapa previa para evidenciar los controles existentes mediante indicadores de niveles de riesgos.

Tabla 36. Verificación

PDCA PASO 3: VERIFICAR (VALIDACIÓN)																				
Indicador:		1																		
			2																	
				3																
Fecha					4															
						5														
NIVEL DE ACCIÓN																				
1	Correcto	1. 0																		
2	Aceptable		2.0																	
3	Mejorable			3.0																
4	Deficiente				4.0															
5	Muy de eficiente					5.0														

Elaborado Por Reinaldo Ramírez

Tabla 37. Validación

PDCA PASO 3: VERIFICAR DATOS (VALIDACIÓN)						
Tracking Chart Hoja 1	Auditor		Auditor		Auditor	
Día	Externo	Día	Externo	Día	Externo	Día
25 -Enero	1	12 -Abril	1	19 -julio	1	23-Octubre
15 -Febrero	1	20-mayo	1	25 Agosto	1	28 Nov.
07-Marzo	1	01-junio	1	16 -Sept	1	10 -Dic
Tiempo						1 Año

Elaborado Por Reinaldo Ramírez

6.3.7. FACTIBILIDAD DE LA PROPUESTA

6.3.8 Factibilidad Administrativa

El Plan podrá ser manejado por el personal administrativo e informático como guía para el control de seguridad de los procesos administrativos así como la utilización, mantenimiento y control de los recursos informáticos ante posibles amenazas y contingencias de desastres naturales que puedan ocurrir dentro de la institución.

6.3.9 Factibilidad Operativa

Comprende la supervisión, recepción y distribución de documentos en forma manual y electrónica del área informática en base a las medidas de seguridad y responsabilidad de los archivos y documentos que son utilizados en las áreas informáticas.

6.4. Factibilidad Técnica

La factibilidad técnica está basada en los análisis de los recursos informáticos utilizados en la unidad de sistemas para obtener información de los servicios y operaciones técnicas que tiene la institución con el mejoramiento e implementación de nuevas tecnologías de acuerdo a los estándares de calidad y seguridad de la información.

6.4.1 Factibilidad Económica

El desarrollo del Plan de control es económico de acuerdo a los beneficios establecidos será financiado por la entidad Municipal, el Plan de auditoria mantiene un costo razonable de materiales sirve guía para los controles de seguridad aplicado a la institución y empresas que administren los sistemas tecnológicos e informáticos con niveles de seguridad para prestar servicios de salvaguarda los activos y recursos informáticos garantizando el manejo eficaz de seguridad de la información y administración de sistemas información dentro de las organizaciones.

6.4.2 FASE DE EJECUCION (DO) HACER

Una vez analizados los recursos en áreas vulnerables se pondrá en marcha el monitoreo de actividades planteando estrategias de reacciones para salvaguardar las áreas informáticas.

Mediante el seguimiento de actividades de recursos humanos, materiales e informáticos.

- Vigilancia recursos informáticos
- Vigilancia de agentes internos
- Vigilancia de agentes externos

6.4.3 CONTROL DE RIESGOS ADMINISTRATIVOS

Los riesgos en la unidad de sistemas en la institución se controlaran mediante acciones para el uso de manuales operativos para administrar los sistemas por parte de los usuarios, la autentificación de claves de acceso de los usuarios para los usos de claves personalizadas las restricciones y refrendaciones de claves e informaciones confidenciales para la administración de seguridad confidencial, el uso de dispositivos de vigilancia para la seguridad física de los equipos informáticos la utilización de mecanismos criptográficos para la administración las claves de accesos a los sistemas y las medidas de respaldos para la recuperación de información en casos de emergencias.

6.4.4 CONTROL OPERACIONAL DE AMENAZAS

Las amenazas en la unidad de sistemas en la institución Municipal se controlaran mediante medidas para evitar incidentes técnicos, errores del personal durante labores de trabajo, las supervisiones informáticas permiten evidenciar las instalaciones de cableado para evitar fallas eléctricas, soporte de mantenimiento preventivo para establecer reparos la administración de claves de acceso de los usuarios autorizados para administrar los sistemas y recursos informáticos, la actualización de antivirus para evitar amenazas y filtración de virus y la integración de sistemas para establecer la comunicación estableciendo acciones de emergencias de respaldos de programas y sistemas ante posibles desastres de incendios inundaciones y terremotos.

6.4.5 CONTROLES TÉCNICOS DE VULNERABILIDADES

Las vulnerabilidades en la unidad de sistemas en la institución Municipal se controlan mediante acciones para supervisar las labores de trabajo realizadas por el personal informático para evitar actos de corrupción y cumplimiento de responsabilidades de recursos y actividades en las áreas informáticas la vigilancia entrada y salida del personal externo para evitar el espionaje y accesos no autorizados monitorear las interferencias de códigos maliciosos y actualizaciones de antivirus establecer restricciones a áreas y quipos restricciones de prevención para evitar el ingresos de bebidas y materiales tóxicos las sanciones para evitar sabotaje de la información de manera óptima confidencial integra y disponibles para las actividades informáticas y uso por parte de los usuarios.

Tabla 38. Verificación de Riesgos Administrativos

Verificación de Riesgos Administrativos	Normas Políticas y Estándares			
	Controles	Implantado	Por implantar	No existe
Unidad de Sistema				
Normas de control interno		I		
Políticas de seguridad			P	
Estándares de Seguridad			P	
Contingencias			P	
Instructivos de Operación			P	
Autentificaciones de claves		I		
Inventarios de Activos		I		
Seguridad de información Confidencial			P	
Administración de quipos informáticos			P	
Administración de Sistemas de información			P	
Procedimientos de respaldos		I		
Accesos Fiscos a los equipos		I		
acceso lógicos los sistemas		I		
Acciones preventivas				N
Medidas de seguridad			P	

Elaborado Por Reinaldo Ramírez

Tabla 39. Verificación de Riesgos Operativos

Verificación de Riesgos Operativos	Normas Políticas y Estándares			
	Controles	Implantado	Por implantar	No existe
Unidad de Sistema				
Capacitación informática				N
Monitoreo y vigilancia			P	
Accesos a Sitios web y Redes Sociales				N
Infraestructura Tecnológica		I		
Actos de corrupción				N
Acciones de Personal interno y externo				N
Actualizaciones de Antivirus		I		
Consumo de bebidas ingreso de materiales tóxicos			P	
Confidencialidad Integridad , Disponibilidad de la información			P	
Restricciones a personal no autorizado		I		
Soporte técnico		I		
Actualizaciones de Seguridad lógica			P	
Herramientas de seguridad física		I		

Elaborado Por Reinaldo Ramírez

Tabla 40. Verificación de Riesgos Técnicos

Verificación de Riesgos Técnicos	Normas Políticas y Estándares			
	Controles	Implantado	Por implantar	No existe
Unidad de Sistema				
Proyectos Tecnológicos			P	
Tecnología de Información			P	
Contingencias			P	
Instalaciones eléctricas		I		
Soporte tecnico de hardware			P	
Soporte tecnico de software		I		
Personal interno y externo				N
Actualización de antivirus		I		
Integración de redes de comunicación				N
Extintores Incendios		I		
Fugas de agua				N
Administración de sistemas y aplicaciones				N
Materiales de emergencia		I		
Respaldos programas e información				N

Elaborado Por Reinaldo Ramírez

6.4.6 FASE DE MONITOREO

Una vez señalado las revisiones se procederá a comenzar los controles de seguridad con la aplicación de dispositivos y herramientas en lugares vulnerables, estas medidas se basan en los mayores esfuerzos de seguridad aun determinado plazo por la institución.

Los mecanismos se pueden dividir en dos partes

- Acciones preventivas
- Acciones correctivas

Estos mecanismos se refieren a los incidentes que se dan para proteger las áreas vulnerables. Una vez custodiados los departamentos de recursos informáticos se confirma la función de los controles sobre las tecnologías de información, los mismos que serán protegidos para mantener el control de seguridad de los sistemas archivos y registros de la unidad de sistemas los que serán encargados de controlar la seguridad de las áreas informáticas.

6.4.7 ACCIONES PREVENTIVAS

Las medidas preventivas del plan de control de seguridad se caracterizan por controlar las causas que provoquen conductas indeseables minimizando las probabilidades de que se producen en la realidad actual.

- Labores de trabajo: operación de actividades e interferencias indeseadas.
- Excluyendo los riesgos que puedan ocurrir
- Incumplimiento: de reglas y requisitos institucionales
- Escenarios: circunstancias de factores ambientales

Escenarios: las correcciones deben ser definidas y explicadas de manera que no afecten a la seguridad es decir realizar pruebas para la a aplicación de medidas correctivas sobre la protección y administración de sistemas de información.

TABLA 41. MONITOREO DE SISTEMAS DE INFORMACIÓN

CONTROL DE RIESGOS	NORMA ISO/IEC 27001				AMENAZAS	VULNERABILIDAD	POSIBLE VULNERAVILIDAD.	VALOR ACTIVO	POSIBLE PRESENCIA	TOTAL
	CONFIDENCIAL	INTEGRIDAD	DISPONIBILIDAD	TOTAL						
INFORMACION DE LOS USUARIOS	3	3	3	3	ERROR DE REGISTROS	ACTUALIZACIÓN DE DATOS	3	3	3	3
					CAMBIOS	MODIFICACIÓN DE DATOS	3			
					ERRORES	ELIMINACIÓN DE DATOS	3			
					FALSIFICACIÓN	CONTENIDO DE DATOS	3			
					PRIVACIDAD	USO INDEBIDO INFOR.	3			
					VIRUS	ACCESO	3			
					ESPIONAJE	AGENTES EXTERNOS	3			
					SUPLANTACIÓN DE IDENTIDAD	PERDIDA DE DATOS	3			
					RESPALDO	COPIAS DE INFORMACIÓN	2	2	2	2
ACCESO A LA INFORMACIÓN	2	2	2	2	VIRUS	CONTROL DE ACCESO	2			
					ERROR DE USUARIO	FALTA DE CAPACITACIÓN	2			
					POCA SEGURIDAD	FALTA DE POLÍTICAS	2			
REGISTROS DE USUARIOS	2	2	2	2	VIRUS	ACCESOS	2	2	2	2
					ERROR DE USUARIO	CAPACITACIÓN	2			
					POCA SEGURIDAD	POLÍTICAS	2			
INTEGRACION Y COMUNICACIÓN	4	4	4	4	FALLAS EN LA RED	DEFICIENCIA ORGANIZACIÓN	4	4	4	4
					ERROR DE APLICACIÓN	INTEGRACIÓN DE REDES	4			
					ERROR DE CONEXIÓN	SERVIDOR SIN CONEXIÓN	4			
					ERROR DE USUARIO	FALTA CAPACITACIÓN	4			
					CÓDIGO MALICIOSO	INTERFERENCIAS	4			
CUENTAS DE USUARIOS	4	4	4	4	ACTUALIZACIÓN	MODIFICACIÓN DE CLAVES	3	3	3	3
					PLAGIO	JQQUEO DE CÓDIGOS	3			
					AUTENTIFICACION	CIFRADO DE CLAVE	3			

6.4.8 ACCIONES CORRECTIVAS DEL PLAN DE CONTROL

Las medidas correctivas del plan de control tienen los siguientes aspectos

Aceptabilidad: La aceptación de mecanismos de seguridad por las organizaciones debido a los altos costos e inversiones en supervisiones, disposición de tiempo para cubrir los riesgos de seguridad en situaciones actuales.

Integración: la adaptabilidad de desarrollo e implementación de mecanismos que no afecten a las organizaciones en los ámbitos de seguridad si un programa se integra a los sistemas que no afecten a la seguridad.

Puede resultar difícil realizar una corrección completa del plan de control de seguridad en base los probabilidades de amenazas que van evolucionando e impactos debido a los altos costos lo que es fundamental una corrección organizada para acreditar que todos los procedimientos y actividades de los usuarios se hayan capacitado e informado en un periodo de tiempo.

Por las propias necesidades de la institución se establecerán nuevos mecanismos, herramientas y estándares a las áreas tecnológicas para los sistemas de información que se van innovando de acuerdo a la propuesta realizada.

Una adecuada planificación de corrección del plan de control de seguridad ahorra tiempo y protegerá la administración de recursos en casos de emergencias de incidentes, como solución a las inseguridades de las organizaciones.

Por las formas de organización de seguridad de los procesos de registros se van adoptando nuevas herramientas y estándares como mecanismos de solución para la protección de recursos tecnológicos que se van innovando de acuerdo a las necesidades de seguridad de las organizaciones.

6.5. ACTIVIDADES CORRECTIVAS DEL PLAN

Tabla 42. Control de Riesgos Administrativos

Controles de riesgos administrativos	Acciones correctivas de controles Sugerencias
Unidad de Sistemas	
Comité Auditoria	Verificar el cumplimiento Normas internas
Unidad de sistemas	Implantar Políticas de seguridad
Comité de Seguridad	Establecer Estándares de Seguridad
Recursos tecnológicos	Establecer Instructivos de Operación
Inventarios	Mantener inventarios de hardware y software
Claves de Accesos	Establecer Autentificaciones
Información Manual y Digital	Establecer Restricciones y Cifrado de Información
Equipos informáticos	Establecer Dispositivos de vigilancia(cámaras)
Sistemas de Información	Establecer Cifrado de claves(huellas y firmas)
Contingencias	Establecer Procedimientos de respaldos

Elaborado Por Reinaldo Ramírez

Tabla 43. Control Operacional de Amenazas

Controles Operativos de Amenazas	**Acciones correctivas de controles**
	Sugerencias
Unidad de Sistemas	
Proyectos Tecnológicos	Desarrollar proyectos informáticos innovadores
Tecnología de Información	Establecer Mecanismos y herramientas de seguridad
Contingencias	Establecer Planes de contingencias
Comunicación local	Establecer Redes Locales
Fallas eléctricas	Establecer Instalaciones de cableado y energía
Fallas en hardware	Establecer Mantenimientos Preventivos
Fallas en software	Realizar Mantenimientos correctivos
Agentes internos	Aplicar Restricciones y accesos Autorizados
Agentes Externos	Controlar los Accesos no Autorizados
Filtración de virus	Mantener Instalaciones de antivirus
Fallas de integración	Establecer comunicación redes
Incendios	Utilizar Extintores
Inundaciones	Controlar las Fugas de agua
Terremotos	Establecer Infraestructuras antisísmicas

Elaborado Por Reinaldo Ramírez

Tabla 44. Control Técnicos de Vulnerabilidades

Controles Técnicos de Vulnerabilidades	**Acciones correctivas de controles** **Sugerencias**
Unidad de Sistemas	
Administración de seguridad	Establecer capacitaciones en medidas de seguridad
Monitoreo y Evaluación	Implantar la salvaguardar la integridad de activos y recursos
Accesos a Sitios web y Redes Sociales	Restringir el accesos a de redes sociales en horas laborables
Infraestructura Tecnológica	establecer mecanismos y herramientas (SGSI, Criptografía, autentificación e identificación de claves)
Accesos físicos y lógicos	Establecer Restricciones de accesos
Equipos de computo	Soporte técnico(mantenimiento preventivo y correctivo)
Firewall	Actualizaciones de Seguridad
Software	Implantar Herramientas de seguridad lógica

Elaborado Por Reinaldo Ramírez

6.6. EVALUACIÓN DE LA PROPUESTA

6.6.1. ESCENARIO DE EVALUACIÓN DE RIESGOS

6.6.2 Indicadores de Riesgos

El objetivo de la etapa de riesgos es determinar las amenazas y vulnerabilidades descritas con niveles de probabilidades de 1 a 5 de incidencias que pueden variar en efecto dado a los procesos de las organizaciones expresados en el ámbito cualitativo adaptado a la organización mediante estudios de probabilidades para identificar las incidencias y el impacto que las produce. Se realizaron exámenes mediante representaciones de escenarios de impactos de riesgos mostrando los resultados.

TABLA 45. Indicadores de Riesgos Amenazas y Vulnerabilidades

Unidad de Sistemas					
Nivel	**indicador**	**Posibilidad**	**indicador**	**Impacto**	**Color**
A3	3	Alta	C	Catastrófico	
A2	2	Media	M	Moderado	
A1	1	Baja	L	Leve	

Tabla4. Indicadores de nivel de Riesgos

Nivel	Indicadores	Interpretación de probabilidades
Alto	3	Posibilidad de que puedan ocurrir con frecuencia
Medio	2	Posibilidad que se de en cualquier momento.
Bajo	1	Posibilidad de que no pueda ocurrir por determinadas actos

Tabla 47. Probabilidades de Riesgos

Nivel	Impacto	Probabilidades
Catastrófico		Trabajos no supervisados que pueden generar daños e incidentes de los recursos que afecten a la institución.
Moderado		Trabajos innecesarios errores y descuido de la información administrativa que afecten a la institución.
Leve		Trabajos supervisados que no afecte a la seguridad de la institución.

Elaborado por: Reinaldo Ramírez

- La aplicación de evaluaciones de controles de seguridad son coordinadas con los administradores de los departamentos informáticos donde se muestran los niveles para expresar los riesgos de acuerdo a la interpretación de los resultados explicados en cada tabla.
- Se evaluaran cada una de las posibles debilidades de que ocurran conforme a las vulneraciones notificadas de posibles incidentes de que puedan causar efectos sobre los procesos de la organización y posibles desastres naturales.
- El tratamiento de riesgos determina la administración de las áreas y recursos informáticos vulnerables para describir las estrategias de salvaguarda de activos.
- Unas ves señaladas los riesgos se establecerán las medidas preventivas para custodiar el ambiente administrativo.
- Unas ves identificadas la expresión de los riegos relacionados con las vulnerabilidades se ubica el escenario de riesgos de acuerdo al grado de posibilidad de ocurrir algún efecto.

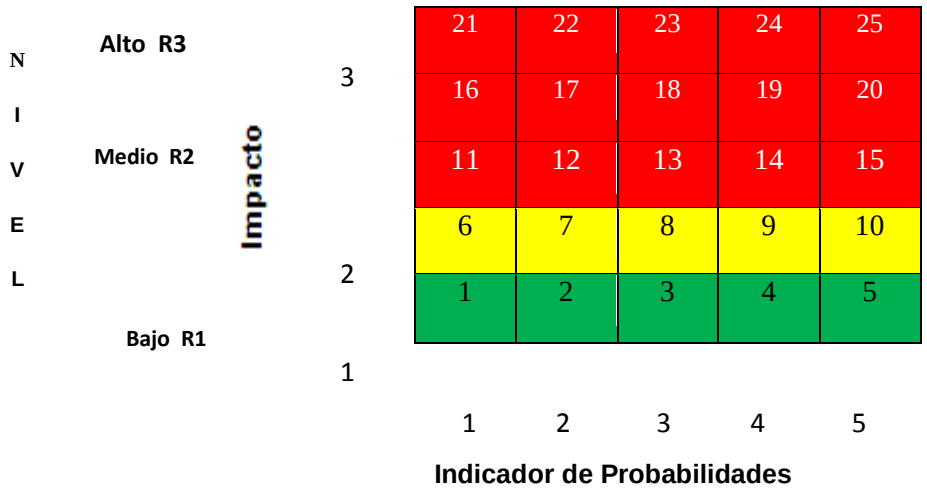
Después de identificar los niveles de posibilidad de riesgos con referencia a los indicadores se establece la matriz de amenazas y vulnerabilidad es que pueden aumentar o disminuir de acuerdo a los controles de niveles de riesgos y los posibles impactos mostrados en la siguiente figura.

Calculo del Nivel de Riesgo Asociado

Nivel de Riesgo Asociado = Nivel de Probabilidad x Nivel de Impacto

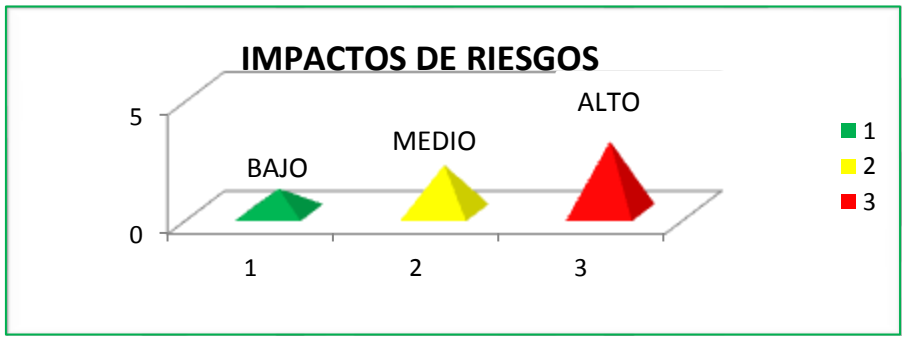
Nivel de Riesgo Asociado = 1 x 2

Nivel de Riesgo Asociado =2Tabla 48. Matriz de Riesgos



En la figura 11 se muestra el porcentaje de amenazas con una exposición al riesgo muy alto, alto, moderado y bajo.

Grafico 11. Porcentaje de amenazas de acuerdo a la exposición de riesgos



El resultado de los porcentajes de riesgos es nivel x indicador

C0DIGOS	RIESGOS DE SEGURIDAD Normas Políticas y estándares	Nivel	Indicador	RS %	Impacto
	CONTROL DE ACCESOS LOGICOS				
1	Cifrado de claves e información confidencial	3	4.00	12 %	
2	Autentificación de claves	2	3.00	6%	
3	Actualización de claves	2	2..00	4%	
	RECEPCION Y DISTRIBUCION DE INFORMACION				
4	vigilancia en la entrada y salida de datos	1.	2,00	2%	
4	Control de información manual y electrónica	2.	4,.00	8%	
5	Autenticidad de la información de los usuarios	3.	5.00	15%	
	CONTROL DE PROYECTOS				
6	planificación entre funcionarios	1.	1.00	2%	
7	Coordinación de actividaes	2.	3.00	6%	
8	Asignación de recursos	2.	3.00	8%	
9	Especialistas en gestión de tecnologías de la información	2.	4.00	8%	
10	Toma de decisiones	3.	2.00	6%	
11	Apoyo Económico	1.	1.00	2%	
	INSTRUCTIVOS DE OPERACION				
12	Manejo de instructivos de operación	3.	5.00	15%	
13	Utilización de los manuales del sistema	2.	4.00	12%	
14	Controles de códigos fuentes	3.	5.00	10%	
15	Controles de modificaciones	3.	5.00	10%	
16	Implementación de aplicaciones	3.	5.00	10%	
17	Adquisición de los instructivos de operación	3.	5.00	10%	
	CONTROLES DE COMUNICACION				
18	Implementación de redes de comunicación y servidores	3.	4.00	12%	
19	Integración con otros sistemas	2.	4.00	8%	
20	Manuales de usuario	3.	5.00	15%	
	CAPTACION DE DATOS				
21	Recepción de documentos	2.	2.00	4%	
22	Anomalías	2.	3.00	6%	
	ACTUALIZACION DE PROCEDIMIENTOS				
23	Manejo de los manuales del usuario	2.	4.00	8%	
24	Actualización de antivirus	2.	3.00	6%	
25	Actualización de claves	2.	4.00	8%	
26	Modificación y eliminación de información	3.	4.00	12%	
	CONTROL DE DATOS Y MANEJO DE CIFRAS DE CONTROL				
27	Responsabilidad de los usuarios con la dirección informática en la	2.	2.00	4%	
28	Ingreso de datos	2.	2.00	4%	
	Información manual y electrónica				
	CONTROL DE ASIGNACION DEL TRABAJO				
29	Capacitación	3.	4.00	12%	
30	Responsabilidades	1.	1.00	2%	
	CONTROL DE ALMACENAMIENTO MASIVO				
31	Espacios en los discos duros	2.	4.00	8 %	
32	Mecanismos de reconstrucción de archivos	2.	3.00	6 %	

CONTROL DE FALLA EN LOS SISTEMAS					
32	Utilización de los manuales de usuario	2.	4.00	8 %	
33	Herramientas de integración de sistemas	2.	3.00	6%	
34	Soporte Tecnico				
CONTROL DE FALLAS EN LOS EQUIPOS					
35	Medidas de protección de los equipos informáticos	2.	3.00	6%	
36	Mantenimiento preventivo y correctivo	1.	1.00	2%	
	Instalaciones eléctricas				
ORDEN EN EL DEPARTAMENTO DE INFORMATICA					
37	Requerimientos de oficina	1.	1.00	2%	
38	Ubicación de recursos de oficina	1.	3.00	3%	
39	Materiales de oficina	1.	4.00	4%	
REQUERIMIENTOS DE OFICINA					
40	Dispositivos de vigilancia	2.	4.00	8%	
41	Inventarios de activos	2.	2.00	4%	
42	Adecuaciones y comunidades de los usuarios	2.	3.00	6%	
43	Suministros de oficina	2.	4.00	8%	
	Ventilación y aire acondicionado				
CONFIGURACION DE SISTEMAS Y EQUIPOS INFORMATICOS					
44	Configuración de claves de usuario	2.	4.00	8%	
45	Utilización de aplicaciones para gestionar procesos de seguridad	2.	3.00	6%	
PRODUCTIVIDAD EN EL AREA INFORMATICA					
46	Capacitación de los usuarios en el control administrativo	2.	4.00	8%	
47	Anomalías	2.	3.00	6%	
CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACION					
48	Restricciones de Acceso fisco	2.	4.00	12%	
49	Cumplimiento de responsabilidades	2.	2.00	4%	
50	herramientas y dispositivos de seguridad	3.	5.00	24%	
SEGURIDAD LOGICA Y CONFIDENCIAL DE LA INFORMACION					
51	Capacitación de los usuarios y administrativos seguridad de la	3.	5.00	18%	
52	Confidencialidad de la información	2.	3.00	6%	
53	Integridad de la información	2.	3.00	6%	
	Disponibilidad de la Información	2.	2.00	4%	
54	Falta de de autentificación y cifrado	3.	5.00	15%	
SEGURIDAD EN EL PERSONAL					
55	Seguridad en la entrada y salida del personal	2.	5.00	10%	
56	Cámaras de seguridad	3.	5.00	15%	
57	Materiales de emergencia	3.	.00	21%	
58	Guardias de seguridad	1.	1.00	1%	
SEGURIDAD EN LA UTILIZACION DE EQUIPOS					
59	Seguridad en la utilización de los equipos informáticos	3.	3.00	18%	
60	Capacitación del uso de los recursos informáticos	2.	3.00	6%	
PROCEDIMIENTOS DE RESPALDO EN CASO DE DESASTRES					
61	Planes de emergencia	3.	5.00	15%	
62	Dispositivos de emergencia	2.	3.00	6%	
63	Mecanismos de respaldo	3.	3.00	9%	

Tabla 49. Escenario de evaluación de Riesgos de seguridad

Elaborado por: Reinaldo Ramírez

Tabla 50. Escenario de evaluación de Amenazas

	RIESGOS DE AMENAZAS Acciones e incidentes	Nivel	Indicador	RS %	Impacto
	Amenazas Humanas				
64	Actos de corrupción	1.00	1.00	2%	
65	Terrorismo	2.00	1.00	6%	
66	Consumo de bebidas e ingreso de materiales tóxicos	3.00	5.00	10%	
67	Ex empleados de la institución	1.00	1.00	2%	
68	Sabotaje	2.00	2.00	4%	
69	Perdida de información	2.00	2.00	4%	
70	Jaqueo	1.00	1.00	2%	
71	Espionaje	1.00	1.00	2%	
72	Errores en los equipos de equipo	2.00	3.00	6%	
73	Ingreso de dispositivos móviles	3.00	4.00	12%	
74	Ingreso de memorias y dispositivos externos	3.00	2.00	6%	
75	Cableado mal instalado	3.00	7.00	21%	
76	Interferencias eléctricas	3.00	2.00	4%	
77	Uso incorrecto de redes sociales en las horas de trabajo	2.00	2.00	4%	
78	Compartir llamadas telefónicas	3.00	6.00	9%	
79	Incumplimiento de normas y políticas institucionales	2.00	3.00	5%	
80	Falta de responsabilidades	2.00	3.00	5%	
81	Falta de capacitación	2.00	3.00	5%	
	Seguridad Física				
82	carencia de dispositivos de vigilancia	3.00	5.00	15%	
83	Carencia de planes de emergencias	3.00	5.00	15%	
84	Carencia equipamiento para soporte técnico	2.00	4.00	8%	
85	Carencia de herramientas de seguridad	3.00	6.00	18%	
86	Carencia de manuales operativos	3.00	6.00	18%	
	Seguridad lógica				
87	Filtraciones de virus	3.00	4.00	12%	
88	Autentificación de claves	3.00	4.00	12%	
89	Cifrado de claves	3.00	5.00	15%	
90	Huella Digital	1.00	5.00	5%	
91	Firma Digital	1.00	5.00	5%	

Elaborado por: Reinaldo Ramírez

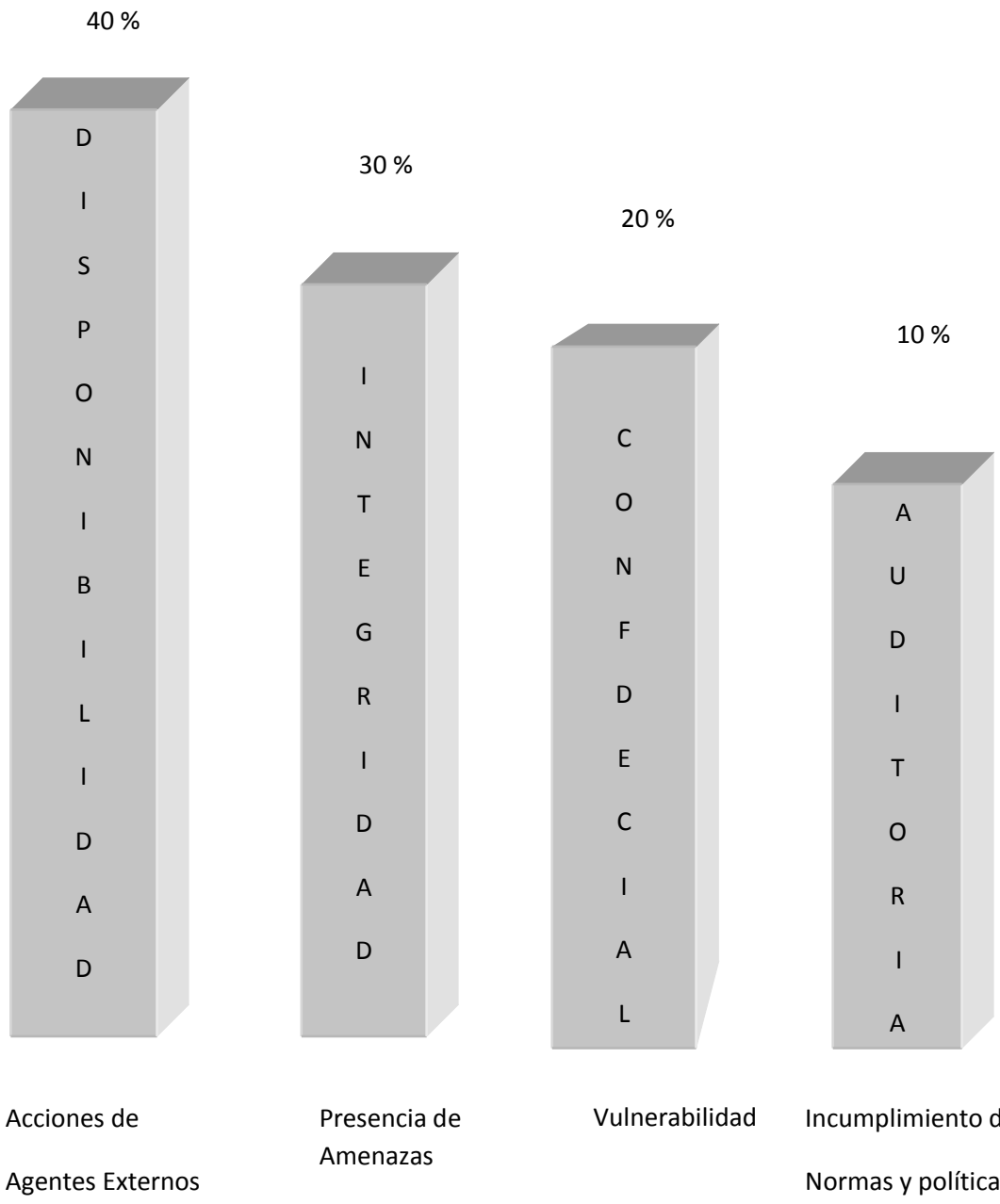
Tabla 51. Escenario de evaluación de vulnerabilidades.

RIESGOS DE VULNERABILIDAD	Indicador	Nivel	CONTROLES DE SEGURIDAD	RECOMENDACIONES
Fallas eléctricas		3	Utilizar reguladores de alta capacidad de voltajes como baterías para recargar energía.	Restablecer reguladores voltaje de alta capacidad de voltajes como baterías
Fallas en hardware		2	Mantenimiento preventivo y correctivo	Remplazar componentes en mal estados en al unidad de soporte técnico.
Fallas en software		2	Mantenimiento e instalación de sistemas y programas.	Reemplazar programas y sistemas afectados en las unidades de soporte técnico.
Accesos no autorizados		2	Coordinar las actividades de monitoreo a equipos de trabajo	Notificar a la directiva informática los accesos a los servidores de red
Filtración de virus		3	Instalar antivirus preventivos manteniendo actualizaciones del firewall	Establecer soluciones a través áreas de soporte técnico de los equipos infectados equipos afectados por virus
Fallas de integración		2	Establecer canales de comunicación	Revisar la configuración de conexiones de redes y servidores
CATASTROFES				
Incendios		3	Restricciones de ingresos de materiales corrosivos tóxicos y de combustión.	Proceder a utilizar extintores de incendios
Inundaciones		3	Mecanismos para controlar las fugas de agua.	Se procederá a controlar que los equipos y dispositivos se mantengan legos de derrames de líquido
Terremotos		3	Establecer capacitación planes de simulacros ante emergencias	Establecer mecanismos de construcciones de infraestructuras antisísmicas
Respaldos		2	Trasladar los respaldos de información a lugares seguros	Establecer los tipos de información a respaldar asignados a dispositivos de almacenamientos

ESTADISTICA DE RIESGOS POR FALTA DE AUDITORIA EXTERNA

Riesgos de inseguridad de activos y recursos informaticos en la Unidad de sistemas presentados por el 100 % de los encuestados del GAD Municipal de Ventanas.

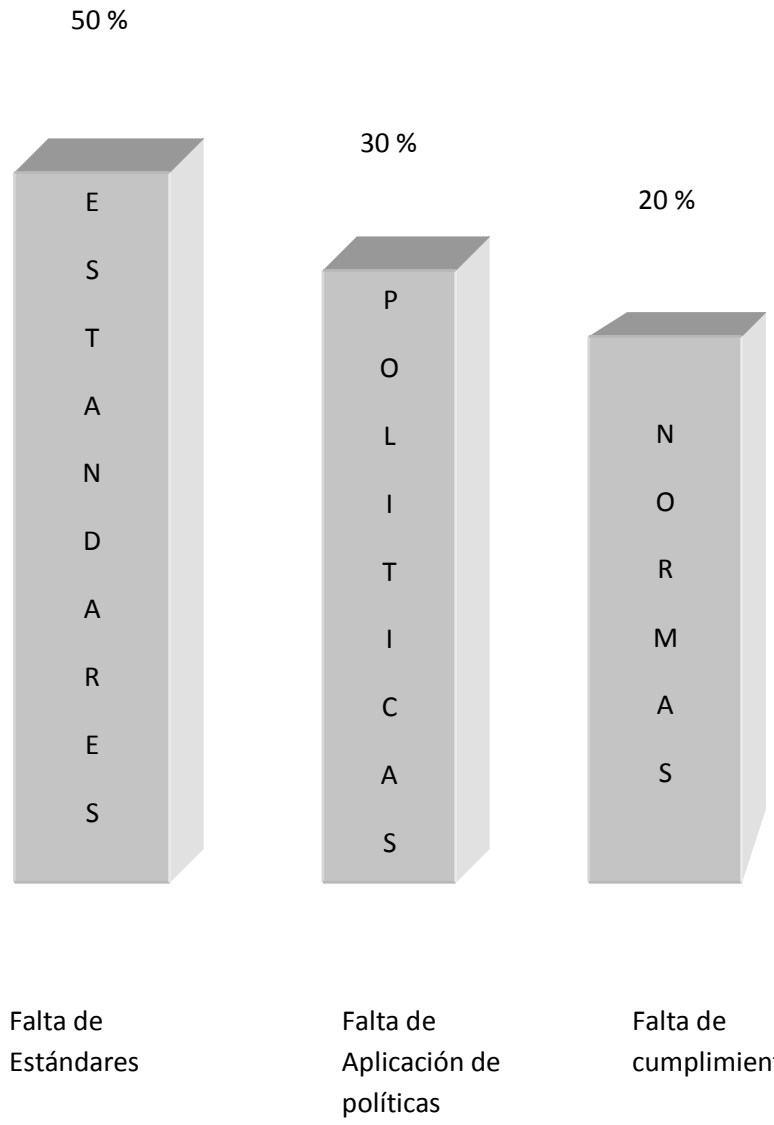
Grafico 12. Porcentaje mínimos de amenazas de acuerdo a la exposición de riesgos



ESTADISTICA DE RIESGOS POR FALTA AUDITORIAS INTERNAS

Riesgos de inseguridad de activos y recursos informaticos en la Unidad de sistemas presentados por el 100 % de los encuestados del GAD Municipal de Ventanas.

Grafico 13. Porcentaje máximos de amenazas de acuerdo a la exposición de riesgos.



6.6.3 MEJORA CONTINUA DEL PLAN

6.6.4 TRATAMIENTO DEL RIESGO

El tratamiento con el riesgo es la acción para reducir y eliminar los riesgos para aceptar, transferir, eliminar, reducir riesgos.

Cálculo de costos de tratamiento de Riesgos

Ejemplo: El costo de impactos de robos de un equipo informático en cyber es de I = $1000 Dólares por mes las pérdidas económicas serian la frecuencia (F) = 12 meces del año el costo anual seria C= f x i

C= 100 X 12 = 12000

I=impacto 1000

F= Frecuencia 12

C=Costo total= 12000

Tabla 52. Tratamiento con el Riesgos

REDUCCIÓN DE RIESGO EN LA UNIDAD DE SISTEMAS			
CONTROL DE ACCIONES	***IMPACTO =I***	***Frecuencia= f***	***COSTO TOTAL***
Agentes Externos	Confidencialidad, Integridad y Disponibilidad de Activos	*Sistema de Gestión de Seguridad de la Información SGSI*	*$ 7000.00*
Agentes Externos	*accesos*	*Criptografía*	*$ 3000.00*
Agentes Internos	*identificación*	*Huella Digital*	*$ 5000.00*
Agentes Externos e	*falsificación*	*Firma Digital*	*$ 5000.00*
Agentes Externos e Internos	*Robos*	*Cámaras de Seguridad*	*$ 5000.00*
respaldos	*Desastres*	*Data center*	*$ 10.000.0*
Costo Anual			*$ 35.000*

Elaborado por Reinaldo Ramírez

Reducir los riesgos: es la probabilidad de descartar los riesgos minimizando las posibilidades de que se filtren y provoquen reacciones causando consecuencias en una organización.

Los riesgos muchas veces no se pueden eliminar en su totalidad pero si pueden se reducidos tomando controles basados en medidas preventivas que deben llevarse a cabo con responsabilidades mediante mecanismos de emergencia cuando se produzca incidentes en una organización.

Reaccionar ante el riesgo: existen las posibilidades de que la organización no posea los suficientes recursos materiales y recursos económicos para implementar herramientas que permitan actuar frente a un riesgo.

Mitigación de los riesgos: es una manera de solucionar los riesgos de manera coordinada con la aplicación de normas, políticas, estándares y herramientas como medidas preventivas y correctivas para la construcción de un plan de fortalecimiento de seguridad a las que están expuestas las organizaciones para controlar las amenazas humanas y naturales que se den en el ámbito administrativo y tecnológico.

Tabla 53.Mitigación del Riesgo

Mitigación del Riesgo en la Unidad de Sistemas				
Accesos Físicos y Lógicos	**Aceptar**	**Transferir**	**Reducir**	**Eliminar**
Agentes Externos e internos	Cámaras de Seguridad	Huella Digital	Cifrado	Antivirus
		Firma Digital	Autentificación	Firewall

Elaborado por Reinaldo Ramírez

Descartar riesgos: existe la incertidumbre de que se pueda descartar un riesgo o eliminarlo completamente dentro de una organización en su mayoría los riesgos se producen por imprudencias, fenómenos naturales ,falta de capacitaciones y conductas morales que se dan en el mundo actual.

Contingencias de prevención y corrección: En la etapa anterior se realizó evaluación de riesgos según los niveles superiores que afecten a la seguridad de los procesos de registros se determinaron estrategias de control ante amenazas basadas en hechos de la realidad para cubrir los riesgos.

Para minimizar los niveles de riesgos se puede reducir la posibilidad de que se susciten mediante mecanismo y prevenciones de riesgos el cual implica acciones de control y responsabilidad usando medidas correctivas.

Para revenir los riegos de mayor efecto se establecerán medidas preventivas a cargo de los comités de controles de seguridad basada en las atribuciones y responsabilidades de operadores y técnicos de seguridad física y lógica.

Para controlar las acciones e incidentes establecerán medidas correctivas de fortalecimientos de seguridad en las áreas de trabajo a cargo de los equipos de trabajo en la unidad informática.

6.6.4.1 MEDIDAS PREVENTIVAS DEL PLAN

6.6.4.2 IDENTIFICACIÓN DEL RIESGO: FALLAS ELÉCTRICAS

Al presentarse una descarga eléctrica por cortes de energía los procesos informáticos se verán afectados debido a que los equipos informáticos depende de conexiones eléctricas para su funcionamientos, si los cortes eléctricos son bajos causara los mínimos inconvenientes en los trabajos y en las operaciones, si los cortes eléctricos son muy altos provocara mayores daños en el servicio informática causando pérdidas de información afectando la productividad de los equipos en las horas de trabajo.

Los equipos informáticos contaran con reguladores de energía con suficiente capacidad para soportar altos voltajes evitando deterioros en los componentes de hardware y software.

Atribuciones y responsabilidades

Responsables:

- Coordinador de la unidad
- Asistente técnico

- Revisar las conexiones de cableado que estén en condiciones adecuadas además utilizar reguladores de voltaje que cuenten con suficiente capacidad de protección y ahorro de energía.

- Revisar si los cableados eléctricos se encuentran en buenas condiciones para ejecutar actividades informáticas.

DIAGRAMADE FLUJO DE PREVENCIÓN POR FALLAS ELÉCTRICAS

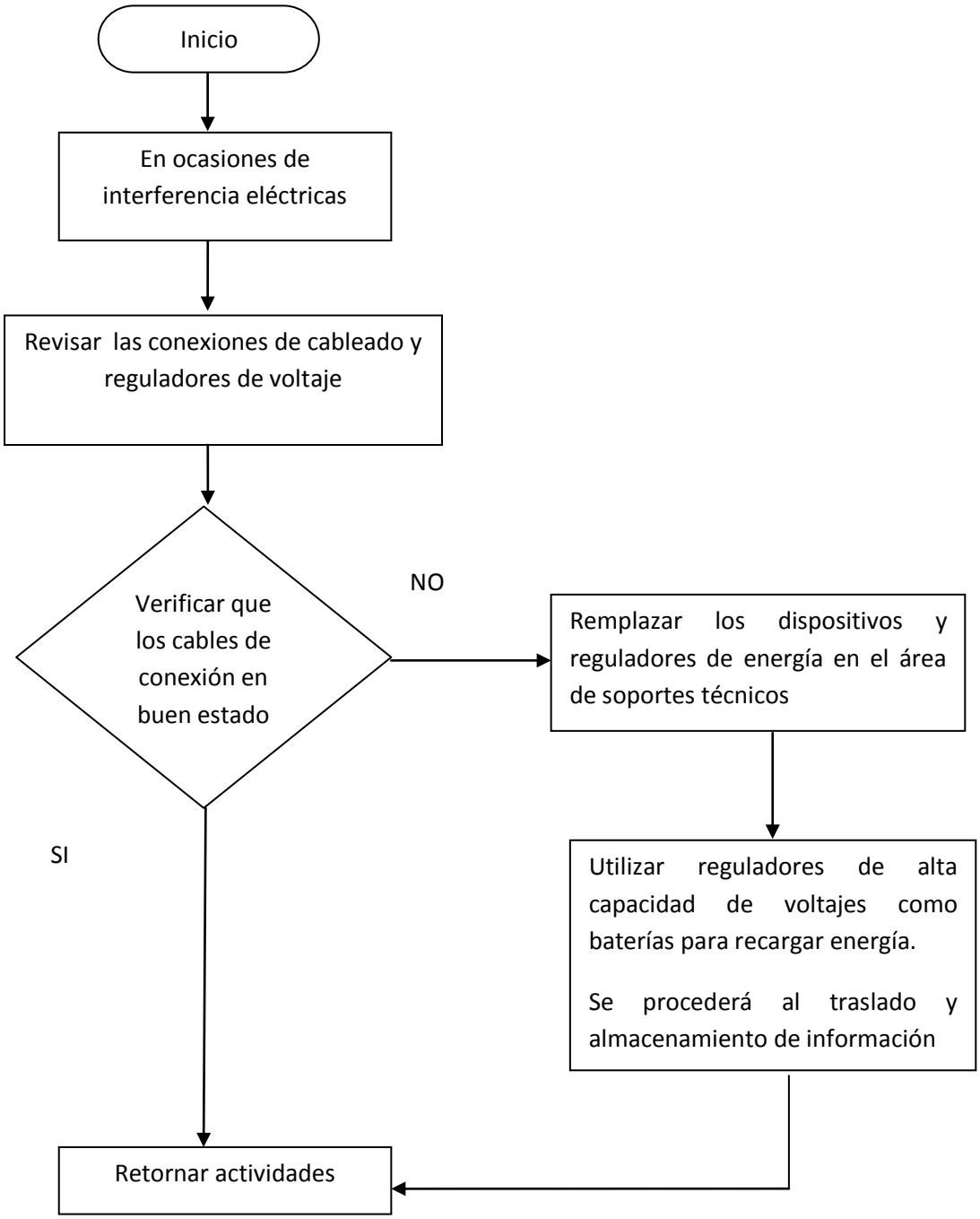


Grafico 14. Diagrama de fallas eléctricas elaborado por: Reinaldo Ramírez

6.6.4.3 IDENTIFICACIÓN DEL RIESGO: FALLAS DE HARDWARE

Por lo general los componentes de hardware en entornos de trabajos se ven afectados por varios motivos. Entre ellos se debe a desgastes de algunos de sus elementos por sobrecargas de trabajos asignados por los usuarios en condiciones de cortes de energía eléctrica por lo cual establecerá medidas preventivas de soporte técnico.

Las fallas en los componentes de hardware se dan muchas veces por falta de mantenimientos preventivos e inconvenientes por desgastes de alguno de los elementos y dispositivos de hardware impidiendo el rendimiento de los trabajos de los usuarios.

Atribuciones y responsabilidades

Responsables:

- Director de la unidad
- Asistente técnico

- Revisar que los componentes de hardware se encuentren en buen estado de ser posible mantenerlos ubicados en lugares secos, limpios, y libres de tráfico de personas, contacto con líquidos y metales que puedan causar inconvenientes.

- Establecer planes de mantenimientos preventivos para cubrir las fallas y reparos de alguno de sus componentes.

- Evitar los traslados de componentes sin previas autorizaciones

- En condiciones extremas se reemplazara los componentes deficientes para retornar las reparaciones.

DIAGRAMA DE FLUJO DE PREVENCIÓN POR FALLAS EN EL HARDWARE

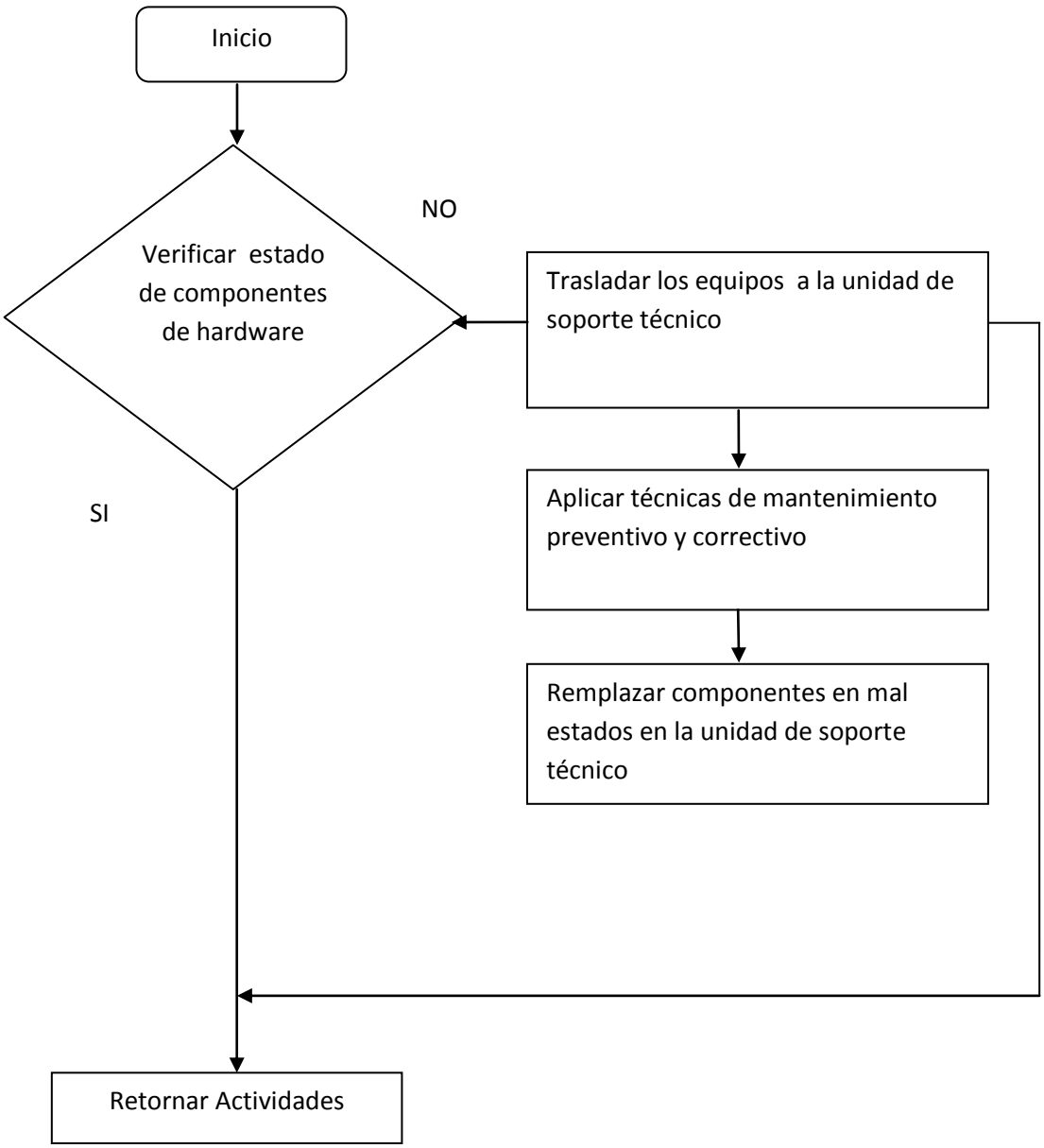


Grafico 15. Diagrama de fallas de hardware elaborado por: Reinaldo Ramírez

6.6.4.4 IDENTIFICACIÓN DEL RIESGO: FALLAS EN EL SOFTWARE

Las mayorías de fallas en el software en los procesos actividades informáticas se deben por filtraciones de virus que pueden ocasionar daños e interferencias en los programas y sistemas operativos en otras ocasiones se dan por manipulaciones inadecuadas de personas que puedan ocasionar daños para retornar los procedimientos de reparos y restauración de programas.

Atribuciones y responsabilidades

Responsables:

- Coordinador de la unidad
- Asistente técnico

- Revisar los archivos y documentos infectados para posterior eliminar virus detectados.

- Establecer planes de mantenimientos correctivos para cubrir las fallas con reparos de programas y sistemas operativos.

- En los casos de fallas de sistemas se recomienda utilizar los manuales operativos para retomar soluciones inmediatas.

- En los casos de filtraciones de virus se establecerá planes de mantenimiento preventivo con escudos protectores de sistemas instalando antivirus de ser posibles reanudar las operaciones de los sistemas.

DIAGRAMA DE FLUJO DE PREVENCIÓN POR FALLAS EN EL SOFTWARE

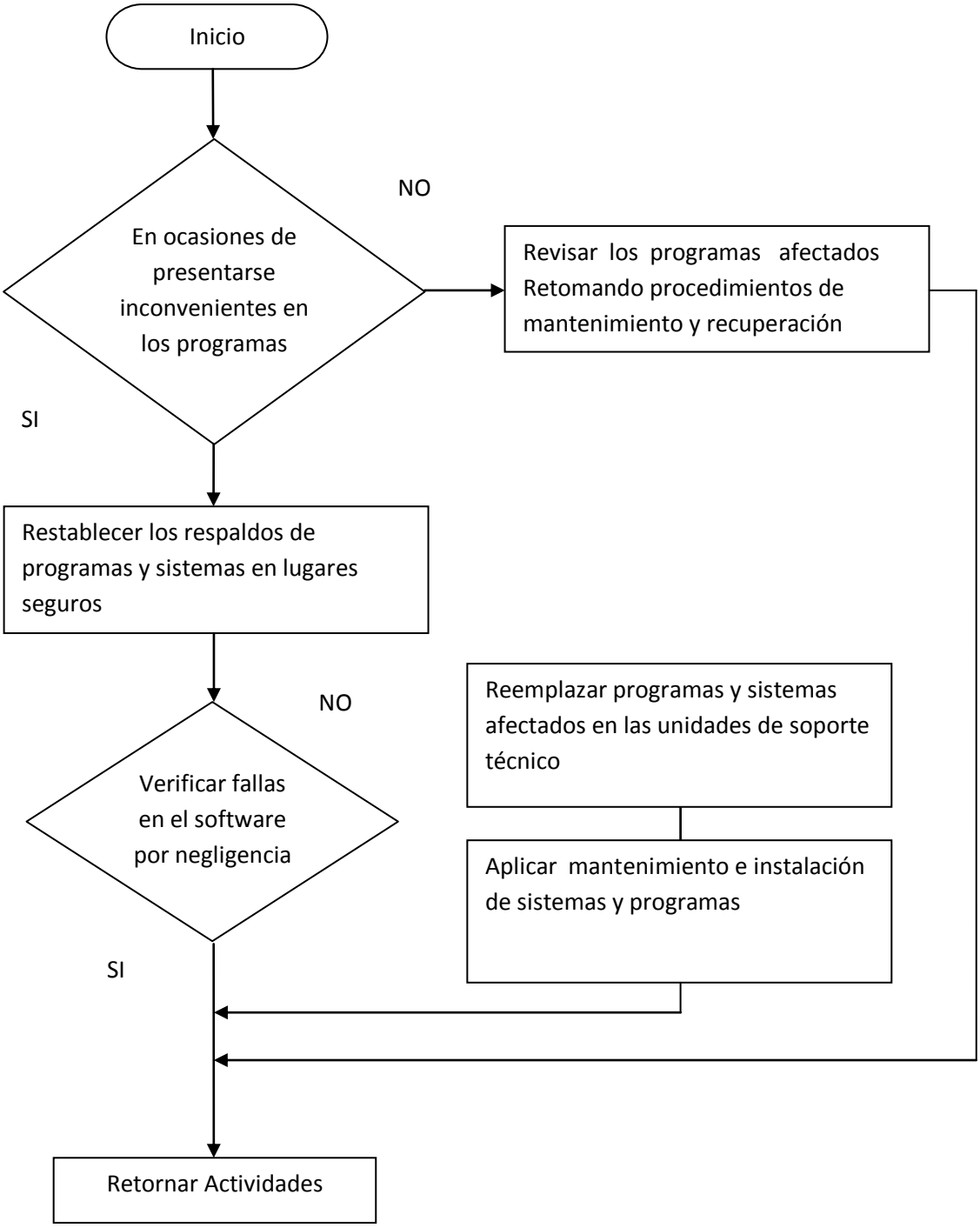


Grafico 16. Diagrama de fallas de software elaborado por: Reinaldo Ramírez

6.6.4.5 IDENTIFICACIÓN DEL RIESGO: FILTRACIONES DE VIRUS

La mayor parte de riesgos en las instituciones se dan por las filtraciones de virus creados por agentes potenciales que provocan daños y contaminación de archivos y programas de cómputo.

Los virus se manifiestan provocando alteraciones de programas y sistemas operativos.

Atribuciones y responsabilidades

Responsables:

- Coordinador de la unidad
- Asistente técnico

Se recomienda las medidas preventivas

- En los casos de filtraciones de virus se establecerá planes de mantenimiento preventivo.

- Instalar antivirus preventivos con actualizaciones periódicas a cargos de las unidades de soporte técnico.

- Revisar los archivos y documentos infectados para posterior eliminar virus detectados.

- En condiciones graves se procederá a formatear los sistemas y programas para luego retornar las funciones y actividades de sistemas.

DIAGRAMA DE FLUJO DE PREVENCIÓN DE VIRUS

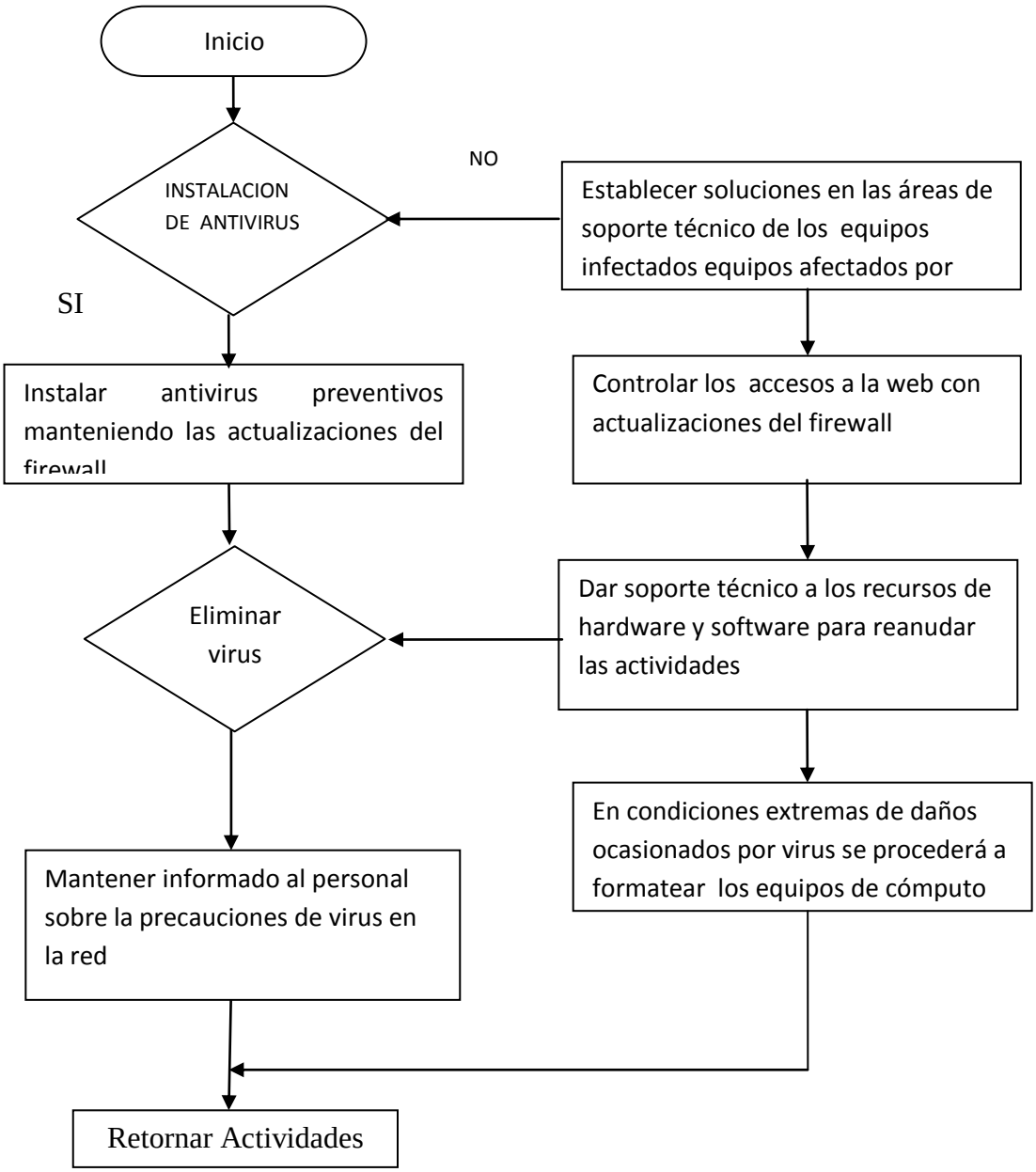


Grafico 17. Diagrama de prevención de virus elaborado por: Reinaldo Ramírez

6.6.4.6 IDENTIFICACIÓN DEL RIESGO: ACCESOS DE AGENTES CIBERNETICOS

Las amenazas más peligrosas por agentes humanos en las instituciones se los describe por diferentes nombres (hacker, cracker, lamer etc.) hasta la actualidad con la evolución de la tecnología no se han podido frenar los delitos informáticos por agentes maliciosos que se encuentran en el medio social, político, económico y tecnológico.

Las vulnerabilidades más activas serán examinadas para identificar las causas de posibles amenazas humanas que puedan causar perdidas.

Atribuciones y responsabilidades

Responsables:

- Coordinador de la unidad
- Asistente técnico

Se recomienda las medidas preventivas

- Realizar auditorías informáticas coordinadas con los comités directivos.
- Implementar sistemas de gestión de seguridad SGSI para el control de acceso a los sistemas de información y comunicaciones
- Implementar cámaras de seguridad de vigilancia en las aéreas informáticas para el monitoreo de actividades.
- Utilizar mecanismos de autentificaciones de claves de los usuarios de sistemas.
- Aplicar mecanismos de Criptografía (cifrado de calves, publicas y privadas)
- Utilizar dispositivos de Huellas digitales de identificación de empleados.
- Utilizar Firmas digitales de verificación de identificaciones de usuarios.

DIAGRAMA DE FLUJO DE PREVENCIÓN DE ACCESOS NO AUTORIZADO

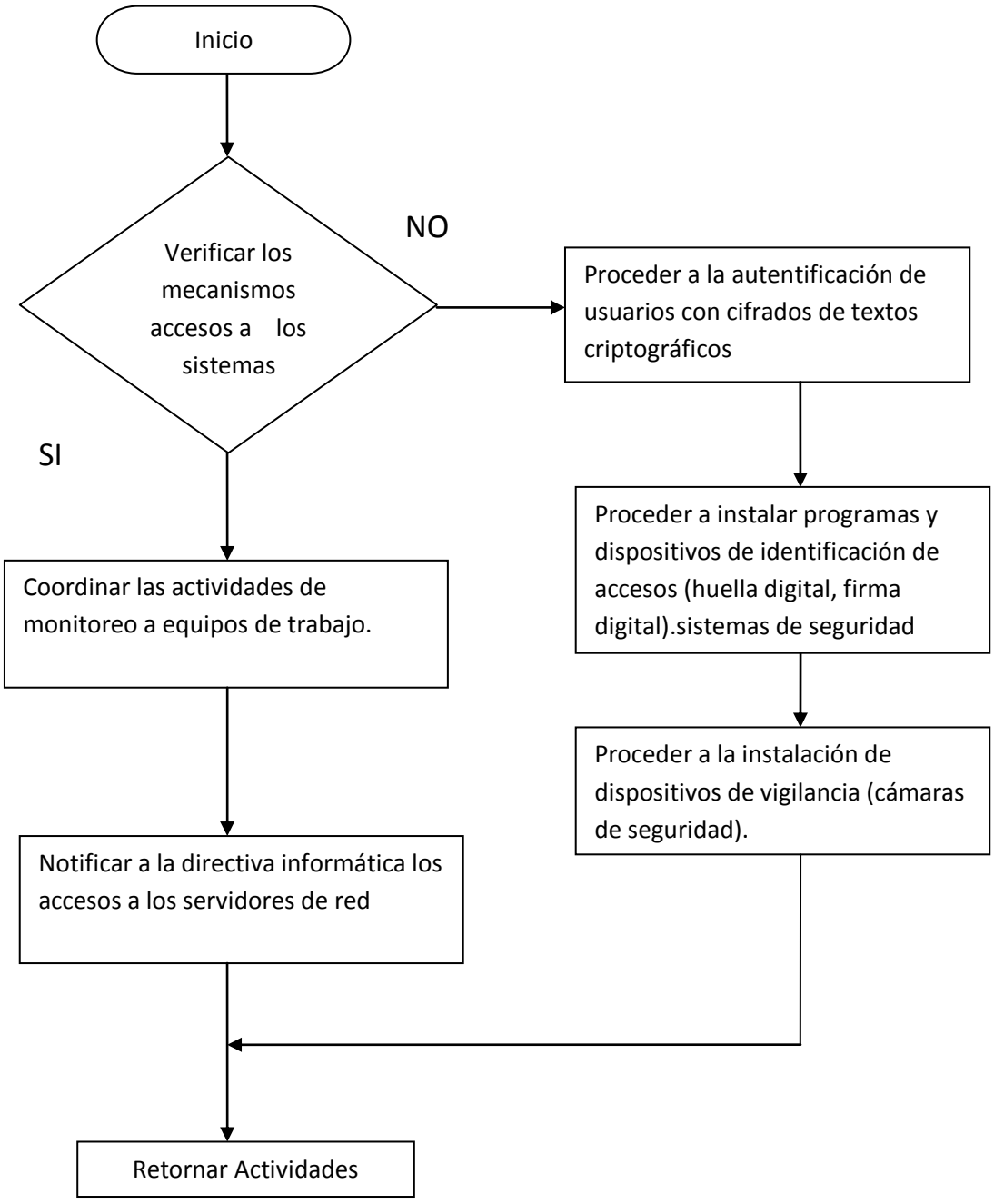


Grafico 18. Diagrama de prevención de accesos elaborado por: Reinaldo Ramírez

6.6.4.7 IDENTIFICACIÓN DEL RIESGO: FALLAS DE INTEGRACIÓN

En la mayoría de los casos las fallas en las comunicaciones se deben a falta de integración de sistemas muchas veces por falta de implementación de redes locales y configuraciones de servidores para la transmisión de datos en las áreas de trabajo.

Se recomienda implementar servidores de redes locales en las áreas de trabajo para agilitar la comunicación de datos.

Atribuciones y responsabilidades

Responsables:

- Coordinador de la unidad
- Asistente técnico

- Implementar y establecer redes locales para facilitar la integración de información dentro de la institución.

- Configurar los servidores para proveer información a las demás áreas.

- Configurar las conexiones de red para facilitar las comunicaciones.

- Retornar actividades.

DIAGRAMA DE FLUJO DE PREVENCIÓN POR FALTA DE INTEGRACIÓN DE SISTEMAS

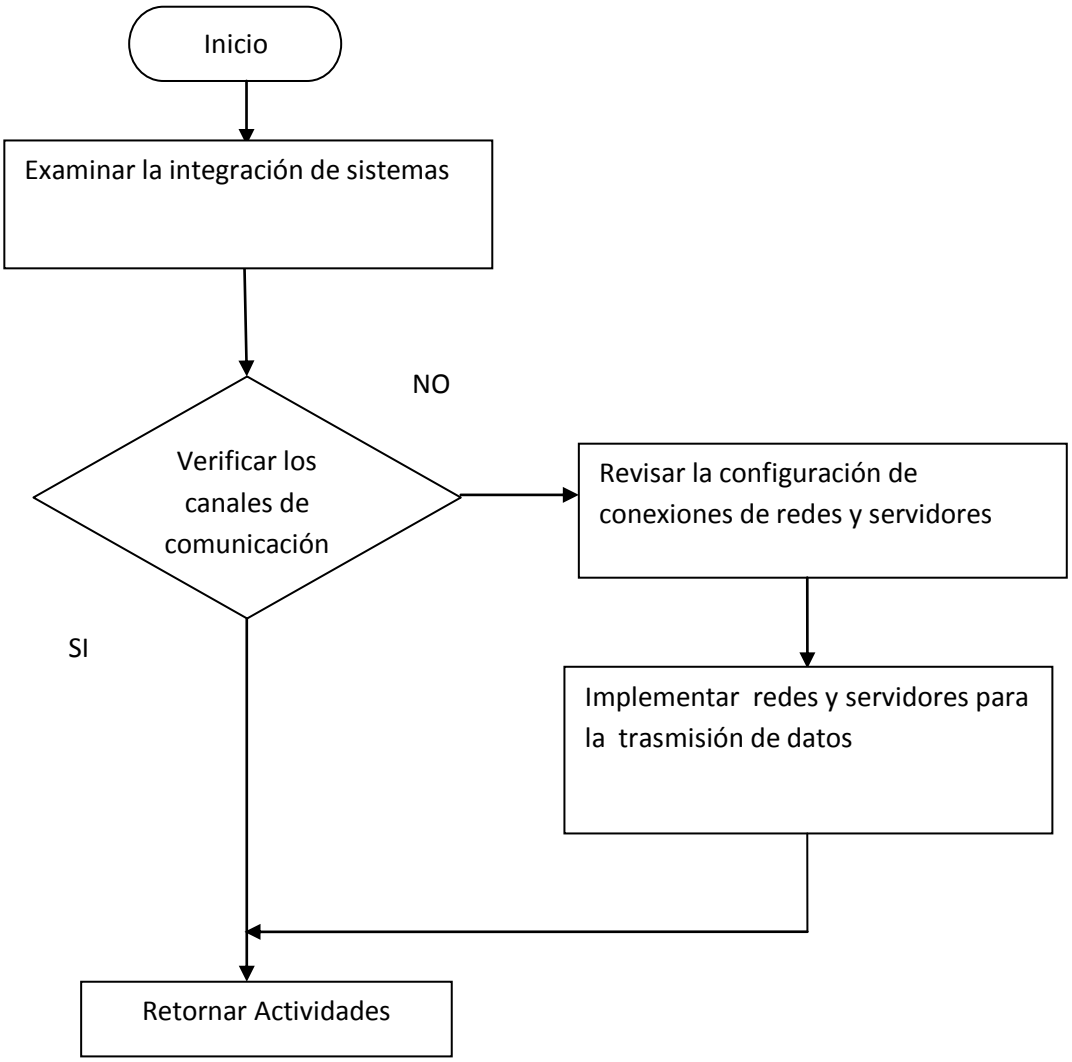


Grafico 19. Diagrama de fallas de integración elaborado por: Reinaldo Ramírez

6.6.4.8 IDENTIFICACIÓN DEL RIESGO: FALTA DE RESPALDOS

En la mayor parte de las instituciones se establecen mecanismos de respaldo de copias y archivos pero estos documentos se encuentran almacenados internamente en cada computador dependientes de su función al ocurrir una catástrofe se perderá toda la información de contenida en el computador.

Por lo general se recomienda establecer mecanismos de respaldos de todos los programas, archivos y documentos para garantizar la recuperación de información.

Atribuciones y responsabilidades

Responsables:

- Coordinador de la unidad
- Asistente técnico

Se recomienda las medidas preventivas

- Establecer mecanismo de respaldos en forma general de programas archivos sistemas y base de datos de la institución en Data center estatales.

- Recibir capacitaciones y planes de accesoria para la prevención y protección de la información manual y automatizada.

- Aplicar medidas de protección y de seguridad de los equipos de informáticos ante posibles desastres.

- Conocer la importancia de capacitaciones y medidas de prevenciones de posibles desastres que puedan ocasionar el deterioro y destrucción en las áreas de informáticas.

DIAGRAMA DE FLUJO DE PREVENCIÓN POR FALTAS DE RESPALDOS

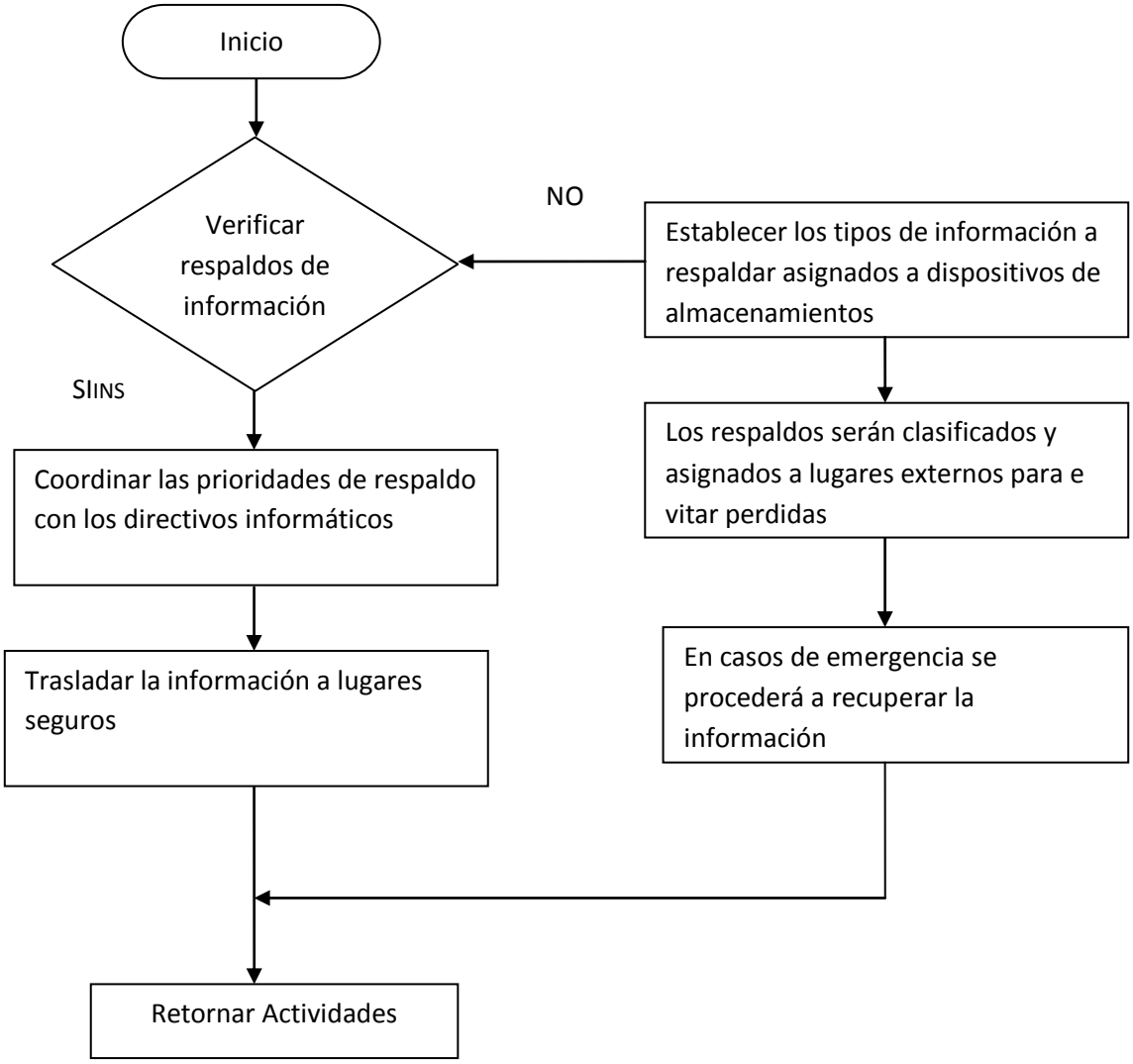


Grafico 20. Diagrama de falta de respaldos elaborado por: Reinaldo Ramírez

6.6.4.9 IDENTIFICACIÓN DEL RIESGO: CATASTROFES NATURALES

Los impactos ambientales de la naturaleza pueden afectar seriamente a las operaciones de las infraestructuras informáticas ocasionado serios daños y deterioros en situaciones inesperadas.

Al presentarse un terremoto afectara las condiciones de trabajo e infraestructuras de los departamentos en casos mayores ocasionara pérdidas de los equipos y materiales de trabajo en la organización.

En caso de incendios afectara la perdida y deterioro documentos manuales como (datos, archivos) de la organización.

En caso de inundaciones afectaran el desempeño de actividades de entornos de trabajo, se tornaran inadecuados para gestionar los procesos informáticos.

Atribuciones y responsabilidades

- Coordinador de la unidad
- Asistente técnico

Se recomienda las medidas preventivas

- En casos de terremotos: Se establecerá construcciones antisísmicas para de infraestructuras de edificios para los casos de protección de información establecerá Data Center en áreas externas a la institución para transmisiones de datos y recuperación de información.
- En casos de incendios: Se usara extintores de fuego en las áreas informáticas.
- En casos de inundaciones: Se evitar las fugas de agua en áreas de trabajo

DIAGRAMA DE FLUJO DE PREVENCIÓN ANTE CATASTROFES NATURALES

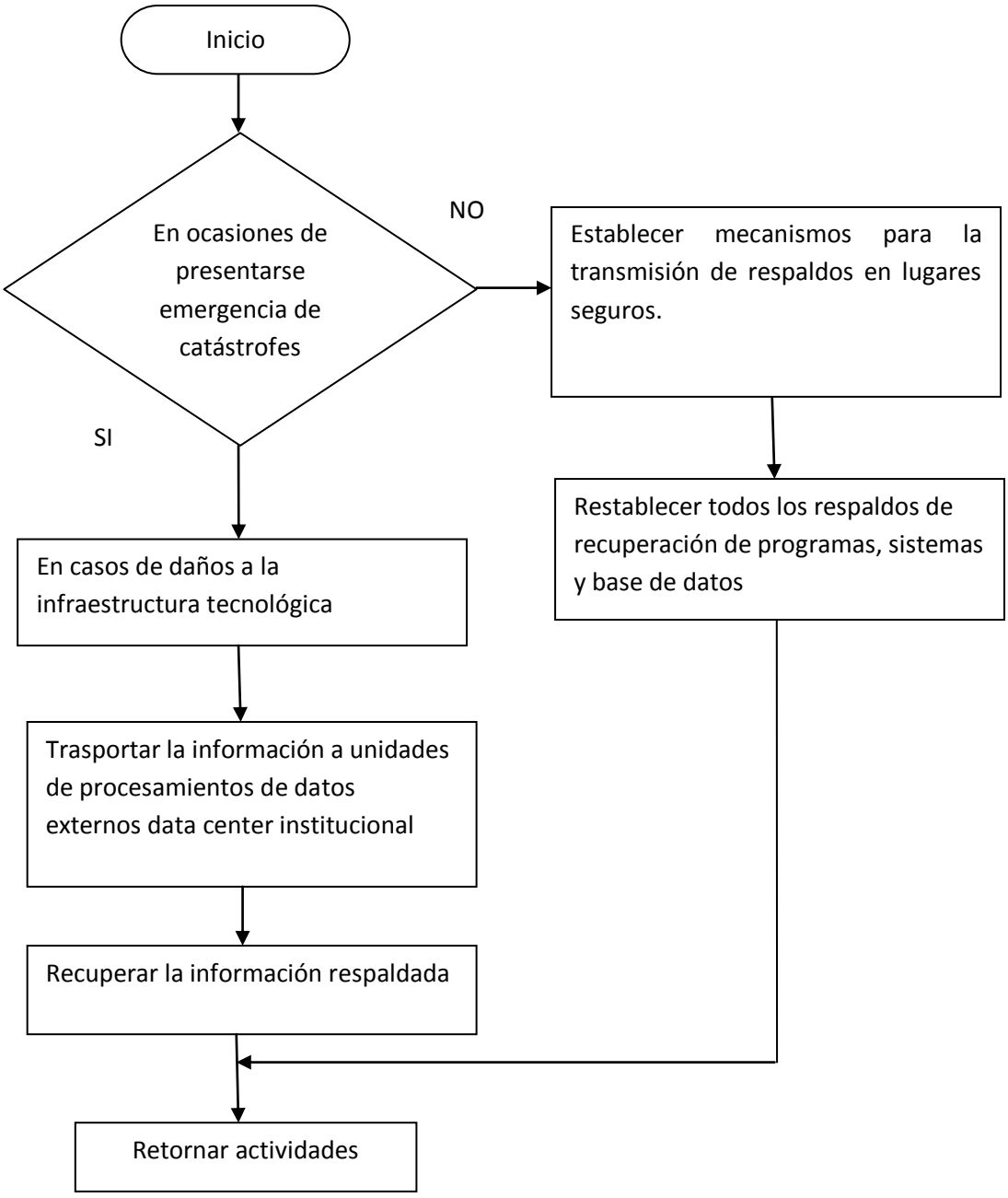


Grafico 21. Diagrama de prevención de catástrofes elaborado por: Reinaldo Ramírez

6.6.5. MEDIDAS CORRECTIVAS DEL PLAN DE CONTROL

Tabla 54. Medidas correctivas del Plan

ÁREAS	PLANIFICACIÓN Y SEGURIDAD
Comité de Planificación y Seguridad Informática	Implementación de reglamentos y restricciones atribuciones y responsabilidades de accesos físicos y lógicos a áreas informáticas.
	Responsabilidades de uso de claves de accesos
	Informes semestrales de evaluación del Plan Operativo Anual.
	Poner en práctica normas para la seguridad de la información (ISO-27001).
	Procedimientos técnicos y metodologías sobre seguridad en aplicaciones y sistemas informáticos.
	Plan de Capacitación Informática e informe de evaluación de Capacitación Informática.
	Plan de contingencias y control de emergencias.
	Propuesta de desarrollo de políticas de gestión tecnológica.
	Informes de implementación, administración y mantenimiento de aplicaciones y sistemas informáticos.
	Términos de restricciones y especificaciones técnicas.
	Proyectos para la adquisición de software propietario y software libre.
	Informes de soporte informático y capacitación en aplicaciones y sistemas de información.
	Procedimientos para accesos a recursos de información.
	Informe de seguridad y confidencialidad de identificaciones de usuario y contraseña.

	Informes de monitoreo de violaciones de seguridad.
	Cumplimiento de Políticas de Seguridad de la información y comunicación.
	Actualizaciones de políticas de seguridad.
	Informe de cumplimiento de procesos establecidos.
	Informes de pruebas y revisiones de software.
	Informes de aseguramiento y calidad de software.
	Actualización de sistema operativo.
	Implementación de redes y comunicaciones.
	Afinamiento a los sistemas operativos.
	Informe de implementación de antivirus.
	Gestión de la seguridad de los sistemas y de la continuidad empresarial.
	Encriptación de datos.
	Autentificación de huellas y firmas digitales
	Análisis de la integridad y confiabilidad de la información.
	Desarrollo de planes de contingencias
	Gestión de Backup Periódicos de la Información y Datos de la organización
	Informes de administración de licencias de programas informáticos comerciales (software).
	Propuestas de gestión e implementación de mejoras e innovaciones en los procesos, procedimientos y normatividad relacionado con la unidad. (pasa a auditoria).
	Informe de cambio de la información física de datos.
	Implementación de herramientas de optimización de datos y acceso a la información.

Sistemas y Base de Datos	Implementación de controles de definición, acceso, actualización y concurrencia de datos.
	Informes de monitoreo de las bases de datos.
	Informes de Auditoría de base de datos en coordinación con la sub unidad de planificación y Seguridad Informática.
	Informes de actualización de la estructura de base de datos.
	Gestión de la migración de datos a otras plataformas operativas y/o servidores.
	Registro de la generación de respaldos.
	Informes de verificación de la integridad de datos.
	Controles de acceso a los datos definidos e implementados.
	Planes de capacitación a programadores e ingenieros para utilizar eficientemente la base de datos.
	Informes de actividades y proyectos de desarrollo de sistemas de información en función de cumplir el Plan Operativo Informático (POI).
	Informes de ejecución de proyectos de desarrollo de sistemas informáticos aplicando estándares de desarrollo establecidos.
	Plan Anual de Mantenimiento de Sistemas de información.
	Informe de ejecución de actividades de mantenimiento de sistemas informáticos.
	Especificaciones técnicas de los servicios de desarrollos informáticos y aplicativos.
	Informe de evaluación y monitoreo de la ejecución de proyectos de desarrollo de sistemas informáticos realizados por terceros.
	Informes de asistencia técnica sobre soluciones tecnológicas puestas a consideración por terceros.

	Propuestas de tecnologías de información en los procesos del Gobierno Municipal como resultado de investigaciones de carácter tecnológico.
	Informes de administración técnica de los sistemas informáticos y los manuales de usuarios de cada sistema informático del Gobierno Municipal.
	Informes de los proyectos de desarrollo informático ejecutados y en ejecución.
	Informes de asesoría a las unidades orgánicas en la identificación de soluciones que involucren el desarrollo o aplicación de sistemas informáticos.
	Portal Web del Gobierno Municipal actualizado y administrado eficientemente.
Soporte Técnico y Mantenimiento	Inventario de equipos de cómputo (hardware).
	Realizar mantenimiento preventivo y correctivo del hardware de la institución (impresoras, computadoras y otros equipos de tecnología informática).
	Asistencia técnica presencial y telefónica a los usuarios de recursos de información del Gobierno Municipal.
	Charlas técnicas de uso de aplicaciones puntuales.
	Capacitación a usuarios en utilización de nuevo hardware para su eficiente aprovechamiento.
	Informes de administración del servicio de asistencia al usuario (“Helpdesk”).

	Informes de mantenimiento preventivo y correctivo de los equipos de cómputo.
	Informes de administración de Activos Informáticos.
	Reporte de actualizaciones de sistemas operativos de los usuarios.
	Estadísticas de malware (virus, etc.).
	Registros de actualización de antivirus.
	Monitoreo de software no licenciado, en conjunto con la sub unidad de Planificación y Seguridad Informática.
Redes y Comunicación de Datos	Informes de ejecución de proyectos de infraestructura tecnológica relacionados con redes y telecomunicaciones.
	Propuestas de aplicación de tecnologías de comunicaciones en los procesos del Gobierno Municipal, como resultados de investigaciones de carácter tecnológico.
	Especificaciones técnicas de procesos de selección referidos a servicios o proyectos de telecomunicaciones.
	Informes de supervisión de proyectos por terceros, relacionados con equipos de redes y comunicaciones.
	Registros de la red de datos (administración de usuarios, servidores y dispositivos de comunicaciones).
	Registros de la administración de accesos a la intranet e internet.
	Gestión del enlace de datos WAN entre diferentes unidades desconcentradas.
	Informes de administración de la red de telefonía.
	Políticas de seguridad informática en redes.
	Informes de ejecución de actividades orientadas al cumplimiento de la normatividad gubernamental en materia de telecomunicaciones y protección de la propiedad intelectual.
	Administración del Correo Electrónico Institucional.

Elaborado por: Reinaldo Ramírez

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD	
Organización de la seguridad de la información	Compromiso con la Dirección Informática
Autorización de recursos para administrar información	Contacto con Autoridades
Contactos con grupos especializados en seguridad	Identificación del Riesgos de agentes Externos
Administración de Activos	Propiedad de los Activos
Uso adecuado de los activos	Clasificación de Información
Seguridad de los recursos humanos	Responsabilidades de la Dirección
Formación en seguridad	Proceso disciplinarios
Eliminación de los derechos de acceso	Seguridad Física
Salvaguarda contra amenazas y desastres ambientales	Instalación y protección de equipos
Seguridad de cableado	Soporte Técnico
Administración de Comunicaciones y Operaciones	Medidas y controles de dispositivos
Seguridad de la documentación del sistema	Acuerdos de intercambio de información
Información electrónica	Sistemas de información corporativos
Comercio Electrónico	Transacciones en línea
Control de Acceso lógico	Registro de usuarios
Revisión de los derechos de acceso de los usuarios	Uso de contraseña
Responsabilidades del usuario	Identificación y autenticación de usuario
Sistema de gestión de contraseñas	Restricciones de acceso a la información
Comunicaciones móviles	Adquisición y mantenimiento de sistemas de información
Integridad disponibilidad de mensajes	Control de procesamiento interno
Validación de los datos de salida	Gestión de claves
Control del software de explotación	Protección de los datos de prueba del sistema
Control de acceso al código fuente de los programas	Seguridad en los procesos de desarrollo y soporte software
Fuga de información	Planes de contingencias
Control de vulnerabilidades técnicas	Registros de la administración de accesos a la intranet e internet.
Administración del Correo Electrónico Institucional[54].	

6.6.5.1 UTILIZACION DEL PLAN DE CONTROL

La utilización del plan de control de seguridad está basada en las siguientes funciones de los equipos de trabajo.

- Coordinación de los equipos de trabajo para la aplicación del Plan de control
- Cumplir con las atribuciones y responsabilidades de los equipos de trabajo.
- La funciones se asignaran a cada equipo de trabajo de control y acción de incidentes que ejecuten el plan
- Se aplicaran las medidas de acción ante amenazas
- Se utilizara todas las estrategia de monitoreo de actividades

6.6.5.2 COORDINACIÓN DE LOS EQUIPOS DE CONTROL

Los equipos de control estarán integrados por los empleados de acuerdo a sus funciones de desempeño fundamentales para la ejecución de Plan de control los equipos que forman parte del Plan de control serán

- Equipo directivo
- Equipo de sistemas y soporte técnico

6.6.5.3 EQUIPO DIRECTIVO DEL ÁREA DE SISTEMAS

El equipo de trabajo estará a cargo de la Ing. Cesar Vara es el encargado de supervisar las acciones e incidentes mediante controles de seguridad.

Objetivo principal de la área directiva minimizara los posibles riesgos de la información mediante supervisiones periódicas para detectar vulnerabilidades de la información y administración de recursos informáticos, el comité informático será el encargado de la toma de decisiones ante posibles acciones e incidentes vinculados a la dirección informática manteniendo informados a todos los miembros y empleados del área administrativa con las tareas principales conformado.

- Estudio de la situación actual.
- Decisiones de poner en marcha los controles de seguridad.
- Realizar procesos de supervisiones de actividades administrativas y manejo de recursos informáticos.
- Monitoreo de cumplimientos de normas y políticas internas.

6.6.5.3 EQUIPOS DE SISTEMAS, CONTROL, SOPORTE Y SEGURIDAD

Este equipo será responsable de todo lo relacionado con asistencia técnica con acciones preventivas y correctivas conformado por el Sr. Israel Conforme.

El equipo de sistemas se responsabilizara del control de la infraestructura tecnológica necesaria para el soporte y seguridad de los recursos informáticos relacionados con la administración de sistemas de información.

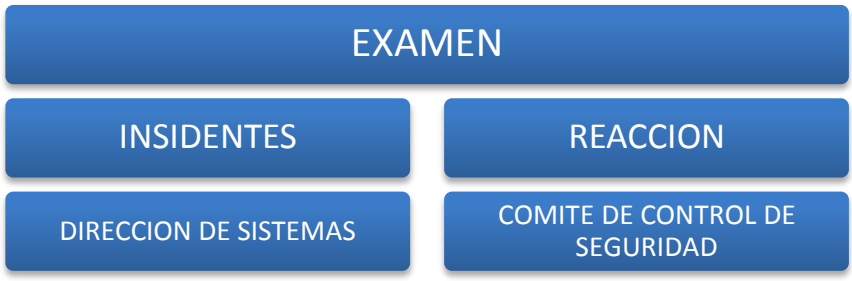
- Mantenimiento de equipos de cómputo
- Soporte de hardware y software

6.6.5.4 PASOS PARA PREVENIR AMENAZAS E INCIDENTES EN LA EJECUCIÓN DEL PLAN DE CONTROL Y SEGURIDAD

Se han designados los equipos de gestiones técnicas y administrativas para las etapas de control de personales encargados para la ejecución de del plan de control de seguridad.

Examen: Es el estudio de medidas de control mediante evaluaciones de incidentes y las posibles reacciones por la dirección de sistemas para dar soluciones por el comité de control de seguridad.

Grafico 23. Fase de evaluación



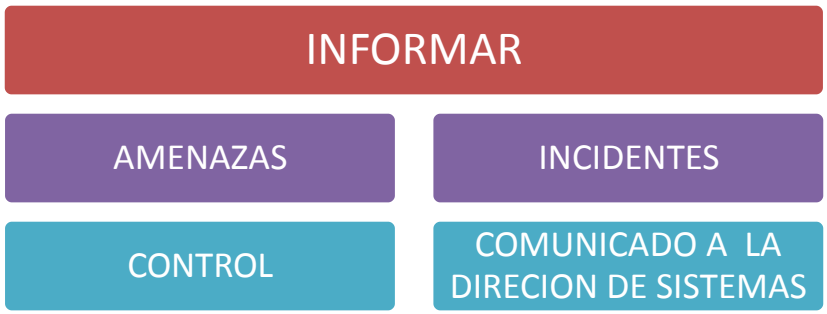
- EJECUCIÓN DEL PLAN: Consiste en la decisión del equipo directivo de proyectar el Plan debido al alcance de los daños.

- PLAN DE CONTROL: Se trata de la toma de desiciones por parte de la direccion de sistemas para la aplicación del plan ante posibles amenazas.

Figura 24. Fase de control

- COMUNICACIÓN: Define cómo y quién debe ser informado en primera instancia de lo ocurrido ante algún incidente.
- INFORMAR: Comunicar a la dirección los hechos observados en forma discreta.

Figura 25. Fase de comunicación



VII. BIBLIOGRAFIA

- ✓ Foddy, W. H. (2011). Constructing questions for interviews and questionnaires: Theory and practice in social research (New ed.). Cambridge, UK: Cambridge University Press.
- ✓ Proyecto: Un trabajo a presentar como cumplimiento al módulo "auditorías" en el posgrado Gerencia en Informática. [En línea] Autor: Muñoz, Do ralba Londoño Vladimir, Dirección,[Proyecto de Auditorias Medellín, Agosto 14 del 2012].
- ✓ *posgrado.pbworks.com/f/AUDITORIAS.doc*
- ✓ Francisco Gómez Rondón. Auditoria Administrativa, Joaquín Rodríguez Valencia. Año 2012. Sinopsis de Auditoria Administrativa.
- ✓ Documento: Sistema de gestión de la seguridad de Información SGSI. [En línea] Autor: Ing. Jaime Enrique López Hernández,[Proyecto Material solo para capacitación para su uso licenciado].
- ✓ Tesis: Auditoria de Seguridad Informática ISO 27001 Empresa de alimentos "Ítalamente SIA.LTDA." [En línea] Autor:ChristiRuiz
- ✓ Tesis: Uso de la norma ISO/IEC 27004 para Auditoría Informática. [En línea] Autor: Agustín Larrondo Quiroz, Dirección, [Proyecto Fin de Carrera el día 14 de Octubre de 2012 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid].
- ✓ Auditoria en Informática, II Edición, José Antonio Echenique García, Mc Graw.

PAGINAS WEB

[1]www.ventanas.gob.ec

[2]Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado del Cantón Ventanas

[3]International Organization for Standardization

[4]WWW.ISO27000.ES

[5] WWW.ISO27000.ES

[6]http://www.iso27001standard.com/es/que-es-iso-27001/

[7]www.**iso**27000.es/sgsi.html

[8]http://www.monografias.com/trabajos12/recoldat/recoldat.shtml

[9]http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

[10]http://www.auditoriasistemas.com

[11]http://www.monografias.com/trabajos12/condeau/condeau.shtml#PASOS

[12]International Organization for Standardization

[13]http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml#ixzz3WB6teL00

[14]https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_III_tecnicas.pdf

[15]Implantación de un SGSI y certificación ISO 27001 en la Administración Pública

[16]http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html

[17]http://www.unsa.edu.ar/sigeco/archivos/semi_material/Apunte%20Software.pdf

[18]http://es.wikipedia.org/wiki/Hardware

[19]http://es.wikipedia.org/wiki/Software

[20]https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_III_tecnicas.pdf

[21]http://www.washington.edu/research/rapid/resources/toolsTemplates/plan_do_check_act.pdf

[22]http://auditordesistemas.blogspot.com/2012/02/analisis-y-evaluacion-de-riesgos.html

[23]http://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

[24]http://es.wikipedia.org/wiki/Hardware

[25]http://es.wikipedia.org/wiki/Software

[26]http://revistas.um.es/analesdoc/article/view/2971/2951

[27]http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

[28]http://es.wikipedia.org/wiki/Desastre_natural

[29] http://es.wikipedia.org/wiki/Cracker

[30] http://es.wikipedia.org/wiki/Lamer_%28inform%C3%A1tica%29

[31]**http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.acis.org.co%2Fmemorias%2FJornadasSeguridad%2FIIJNSI%2Fpamplona.doc&ei=A7IiVdvBDcujNv-3gKgH&usg=AFQjCNFakSrKbN2XFGBRRIvlaZ77VA8grA&bvm=bv.89947451,d.cWc**

[32]**http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.acis.org.co%2Fmemorias%2FJornadasSeguridad%2FIIJNSI%2Fpamplona.doc&ei=A7IiVdvBDcujNv-3gKgH&usg=AFQjCNFakSrKbN2XFGBRRIvlaZ77VA8grA&bvm=bv.89947451,d.cWc**

[33]http://auditordesistemas.blogspot.com/2012/02/analisis-y-evaluacion-de-riesgos.html

[34]Federal Information Processing Standards Publications FIPS PUB65 - Guideline for Automatic Data Processing Risk Analysis, 1979

[35]https://protejete.wordpress.com/gdr_principal/control_riesgo/

[36]https://protejete.wordpress.com/gdr_principal/control_riesgo/

[38]Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado Municipal Del Cantón ventanas.

[39]Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado Municipal Del Cantón ventanas.

[40]http://ventanas.gob.ec/municipio/

[41]Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado Municipal Del Cantón ventanas.

[42]www.ventanas.gob.ec

[43]https://www.google.com.ec/?gws_rd=ssl#q=+3.+POL%C3%8DTICAS+DE+SEGURIDAD+++3.1+GENERALIDADES+

[44]http://www.monografias.com/trabajos7/sisinf/sisinf.shtml

[45]http://www.eoi.es/blogs/cod/2-tipos-de-informacion/

[46]http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml#ixzz3WB6teL00

[47]https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_III_tecnicas.pdf

[48]Instrucción A.F.I.P. 419/98: I.G. 359/97 (D.P.N.F.). Normas Complementarias. Responsabilidad Profesional de los Auditores Externos. Diferencias significativas en los Estados Contables.

[49]Instrucción A.F.I.P. 419/98: I.G. 359/97 (D.P.N.F.). Normas Complementarias. Responsabilidad Profesional de los Auditores Externos. Diferencias significativas en los Estados Contables.

[50]http://es.wikipedia.org/wiki/Servidor

[51]https://www.google.com.ec/search?q=DIAGRAMA+DE+UN+FIREWALL&biw=1024&bih=634&source=lnms&tbm=isch&sa=X&ei=13xOVLbeMMTCsATThoHIDQ&ved=0CAYQ_AUoAQ

[52]http://es.wikipedia.org/wiki/Servidor_de_archivos

[53]Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado Municipal Del Cantón ventanas.

[54]https://www.google.com.ec/?gws_rd=ssl#q=+3.+POL%C3%8DTICAS+DE+SEGURIDAD+++3.1+GENERALIDADES+

ANEXO Nº 1. FORMULARIO DE ENCUESTA A USUARIOS

Nombre de la unidad	**Lista de Chequeo** **Unidad de sistemas**				
Nombre del Instructor	**RSRC**	**Fecha:**	**Día:**	**Mes:**	**Año:**

EVALUCIÓN DE RIESGOS					
		Cumple			
Nº	**Variable / Indicadores**	**Si**	**no**	**a veces**	**Observaciones**
1	¿Existe un Comité Directivo de informática para Unidad de sistemas?	✓			Cumple con las disposiciones
2	¿Existe un Comité de Seguridad Informática en la Unidad de sistemas?		✓		No cumple con las disposiciones
3	¿Se establecen políticas de seguridad informática para Unidad de sistemas?			✓	Las políticas se encuentran en fase de desarrollo
4	¿Existe un sistema Seguridad Informática en la Unidad de sistemas?		✓		No cumple con las disposiciones normativas

EVALUACIÓN DE AMENAZAS

Nombre de la unidad	**Lista de Chequeo** Unidad de sistemas				
Nombre del Instructor	**RSRC**	**Fecha:**	**Día:**	**Mes:**	**Año:**

EVALUACIÓN DE AMENAZAS					
N°	**Variable / Indicadores**	**Cumple**			
		Si	**no**	**a veces**	**Observaciones**
1	¿Existen seminarios y talleres capacitaciones a los usuarios para las administraciones informáticas		✓		Cumple con las disposiciones
2	¿Se realizan actividades programadas para evaluar Monitorear las áreas informáticas?			✓	cumple a medias disposiciones
3	¿Se realizan Supervisiones Informáticas en la Unidad de sistemas?			✓	Cumple a medias con las disposiciones
4	¿Se establecen restricciones Sitios web y Redes Sociales		✓		No cumple con las disposiciones normativas
5	¿Existen estándares de soporte de tecnologías para la Infraestructura Tecnológica.		✓		
6	¿Existe el Equipamiento Informático de necesario (cámaras de seguridad) para las funciones de la Unidad de sistemas?		✓		No cumple con las disposiciones

EVALUACIÓN DE VULNERABILIDADES

Nombre de la unidad	**Lista de Chequeo** Unidad de sistemas				
Nombre del Instructor	**RSRC**	**Fecha:**	**Día:**	**Mes:**	**Año:**

EVALUCION DE VULNERABILIDADES					
		Cumple			
N^{O}	**Variable / Indicadores**	**Si**	**no**	**a veces**	**Observaciones**
1	¿Existen Proyectos Tecnológicos en la unidad de sistemas		✓		No Cumple con las disposiciones
2	¿Existen mecanismos y herramientas para administrar la seguridad de las Tecnologías de Información?		✓		No cumple con las disposiciones
3	¿Existen planes de Contingencias ante posibles desastres naturales?		✓		No cumple con las disposiciones
4	¿Existen mecanismos de comunicación abierta redes y servidores locales?		✓		No cumple con las disposiciones normativas
5	¿Existen mecanismos de de seguridad de comunicación redes y servidores locales?		✓		No cumple con las disposiciones

ANEXO Nº 2. FORMULARIO DE ENTREVISTA

Entrevista aplicada a Directivos	**RESPUESTAS**
¿Se ha realizado una auditoria al sistema de control Municipal?	Si ( ) No ( )
Porqué	
¿Existen políticas de seguridad para el sistema de control Municipal?	Si ( ) No ( )
Porqué	
¿El departamento de sistemas cuenta con una infraestructura de tecnología?	Si ( ) No ( )
Por que	
¿El departamento de sistemas cuenta con estándares de seguridad tecnológicos ISO 27001?	Si ( ) No ( )
¿El departamento de sistemas cuenta con una certificación ISO en seguridad de la información?	Si ( ) No ( )
¿El departamento de Avalúos y catastros cuenta con controles de identificación de huellas digitales?	Si ( ) No ( )
¿Sistema de control Municipal cuenta criptografía de seguridad de la información?	Si ( ) No ( )
¿El departamento de Avalúos y catastros cuenta mensajes de firmas electrónicas?	Si ( ) No ( )

GUÍA PARA LA EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONEN DE RECURSOS PÚBLICOS

Entidad: GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN VENTANAS

Área o rubro evaluado: EVALUACIÓN INTEGRAL DEL SISTEMA DE CONTROL INTERNO INSTITUCIONAL

Período : DEL 10 DE ENERO DEL 2014 AL 31 DE MARZO DEL 2014

Norma Técnica aplicada: 410-09 Mantenimiento y control de la infraestructura tecnológica

No.	Preguntas	INCIPIENTE	BASICO	CONFIABLE	MUY CONFIABLE	OPTIMO	NO APLICA	Recomendaciones	Acciones Tomadas por la Entidad
1	¿La unidad de tecnología de información definió e implementó formalmente los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de la institución?			X					
2	¿Se registró, evaluó y autorizó los cambios de procedimientos, procesos, sistemas y acuerdos de servicios previo a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción?	X							
3	¿Se mantuvo una bitácora de las modificaciones realizadas a los procesos de tecnológica y se informó a todos los actores de usuarios finales relacionados?								X
4	¿La unidad de tecnología de información mantuvo actualizados los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice a los sistemas informáticos y se estableció su difusión y publicación permanente?								X
5	¿La entidad mantiene ambientes de desarrollo/pruebas y de producción independientes, en los cuales se verifican medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar la integridad, disponibilidad, confiabilidad y seguridad de la infraestructura de tecnología de información disponible?								X
6	La unidad de tecnología de información elaboró e implementó formalmente el plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas, monitoreo, en las necesidades organizacionales, estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad?			X					
7	¿La unidad de tecnología de información mantiene un 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?			X					
8	¿El mantenimiento de los bienes relacionados con la infraestructura tecnológica, que se encuentran en garantía fueron proporcionados por el proveedor, sin que represente un costo adicional para la entidad?			X					

Elaborado por: Aplicado a:

Ing. Martha aguirre
AUDITORA GENERAL INTERNA

Srta. Viviana Andreina Olaya Wellington
COORDINADORA DE LA UNIDAD SE SISTEMAS INFORMÁTICOS

Ab.

Carlos Carriel Abad

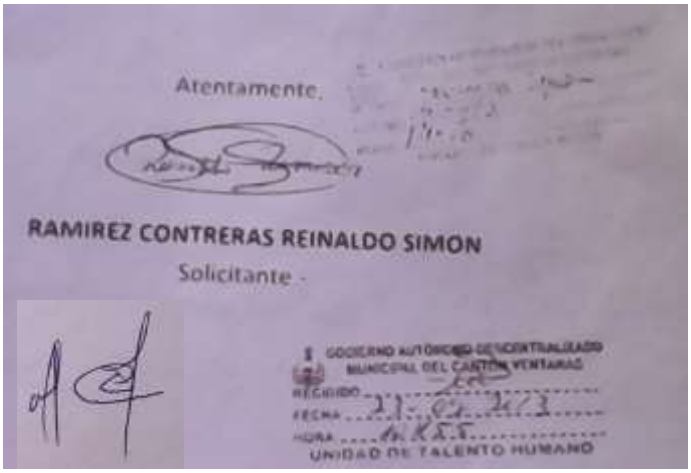
ALCALDE DEL CANTON VENTANAS

Ciudad.-

De mis consideraciones:

RAMIREZ CONTRERAS REINALDO SIMON, Egresado de la Facultad de Administración, Finanzas e Informática, Especialización Ingeniería en Sistemas de la Universidad Técnica de Babahoyo, me dirijo a usted de la manera más cordial para solicitarle muy comedidamente, se sirva ordenar a quien corresponda seme brinden todas las facilidades para poder realizar mi Tesis, cuyo tema es Plan de auditoria informática para la unidad de Sistemas en el Gobierno Autónomo Descentralizado del Cantón Ventanas previo a la obtención de mi Título de Ingeniero en Sistemas, trabajo que requiero hacerlo desde el mes de octubre en adelante.

Esperando que mi petición tenga la acogida favorable de su parte, reciba mi agradecimiento.



Atentamente,

RAMIREZ CONTRERAS REINALDO SIMON

Solicitante.-


GOBIERNO AUTONOMO DESCENTRALIZADO
MUNICIPAL DEL CANTON
VENTANAS

[1]www.ventanas.gob.ec

[2]Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado del Cantón Ventanas

[3]International Organization for Standardization

[4]WWW.ISO27000.ES

[5] WWW.ISO27000.ES

[6]http://www.iso27001standard.com/es/que-es-iso-27001/

[7]*www.**iso**27000.es/sgsi.html*

[8]http://www.monografias.com/trabajos12/recoldat/recoldat.shtml

[9]http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

[10]http://www.auditoriasistemas.com

[11]http://www.monografias.com/trabajos12/condeau/condeau.shtml#PASOS

[12]International Organization for Standardization

[13] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml#ixzz3WB6teL00

[14] https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_III_tecnicas.pdf

[15]Implantación de un SGSI y certificación ISO 27001 en la Administración Pública

[16]http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html

[17]http://www.unsa.edu.ar/sigeco/archivos/semi_material/Apunte%20Software.pdf

[18]http://es.wikipedia.org/wiki/Hardware

[19]http://es.wikipedia.org/wiki/Software

[20] https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_III_tecnicas.pdf

[21] http://www.washington.edu/research/rapid/resources/toolsTemplates/plan_do_check_act.pdf

[22] http://auditordesistemas.blogspot.com/2012/02/analisis-y-evaluacion-de-riesgos.html

[23] http://es.wikipedia.org/wiki/An%C3%A1lisis_de_riesgo_inform%C3%A1tico

[24] http://es.wikipedia.org/wiki/Hardware

[25] http://es.wikipedia.org/wiki/Software

[26] http://revistas.um.es/analesdoc/article/view/2971/2951

[27] http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

[28] http://es.wikipedia.org/wiki/Desastre_natural

[29] http://es.wikipedia.org/wiki/Cracker

[30] http://es.wikipedia.org/wiki/Lamer_%28inform%C3%A1tica%29

[31] **http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.acis.org.co%2Fmemorias%2FJornadasSeguridad%2FIIJNSI%2Fpamplona.doc&ei=A7IiVdvBDcujNv-3gKgH&usg=AFQjCNFakSrKbN2XFGBRRIvlaZ77VA8grA&bvm=bv.89947451,d.cWc**

[32] **http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.acis.org.co%2Fmemorias%2FJornadasSeguridad%2FIIJNSI%2Fpamplona.doc&ei=A7IiVdvBDcujNv-3gKgH&usg=AFQjCNFakSrKbN2XFGBRRIvlaZ77VA8grA&bvm=bv.89947451,d.cWc**

[33] http://auditordesistemas.blogspot.com/2012/02/analisis-y-evaluacion-de-riesgos.html

[34] Federal Information Processing Standards Publications FIPS PUB65 - Guideline for Automatic Data Processing Risk Analysis, 1979

[35] https://protejete.wordpress.com/gdr_principal/control_riesgo/

[36] https://protejete.wordpress.com/gdr_principal/control_riesgo/

[38] Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado Municipal Del Cantón ventanas.

[39] Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado Municipal Del Cantón ventanas.

[40]http://ventanas.gob.ec/municipio/

[41] Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado Municipal Del Cantón ventanas.

[42]**www.ventanas.gob.ec**

[43]https://www.google.com.ec/?gws_rd=ssl#q=+3.+POL%C3%8DTICAS+DE+SEGURIDAD+++3.1+GENERALIDADES+

[44]http://www.monografias.com/trabajos7/sisinf/sisinf.shtml

[45]http://www.eoi.es/blogs/cod/2-tipos-de-informacion/

[46]http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml#ixzz3WB6teL00

[47]https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_III_tecnicas.pdf

[48] Instrucción A.F.I.P. 419/98: I.G. 359/97 (D.P.N.F.). Normas Complementarias. Responsabilidad Profesional de los Auditores Externos. Diferencias significativas en los Estados Contables.

[49] Instrucción A.F.I.P. 419/98: I.G. 359/97 (D.P.N.F.). Normas Complementarias. Responsabilidad Profesional de los Auditores Externos. Diferencias significativas en los Estados Contables.

[50]http://es.wikipedia.org/wiki/Servidor

[51]https://www.google.com.ec/search?q=DIAGRAMA+DE+UN+FIREWALL&biw=1024&bih=634&source=lnms&tbm=isch&sa=X&ei=13xOVLbeMMTCsATThoHIDQ&ved=0CAYQ_AUoAQ

[52]http://es.wikipedia.org/wiki/Servidor_de_archivos

[53]Manual Orgánico Funcional Por Proceso del Gobierno Autónomo Descentralizado Municipal Del Cantón ventanas.

[54]https://www.google.com.ec/?gws_rd=ssl#q=+3.+POL%C3%8DTICAS+DE+SEGURIDAD+++3.1+GENERALIDADES+