



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

CARRERA INFORMÁTICA

**TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN
INFORMÁTICA**

TEMA:

**PLAN DE CONTINGENCIA DE LOS EQUIPOS Y SISTEMAS
INFORMÁTICOS EN EL GOBIERNO AUTÓNOMO
DESCENTRALIZADO MUNICIPAL DEL CANTÓN JUNÍN**

AUTORES:

**RAÚL ALEJANDRO PALACIOS PACHECO
JUAN DIEGO QUIROZ CARRANZA**

TUTOR:

ING. HAROLD MIGUEL BUENAVENTURA AVEIGA

CALCETA, SEPTIEMBRE 2013

DERECHOS DE AUTORÍA

Raúl Alejandro Palacios Pacheco y Juan Diego Quiroz Carranza, declaran bajo juramento que el trabajo aquí descrito es de nuestra autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

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

.....
RAÚL A. PALACIOS PACHECO

.....
JUAN D. QUIROZ CARRANZA

CERTIFICACIÓN DEL TUTOR

Harold Miguel Buenaventura Aveiga, certifica haber tutelado la tesis **PLAN DE CONTINGENCIA DE LOS EQUIPOS Y SISTEMAS INFORMÁTICOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN JUNÍN**, que ha sido desarrollada por Raúl Alejandro Palacios Pacheco y Juan Diego Quiroz Carranza, previa la obtención del título de Ingeniero en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

.....
ING. HAROLD M. BUENAVENTURA AVEIGA

APROBACIÓN DEL TRIBUNAL

Los suscritos integrantes del tribunal correspondiente, declaran que han **APROBADO** la tesis **PLAN DE CONTINGENCIA DE LOS EQUIPOS Y SISTEMAS INFORMÁTICOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN JUNÍN**, que ha sido propuesta, desarrollada y sustentada por Raúl Alejandro Palacios Pacheco y Juan Diego Quiroz Carranza, previa la obtención del título de Ingeniero en Informática, de acuerdo al **REGLAMENTO PARA LA ELABORACIÓN DE TESIS DE GRADO DE TERCER NIVEL** de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López.

.....
ING. DANIEL A. MERA MARTÍNEZ
SECRETARIO

.....
ING. ORLANDO AYALA PULLAS
MIEMBRO DEL TRIBUNAL

.....
ING. RICARDO A. VÉLEZ VALAREZO
PRESIDENTE

AGRADECIMIENTO

En primer lugar estamos infinitamente agradecidos con Dios, por ser el que nos da las fuerzas para afrontar cada una de las tareas que se nos presentan con el pasar de nuestros días.

A nuestros padres por ese apoyo incondicional que nos dieron durante nuestros estudios de pregrado.

A todos y cada uno de los catedráticos que fueron fuente permanente de conocimientos y apoyo académico hacia nosotros.

A la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López que nos dio la oportunidad de formarnos con una educación superior de calidad y en la cual hemos formado nuestros conocimientos profesionales día a día.

LOS AUTORES

DEDICATORIA

El presente trabajo de tesis está dedicado en primer lugar a Dios por darnos fortaleza en cada instante de nuestro transitar por esta prestigiosa institución educativa, en segundo lugar a la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López por formarnos como profesionales capaces de desenvolvemos en el ámbito laboral, dedicamos también esta investigación a nuestras familias quienes fueron pilares fundamentales de nuestro trabajo y a nuestros compañeros por ser parte de este logro.

LOS AUTORES

CONTENIDO GENERAL

CAPÍTULO I. ANTECEDENTES.....	1
1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA.....	1
1.2. JUSTIFICACIÓN	3
1.3. OBJETIVOS	4
1.3.1. OBJETIVO GENERAL	4
1.3.2. OBJETIVOS ESPECÍFICOS.....	4
1.4. IDEAS A DEFENDER.....	5
CAPITULO II. MARCO TEÓRICO	1
2.1. SEGURIDAD INTEGRAL DE LA INFORMACIÓN.....	1
2.2. PLAN DE CONTINGENCIA	1
2.3. DIFERENCIA ENTRE UN PLAN DE CONTINGENCIAS INFORMÁTICAS Y PLAN DE CONTINUIDAD DEL NEGOCIO	3
2.4. RESPALDO	4
2.4.1. RESPALDO INTERNO	4
2.4.2. RESPALDO EXTERNO	5
2.5. LA MATRIZ DE EVALUACIÓN DE RIESGOS.....	6
2.6. LA AMENAZA NATURAL COMO ETIOLOGÍA.....	7
2.6.1. ELEMENTOS PARA LA EVALUACIÓN DE LA AMENAZA	7
2.6.2. CARACTERÍSTICAS DE LA AMENAZA	8
2.7. VULNERABILIDAD.....	9
2.7.1. EVALUACIÓN DE LA VULNERABILIDAD	9
2.8. RIESGOS	9
1. PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS:.....	10
2. IDENTIFICACIÓN DE RIESGOS:	10
3. ANÁLISIS CUALITATIVO DE RIESGOS:.....	10
4. ANÁLISIS CUANTITATIVO DE RIESGOS:	10
5. PLANIFICACIÓN DE LA RESPUESTA A LOS RIESGOS:	11
6. SEGUIMIENTO Y CONTROL DE RIESGOS:	11
2.8.1. EVALUACIÓN DEL RIESGO.....	11
2.8.2. ANÁLISIS DE RIESGO	13
2.8.3. EVALUACIÓN DE RIESGO.....	13
2.8.4. TRATAMIENTO DE RIESGO	14
2.8.5. PARÁMETROS PARA LA EVALUACIÓN DE LOS CONTROLES.	14
2.9. RECUPERACIÓN BÁSICA DE DESASTRES.....	15
2.10. METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT)	16
2.10.1. OBJETIVOS DE MAGERIT	17
2.10.2. IDENTIFICACIÓN DE RIESGOS.....	18
2.10.3. VALORACIÓN DE LAS AMENAZAS.....	19
2.10.4. DETERMINACIÓN DEL IMPACTO	20
2.10.5. DETERMINACIÓN DEL RIESGO.....	20
2.10.6. SALVAGUARDAS.....	21
2.11. ESTÁNDAR ISO 27001	21
CAPÍTULO III. DESARROLLO METODOLÓGICO.....	23
3.1. METODOS CIENTÍFICOS.....	23
3.1.1. ACTIVOS INFORMÁTICOS RELEVANTES DE LA INSTITUCIÓN	24
3.1.2. ANÁLISIS FODA.....	33
3.1.3. IDENTIFICACIÓN DE LOS PROCESOS DE CADA DEPARTAMENTO	35

3.1.4.	IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS	42
3.1.5.	EVALUAR LOS RIESGOS DE TI	73
3.1.6.	ASIGNACIÓN DE PRIORIDADES A LAS APLICACIONES (SI) Y EVALUACIÓN DE LA CRITICIDAD DE LOS PROCESOS DE CADA DEPARTAMENTO	73
3.1.7.	SALVAGUARDAS.....	77
3.2.	ESTRATEGIAS DE CONTINUIDAD DE ACTIVIDADES.....	96
3.2.1.	RESPALDO DE SERVIDORES.....	96
3.2.2.	SERVIDOR DE ARCHIVOS CENTRALIZADO	100
3.2.3.	CONTINGENCIAS PARA LOS SISTEMAS INFORMÁTICOS.....	102
3.2.4.	CORTE DE SUMINISTRO ELECTRICO	106
3.2.5.	CONTINUIDAD DEL SERVICIO INTERNET.....	107
3.2.6.	DESTRUCCIÓN TOTAL DE LAS INSTALACIONES DEL GAD MUNICIPAL DEL CANTÓN JUNÍN.....	109
	CAPÍTULO IV. RESULTADOS Y DISCUSIÓN	111
4.1.	RESULTADOS	111
4.2.	DISCUSIÓN.....	112
	CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES	114
5.1.	CONCLUSIONES.....	114
5.2.	RECOMENDACIONES	115
	BIBLIOGRAFÍA.....	117
	ANEXOS	121

CONTENIDO DE CUADROS Y FIGURAS

Figura 2.1 Principales amenazas e influencias en el Ecuador	2
Figura 2.2. Ejemplo de la matriz de evaluación de riesgos	7
Figura 2.3. Proceso de gestión de riesgo	11
Figura 2.4. Esquema de implementación de controles	15
Cuadro 3.1. Valoración de impactos y riesgos.....	18
Cuadro 3.1. Valor actual de los computadores del GAD Municipal del Cantón Junín según su depreciación.24	
Cuadro 3.2. Valor actual de los computadores tipo servidor del GAD Municipal del Cantón Junín según su depreciación.	25
Cuadro 3.3. Valor actual de los computadores tipo servidor del GAD Municipal del Cantón Junín según su depreciación.	26
Cuadro 3.4. Valor actual de los Sistema De Alimentación Ininterrumpida del GAD Municipal del Cantón Junín según su depreciación.....	27
Cuadro 3.5. Valor actual de los Equipos de Red del GAD Municipal del Cantón Junín según su depreciación.....	27
Figura. 3.1 Diagrama de enlaces inalámbricos exteriores del GADM del Cantón Junín.	28
Cuadro 3.6. Costo Anual de licencias de Software utilizado en el GAD Municipal del Cantón Junín.	29
Cuadro 3.7. Servidores públicos administrativos del GAD Municipal del Cantón Junín clasificados por departamentos.....	30
Figura 3.2. Infraestructura de la planta baja del edificio Municipal del Cantón Junín.	32
Figura 3.3. Infraestructura de la segunda planta del edificio Municipal del Cantón Junín.	32
Cuadro 3.8 Amenaza – Fuego	43
Cuadro 3.9 Amenaza – Daños por Agua	44
Cuadro 3.10 Amenaza – Desastres Naturales.....	44
Cuadro 3.11 Origen Industrial – Fuego	45
Cuadro 3.12 Origen Industrial – Daños por Agua	46
Cuadro 3.13 Origen Industrial – Desastres Industriales	46
Cuadro 3.14 Origen Industrial – Contaminación Mecánica	47
Cuadro 3.15 Origen Industrial – Contaminación Electromagnética	47
Cuadro 3.16 Origen Industrial – Avería de Origen Físico o Lógico.....	48
Cuadro 3.17 Origen Industrial – Corte del Suministro Eléctrico	49
Cuadro 3.18 Origen Industrial – Condiciones Inadecuadas De Temperatura Y/O Humedad.....	49
Cuadro 3.19 Origen Industrial – Fallo De Servicios De Comunicaciones	50
Cuadro 3.20 Origen Industrial – Interrupción De Otros Servicios Y Suministros Esenciales	50
Cuadro 3.21 Origen Industrial – Degradación De Los Soportes De Almacenamiento De La Información.....	51
Cuadro 3.22 Origen Industrial – Emanaciones Electromagnéticas.....	51
Cuadro 3.23 Errores y Fallos No Intencionados – Errores de los Usuarios.....	52
Cuadro 3.24 Errores y Fallos No Intencionados – Errores de Administrador	53
Cuadro 3.25 Errores y Fallos No Intencionados – Errores de Configuración	53
Cuadro 3.26 Errores y Fallos No Intencionados – Diferencias de la Organización	54
Cuadro 3.27 Errores y Fallos No Intencionados – Difusión de Software Dañino.....	55

Cuadro 3.28 Errores y Fallos No Intencionados – Errores de [Re] Encaminamiento.....	55
Cuadro 3.29 Errores y Fallos No Intencionados – Escapes de Información.....	56
Cuadro 3.30 Errores y Fallos No Intencionados – Alteración De La Información.....	56
Cuadro 3.31 Errores y Fallos No Intencionados – Introducción De Información Incorrecta	57
Cuadro 3.32 Errores y Fallos No Intencionados – Degradación De La Información	57
Cuadro 3.33 Errores y Fallos No Intencionados – Destrucción De Información.....	58
Cuadro 3.34 Errores y Fallos No Intencionados – Divulgación De La Información.....	58
Cuadro 3.35 Errores y Fallos No Intencionados – Vulnerabilidades De Los Programas (SOFTWARE).....	59
Cuadro 3.36 Errores y Fallos No Intencionados – Errores De Mantenimiento/Actualización De Programas (Software)	59
Cuadro 3.37 Errores y Fallos No Intencionados – Errores De Mantenimiento/Actualización De Equipos (HARDWARE).....	60
Cuadro 3.38 Errores y Fallos No Intencionados – Caída Del Sistema Por Agotamiento De Recursos	60
Cuadro 3.39 Errores y Fallos No Intencionados – Indisponibilidad Del Personal	61
Cuadro 3.40 Ataques Intencionados – Manipulación de la Configuración.....	62
Cuadro 3.41 Ataques Intencionados – Suplantación de Información del Usuario	62
Cuadro 3.42 Ataques Intencionados – Abusos De Privilegios De Acceso	63
Cuadro 3.43 Ataques Intencionados – Uso No Previsto	63
Cuadro 3.44 Ataques Intencionados – Difusión De Software Dañino	64
Cuadro 3.45 Ataques Intencionados – Acceso No Autorizado	65
Cuadro 3.46 Ataques Intencionados – Análisis De Tráfico	65
Cuadro 3.47 Ataques Intencionados – Repudio	66
Cuadro 3.48 Ataques Intencionados – Intercepción De Información.....	66
Cuadro 3.49 Ataques Intencionados – Modificación De La Información	67
Cuadro 3.50 Ataques Intencionados – Introducción De Falsa Información	67
Cuadro 3.51 Ataques Intencionados – Destrucción A La Información	68
Cuadro 3.52 Ataques Intencionados – Divulgación De La Información.....	68
Cuadro 3.53 Ataques Intencionados – Manipulación de Programas.....	69
Cuadro 3.54 Ataques Intencionados – Robo	69
Cuadro 3.55 Ataques Intencionados – Ataque Destructivo.....	70
Cuadro 3.56 Ataques Intencionados – Ocupación Enemiga.....	71
Cuadro 3.57 Ataques Intencionados – Indisponibilidad Del Personal	71
Cuadro 3.58 Ataques Intencionados – Extorsión.....	72
Cuadro 3.59 Ataques Intencionados – Ingeniería Social.....	72
Tabla 3.1. Priorización de Dependencias Municipales.	76
Tabla 3.2. Determinación de Salvaguardas – Contaminación Mecánica.....	78
Tabla 3.3. Determinación de Salvaguardas – Condiciones Inadecuadas De Temperatura Y/O Humedad.....	78
Tabla 3.4. Determinación de Salvaguardas – Difusión De Software Dañino.	78
Tabla 3.5. Determinación de Salvaguardas – Ingeniería Social	79
Tabla 3.6. Determinación de Salvaguardas – Desastres Industriales	79
Tabla 3.7. Determinación de Salvaguardas – Corte De Suministro Eléctrico	80
Tabla 3.8. Determinación de Salvaguardas – Uso No Previsto	80

Tabla 3.9. Determinación de Salvaguardas – Escape De Información.....	81
Tabla 3.10. Determinación de Salvaguardas – Divulgación De La Información.....	81
Tabla 3.11. Determinación de Salvaguardas – Emanaciones Electromagnéticas.....	81
Tabla 3.12. Determinación de Salvaguardas – Errores De Re-Encaminamiento	82
Tabla 3.13. Determinación de Salvaguardas – Intercepción De Información	82
Tabla 3.14. Determinación de Salvaguardas – Degradación De Los Soportes De Almacenamiento De La Información.....	82
Tabla 3.15. Determinación de Salvaguardas – Daños Por Agua	83
Tabla 3.16. Determinación de Salvaguardas – Avería De Origen Físico O Lógico.....	83
Tabla 3.17. Determinación de Salvaguardas – Introducción De Información Incorrecta.....	84
Tabla 3.18. Determinación de Salvaguardas – Errores De Mantenimiento O Actualización De Programas	84
Tabla 3.19. Determinación de Salvaguardas – Errores Del Administrador.....	84
Tabla 3.20. Determinación de Salvaguardas – Alteración De Información	85
Tabla 3.21. Determinación de Salvaguardas – Divulgación De La Información.....	85
Tabla 3.22. Determinación de Salvaguardas – Errores De Mantenimiento O Actualización De Equipos (Hardware).....	86
Tabla 3.23. Determinación de Salvaguardas – Abuso De Privilegios De Acceso	86
Tabla 3.24. Determinación de Salvaguardas – Extorsión.....	86
Tabla 3.25. Determinación de Salvaguardas – Indisponibilidad Del Personal.....	86
Tabla 3.26. Determinación de Salvaguardas – Interrupción De Otros Servicios Y Suministros Esenciales	87
Tabla 3.27. Determinación de Salvaguardas – Diferencias De La Organización.....	87
Tabla 3.28. Determinación de Salvaguardas – Fallo De Servicios De Comunicaciones	87
Tabla 3.29. Determinación de Salvaguardas – Errores De Los Usuarios	88
Tabla 3.30. Determinación de Salvaguardas – Errores De Configuración	88
Tabla 3.31. Determinación de Salvaguardas – Caída Del Sistema Por Agotamiento De Recursos	89
Tabla 3.32. Determinación de Salvaguardas – Repudio	89
Tabla 3.33. Determinación de Salvaguardas – Indisponibilidad Del Personal.....	89
Tabla 3.34. Determinación de Salvaguardas – Fuego	90
Tabla 3.35. Determinación de Salvaguardas – Manipulación De Información.....	90
Tabla 3.36. Determinación de Salvaguardas – Suplantación De Información Del Usuario	90
Tabla 3.37. Determinación de Salvaguardas – Difusiones De Software Dañino.....	91
Tabla 3.38. Determinación de Salvaguardas – Modificación De La Información	91
Tabla 3.39. Determinación de Salvaguardas – Manipulación De Programas	92
Tabla 3.40. Determinación de Salvaguardas – Ataque Destructivo.....	92
Tabla 3.41. Determinación de Salvaguardas – Ocupación Enemiga.....	92
Tabla 3.42. Determinación de Salvaguardas – Vulnerabilidades De Los Programas (Software)	93
Tabla 3.43. Determinación de Salvaguardas – Acceso No Autorizado	93
Tabla 3.43. Determinación de Salvaguardas – Introducción De Información Falsa	93
Tabla 3.44. Determinación de Salvaguardas – Destrucción De Información.....	94
Tabla 3.45. Determinación de Salvaguardas – Robo	94
Tabla 3.46. Determinación de Salvaguardas – Degradación De La Información	94
Tabla 3.47. Determinación de Salvaguardas – Destrucción De Información.....	95

Tabla 3.48. Determinación de Salvaguardas – Análisis De Tráfico	95
Tabla 3.49. Determinación de Salvaguardas – Contaminación Electromagnética.	95
Tabla 3.50. Presupuesto Referencial para la adquisición de dispositivos de almacenamiento masivo.	97
Figura 3.4. Propuesta de tendido de cable de fibra óptica hacia otro edificio para servidor de respaldo.....	98
Tabla 3.51. Presupuesto Referencial de los sistemas informáticos a utilizar.	99
Tabla 3.52. Servicios de respaldo que ofrece TELCONET. S.A.	100
Figura 3.5. Propuesta de montar un servidor de archivos centralizado en la institución.	101
Figura 3.6. Propuesta de montar un servidor de archivos centralizado en la institución.	102
Tabla 3.53. Presupuesto referencial de los servicios que ofrece PROTELCOTELSA S.A.....	104
Tabla 3.54. Presupuesto referencial para poner en marcha el SIC.....	106
Tabla 3.55. Métodos de acción a seguir en caso de cortes de suministro eléctrico	107
Tabla 3.56. Métodos de acción a seguir con la adquisición de planta generadora de energía eléctrica.....	107
Figura 3.7. Propuesta de contingencia referente al servicio de internet en el edificio del Patronato de Amparo Social.	109
Tabla 3.57. Dependencias Municipales con el número de activos requeridos.	110
Tabla 4.1. Valores de los activos del GAD Municipal del Cantón Junín	111

RESUMEN

Con el objetivo de que el Gobierno Autónomo Descentralizado Municipal del Cantón Junín cuente con un plan de contingencia de los equipos y sistemas informáticos, se realizó el análisis, detección, evaluación y la priorización de amenazas potenciales de las que puede ser víctima la institución, así mismo se priorizó las tareas más relevantes e importantes para la organización. Para lograr este propósito se utilizó MAGERIT debido a que es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, el cual está directamente relacionado con la generalización del uso de los medios electrónicos, informáticos y telemáticos. El producto final contribuye para que la institución conozca sus vulnerabilidades y de esta manera lograr precautelar la integridad de la información y componentes físicos y lógicos con los que se cuenta.

PALABRAS CLAVES

Plan de contingencia, amenazas, MAGERIT, vulnerabilidades.

ABSTRACT

In order for the Municipal Autonomous Decentralized Government of Junín have an contingency plan for equipment and systems, it was performed the analysis, detection, evaluation and prioritization of potential threats that may suffer the institution and at same time prioritized relevance and important to the organization. To achieve this purpose MAGERIT was used because it is a Methodology of Risk Analysis and Management Information Systems, which is directly related to the widespread use of electronic, computer and telematics. The final product contributes to the institution known vulnerabilities and thus achieves to protect the integrity of information and physical and logical components.

KEYWORDS

Contingency Plan, threats, MAGERIT, vulnerabilities.

CAPÍTULO I. ANTECEDENTES

1.1. PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

Antes o después de la ocurrencia de una catástrofe, los gobiernos del mundo entero se ven obligados a utilizar gran parte de los recursos públicos en la prevención de las poblaciones vulnerables, en la reconstrucción de viviendas y en el restablecimiento, en el menor plazo posible, de estructuras vitales para el país o la región afectada. En casos de desastres de gran magnitud, países que carecen de recursos suficientes se ven obligados a pedir ayuda a otros países, a organizaciones internacionales o no-gubernamentales (Szlafsztein, 2006).

Según ETAPA EP (2011), dentro del ámbito de la gestión de riesgos en el Ecuador, el sector educativo tiene especial relevancia dado que las instituciones escolares constituyen la instancia ideal en la que se pueden construir los fundamentos de una cultura de gestión de riesgos; a diferencia de los Gobiernos Autónomos Descentralizados Municipales del Ecuador que no cuentan con un plan de contingencia informático, debido a la falta de conocimientos técnicos y de la normativa vigente de control interno de la Contraloría General del Estado por parte de los profesionales que trabajan en esta área tan importante de la institución, además los administradores de las instituciones públicas generalmente presentan cierta resistencia al momento de realizar una inversión en este tipo de planes por razones económicas, puesto a que los presupuestos son un poco reducidos, sin muchas veces conocer los beneficios que conlleva tener un plan¹ (Anexo 2-A).

Es por esto que los autores de la presente tesis plantearon la posibilidad de crear un plan de contingencia para el Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Junín (Anexo 1-A), que le permita a esta institución mantener un plan sustentable y sostenible para contrarrestar cualquier anomalía o problemas internos o externos de los que puedan ser afectados. Ya que para esta institución, es indispensable recurrir a los recursos informáticos

¹Peñarrieta, D. 2012. Plan de contingencia informático Municipal. (Entrevista).Junín-Manabí. EC. Gobierno Autónomo Descentralizado Municipal del Cantón Junín.

como un medio de proveer información a todos los niveles de la misma, y es de vital importancia que dicha información sea lo más exacta posible.

Por los motivos antes mencionados los autores de la tesis se plantearon la siguiente interrogante.

¿De qué manera se podría contribuir con el GAD Municipal del cantón Junín ante vulnerabilidades informáticas que puedan afectar el normal funcionamiento del mismo?

1.2. JUSTIFICACIÓN

El uso cada vez más creciente de las tecnologías de la información por parte de las diversas instituciones y demás organizaciones, también se refleja en el medio, donde cada vez son más las oficinas, instituciones y entidades sistematizadas, lo que ha dado lugar en la mayoría de los casos a la dependencia de frágiles sistemas informáticos y redes de datos para soportar las funciones más críticas de la actividad institucional; pero lamentablemente no existe una amplia conciencia sobre la importancia de garantizar en la misma medida, la seguridad de los recursos involucrados al trato de la información (INDECI, 2005).

La elaboración de un plan de contingencia ayudó a la institución en la identificación de aquellos sistemas y recursos informáticos que son susceptibles de deterioro, violación o pérdida y que pueden ocasionar graves trastornos para el desenvolvimiento normal de la Institución. Con el propósito de estructurar y ejecutar los procedimientos que admitan una pronta recuperación, así como asignar responsables de salvaguardar los componentes físicos, lógicos y sobre todo la información que permita su recuperación, garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible, brindando un ambiente de tranquilidad y seguridad en cuanto a los activos de Tecnologías de Información (TI) de la institución minimizando los costos en el levantamiento de la información y de los recursos informáticos.

El desarrollo de esta tesis se realizó en base al Reglamento de Tesis del grado de la Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López, el cual regula el proceso de notificación del tema, elaboración de proyecto y desarrollo de la tesis (ESPAM, 2012) con la elaboración de este plan de contingencia se benefició todo el recurso tecnológico y por ende toda la administración municipal en concordancia con los literales f), g) y h) del Artículo 8 de la Ley Orgánica de Educación Superior (LOES, 2010), los mismos que impulsan a la investigación y por ende promueve el desarrollo sustentable.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Elaborar un plan de contingencia para proteger los equipos y sistemas informáticos en el Gobierno Autónomo Descentralizado Municipal del Cantón Junín con el fin de precautelar la información, componentes físicos y lógicos del mismo.

1.3.2. OBJETIVOS ESPECÍFICOS

- Determinar los activos relevantes para la Organización, su interrelación y su valor actual.
- Detectar los riesgos y amenazas tanto físicas como lógicas que puedan causar fallos en el normal funcionamiento de los sistemas de información.
- Definir las actividades de ejecución de las tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- Establecer un plan de recuperación, formación de componentes e instruir al personal, para recuperar la operatividad del sistema en el menor tiempo posible.

1.4. IDEAS A DEFENDER

La elaboración del plan de contingencia informático ayudará sustancialmente a la institución dando una solución alternativa y confiable, ante la eventualidad de todo aquello que pueda paralizar el normal funcionamiento de la misma.

El Plan de Contingencia Informático impactó en la institución, tanto en las funciones como en las responsabilidades.

CAPITULO II. MARCO TEÓRICO

2.1. SEGURIDAD INTEGRAL DE LA INFORMACIÓN

La función del procesamiento de datos es un servicio de toda la institución, que apoya no sólo a los sistemas de información administrativa sino también a las operaciones funcionales. La seguridad es un aspecto de mucha importancia en la correcta Administración Informática, lo es también de toda la Institución.

Las medidas de seguridad están basadas en la definición de controles físicos, funciones, procedimientos y programas que conlleven no sólo a la protección de la integridad de los datos, sino también a la seguridad física de los equipos y de los ambientes en que éstos se encuentren.

En relación a la seguridad misma de la información, estas medidas han de tenerse en cuenta para evitar la pérdida o modificación de los datos, información o software inclusive, por personas no autorizadas, para lo cual se deben tomar en cuenta una serie de medidas, entre las cuales figurarán el asignar números de identificación y contraseñas a los usuarios.

2.2. PLAN DE CONTINGENCIA

Se puede definir a un plan de contingencias como una estrategia planificada con una serie de procedimientos que faciliten tener una solución alternativa que permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total. El Plan de Contingencias de los Sistemas y Equipos Informáticos es una herramienta que le ayudará a que los procesos críticos de una institución continúen funcionando a pesar de una posible falla en los sistemas de información (Lara, 2009).

Todas las organizaciones están expuestas a diversos tipos de riesgos en sus sistemas de información, tanto físicos (fuego, inundación, sabotaje, Entre otros) como lógicos (virus, problemas de seguridad en la información, calidad

de software, almacenamiento de datos inapropiado, entre otros), que pueden paralizar parcial o totalmente la normal actividad de los mismos, con el consiguiente perjuicio para la organización.

Una eventualidad en los sistemas y equipos informáticos tendrá diferente impacto en la organización según la criticidad de los servicios afectados, pudiendo afectar a la supervivencia de la propia institución, si no tiene definidas previamente diversas medidas que minimicen dicho impacto.

El plan de Contingencias se basa en la minimización del impacto que pueda tener un siniestro en los sistemas de informáticos de la compañía, asegurando la continuidad del servicio, la satisfacción del cliente y la productividad a pesar de una catástrofe, tratando de alcanzar una alta disponibilidad para la infraestructura crítica (DPAE, 2009).

Las contingencias afectan a las personas y los medios con los que estas desarrollan su actividad, su trabajo. Es imposible para una institución conocer todos los riesgos y enemigos potenciales en el Ecuador como se muestra en la **figura 2.1**, y sus motivaciones, por lo que una aproximación más acertada es conocer con detalle la organización que se quiere proteger:

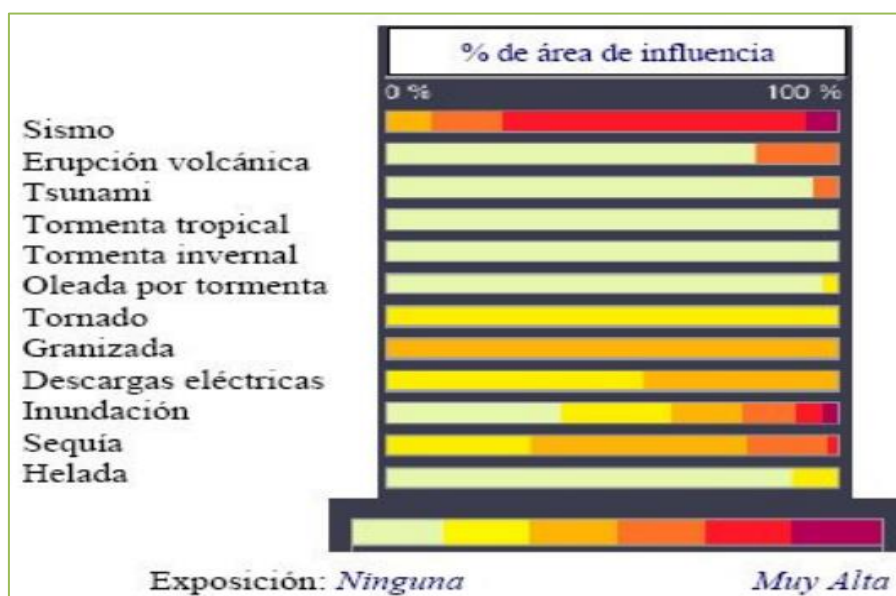


Figura 2.1. Principales amenazas e influencias en el Ecuador
Fuente: Semblantes, 2005.

No sólo se deben identificar los riesgos, también evaluarlos para posteriormente decidir sobre las medidas que puedan mitigarlos. Para ello, deberán identificarse los activos de la institución, así como las debilidades que puedan padecer, estimando probabilidades de ocurrencia y asignándoles una importancia para la misión de la institución, entre los principales activos tenemos.

Organización	= Personas
Objetos, funciones	= Misión
Información	= Datos
Procesos	= Tecnología

En los negocios la tecnología de la información del entorno actual (TI), incluyendo datos, son algunos de los más importantes activos de propiedad de las organizaciones. Los terremotos, ciclones, huracanes, inundaciones, hackers, virus informáticos, sabotaje y ataques terroristas son desastres que amenazan a estos activos. Las organizaciones tienen que estar preparadas y ser capaces para responder a estos ataques. Para asegurar su supervivencia, deben ser capaces de forma rápida recuperar sus datos, continuar sus operaciones y proteger su reputación. Si lo hacen no perderán recursos vitales informáticos que puede aportar que las empresas no cierren sus puertas para siempre. Una planificación eficaz de desastres no es opcional, es crítico para el éxito de las organizaciones. Varios tipos de desastres han causado estragos en los datos valiosos almacenados por empresas de todo el mundo (Al-Badi, *et al.* 2008).

2.3. DIFERENCIA ENTRE UN PLAN DE CONTINGENCIAS INFORMÁTICAS Y PLAN DE CONTINUIDAD DEL NEGOCIO

El ámbito y alcance del primero se concentran en conseguir que las Tecnologías de la Información (TI) y los servicios informáticos se restablezcan, poniendo en funcionamiento el equipo de personal técnico (la organización de contingencia) necesario para ello.

En cambio, en el plan de continuidad también se involucra a las áreas usuarias, teniendo que incluir en las características del centro de respaldo externo la infraestructura necesaria para que los usuarios se conecten a los sistemas de información. Y utilicen los servicios informáticos, así como ampliar la organización de contingencia, además del personal técnico, a personal de las áreas usuarias (organización de continuidad).

Una organización necesita de la suma de los dos para disponer de una cobertura completa, si bien no siempre la naturaleza y gravedad de la contingencia obliga a activar ambos planes (INDRA, 2006).

Según Paton 2004, la gestión de crisis y continuidad del negocio comprende las prácticas que se centran y orientan a las decisiones y las acciones necesarias para prevención, mitigación, preparación, respuesta a, reanudar, recuperar, restaurar y tránsito a partir de un evento de crisis. Por otra parte, se argumentan que este tipo de actividades deben ser en consonancia con sus objetivos estratégicos. Mientras que las empresas no pueden influir en la probabilidad de actividad de los peligros naturales que ocurren, pueden gestionar el riesgo mediante la implementación de estrategias para alterar las consecuencias de actividad de riesgo mediante una mejor planificación y la preparación. Es estas últimas actividades que confieren a un negocio y sus empleados una capacidad de mantener los niveles de funcionamiento durante y después de un desastre y/o acelerar su retorno al normal funcionamiento.

2.4. RESPALDO

2.4.1. RESPALDO INTERNO

Las soluciones de respaldo interno tienen como objeto resolver contingencias leves que no precisen el desplazamiento fuera de los locales donde están ubicados los elementos informáticos afectados (Arias, 2009).

Cuando se trata del respaldo interno, generalmente las soluciones buscan uno o varios de estos objetivos:

- Redundancia de elementos (en ocasiones, disponer de más de un elemento con el fin de sustituir al que deja de funcionar, también puede considerarse como redundancia).
- Evitar los puntos únicos de fallo.
- Alta Disponibilidad.

VENTAJAS

- Solución con un coste moderado.
- No aumenta excesivamente la complejidad de la operativa actual.
- Incrementa la seguridad de los sistemas de información.
- No hace necesario acudir a un centro externo para continuar el funcionamiento.

INCONVENIENTES

- En algún caso el respaldo proporciona un funcionamiento degradado, esto es, que no alcanza el grado de funcionalidad y/o de operatividad que tiene el funcionamiento normal.
- Este tipo de soluciones no soporta contingencias graves, que afecten a la seguridad física de la informática o de las instalaciones donde esta se ubica (DPAE, 2009).

2.4.2. RESPALDO EXTERNO

Tiene como objeto resolver contingencias graves (desaparición del edificio, desaparición del CPD, la avería de una plataforma, etc.), que precisan el desplazamiento a ubicaciones diferentes a la habitual (los denominados centros de respaldos alternativos o CAR).

Estas soluciones se aplican cuando la gravedad de la contingencia es tal que las soluciones de respaldo interno no se pueden aplicar, bien porque no cubran la contingencias, bien porque las instalaciones han quedado inoperantes para su uso.

Para que las soluciones de respaldo externo se apliquen, hay que pasar por un proceso de toma de decisión a lo que se denomina modo contingencia, o lo que es lo mismo, se decide activar el Plan de Contingencias Informáticas (PCI) (Arias, 2009).

VENTAJAS

- Este tipo de soluciones soportan contingencias graves que afecten a la seguridad física de la informática o al lugar donde se encuentran ubicada.
- Con el grado de inversión adecuado, el respaldo puede proporcionar un funcionamiento similar al ordinario.

INCONVENIENTES

- Coste elevado.
- Aumenta la complejidad de la operativa actual: más equipos que mantener y actualizar, desplazamientos, etc. (DPAE, 2009).

2.5. LA MATRIZ DE EVALUACIÓN DE RIESGOS

Permite reconocer eficazmente los riesgos a los que está expuesta la institución o institución y según esta información, poder planificar las acciones que se implementará para reducir los niveles de riesgo existentes y estar mejor preparados para manejar una emergencia o desastre.

Para la construcción de una matriz de evaluación de riesgos, se sigue 4 pasos: descripción del área interna y externa de la institución o institución, dos evaluaciones, una de amenaza y la otra de vulnerabilidad. El resultado de estos tres pasos se conjuga en una sola matriz para construir el primer producto del escenario de riesgos: el Cuadro de Evaluación de Riesgos, que es el cuarto paso (SNR, 2010).

Identificación de la amenaza	Factores de vulnerabilidad	Capacidad de respuesta	Riesgos
SISMO	Construcción del edificio de la CFN no es sismo resistente.	4 Salidas de evacuación. Personal de la Inst. Preparado. Lugar seguro para en caso de evacuación.	Sismo de origen tectónico de 6.5°, la estructura del edificio puede presentar graves daños por las ondas de frecuencia sobre todo en los muros de carga de la mampostería y muros de construcción.
INCENDIO	Existen numerosas instalaciones de energía.	2 extintores por cada piso. Personal técnico capacitado contra incendios.	Incendio por cortocircuito en la zona del bar de los empleados, estallido del tanque de gas; quedando afectado el 5, 6,7 pisos, insuficiente los 2 extintores del piso.

Figura 2.2. Ejemplo de la matriz de evaluación de riesgos
Fuente: SNR, 2010

Es necesario empezar a evaluar la amenaza; es decir responder a las siguientes preguntas y hacer la ponderación de la frecuencia, la intensidad y la cobertura, como se explica a continuación. Para el manejo de riesgos se necesitan: definición de políticas para el manejo de riesgos, inclusión del sistema de control interno y el establecimiento de planes de contingencia (Marulanda; López; Cuesta 2009).

2.6. LA AMENAZA NATURAL COMO ETIOLOGÍA

Es entendida como el peligro latente asociado a un fenómeno de origen natural que puede manifestarse en un sitio específico y durante un periodo determinado, produciendo efectos adversos sobre las personas, sus bienes y el medio ambiente. El impacto potencial de una amenaza natural está normalmente representado en términos de su posible magnitud o intensidad. En términos matemáticos la amenaza está expresada como la probabilidad de ocurrencia de un evento de ciertas características en un sitio determinado y durante un tiempo específico de exposición (Morales y Alfaro, 2008).

2.6.1. ELEMENTOS PARA LA EVALUACIÓN DE LA AMENAZA

La evaluación de la amenaza puede realizarse a partir de responder algunas preguntas básicas y consultar algunas fuentes de información importantes.

Preguntas básicas:

1. ¿Qué tipo de eventos pueden afectarnos o ponernos en riesgo?
2. ¿Cuál es el origen de dichos eventos?
3. Anteriormente, ¿qué eventos han ocurrido en este sector?, ¿en esta institución?, reseña histórica sobre eventos pasados
4. ¿Cómo están relacionados con otras amenazas?
5. ¿Cuál es la frecuencia o recurrencia con que se han presentado en el pasado?
6. ¿Cuál ha sido su intensidad?
7. ¿Cuáles son los lugares o zonas más expuestos al evento?

Una vez respondidas las preguntas anteriores, con la ayuda de las fuentes de información y acudiendo, en caso de ser necesario, a actores sociales, tales como vecinos dueños de locales alrededor de la institución o institución, los funcionarios o empleados más antiguos, etc., la evaluación de la amenaza sólo queda completa al tomar en cuenta tres características principales: la frecuencia de la amenaza, la intensidad de la amenaza y la cobertura de la misma, características que presentan un nivel de ponderación que determina el grado de amenaza. La ponderación se puede efectuar siguiendo estas indicaciones:

2.6.2. CARACTERÍSTICAS DE LA AMENAZA

Frecuencia: Representa el número de veces en el año que ocurre determinada amenaza.

Magnitud: Se refiere a la afectación/suspensión de actividades o funciones de la institución en relación con la amenaza analizada pudiendo ser considerada como: baja, media, alta y muy alta.

Intensidad: Nos permite estimar la fuerza con la que se manifiesta la amenaza, además determinar un porcentaje de área física que se vería afectada por la amenaza analizada.

La identificación de la amenaza se alcanza al analizar la intensidad, cobertura y frecuencia, de la amenaza y se constituye en la primera parte para la construcción del escenario de riesgo.

2.7. VULNERABILIDAD

Grado de resistencia y/o exposición de un elemento o conjunto de elementos frente a la ocurrencia de un peligro. Puede ser física, social, económica, cultural, institucional y otros.

2.7.1. EVALUACIÓN DE LA VULNERABILIDAD

Otro insumo para la construcción del escenario de riesgos, consiste en evaluar la vulnerabilidad. Es importante tener siempre en cuenta que ésta depende de la amenaza, es decir, se dimensiona en función de la amenaza.

Para determinar los factores se debe responder a las siguientes preguntas:

1. Frente a una determinada amenaza, ¿Qué elementos (físicos, económicos, ambientales, sociales) representan fortalezas o debilidades?
2. ¿Cuál es la causa (o causas) de que esto sea así?
3. ¿De estos factores, cuáles son más importantes?

La evaluación de la vulnerabilidad global puede realizarse a partir de identificar los principales factores de vulnerabilidad que la componen y hacer una descripción de la importancia de cada una en las posibles pérdidas que generaría una amenaza determinada.

El Análisis de Vulnerabilidad corresponde a la descripción de cada una de las condiciones relacionadas con los factores de vulnerabilidad según el tipo de amenaza (SNR, 2010).

2.8. RIESGOS

El riesgo es definido como la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular (Peltier, 2001). En lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida (por ejemplo de perder datos debido a ruptura de un disco duro, virus informático, etc.) (Sena y Tenzer, 2004).

La organización internacional por la normalización (ISO) define riesgo tecnológico (guías para la gestión de seguridad de TI/TEC TR 13335-1, 1996) como:

“La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generando pérdidas o daños”.

La Gestión de los Riesgos incluye los procesos relacionados con la planificación de la gestión de riesgos, la identificación y el análisis de riesgos, las respuestas a los riesgos, y el seguimiento y control de riesgos; la mayoría de estos procesos se actualizan periódicamente. Los objetivos de la Gestión de los Riesgos, son aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos adversos a la TI. Un riesgo de un proyecto es un evento o condición inciertos que, si se produce, tiene un efecto positivo o negativo sobre al menos un objetivo de la institución.

Los procesos de Gestión de los Riesgos del Proyecto incluyen lo siguiente:

1. **PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS:** Decidir cómo enfocar, planificar y ejecutar las actividades de gestión de riesgos para un proyecto.
2. **IDENTIFICACIÓN DE RIESGOS:** Determinar qué riesgos pueden afectar al proyecto y documentar sus características.
3. **ANÁLISIS CUALITATIVO DE RIESGOS:** Priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto.
4. **ANÁLISIS CUANTITATIVO DE RIESGOS:** Analizar numéricamente el efecto de los riesgos identificados en los objetivos generales del proyecto.

5. **PLANIFICACIÓN DE LA RESPUESTA A LOS RIESGOS:** Desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.
6. **SEGUIMIENTO Y CONTROL DE RIESGOS:** Realizar el seguimiento de los riesgos identificados, supervisar los riesgos residuales, identificar nuevos riesgos, ejecutar planes de respuesta a los riesgos y evaluar su efectividad a lo largo del ciclo de vida del proyecto (PMBOK, 2011).

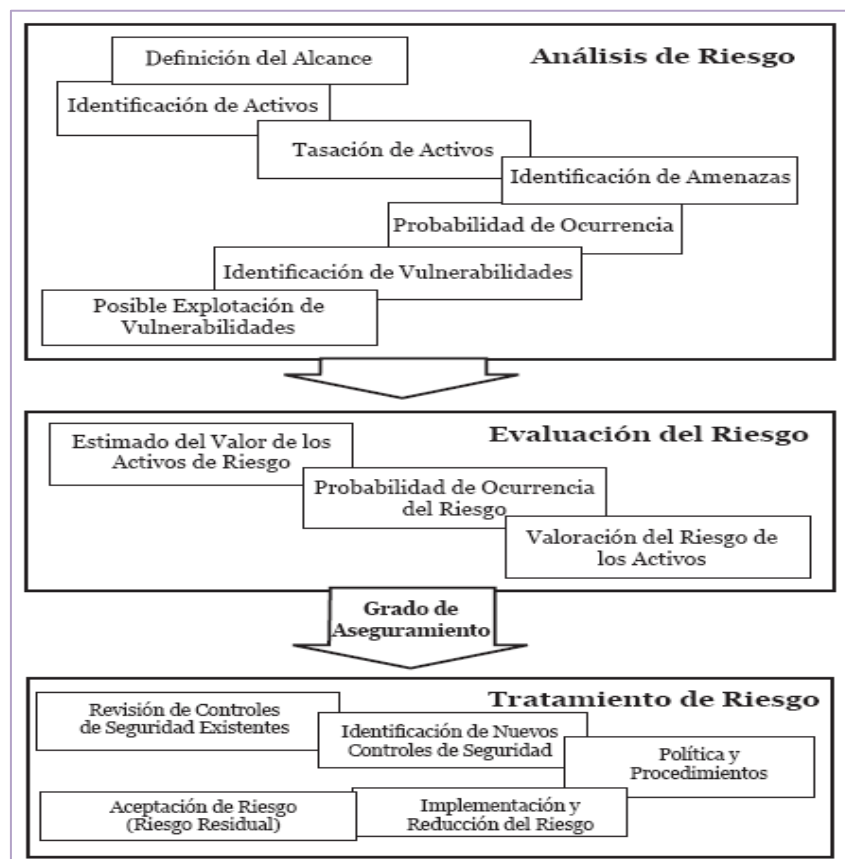


Figura 2.3. Proceso de gestión de riesgo
Fuente: Fleitas, 2009

2.8.1. EVALUACIÓN DEL RIESGO

Conocer el riesgo a los que están sometidos los activos es imprescindible para poder gestionarlos, y por ello han surgido una multitud de guías informales, aproximaciones metódicas y herramientas de soporte las cuales buscan objetivar el análisis para saber cuán seguros (o inseguros) están dichos activos y no llamarse a engaño.

En los actuales momentos la norma ISO 27001:2007, presenta un compendio que proporciona una base común para la elaboración de reglas, un método de gestión eficaz de la seguridad y permite establecer informes de confianza en las transacciones y las relaciones entre instituciones.

La norma ha sido publicada en dos partes:

- ISO/IEC 27002:2007: Código de buenas prácticas para la Gestión de la seguridad de la información;
- ISO/IEC 27001:2007 - BS 7799 Parte 2: Especificaciones relativas a la gestión de la seguridad de la información.

Si la institución no conoce sobre el riesgo que corren sus activos de información, difícilmente llegará a estar preparada para evitar su posible ocurrencia, de allí la importancia de conocerlo y crear controles para disminuir o eliminar su posible ocurrencia.

La ISO 27001:2007 recomienda para llevar a cabo una gestión de riesgo, que se defina primero el alcance del estándar en la institución, y con base en ello, identificar todos los activos de información (Velasco, 2008).

Los activos de información deben ser tasados para identificar su impacto en la organización. Luego se debe realizar un análisis para determinar qué activos están bajo riesgo. Es en ese momento que se deben tomar decisiones en relación a qué riesgos aceptará la organización y qué controles serán implantados para mitigar el riesgo (Alberts y Dorofee, 2003).

A la gerencia le corresponde revisar los controles implantados a intervalos de tiempo regular para asegurar su adecuación y eficacia. Se le exige a la gerencia que controle los niveles de riesgos aceptados y el estado del riesgo residual (que es el riesgo que queda después del tratamiento del riesgo).

El objetivo final de la evaluación de riesgos es realizar un cálculo de las amenazas a los activos de información, con vistas a seleccionar los controles ISO 27002:2007 o ISO 17799:2005 adecuados para mitigar ese riesgo.

2.8.2. ANÁLISIS DE RIESGO

En forma general, el análisis o evaluación de riesgos se define como el proceso de estimar la probabilidad de que ocurra un evento no deseado con una determinada severidad o consecuencias en la seguridad, salud, medio ambiente y/o bienestar público. Asimismo, se deberá elaborar un Plan de Emergencia y Contingencias que permita prevenir y mitigar riesgos, atender los eventos con la suficiente eficacia, minimizando los daños a la comunidad y al ambiente, y recuperarse en el menor tiempo posible.

En una adecuada evaluación se debe considerar la naturaleza del riesgo, su facilidad de acceso o vía de contacto (posibilidad de exposición), las características del sector y/o población expuesta (receptor), la posibilidad de que ocurra y la magnitud de exposición y sus consecuencias, para, de esta manera, definir medidas que minimicen los impactos que puedan generarse. Dentro de este análisis se deben identificar los peligros asociados con los riesgos mencionados, entendiendo a estos peligros como el potencial de causar daño. Los objetivos específicos del análisis de riesgos son los siguientes:

- Identificar y analizar los diferentes factores de riesgo que involucren peligros potenciales que podrían afectar las condiciones socio ambiental de la organización.
- Establecer con fundamento, en el análisis de riesgos, las bases para la preparación del Plan de Emergencia y Contingencias (Brenes, 2007).

2.8.3. EVALUACIÓN DE RIESGO

El proceso de evaluación del riesgo permite a una organización alcanzar los requerimientos del estándar. Este proceso ayuda a cualquier organización que

desea establecer un Sistema de Gestión de la Seguridad de la Información (SGSI).

La evaluación de riesgo es el proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de importancia del riesgo.

El objetivo de esta evaluación es la de identificar y evaluar los riesgos. Los riesgos son calculados por una combinación de valores de activos y niveles de requerimientos de seguridad.

El riesgo se evalúa contemplando tres elementos básicos:

1. Estimado del valor de los activos de riesgo
2. Probabilidad de ocurrencia del riesgo
3. Valoración del riesgo de los activos

2.8.4. TRATAMIENTO DE RIESGO

El tratamiento de riesgo se define, como el conjunto de decisiones tomadas con cada activo de información. El ISO/IEC Guide 73:2002, lo conceptualiza “como el proceso de selección e implementación de medidas para modificar el riesgo”. Las medidas de tratamiento del riesgo pueden contemplar acciones como: evitar, optimizar, transferir o retener el riesgo (Fritalina, 2009).

2.8.5. PARÁMETROS PARA LA EVALUACIÓN DE LOS CONTROLES.

- Administración de los recursos de TI: Para asegurar que la entidad utilice tecnología de información bajo criterios de costo-beneficio, considerando las necesidades de automatización y adecuación de cambios del entorno en que se desenvuelve.
- Seguridad física y seguridad de la información: Para garantizar que el ambiente en que los sistemas funcionan protegen su confidencialidad,

integridad y confiabilidad, la reducción al mínimo del riesgo de que ocurran danos accidentales o intencionales a los equipos.

- Desarrollo y mantenimiento de sistemas de información de la entidad: para garantizar la disponibilidad de los sistemas cuando se necesiten, que se controle la integridad de los datos y que satisfagan a los usuarios.
- Continuidad de SI de la entidad: reducir al mínimo la posibilidad de que ocurra un desastre total y garantizar que el negocio pueda reanudar sus operaciones con efectividad en caso de que ya no se disponga de las instalaciones de procesamiento existentes (Ramírez y Álvarez, 2003).

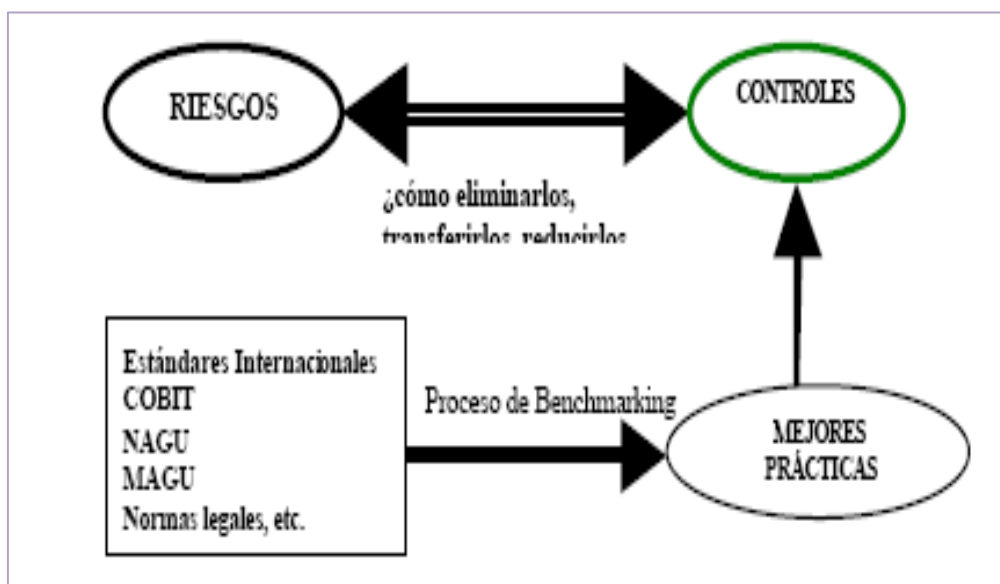


Figura 2.4. Esquema de implementación de controles

Fuente: Ramírez y Álvarez, 2003

2.9. RECUPERACIÓN BÁSICA DE DESASTRES

El riesgo y los efectos de una interrupción imprevista del suministro eléctrico (tiempo de inactividad) para las pequeñas y medianas instituciones actuales crecen con cada nueva aplicación esencial, mejora de la red o actualización del sistema. No tenemos que mirar muy atrás para comprobar las consecuencias de desastres repentinos e imprevistos que afectan a las estructuras informáticas de grandes ciudades e instituciones de todo tipo.

Por consiguiente, los responsables de la tecnología de la información han tenido la tarea, o la tendrán próximamente, de encontrar formas de mitigar, eliminar o reducir, en la medida de lo posible y de forma rentable, los riesgos y los efectos de las interrupciones imprevistas del suministro eléctrico en la institución. Y, lo que es más importante, sus directivos desearán tener la garantía de que sus activos de información, datos y aplicaciones, estarán siempre disponibles pase lo que pase (PBP, 2010).

2.10. METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT)

La CSAE² ha elaborado y promueve MAGERIT³ como respuesta a la percepción de la Administración (y en general toda la sociedad) depende de forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios. El análisis de riesgos se ha consolidado como paso necesario para la gestión de la seguridad. Así se recoge claramente en las guías de la OCDE⁴ que, en su principio número 6 dice.- Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo.

Conocer los riesgos al que están sometidos los sistemas de información con los que se trabaja es imprescindible para poder gestionarlos y por este motivo existen multitud de guías informales para la realización del análisis y gestión de riesgos, aproximaciones metódicas y herramientas de soporte. Todas estas guías (informales, metódicas) buscan poder evaluar cuanto de seguros (o inseguros) están los sistemas de información, para evitar llevarse a engaño.

²CSAE: Consejo Superior de Administración Electrónica

³MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. La información mostrada en este capítulo ha sido obtenida de dicha metodología, elaborada por el Ministerio de Administraciones Públicas.

⁴Guías de la OCDE para la seguridad de los sistemas de información y redes. Hacia una cultura de seguridad. 2002.

Una aproximación metódica no deja lugar a la improvisación, como es el caso de MAGERIT, no depende de la arbitrariedad del analista. El asunto no es tanto conocer la ausencia de incidentes como la confianza en que están bajo control: Se sabe qué puede pasar y se sabe qué hacer cuando pasa.

La primera versión de esta metodología de análisis y gestión de riesgo apareció en el año de 1997, actualmente existe la versión III. El aspecto positivo de esta metodología es que el resultado se expresa en valores económicos mostrando de forma cuantitativa cual podría ser el impacto al negocio en caso que ocurra una eventualidad que pueda paralizar el normal funcionamiento de la institución (Carvajal, 2009).

2.10.1. OBJETIVOS DE MAGERIT

- Concienciar a los responsables de los sistemas de información (dueños del proceso) de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Apoyar la preparación a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

También se ha buscado la uniformidad de los informes que recogen los hallazgos y las conclusiones de un proyecto de análisis y gestión de riesgos:

Modelo de valor

Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos

Relación de las amenazas a que están expuestos los activos.

Evaluación de salvaguardas

Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo

Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias

Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

Plan de seguridad

Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos (MAP, 2006).

2.10.2. IDENTIFICACIÓN DE RIESGOS

La identificación de riesgo se realiza de acuerdo al Cuadro 3.1 valorando así de esta manera los impactos y riesgos de las diferentes amenazas que puedan materializarse sobre los activos del GAD Municipal del cantón Junín, es el siguiente:

Cuadro 3.1. Valoración de impactos y riesgos.

[CÓDIGO] Descripción sucinta de lo que puede pasar										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> Que se puede ver afectado por este tipo de amenazas. 					1. De seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante.					
DESCRIPCIÓN:										
complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
MA	M	A	MA	MA	A	MA	MA	MA	MA	

VALOR	A	B	M	A	IMPACTO	A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
Razón detallada por la cual se considera el impacto y el riesgo de la amenaza en el gobierno autónomo descentralizado municipal del cantón Junín.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

2.10.3. VALORACIÓN DE LAS AMENAZAS

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- **Degradación:** Cuán perjudicado resultaría el activo
- **Frecuencia:** Cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto “totalmente degradado”, o “degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos

100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco frecuente	Cada varios años

2.10.4. DETERMINACIÓN DEL IMPACTO

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del Sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

Para la valoración del impacto, se consideró la siguiente escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- **MB:** muy bajo
- **B:** bajo
- **M:** medio
- **A:** alto
- **MA:** muy alto

2.10.5. DETERMINACIÓN DEL RIESGO

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia (MAP, 2006).

La escala para calificar la frecuencia del riesgo según la metodología Magerit mediante alguna escala sencilla: es la siguiente:

- **MF:** muy frecuente (a diario)

- **F:** frecuente (mensual)
- **FN:** frecuencia normal (anual)
- **PF:** poco frecuente (cada varios años)

2.10.6. SALVAGUARDAS

Las salvaguardas son procedimientos o mecanismos tecnológicos con los cuales se reduce el riesgo en una organización. Las salvaguardas entran en el cálculo del riesgo de dos formas:

- **Reduciendo la frecuencia de las amenazas**

Estas son denominadas salvaguardas preventivas las cuales se aplican antes de que se materialice una amenaza con lo cual se puede cubrir las mismas en su totalidad.

- **Limitando el daño causado**

En este tipo de salvaguardas, en todos los escenarios se materializan las amenazas sobre uno o varios activos, el objetivo de este tipo de salvaguardas es identificar las amenazas y minimizar su impacto para de esa forma limitar sus consecuencias.

Las salvaguardas se miden por su eficacia frente a la amenaza a la cual pretende minimizar su riesgo, la salvaguarda ideal es 100% eficaz lo que implicará que:

- Es teóricamente idónea
- Está perfectamente desplegada, configurada y mantenida
- Se emplea siempre
- Existen procedimientos claros de uso normal y en caso de incidencias
- Los usuarios están formados y concienciados
- Existen controles que avisan de posible fallos (EPN, 2011).

2.11. ESTÁNDAR ISO 27001

El estándar ISO 27001 es una norma reconocida mundialmente para los sistemas de Gestión de Seguridad de la Información (SGSI), la cual indica los

controles a seguir al momento de diseñar e implementar un sistema de seguridad informática.

La certificación de los Sistemas de Gestión de Seguridad de la Información (SGSI) de la norma ISO 27001 está orientada a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las instituciones, de amenazas externas o internas.

El estándar se compone de dos partes:

1. ISO 17799: Guía de controles y buenas prácticas.
2. ISO 27001: Estándar por el que se certifica el SGSI.

El estándar ISO 27001 está formado por varios controles que ayudan a administrar la protección de un activo (físico o intelectual) de una organización, asegurando así el continuo funcionamiento del negocio y la minimización de los daños después de un desastre.

Los controles de seguridad son parte de este estándar, y como cada organización tiene sus propios requerimientos y riesgos podrá escoger todos o algunos de estos controles para lograr la certificación ISO 27001.

Esta norma, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos únicamente organizativos, es decir, organizar la seguridad de la información, por ello se compone de una secuencia de acciones destinadas al establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI (Heras, 2011).

CAPÍTULO III. DESARROLLO METODOLÓGICO

El trabajo de tesis se realizó en el Gobierno Autónomo Descentralizado Municipal del Cantón Junín. El mismo que lo proporcionó de un plan de contingencia para proteger los equipos y sistemas informáticos del mismo con el fin de precautelar la información, componentes físicos y lógicos del mismo, el cual tuvo una duración de nueve meses desde noviembre del 2012 hasta julio del 2013 cumpliendo con el cronograma de actividades propuesto.

3.1. MÉTODOS CIENTÍFICOS

Para el análisis y gestión de riesgos de los sistemas de Información se utilizó MAGERIT, ya que el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se tratan primero los pasos 1, 2, 4 y 5, obviando el paso 3, de forma que las estimaciones de impacto y riesgo sean “potenciales”: caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

En la primera etapa se determinaron los activos relevantes y el análisis FODA para el Gobierno Autónomo Descentralizado Municipal del Cantón Junín, los resultados se obtuvieron realizando un censo de ámbito informático (Anexo 2-C), incluyendo en este: Hardware, software, talento humano y servicios.

3.1.1. ACTIVOS INFORMÁTICOS RELEVANTES DE LA INSTITUCIÓN

3.1.1.1. HARDWARE

El censo se realizó minuciosamente en la parte del hardware tomando en cuenta todos los computadores, impresoras, ups, de cada uno de los departamentos dependientes de esta institución, así como también los dispositivos de la red, y servicios de ámbito informático que posee dicho establecimiento detallándolos de la siguiente manera:

COMPUTADORES

Mediante este censo, una vez analizando los datos, se determinó que el Gobierno Autónomo Descentralizado Municipal Del Cantón Junín, en el área administrativa cuenta con un total de treinta y nueve computadores, los cuales se describen en la siguiente tabla, la información que se muestra en esta detalla los computadores e información correspondiente a compra y precios, determinando el valor actual de los bienes con su respectiva depreciación según la ley y reglamento de régimen tributario interno vigente.

Cuadro 3.1. Valor actual de los computadores del GAD Municipal del Cantón Junín según su depreciación.

COMPUTADORES											
ITEM	DETALLE	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL	AÑO DE COMPRA	MESES DE USO	DEPRECIACION ANUAL	DEPRECIACION MENSUAL	DEPRECIACION ACTUAL	VALOR ACTUAL DEL BIEN	VALOR UNITARIO DEL BIEN
1	INTEL PENTIUM 4 2,8 GHZ	4	504.00	2016.00	2005	90	604.80	50.40	4536.00	201.60	50.40
2	INTEL DUAL CORE 1,80 GHZ	2	725.00	1450.00	2008	58	435.00	36.25	2102.50	145.00	72.50
3	INTEL CORE 2 DUO 3,10 GHZ	1	767.20	767.20	2008	58	230.16	19.18	1112.44	76.72	76.72
4	INTEL PENTIUM DUAL	2	738.08	1476.16	2009	48	442.85	36.90	1771.39	147.62	73.81
5	INTEL DUAL CORE 2,80 GHZ	1	782.88	782.88	2010	36	234.86	19.57	704.59	78.29	78.29
6	INTEL CORE 2 DUO 3,10 GHZ	5	846.72	4233.60	2010	36	1270.08	105.84	3810.24	423.36	84.67
7	INTEL CORE I3 3,0 GHZ	1	800.00	800.00	2010	36	240.00	20.00	720.00	80.00	80.00
8	INTEL CORE I3 3,10 GHZ	4	750.00	3000.00	2011	23	900.00	75.00	1725.00	1275.00	318.75
9	INTEL CORE I3 3,00 GHZ	2	765.00	1530.00	2011	22	459.00	38.25	841.50	688.50	344.25
10	INTEL CORE I7 2,8 GHZ	1	925.00	925.00	2011	24	277.50	23.13	555.00	370.00	370.00
11	INTEL CORE I7 3,00 GHZ	1	980.00	980.00	2011	24	294.00	24.50	588.00	392.00	392.00
12	INTEL CORE I7 3,40 GHZ	1	1058.71	1058.71	2011	24	317.61	26.47	635.23	423.48	423.48
13	INTEL CORE I5 3,20 GHZ	2	919.24	1838.48	2012	22	551.54	45.96	1011.16	827.32	413.66
14	INTEL CORE I3 3,10 GHZ	1	780.00	780.00	2012	22	234.00	19.50	429.00	351.00	351.00
15	HP INTEL CORE I5 3,10 GHZ	10	884.80	8848.00	2012	7	2654.40	221.20	1548.40	7299.60	729.96
16	LAPTOP TOSHIBA INTEL CORE I5 3,40 GHZ	1	1060.00	1060.00	2012	4	318.00	26.50	106.00	954.00	954.00
TOTAL \$										13733.48	

Fuente: Los Autores.

Una vez realizada la respectiva depreciación de los computadores según los precios adquisición se determinó que la instrucción actualmente tiene en computadores \$ 13.733,48 dólares de los Estados Unidos de América.

SERVIDORES

El Gobierno Autónomo Descentralizado Municipal Del Cantón Junín, en el área informática cuenta con un total de cuatro computadores tipo Servidor en óptimo funcionamiento, mismos que sirven para alojar sistemas para los diferentes servicios como:

Cuadro 3.2. Valor actual de los computadores tipo servidor del GAD Municipal del Cantón Junín según su depreciación.

COMPUTADORES TIPO SERVIDORES											
ITEM	DETALLE	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL	AÑO DE COMPRA	MESES DE USO	DEPRECIACION ANUAL	DEPRECIACION MENSUAL	DEPRECIACION ACTUAL	VALOR ACTUAL DEL BIEN	VALOR UNITARIO DEL BIEN
1	Servidor de sistema financiero Olympe Intel pentium D 3,00 GHZ con Windows Server 2003	1	1500.00	1500.00	2009	48	450.00	37.50	1800.00	150.00	150.00
2	Servidor-PC dual core, 4GB Ram, 500GB Disco Duro 2 tarjetas de red con sistema Asterisk - Elastix	1	800.00	800.00	2012	4	240.00	20.00	80.00	720.00	720.00
3	Servidor-PC dual core, 4GB Ram, 500GB Disco Duro 2 tarjetas de red con Endiam Ferewall	1	800.00	800.00	2012	4	240.00	20.00	80.00	720.00	720.00
4	Servidor-PC dual core, 4GB Ram, 500GB Disco Duro 2 tarjetas de red con zimbra	1	1150.00	1150.00	2012	4	345.00	28.75	115.00	1035.00	1035.00
5	Monitor LCD 19" Samsung	1	120.00	120.00	2012	4	36.00	3.00	12.00	108.00	108.00
6	Switch Kvm De 4 Puertos D-link Dkvm-4k	1	80.00	80.00	2012	4	24.00	2.00	8.00	72.00	72.00
TOTAL										\$	2805.00

Fuente: Los Autores.

Una vez realizada la respectiva depreciación de los equipos detallados en el cuadro anterior, pudimos determinar que actualmente tiene servidores por un monto total de \$ 2.805,00 dólares de los Estados Unidos de América

IMPRESORAS

El Gobierno Autónomo Descentralizado Municipal Del Cantón Junín, en el área administrativa cuenta con un total de veintiocho impresoras en funcionamiento,

así mismo las características como precio y año de compra fueron facilitadas por parte del departamento de proveeduría de la institución.

Cuadro 3.3. Valor actual de los computadores tipo servidor del GAD Municipal del Cantón Junín según su depreciación.

IMPRESORAS											
ITEM	DETALLE	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL	AÑO DE COMPRA	MESES DE USO	DEPRECIACION ANUAL	DEPRECIACION MENSUAL	DEPRECIACION ACTUAL	VALOR ACTUAL DEL BIEN	VALOR UNITARIO DEL BIEN (DEPRECIACION)
1	EPSON FX-2180	1	180.00	180.00	2002	120	54.00	4.50	540.00	18.00	18.00
2	CANON MP-190	1	125.00	125.00	2009	48	37.50	3.13	150.00	12.50	12.50
3	SAMSUNG ML-2240	1	150.00	150.00	2010	36	45.00	3.75	135.00	15.00	15.00
4	CANNON 190	1	125.00	125.00	2010	36	37.50	3.13	112.50	12.50	12.50
5	SAMSUNG ML-1860	4	135.00	540.00	2011	24	162.00	13.50	324.00	216.00	54.00
6	SAMSUNG ML-2240	3	154.00	462.00	2011	24	138.60	11.55	277.20	184.80	61.60
7	HP-OFFICEJET PROK8600	1	154.00	154.00	2011	24	46.20	3.85	92.40	61.60	61.60
8	CANON MP-250	1	130.00	130.00	2011	24	39.00	3.25	78.00	52.00	52.00
9	EPSON FX-2190	1	551.04	551.04	2012	9	165.31	13.78	123.98	427.06	427.06
10	RICOH AFICIO MP 206	1	2234.40	2234.40	2012	10	670.32	55.86	558.60	1675.80	1675.80
11	EPSON FX-890	3	430.08	1290.24	2012	8	387.07	32.26	258.05	1032.19	344.06
12	EPSON-L200	10	336.00	3360.00	2012	8	1008.00	84.00	672.00	2688.00	268.80
									TOTAL	\$ 6395.45	

Fuente: Los Autores.

Los cálculos de la depreciación de las impresoras de esta entidad, según los precios en adquisición permitieron determinar el valor que la institución actualmente tiene en impresoras incluyendo en esta familia la copiadora (ricoh aficio MP 206) detallada también en la tabla, es de \$ 6.395,45 dólares de los Estados Unidos de América.

SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA

El Gobierno Autónomo Descentralizado Municipal Del Cantón Junín, cuenta con UPS, que se detallan a continuación tomando en cuenta los datos facilitados por parte del departamento de proveeduría de la institución y estos son:

Cuadro 3.4. Valor actual de los Sistema De Alimentación Ininterrumpida del GAD Municipal del Cantón Junín según su depreciación.

UPS											
ITEM	DETALLE	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL	AÑO DE COMPRA	MESES DE USO	DEPRECIACION ANUAL	DEPRECIACION MENSUAL	DEPRECIACION ACTUAL	VALOR ACTUAL DEL BIEN	VALOR UNITARIO DEL BIEN
1	Ups Thor 600 W	12	40.00	480.00	2010	36	144.00	12.00	432.00	48.00	4.00
2	APC Back-UPS 550VA, 8 outlet	38	78.00	2964.00	2012	6	889.20	74.10	444.60	2519.40	66.30
									TOTAL	\$ 2567.40	

Fuente: Los Autores.

Una vez realizada la respectiva depreciación de los Sistema de alimentación ininterrumpida (UPS) detallados en el cuadro anterior, se determinó que actualmente tiene equipos por un monto total de \$ 2.567,40 dólares de los Estados Unidos de América.

EQUIPOS DE RED

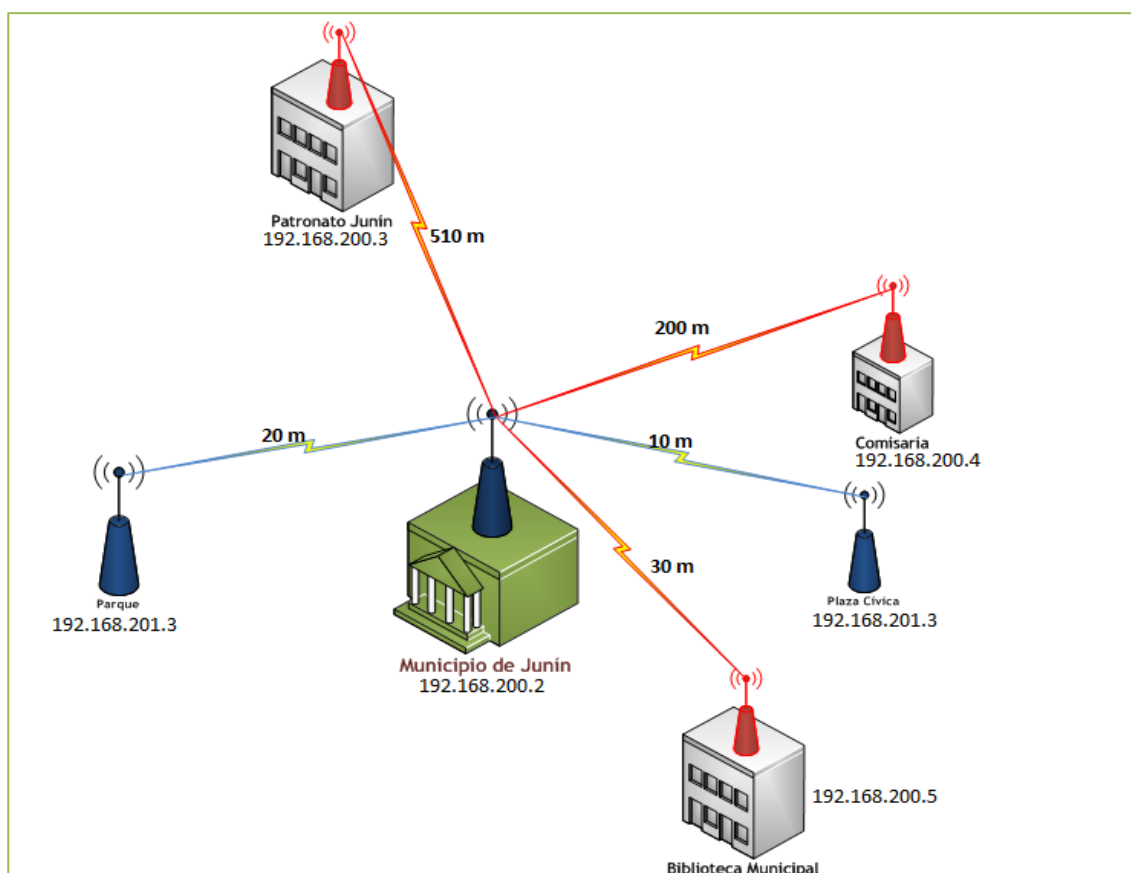
El Gobierno Autónomo Descentralizado Municipal Del Cantón Junín, cuenta con una RED de datos, que comprende el uso de equipos de RED que se detallan a continuación tomando en cuenta los datos facilitados por parte del departamento de proveeduría de la institución y estos son:

Cuadro 3.5. Valor actual de los Equipos de Red del GAD Municipal del Cantón Junín según su depreciación.

EQUIPOS DE RED											
ITEM	DETALLE	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL	AÑO DE COMPRA	MESES DE USO	DEPRECIACION ANUAL	DEPRECIACION MENSUAL	DEPRECIACION ACTUAL	VALOR ACTUAL DEL BIEN	VALOR UNITARIO DEL BIEN (DEPRECIACION)
1	Switch TP-LINK 16 Puertos	1	79.00	79.00	2008	60	23.70	1.98	118.50	7.90	7.90
2	Switch TP-LINK 24 Puertos	1	98.00	98.00	2009	48	29.40	2.45	117.60	9.80	9.80
3	Router QPCOM	1	45.00	45.00	2009	48	13.50	1.13	54.00	4.50	4.50
4	Router D-LINK DIR 600	1	62.50	62.50	2010	36	18.75	1.56	56.25	6.25	6.25
5	Ubiquiti NanoStation2 2.4ghz	2	90.00	180.00	2010	36	54.00	4.50	162.00	18.00	9.00
6	Reloj Biometrico	1	650.00	650.00	2011	22	195.00	16.25	357.50	292.50	292.50
7	Switch TP-LINK 24 PUERTOS	3	89.00	267.00	2012	4	80.10	6.68	26.70	240.30	80.10
8	Análogo IP Gateway GXW4108 8FXO, 2 R.J45 10/100Mbps (LAN/WAN), Video Input	1	641.00	641.00	2012	4	192.30	16.03	64.10	576.90	576.90
9	Ubiquiti NanoStation2 2.4ghz	5	150.00	750.00	2012	4	225.00	18.75	75.00	675.00	135.00
10	Antena Omidireccional 2.4ghz de 15dBi	1	450.00	450.00	2012	4	135.00	11.25	45.00	405.00	405.00
11	Ubiquiti Bullet 2.4ghz 1000mW	1	219.00	219.00	2012	4	65.70	5.48	21.90	197.10	197.10
12	Teléfonos IP GXP285, 2x R.J45 10/100Mbps	24	125.00	3000.00	2012	4	900.00	75.00	300.00	2700.00	112.50
									TOTAL	\$ 5133.25	

FUENTE: Los Autores.

Justificando los equipos detallados en la tabla, el municipio consta con el servicio de telefonía IP, internet, además la institución provee de internet a otras entidades ajenas a ella como son: patronato, biblioteca y comisaria que están ubicados alrededor de la institución mediante enlaces inalámbricos como se muestra en la figura 3.1, realizados mediante antenas Ubiquiti Nano station 2 de 2.4 GHz; además el municipio ofrece internet inalámbrico de forma abierta y para la comunidad en el Parque Central y en la Plaza Cívica del Cantón (Anexos 3-A, 3-B).



10 Figura. 3.1 Diagrama de enlaces inalámbricos exteriores del GAD Municipal del Cantón Junín.

3.1.1.2. SOFTWARE

Se realizó un levantamiento de la información en la parte del Software tomando en cuenta todos los sistemas informáticos utilizados en el GAD Municipal del Cantón Junín, detallándolos de la siguiente manera:

Cuadro 3.6. Costo Anual de licencias de Software utilizado en el GAD Municipal del Cantón Junín.

SOFTWARE				
ITEM	DETALLE	CANTIDAD	LICENCIA	PRECIO ANUAL
1	OLYMPO V7.0	1	DE PAGO ANUAL	5000.00
2	ESET SMART SECURITY 4.2.76.1	50	DE PAGO ANUAL	850.00
3	SIC (Sistema Integral de Catastro)	5	FREE	-
4	ASTERISK (ELASTIX)	1	FREE	-
5	ENDIAM FIREWALL COMUNIDAD 2.5.1	1	FREE	-
6	ZIMBRA 8.0.0_GA_5434	1	FREE	-
7	JOOMLA 2.5	2	FREE	-
8	MICROSOFT OFFICE	39	SIN LICENCIA	-
9	AUTODESK AUTOCAD	8	SIN LICENCIA	-
10	ADOBE CREATIVE SUITE	3	SIN LICENCIA	-
11	WINRAR	39	SIN LICENCIA	-
12	NERO BURNING ROM	39	SIN LICENCIA	-
			TOTAL	5850.00

FUENTE: Los Autores

Una vez realizado el respectivo censo de los sistemas informáticos, se determinó que actualmente el GAD Municipal del Cantón Junín tiene contratados licencias anuales por las cuales cancela un monto total de \$ 5.850,00 dólares de los Estados Unidos de América.

3.1.1.3. TALENTO HUMANO

Después de haber realizado el levantamiento de la información tanto con el hardware como con el software, se procedió a realizar un censo para determinar el número de personas que trabajan en el área Administrativa y por ende están en constante contacto y utilización de los equipos y servicios informáticos con los que cuenta la municipalidad, a continuación se describe lo indicado:

Cuadro 3.7. Servidores públicos administrativos del GAD Municipal del Cantón Junín clasificados por departamentos.

TALENTO HUMANO - ÁREA ADMINISTRATIVA		
ITEM	DEPENDENCIA MUNICIPAL	NUMERO DE EMPLEADOS
1	ALCALDÍA	2
2	TECNOLÓGICO	2
3	SECRETARIA GENERAL	4
4	ASESORÍA JURÍDICA	4
5	COORDINACIÓN INSTITUCIONAL	3
6	DIRECCIÓN DE OBRAS PÚBLICAS	5
7	TESORERÍA	2
8	RECAUDACIÓN	2
9	TALENTO HUMANO	3
10	AUDITORIA INTERNA	2
11	COMPRAS PUBLICAS	2
12	DIRECCIÓN FINANCIERA	2
13	CONTABILIDAD	2
14	PROVEEDURÍA	3
15	DESARROLLO COMUNITARIO	2
16	AVALÚOS Y CATASTRO	3
17	PLANIFICACIÓN Y RIESGO	3
18	PLANEAMIENTO URBANO	3
19	REGISTRO PROPIEDAD	2
	TOTAL	51

FUENTE: Los Autores

El censo realizado determinó que el GAD Municipal del Cantón Junín cuenta con un número total de cincuenta y un servidores públicos en el área administrativa.

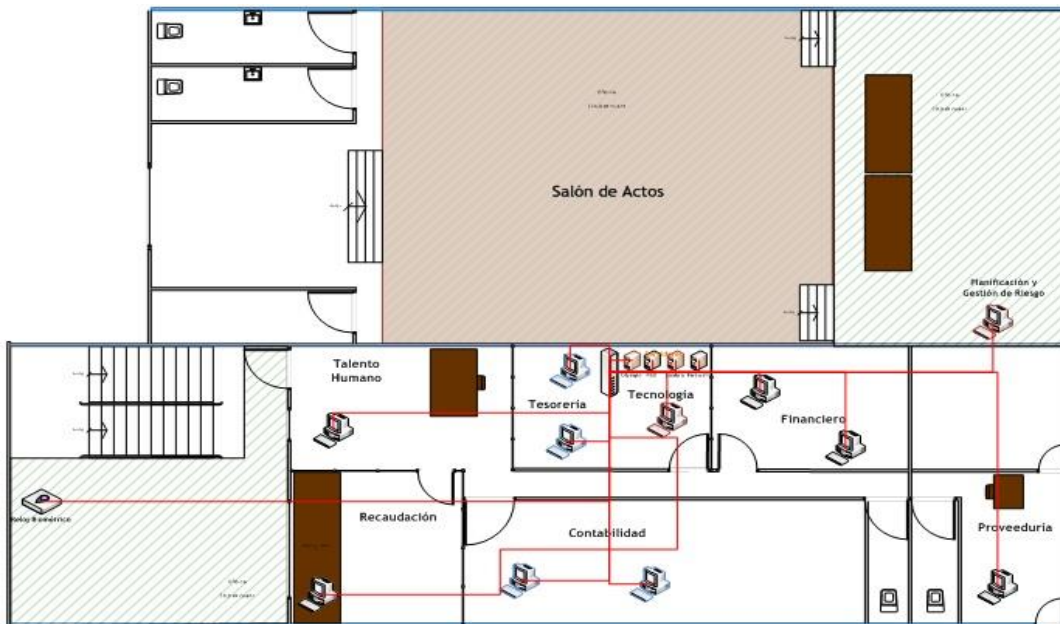
SOPORTES DE INFORMACIÓN

Los soportes de información que son dispositivos de almacenamiento de datos, el GAD Municipal del Cantón Junín no cuenta con un sistema para el respaldo de archivos, sin embargo el Municipio posee dos discos externos que son administrados por el Jefe del Dpto. Tecnológico, y es en ese dispositivos donde se almacena la información.

ESTRUCTURA QUE ACOGE LOS EQUIPOS

Una vez determinado los activos informáticos relevantes del GAD Municipal del cantón Junín mismos que se fueron utilizados para determinar y cuantificar el monto total con el que cuenta la Institución, se procedió a realizar al levantamiento y diseño de la estructura informática del edificio Municipal.

El edificio municipal cuenta con dos plantas distribuidas de la siguiente manera: La planta baja está dividida en 6 oficinas donde funcionan 7 Departamentos Municipales con 10 computadores de escritorios, 2 computadores portátiles y 4 computadores tipo servidores y demás equipos de red, como se puede apreciar en la figura 3.2, siendo estos los departamentos de proveeduría, dirección financiera, contabilidad, tesorería, talento humano, recaudación y el departamento tecnológico (Anexo 2-B) estando ubicados en este último todos los computadores tipo servidores en los cuales se encuentran instaladas las diferentes aplicaciones y sistemas que soportan la estructura tecnológica con la que cuenta el GAD Municipal del Cantón Junín.



13**Figura 3.2.** Infraestructura de la planta baja del edificio Municipal del Cantón Junín.

La segunda planta está dividida en 9 oficinas donde se encuentra la Alcaldía y 13 Departamentos Municipales con 19 computadores de escritorios, 2 computadores portátiles, como se muestra en la figura 3.3.

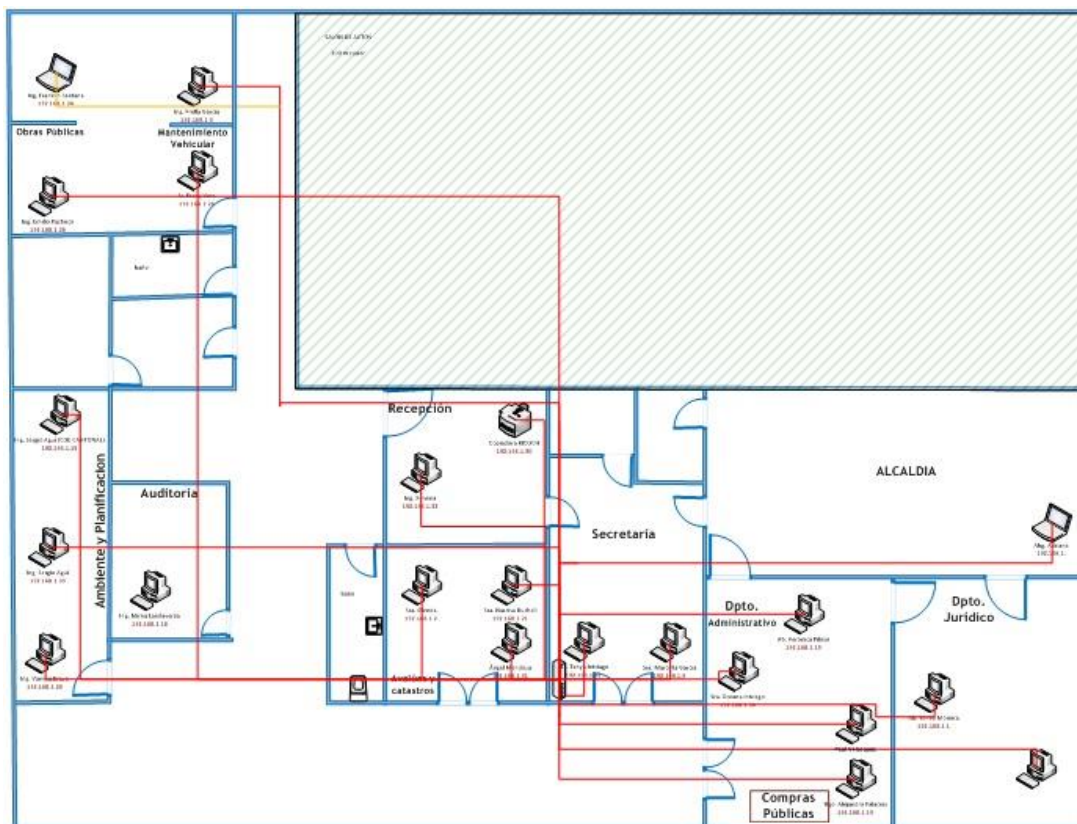


Figura 3.3. Infraestructura de la segunda planta del edificio Municipal del Cantón Junín.

El edificio Municipal del cantón Junín está conformado por 15 oficinas, con una serie de computadores interconectados a través de equipos de red y todos estos poseen el servicio internet. Además cabe recalcar, como se puede observar en las figuras 3.2 y 3.3, que existe aglomeración de departamentos por cada oficina ya que en algunas de estas se encontró hasta dos departamentos municipales.

3.1.2. ANÁLISIS FODA

El análisis FODA se realizó luego de mantener reuniones con el Jefe del Dpto. Tecnológico, mismo que indicó que el GAD Municipal del Cantón Junín no posee ninguno, estas fueron de gran importancia ya que permitieron conocer la realidad de los procesos, el FODA del área informática es el siguiente:

Fortalezas

- ✓ Nivel profesional del Talento humano con el que cuenta el Departamento.
- ✓ Plataforma tecnológica disponible, hardware, software y Comunicaciones.
- ✓ Administración comprometida con el uso de tecnología de punta.
- ✓ Trabajo en equipo, solidaridad y colaboración.
- ✓ Coordinación con la Asociativa de los GAD's, con el Ministerio y Subsecretaría del Ramo.
- ✓ Trabajo comprometido con ética y profesionalismo.
- ✓ Confianza y actitud positiva de los servidores de esta unidad.

Oportunidades

- ✓ Apoyo constante de la Asociativa (AME) con productos tecnológicos y el Ministerio de Telecomunicaciones con Conectividad Global.
- ✓ Capturar inversión extranjera.
- ✓ Cambio de nivel de esta jefatura a nivel de asesoría y toma de decisiones.
- ✓ Sistema de Gestión documental ahorrara recursos económicos a la institución.
- ✓ Propagar el uso del servicio de internet a la colectividad Juninense.

- ✓ Establecer alianzas estratégicas con otras instituciones para mejorar el servicio de la institución.
- ✓ Uso de la Firma Digital.
- ✓ Cambio de aptitud con el uso del internet, mejor aprovechamiento con este servicio.

Debilidades

- ✓ Falta de Capacitación.
- ✓ Problemas de infraestructura de comunicaciones.
- ✓ Carencia de Autonomía en la toma de decisiones y administración de recursos.
- ✓ Inadecuada gestión de incidencias.
- ✓ Área del Departamento compartida e insegura sin climatización.
- ✓ Ausencia de Talento Humano formado en esta rama. Pocos proyectos elaborados.
- ✓ Bajo presupuesto para un periodo fiscal para la adquisición de Hardware, Software, Servicios, Capacitación y Convenios de Cooperación.
- ✓ Falta del Plan de Contingencia Informático.

Amenazas

- ✓ Seguridad de la información ataques de virus, malware, hackers que puedan producirse.
- ✓ Desastres Naturales que puedan provocar afectación a la infraestructura tecnológica.
- ✓ Decisiones Administrativas que afecten la ejecución del Plan Operativo Anual.
- ✓ Resistencia al cambio de software Libre por parte de los empleados municipales.
- ✓ Seguridad Física.
- ✓ Riesgos asociados con la sostenibilidad actual de la plataforma tecnológica.
- ✓ Pérdida de información.

3.1.3. IDENTIFICACIÓN DE LOS PROCESOS DE CADA DEPARTAMENTO

A continuación se detallan los Departamentos con cada una de las actividades que se realizan cotidianamente:

Departamento de Avalúos y Catastros

- ✓ Cobro de títulos de créditos o de las obligaciones (impuestos y tasas)
- ✓ Resolver problemas presentados por las contribuyentes por informalidad de su propiedad registradas en el catastro.
- ✓ Mantener actualizado el catastro de los predios urbanos y rurales.
- ✓ Elaboración de títulos de créditos (alcabalas, patentes, arrendamiento de locales comerciales, arrendamiento de bóvedas, permiso de construcción de bóvedas).
- ✓ Realizar inspecciones de campo urbano y rural.
- ✓ Actualización y digitalización de fichas prediales urbanas y rurales.
- ✓ Controlar el sistema Catastral (SIC).

Departamento de Planeamiento Urbano

- ✓ Planificar el desarrollo de la ciudad
- ✓ Controlar nuevas contribuciones
- ✓ Atender asuntos relacionados con la sala situacional y el COE, sobre desastres naturales
- ✓ Orientar a los ciudadanos con los trámites con las viviendas del MIDUVI
- ✓ Plan regulador de permisos de construcción
- ✓ Aprobación de planos
- ✓ Desmembraciones
- ✓ Cambio de dominio
- ✓ Permiso de conexión de agua servida y potable
- ✓ Inspecciones a terrenos para otorgar certificados antes mencionados

Departamento de Registro de la Propiedad y Mercantil

- ✓ Facturar lo que el usuario va a facturar
- ✓ Inscribir las escrituras
- ✓ Certificados de solvencia
- ✓ Llevar repertorio general o al registro mercantil
- ✓ Revisar archivos e índices para dar petitorio a lo que necesita el usuario

Departamento de Comunicación

- ✓ Coordinar con los medios de comunicación
- ✓ Elaboración de boletines
- ✓ Subir información a la página web de la institución
- ✓ Coordinación de eventos con los departamentos
- ✓ Elaboración de programas
- ✓ Coordinación de agenda de alcaldía
- ✓ Reportajes
- ✓ Encargado del espacio radial municipal

Departamento de Tesorería

- ✓ Realiza transferencias de pago
- ✓ Declaraciones al servicio de rentas internas
- ✓ Devoluciones de IVA
- ✓ Anexos transaccionales
- ✓ Responsable de los depósitos recaudados
- ✓ Responsable de las pólizas de seguro
- ✓ Revisión de roles de pagos y convenios
- ✓ Revisión de valores recaudados
- ✓ Realización de oficios
- ✓ Declaraciones al SRI

Departamento de Medio Ambiente

- ✓ Inspecciones por denuncias y/o rutinas
- ✓ Otorgar permisos ambientales
- ✓ Coordinación con diferentes dependencias municipales para la selección de obras
- ✓ Monitoreo en la ejecución de obras
- ✓ Tramitar licencias ambientales de los proyectos a través de SUIA (Sistema Único de Información Ambiental) del Ministerio del Ambiente.
- ✓ Elaboración de informes PMA, TDR, fichas ambientales.
- ✓ Capacitación en coordinación con técnicos de otras entidades públicas a instituciones educativas.

Departamento de Contabilidad

- ✓ Revisión de información de sustento para realizar el ingreso al sistema OLYMPO
- ✓ Realizar todos los ingresos al sistema OLYMPO en el módulo de Contabilidad
- ✓ Conciliar las cuentas bancarias con el libro banco que arroja el sistema
- ✓ Archivar documentos sustentatorios con los respectivos comprobantes de ingreso y egreso.
- ✓ Revisar roles de pagos antes de ser enviados para su debida cancelación.
- ✓ Subir información contable al sistema ESIGEF del ministerio de Finanzas.
- ✓ Revisar y elaborar estados financieros.
- ✓ Ingreso de rubros al sistema OLYMPO
- ✓ Elaboración de roles de pagos en el sistema OLYMPO
- ✓ Elaboración detallada de los descuentos por convenio
- ✓ Imprimir roles generales y distributivos.
- ✓ Elabora los auxiliares de recaudación y de caja chica para ser ingresados por la Contadora.

Departamento de Recaudación

- ✓ Cobro de impuestos prediales urbanos y rurales a través del Sistema Integral de Catastro (SIC)
- ✓ Cobro de títulos de créditos (varios)
- ✓ Control y ventas de especies valoradas.
- ✓ Arqueo de caja diario
- ✓ Lleva registros de ingresos y egresos de todos los títulos de créditos generados.
- ✓ Encargado de llevar a cabo el proceso de coactiva.
- ✓ Cobro de impuestos por concepto de explotación de canteras.
- ✓ Cobro de impuestos por concepto de uso de la vía pública.

Departamento de Cultura y Turismo

- ✓ Dirigir aspectos culturales y turísticos del Cantón
- ✓ Elaborar proyectos culturales y turísticos
- ✓ Coordina acciones con el Ministerio de Turismo para realizar campañas de promoción turística del Cantón
- ✓ Proveer de información turística del cantón

Dirección de Desarrollo Institucional y Humano

- ✓ Control y seguimiento de los procesos relacionados con la adquisición de bienes.
- ✓ Elaboración anual de Planes, para la organización, planificación y funcionamiento de la Institución.

Dirección de Asesoría Jurídica

- ✓ Representación judicial y extrajudicial al GAD Municipal del Cantón Junín
- ✓ Participar y vigilar de los procesos civiles, penales, laborales y administrativos propuestos contra la misma.
- ✓ Comparecer a las audiencias, tribunales, juzgados, fiscalía e inspectoría.
- ✓ Elaboración de contratos, minutas, resoluciones, convenios entre otros.

Dirección Financiera

- ✓ Realización de los compromisos de las facturas canceladas en el Sistema OLYMPO
- ✓ Control previo de las facturas antes de realizar los pagos
- ✓ Revisión de roles previo a la realización de pago de sueldos
- ✓ Análisis de cuentas pendientes de pago a proveedores
- ✓ Despacho de comunicaciones
- ✓ Análisis de partidas presupuestarias y soluciones
- ✓ Análisis y alimentación de partidas presupuestarias
- ✓ Ingresos, salidas, cambio de nominaciones, consultas e impresiones de planillas del IESS de los servidores públicos de la institución
- ✓ Realización del presupuesto general
- ✓ Revisión de la contabilidad

Departamento de Talento Humano

- ✓ Registro de movimientos de acciones de personal
- ✓ Seguimiento a los procesos de los manuales del GAD Municipal
- ✓ Despacho de comunicaciones

Departamento De Productividad, Competitividad Y Desarrollo Comunitario

- ✓ Emite certificados a agricultores para trámites correspondientes
- ✓ Gestión para la firma de convenios
- ✓ Supervisión y seguimiento de los proyectos productivos y de saneamiento ambiental
- ✓ Supervisión y legalización de terrenos

Comisaría Municipal

- ✓ Despacho de comunicaciones

- ✓ Control de comerciantes en vías públicas conforme a las ordenanzas municipales vigentes

Dirección de Obras Públicas

- ✓ Elaboración de términos de referencia para obras
- ✓ Elaboración de presupuesto referencial para proyectos
- ✓ Elaboración del Plan operativo anual de obras
- ✓ Fiscalización de obras en ejecución y realizadas
- ✓ Elaboración de hojas de ruta para las maquinarias de la Institución.

Departamento de Compras Públicas

- ✓ Dirigir, coordinar y/o ejecutar los procesos precontractuales de contratación y adquisiciones conforme a las disposiciones de la LOSNCP y su Reglamento, así como de las disposiciones internas.
- ✓ Operar la ejecución del Plan Anual de Contrataciones de la institución de acuerdo a la normativa nacional vigente
- ✓ Solicitar en el portal de compras públicas ofertas de bienes, materiales, insumos, repuestos en función de la calidad, cantidad y precios requeridos, de acuerdo a los procedimientos de contratación pública y demás normas legales u ordenanzas establecidas.
- ✓ Mantener la información oportuna al área financiera – contable, asesoría jurídica, áreas técnicas y proveeduría para efectos de los registros legales correspondientes.
- ✓ Participar en la formulación del plan anual de adquisiciones en coordinación con las diferentes dependencias, a efectos de someterla a consideración del Director Financiero para aprobación del Alcalde, que permita por el volumen, abaratar los costos y mantener un stock de productos y materiales de acuerdo a las prioridades de consumo.
- ✓ Elaboración de cuadros mensuales con respecto a las labores del área.
- ✓ Cumplir las disposiciones contenidas en la Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP) y su respectivo Reglamento.

- ✓ Revisar los documentos precontractuales, en coordinación con las diferentes Direcciones y hacer las observaciones que correspondan para que todos los procesos establecidos en la Ley Orgánica del Sistema de Contratación Pública y su Reglamento se cumplan bajo sus disposiciones.
- ✓ Colaborar con la elaboración de los pliegos para las contrataciones (obras, bienes y servicios) que realice el GAD Municipal.
- ✓ Coordinar y apoyar a la administración en los procesos de contratación e informar a la máxima autoridad y/o a la respectiva comisión Técnica sobre el estado de los mismos.
- ✓ Mantener una base de datos actualizada de los procesos de contratación. En digital y físico.
- ✓ Monitorear y presentar informes cuatrimestralmente de los procesos de contratación realizados o ejecutados (PAC).
- ✓ Las demás que le disponga el Alcalde, o su superior jerárquico, con relación a sus funciones.

Departamento Tecnológico

- ✓ Administrar y actualizar la página WEB de la institución, conforme a los requerimientos de las diferentes áreas administrativas, previa evaluación y aprobación.
- ✓ Proporcionar, en el ámbito de su competencia, la información y el soporte necesario para mantener operativa la plataforma tecnológica de la Institución.
- ✓ Participar, en el ámbito de su competencia, en la elaboración y actualización de los manuales de procedimientos e inventarios relacionados con el parque tecnológico.
- ✓ Investigar y evaluar permanentemente los productos y servicios de la tecnología de información, así como los riesgos de la seguridad en la infraestructura informática.
- ✓ Elaborar y presentar los diferentes informes del Departamento que le sean requeridos.
- ✓ Administrar servidores (correo, telefonía e internet), de la institución.

- ✓ Implementa soluciones integrales de cómputo.
- ✓ Creación de correos electrónicos institucional.
- ✓ Administración de red de información y comunicación.
- ✓ Diseño de sitio web de la institución
- ✓ Mantenimiento y soporte para la solución de problemas tanto de hardware como software.
- ✓ Participa en el entrenamiento a usuarios en la operación de los recursos informáticos.
- ✓ Instalación de hardware y software los recursos de las tecnologías de información y comunicación.
- ✓ Instalación puntos de red de tecnologías de información y comunicación.
- ✓ Diseña presentaciones graficas que sean requeridas (portadas, credenciales, etc.)
- ✓ Administración de red de información y comunicación.
- ✓ Creación y entrega de correos electrónicos institucional.
- ✓ Realiza cualquier otra tarea afín que le sea asignada

3.1.4. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a los activos y causar un daño.

Se tomó en cuenta tres clasificaciones principales que puedan haber tales como: accidentes naturales (terremotos, inundaciones), desastres industriales (contaminación, fallos eléctricos) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos, y también existen amenazas causadas por las personas, sean estos errores, o ataques intencionados. Deterioro

La tabla que se utilizó para la valoración de los impactos y riesgos de las diferentes amenazas que puedan materializarse sobre los activos del GAD Municipal del cantón Junín, como se muestra en el Cuadro 2.1.

3.1.4.1. [N] DESASTRES NATURALES

El Planeta se encuentra en constante transformación, sometido a colosales fuerzas tectónicas y cambios atmosféricos drásticos debido a los desastres naturales, en el siguiente apartado se procedió a determinar las amenazas que se pudieran presentar por el motivo antes citado.

Cuadro 3.8 Amenaza – Fuego

[N.1] FUEGO										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar [L] instalaciones 					<ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN:										
Incendios: posibilidad de que el fuego acabe con recursos del sistema.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		B	M	A			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: incendio una amenaza activa										
Según los datos registrados por el cuerpo de bomberos del cantón Junín, los daños por incendio no son frecuentes en el cantón; además hay que tener en cuenta que a un costado del edificio municipal existe una distribuidora de Gas de uso doméstico, que hasta el momento no registra accidente alguno de incendio y el hecho que se materialice esta amenaza afectaría en todos los ámbitos a la institución, incluido el parque tecnológico.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.9 Amenaza – Daños por Agua

[N.2] DAÑOS POR AGUA										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar [L] instalaciones 					<ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN:										
Inundaciones: posibilidad de que el agua acabe con recursos del sistema.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
El departamento tecnológico está ubicado en la parte baja del edificio del gobierno autónomo descentralizado municipal del cantón Junín, es por esta razón que se considera el impacto y un riesgo en esta amenaza, cabe indicar que no se registran datos de inundaciones en este sector del Cantón.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.10 Amenaza – Desastres Naturales

[N.3] DESASTRES NATURALES										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar [L] instalaciones 					<ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN:										
Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, entre otras.										
Se excluyen desastres específicos como incendio e inundaciones.										
Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
	MA	M	A	MA		MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA

VALOR	M	MB	B	M	IMPACTO	M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:

No existe dato alguno que registre cualquier incidencia de estos fenómenos en esta parte del cantón, razón por la cual se determina el impacto y el riesgo de la amenaza en el gobierno autónomo descentralizado municipal del cantón Junín.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

3.1.4.2. [I] DE ORIGEN INDUSTRIAL

Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

Cuadro 3.11 Origen Industrial – Fuego

[I.1] FUEGO										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar [L] instalaciones 					<ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN:										
Incendios: posibilidad de que el fuego acabe con recursos del sistema.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
Según los datos registrados por el cuerpo de bomberos del cantón Junín, los daños por incendio no son frecuentes en el cantón; además hay que tener en cuenta que a un costado del edificio municipal existe una distribuidora de Gas de uso doméstico, que hasta el momento no registra accidente alguno de incendio, es importante recalcar que las instalaciones eléctricas con las cuenta el Municipio de Junín prácticamente cumplieron su ciclo de vida útil; y, el hecho que se materialice esta amenaza afectaría en todos los ámbitos a la institución, incluido el parque tecnológico.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.12 Origen Industrial – Daños por Agua

[I.2] DAÑOS POR AGUA										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar [L] instalaciones 					<ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN:										
Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
En el ámbito industrial se considera que la red de agua potable es igual de antigua como el edificio municipal (25 años), por lo que se ha notado que las reparaciones de esta que se han hecho se las ha tenido que hacer sobrepuesta ya que no existe un plano de esta red de agua en la institución. Además hasta el momento se registra una reparación en este año por tubería perforada con una broca cuando se intentaba realizar un trabajo de red de datos con canaletas.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.13 Origen Industrial – Desastres Industriales

[I.3] DESASTRES INDUSTRIALES										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar [L] instalaciones 					<ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN:										
Otros desastres debido a la actividad humana: explosiones, derrumbes, entre otros. Contaminación química Sobre carga eléctrica, fluctuaciones eléctricas. Accidentes de tráfico										
Se excluyen desastres específicos como incendio e inundaciones.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
	MA	M	A	MA		MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA

VALOR	M	MB	B	M	IMPACTO	M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
 Datos registrados:

- Calentamiento de red eléctrica en el mes de febrero de 2013, no registro datos de daños
- Constantes cortes de fluido eléctrico en el área donde se encuentra ubicada la institución con duraciones mayores de 30 minutos.
- Continuas variaciones del fluido del voltaje de la energía eléctrica
- Cables de tendido eléctrico urbano cerca del edificio

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.14 Origen Industrial – Contaminación Mecánica

[1.4] CONTAMINACIÓN MECÁNICA										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar 					<ol style="list-style-type: none"> 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos 					
DESCRIPCIÓN: Vibraciones, polvo, suciedad, entre otros.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
 El edificio municipal se encuentra ubicado en la arteria principal de la ciudad donde el tráfico es muy constante y además el deterioro de las instalaciones del palacio municipal y además las oficinas no cuentan con un sistema de aislamiento de influencias externas (polvo), provocan que la presencia del polvo y la suciedad sea constante, es por esta razón que los equipos informáticos sufren un gran deterioro producto de la gran cantidad de esta amenaza.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

22Cuadro 3.15 Origen Industrial – Contaminación Electromagnética

[1.5] CONTAMINACIÓN ELECTROMAGNÉTICA									
TIPOS DE ACTIVOS:					DIMENSIONES:				
<ul style="list-style-type: none"> • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información (electromagnéticos) • [AUX] equipamiento auxiliar 					<ol style="list-style-type: none"> 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos 				

DESCRIPCIÓN: Inferencias de radio, campos magnéticos, luz ultravioleta, entre otras.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: Ya que en el cantón Junín no existe un centro o una estación que provoque esta clase de incidentes y por ende la estimación del impacto y del riesgo es muy baja.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.16 Origen Industrial – Avería de Origen Físico o Lógico

[I.6] AVERÍA DE ORIGEN FÍSICO O LÓGICO										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [SW] Aplicaciones (Software) [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar 					<ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN: Fallos en los equipos y/o en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.										
En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: El GAD Junín cuenta con un solo servidor para cada uno de los servicios informáticos que brinda el Municipio a los cliente externos, es decir no existen un plan de contingencia de equipos que suplan la necesidad en caso de que un equipo deje de funcionar, es por esta razón que la estimación del impacto y del riesgo es medio por que afectaría las actividades normales en caso de que ocurra un incidente; es importante indicar desde que el municipio posee estos equipos y sistemas no registran fallos graves de hardware, y de origen lógico si han registrado fallos por falta de administración de estos por parte de los encargados de estos nombrados anteriormente.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo
 PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.17 Origen Industrial – Corte del Suministro Eléctrico

[I.7] CORTE DEL SUMINISTRO ELÉCTRICO										
TIPOS DE ACTIVOS: <ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información (electrónicos) [AUX] equipamiento auxiliar 					DIMENSIONES: <ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN: Cese de la alimentación de potencia.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: <ul style="list-style-type: none"> Calentamiento de red eléctrica febrero de 2013, no registro datos de daños 3 Cortocircuitos registrados que se han reparado en no menos de 1 día Constantes cortes de fluido eléctrico en el área donde se encuentra ubicada la institución con duraciones mayores de 30 minutos. 										

MA muy alto, A alto, M medio, B bajo, MB muy bajo
 PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.18 Origen Industrial – Condiciones Inadecuadas De Temperatura Y/O Humedad

[I.8] CONDICIONES INADECUADAS DE TEMPERATURA Y/O HUMEDAD										
TIPOS DE ACTIVOS: <ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [SI] soportes de información [AUX] equipamiento auxiliar 					DIMENSIONES: <ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN: Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo de calor, excesivo de frío, exceso de humedad, entre otros.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA

	B	MB	MB	B			B	MB	B	M	A
	MB	MB	MB	MB			MB	MB	MB	B	M

MOTIVO:
El Departamento tecnológico se encuentra ubicado en un área cerrada y no cuenta con la debida climatización, para los equipos donde están los servidores tanto del sistema contable como de los demás servicios que posee la institución como son (internet, Telefonía IP, Correo Corporativo, Sistema de catastros), además en el mismo lugar se encuentran otros equipos como switch, router, entre otros equipos de la RED de datos de la institución.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.19 Origen Industrial – Fallo De Servicios De Comunicaciones

[I.9] FALLO DE SERVICIOS DE COMUNICACIONES										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [COM] redes de comunicaciones 					4. [D] disponibilidad					
DESCRIPCIÓN:										
Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción o simple incapacidad para atender al tráfico presente.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
Los equipos de red, se encuentran ubicados en el departamento Tecnológico, además existen otros equipos que están ubicados en otras oficinas donde hay acceso a personas particulares que pueden destruir alguno de estos equipos, es por esta razón que los equipos podrían sufrir algún tipo de manipulación o daños mal intencionados y esto repercutiría en el normal funcionamiento del mismo.										
Según conversaciones mantenidas con el Jefe del Departamento Tecnológico, en estos dos últimos años se han registrados alrededor de 7 fallos de red (colapso) por conexiones de nuevos equipos y clientes de datos.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.20 Origen Industrial – Interrupción De Otros Servicios Y Suministros Esenciales

[I.10] INTERRUPCIÓN DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES									
TIPOS DE ACTIVOS:					DIMENSIONES:				
<ul style="list-style-type: none"> [AUX] equipamiento auxiliar 					1. [D] disponibilidad				
DESCRIPCIÓN:									
Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, entre otros.									
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO				

IMPACTO		DEGRADACION			RIESGO	FRECUENCIA				
		1 %	10 %	100%		PF	FN	F	MF	
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:

Como Institución pública, los trámites para la adquisición de estos insumos y/o repuestos, son un poco tediosos, ya que es todo un proceso que debe de seguirse, y en varias ocasiones se han quedado represados los tramites por fallas administrativas, por lo que esta amenaza ha provocado algunos inconvenientes para el soporte técnico de computadores debido a la escases de los mismos y por ende el retraso en las operaciones

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.21 Origen Industrial – Degradación De Los Soportes De Almacenamiento De La Información

[I.11] DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [SI] soportes de información 					<ol style="list-style-type: none"> [D] disponibilidad [T_S] trazabilidad de los servicios [T_D] trazabilidad de los datos 					
DESCRIPCIÓN:										
Como consecuencia del paso del tiempo.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO	FRECUENCIA				
		1 %	10 %	100%		PF	FN	F	MF	
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
El GAD Municipal de Cantón Junín cuenta con tan solo dos dispositivos de almacenamiento masivo, los cuales son utilizados para el respaldo de la información, y por ende la estimación del impacto es muy alto obviamente el daño de estos dispositivos no ocurre con mucha frecuencia.										
MA muy alto, A alto, M medio, B bajo, MB muy bajo										
PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.										

Cuadro 3.22 Origen Industrial – Emanaciones Electromagnéticas

[I.12] EMANACIONES ELECTROMAGNÉTICAS	
TIPOS DE ACTIVOS:	DIMENSIONES:
<ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones [L] instalaciones 	<ol style="list-style-type: none"> [C] confidencialidad

DESCRIPCIÓN:

Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.

Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.

Esta amenaza se denomina incorrecta pero frecuentemente, ataque TEMPEST (del inglés *“Transient Electromagnetic Pulse Standard”*). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de *“TEMPEST protection”*, queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara.

No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, entre otras, que estarán amenazadas de interceptación.

ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:

El GAD Municipal del cantón Junín provee del servicio de internet gratuito a través de zonas wifi en parque y plaza de la ciudad, y esto se vuelve en un riesgo eminente para la información con la cuenta este Gobierno Municipal.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

3.1.4.3. [E] ERRORES Y FALLOS NO INTENCIONADOS

Fallos no intencionales causados por las personas.

La única numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Cuadro 3.23 Errores y Fallos No Intencionados – Errores de los Usuarios

[E.1] ERRORES DE LOS USUARIOS	
TIPOS DE ACTIVOS: <ul style="list-style-type: none"> [S] Servicios [D] Datos/Información [SW] soportes de información 	DIMENSIONES: <ol style="list-style-type: none"> [I] Integridad [D] Disponibilidad
DESCRIPCIÓN: Equivocaciones de las personas cuando usan los servicios, datos, entre otros.	
ESTIMACIÓN DEL IMPACTO	ESTIMACIÓN DEL RIESGO

IMPACTO		DEGRADACION			RIESGO	FRECUENCIA				
		1 %	10 %	100%		PF	FN	F	MF	
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
El Municipio de Junín cuenta con un personal capacitado que manipulan todos los equipos y sistemas con los que trabaja este GAD, por ende el frecuencia del riesgo por esta amenaza es baja.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.24 Errores y Fallos No Intencionados – Errores de Administrador

[E.2] ERRORES DEL ADMINISTRADOR										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [S] Servicios [D] Datos/Información [SW] soportes de información [HW] equipos informáticos (hardware) [COM] redes de comunicaciones 					<ol style="list-style-type: none"> [I] Integridad [D] Disponibilidad [C] Confidencialidad [A_S] Autenticidad del servicio [A_D] Autenticidad de los datos [T_S] Trazabilidad del servicio [T_D] Trazabilidad de los datos 					
DESCRIPCIÓN: Equivocaciones de personas con responsabilidades de instalación y operación.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO	FRECUENCIA				
		1 %	10 %	100%		PF	FN	F	MF	
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
El administrador de los equipos informáticos es un profesional altamente capacitado en esta área y con vasta experiencia en la manipulación de este tipo de equipos; cabe indicar que existen otros usuarios que alimentan las bases de datos y estos a la vez representan un riesgo potencial en el manejo de la información.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.25 Errores y Fallos No Intencionados – Errores de Configuración

[E.3] ERRORES DE CONFIGURACIÓN										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [S] Servicios [D] Datos/Información [SW] Aplicaciones (software) 					<ol style="list-style-type: none"> [I] Integridad [D] Disponibilidad [C] Confidencialidad [A_S] Autenticidad del servicio 					

<ul style="list-style-type: none"> [HW] equipos informáticos (hardware) [COM] redes de comunicaciones 	<ul style="list-style-type: none"> 5. [A_D] Autenticidad de los datos 6. [T_S] Trazabilidad del servicio 7. [T_D] Trazabilidad de los datos 									
<p>DESCRIPCIÓN: Introducción de datos de configuración erróneos.</p> <p>Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, entre otros.</p>										
ESTIMACIÓN DEL IMPACTO		ESTIMACIÓN DEL RIESGO								
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
<p>MOTIVO: La configuración de los servicios es de exclusiva responsabilidad del administrador del sistema y de los equipos informáticos, y de este depende el normal funcionamiento de las aplicaciones utilizadas en esta institución, donde se hace necesaria el óptimo y eficiente trabajo que realice este funcionario.</p> <p>MA muy alto, A alto, M medio, B bajo, MB muy bajo PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.</p>										

Cuadro 3.26 Errores y Fallos No Intencionados – Diferencias de la Organización

[E.4] DIFERENCIAS DE LA ORGANIZACIÓN										
TIPOS DE ACTIVOS: <ul style="list-style-type: none"> [P] Personal 					DIMENSIONES: <ul style="list-style-type: none"> 1. [D] Disponibilidad 					
<p>DESCRIPCIÓN: Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.</p> <p>Acciones descoordinadas, errores por omisión, entre otras.</p>										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
<p>MOTIVO: La determinación exacta de las funciones de cada servidor público sus alcances y limitaciones, es la clave del éxito en la organización, más aun cuando está de por medio equipos y sistemas informáticos que contribuyen con el normal funcionamiento del Gobierno Municipal.</p> <p>MA muy alto, A alto, M medio, B bajo, MB muy bajo</p>										

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.27 Errores y Fallos No Intencionados – Difusión de Software Dañino

[E.5] DIFUSIÓN DE SOFTWARE DAÑINO										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [SW] Aplicaciones (software) 					<ol style="list-style-type: none"> [I] Integridad [D] Disponibilidad [C] Confidencialidad [A_S] Autenticidad del servicio [A_D] Autenticidad de los datos [T_S] Trazabilidad del servicio [T_D] Trazabilidad de los datos 					
DESCRIPCIÓN:										
Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, entre otros.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
A pesar de que existe un servidor firewall y políticas bien establecidas sobre el uso de dispositivos de almacenamiento masivo externo, esto se vuelve una amenaza latente, para los sistemas informáticos.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.28 Errores y Fallos No Intencionados – Errores de [Re] Encaminamiento

[E.6] ERRORES DE [RE-]ENCAMINAMIENTO										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [S] Servicios [SW] soportes de información [COM] redes de comunicaciones 					<ol style="list-style-type: none"> [I] Integridad [C] Confidencialidad [T_S] Trazabilidad del servicio 					
DESCRIPCIÓN:										
Envío de Información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.										
Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
	MA	M	A	MA		MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA

VALOR	M	MB	B	M	IMPACTO	M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
La utilización de la red para el envío de información es constante en las labores diarias de las dependencias municipales, y esto acarrea una amenaza frecuente ya que debido al cruce de información que existe es mayor el riesgo.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.29 Errores y Fallos No Intencionados – Escapes de Información

[E.7] ESCAPES DE INFORMACIÓN										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [D] Datos/Información [SW] Aplicaciones (software) [COM] redes de comunicaciones 					1. [C] Confidencialidad					
DESCRIPCIÓN:										
La información llega accidentalmente al conocimiento de personas de no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
El constante intercambio de información provocan que el riesgo sea frecuente, y esto implica que cierto tipo de información se vea alterada.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.30 Errores y Fallos No Intencionados – Alteración De La Información

[E.8] ALTERACIÓN DE LA INFORMACIÓN										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [D] Datos/Información 					1. [I] Integridad					
DESCRIPCIÓN:										
Alteración accidental de la información										
Esta amenaza solo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF

VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: La información que se intercambia entre dependencias municipales y sobre todo la información que se encuentra almacenada en diferentes dispositivos el riesgo es medio y con una frecuencia normal. .										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.31 Errores y Fallos No Intencionados – Introducción De Información Incorrecta

[E.9] INTRODUCCIÓN DE INFORMACIÓN INCORRECTA										
TIPOS DE ACTIVOS: • [D] Datos/Información					DIMENSIONES: 1. [I] Integridad					
DESCRIPCIÓN: Inserción accidental de información incorrecta. Esta amenaza solo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: En este tipo de información el riesgo es medio, gracias al control previo de la información, sin embargo el impacto en este tipo de amenaza es muy alto en caso de que ocurra algún tipo de eventualidad.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.32 Errores y Fallos No Intencionados – Degradación De La Información

[E.10] DEGRADACION DE LA INFORMACIÓN										
TIPOS DE ACTIVOS: • [D] Datos/Información					DIMENSIONES: 2. [I] Integridad					
DESCRIPCIÓN: Degradación accidental de información incorrecta. Esta amenaza solo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.										

ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO	FRECUENCIA				
		1 %	10 %	100%		PF	FN	F	MF	
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
 Cuando se cuenta con dispositivos de almacenamiento masivos para respaldar información, existe una amenaza donde la información sufre una degradación, aunque cabe recalcar que es poco frecuente con un riesgo de impacto medio.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.33 Errores y Fallos No Intencionados – Destrucción De Información

[E.11] DESTRUCCION DE INFORMACIÓN										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [D] Datos/Información 					1. [D] disponibilidad					
DESCRIPCIÓN:										
Pérdida accidental de información incorrecta.										
Esta amenaza solo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO	FRECUENCIA				
		1 %	10 %	100%		PF	FN	F	MF	
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
 En este tipo de información el riesgo es medio gracias al control previo de la información, sin embargo el impacto en este tipo de amenaza es medio en caso de que ocurra algún tipo de eventualidad.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.34 Errores y Fallos No Intencionados – Divulgación De La Información

[E.12] DIVULGACIÓN DE LA INFORMACIÓN									
TIPOS DE ACTIVOS:					DIMENSIONES:				
<ul style="list-style-type: none"> [D] Datos/Información 					1. [C] Confidencialidad				

DESCRIPCIÓN: Revelación por indiscreción										
Incontinencia verbal, medios electrónicos, soporte papel, entre otros.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: La mala publicidad afecta a la cualquier institución, es por esta razón que el riesgo de la desinformación es alto pero poco frecuente ya que existe una dependencia municipal encargada de velar la correcta divulgación de la información.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.35 Errores y Fallos No Intencionados – Vulnerabilidades De Los Programas (SOFTWARE)

[E.13] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)										
TIPOS DE ACTIVOS: • [SW] Aplicaciones (software)					DIMENSIONES: 1. [I] Integridad 2. [D] Disponibilidad 3. [C] Confidencialidad					
DESCRIPCIÓN: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: La utilización de software implica tener un riesgo muy alto en la aplicación de estas herramientas, pero sin embargo es poco frecuente el fallo ya que los sistemas que utiliza el GAD Municipal del Cantón Junín son códigos con el debido proceso de desarrollo, ejecución y aplicación de los mismos.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.36 Errores y Fallos No Intencionados – Errores De Mantenimiento/Actualización De Programas (Software)

[E.14] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)
--

TIPOS DE ACTIVOS:				DIMENSIONES:						
<ul style="list-style-type: none"> [SW] Aplicaciones (software) 				<ol style="list-style-type: none"> [I] Integridad [D] Disponibilidad 						
DESCRIPCIÓN:										
Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.										
ESTIMACIÓN DEL IMPACTO				ESTIMACIÓN DEL RIESGO						
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
Los sistemas informáticos con los que trabaja el Municipio de Junín cuentan con el debido soporte en la instalación y puesta en marcha, donde el riesgo de fallo es medio y con una frecuencia normal.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.37 Errores y Fallos No Intencionados – Errores De Mantenimiento/Actualización De Equipos (HARDWARE)

[E.15] ERRORES DE MANTENIMIENTO/ACTUALIZACIÓN DE EQUIPOS (HARDWARE)										
TIPOS DE ACTIVOS:				DIMENSIONES:						
<ul style="list-style-type: none"> [HW] Equipos Informáticos (hardware) 				<ol style="list-style-type: none"> [D] Disponibilidad 						
DESCRIPCIÓN:										
Defectos en los procedimientos y los controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.										
ESTIMACIÓN DEL IMPACTO				ESTIMACIÓN DEL RIESGO						
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
El GAD Municipal del Cantón Junín cuenta con un plan de mantenimiento preventivo de los equipos informáticos, esta tarea la realiza un personal debidamente capacitado, es por esto que el impacto del riesgo es medio con una frecuencia normal.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.38 Errores y Fallos No Intencionados – Caída Del Sistema Por Agotamiento De Recursos

[E.16] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS

TIPOS DE ACTIVOS:				DIMENSIONES:						
<ul style="list-style-type: none"> [S] Servicios [HW] Equipos Informáticos (hardware) [COM] Redes de Comunicaciones 				1. [D] Disponibilidad						
DESCRIPCIÓN:										
La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.										
ESTIMACIÓN DEL IMPACTO				ESTIMACIÓN DEL RIESGO						
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
En esta institucional municipal el riesgo por este tipo de amenazas es bajo y con una frecuencia normal, debido a que los sistemas y los equipos donde está cada uno de estos servicios están en buenas condiciones.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.39 Errores y Fallos No Intencionados – Indisponibilidad Del Personal

[E.17] INDISPONIBILIDAD DEL PERSONAL										
TIPOS DE ACTIVOS:				DIMENSIONES:						
<ul style="list-style-type: none"> [P] Personal Interno 				1. [D] Disponibilidad						
DESCRIPCIÓN:										
Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, entre otros motivos.										
ESTIMACIÓN DEL IMPACTO				ESTIMACIÓN DEL RIESGO						
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
La ausencia del personal dentro de ciertas dependencias municipales es frecuente a pesar de esto el impacto en el riesgo es muy bajo, debido a que los sistemas trabajan de una manera correcta.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

3.1.4.4. [A] ATAQUES INTENCIONADOS

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Cuadro 3.40 Ataques Intencionados – Manipulación de la Configuración

[A.1] MANIPULACIÓN DE LA CONFIGURACIÓN										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [S] Servicios [D] Datos / Información [SW]Aplicaciones (software) [HW] Equipos Informáticos [COM] Redes de comunicaciones 					<ol style="list-style-type: none"> [I] Integridad [C] Confidencialidad [A_S] Autenticación de servicios [A_D] Autenticación de los datos [T_S]Trazabilidad del servicio [T_D]Trazabilidad de los datos [D] Disponibilidad 					
DESCRIPCIÓN:										
Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registros de actividad, encaminamiento, entre otros.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
En este tipo de amenazas el riesgo es bajo y con una frecuencia normal, debido a que solamente personal autorizado manipula la configuración de los equipos y por ende la administración de los sistemas es responsabilidad de un servidor público que hace las veces de custodio de lo indicado.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.41 Ataques Intencionados – Suplantación de Información del Usuario

[A.2] SUPLANTACION DE INFORMACION DEL USUARIO									
TIPOS DE ACTIVOS:					DIMENSIONES:				
<ul style="list-style-type: none"> [S] Servicios [SW]Aplicaciones (software) [COM] Redes de comunicaciones 					<ol style="list-style-type: none"> [C] Confidencialidad [A_S] Autenticación de servicios [A_D] Autenticación de los datos [D] Disponibilidad 				
DESCRIPCIÓN:									
Cuando un ataque consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.									
Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la organización o por personal contratado temporalmente.									

ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
El riesgo es eminente en esta amenaza, debido a que personas mal intencionadas podrían interferir manipulando, extrayendo o destruyendo datos de un alto valor funcional e institucional.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.42 Ataques Intencionados – Abusos De Privilegios De Acceso

[A.3] ABUSOS DE PRIVILEGIOS DE ACCESO										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [S] Servicios [SW]Aplicaciones (software) [HW] Equipos Informáticos [COM] Redes de comunicaciones 					<ol style="list-style-type: none"> [I] Integridad [C] Confidencialidad 					
DESCRIPCIÓN:										
Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
El abuso de los privilegios de acceso se constituye en una amenaza con un impacto de riesgo medio y con una frecuencia de incidencia dentro de los parámetros normales.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.43 Ataques Intencionados – Uso No Previsto

[A.4] USO NO PREVISTO										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [S] Servicios [SW]Aplicaciones (software) [HW] Equipos Informáticos [COM] Redes de comunicaciones [SI] Soporte de Información 					<ol style="list-style-type: none"> [D] Disponibilidad 					

<ul style="list-style-type: none"> [AUX] Equipamiento Auxiliar [L] Instalaciones 										
<p>DESCRIPCIÓN: Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, entre otros.</p>										
ESTIMACIÓN DEL IMPACTO			ESTIMACIÓN DEL RIESGO							
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
<p>MOTIVO: La utilización de recursos del sistema es muy alta y muy frecuente, ya que existen encargados de un equipo que lo utiliza para realizar trabajos personales tales como consultas, impresiones de trabajos entre otros, esto podría derivar a un problema para el departamento de informática y por ende al municipio.</p>										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.44 Ataques Intencionados – Difusión De Software Dañino

[A.5] DIFUSIÓN DE SOFTWARE DAÑINO										
TIPOS DE ACTIVOS:			DIMENSIONES:							
<ul style="list-style-type: none"> [SW]Aplicaciones (software) 			<ol style="list-style-type: none"> [I] Integridad [C] Confidencialidad [A_S] Autenticación de servicios [A_D] Autenticación de los datos [T_S]Trazabilidad del servicio [T_D]Trazabilidad de los datos [D] Disponibilidad 							
<p>DESCRIPCIÓN: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, entre otros.</p>										
ESTIMACIÓN DEL IMPACTO			ESTIMACIÓN DEL RIESGO							
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
<p>MOTIVO: La propagación de esta amenaza afectarían en gran magnitud el normal desempeño de los equipos y sistemas informáticos y esto a su vez significaría un impacto medio en el riesgo con una frecuencia normal.</p>										

MA muy alto, A alto, M medio, B bajo, MB muy bajo
 PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.45 Ataques Intencionados – Acceso No Autorizado

[A.6] ACCESO NO AUTORIZADO										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [S] Servicios [D] Datos / Información [SW]Aplicaciones (software) [HW] Equipos Informáticos (hardware) [COM] Redes de comunicaciones [SI] Soporte de Información [AUX] Equipamiento auxiliar [L] Instalaciones 					<ol style="list-style-type: none"> [I] Integridad [C] Confidencialidad [A_S] Autenticación de servicios 					
DESCRIPCIÓN:										
El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
El compartir información a través de la red de datos, es un potencial riesgo si no se toman las debidas medidas de seguridad, la información puede ser vulnerable ataques de personas no autorizadas, esto conlleva a un riesgo alto debido a que las contraseñas utilizadas generalmente no cumplen con el estándar recomendado para el efecto.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo
 PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.46 Ataques Intencionados – Análisis De Tráfico

[A.7] ANÁLISIS DE TRÁFICO										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [COM] Redes de comunicaciones 					<ol style="list-style-type: none"> [C] Confidencialidad 					
DESCRIPCIÓN:										
El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización del tráfico”.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA

	B	MB	MB	B			B	MB	B	M	A
	MB	MB	MB	MB			MB	MB	MB	B	M
MOTIVO: Se considera que la monitorización en los sistemas informáticos, acarrea un riesgo bajo debido a que el GAD Municipal del cantón Junín no ha sufrido ataques de este tipo.											

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.47 Ataques Intencionados – Repudio

[A.8] REPUDIO											
TIPOS DE ACTIVOS: • [S] Servicios						DIMENSIONES: 1. [T_S]Trazabilidad del servicio					
DESCRIPCIÓN: Negación a posteriores actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente de un mensaje o comunicación Repudio de recepción: negación de haber recibido un mensaje o comunicación Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.											
ESTIMACIÓN DEL IMPACTO						ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA				
		1 %	10 %	100%			PF	FN	F	MF	
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA	
	A	B	M	A		A	M	A	MB	MA	
	M	MB	B	M		M	B	M	A	MA	
	B	MB	MB	B		B	MB	B	M	A	
	MB	MB	MB	MB		MB	MB	MB	B	M	
MOTIVO: La negación de recibir comunicados en una amenaza con un riesgo bajo y con un impacto muy bajo, debido a que este tipo de situaciones no ocurre con frecuencia.											

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.48 Ataques Intencionados – Intercepción De Información

[A.9] INTERCEPCIÓN DE INFORMACIÓN											
TIPOS DE ACTIVOS: • [D] Datos / Información • [SW]Aplicaciones (software) • [HW] Equipos Informáticos • [COM] Redes de comunicaciones						DIMENSIONES: 1. [C] Confidencialidad					
DESCRIPCIÓN: El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.											
ESTIMACIÓN DEL IMPACTO						ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA				
		1 %	10 %	100%			PF	FN	F	MF	
	MA	M	A	MA		MA	A	MA	MA	MA	

VALOR	A	B	M	A	IMPACTO	A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: El acceso a información que no les corresponde a ciertos funcionarios tiene una incidencia frecuente debido al intercambio de información a través de la red de datos.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.49 Ataques Intencionados – Modificación De La Información

[A.10] MODIFICACIÓN DE LA INFORMACIÓN										
TIPOS DE ACTIVOS: • [D] Datos / Información					DIMENSIONES: 1. [I] Integridad					
DESCRIPCIÓN: Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: Esta amenaza es poco frecuente con un impacto de riesgo muy bajo, a pesar de que la información que se comparte es constante, esto se debe a que los funcionarios responsables del manejo de cada una de la información que genera, realizan el control previo tal como lo indica la normativa vigente.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.50 Ataques Intencionados – Introducción De Falsa Información

[A.11] INTRODUCCIÓN DE FALSA INFORMACION										
TIPOS DE ACTIVOS: • [D] Datos / Información					DIMENSIONES: 1. [I] Integridad					
DESCRIPCIÓN: Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF

VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
La inserción de información falsa en las oficinas del GAD Municipal del Cantón Junín, tiene una estimación de riesgo muy baja y poco frecuente, debido a los controles previos que deben de seguir los responsables de cada área.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.51 Ataques Intencionados – Destrucción A La Información

[A.12] DESTRUCCIÓN A LA INFORMACION										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [D] Datos / Información 					1. [D] Disponibilidad					
DESCRIPCIÓN:										
Eliminación intencional de información, con ánimo de obtener beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO:										
En el Municipio de Junín no se registran incidentes de este tipo y por ende es considerado como poco frecuente aunque si esto ocurriera el impacto sería alto.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.52 Ataques Intencionados – Divulgación De La Información

[A.13] DIVULGACIÓN DE LA INFORMACIÓN										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [D] Datos / Información 					2. [C] Confidencialidad					
DESCRIPCIÓN:										
Revelación de Información										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF

VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: La divulgación de la información es muy frecuente en las entidades públicas, pero el riesgo de impacto de bajo debido a que existen normas que determinan el acceso a la información pública.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.53 Ataques Intencionados – Manipulación de Programas

[A.14] MANIPULACIÓN DE PROGRAMAS										
TIPOS DE ACTIVOS: • [SW] Aplicaciones (software)					DIMENSIONES: 1. [C] Confidencialidad 2. [I] Integridad 3. [A_S] Autenticidad del servicio 4. [A_D] Autenticidad de los datos 5. [T_S] Trazabilidad del servicio 6. [T_D] Trazabilidad de los datos					
DESCRIPCIÓN: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: La manipulación de código fuente por parte de personas ajenas a la institución podría provocar un colapso en el trabajo cotidiano y este a su vez convertirse en una amenaza con un riesgo de impacto alto aunque cabe indicar que en Municipio de Junín no ha sufrido ataques de este tipo.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.54 Ataques Intencionados – Robo

[A.15] ROBO										
TIPOS DE ACTIVOS: • [HW] Equipos informáticos (hardware) • [COM] Redes de comunicaciones • [SI] Soportes de información • [AUX] Equipamiento Auxiliar					DIMENSIONES: 1. [D] Disponibilidad 2. [C] Confidencialidad					

MOTIVO:

Los ataques de los que son víctimas las empresas, tienden a ser muy dañinos para toda la organización, sin embargo la estimación del riesgo es muy baja con poca frecuencia.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.56 Ataques Intencionados – Ocupación Enemiga

[A.17] OCUPACIÓN ENEMIGA**TIPOS DE ACTIVOS:**

- [HW] Equipos informáticos (hardware)
- [COM] Redes de comunicaciones
- [SI] Soportes de información
- [AUX] Equipamiento Auxiliar
- [L] Instalaciones

DIMENSIONES:

1. D] Disponibilidad
2. [C] Confidencialidad

DESCRIPCIÓN:

Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

ESTIMACIÓN DEL IMPACTO**ESTIMACIÓN DEL RIESGO**

IMPACTO		DEGRADACION			RIESGO	FRECUENCIA				
		1 %	10 %	100%		PF	FN	F	MF	
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:

Este tipo de amenazas son poco frecuentes con un riesgo de impacto muy bajo, pero con un impacto de degradación muy alto.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.57 Ataques Intencionados – Indisponibilidad Del Personal

[A.18] INDISPONIBILIDAD DEL PERSONAL**TIPOS DE ACTIVOS:**

- [P] Personal interno

DIMENSIONES:

1. D] Disponibilidad

DESCRIPCIÓN:

Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, entre otros.

ESTIMACIÓN DEL IMPACTO**ESTIMACIÓN DEL RIESGO**

IMPACTO		DEGRADACION			RIESGO	FRECUENCIA				
		1 %	10 %	100%		PF	FN	F	MF	
	MA	M	A	MA		MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA

VALOR	M	MB	B	M	IMPACTO	M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
En caso de que ocurra esta amenaza tiene consecuencias perjudiciales para la organización, con un riesgo de impacto alto pero con poca frecuencia.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.58 Ataques Intencionados – Extorsión

[A.19] EXTORSIÓN										
TIPOS DE ACTIVOS:					DIMENSIONES:					
<ul style="list-style-type: none"> [P] Personal interno 					<ol style="list-style-type: none"> [C]Confidencialidad [I] Integridad [A_S] Autenticidad del servicio [A_D] Autenticidad de los datos [T_S] Trazabilidad del servicio [T_D] Trazabilidad de los datos 					
DESCRIPCIÓN:										
Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MB	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M

MOTIVO:
Esta amenaza es un riesgo con impacto medio y poco frecuente debido a que estos hecho no ocurren con frecuencia debido a que se trata de una institución gubernamental de servicio a la colectividad.

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

Cuadro 3.59 Ataques Intencionados – Ingeniería Social

[A.20] INGENIERÍA SOCIAL									
TIPOS DE ACTIVOS:					DIMENSIONES:				
<ul style="list-style-type: none"> [P] Personal interno 					<ol style="list-style-type: none"> [C]Confidencialidad [I] Integridad [A_S] Autenticidad del servicio [A_D] Autenticidad de los datos [T_S] Trazabilidad del servicio [T_D] Trazabilidad de los datos 				

DESCRIPCIÓN: Abuso de la buena fe de las personas para que realicen las actividades que interesan a un tercero.										
ESTIMACIÓN DEL IMPACTO					ESTIMACIÓN DEL RIESGO					
IMPACTO		DEGRADACION			RIESGO		FRECUENCIA			
		1 %	10 %	100%			PF	FN	F	MF
VALOR	MA	M	A	MA	IMPACTO	MA	A	MA	MA	MA
	A	B	M	A		A	M	A	MA	MA
	M	MB	B	M		M	B	M	A	MA
	B	MB	MB	B		B	MB	B	M	A
	MB	MB	MB	MB		MB	MB	MB	B	M
MOTIVO: Esta amenaza es un riesgo constante porque al ser una entidad pública el acceso a personas ajenas o no a la institución es constante, y estas pueden hacer uso de esa confianza para sustraer información relevante para la institución de cualquiera de los departamentos.										

MA muy alto, A alto, M medio, B bajo, MB muy bajo

PF poco frecuente, FN frecuencia normal, F frecuente, MF muy frecuente.

3.1.5. EVALUAR LOS RIESGOS DE TI

Es necesaria la evaluación de la seguridad de los sistemas de información, tanto internamente como parte de los procesos de gestión, como por medio de evaluadores independientes externos. Las evaluaciones permiten medir el grado de confianza que merece o inspira un sistema de información, La evaluación de los riesgos de la tecnología de la información puede llevar a una certificación o registro de la seguridad del sistema. En la práctica se certifican productos y se certifican todos los sistemas de gestión de la seguridad.

3.1.6. ASIGNACIÓN DE PRIORIDADES A LAS APLICACIONES (SI) Y EVALUACIÓN DE LA CRITICIDAD DE LOS PROCESOS DE CADA DEPARTAMENTO

Después de que acontezca un desastre y se inicie la recuperación de los sistemas, debe conocerse qué aplicaciones recuperar en primer lugar. No hay que perder el tiempo restaurando los datos y sistemas equivocados cuando la actividad de la empresa necesita primero sus aplicaciones esenciales para así de esta manera poder seguir brindado un servicio de calidad a toda la colectividad.

El GAD Municipal del Cantón Junín cuenta con aproximadamente 25 departamentos, que colaboran día a día con el desarrollo de la cantón y con la atención al usuario; toda empresa cuenta con dependencias unas más relevantes que otras, indispensables para poner en marcha la institución en caso de que ocurra un desastre.

Para el caso de esta Institución Pública se tomaron en cuenta criterios de orden jerárquico conforme al organigrama estructural (Anexo 4-A) y a la relevancia de los procesos que realizan cada una de estas; y, así de esta manera continuar con las obligaciones y la razón de ser de acuerdo al Art. 31 del Código Orgánico de Organización Territorial Autonomía y Descentralización.

Después de haber realizado la investigación correspondiente y haber conocido las funciones de cada uno de los departamentos, se procede a realizar la evaluación utilizando los criterios descritos en el párrafo anterior, las dependencias municipales que se priorizaron son las siguientes:

1. Tecnología de la Información y Comunicación
2. Dirección Financiera
3. Compras Públicas
4. Obras Públicas
5. Recaudación – Avalúos y Catastro
6. Asesoría Jurídica

1.- Tecnología de la Información y Comunicación.- El Departamento de Tecnología de Información y Comunicación, esta dependencia es la encargada de brindar soporte técnico informático a todo el Municipio, otra de las tareas relevantes es la administrar todos los servidores con los que cuenta el Municipio, estos son los siguientes: Internet, Telefonía IP, Correo corporativo (Mail), sistema contable financiero OLYMPO de la dirección financiera y el Sistema Integral de Catastros (SIC) del departamento de Avalúos y catastros, el sitio web de la institución, red de datos y soporte técnico a los equipos informáticos de la institución que comprenden software, hardware.

2.- Dirección Financiera.- El GAD Municipal del Cantón Junín cuenta con la dirección financiera y esta a su vez comprendida por los departamentos de contabilidad, Presupuesto y tesorería; esta dirección es la encargada de administrar todos los recursos económicos de la municipalidad, cabe recalcar que para llevar un buen control de estos recursos se debe garantizar al resto de la empresa una información constante y en la forma correcta, para que sea útil a la hora de tomar las diferentes decisiones que surjan a lo largo de la administración municipal, una herramienta informática que se utiliza para dicha labor es el sistema contable financiero OLYMPO, este es utilizado por el Municipio desde el año 2008 ejecutándose sobre un servidor IBM.

3.- Compras Públicas.- El departamento de compras públicas es otro de las dependencias fundamentales al momento de hacer alguna contratación de obras, servicios o adquisición de bienes para la institución, como también para cualquier proceso que se esté llevando a cabo en beneficio del cantón, este departamento si se sirve de la plataforma informática que es el portal de compras públicas, donde se encuentran todos los procesos de contratación y es accesible desde cualquier computador que tenga una conexión a internet, pero la documentación que genere cada uno de estos procesos reposa solo de forma física en los archivos de este departamento.

4.- Obras Públicas.- El departamento de Obras Públicas es de gran importancia para la institución, este se encarga de atender las necesidades de los habitantes de este cantón tanto del sector urbano y en especial al sector rural, además este departamento esta soportado informáticamente con computadores e impresoras, pero cabe recalcar que no usa un sistema informático específico para el control y registro de obras realizadas, por lo que toda la documentación se la mantiene en físico, desde el año en que se fundó esta institución municipal.

5.- Recaudación – Avalúos Y Catastros.- El departamento de Recaudación que tiene estricta relación con el departamento de Avalúos Y Catastros, son de gran importancia porque están en directa atención con los habitantes del cantón, además estos son los responsables de recaudar los impuestos de los

predios tanto urbanos como rural del cantón Junín; el sistema que utiliza es el sistema integral de catastros (SIC), donde se encuentra soportada toda la información catastral del cantón.

6.- Asesoría Jurídica.- El departamento Jurídico es de gran importancia en toda entidad pública porque este es el encargado de representar judicial y extrajudicialmente al GAD Municipal del Cantón Junín, además este también se encarga de la elaboración de contratos, minutas, resoluciones, convenios, los llevados a cabo de la contratación de obras, empleados y demás actividades detalladas en el apartado anterior de las actividades por departamentos, este así mismo no cuenta con un sistema informático específico para el control y registro de actividades realizadas por este departamento, por lo que toda la documentación se la mantiene en documentos físico y respaldadas una parte de forma digital en los computadores que prestan servicios en esta dependencia.

Nombre del Departamento	Funcionamiento	
	Software Utilizado	Hardware Utilizado
Dirección Financiera	Internet, OLYMPO V7	Red de datos,2 Computadores de escritorio e impresora
Compras Públicas	Internet, Software utilitario	Red de datos, Computador de escritorio e impresora
Obras Públicas	Internet, Software utilitario, AutoCad	Red de datos, Computador de escritorio e impresora
Recaudación – Avalúos Catastros	Sistema Integral de Catastro SIC	Red de datos, Computador de escritorio e impresora
Asesoría Jurídica	Internet, Software utilitario	Red de datos, Computador de escritorio e impresora

Tabla 3.1. Priorización de Dependencias Municipales.

En caso de que se materialice una amenaza las dependencias municipales que tienen que ser intervenidas en el menor tiempo posible son las que se detallan en la **tabla 3.1** con el fin de poner en marcha provisionalmente las labores de la institución; estos departamentos son denominados prioridad uno es decir en el caso de que se materialice una amenaza estos departamentos se intervendrían de una manera inmediata, con el fin de poner en marcha las labores diarias en

el menor tiempo posible, es tal su importancia que sin estas en GAD dejaría de brindar servicio a los usuarios y de no obtendría ingresos económicos por concepto de cobros que se realizan a través del recaudación.

Es importante recalcar que otro departamento que intervendría de manera directa y contundente es Tecnología de la Información y Comunicación, porque este tendría la labor de poner en marcha todos los servicios utilizados en el Municipio de Junín; este realizaría soporte técnico informático, pondría en marcha todos los servicios.

3.1.7. SALVAGUARDAS

Las salvaguardas a establecer han sido seleccionadas teniendo en cuenta los atributos del bien y la información a proteger (confidencialidad, integridad y disponibilidad). En la selección de las salvaguardas se consideraron las características de la amenaza, la vulnerabilidad o probabilidad de materialización y el impacto o daño producido por una potencial amenaza.

En las tablas se describe cada una de las amenazas incluido en este el código y el riesgo intrínseco, además se determina la o las salvaguardas para cada una de estas y el costo monetario que esta implica.

AMENAZAS			SALVAGUARDAS		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
14	CONTAMINACION MECANICA	308440,96	Utilizar brazos hidráulicos en las puertas de acceso, es de mucha importancia ya que estos mantendrán las puerta cerradas	1568,00	42622,00
			Limpieza especializada de las oficinas, este tipo de actividad se encarga de remover todo el polvo con máquinas apropiadas para dicha labor y así de esta manera todo el polvo que se acumula sea extraído por estos equipos y no afecten a los sistemas informáticos	1054,00	

			Acondicionamiento de las oficinas, en la actualidad el GAD del Cantón Junín cuenta con un edificio que data de la época de los 80's y es necesario el acondicionamiento de las oficinas ya que estas han incrementado en número y obviamente en el personal que ahí labora.	40000,00	
--	--	--	---	----------	--

Tabla 3.2. Determinación de Salvaguardas – Contaminación Mecánica.

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
18	CONDICIONES INADECUADAS DE TEMPERATURA Y/O HUMEDAD	32848,96	Climatización de las oficinas, para ofrecer un ambiente de trabajo más agradable ya que las oficinas actualmente no cuentan en su totalidad con equipos para la climatización	7200,00	7280,00
			Optima climatización del Dpto. Tecnológico, para evitar el sobrecalentamiento de los equipos que se encuentra asilados en esta dependencia y que soportan todos los servicios informáticos de la institución	80,00	

Tabla 3.3. Determinación de Salvaguardas – Condiciones Inadecuadas De Temperatura Y/O Humedad.

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E5	DIFUSION DE SOFTWARE DAÑINO	32848,96	Mantenimiento del ESET ENDPOINT SECURITY que es el antivirus con el que actualmente cuenta la institución actualizado con sus respectivas licencias, para minimizar el riesgo de infiltraciones de programas no deseados en los sistemas de información y demás computadores y equipos de almacenamiento y de comunicación.	1200,00	1200,00
			Dar una correcta administración al servidor ENDIAN FIREWALL con el que cuenta la institución el cual ayuda a la administración y distribución del ancho de banda de internet y así mismo este permite bloquear sitios de poca confianza que puedan traer consigo este tipo de software		
			Crear una política para análisis y desinfección de cualquier dispositivo de almacenamiento, antes de insértala en cualquier computador de la institución para prevenir infecciones de estos y de la red de datos del municipio		

Tabla 3.4. Determinación de Salvaguardas – Difusión De Software Dañino.

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A20	INGENIERIA SOCIAL	29199,25	Restringir el acceso a personas no autorizadas ya que estas actúan de forma normal y podrían hacer mal uso de documentos o de información relevante para la institución		1245,00
			Dotar a las oficinas con archivadores seguros, para así de esta forma tener documentos a buen recaudo y seguros ante cualquier ingreso de personas mal intencionado que busquen hacer daño a la institución.	1245,00	

Tabla 3.5. Determinación de Salvaguardas – Ingeniería Social

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
13	DESASTRES INDUSTRIALES	29199,08	Se deben adoptar medidas adicionales específicas para el control de acceso de terceras partes		17965,00
			Climatización de las oficinas, para ofrecer un ambiente de trabajo más agradable ya que las oficinas actualmente no cuentan en su totalidad con equipos para la climatización	7200,00	
			Mantenimiento constante a la red de cableado eléctrico, como hemos indicado el edificio de GAD Municipal ya tiene varios años de construcción y por ende muchos de las estructuras de cableado eléctrico ya cumplieron con su ciclo de vida útil por ende es necesario el cambio de este sistema	10765,00	
			Se deberá preparar y mantener operativo un plan de contingencias.		

Tabla 3.6. Determinación de Salvaguardas – Desastres Industriales

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
17	CORTE DE SUMINISTRO ELÉCTRICO	25549,19	Mantenimiento constante a la red de cableado eléctrico, como hemos indicado el edificio de GAD Municipal ya tiene varios años de construcción y por ende muchos de las estructuras de cableado eléctrico ya cumplieron con su ciclo de vida útil por ende es necesario el cambio de este sistema	10765,00	49965,00

			Repotenciar el sistema eléctrico del GAD Municipal, debido al crecimiento de dependencias a las que ha sido víctima el Municipio este sistema debe de ser repotenciado para así de esta manera satisfacer con las necesidades de electricidad de todos los equipos	7200,00	
			Adquirir una planta generadora de electricidad, que en el caso de que el fluido de energía sea suspendido por cualquier inconveniente esta se ponga en marcha y así el GAD no paralice sus actividades	32000,00	

Tabla 3.7. Determinación de Salvaguardas – Corte De Suministro Eléctrico

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A4	USO NO PREVISTO	25549,19	Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		0,00
			Política de autenticación y acceso a la información, de esta manera se sabrá a ciencia cierta los usuarios que están acezando a la información		
			Asignar responsabilidades en el manejo de los datos a los usuarios, están responsabilidades tendrán un perfil de manejo de la información		
			Restringir el acceso a los usuarios a páginas con fines de ocio		

Tabla 3.8. Determinación de Salvaguardas – Uso No Previsto

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E7	ESCAPE DE INFORMACION	18249,42	Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		1200,00
			Se debe asignar responsabilidad del manejo de los datos a los usuarios los cuales tienen un perfil para el manejo de la información.		
			El Administrador del Sistema deberá llevar un control actualizado y seguro de los datos, evitando duplicidad de los mismos.		

			Mantenimiento del ESET ENDPOINT SECURITY que es el antivirus con el que actualmente cuenta la institución actualizado con sus respectivas licencias, para minimizar el riesgo de infiltraciones de programas no deseados en los sistemas de información y demás computadores y equipos de almacenamiento y de comunicación.	1200,00	
			Establecer manuales de respaldo y duplicados de los sistemas, programas y archivos.		

Tabla 3.9. Determinación de Salvaguardas – Escape De Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A13	DIVULGACION DE LA INFORMACION	18249,42	Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		0,00
			Difusión de políticas de seguridad educando a los usuarios y conviértalos en sus mejores aliados, esto implicara proteger la calidad de los servicios y acceso a los datos de no se degradada o negada sin la autorización correcta.		

Tabla 3.10. Determinación de Salvaguardas – Divulgación De La Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
I12	EMANACIONES ELECTROMAGNÉTICAS	14599,54	Mantenimiento a los servidores web, este se debe de realizar periódicamente y de esta manera cumplir con las políticas y procedimientos de seguridad de la institución		0,00
			Fomentar políticas de seguridad, de esta manera proteger el sistema contra aquellas amenazas que aplican a las tecnologías empleadas		
			Aplicar protocolos y normas internacionales de seguridad aplicada a los sistemas y servidores web de la Institución		

Tabla 3.11. Determinación de Salvaguardas – Emanaciones Electromagnéticas

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO

					\$
E6	ERRORES DE RE-ENCAMINAMIENTO	10949,65	Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente entre otras cosas los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		500,00
			Capacitación a los usuarios de la red de datos, de esta manera se educa al personal en el manejo adecuado de la misma.	500,00	

Tabla 3.12. Determinación de Salvaguardas – Errores De Re-Encaminamiento

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A9	INTERCEPCIÓN DE INFORMACIÓN	10949,65	Aplicar protocolos y normas internacionales de seguridad aplicada a los sistemas y servidores web de la Institución		0,00
			El jefe del Dpto. Tecnológico será el responsable de tomar las decisiones de seguridad sobre todos los Sistemas y servicios informáticos que operan en el GAD		

Tabla 3.13. Determinación de Salvaguardas – Intercepción De Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
I11	DEGRADACIÓN DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACIÓN	7402,58	Respaldo de la información, es de suma importancia el Backup de la información en la nube esto ayudará en el inmediata recuperación del dato y por ende en la pronta utilización del mismo	0,00	600,00
			Utilización de nuevos y modernos dispositivos de almacenamiento masivo sean estos discos duros externos, flash memory y/o CD; esto servirá para tener a disposición en cualquier momento le información y sobre todo respaldada la información en varios medios	600,00	

Tabla 3.14. Determinación de Salvaguardas – Degradación De Los Soportes De Almacenamiento De La Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$

12	DAÑOS POR AGUA	6580,07	Cambio de oficina pre-amenaza, el GAD cuenta en su segunda planta con una oficina acorde a las normas de seguridad de la información, que serviría de centro y alojamiento de los equipos informáticos		0,00
			Mantenimiento de la red de agua, ya que por razones del paso del tiempo esta se ha deteriorado y es necesario el mantenimiento de la misma		

Tabla 3.15. Determinación de Salvaguardas – Daños Por Agua

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
16	AVERÍA DE ORIGEN FÍSICO O LÓGICO	6580,07	Mantenimiento periódico del hardware, este ayudará a mantener los equipos en óptimas condiciones, ya que por condiciones ambientales están podrían averiar o colapsar.	185,00	1550,00
			El Dpto. Tecnológico deberá ser abastecido con un stock mínimo de repuestos para los equipos informáticos como: tarjetas de red, discos duros, memoria, bus de datos, fuentes de poder, cables, etc.		
			Mantenimiento del ESET FILE SECURITY para ordenadores tipo servidor, esta versión de antivirus protege los datos que se encuentran almacenados en los servidores del GAD, este antivirus sirve para minimizar el riesgo de infiltraciones de programas no deseados en los sistemas de información y demás computadores y equipos de almacenamiento y de comunicación.	1200,00	
			Los equipos que soporten la aplicación y cuya interrupción accidental pueda provocar alteración o pérdida de datos o documentos administrativos, deben estar protegidos contra fallos de suministro eléctrico mediante sistemas de alimentación ininterrumpida.	165,00	
			Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente entre otras cosas los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		

Tabla 3.16. Determinación de Salvaguardas – Avería De Origen Físico O Lógico

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$

E9	INTRODUCCION DE INFORMACION INCORRECTA	6580,07	Capacitación a los usuarios de la red de datos, de esta manera se educa al personal en el manejo adecuado de la misma.	0,00	0,00
			Respaldo de la información; es de suma importancia el Backup de la información en la nube esto ayudará en el inmediata recuperación del dato y por ende en la pronta utilización del mismo, este tipo de soluciones son más prácticas que las empleadas cotidianamente en medios de almacenamiento masivo como son discos externos y otros.		

Tabla 3.17. Determinación de Salvaguardas – Introducción De Información Incorrecta

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E14	ERRORES DE MANTENIMIENTO O ACTUALIZACION DE PROGRAMAS	6580,07	Capacitación continua al personal que administra los sistemas informáticos		5700,00
			El jefe del Dpto. Tecnológico será el responsable de tomar las decisiones de seguridad sobre todos los Sistemas y servicios informáticos que operan en el GAD		
			Actualización de los sistemas y paquetes informáticos, para que de esta manera se mantengan acorde a las necesidades tecnológicas que exige las normas gubernamentales.	5700,00	

Tabla 3.18. Determinación de Salvaguardas – Errores De Mantenimiento O Actualización De Programas

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E2	ERRORES DEL ADMINISTRADOR	5757,56	Disponer con el recurso humano que reúna los perfiles necesarios para el correcto funcionamiento de los laboratorios de Redes e Informática		2000,00
			Capacitación continua al personal que administra los sistemas informáticos	2000,00	
			Respaldos de la configuración inicial de los sistemas y servidores con los que cuenta el GAD, por tanto en caso de que se materialice esta amenaza sean utilizados estos respaldos		
			Se debe asignar responsabilidad del manejo de los datos de administrador los cuales tienen un perfil para el manejo de la información.		

Tabla 3.19. Determinación de Salvaguardas – Errores Del Administrador

AMENAZAS	SALVAGUARDA
----------	-------------

CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E8	ALTERACION DE INFORMACION	5757,56	Se deben adoptar medidas de identificación y autenticación proporcionadas a la naturaleza de la información y de los tratamientos, de los riesgos a los que están expuestos		0,00
			Se debe asignar a cada usuario un identificador único para su uso exclusivo y personal, de forma que cualquier actuación suya pueda ser trazada. Con el identificador de usuario el administrador de seguridad debe poder identificar al usuario específico.		
			Se deben aplicar técnicas de comprobación de la integridad de la información: funciones resumen o hash, firma electrónica, etc. (en particular a documentos y mensajes) para verificar la integridad de la misma.		

Tabla 3.20. Determinación de Salvaguardas – Alteración De Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E12	DIVULGACION DE LA INFORMACION	5757,56	Se deben adoptar procedimientos en relación con la identificación y autenticación de usuarios, la gestión y revisión de derechos y privilegios de acceso de los usuarios, la comprobación de los accesos solo a personal autorizado y responsable de la información que manipula		0,00
			Se debe limitar el acceso a los recursos tecnológicos según la función o la necesidad del usuario.		
			Se deben adoptar medidas en relación con el trabajo desde fuera de las instalaciones de la organización.		

Tabla 3.21. Determinación de Salvaguardas – Divulgación De La Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E15	ERRORES DE MANTENIMIENTO O ACTUALIZACION DE EQUIPOS (HARDWARE)	5757,56	Si la naturaleza de los tratamientos y de los datos lo hace apropiado, se deben implantar equipos dotados de mecanismos tolerantes a fallos.		480,00

			Los equipos que soporten la aplicación y cuya interrupción accidental pueda provocar alteración o pérdida de datos o documentos administrativos, deben estar protegidos contra fallos de suministro eléctrico mediante sistemas de alimentación ininterrumpida.	480,00	
			Los equipos deben mantenerse de acuerdo con las especificaciones de los suministradores respectivos.		

Tabla 3.22. Determinación de Salvaguardas – Errores De Mantenimiento O Actualización De Equipos (Hardware)

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A3	ABUSO DE PRIVILEGIOS DE ACCESO	5757,56	Se deben adoptar procedimientos en relación con la identificación y autenticación de usuarios, la gestión y revisión de derechos y privilegios de acceso de los usuarios, la comprobación de los accesos.		0,00
			Se debe limitar el acceso a los recursos según la función o la necesidad de conocer.		
			Se debe definir en cada sistema y aplicación los usuarios que pueden acceder		

Tabla 3.23. Determinación de Salvaguardas – Abuso De Privilegios De Acceso

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A19	EXTORCION	4935,07	Capacitación a los servidores públicos en temas relacionados con código de ética profesional, para concientizar a los mismos en el probable daño que pueden sufrir los sistemas y equipos, en caso de que se cumpla con disposiciones ajenas que no estén enmarcadas en derecho	2000,00	2000,00

Tabla 3.24. Determinación de Salvaguardas – Extorsión

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A18	INDISPONIBILIDAD DEL PERSONAL	4935,06	Capacitación a los servidores públicos en temas relacionados con código de ética profesional, para consienta a los mismos que la realización deliberada de conflictos tales como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, entre otros, afectan al normal funcionamiento de las labores cotidianas	2000,00	2000,00

Tabla 3.25. Determinación de Salvaguardas – Indisponibilidad Del Personal

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
I10	INTERRUPCIÓN DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	4935,06	Elaboración de un plan de adquisición para el Dpto. de Proveduría ya que de esta manera se puede mantener abastecida las dependencias municipales con suministros de impresión tales como papel para las impresoras, toner, refrigerante, entre otros; este plan implicara la planificación de las adquisiciones y las entregas programas de insumos a todos los Departamentos Municipales		0,00

Tabla 3.26. Determinación de Salvaguardas – Interrupción De Otros Servicios Y Suministros Esenciales

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E4	DIFERENCIAS DE LA ORGANIZACIÓN	4935,06	El GAD como institución publica, está en la obligación de mantener un manual de funciones actualizado en el cual se deben asignar responsabilidades, acciones y cargos, a la vez que debe establecer los niveles jerárquicos y funciones para cada uno de sus servidoras y servidores.		0,00

Tabla 3.27. Determinación de Salvaguardas – Diferencias De La Organización

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
I9	FALLO DE SERVICIOS DE COMUNICACIONES	4112,55	Respaldo de la información; es de suma importancia el Backup de la información en la nube esto ayudará en el inmediata recuperación del dato y por ende en la pronta utilización del mismo, este tipo de soluciones son más prácticas que las empleadas cotidianamente en medios de almacenamiento masivo como son discos externos y otros		0,00

Tabla 3.28. Determinación de Salvaguardas – Fallo De Servicios De Comunicaciones

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO

					\$
E1	ERRORES DE LOS USUARIOS	4112,55	Se deben definir y documentar las funciones y obligaciones del personal Se debe suministrar al personal que maneje datos de carácter personal u otra información cuya protección sea necesaria, el mobiliario adecuado para guardar la información		0,00

Tabla 3.29. Determinación de Salvaguardas – Errores De Los Usuarios

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E3	ERRORES DE CONFIGURACION	4112,55	Se deben establecer procedimientos de realización, recuperación y pruebas de las copias de respaldo que contemplen copias de los programas, aplicaciones, documentación, bases de datos, sistemas operativos, logs, etc.; debe definirse la periodicidad con que se realizan las copias (diaria, semanal, mensual), número de copias que se realizan y versiones distintas que se conservan. Los procedimientos de realización de copias serán automáticos y periódicos. Se debe mantener un registro de entrada y salida de los soportes de información. Permitirá conocer: el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.		0,00

Tabla 3.30. Determinación de Salvaguardas – Errores De Configuración

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E16	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	4112,55	Se debe incluir entre las prácticas de protección de los soportes de información medidas básicas como las siguientes, dentro y fuera del horario normal de trabajo, para evitar su pérdida o destrucción: armarios, llaves, contraseñas, etc. Se deben adoptar procedimientos de explotación adecuados para salvaguardar la disponibilidad, integridad y confidencialidad de la información.		0,00

			Se debe formar a los usuarios en el uso adecuado de la aplicación y en los procedimientos de reacción ante incidentes.		
--	--	--	--	--	--

Tabla 3.31. Determinación de Salvaguardas – Caída Del Sistema Por Agotamiento De Recursos

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A8	REPUDIO	4112,55	Se debe controlar periódicamente la forma en que el personal que disponga algún tipo de obligación en relación con la seguridad de la información de la Organización, cumple este tipo de obligaciones.		0,00
			En relación con los activos de tipo información, se debe documentar a qué usuarios se autoriza el acceso y los atributos relacionados con el referido acceso.		

Tabla 3.32. Determinación de Salvaguardas – Repudio

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E17	INDISPONIBILIDAD DEL PERSONAL	3290,04	Capacitación a los servidores públicos en temas relacionados con código de ética profesional, para concientizar a los mismos que la realización deliberada de conflictos tales como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, entre otros, afectan al normal funcionamiento de las labores cotidianas	2000,00	2000,00

Tabla 3.33. Determinación de Salvaguardas – Indisponibilidad Del Personal

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
I1	FUEGO	2313,31	Se debe situar el equipamiento que soporta a la aplicación así como los soportes de información en áreas seguras y protegidas adecuadamente.		4920,00
			Se debe proteger los departamentos de amenazas potenciales: eléctricas, incendios, clima, agua, interferencias, agentes químicos y otros.	4000,00	

			Dotar de extintores a las dependencias municipales, estos serán ubicados en lugares estratégicos para que sean utilizados de manera oportuna por los usuarios, además se debe de tomar en cuenta que son equipos de fácil manejo y por ende la capacitación de todo el personal en el manejo de las mismas es muy importante ya que serán estos quienes serán los encargados de utilizarlos en el momento adecuado	920,00	
--	--	--	--	--------	--

Tabla 3.34. Determinación de Salvaguardas – Fuego

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A1	MANIPULACION DE INFORMACION	2313,31	Se debe identificar el papel de los diversos actores en relación con los activos a proteger		0,00
			Para cada activo se debe identificar a su custodio, así como su valor e importancia en términos cuantitativos o cualitativos, en función de los requisitos de autenticidad, integridad, confidencialidad y disponibilidad que le son aplicables. Esta información es crucial, pues facilita el análisis y gestión de riesgos y, por tanto sirve, para determinar las medidas de seguridad proporcionadas.		
			En relación con los activos de tipo información, se debe documentar a qué usuarios se autoriza el acceso y los atributos relacionados con el referido acceso.		

Tabla 3.35. Determinación de Salvaguardas – Manipulación De Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A2	SUPLANTACION DE INFORMACION DEL USUARIO	2313,31	Se debe controlar periódicamente la forma en que el personal que disponga algún tipo de obligación en relación con la seguridad de la información de la Organización, cumple este tipo de obligaciones.		0,00
			Establecer obligaciones de confidencialidad en los casos de personal con contratos temporales o personal perteneciente a empresas subcontratadas, cuando la información que puedan manejar en el desempeño de sus obligaciones temporales sean datos de carácter específico, u otra información sensible		
			El personal temporal o contratado deberá aceptar expresamente las obligaciones y prescripciones de confidencialidad en el manejo y uso de la información.		

Tabla 3.36. Determinación de Salvaguardas – Suplantación De Información Del Usuario

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A5	DIFUSIONES DE SOFTWARE DAÑINO	2313,31	Se debe elaborar y mantener una lista de usuarios autorizados; éstos deben tener un conjunto de atributos de seguridad que puedan ser mantenidos individualmente.		2000,00
			Disponer con el recurso humano que reúna los perfiles necesarios para el correcto funcionamiento de los laboratorios de Redes e Informática		
			Capacitación a los servidores públicos en temas relacionados con código de ética profesional, para consienta a los mismos en el probable daño que pueden sufrir los sistemas y equipos, en caso de que se materialice esta amenaza	2000,00	

Tabla 3.37. Determinación de Salvaguardas – Difusiones De Software Dañino

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A10	MODIFICACION DE LA INFORMACION	2313,31	Se deben implantar procedimientos de explotación de la aplicación y de los sistemas adecuados a la protección de la integridad.		0,00
			Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		
			Política de autenticación y acceso a la información, de esta manera se sabrá a ciencia cierta los usuarios que están accedendo a la información		

Tabla 3.38. Determinación de Salvaguardas – Modificación De La Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A14	MANIPULACIÓN DE PROGRAMAS	2313,31	Se debe identificar el papel de los diversos actores en relación con los activos a proteger		0,00

			Para cada activo se debe identificar a su custodio, así como su valor e importancia en términos cuantitativos o cualitativos, en función de los requisitos de autenticidad, integridad, confidencialidad y disponibilidad que le son aplicables. Esta información es crucial, pues facilita el análisis y gestión de riesgos y, por tanto sirve, para determinar las medidas de seguridad proporcionadas.		
			En relación con los activos de tipo información, se debe documentar a qué usuarios se autoriza el acceso y los atributos relacionados con el referido acceso.		

Tabla 3.39. Determinación de Salvaguardas – Manipulación De Programas

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A16	ATAQUE DESTRUCTIVO	2313,31	Capacitación a los servidores públicos en temas relacionados con código de ética profesional, para concientizar los mismos en el probable daño que pueden sufrir los sistemas y equipos, en caso de que se materialice esta amenaza	2000,00	2000,00
			Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		

Tabla 3.40. Determinación de Salvaguardas – Ataque Destructivo

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A17	OCUPACION ENEMIGA	2313,31	Utilización de cámaras de seguridad, esto servirá para tener una idea más clara de los sucesos que ocurren dentro de la institución, por lo general estos equipos generan cierto respeto o temor a las personas a ser filmadas y descubiertas en cualquier tipo de ilícito	5000,00	5000,00

Tabla 3.41. Determinación de Salvaguardas – Ocupación Enemiga

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$

E13	VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	2056,27	Políticas de prueba de puesta a punto de los sistemas informáticos ha ser utilizados por la institución, esto servirá para evitar conflictos al momento de la manipulación de los sistemas por parte de los usuarios		0,00
-----	--	---------	--	--	------

Tabla 3.42. Determinación de Salvaguardas – Vulnerabilidades De Los Programas (Software)

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A6	ACCESO NO AUTORIZADO	2056,27	Utilización de cámaras de seguridad, esto servirá para tener una idea más clara de los sucesos que ocurren dentro de la institución, por lo general estos equipos generan cierto respeto o temor a las personas a ser filmadas y descubiertas en cualquier tipo de ilícito	5000,00	5500,00
			Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente entre otras cosas los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		
			Capacitación a los usuarios de la red de datos, de esta manera se educa al personal en el manejo adecuado de la misma.	500,00	
			Aplicar protocolos y normas internacionales de seguridad aplicada a los sistemas y servidores web de la Institución		

Tabla 3.43. Determinación de Salvaguardas – Acceso No Autorizado

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A11	INTRODUCCION DE INFORMACIÓN FALSA	2056,27	Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente entre otras cosas los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		500,00
			Capacitación a los usuarios de la red de datos, de esta manera se educa al personal en el manejo adecuado de la misma.	500,00	

Tabla 3.43. Determinación de Salvaguardas – Introducción De Información Falsa

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$

A12	DESTRUCCION DE INFORMACION	2056,27	Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente entre otras cosas los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		500,00
			Se debe limitar el acceso a los recursos según la función o la necesidad de conocer.		
			Capacitación a los usuarios de la red de datos, de esta manera se educa al personal en el manejo adecuado de la misma.	500,00	

Tabla 3.44. Determinación de Salvaguardas – Destrucción De Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A15	ROBO	2056,27	Implementar el Manual de Políticas de Seguridad Informática para la Red, detallando claramente entre otras cosas los objetivos y alcances de cada uno de los usuarios dentro de la red de datos		5000,00
			Utilización de cámaras de seguridad, esto servirá para tener una idea más clara de los sucesos que ocurren dentro de la institución, por lo general estos equipos generan cierto respeto o temor a las personas a ser filmadas y descubiertas en cualquier tipo de ilícito	5000,00	
			Limitar el acceso a personas ajenas a las funciones que se realizan en el Dpto. Tecnológico, esto evitara que personas no autorizadas tengan acceso a esta dependencia y así evitan la posible pérdida equipos		

Tabla 3.45. Determinación de Salvaguardas – Robo

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
E10	DEGRADACION DE LA INFORMACION	1285,17	Se debe elegir un lugar de almacenamiento adecuado para los soportes de información.		0,00

Tabla 3.46. Determinación de Salvaguardas – Degradación De La Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$

E11	DESTRUCCION DE INFORMACION	1285,17	Se debe elegir un lugar de almacenamiento adecuado para los soportes de información.	0,00
			Se debe incluir entre las prácticas de protección de los soportes de información medidas básicas como las siguientes, dentro y fuera del horario normal de trabajo, para evitar su pérdida o destrucción: armarios, llaves, contraseñas, etc.	
			Verificar la definición y correcta aplicación de las medidas de protección de los soportes de información.	

Tabla 3.47. Determinación de Salvaguardas – Destrucción De Información

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
A7	ANALISIS DE TRÁFICO	1028,14	Se deben definir procedimientos para el paso de aplicaciones a explotación, ya sean nuevas o actualizaciones de las existentes, que recojan los requisitos que estas deben cumplir y las pruebas a realizar antes de su aceptación.	1200,00	1200,00
			Se deben realizar mantenimientos preventivos, como la instalación de las actualizaciones de seguridad recomendadas por los fabricantes, o el aumento de capacidad para evitar saturaciones.		
			Se debe cifrar la información transmitida a través de redes, para evitar su modificación y divulgación no autorizadas.		

Tabla 3.48. Determinación de Salvaguardas – Análisis De Tráfico

AMENAZAS			SALVAGUARDA		
CODIGO	AMENAZA	RIESGO INTRINSECO	TIPO DE SALVAGUARDA	VALOR \$	COSTO ESTIMADO \$
15	CONTAMINACION ELECTROMAGNÉTICA	308,44	El acceso a los sistemas de forma remota se debe realizar, siempre que sea técnicamente factible, mediante redes privadas virtuales.	0,00	0,00
			Se deben definir procedimientos para el paso de aplicaciones a explotación, ya sean nuevas o actualizaciones de las existentes, que recojan los requisitos que estas deben cumplir y las pruebas a realizar antes de su aceptación.		

Tabla 3.49. Determinación de Salvaguardas – Contaminación Electromagnética.

3.2. ESTRATEGIAS DE CONTINUIDAD DE ACTIVIDADES

3.2.1. RESPALDO DE SERVIDORES

La tarea de respaldar la información es una de las más importantes en cualquier organización ya que la información es alojada en ordenadores tipo servidor que se encuentran ubicados fuera de la organización y esto garantiza la integridad del dato que incrementa día a día su valor; a diferencia de los equipos informáticos (Hardware) que con el pasar del tiempo se van deteriorando y perdiendo valor para la organización, se puede indicar que es relativamente proporcional al dato ya que mientras la información aumenta su valor este se deprecia llegando a un valor residual. La institución cuenta con dos sistemas informáticos que son:

Sistema Contable OLYMPO

Este sistema opera simultáneamente con 5 base de datos que son (Finanzas, Nomina, Bienes, Existencias Y Activos), soportadas en un servidor IBM con sistema operativo Windows server 2003 y el gestor de base de datos SQL SERVER 2005, ubicado en el departamento tecnológico, las cuales contiene toda la información contable y financiera del municipio desde el año 2005, información que es de gran importancia para realizar los procesos de ámbito financiero de la municipalidad.

Esta información tomando en cuenta gastos de instalaciones y renovaciones anuales de licencias proveídas por la empresa PROTELCOTELSA S.A., mantenimiento y gastos de sueldos en empleados que operan este sistema y por ende son quienes alimentan las bases de datos del sistema, ha costado a la institución un monto aproximado de \$ 398,440.00 dólares americanos.

Sistema Integral De Catastros (SIC)

Es un sistema que no tiene costo de adquisición o instalación ya que es puesto a disposición de los municipios del Ecuador por la Asociación de

Municipalidades Ecuatorianas (**AME**), sin embargo la información que contienen la base de datos con la que opera si representa un valor económico, ya que así mismo la municipalidad ha gastado o invertido una gran cantidad de dinero en: el levantamiento de la información catastral en el año 2004, actualización del catastro en el año 2008, y gastos de operadores del sistema que son los responsables de los departamentos de Avalúos y Catastros así mismo el departamento de recaudación, alrededor de \$ 270,060.00 dólares americanos.

Esta información permite a la institución recaudar anualmente alrededor de \$ 90,000.00 dólares americanos, dinero que sirve para realización de obras que son de gran ayuda para desarrollo del cantón.

El valor de la información de cualquier organización se va elevando al paso del tiempo es por eso que es uno de los activos más importantes para la institución, como se muestran en los cuadros siguientes.

3.2.1.1. SOLUCIÓN DE RESPALDO INTERNO

Respaldo la información de estos dos sistemas en discos duros externos de forma diaria y manual para tener salvaguardada la información de estos en caso de que se materialice una amenaza física o lógica que acabe con la información alojada en los servidores paralizando el trabajo de estos departamentos:

RESPONSABLE	EQUIPOS NECESARIOS	COSTO APROXIMADO
Personal de tecnologías de información y comunicación de la institución.	2 Discos duros externo de 1 TB	\$ 300.00
	50 Discos compactos de 4,7 GB para entregar copia de respaldo del último día de cada mes autoridades	\$ 40.00

Tabla 3.50. Presupuesto Referencial para la adquisición de dispositivos de almacenamiento masivo.

3.2.1.2. SOLUCIÓN DE RESPALDO EXTERNO

La alternativa de respaldos fuera de la institución es más confiable y esta información está disponible en menos tiempo en caso de que suceda alguna eventualidad que dañe la información almacenada de forma local, para así restablecer las operaciones normales de estos sistemas.

El tener otras dependencias bajo cargo de la municipalidad nos da una gran oportunidad de respaldos evitando gasto de otra infraestructura para alojar servidores de respaldos.

Una propuesta es adquirir un servidor de respaldos y ubicarlo en el cuarto de telecomunicaciones del el patronato municipal en el cual ya existe una conexión de datos de forma inalámbrica, la misma que se puede mejorar con cable de fibra óptica para optimizar el tráfico de la información y así obtener grandes resultados para la organización.

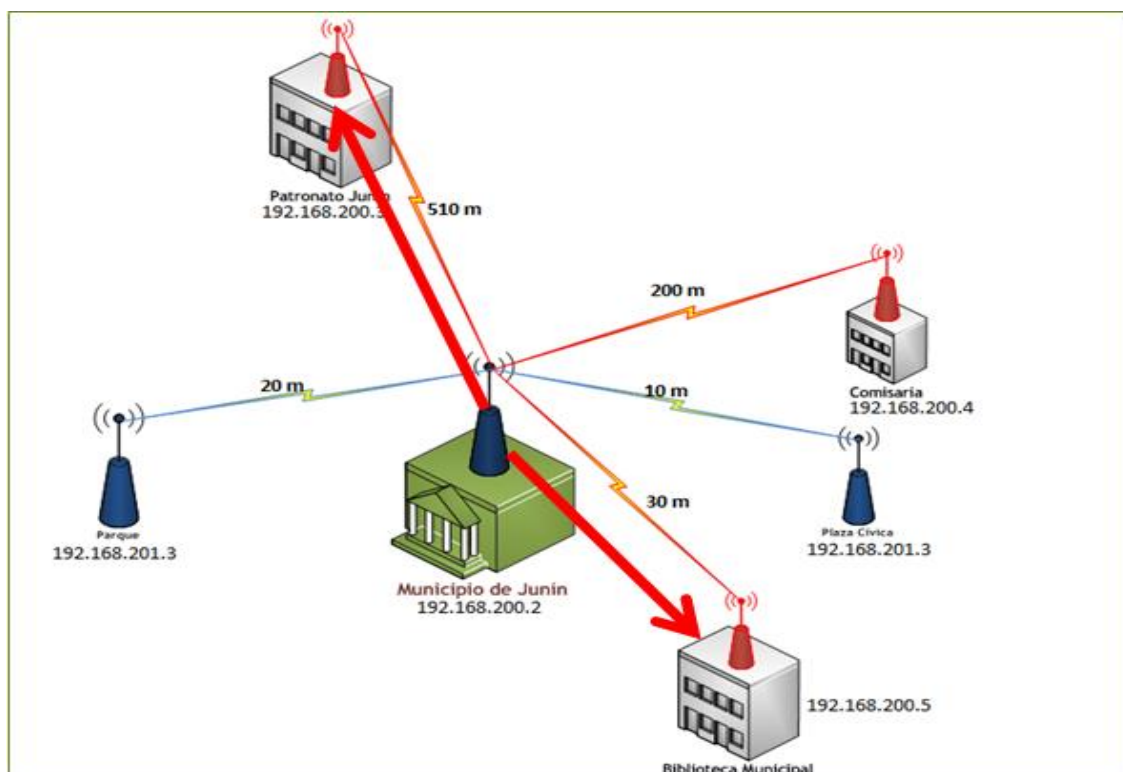


Figura 3.4. Propuesta de tendido de cable de fibra óptica hacia otro edificio para servidor de respaldo.

RESPONSABLE	NECESIDAD	COSTO APROXIMADO	LOGRO
Personal de tecnología y Información	de Conexión mediante cable de fibra óptica hasta el patronato de	\$ 5,000.00	Mantener un plan de respaldo manual o automático de las

Comunicación	amparo social del Cantón Junín		bases de datos de los sistemas informáticos del municipio.
	Servidor para respaldos	Entre \$ 3000.00 y \$ 6000.00	
	Sistema operativo Windows server	\$ 500.00	Mantener actualizado los sistemas operativos y gozar plenamente de las bondades que ofrece el soporte técnico de los mismos
	Gestor de bases de datos SQL SERVER 2005, 2008	\$ 898.00	

Tabla 3.51. Presupuesto Referencial de los sistemas informáticos a utilizar.

3.2.1.3. SOLUCION DE RESPALDO EN LA NUBE

Otra solución que ha ido evolucionando y que permite tener la información segura y en tiempo real disponible en caso de que suceda algún evento que paralice el normal funcionamiento de la institución por falta de esta, es el CLOUD BACKUP o respaldos en la nube, el cual es más costoso por sus características.

En el Ecuador la única empresa que ofrece este servicio es TELCONET S.A., el mismo que consiste en alojar la información que las empresas creen pertinentes todo esto en tiempo real, para que la información esté disponible y segura en cualquier momento cuando sea requerida. Esta empresa tiene los siguientes planes de mantenimiento (Anexo 8-A).

Descripción	Detalle	Precio	Tipo de Cargo
Entrega de datos en Unidad USB 500GB en DC	Entrega de Backups en instalaciones del datacenter en unidad USB de 500GB por una ocasión	\$ 500.00	Cargo Único
Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 100 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 75.00	Mensual

Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 400 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 105.00	Mensual
Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 500 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 115.00	Mensual
Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 1000 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 200.00	Mensual
Entrega de datos en Unidad USB 1000GB en DC x svr	Entrega de Backups en instalaciones del datacenter en unidad USB de 1000GB por una ocasión	\$ 800.00	Cargo Único

Tabla 3.52. Servicios de respaldo que ofrece TELCONET. S.A.

3.2.2. SERVIDOR DE ARCHIVOS CENTRALIZADO

Hoy en día las empresas de una u otra forma se vuelven cada vez más dependientes de los equipos y sistemas informáticos para realizar sus tareas cotidianas de admiración, si bien es cierto en el la institución existen dependencias en las cuales sus tareas no depende del uso de los sistemas OLYMPO o SIC, mencionados anteriormente, pero que son tan importantes como todas, ya que estas manejan una gran cantidad de información importante para esta municipalidad, información que ayudan a llevar una correcta administración de este organismo de servicio público.

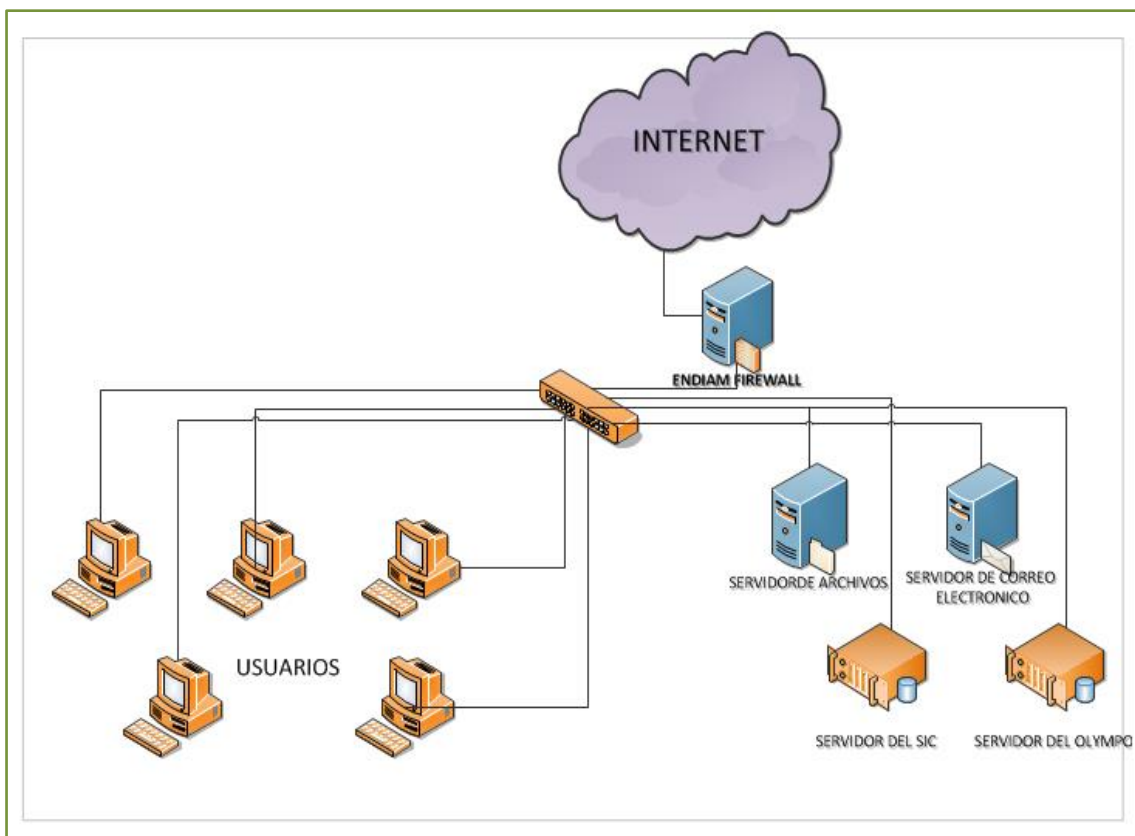


Figura 3.5. Propuesta de montar un servidor de archivos centralizado en la institución.

Con el modelo que se muestra en la figura anterior se evita que por el fallo de algún disco duro de un computador de cualquier departamento donde se almacena información importante para este y por ende para la institución se pierda; almacenando la información de cada uno de estos equipos en un servidor centralizado con RAID para tener disponible la información cuando sea necesario. Sin que el departamento paralice su funcionamiento normal.

Para evitar que toda la información almacenada en este servidor se pueda perder si se materializa una de las amenazas que ataque a estos servidores, el municipio para proteger ésta puede optar por contratar un servicio al igual que con los servidores de los sistemas mantenerlo respaldado en la nube, como se muestra en la figura 3.6.

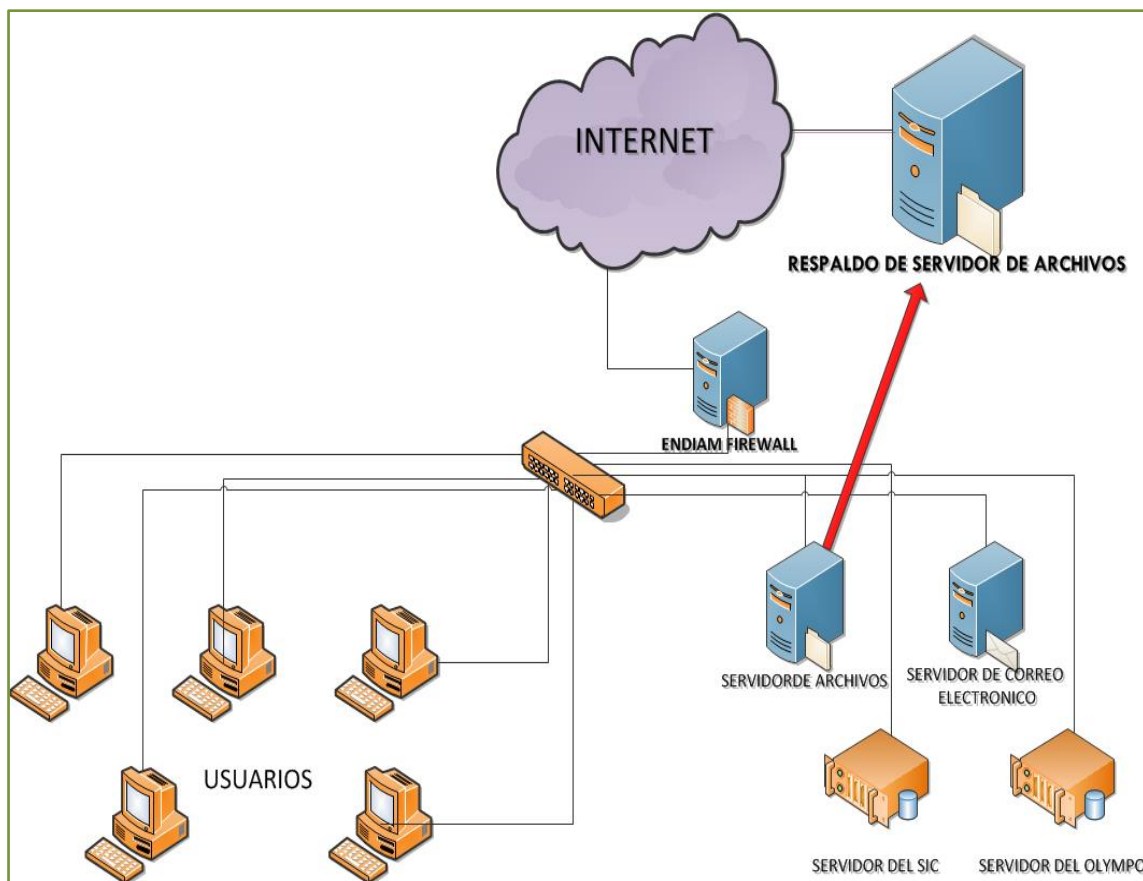


Figura 3.6. Propuesta de montar un servidor de archivos centralizado en la institución.

3.2.3. CONTINGENCIAS PARA LOS SISTEMAS INFORMÁTICOS

3.2.3.1. SERVIDOR DEL SISTEMA CONTABLE OLYMPO - TOTALMENTE DAÑADO

Buenas Prácticas Para La Seguridad De La Información

1. Tener en cuenta la ubicación, seguridad física, climatización, suministro eléctrico del espacio físico donde se encuentre alojado el servidor.
2. Poner en práctica un plan de mantenimiento de hardware y software dedicado a este servidor de datos.

3. Realizar respaldos diarios de las bases de datos FINANZAS, que es la que se utiliza diariamente en importantes procesos.
4. Realizar y almacenar copias de seguridad semanales a las bases de datos restantes como son NOMINA, BIENES y EXISTENCIA, las cuales su uso es en menor grado y se la hace semanalmente.
5. Realizar y almacenar copias de seguridad de las configuraciones del sistema cada que se genere algún tipo de cambio en la configuración.
6. Realizar monitoreo diario sobre accesos al sistema para prevenir alguna infiltración no deseada que pueda causar daño al sistema y por ende a los datos.

Tareas A Realizar Para La Continuidad De Las Labores Normales

Responsables: Personal de tecnologías de información y comunicación del GADMC Junín y personal técnico de la empresa PROTELOTELSA S.A.

1. Tomar el servidor que se encuentra disponible en el departamento de proveeduría el cual deberá, como medida de gestión de riesgo tener previamente instalado el sistema operativo WINDOWS SERVER 2003 y el SQL SERVER 2005, que son con los que básicamente esta soportado el sistema OLYMPO.
2. Realizar las configuraciones necesarias como conexión a la red de datos del municipio, configuraciones de seguridad entre otras.
3. Contactarse con la empresa PROTELCOTELSA S.A. que es quien provee a la institución de este sistema y además se encarga de dar soporte técnico el cual está incluido en el valor de la licencia de este producto, para que colaboren en la instalación de la consola del software.

4. Restaurar los respaldos de las bases de datos previamente respaldadas y almacenadas en los soportes de respaldos considerados por la institución.
5. Realizar pruebas desde las estaciones de trabajos de los departamentos de Tesorería, Contabilidad, Dirección Financiera y proveeduría; que son los encargados de la utilización del mismo.

RESPONSABLE	NECESIDAD	COSTO APROXIMADO
Personal de tecnología de Información y Comunicación y empresa PROTELCOTELSA S.A.	1 Servidor disponible en bodega	\$ 3500.00
	Vigente el contrato de licenciamiento del sistema	\$ 5,000.00 cada año
	Sistema operativo Windows server	Incluido en licencia
	Gestor de bases de datos SQL SERVER 2005, 2008	Incluido en licencia

Tabla 3.53. Presupuesto referencial de los servicios que ofrece PROTELCOTELSA S.A.

3.2.3.2. SERVIDOR DEL SISTEMA INTEGRAL DE CATASTROS (SIC) DAÑADO

Buenas Prácticas Para La Seguridad De La Información

1. Tener en cuenta la ubicación, seguridad física, climatización, suministro eléctrico del espacio físico donde se encuentre alojado el servidor.
2. Poner en práctica un plan de mantenimiento de hardware y software dedicado a este servidor de datos.
3. Realizar y almacenar copias de seguridad diarios de la base de datos DBAME, que se utiliza diariamente por los departamentos de Recaudación y Avalúos/Catastros, en los diferentes procesos que realizan estos departamentos.

4. Realizar y almacenar copias de seguridad de las configuraciones del sistema cada que se genere algún tipo de cambio en la configuración.
5. Realizar monitoreo diario sobre accesos al sistema para prevenir alguna infiltración no deseada que pueda causar daño al sistema y por ende a los datos.

Tareas a Realizar Para la Continuidad De Las Labores Normales

Responsables: Personal de tecnologías de información y comunicación del GADMC Junín y personal técnico la asociación de Municipalidades Ecuatorianas (AME)

1. Tomar el servidor que se encuentra disponible en el departamento de proveeduría el cual deberá, como medida de gestión de riesgo tener previamente instalado el sistema operativo y el SQL SERVER 2003 y 2005, que son con los que básicamente esta soportado el sistema SIC.
2. Realizar las configuraciones necesarias como conexión a la red de datos del municipio, configuraciones de seguridad entre otras.
3. Contactarse con los técnicos de AME que son quienes dotan a la institución de este sistema y además se encarga de dar soporte técnico
4. Restaurar los respaldos de las bases de datos previamente respaldadas y almacenadas en los soportes de respaldos considerados por la institución.
5. Realizar pruebas desde las estaciones de trabajos de los departamentos de Recaudación y Avalúos/Catastros; que son los encargados dela utilización del mismo.

RESPONSABLE	NECESIDAD	COSTO APROXIMADO
Personal de tecnología de Información y Comunicación y AME	1 Servidor disponible en bodega	\$ 3500.00
	Gestor de bases de datos SQL SERVER 2005, 2008	\$ 898.00

Tabla 3.54. Presupuesto referencial para poner en marcha el SIC

3.2.4. CORTE DE SUMINISTRO ELECTRICO

Estado Actual

Actualmente todos los equipos están protegidos por equipos UPS que permiten almacenar energía eléctrica para dotar a los equipos informáticos de este suministro por un tiempo aproximado que va de 15 o 30 minutos aproximados, después que falte por cualquier circunstancia éste en el tendido eléctrico de la institución.

Pasos Para Proteger Los Equipos En Caso De Este Fallo

Sin Planta Generadora De Energía Eléctrica En La Institución

N°	RESPONSABLE	ACCIÓN
1	PERSONAL DE TECNOLOGÍA	Contactar vía telefónica a la agencia CNEI Junín, para obtener información del daño que produjo este fallo y tiempo aproximado de reparación del mismo
2		En caso de que exceda el tiempo de almacenamiento de los UPS, avisar a todo el personal que procedan a apagar los equipos a su cargo para evitar daños en caso de sobrecarga eléctrica
3		En caso de que exceda el tiempo de almacenamiento de los UPS, proceder a apagar los servidores de sistemas
4		Una vez que se restablezca este suministro a la institución, proceder a poner en marcha los

		servidores de sistemas y de servicios de internet, telefonía IP y mail.
TIEMPO DE RECUPERACION ---->		DEFINIDO POR EL CORTE ELECTRICO

Tabla 3.55. Métodos de acción a seguir en caso de cortes de suministro eléctrico

Con La Adquisición De Planta Generadora De Energía Eléctrica En La Institución

El costo de una planta eléctrica oscila entre los \$ 10.000,00 y \$ 14.000,00 dólares americanos dependiendo de sus características.

N°	RESPONSABLE	ACCION
1	JEFE DE TECNOLOGIA	Contactar vía telefónica a la agencia CNEL Junín, para obtener información del daño que produjo este fallo y tiempo aproximado de reparación del mismo
2		Coordinar con técnico de mantenimiento eléctrico de la institución.
3	TECNICO DE MANTENIMIENTO ELECTRICO	Activar la planta eléctrica de la institución restableciendo el suministro eléctrico en todo el edificio municipal
TIEMPO DE RECUPERACION ---->		MAXIMO APROXIMADO 15 MINUTOS

Tabla 3.56. Métodos de acción a seguir con la adquisición de planta generadora de energía eléctrica.

3.2.5. CONTINUIDAD DEL SERVICIO INTERNET

Las entidades públicas están en constante uso de portales web de administración pública centralizados en sistemas que requieren de una conexión a internet para poder realizar de forma normal estos procesos. Así mismo este medio es muy utilizado para uso de correo electrónico entre otros servicios de comunicación con ministerios y otras entidades de este tipo para una correcta administración, los cuales son de uso diario y concurrente.

Estado Actual

El GADMC Junín mantiene un contrato de este servicio con la Corporación Nacional de Telecomunicaciones, con un ancho de banda de 12 Mbps con un costo mensual por el servicio de \$ 850 dólares americanos.

Se ha comprobado mediante pruebas de velocidad de internet, que el servicio desde su contratación no es el esperado ya que la velocidad de subida oscila entre 8 y 11 Mbps, mientras que la velocidad de descarga esta entre 5 y 8 Mbps, y el servicio se torna lento en muchas ocasiones.

Propuesta

Como solución alternativa para la continuidad del servicio de internet se sugiere que, la municipalidad adquiera con otra empresa proveedora del mismo por lo menos 2 Mbps de ancho de banda, para utilizarlos en caso de que por cualquier motivo falle este servicio con la empresa CNT, que es con la que actualmente mantiene contratado el servicio.

Además se sugiere que como el Patronato Municipal de Amparo Social (Anexo 6-A, 6-B) es la mejor opción de una contingencia de carácter mayor, la instalación de los equipos se la haga en ese edificio conectado directamente mediante cable de fibra óptica para mayor optimizar el uso del mismo.

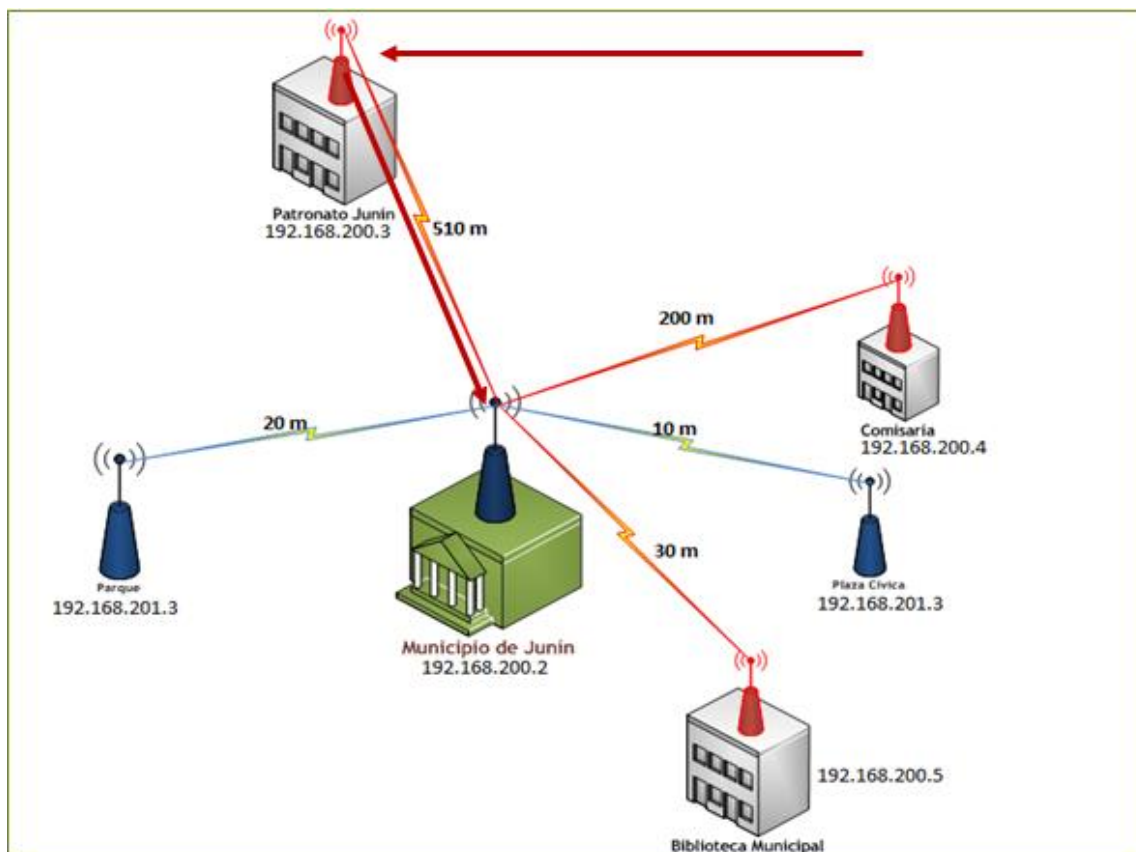


Figura 3.7. Propuesta de contingencia referente al servicio de internet en el edificio del Patronato de Amparo Social.

3.2.6. DESTRUCCIÓN TOTAL DE LAS INSTALACIONES DEL GAD MUNICIPAL DEL CANTÓN JUNÍN

Entre los estudios realizados este tipo de accidentes en poco probable en este medio, pero no hay que hacer caso omiso a que en algún momento pueda materializarse una amenaza de gran magnitud que pueda acabar con las instalaciones, tomando como antecedente y referencia la municipalidad del Cantón Chone la cual sufrió un atentado donde los daños que este causó fueron de gran magnitud debido a que se quemó la institución perdiéndose consigo toda la documentación e información que tenía hasta el momento, el mayor inconveniente radicó en que esta institución nunca adquirió una solución alternativa de recuperación o continuidad de las operaciones de la institución.

En el caso de que materialice este tipo de amenaza en el GADM Cantón Junín, se pondría en marcha con sus operaciones básicas según la razón de ser de

este tipo de instituciones y mediante la priorización de aplicaciones y procesos, dotándose de manera inmediata los siguientes recursos:

DEPARTAMENTO	COMPUTADORES	IMPRESORAS	TALENTO HUMANO
Tecnología de información	2	1	2
Compras Publicas	2	1	2
Dirección Administrativa	2	1	2
Recaudación – Avalúos y Catastro	3	2	3
Dirección financiera	2	1	2
Asesoría Jurídica	2	1	2
Gestión de riesgos	1	1	1
Secretaria General	1	1	2
Comunicación Social	1	1	2

Tabla 3.57. Dependencias Municipales con el número de activos requeridos.

CAPÍTULO IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

El censo informático que se realizó en el GAD Municipal del Cantón Junín permitió determinar la cantidad de equipos y sistemas informáticos con los que cuenta la Institución, así como también se obtuvo el valor real de los mismos; entre los activos se encuentran, computadores, impresoras, computadores tipo servidor, sistemas de alimentación ininterrumpida y equipos de red, llegando a un monto total de treinta mil doscientos cincuenta y seis con cincuenta y ocho dólares de los Estados Unidos de América; de igual manera se obtuvo datos de las licencias (software) llegando a un monto total de cinco mil ochocientos cincuenta dólares; el Municipio invierte en servicio de telecomunicación y energía eléctrica la cantidad de catorce mil cuatrocientos cuarenta dólares; y, el valor de información asciende a un monto total de quinientos un mil quinientos cuarenta dólares, como se muestra en la tabla 4.1.

DETALLES	COSTO INICIAL	COSTO ACTUAL
Hardware	53003,21	30256,58
Software		5850,00
Servicio		14400,00
Información (Dato)		501540,00

Tabla 4.1. Valores de los activos del GAD Municipal del Cantón Junín

Con la estimación del riesgo y del impacto sobre el activo, se obtuvo un catálogo de posibles amenazas sobre los activos de un sistema de información, para cada amenaza se recurre a una matriz tal como se ilustra en el Cuadro 3.1 y se determinó la priorización de los activos a ser intervenidos de manera prioritaria (Anexo 5-A, 5-B, 5-C).

Se elaboró un listado amenazas para los equipos y sistemas de información valorando el riesgo para cada una de ellas según el impacto y la frecuencia de estas, además se establecieron salvaguardas para cada una de estas amenazas según la magnitud de riesgo dentro de la institución.

Se desarrolló un plan de contingencia con la utilización de todos los componentes que forman parte de los sistemas informáticos, en el mencionado Plan se encuentran recomendaciones de soluciones que ayudaran a reducir el riesgo de cada una de las amenazas contempladas, así mismo un conjunto de soluciones que la institución puede adoptar para asegurar la continuidad de las funciones en caso de que se materialice amenazas (Anexo 7-A, 7-B, 7-C).

Una vez concluida la elaboración del Plan de Contingencia de los equipos y sistemas informáticos del GAD Municipal del Cantón Junín, se procedió a realizar una capacitación al personal que labora en las áreas más vulnerables a que una amenaza se materialice, dando a conocer los activos con los que cuenta la institución, el valor económico que tiene la información y cuán importante es utilizar normas básicas para el tratamiento de la misma (Anexo 9-A, 9-B).

4.2. DISCUSIÓN

Para el desarrollo del plan de contingencia de los equipos y sistemas informáticos, se realizó el análisis, detección, evaluación y priorización de las amenazas potenciales de las que puede ser víctima la institución, así mismo se priorizó las actividades más relevantes para la organización, además a través de este se pudo determinar el valor económico actual de los equipos y principalmente de los sistemas informáticos (valor del dato); en comparación de otros trabajos que se limitan en abarcar solo el hardware o la parte del software en su defecto tratan de manera superficial cada uno de estos, en varios repositorios que se encuentran ubicados en la nube se pueden encontrar trabajos como el desarrollado por un estudiante de Escuela Politécnica Del Ejército Extensión Latacunga con el tema titulado **PLAN DE CONTINGENCIAS PARA LOS LABORATORIOS DE REDES E INFORMÁTICA**, inclinado este para los Laboratorios de Redes e Informática que comprenden tres subplanes (Prevención Contención y Recuperación), permitiendo que el personal que labora en los Laboratorios de Redes e Informática pueda actuar ante cualquier desastre, ya este sea natural o accidental reduciendo el costo y tiempo.

Otros de los temas que sirvió de análisis para el desarrollo de esta tesis fue el proyecto titulado **PLAN DE CONTINGENCIA INFORMÁTICO PARA EL CONJUNTO DE BODEGAS PARKENOR**, trabajo desarrollado por estudiantes de la Escuela Superior Politécnica del Ejército.

En ambos trabajos implica el estudio de los componentes del Hardware y Software abarcando de esta manera el estudio de los mismos sin determinar el valor de los activos y mucho menos de los datos; es por esta razón que se considera que el presente trabajo investigativo tiene relevancia, ya que se considera de un valor muy importante los activos y de mayor consideración la información ambas necesarias para llevar a efecto un plan de contingencia en una organización.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Se puede concluir que:

Mientras el valor del hardware se deprecia en su valor monetario el valor de la información incrementa de una manera considerable para la Institución.

Con la ponderación del riesgo se puede establecer que los activos dentro de la institución están propensos a múltiples amenazas de diversa índole que podrían materializarse en cualquier momento.

Con la utilización de actividades destinadas a la protección de los equipos y sistemas de información se puede mitigar el riesgo de una forma considerable para la institución.

Con la implementación de cualquier tipo de salvaguardas no existe la seguridad de eliminar totalmente la amenaza y por ende el riesgo que conlleva para los activos.

El Plan de contingencia servirá como una guía didáctica en caso de que se materialice una amenaza afectando al normal funcionamiento de la Institución.

Estableciendo además una manera ordenada de actividades que se deben de poner en práctica, el Municipio del Cantón Junín contará con una herramienta muy importante la cual le permitirá recuperarse ante las posibles fallas y siniestros ocasionados por agentes internos o externos a la misma.

5.2. RECOMENDACIONES

A las Autoridades que administran las Instituciones Públicas y que son los encargados de la toma de decisiones, se recomienda lo siguiente:

- No presentar resistencia al momento de invertir en seguridad informática y por ende de la institución, es decir destinar recursos económicos para salvaguardar la información que tiene un alto valor y es de mucha relevancia, de no hacerlo se continua con el riesgo de que se materialice una amenaza, claro ejemplo fue lo sucedido en la Ciudad de Chone en el llamado “Gran Paro de Chone”, en este hecho se perdió toda la información que reposaba en la Institución y por ende el Municipio sufrió una perdida incalculable.

Al Jefe del Departamento Tecnológico, se recomienda lo siguiente:

- Presentar proyectos que incluya la implementación de las salvaguardas de acuerdo el grado de riesgo de las mismas contemplados en el plan de contingencias informáticas.
- Dar seguimiento al presente plan, manteniéndolo actualizado en activos y en la disminución de los riesgos de acuerdo como se vayan implementando las salvaguardas en la institución para así tener una guía actualizada de las salvaguardas realizadas y pendientes de implementación.
- A los encargados del Departamento tecnológico, impartir capacitaciones al personal municipal, mismo que tendrá como objetivo concientizar y dar a conocer las bondades que cuenta y ofrece el mencionado plan.

A futuros investigadores de planes de contingencia:

- Basar la investigación en el hardware y software, determinando el valor económico de los equipos y principalmente de los sistemas informáticos (valor del dato).

BIBLIOGRAFÍA

- Al-Badi A, Ashrafi R, Al-Majeeni A y Mayhew P. 2008. It disaster recovery: Oman and Cyclone Gonu lessons learned. Norwich UK. Consultado, 2 de Julio del 2013. Disponible en www.emeraldinsight.com/0968-5227.htm.
- Alberts, C. y Dorofee, A. 2003. Managing Information Security Risk. Boston. Revista Enlace: Revista Venezolana de Información, tecnología y conocimiento. Vol. 5. Núm. 2. p 16.
- Arias, M. 2009. Percepción general de la virtualización de los recursos informáticos. CR. InterSedes: Revista de las Sedes Regionales. Vol. 9. pág. 152.
- Brenes, A. 2007. Elementos conceptuales y desarrollo histórico de la noción de gestión del riesgo y los desastres. Bogotá. CO. Revista Reflexiones. Vol. 86. p 82.
- Carvajal, A. 2009. Análisis y Gestión de Riesgos Metodología MAGERIT. Bogotá. p 32. Consultado, 14 de Ago. 2012. Formato PDF. Disponible en <http://www.globalteksecurity.com>.
- DPAE (Dirección de Prevención y Atención de Emergencias). 2009. Guía para la elaboración de plan de emergencia y contingencia. Bogotá. p 20. Consultado, 16 de jul. 2012. Formato PDF. Disponible en <http://www.fopae.com>.
- EPN (Escuela Politécnica Nacional). 2011. Análisis de Riesgo Informáticos y Elaboración de un plan de contingencia T.I. Para la empresa eléctrica Quito S.A., EC. p 12. Consultado, 20 de feb. 2013. Disponible en <http://bibdigital.epn.edu.ec/bitstream/15000/3790/1/CD-3510.pdf>.

- ESPAM MFL (Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López). 2012. Manual de Sistema de Investigación Institucional. Calceta, Manabí, EC. p 29-43.
- Freitas, V. 2009. Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Zulia, VE. Revista Enlace: Revista Venezolana de Información, tecnología y conocimiento. Vol. 6. Núm. 1. pág. 46.
- Guía del PMBOK. 2011. Guía de los Fundamentos de la Dirección de Proyectos. 3 ed. p. 237.
- Heras, I. 2011. ¿Qué fue de la isomanía? ISO 9000, ISO 14000 y otros Meta estándares en perspectiva. Madrid, ES. Revista Universia Business Review. núm. 29. p 72.
- INDECI (Instituto Nacional de Defensa Civil). 2005. Guía Marco de Elaboración de Plan de Contingencias. México, ME. p 4. Consultado, 2 de jun. 2012. Formato PDF.
- Lara, R. 2009. Plan de Contingencia Informático del “Conjunto de bodegas Parkenor”. Tesis. Ing. Sistemas. ESPE. Quito, EC. p 14.
- Morales, N; Alfaro, D. 2008. Génesis de las contingencias catastróficas: etiopatogenia del desastre. PE. Revista Peruana de Medicina Experimental y Salud Pública. Vol. 25. p. 104.
- Marulanda, C; López, M; Cuesta, C. 2009. Modelos de desarrollo para gobierno ti. Pereira, CO. Revista Scientia Et Technica. Vol. XV. Núm. 41. pág. 186.
- MAP (Ministerio de Administración Pública). 2006. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid, España. p 7. Consultado 8 de jul. 2012. Formato PDF. Disponible en <http://publicaciones.administracion.es>.

- PBP (Premier Business Partner). 2010. La guía fundamental para la recuperación de desastres: Cómo garantizar la continuidad en equipos informáticos y actividades comerciales. California, EE.UU. p 1. Consultado, 16 de jul. 2012. Formato PDF. Disponible en <http://www.visionsolution.com>.
- Pertier, T. 2001. Information Security Risk Analysis. Auerbach. London. Zulia, VE. Revista Enlace: Revista Venezolana de Información, tecnología y conocimiento. Vol. 6. Núm. 1. p 37.
- Ramírez, G; Alvares, E. 2003. Auditorías a la gestión de las tecnologías y sistemas de información. Lima, PE. Revista Industrial Data. Vol. 6. Núm. 001. pág. 101.
- Seminario Plan de contingencias informáticas (2006, Bogotá). 2006. Contingencias, recuperación de desastres y continuidad de los servicios. Bogotá.CO. p 9.
- Sena, L; Tenzer, M. 2004. Introducción al riesgo informático. Uruguay. p 2. Consultado, 9 Ago. 2012. Formato PDF. Disponible en <http://www.ccee.edu.uy/ensenian/catcomp/material/riesgo.pdf>.
- Semblantes V. 2005. El Ecuador frente a los desastres naturales. Ecuador. p 3. Consultado, 11 de Ago. 2012. Formato PDF. Disponible en http://www.acose.org/publicaciones/presentaciones/Ecuador_frente_a_los_desastres_naturales.pdf.
- Paton, D. 2004. Business Continuity During and After Disaster: Building Resilience through Continuity Planning and Management. Disponible en <http://www.bepress.com/jhsem>.

SNR (Secretaría Nacional de Gestión de riesgo). 2010. Guía Institucional de Gestión de Riesgos 2010. Quito. EC. Formato PFD. pág. 6-9. Disponible en <http://www.snriesgo.gov.ec>.

Szlafsztein, C. 2006. Análisis de las coberturas aseguradoras públicas contradesastres naturales en algunos países de América Latina. Cali, CO. Ingeniería de Recursos Naturales y del Ambiente. Núm. 5. p. 6.

Velasco, A. 2008. El derecho informático y la gestión de seguridad de la información una perspectiva con base a la norma ISO 27001. Barranquilla, CO. Revista de Derecho. Vol. 029. pág. 337.

ANEXOS

ANEXO 1

**FOTOGRAFÍAS DE LA INFRAESTRUCTURA DEL PALACIO MUNICIPAL Y
DEL PATRONATO DE AMPARO SOCIAL DEL CANTÓN JUNÍN**



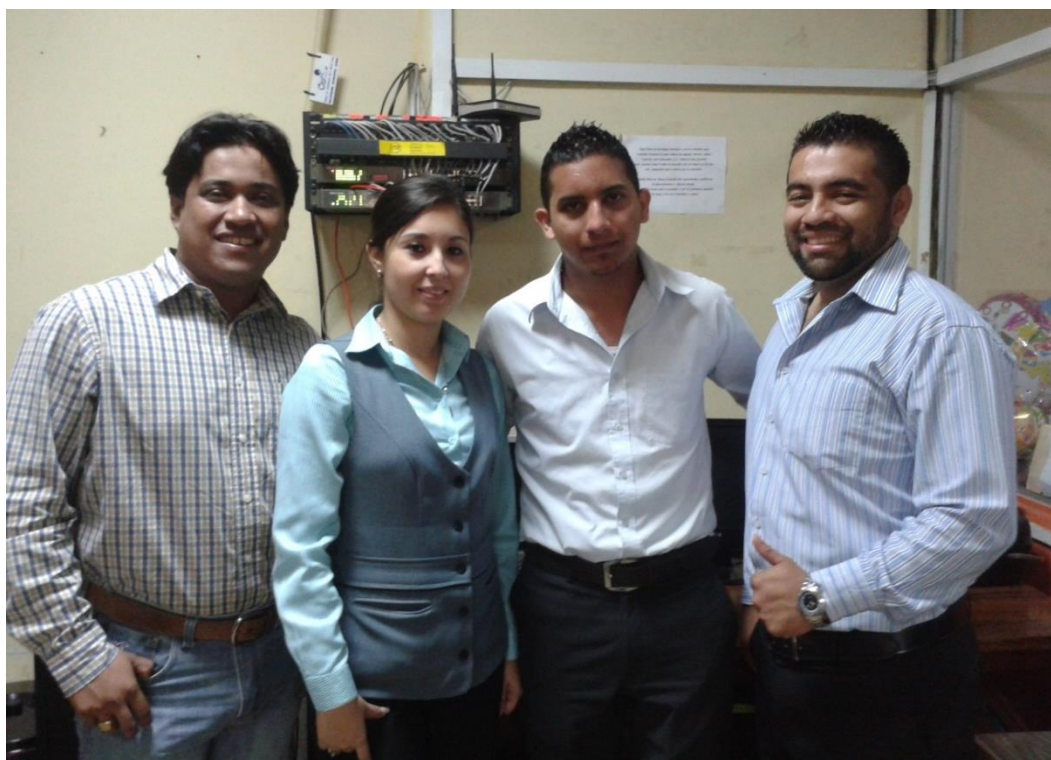
Anexo 1-A. Vista De La Fachada Frontal Del Gobierno Autónomo Descentralizado Municipal Del Cantón Junín

ANEXO 2

**ACTIVIDADES REALIZADAS DENTRO DEL GAD MUNICIPAL DEL
CANTÓN JUNÍN POR LOS AUTORES**



Anexo 2-A. Entrevista Realizada Al Jefe Del Departamento Tecnológico



Anexo 2-B. Personal Municipal que labora en el Departamento Tecnológico y Autores.



Anexo 2-C. Censo realizado a los equipos y sistemas informáticos del GAD Municipal del Cantón Junín

ANEXO 3
ENLACES WIFI



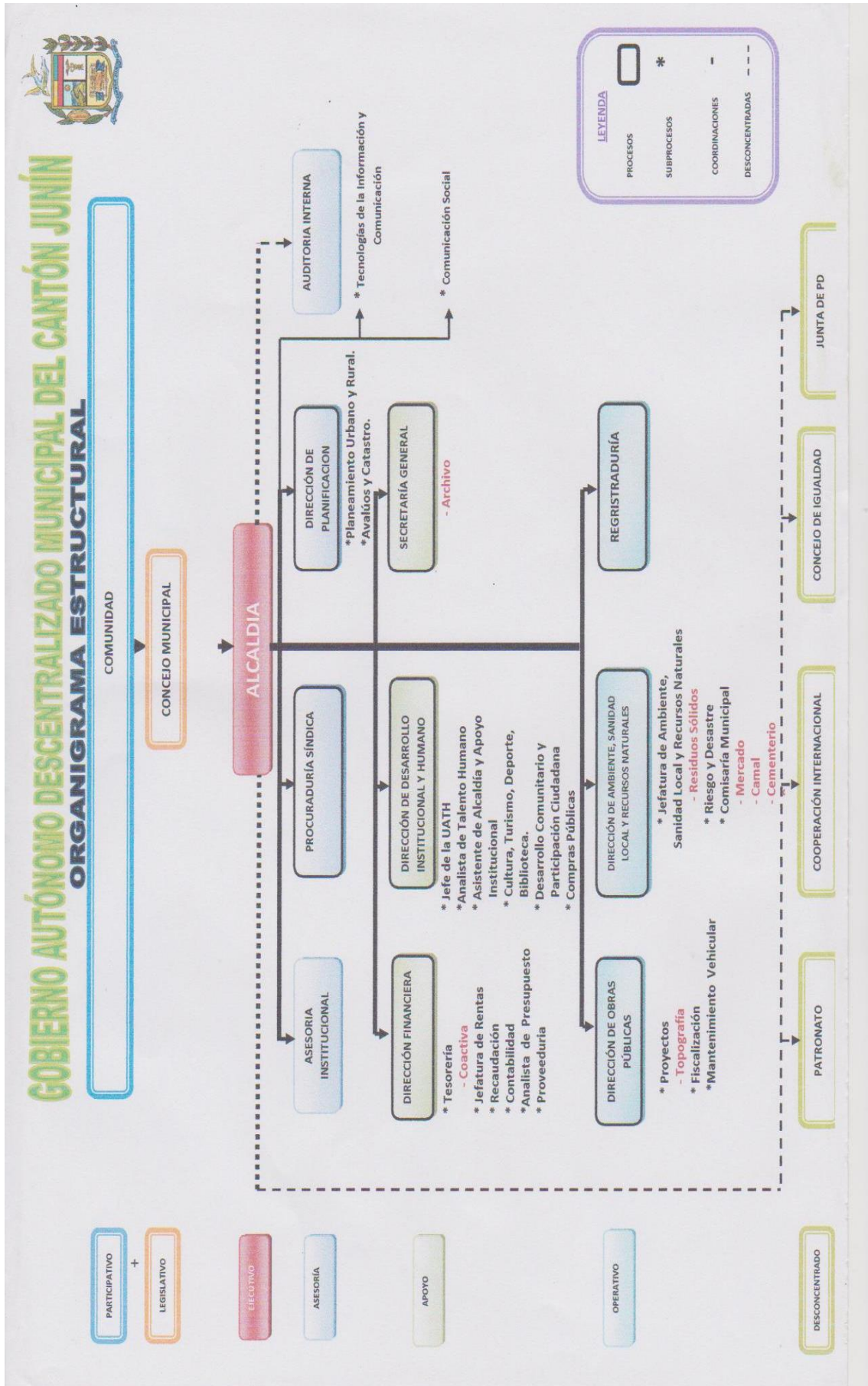
Anexo 3-A. Vista de la antena Omdireccional del GAD Municipal del Cantón Junín



Anexo 3-B. Vista de la antena Ubiquiti Nano Station 2 de 2.4 GHz del GAD Municipal del Cantón Junín

ANEXO 4

ORGANIGRAMA ESTRUCTURAL



Anexo 4-A. Organigrama Estructural del GAD Municipal del Cantón Junín

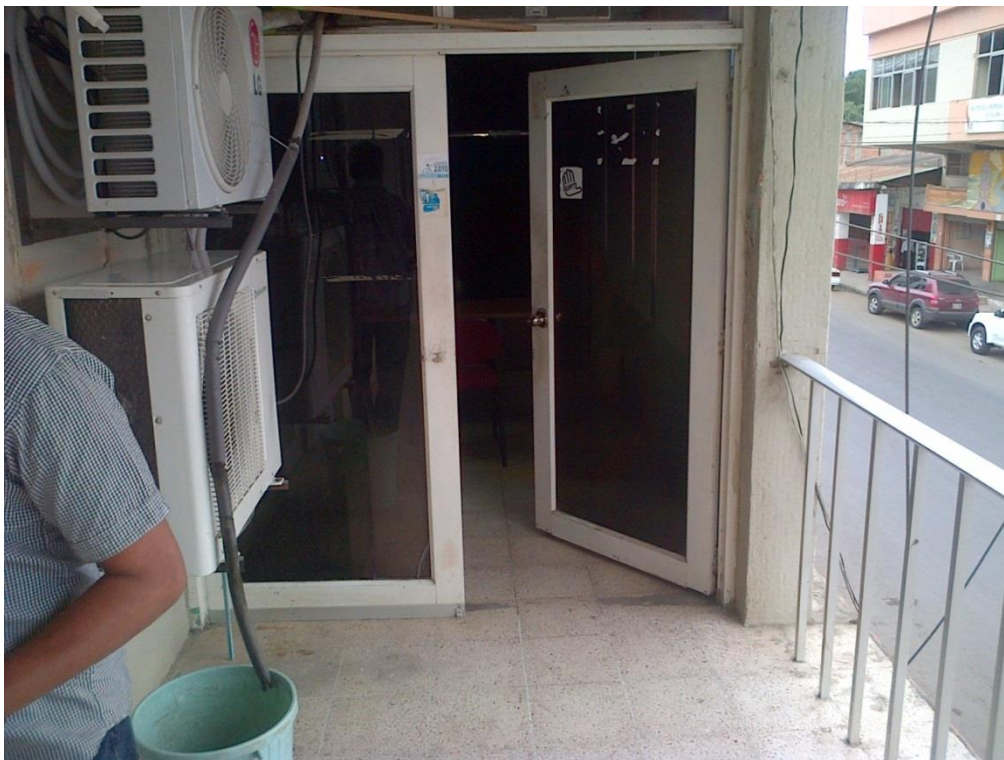
ANEXO 5
ESPACIOS CRÍTICOS



Anexo 5-A. Hacinamiento de servidores informáticos en el Departamento Tecnológico



Anexo 5-B. Escasa seguridad de los equipos de red



Anexo 5-C. Riesgo permanente para los activos del GAD Municipal del Cantón Junín

ANEXO 6

PROPUESTA PARA LA CONTINUIDAD DE SERVICIO



Anexo 6-A. Fachada frontal del Edificio del Patronato Municipal de Amparo Social



Anexo 6-B. Espacio para la implementación provisional de oficinas Municipales

ANEXO 7

**PLAN DE CONTINGENCIA DE LOS EQUIPOS Y SISTEMAS
INFORMATICOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DEL CANTÓN JUNÍN**



**PLAN DE CONTINGENCIA DE LOS EQUIPOS Y SISTEMAS
INFORMATICOS DEL GOBIERNO AUTÓNOMO
DESCENTRALIZADO MUNICIPAL DEL CANTÓN JUNÍN**

Escuela Superior Politécnica Agropecuaria de
Manabí – Manuel Félix López (ESPAM – M.F.L)

Anexo 7-A. Portada del Plan de Contingencia de los equipos y sistemas informáticos del Gobierno Autónomo Descentralizado Municipal Del Cantón Junín

ESTRUCTURA DEL DOCUMENTO

1. FICHA TÉCNICA.....	3
1.1. NOMBRE DEL PROYECTO:.....	3
1.2. FASE DE OPERACIÓN:.....	3
1.3. RAZÓN SOCIAL:.....	3
1.4. DIRECCIÓN, DOMICILIO, TELÉFONO, FAX, CORREO ELECTRÓNICO:.....	3
1.5. REPRESENTANTE LEGAL:.....	3
1.6. COMPOSICIÓN DEL EQUIPO TÉCNICO:.....	4
3. METODOLOGÍA.....	6
4. OBJETIVOS.....	7
4.1. OBJETIVOS GENERALES.....	7
4.2. OBJETIVOS ESPECÍFICOS.....	7
5. ALCANCE Y COBERTURA.....	7
6. MARCO LEGAL.....	7
7. LÍNEA BASE DEL CANTÓN.....	7
8. LA INSTITUCIÓN.....	7
8.1. MISIÓN.....	16
8.2. VISIÓN.....	16
8.3. FUNCIONES.....	16
8.4. ORGANIGRAMA.....	18
8.5. ESTRUCTURA DEL EDIFICIO MUNICIPAL.....	19
9. DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.....	22
10. PLAN DE CONTINGENCIA INFORMÁTICO.....	24
10.1. ACTIVOS INFORMÁTICOS RELEVANTES DE LA INSTITUCIÓN.....	24
10.2. AMENAZAS QUE ESTÁN EXPUESTOS LOS ACTIVOS.....	35
10.3. ESTIMACIÓN DEL IMPACTO Y EL RIESGO, DEFINIDO COMO EL DAÑO SOBRE EL ACTIVO DERIVADO DE LA MATERIALIZACIÓN DE LA AMENAZA SEGÚN LAS MEDIDAS YA IMPLEMENTADAS EN LA INSTITUCIÓN.....	38
10.4. SALVAGUARDAS POR AMENAZA.....	43
10.5. ESTRATEGIAS DE CONTINUIDAD DE ACTIVIDADES.....	63
10.5.1. RESPALDO DE SERVIDORES.....	63
10.5.2. SERVIDOR DE ARCHIVOS CENTRALIZADO.....	67
10.5.3. CONTINGENCIAS PARA LOS SISTEMAS INFORMÁTICOS.....	69
10.5.4. CORTE DE SUMINISTRO ELÉCTRICO.....	73
10.5.5. CONTINUIDAD DEL SERVICIO INTERNET.....	74
10.5.6. DESTRUCCIÓN TOTAL DE LAS INSTALACIONES DEL GADM DEL CANTÓN JUNÍN.....	76
10.6. ORGANIGRAMA DE FUNCIONES EN CASO DE EMERGENCIA.....	77
10.7. GUÍA TELEFÓNICA EN CASO DE EMERGENCIAS.....	78

Anexo 7-B. Tabla de contenido del Plan de Contingencia de los equipos y sistemas informáticos del Gobierno Autónomo Descentralizado Municipal Del Cantón Junín

Junín, 28 de agosto de 2013

Señor Licenciado
Sergio Gustavo Alcívar Sánchez
ALCALDE DEL CANTÓN JUNÍN
En su despacho

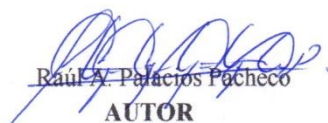
De nuestras consideraciones,

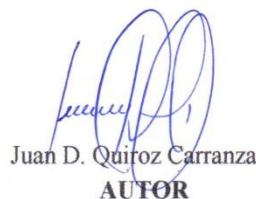
Reciba un cordial y afectuoso saludo de parte de quienes suscribimos la presente, a la vez aprovechamos la oportunidad para hacerle extensivo nuestros más sinceros agradecimientos por habernos dado la oportunidad de poder desarrollar nuestra tesis de grado titulada **“PLAN DE CONTINGENCIA DE LOS EQUIPOS Y SISTEMAS INFORMÁTICOS EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN JUNÍN”**, previa la obtención del título de Ingeniero en Informática.

Producto de nuestra investigación es el **“Plan de Contingencia”** para la Municipalidad, el cual constituye una herramienta invaluable en caso de que se materialice una amenaza, por lo que a la presente nos servimos adjuntar lo mencionado.

Sin otro particular nos suscribimos de Usted.

Cordialmente


Raúl A. Palacios Pacheco
AUTOR


Juan D. Quiroz Carranza
AUTOR



ANEXO 8

PROFORMA DE TELCONET DE SERVICIO DE BACKUP

Descripción	Detalle	Precio	Tipo de Cargo
Servicio BackupNet WorkStation	Servicio BackupNet WorkStation, paquete de 25 usuarios con 100 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac OS y Linux	\$ 375.00	Mensual
Servicio BackupNet WorkStation	Servicio BackupNet WorkStation, paquete de 25 usuarios con 200 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac OS y Linux	\$ 625.00	Mensual
Servicio BackupNet WorkStation	Servicio BackupNet WorkStation, paquete de 25 usuarios con 300 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac OS y Linux	\$ 875.00	Mensual
Servicio BackupNet WorkStation	Servicio BackupNet WorkStation, paquete de 25 usuarios con 400 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac OS y Linux	\$ 1,125.00	Mensual
Servicio BackupNet WorkStation	Servicio BackupNet WorkStation, paquete de 25 usuarios con 500 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac OS y Linux	\$ 1,375.00	Mensual
Entrega de datos en Unidad USB 500GB en DC	Entrega de Backups en instalaciones del datacenter en unidad USB de 500GB por una ocasión	\$ 500.00	Cargo Unico
Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 100 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 75.00	Mensual
Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 200 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 85.00	Mensual

Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 300 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 95.00	Mensual
Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 400 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 105.00	Mensual
Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 500 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 115.00	Mensual
Servicio BackupNet Servidor	Servicio BackupNet Server, paquete de 1 servidor con 1000 GigaBytes por Usuario, incluye un usuario Master y Agentes para Sistemas Operativos Windows, Mac y Linux	\$ 200.00	Mensual
Entrega de datos en Unidad USB 1000GB en DC x svr	Entrega de Backups en instalaciones del datacenter en unidad USB de 1000GB por una ocasión	\$ 800.00	Cargo Unico

Anexo 8-A. Servicio de BACKUP que ofrece TELCONET S.A.

ANEXO 9

CAPACITACIÓN A PERSONAL MUNICIPAL



Anexo 9-A. Capacitación al personal Municipal vinculado a los Departamentos que son parte integral del Plan de Contingencia



Anexo 9-B. Capacitación al personal Municipal vinculado a los Departamentos que son parte integral del Plan de Contingencia