



**UNIVERSIDAD TÉCNICA DE AMBATO**  
**FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E**  
**INDUSTRIAL**  
**CARRERA DE INGENIERÍA EN SISTEMAS**  
**COMPUTACIONALES E INFORMÁTICOS**

**TEMA:**

---

**PLAN DE CONTINGENCIA INFORMÁTICO EN EL GOBIERNO**  
**AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN**  
**SALCEDO PROVINCIA DE COTOPAXI.**

---

**Trabajo de Titulación. Modalidad:** Proyecto de Investigación, presentado previo a la obtención del título de Ingeniero en Ingeniero en Sistemas Computacionales e Informáticos.

**ÁREA:** Administrativas Informáticas.

**LÍNEA DE INVESTIGACIÓN:** Administración de Recursos.

**AUTOR:** Saltos Ponce Cristian Javier.

**TUTOR:** Ing. Julio Balarezo, PhD.

**Ambato - Ecuador**

**Octubre - 2020**

## APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de titulación con el tema: “PLAN DE CONTINGENCIA INFORMÁTICO EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SALCEDO PROVINCIA DE COTOPAXI”, desarrollado bajo la modalidad Proyecto de Investigación por el señor Saltos Ponce Cristian Javier, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que el estudiante ha sido tutorado durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, octubre 2020



Firmado electrónicamente por:  
**JULIO ENRIQUE  
BALAREZO LOPEZ**

---

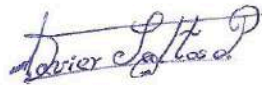
Ing. Julio Balarezo, PhD.

TUTOR

## AUTORÍA

El presente Proyecto de Investigación titulado: “PLAN DE CONTINGENCIA INFORMÁTICO EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SALCEDO PROVINCIA DE COTOPAXI.”. Es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, octubre 2020



---

Saltos Ponce Cristian Javier

CC: 0504232240

AUTOR

## APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por el señor Saltos Ponce Cristian Javier, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación titulado “PLAN DE CONTINGENCIA INFORMÁTICO EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SALCEDO PROVINCIA DE COTOPAXI”, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, octubre 2020



Firmado electrónicamente por:  
**ELSA PILAR  
URRUTIA**

---

Ing. Pilar Urrutia, Mg.

PRESIDENTA DEL TRIBUNAL



Firmado electrónicamente por:  
**DENNIS VINICIO  
CHICAIZA  
CASTILLO**

---

Ing. Dennis Chicaiza, Mg.  
DOCENTE CALIFICADOR



Firmado electrónicamente por:  
**CARLOS ISRAEL  
NUNEZ MIRANDA**

---

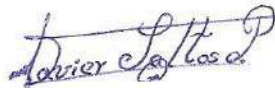
Ing. Carlos Núñez, Mg.  
DOCENTE CALIFICADOR

## DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, octubre 2020



---

Saltos Ponce Cristian Javier

CC: 0504232240

AUTOR

## DEDICATORIA

Quiero dedicar el presente trabajo a Dios, quien me ha brindado fortaleza y sabiduría a lo largo de mi carrera universitaria.

Mi más respetuoso reconocimiento a las personas más importantes de mi vida, mis padres, Luis Saltos y Emperatriz Ponce que juntos con su amor y dedicación me supieron inculcar valores y enseñanzas, para superar mis metas trazadas, por eso quiero contribuir a su felicidad y anhelo.

A mis queridos abuelitos quienes son mis segundos padres, mis dos viejitos que me acompañan en vida y a mis viejitos que partieron y están en el cielo, que gracias a Dios me cobijaron con su amor brindándome sus consejos y bendición.

De manera especial a mi familia por su apoyo constante y motivación para alcanzar a ser un buen profesional siendo así un apoyo y ejemplo para todos, enseñándome a valorar cada esfuerzo que hacen mis padres.

Cristian Javier Saltos Ponce

## AGRADECIMIENTO

El tesoro más valioso que un ser humano puede tener la familia, mi más profundo agradecimiento a todos quienes con sus consejos y fortalezas me motivaron a continuar a lo largo de mi vida.

A la Universidad Técnica de Ambato, por acogerme en sus aulas convirtiéndose en mi segundo hogar, donde a través de docentes adquirí conocimientos, así como la amistad de cada uno de ellos.

A mi tutor, Ing. Julio Balarezo por compartir su conocimiento y experiencia, así como su don de persona que lo caracteriza, brindándome su apoyo y asesoramiento durante la elaboración de mi proyecto de titulación.

Al G.A.D. Municipal del cantón Salcedo, por permitirme elaborar mi proyecto de titulación, de manera especial a la administración del señor Alcalde MSc. Willan Naranjo.

Cristian Javier Saltos Ponce

## ÍNDICE

<b>APROBACIÓN DEL TUTOR</b>	<b>ii</b>
<b>AUTORÍA</b>	<b>iii</b>
<b>APROBACIÓN DEL TRIBUNAL DE GRADO</b>	<b>iv</b>
<b>DERECHOS DE AUTOR</b>	<b>v</b>
<b>DEDICATORIA</b>	<b>vi</b>
<b>AGRADECIMIENTO</b>	<b>vii</b>
<b>RESUMEN EJECUTIVO</b>	<b>xix</b>
<b>ABSTRACT</b>	<b>xx</b>
<b>CAPÍTULO 1 MARCO TEÓRICO</b>	<b>1</b>
1.1 Antecedentes Investigativos . . . . .	1
1.2 Objetivos . . . . .	3
1.2.1 General . . . . .	3
1.2.2 Específicos . . . . .	3
<b>CAPÍTULO 2 METODOLOGÍA</b>	<b>4</b>
2.1 Materiales . . . . .	4
2.1.1 Humanos . . . . .	4
2.1.2 Institucionales . . . . .	4
2.1.3 Otros . . . . .	4
2.1.4 Seguridad informática . . . . .	6
2.1.4.1 Propiedades de un sistema de información seguro	6
2.1.4.2 Análisis de riesgo . . . . .	6
2.1.4.3 Control de riesgo . . . . .	8
2.2 Metodos . . . . .	9



2.2.1	Análisis de algunas metodologías disponibles y ampliamente utilizadas en la actualidad . . . . .	9
2.2.2	Proceso para la gestión de riesgos operativos . . . . .	16
2.2.2.1	Etapa de establecimiento del contexto . . . . .	18
2.2.2.2	Etapa de valoración del riesgo . . . . .	19
2.2.2.3	Etapa de tratamiento del riesgo . . . . .	30
2.2.2.4	Etapa de comunicación y consulta . . . . .	31
2.2.2.5	Etapa de monitoreo y revisión . . . . .	32
2.2.2.6	Etapa de seguimiento . . . . .	33
2.2.3	Modalidad de la Investigación . . . . .	33
2.2.4	Recolección de Información . . . . .	34
2.2.5	Procesamiento y Análisis de Datos . . . . .	34
2.2.6	Desarrollo del Proyecto . . . . .	35

**CAPÍTULO 3 RESULTADOS Y DISCUSIÓN 36**

3.1	Análisis y discusión de los resultados . . . . .	36
3.1.1	Desarrollo de la propuesta . . . . .	36
3.1.2	Etapa de establecimiento del contexto . . . . .	36
3.1.2.1	Consideraciones iniciales del G.A.D. Municipal del cantón Salcedo . . . . .	36
3.1.2.2	Criterios básicos . . . . .	48
3.1.2.3	Alcance y límites . . . . .	53
3.1.2.4	Organización para la gestión del riesgo de seguridad de la información . . . . .	60
3.1.3	Etapa de valoración del riesgo . . . . .	61
3.1.3.1	Identificación del riesgo . . . . .	61
3.1.3.2	Análisis del riesgo . . . . .	74
3.1.3.3	Evaluación del riesgo . . . . .	97
3.2	Plan de contingencia informático . . . . .	99
3.2.1	Contenidos . . . . .	100
3.2.2	Objetivo . . . . .	100
3.2.3	Alcance . . . . .	100
3.2.4	Definiciones . . . . .	101
3.2.5	Comité de roles . . . . .	102
3.2.6	Clases de riesgos que amenazan a la institución . . . . .	104
3.2.6.1	Flujo de lodos y escombros (lahares). . . . .	107
3.2.6.2	Lluvia de ceniza y piroclastos. . . . .	107
3.2.6.3	Sismos (volcánicos/repentinos). . . . .	108

3.2.6.4	Interrupción del servicio de energía eléctrica. . . .	109
3.2.6.5	Filtración de agua. . . . .	109
3.2.6.6	Incendio o Fuego. . . . .	110
3.2.6.7	Daño en el ventilador. . . . .	111
3.2.6.8	Daño en fuente de poder. . . . .	111
3.2.6.9	Falla de disco duro SATA/IDE. . . . .	112
3.2.6.10	Falla de Tarjeta de Red. . . . .	112
3.2.6.11	Fallas de Software/Configuración. . . . .	113
3.2.6.12	Falla de cableado y conectores. . . . .	113
3.2.6.13	Acceso no autorizado (Robo o alteración de información). . . . .	114
3.2.6.14	Ataques DoS o denegación de servicio. . . . .	115
3.2.6.15	Falla de Hardware. . . . .	116
3.2.6.16	Error Humano (Falta de conocimiento). . . . .	116
3.2.6.17	Robo de dispositivos. . . . .	117
3.2.6.18	Atasco de papel en la impresora. . . . .	117
3.2.6.19	El dispositivo no reconoce la impresora. . . . .	118
3.2.6.20	Presencia de interferencias electromagnéticas. . .	118
3.2.6.21	Ingeniería social. . . . .	119
3.2.7	Actividades generales previas al desastre . . . . .	120
3.2.7.1	Equipos Informáticos . . . . .	120
3.2.7.2	Sistemas e Información . . . . .	121
3.2.7.3	Obtención y almacenamiento de los respaldos de Información . . . . .	121
3.2.7.4	Políticas (normas y procedimientos de respaldos)	122
3.2.7.5	Formación de equipos operativos . . . . .	123
3.2.8	Actividades generales durante el desastre . . . . .	124
3.2.8.1	Plan de Emergencias . . . . .	124
3.2.8.2	Formación de Equipos . . . . .	125
3.2.8.3	Entrenamiento . . . . .	125
3.2.9	Actividades generales después del desastre . . . . .	126
3.2.9.1	Evaluación de daños . . . . .	126
3.2.9.2	Priorizar Actividades del Plan de Acción . . . . .	126
3.2.9.3	Ejecución de actividades . . . . .	126
3.2.9.4	Evaluación de los resultados . . . . .	127
3.2.9.5	Retroalimentación del Plan de Acción . . . . .	127
3.2.10	Acciones específicas frente a los tipos de riesgo . . . . .	127

3.2.10.1	Clase de Riesgo: Flujo de lodos y escombros (lahares) . . . . .	128
3.2.10.2	Clase de Riesgo: Lluvia de ceniza o piroclastos . .	133
3.2.10.3	Clase de Riesgo: Sismos (volcánicos/repentinos) .	140
3.2.10.4	Clase de Riesgo: Interrupción del servicio de energía eléctrica . . . . .	144
3.2.10.5	Clase de Riesgo: Filtración de agua . . . . .	149
3.2.10.6	Clase de Riesgo: Incendio . . . . .	153
3.2.10.7	Clase de Riesgo: Daño en el ventilador . . . . .	158
3.2.10.8	Clase de Riesgo: Daño en la fuente de poder . . .	161
3.2.10.9	Clase de Riesgo: Falla de disco duro SATA/IDE .	164
3.2.10.10	Clase de Riesgo: Falla de Tarjeta de Red . . . . .	168
3.2.10.11	Clase de Riesgo: Fallas de Software/Configuración	171
3.2.10.12	Clase de Riesgo: Falla de cableado y conectores .	175
3.2.10.13	Clase de Riesgo: Acceso no autorizado (Robo o alteración de información) . . . . .	180
3.2.10.14	Clase de Riesgo: Ataques DoS o denegación de servicio . . . . .	184
3.2.10.15	Clase de Riesgo: Falla de Hardware . . . . .	187
3.2.10.16	Clase de Riesgo: Error Humano (Falta de conocimiento) . . . . .	191
3.2.10.17	Clase de Riesgo: Robo de dispositivos . . . . .	195
3.2.10.18	Clase de Riesgo: Atasco de papel en la impresora	199
3.2.10.19	Clase de Riesgo: El dispositivo (PC) no reconoce la impresora . . . . .	202
3.2.10.20	Clase de Riesgo: Presencia de interferencias electromagnéticas . . . . .	204
3.2.10.21	Clase de Riesgo: Ingeniería social . . . . .	207
<b>CAPÍTULO 4 CONCLUSIONES Y RECOMENDACIONES</b>		<b>210</b>
4.1	Conclusiones . . . . .	210
4.2	Recomendaciones . . . . .	212
<b>Bibliografía</b>		<b>213</b>
<b>ANEXOS</b>		<b>218</b>

## ÍNDICE DE TABLAS

2.1	Recursos económicos . . . . .	5
2.2	Metodologías de análisis de Riesgos . . . . .	11
2.3	Metodologías de análisis de Riesgos . . . . .	12
2.4	Analogía de las principales técnicas para la gestión de riesgos . . .	15
2.5	NTC-ISO/IEC 27005 con el modelo PHVA . . . . .	16
2.6	Sección 7 de la norma ICONTEC NTC-ISO/IEC 27005 . . . . .	19
2.7	Probabilidad de ocurrencia . . . . .	22
2.8	Parámetros de impacto . . . . .	23
2.9	Niveles de aceptabilidad del riesgo . . . . .	25
2.10	Evaluación del diseño (eficiencia) del control . . . . .	28
2.11	Evaluación del diseño (eficiencia) del control . . . . .	28
2.12	Rangos de eficiencia del control . . . . .	29
3.1	Cargos del personal del departamento de Tecnologías de la Información del G.A.D. Municipal del Cantón Salcedo . . . . .	43
3.2	Cargos del personal primera planta (edificio antiguo y nuevo) . . .	44
3.3	Cargos del personal segunda planta (edificio antiguo y nuevo) . .	44
3.4	Cargos del personal Casa Yerovy Mackuart . . . . .	44
3.5	Cargos del personal Terminal terrestre . . . . .	45
3.6	Análisis FODA del departamento de TI . . . . .	47
3.7	Principales servidores del G.A.D. Municipal del cantón Salcedo . .	48
3.8	Principales computadores a cargo de los funcionarios del departa- mento de TI . . . . .	48
3.9	Informe de las impresoras de tinta y toner dentro del departamento de TI . . . . .	49
3.10	Principales equipos informáticos dentro del departamento de TI .	49
3.11	Principales servidores de la institución y sus principales servicios .	50
3.12	Impacto potencial . . . . .	51
3.13	Valoración de los activos acorde a la disponibilidad, integridad y confidencialidad . . . . .	52

3.14	Valoración de los activos acorde a la disponibilidad, integridad y confidencialidad . . . . .	53
3.15	Matriz de ponderación de amenazas identificadas . . . . .	64
3.16	Listado de los posible riesgos que pueden materializarse . . . . .	67
3.17	Clasificación de causas . . . . .	68
3.18	Clasificación de consecuencias . . . . .	69
3.19	Clasificación inicial según el grado de negatividad . . . . .	69
3.20	Identificación de riesgos en esquema de corbatín (bow tie) . . . . .	70
3.21	Identificación de riesgos en esquema de corbatín (bow tie) . . . . .	71
3.22	Identificación de riesgos en esquema de corbatín (bow tie) . . . . .	72
3.23	Identificación de riesgos en esquema de corbatín (bow tie) . . . . .	73
3.24	Análisis del riesgo sobre el (Servidor 1) . . . . .	76
3.25	Análisis del riesgo sobre el (Servidor 2) . . . . .	77
3.26	Análisis del riesgo sobre el (Servidor 3) . . . . .	78
3.27	Análisis del riesgo sobre el (Servidor 4) . . . . .	79
3.28	Análisis del riesgo sobre el (Servidor 5) . . . . .	80
3.29	Análisis del riesgo sobre el (Servidor 6) . . . . .	81
3.30	Análisis del riesgo sobre el (Servidor 7) . . . . .	82
3.31	Análisis del riesgo sobre las (PCs del departamento de TI) . . . . .	83
3.32	Análisis del riesgo sobre las (Impresoras del departamento de TI) . . . . .	84
3.33	Análisis del riesgo sobre el (Tripp Lite Rack Cpnsole 1URM) . . . . .	85
3.34	Análisis del riesgo sobre el (Cisco Router) . . . . .	86
3.35	Análisis del riesgo sobre (Switches) . . . . .	87
3.36	Análisis del riesgo sobre (Switches) . . . . .	88
3.37	Análisis del riesgo sobre (Switches) . . . . .	89
3.38	Principales integrantes del Plan de Contingencia institucional . . . . .	102
3.39	Principales integrantes del departamento de TI y sus acciones operativas . . . . .	103
3.40	Actores institucionales operativos del G.A.D. SALCEDO . . . . .	104
3.41	Promedio general del análisis de los riesgos sobre los equipos informáticos . . . . .	105
3.42	Tipos de Backups y responsables . . . . .	122
3.43	Coordinación operativa en la atención de la emergencia (Flujo de lodos y escombros, lahares) . . . . .	128
3.44	Coordinación operativa en la atención de la emergencia (Lluvia de ceniza y piroclastos) . . . . .	134
A.1	Servidores del G.A.D. Municipal del cantón Salcedo . . . . .	218

A.2	Principales equipos informáticos del departamento de TI . . . . .	218
B.1	Niveles de prioridad de Sistemas de información del G.A.D. Municipal . . . . .	219
B.2	Principales servicios del G.A.D. Municipal alojados en los servidores de la institución . . . . .	220
B.3	Principales servicios del G.A.D. Municipal alojados en los servidores de la institución . . . . .	221
B.4	Principales servicios del G.A.D. Municipal alojados en los servidores de la institución . . . . .	222
C.1	Formato para el inventario de PC'S de la institución . . . . .	223
D.1	Formato para solicitar acceso a los sistemas de información . . . . .	224
E.1	Formato para la creación de usuario y responsabilidad de contraseña	225
F.1	Formato para el registro de Backups . . . . .	226
G.1	Formato para el registro, tratamiento, y valoración de incidentes . . . . .	227
H.1	Equipos del departamento de tesorería . . . . .	228
H.2	Equipos del departamento de contabilidad . . . . .	229
H.3	Equipos del departamento de rentas . . . . .	229
H.4	Equipos del departamento de avalúos y catastros . . . . .	230
H.5	Equipos del departamento de obras públicas . . . . .	231
H.6	Equipos del departamento de agua potable . . . . .	231
H.7	Equipos del departamento de archivo . . . . .	232
H.8	Equipos del departamento de TI . . . . .	232
H.9	Equipos del departamento de comunicación social . . . . .	232
H.10	Equipos del departamento de compras públicas . . . . .	233
H.11	Equipos del departamento financiero . . . . .	233
H.12	Equipos del departamento de planificación . . . . .	234
H.13	Equipos del departamento de presupuesto . . . . .	234
H.14	Equipos del departamento administrativo . . . . .	235
H.15	Equipos del departamento de la alcaldía . . . . .	235
H.16	Equipos del departamento de secretaría general . . . . .	235
H.17	Equipos del departamento de auditoría - procuraduría . . . . .	236
H.18	Equipos del departamento de desarrollo organizacional . . . . .	236
H.19	Equipos del departamento de talento humano . . . . .	236

H.20 Equipos del departamento de gestión ambiental y servicios públicos	237
H.21 Equipos del departamento de archivo financiero . . . . .	237
H.22 Equipos del departamento de los consejales . . . . .	238
H.23 Equipos del departamento de fiscalización . . . . .	238
H.24 Equipos del departamento de bodega . . . . .	239
H.25 Equipos del departamento de seguridad ciudadana . . . . .	239
H.26 Equipos del departamento de cultura y patrimonio . . . . .	239
H.27 Equipos del departamento de desarrollo humano . . . . .	240
H.28 Equipos del departamento de turismo . . . . .	240
H.29 Equipos del departamento del terminal . . . . .	241

## ÍNDICE DE FIGURAS

2.1	Organigrama de seguridad informática y plan de contingencia. . .	9
2.2	Proceso para la gestión del riesgo . . . . .	17
2.3	Identificación de riesgos en esquema de corbatín (bow tie) . . . .	20
2.4	Frase del riesgo . . . . .	21
2.5	Matriz de calificación de riesgos operativos . . . . .	24
2.6	Identificación de riesgos en esquema de corbatín (bow tie) . . . .	27
2.7	Tiempos ante el diseño del plan de contingencia . . . . .	31
3.1	Organigrama G.A.D Municipal del cantón Salcedo . . . . .	40
3.2	Actualización del organigrama G.A.D Municipal del cantón Salcedo	41
3.3	Primera planta edificio antiguo y nuevo . . . . .	42
3.4	Segunada planta edificio nuevo . . . . .	42
3.5	Segunda planta edificio antiguo y tercera planta del edificio nuevo	43
3.6	Investigar sobre tecnología útil para la institución. . . . .	54
3.7	Determinar necesidades de automatización. . . . .	55
3.8	Elaborar planes informáticos. . . . .	56
3.9	Mantenimiento de sistemas. . . . .	57
3.10	Asesoramiento institucional . . . . .	58
3.11	Red de área local (LAN) . . . . .	59
3.12	Vista Satelital ubicación geográfica de G.A.D. Municipal del cantón Salcedo . . . . .	60
3.13	Riesgos para la seguridad de la información. . . . .	61
3.14	Principales capas concéntricas del planeta Tierra . . . . .	62
3.15	Representación de las diferentes “placas tectónicas” . . . . .	63
3.16	Subducción de la placa Nazca bajo la Sudamericana . . . . .	63
3.17	Mapa de rutas de evacuación y zonas seguras de Salcedo . . . . .	65
3.18	Matriz de calificación de riesgos operativos (Servidor 1) . . . . .	90
3.19	Matriz de calificación de riesgos operativos (Servidor 2) . . . . .	91
3.20	Matriz de calificación de riesgos operativos (Servidor 3) . . . . .	91
3.21	Matriz de calificación de riesgos operativos (Servidor 4) . . . . .	92
3.22	Matriz de calificación de riesgos operativos (Servidor 5) . . . . .	92



3.23	Matriz de calificación de riesgos operativos (Servidor 6) . . . . .	93
3.24	Matriz de calificación de riesgos operativos (Servidor 7) . . . . .	93
3.25	Matriz de calificación de riesgos operativos (PCs TI) . . . . .	94
3.26	Matriz de calificación de riesgos operativos (Impresoras TI) . . . . .	94
3.27	Matriz de calificación de riesgos operativos (Tripp Lite Rack Console)	95
3.28	Matriz de calificación de riesgos operativos (Cisco Router) . . . . .	95
3.29	Matriz de calificación de riesgos operativos (Switches) . . . . .	96
3.30	Matriz de calificación de riesgos operativos (Red de datos) . . . . .	96
3.31	Matriz de calificación de riesgos operativos (Información) . . . . .	97
3.32	Promedio general del análisis de los riesgos sobre los equipos informáticos . . . . .	106
3.33	Acciones frente al flujo de lodos y escombros (lahares) . . . . .	133
3.34	Acciones frente a la lluvia de ceniza y piroclastos . . . . .	139
3.35	Acciones frente a sismos volcánicos o repentinos . . . . .	144
3.36	Acciones frente a la interrupción del servicio de energía eléctrica .	148
3.37	Acciones frente a una filtración de agua . . . . .	152
3.38	Acciones frente a un incendio . . . . .	157
3.39	Acciones frente a un daño de ventilador. . . . .	160
3.40	Acciones frente a un daño de la fuente de poder . . . . .	163
3.41	Acciones frente a una falla de disco duro SATA/IDE . . . . .	167
3.42	Acciones frente a la falla en la tarjeta de red . . . . .	170
3.43	Acciones frente a una falla de software/configuración . . . . .	174
3.44	Acciones frente a una falla de cableado y conectores de red . . . . .	178
3.45	Acciones frente a una falla de cableado eléctrico . . . . .	179
3.46	Acciones frente al acceso no autorizado (robo o alteración de la información) . . . . .	183
3.47	Acciones frente a los ataques DoS o denegación de servicio . . . . .	186
3.48	Acciones frente a una falla de hardware . . . . .	190
3.49	Acciones frente a un error humano (falta de conocimiento) . . . . .	194
3.50	Acciones frente a un robo de dispositivos . . . . .	198
3.51	Acciones frente a un atasco de papel en la impresora . . . . .	201
3.52	Acciones frente a un equipo que no reconoce la impresora . . . . .	203
3.53	Acciones frente a inteferencias electromagnéticas . . . . .	206
3.54	Acciones frente a un caso de ingeniería social . . . . .	209
I.1	Autorización para la valoración de los activos (página 1) . . . . .	242
I.2	Autorización para la valoración de los activos (página 2) . . . . .	243
I.3	Autorización para la valoración de los activos (página 3) . . . . .	244

I.4	Autorización para la valoración de los activos (página 4)	245
I.5	Autorización para la valoración de los activos (página 5)	246
I.6	Autorización para la valoración de los activos (página 6)	247
I.7	Autorización para la valoración de los activos (página 7)	248
I.8	Autorización para la valoración de los activos (página 8)	249
I.9	Autorización para la valoración de los activos (página 9)	250
I.10	Autorización para la valoración de los activos (página 10)	251
I.11	Autorización para la valoración de los activos (página 11)	252
I.12	Respaldo de la valoración, firma del Jefe del departamento de TI	253
I.13	Respaldo de la valoración, firma del Analista de Sistemas	254
I.14	Respaldo de la valoración, firma del Técnico de Sistemas	254

## RESUMEN EJECUTIVO

El presente Plan de Contingencia Informático elaborado para el G.A.D. Municipal del cantón Salcedo involucra un análisis detenido ante posibles catástrofes, pérdidas materiales, robo o alteración de la información entre otros riesgos a los cuales se encuentran expuestos los equipos informáticos y por ende sus sistemas de información. Se considera la aplicación de medidas de seguridad al departamento de TI con las acciones respectivas que deberán tomarse de manera inmediata tras materializarse algún desastre contra daños producidos por hechos naturales o por el hombre y de esta manera estar preparados para afrontar contingencias de cualquier tipo, retomando así la operatividad de la institución con la brevedad del caso evitando así grandes pérdidas económicas.

Sin embargo el departamento de TI (Tecnologías de la Información) es el responsable de garantizar una correcta operatividad de las actividades desarrolladas en la institución por este motivo se hace necesario contar con un plan de contingencia orientado a establecer un adecuado sistema de seguridad física y lógica ante posibles desastres. Como primer aspecto del plan es la organización de la contingencia, en el presente proyecto se hace un estudio de los posibles riesgos que se han visto involucrados dentro de la institución a lo largo del tiempo, considerando la experiencia del personal de seguridad institucional como de los miembros del departamento de TI, que serán el punto de partida para este plan de contingencia. Como segundo aspecto se tendrá una breve descripción de algunas metodologías disponibles y ampliamente utilizadas en la actualidad en la cual se elegirá la que más se adapte a la institución y contribuya adicionalmente al cumplimiento de la Norma 410-11 de la C.G.E. (Contraloría General del Estado) del Ecuador, que corresponde a la aprobación de un plan de contingencia informático en una entidad pública.

El diseño de un Plan de Contingencia Informático basado en la Norma 410-11 de la C.G.E. que se plantea en el presente proyecto permitirá establecer prioridades claras sobre que tipo de procesos son los más esenciales para la institución ayudándola a recobrar el control y restablecer la marcha normal de sus actividades.

**PALABRAS CLAVES:** riesgo, equipos informáticos, sistemas de información, Norma 410-11 de la (C.G.E.), plan de contingencia informático, procesos.

## ABSTRACT

This Computer Contingency Plan prepared for the G.A.D. Municipal of the canton Salcedo involves a careful analysis before possible catastrophes, material losses, theft or alteration of the information among other risks to which the computer equipment and therefore its information systems are exposed. The application of security measures to the IT department is considered, with the respective actions that must be taken immediately after a disaster has materialized against damage caused by natural or man-made events and, in this way, be prepared to face contingencies of any kind, retaking thus the operation of the institution with the brevity of the case thus avoiding large economic losses.

However, the IT (Information Technology) department is responsible for ensuring the correct operation of the activities carried out in the institution, for this reason it is necessary to have a contingency plan aimed at establishing an adequate physical and logical security system. before possible disasters. As the first aspect of the plan is the organization of the contingency, in this project a study is made of the possible risks that have been involved within the institution over time, considering the experience of institutional security personnel as well as the members of the IT department, who will be the starting point for this contingency plan. As a second aspect, there will be a brief description of some methodologies available and widely used at the present time, in which the one that best suits the institution and additionally contributes to compliance with Regulation 410-11 of the C.G.E. (General Comptroller of the State) of Ecuador, which corresponds to the approval of a computer contingency plan in a public entity.

The design of a Computer Contingency Plan based on Regulation 410-11 of the C.G.E. The proposal of this project will allow establishing clear priorities on what type of processes are the most essential for the institution, helping it to regain control and restore the normal course of its activities.

**KEY WORDS:** risk, computer equipment, information systems, Regulation 410-11 of the (C.G.E.), computer contingency plan, processes.

# CAPÍTULO 1

## MARCO TEÓRICO

### 1.1. Antecedentes Investigativos

Dentro de los diferentes trabajos de investigación a nivel internacional y a nivel país en el campo de las medidas de prevención y protección de la información ante diversos tipos de amenazas en una institución, se pueden mencionar los siguientes trabajos:

En México en el año 2009, en la Universidad Nacional Autónoma de México se desarrolló la tesis titulada “Propuesta de aplicación de una metodología para la Seguridad Informática en la división de Ciencias Básicas”. Elaborado por Gaínza Sánchez Sabino.[1] Este trabajo de grado se basa en un análisis exhaustivo sobre los antecedentes de seguridad donde se elabora un plan de continuidad del negocio y un plan de recuperación de desastres en el que se detectan áreas que es indispensable tomar en cuenta para clasificar las estrategias de procesos además de una concientización a todo el personal de la importancia de la seguridad informática en el que representa como un primer paso para una seguridad óptima.

En Guatemala en el año 2015, en la Universidad de San Carlos de Guatemala se desarrolló la tesis titulada “Seguridad Informática orientada a particulares”. Elaborado por Flores Barco Jorge.[2] Como aporte a la investigación en el documento redacta diversas estadísticas sobre ataques malintencionados que afectan directamente a personas particulares en la que se muestra grandes cifras de ataques a nivel mundial.

En Valledupar – Colombia en el año 2018, en la Universidad Nacional Abierta y a Distancia UNAD se desarrolló la tesis titulada “Diseño de un Plan de Contingencia Informático basado en las normas ISO/IEC 22301 e ISO/IEC 27031 para la ferretería Cesar S.A.S”. Elaborado por Shirley Pitta Picón.[3] La misma que creo un conjunto de tácticas preventivas, de recuperación y procedimientos que buscan prevenir posibles fallos informáticos y/o restaurar de manera ordenada, ágil la infraestructura tecnológica en caso de incidentes que provoquen una paralización en las actividades de la institución.

En Ibarra – Ecuador en el año 2015, en la Universidad Técnica del Norte se desarrolló la tesis titulada “Plan de Contingencia para la Unidad de Sistemas y Tecnología de Información del G.A.D. Antonio Ante en base a la norma ISO/IEC 27002.” Elaborado por Karina Méndez Luna.[4] El proyecto de investigación analiza una metodología para el desarrollo de un plan de contingencia en el que evalúa los escenarios de contingencia y así brindar soluciones que permitan garantizar la continuidad de las actividades, de la misma manera se toma en cuenta el artículo 410-11 de la Ley de Control Interno del Ecuador para brindar la seguridad necesaria a la institución.

En Quito – Ecuador en el año 2016, en la Escuela Politécnica Nacional se desarrolló la tesis titulada “Propuesta de una Plan de Contingencia de TI para la empresa LOGICIEL”. Elaborado por Diana Pacheco Pozo.[5] El trabajo de grado presenta el desarrollo de marcos de referencia donde se realizó un análisis comparativo para establecer un modelo donde se explique las etapas para elaborar un plan de contingencia de forma sencilla y fácil. De esta manera enfocarse en la continuidad del negocio y disminuir pérdidas considerables de dinero.

En Sangolquí – Ecuador en el año 2014, en la Universidad de las Fuerzas Armadas ESPE se elaboró una tesis de maestría titulada “Plan de contingencias para el área de tecnologías de la información de CTT ESPE CECAI innovativa Matriz Sangolquí”. Elaborado por Ing. Lilian Alcívar Valencia.[6] El trabajo presenta un estudio en cuanto a la factibilidad operativa que es cubierto por el Plan de Contingencias las 24 horas del día los 365 días del año donde se apoya en el marco legal en las Normas de Control Interno para el Sector Público.

En Ambato – Ecuador en el año 2018, en la Universidad Técnica de Ambato se elaboró la tesis titulada “Plan de riesgos y contingencias informáticas basado en un acuerdo de nivel de servicio aplicada a la Empresa Plasticaucho Industrial”. Elaborado por Guevara Aulestia David.[7] Esta tesis identifica el nivel de riesgo en que se encontraban los activos informáticos, para establecer procesos de gestión que reduzcan el impacto ante una amenaza. Demostrando que para una organización es de vital importancia contar con un Plan de Contingencia en el que se pueda garantizar la continuidad del negocio.

## **1.2. Objetivos**

### **1.2.1. General**

Diseñar un plan de contingencia informático para el área de TI en el G.A.D Municipal del cantón Salcedo de la provincia de Cotopaxi, amparando el cumplimiento de la Norma 410-11 de la C.G.E. (Contraloría General del Estado) del Ecuador.

### **1.2.2. Específicos**

- Evaluar los sistemas informáticos que se encuentran alojados en los distintos departamentos para conocer el nivel de exposición al que se enfrentan.
- Identificar las posibles fallas que pueden originarse frente a daños catastróficos por diversos factores de riesgo humano o físicos.
- Categorizar el nivel de impacto que pueden afectar a los servicios con la que la institución actualmente cuenta.
- Crear un plan de contingencia informático basado en las normas de control interno para organismos del sector público del Ecuador.

## **CAPÍTULO 2**

### **METODOLOGÍA**

#### **2.1. Materiales**

##### **2.1.1. Humanos**

- Investigador.
- Docente tutor de la investigación de la Universidad Técnica de Ambato, Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Carrera de Ingeniería en Sistemas Computacionales e Informáticos.
- Alcalde del G.A.D. Municipal del cantón Salcedo.
- Jefe del departamento de sistemas del G.A.D. Municipal del cantón Salcedo.

##### **2.1.2. Institucionales**

- Bibliotecas y repositorios virtuales de la Universidad Técnica de Ambato.
- Departamento de Tecnologías de la Información - G.A.D. Municipal del cantón Salcedo.
- Acceso a internet que brinda la Universidad Técnica de Ambato.

##### **2.1.3. Otros**

El financiamiento del proyecto será cubierto en su totalidad por el investigador.



No.	Descripción	Unidad	Cantidad	Valor Unitario	Total
1	servicio de internet	mensual	4	\$ 18,00	\$ 72,00
2	energía eléctrica	mensual	4	\$ 15,00	\$ 60,00
3	copias	c/u	500	\$ 0,02	\$ 10,00
4	impresiones	c/u	500	\$ 0,05	\$ 25,00
5	lápices	c/u	2	\$ 0,50	\$ 1,00
6	esferos	c/u	2	\$ 0,50	\$ 1,00
7	borrador	c/u	1	\$ 0,25	\$ 0,25
8	transporte	mensual	4	\$ 80,00	\$ 320,00
9	laptop	c/u	1	\$ 800,00	\$ 800,00
10	memoria USB	c/u	1	\$ 15,00	\$ 15,00
11					
<b>TOTAL</b>					<b>\$ 1.304,25</b>

Tabla 2.1: Recursos económicos

Fuente: Elaborado por el autor

El presente proyecto de investigación se efectúa de acuerdo con la metodología de investigación bibliográfica dado a que es necesario analizar investigaciones ya existentes, también se cuenta con la investigación aplicada ya que se obtiene información para así procesarla acorde al problema planteado, a su vez es necesario utilizar la investigación de campo en el departamento de TI (Tecnologías de la Información) dentro de la institución pública.

Para el presente proyecto de investigación cuenta con fundamentación teórica.

## **PLAN DE CONTINGENCIA**

Como se menciona en el libro sobre Seguridad informática escrito por Purificación Aguilera, “el plan de contingencias es un instrumento de gestión en el cual consta de varias medidas como son: tecnológicas, humanas y de organización, las cuales garantizan una continuidad de la operatividad ya sea de un negocio o una determinada institución, brindando una protección a los sistemas de información ante peligros que lo amenazan luego de materializarse un riesgo”. [8]

## **SEGURIDAD**

“La RAE para el término seguro, define como estar libre y exento de todo peligro, daño o riesgo”. [9]

## **SEGURIDAD INFORMÁTICA**

“La seguridad informática se encuentra ligada con la protección de la infraestructura informática y por ende a la protección de la integridad y privacidad de la información que se encuentra almacenada en un determinado sistema informático, ante un determinado tipo de amenaza, minimizando los riesgos a los que se encuentran expuestos estos recursos”.[10]

### **2.1.4. Seguridad informática**

#### **2.1.4.1. Propiedades de un sistema de información seguro**

##### **Integridad**

En un artículo sobre, Los pilares de la Seguridad de la Información hace referencia a la integridad como “la característica de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros”.[11]

##### **Confidencialidad**

“El termino está enfocado en la seguridad como disposiciones tanto políticas como legales, en un artículo del organismo de cooperación internacional OECD se refiere a la confidencialidad como el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada”.[12]

##### **Disponibilidad**

Se refiere cuando “los recursos deben estar disponibles cuando sean requeridos en cualquier instante de tiempo”.[13]

#### **2.1.4.2. Análisis de riesgo**

##### **Riesgo**

Como se menciona en la ISO 27000, “el riesgo se encuentra asociado de acuerdo con la posibilidad de que las amenazas se aprovechen de las vulnerabilidades que tenga una institución para causar daños en la misma a sus activos informáticos”.[14]

## **Activo**

En el libro Cuerpo Auxiliar de la Junta de Comunidades de Castilla-La Mancha menciona el activo como un “componente de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización”. Es considerado como parte de un activo a la información, los datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones y recursos humanos los cuales son susceptibles a diferentes ataques.[15]

## **Amenaza**

En un artículo de la Universidad Nacional de Luján una amenaza es considerado como “todo elemento o acción capaz de atentar contra la seguridad de la información, ya que una amenaza surge a partir de la existencia de vulnerabilidades”. [16]

## **Vulnerabilidad**

La vulnerabilidad se define como los “fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que genera un problema. Hay que tomar las medidas de precaución para que la vulnerabilidad sea mínima ya que siempre existirá el riesgo que ocurra un problema” .[17]

## **Ataque**

“Se entiende como ataque informático aquellas acciones deliberadas por actores internos o externos que afectan un sistema informático, redes de datos alámbricas o inalámbricas, estos ataques pueden ser propiciados por una o más personas para causar un perjuicio hacia las infraestructuras tecnológicas” .[18]

## **Impacto**

“Puede ser expresado por las consecuencias o daños que afectan a un activo, atestado contra la integridad o la pérdida de disponibilidad de un negocio” .[19]

### 2.1.4.3. Control de riesgo

## MECANISMOS DE SEGURIDAD

### Físicos

“Se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control. Empleado para proteger físicamente el sistema informático. Las amenazas físicas se pueden producir provocadas por el hombre, de forma accidental o voluntaria, o por factores naturales”. [20]

### Lógicos

En un artículo sobre seguridad informática menciona que “los mecanismos lógicos se encargan de asegurar la parte software de un sistema informático, que se compone de todo lo que no es físico, programas y datos”. [21]

## SERVICIOS DE SEGURIDAD

### Autenticación

“Garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje”. [22]

### No repudio

“Los servicios de no repudio ofrecen una prueba al emisor de que la información fue entregada y una prueba al receptor del origen de la información recibida”. [23]

### Control de acceso

“Los sistemas de control de acceso de seguridad informática resultan muy útiles para autorizar o denegar el ingreso de un usuario, así como también para prevenir fraudes al momento de identificar o autenticar a una persona que intenta ingresar al sistema”. [24]

### Organigrama

Para entender de mejor manera los principales conceptos de seguridad informática y motivo por cual se encuentran vinculados a un plan de contingencia junto con las políticas de seguridad de una determinada institución se representa el siguiente diagrama. Figura 2.1

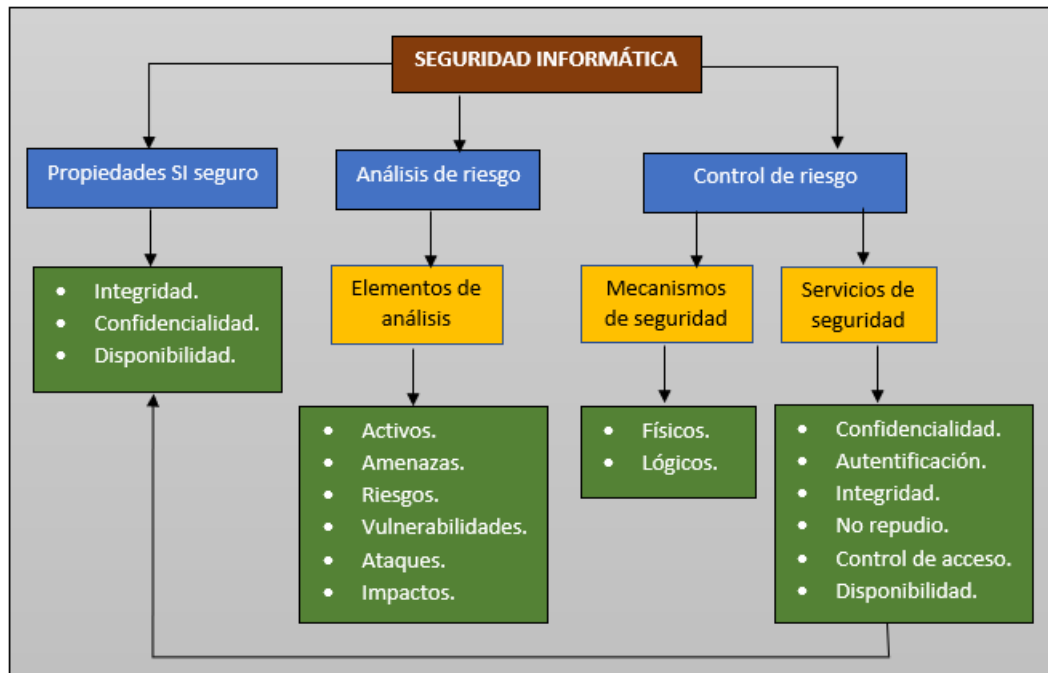


Figura 2.1: Organigrama de seguridad informática y plan de contingencia.  
Fuente: Elaborado por el autor a partir de [8]

## 2.2. Metodos

Existen diversas metodologías para realizar análisis de riesgos.

Para el presente proyecto se hace un estudio de las metodologías disponibles para de esta manera evaluar y elegir aquella que se ajuste a las necesidades de la institución. Se debe tener en cuenta que el análisis de riesgos debe ser revisado periódicamente por lo que, si se hace con una metodología complicada, este trabajo exigirá mucho tiempo y dedicación, de allí la importancia de conocer las metodologías existentes.

### 2.2.1. Análisis de algunas metodologías disponibles y ampliamente utilizadas en la actualidad

#### Breve descripción de metodologías a ser comparadas

### **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**

Se desarrolló en 2001 en la Universidad Carnegie Mellon (CMU), para el Departamento de Defensa de los Estados Unidos, se define como una metodología para ayudar a las organizaciones a minimizar la exposición a amenazas probables y analizar información de manera que se pueda mitigar los riesgos. Existen dos versiones, OCTAVE-S, una metodología simplificada para organizaciones más pequeñas que tienen estructuras jerárquicas planas, y OCTAVE Allegro, una versión más completa para organizaciones grandes o con estructuras multinivel.[25]

**MAGERIT** MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica publicado por el Ministerio de Administraciones Públicas español donde se propone la realización de un análisis de los riesgos que implica la evaluación del impacto ante una violación de la seguridad en la organización. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.[26]

**ESTÁNDAR INTERNACIONAL NTC-ISO/IEC 27005** La NTC-ISO/IEC 27005, esta norma es una adopción idéntica (IDT) por su traducción, respecto a su documento de referencia, la norma ISO/IEC 27005:2008, siendo así una norma Internacional que proporciona directrices para la gestión del riesgo de seguridad de la información en una organización, apoyando en particular los requisitos de una gestión de la seguridad de la información (SGSI) de acuerdo con ISO/IEC 27001. Esta norma describe todo el proceso necesario para la gestión del riesgo de seguridad de la información y las actividades necesarias para la perfecta ejecución de la gestión.[27]

**MEHARI** Método Armonizado de Análisis de Riesgos. Esta metodología fue propuesta y desarrollada por el Club Francés de la Seguridad de la Información CLUSIF en el año 1996. Es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgo. MEHARI se basa en una base de datos de conocimientos y en procedimientos automatizados.[28]

En la tabla 2.2 y en la tabla 2.3 se muestra una comparación entre algunas metodologías disponibles y ampliamente utilizadas en la actualidad.

Metodología	Principales Características	Fases	Ámbito de aplicación	Ventajas	Desventajas
<b>OCTAVE</b>	<p>Octave Tiene dos objetivos específicos que son:</p> <ol style="list-style-type: none"> <li>1. Disminuir la falsa creencia: La Seguridad Informática es un asunto meramente técnico.</li> <li>2. Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos.</li> </ol> <p>Octave divide los activos en dos tipos que son:</p> <ol style="list-style-type: none"> <li>1. Sistemas, (Hardware. Software y Datos).</li> <li>2. Personas.</li> </ol>	<ol style="list-style-type: none"> <li>1. Visión de organización.</li> <li>2. Visión tecnológica.</li> <li>3. Estrategia y desarrollo del plan.</li> </ol>	<p>Análisis de riesgos para seguridad de sistemas de información: PYMES</p>	<ul style="list-style-type: none"> <li>• Es una metodología autodirigida, es decir, la institución gestiona y dirige la evaluación de sus riesgos a través de un equipo multidisciplinario.</li> <li>• Involucra en el proceso a todo el personal de la institución.</li> <li>• Es una de las metodologías más completas ya que incluye elementos tales como: procesos, activos, dependencias, recursos, vulnerabilidades, amenazas y salvaguardas.</li> </ul>	<ul style="list-style-type: none"> <li>• Solo es aplicable en pequeñas y medianas empresas "PYMES".</li> <li>• Usa muchos documentos anexos para llevar a cabo el proceso de análisis de riesgos, lo que la hace tediosa y complicada de entender.</li> <li>• Requiere de profundos conocimientos técnicos.</li> <li>• No explica en forma clara la definición y determinación de los activos de información.</li> </ul>
<b>MAGERIT</b>	<ol style="list-style-type: none"> <li>1. Tomar medidas en la institución para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.</li> <li>2. Está constituido en tres libros: "El Método", un "Catálogo de Elementos" y una "Guía de Técnicas".</li> <li>3. Ayudar a descubrir y planificar las medidas pertinentes para conservar los riesgos bajo control.</li> <li>4. Ofrecer un método sistemático para analizar tales riesgos.</li> </ol>	<ol style="list-style-type: none"> <li>1. Análisis de riesgos.</li> <li>2. Caracterización de los activos: <ol style="list-style-type: none"> <li>a. Caracterización de las amenazas.</li> <li>b. Caracterización de las salvaguardas.</li> <li>c. Estimación del estado del riesgo.</li> </ol> </li> <li>3. Gestionar los riesgos.</li> </ol>	<p>Análisis y gestión de riesgos de los sistemas de información: Gobierno, Organismos, Compañías grandes, PYME, compañías comerciales y no comerciales.</p>	<ul style="list-style-type: none"> <li>• Se le considera con un alcance completo, tanto en el análisis como en la gestión de riesgos.</li> <li>• Valoración en cuanto a disponibilidad, integridad, trazabilidad, autenticidad, y confidencialidad.</li> <li>• No requiere autorización previa para su uso.</li> <li>• Es una metodología líder en España.</li> <li>• De carácter Público.</li> </ul>	<ul style="list-style-type: none"> <li>• El hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa.</li> <li>• No involucra a los procesos, recursos ni vulnerabilidades como elementos del modelo a seguir.</li> </ul>

Tabla 2.2: Metodologías de análisis de Riesgos

Fuente: Elaborado por el autor a partir de [25] [26]

Metodología	Principales Características	Fases	Ámbito de aplicación	Ventajas	Desventajas
<b>NTC-ISO/IEC 27005</b>	<ol style="list-style-type: none"> <li>Describe todo el proceso necesario para la gestión del riesgo de seguridad de la información y las actividades necesarias para la perfecta ejecución de la gestión.</li> <li>Describe formas de valoración.</li> <li>Detalla la forma de identificar activos y hacer su valoración, provee ejemplos.</li> <li>Se ajusta a la metodología de gestión de calidad de Deming, (ciclo PDCA).</li> <li>Presenta ejemplos de amenazas típicas</li> </ol>	<ol style="list-style-type: none"> <li>Establecimiento del plan de comunicación.</li> <li>Establecimiento del contexto organizacional.</li> <li>Valoración de los riesgos.</li> <li>Tratamiento de los riesgos.</li> <li>Monitoreo y mejora continua del proceso de gestión.</li> </ol>	<p>Estándar para la gestión de riesgos de seguridad de la información:</p> <p>Aplicable a cualquier organización sin importar tipo, tamaño o naturaleza.</p>	<ul style="list-style-type: none"> <li>Estándar internacional, lo que le acredita mayor aprobación.</li> <li>Compatible con los conceptos generales especificados en la norma ISO 27001.</li> <li>Permite un análisis completo cuantitativo.</li> <li>Los usuarios elijen el método que mejor se adapte, por ejemplo, una evaluación de riesgos, acorde análisis de riesgos, acorde a la institución.</li> </ul>	<ul style="list-style-type: none"> <li>No detalla la forma de valorar las amenazas.</li> <li>No posee herramientas, técnicas, ni comparativas de ayuda para su implementación.</li> <li>No es certificable.</li> </ul>
<b>MAGERIT</b>	<ol style="list-style-type: none"> <li>Método para la evaluación y gestión de riesgos según requerimientos de ISO/IEC 27005:2008.</li> <li>Comprende bases de datos de conocimiento, con manuales y guías que describen los diferentes módulos (amenazas, riesgos, vulnerabilidades).</li> <li>Modelo de riesgos cualitativo y cuantitativo.</li> <li>Capacidad para evaluar y simular los niveles de riesgo.</li> </ol>	<ol style="list-style-type: none"> <li>Diagnóstico de la Seguridad.</li> <li>Análisis de los Intereses implicados por la Seguridad.</li> <li>Análisis de Riesgos.</li> </ol>	<p>Gobierno, Organismos, Empresas medianas y grandes, compañías comerciales, sin fines de lucro (educación, salud, servicios públicos, Organizaciones no gubernamental).</p>	<ul style="list-style-type: none"> <li>Usa un modelo de análisis de riesgos cualitativo y cuantitativo.</li> <li>Se respalda en los requerimientos de la ISO/IEC 27005:2008.</li> </ul>	<ul style="list-style-type: none"> <li>La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión de los riesgos.</li> <li>Sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información, dejando a un lado el no repudio.</li> </ul>

Tabla 2.3: Metodologías de análisis de Riesgos

Fuente: Elaborado por el autor a partir de [27] [28]



Las metodologías de análisis de riesgo son técnicas que apoyan a la gestión de riesgos donde permiten la evaluación de un proyecto, proceso o institución, las mismas que garantizan etapas aprobadas y estandarizadas para un correcto análisis de riesgos que pueden surgir en la institución.

Por lo que resulta importante conocer las principales características, fases, ámbito de aplicación, ventajas y desventajas relacionadas, y de esta manera elegir la que mejor se adecúe a las necesidades de la institución. Sin embargo, como se puede apreciar en la tabla 2.2 y en la tabla 2.3, la metodología NTC-ISO/IEC 27005 es la que mejor se ajusta a los requerimientos de la institución ya que los demás estándares tienen lineamientos generales sobre la gestión de riesgos, por lo que les hace falta una guía más práctica, que brinde pautas sobre cómo cumplir con los aspectos más importantes de seguridad necesarios como identificar, evaluar, valorar y dar tratamiento a los riesgos.

Para el presente proyecto se ha tomado en cuenta el cumplimiento de la Norma 410-11 de la C.G.E. (Contraloría General del Estado) del Ecuador, que corresponde a la aprobación de un plan de contingencia en el que se detalla las medidas necesarias a considerarse en caso de suscitarse una emergencia o suspensión en el procesamiento de la información. En razón que en la norma 410-11 de la C.G.E. se detallan diversas fases, mismas que al considerar un estudio de las metodologías de análisis de riesgo disponibles se encuentra una similitud entre la metodología NTC-ISO/IEC 27005 y la norma 410-11 de la C.G.E en la descripción de las principales etapas a considerar en cada una de ellas.

### **Norma 410-11 de la Contraloría General del Estado del Ecuador.**

C.G.E. son las siglas de la Contraloría General del Estado, amparada a partir de la emisión de la nueva Constitución de la República del Ecuador, reformas a la Ley Orgánica de la Contraloría General del Estado, para proveer a las entidades, organismos del sector público, de un importante marco normativo a través del cual puedan desarrollarse para alcanzar sus objetivos y maximizar los servicios públicos que deben proporcionar a la comunidad. La C.G.E. aborda diversas normativas las mismas que son concordantes con el marco legal vigente y están diseñadas bajo principios administrativos, disposiciones legales y normativa técnica pertinente. Dado a que en la actualidad la información se a convertido en un ente principal para la sociedad de la información y del conocimiento sendo así un tema de vital importancia para el sector público o privado.[29]

Para la presente investigación se toma en consideración la norma 410-11 que corresponde al “Plan de contingencias”, teniendo en cuenta que el departamento de Tecnologías de Información (TI) debe tomar las medidas pertinentes en caso de ocurrir una emergencia o suspensión en el procesamiento de la información acorde a problemas en los equipos informáticos, programas o personal relacionado.

Los aspectos a considerar según la norma 410-11 de la C.G.E. son:

1. “Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento”.
2. “Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización”.
3. “Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un Data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos”.
4. “Plan de recuperación de desastres que comprenderá:
  - Actividades previas al desastre (bitácora de operaciones).
  - Actividades durante el desastre (plan de emergencias, entrenamiento).
  - Actividades después del desastre”.
5. “Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia”.
6. “El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información”.
7. “El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento”.

Fuente: [29]

A continuación, en la tabla 2.4 se puede apreciar un ajuste de los pasos de la norma 410-11 de la C.G.E con la metodología NTC-ISO/IEC 27005 al contemplar una semejanza entre estas dos grandes técnicas que permiten un correcto análisis de riesgo.

ANALOGÍA ENTRE LAS PRINCIPALES FASES	
NTC-ISO/IEC 27005:2008	Norma 410-11 de la C.G.E del Ecuador
1. Establecimiento del plan de comunicación.	7. El plan de contingencias aprobado será difundido entre el personal responsable de su ejecución.
2. Establecimiento del contexto organizacional. Las empresas tienen un contexto interno que contiene su misión, visión, políticas, objetivos, estrategias, metas, roles y responsabilidades, estructura, normativas internas y externas.	1. Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de TI.  5. Es indispensable designar un comité de roles específicos y nombre de los encargados de ejecutar las funciones.
3. Valoración de los riesgos.  a. Identificación del riesgo. b. Estimación del riesgo. c. Evaluación del riesgo.	4. Plan de recuperación de desastres que comprenderá. a. Actividades previas al desastre. b. Actividades durante el desastre. c. Actividades después del desastre.
4. Tratamiento de los riesgos.	6. El plan de contingencia será un documento de carácter confidencial, que permitirá recuperar la operación de los sistemas de información.
5. Monitoreo y mejora continua del proceso de gestión.	7. El plan de contingencias aprobado será sometido a pruebas, entrenamientos y evaluaciones periódicas.
5. Monitoreo y mejora continua del proceso de gestión.	2. Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan se mantenga actualizado.
5. Monitoreo y mejora continua del proceso de gestión.	3. Plan de continuidad de las operaciones.

Tabla 2.4: Analogía de las principales técnicas para la gestión de riesgos

Fuente: Elaborado por el autor a partir de [29] [30]

El motivo principal que llevo al análisis de algunas metodologías disponibles y ampliamente utilizadas en la actualidad fue contar con un método adecuado para la gestión de riesgos. Es necesario considerar que el G.A.D. Municipal del cantón Salcedo maneja información crítica como son los datos de los ciudadanos, transacciones diarias principalmente cobros de distintos servicios a la ciudadanía del cantón, siendo necesario que toda esta información tenga la seguridad adecuada.

### 2.2.2. Proceso para la gestión de riesgos operativos

En el presente trabajo de investigación define una técnica clara y simple del planteamiento de un método apropiado para la identificación, análisis, evaluación, tratamiento y monitoreo de riesgos.

La metodología propuesta sigue los pasos del proceso de gestión de riesgos NTC-ISO/IEC 27005, que contempla los siguientes 5 niveles:

- Establecimiento del plan de comunicación.
- Establecimiento del contexto organizacional.
- Valoración de los riesgos.
- Tratamiento de los riesgos.
- Monitoreo y mejora continua del proceso de gestión.

Fuente: [27]

Se muestra a continuación en la tabla 2.5, la metodología diseñada junto al modelo “PDCA, por sus siglas en inglés (Plan, Do, Check, Act) ó PHVA en español: Planificar, Hacer, Verificar, Actuar. La familia de estándares ISO 27000 se refiere claramente al ciclo Plan-Do-Check-Act (ciclo PDCA)”.[30]

PHVA	NTC-ISO/IEC 27005	
	Definir Plan de gestión de riesgos	
<b>Planear</b>	Establecimiento del contexto.	<b>Valoración del Riesgo</b>
	Identificación del riesgo.	
	Estimación del riesgo.	
	Evaluación del riesgo.	
	Desarrollar el plan de tratamiento del riesgo.	<b>Proceso de gestión del riesgo</b>
Aceptación del riesgo.		
<b>Hacer</b>	Implementar el plan de tratamiento.	
	Implementar el plan de comunicación del riesgo.	
<b>Verificar</b>	Monitoreo y revisión del riesgo.	
<b>Actuar</b>	Mantener y mejorar el proceso de gestión.	

Tabla 2.5: NTC-ISO/IEC 27005 con el modelo PHVA

Fuente: Elaborado por el autor a partir de [30]

Como se puede apreciar en la Figura 2.2, el ciclo de la gestión de riesgo es iterativo, en el cual la gestión se lo realiza por fases, y en cada fase se obtiene resultados para el siguiente nivel, disminuyendo tiempo y esfuerzo para la municipalidad.

En la Figura 2.2, se puede observar el proceso para la gestión de riesgos según la norma NTC-ISO/IEC 27005.

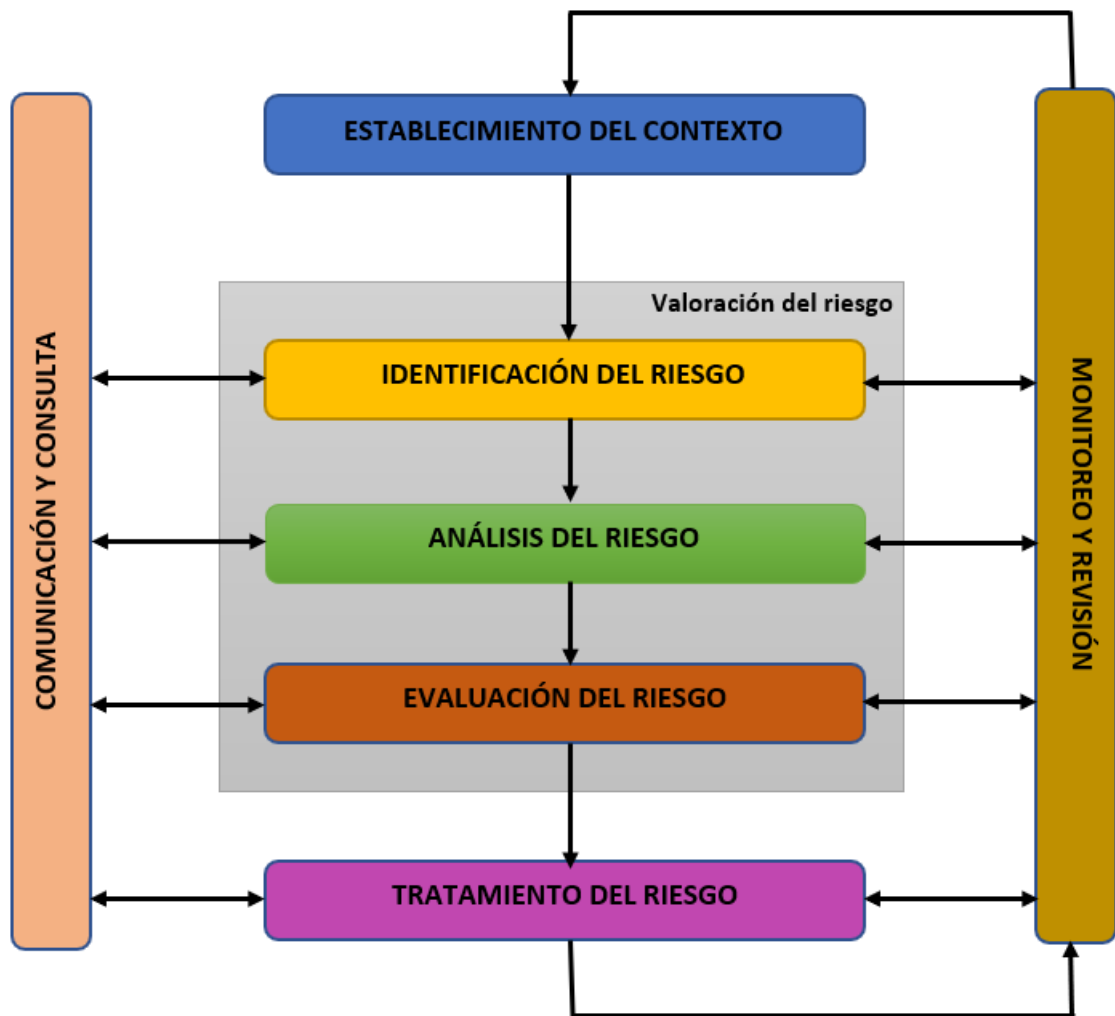


Figura 2.2: Proceso para la gestión del riesgo  
Fuente: Elaborado por el autor a partir de [27]

De acuerdo con lo descrito anteriormente y frente a la incertidumbre que rodea la operación de las actividades en el departamento de TI del G.A.D. Municipal del cantón Salcedo concerniente a la gestión del riesgo de seguridad informática, se ha tomado como referente la norma NTC-ISO/IEC 27005 para una mejor sustentabilidad hacia la norma 410-11 de la C.G.E. (Contraloría General del Estado) del Ecuador, mismas que se ven envueltas en la necesidad de aplicar sistemáticamente una serie de etapas estructuradas enfocadas a identificar, analizar, evaluar y monitorear los riesgos, con el propósito de ayudar a gestionar el riesgo. Dicho proceso está compuesto de cinco (5) etapas, en las que se encuentran inmersos los pasos de la norma 410-11 de la C.G.E. .

A continuación, se explican cada una de las etapas para su posterior desarrollo:

### **2.2.2.1. Etapa de establecimiento del contexto**

Al empezar cualquier tipo de gestión, la primera función que debe ejecutarse es relacionarse con el ambiente en que se desarrollará el trabajo, las personas que de alguna forma irán a interactuar junto con sus cargos desempeñados, es fundamental tener conocimiento de la institución.

Es importante comprender el significado conceptual de “contexto” y su utilidad en la gestión del riesgo. En la búsqueda de su significado, se encuentra, entre otras definiciones, que contexto es un “entorno físico o de situación, político, histórico, cultural o de cualquier otra índole, en el que se considera un hecho”. [9]

Para el desarrollo de esta etapa se puede hacer uso de diferentes técnicas como son entrevistas con expertos en el departamento de TI, reunión con el directivo de la institución. La técnica recomendada para el caso es la aplicación de la matriz DOFA, misma que permitirá descubrir cual es la situación actual de la empresa, en base al diagnóstico, plantear la estrategia a seguir. Para desarrollar correctamente esta etapa se debe tomar en cuenta los factores internos (debilidades y fortalezas) y externos (amenazas y oportunidades).

La sección siete (7) de la norma ICONTEC NTC-ISO/IEC 27005, describe las actividades que deben realizarse en el transcurso de la fase de contexto de la gestión del riesgo. Dichas actividades deben realizarse por el equipo de gestión de riesgo encargado, pero en este caso está a cargo del investigador, siendo realizadas mediante interacciones con los encargados del departamento de TI de la institución evaluada.

La sección 7 de este módulo está organizada de la siguiente forma:

<b>(CONTEXTO) SECCIÓN 7 DE LA NORMA ICONTEC NTC-ISO/IEC 27005</b>		
<b>Nº SECCIÓN</b>	<b>ACTIVIDADES</b>	<b>DESCRIPCIÓN</b>
7.1	Consideraciones iniciales	<ul style="list-style-type: none"> <li>• El objetivo principal de la organización.</li> <li>• Misión de la organización.</li> <li>• Visión de la organización.</li> <li>• Políticas de la organización.</li> <li>• La estructura organizacional.</li> <li>• Las instalaciones.</li> <li>• Los funcionarios y sus roles en la organización.</li> <li>• Análisis de la situación actual del área de TI.</li> </ul>
7.2	Criterios básicos	<ul style="list-style-type: none"> <li>• Principales activos de información involucrados.</li> <li>• La importancia de la disponibilidad, integridad y confidencialidad para las operaciones.</li> <li>• Nivel de clasificación de los activos de información que pueden sufrir un impacto.</li> </ul>
7.3	Alcance y límites	<ul style="list-style-type: none"> <li>• Definir el alcance y los límites de la gestión del riesgo de la seguridad de la información.</li> <li>• Procesos de la organización.</li> <li>• Ubicación geográfica de la organización.</li> </ul>
7.4	Organización para la gestión del riesgo de seguridad de la información.	<ul style="list-style-type: none"> <li>• Establecer una recomendación sobre el proceso de gestión del riesgo y la seguridad de la información.</li> </ul>

Tabla 2.6: Sección 7 de la norma ICONTEC NTC-ISO/IEC 27005

Fuente: Elaborado por el autor a partir de [31]

#### 2.2.2.2. Etapa de valoración del riesgo

Esta etapa comprende las fases de identificación, análisis y evaluación del riesgo.

#### IDENTIFICACIÓN DEL RIESGO

La palabra riesgo hace relación a cualquier evento en la que se puedan presentar resultados no planificados, se consideran cómo aquellas circunstancias que afectan de manera negativa a la institución. Es fundamental que cualquier institución identifique a sus orígenes de riesgo, sus causas y consecuencias. El principal objetivo es plasmar una lista completa de los riesgos basados en eventos que tienen la posibilidad de interrumpir el normal funcionamiento de las actividades de la institución evitando el cumplimiento de sus objetivos. La fase de identificación del riesgo debe ser constante e interactiva, fundamentarse en el resultado del análisis del contexto a partir de la claridad de sus objetivos.

Hay que tomar en cuenta que para identificar los riesgos operativos es importante partir de las debilidades y amenazas detectadas en la institución.

Es necesario considerar que:

- Un activo amenazado es cualquier recurso de la municipalidad, que puede ser afectado por una amenaza. Este activo puede ser tangible (infraestructura física, hardware) o intangible (información, software), ya que si no cuentan con la disponibilidad generarían pérdidas para la institución.
- La amenaza es una ocurrencia de un hecho adverso que puede acontecer en un determinado lugar y que tiene efectos negativos para el activo amenazado provocando que pierda su valor y que trabaje de manera incorrecta perdiendo su disponibilidad para su correcta operación. Se puede considerar que es la materialización del riesgo. (En esta sección se debe incluir la amenaza o debilidad encontrada a partir del análisis del contexto).

Una vez detectado correctamente el riesgo operativo, se procede a relacionar sus causas y consecuencias.

**Causas:** Se puede considerar que son los agentes generadores del riesgo, situaciones, sujetos u objetos que pueden provocar una amenaza. Por lo que las causas van relacionadas con el evento adverso y pueden ser externas o internas.

**Consecuencias:** Se considera como los efectos concretos de la presencia del riesgo que recae sobre el activo amenazado afectando así a la institución.

En un artículo sobre la Iniciativa ERM (Enterprise Risk Management) de la Escuela de Administración de la Universidad de Carolina del Norte, Bonnie Hancock comparte una técnica denominada "análisis de corbata" (bow tie analysis) para evaluar riesgos. Se trata de un esquema sencillo para describir y analizar los riesgos, representando el riesgo en el centro, a la izquierda las posibles causas como agentes generadores del riesgo, a la derecha se encuentran las consecuencias como alcance del daño de la materialización del riesgo.[32]

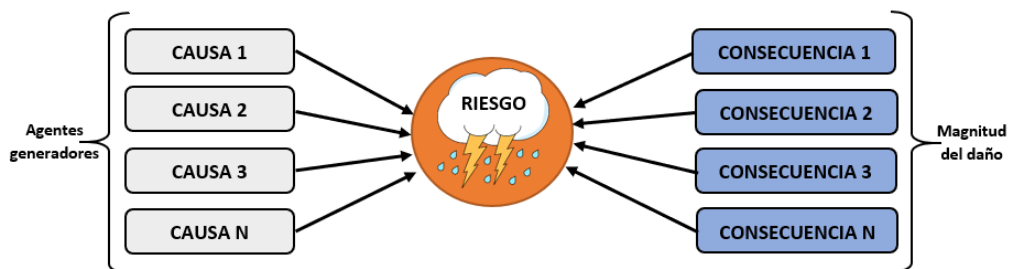


Figura 2.3: Identificación de riesgos en esquema de corbata (bow tie)  
Fuente: Elaborado por el autor a partir de [32]



Para evitar cualquier duda en la identificación del riesgo se puede emplear la frase del riesgo:

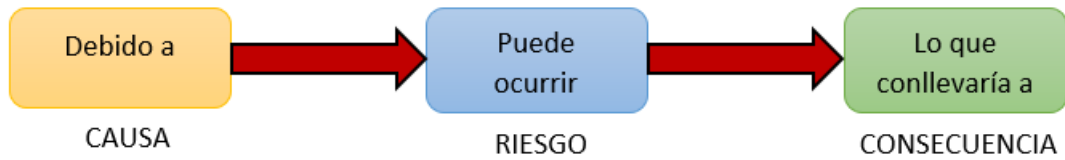


Figura 2.4: Frase del riesgo  
Fuente: Elaborado por el autor

## ANÁLISIS DEL RIESGO

El análisis del riesgo busca establecer su probabilidad de ocurrencia y su factor de exposición (impacto) de materializarse el riesgo y la determinación del riesgo con su correcta evaluación. Este análisis depende de la información obtenida en la identificación de riesgos y el aporte de quienes forman parte del equipo de trabajo del departamento de Tecnologías de la Información (TI) del G.A.D Municipal.

Para determinar la calificación del riesgo depende de los antecedentes de la ocurrencia de dichos riesgos, así como de la experiencia y conocimiento de las personas involucradas en el análisis. Para fines académicos para el caso de estudio se respalda en el método Delphi, datos históricos y estadísticos.

El método Delphi es una técnica de recolección de información que permite obtener la opinión de un grupo de expertos (se sugiere aplicarla mínimo a 3 o 4 personas), en el artículo menciona que es una técnica recomendable cuando no se dispone de información suficiente para la toma de decisiones, para la investigación.[33]

### Análisis de evaluación

Un método de evaluación (Annualized Loss Expectancy o ALE por sus siglas en inglés), mencionado en el libro (INFORMATION SECURITY), por Cesare Gallotiti, enero 2019, en conjunto con la ISO/IEC 27001 STANDARD, permite modelar el impacto que los riesgos de seguridad pueden tener sobre los activos de una organización.[34]

**Parámetros de probabilidad:** Es importante entender bajo qué circunstancias los activos informáticos de la municipalidad se encuentran vulnerables como es la probabilidad de ocurrencia del riesgo misma que se la puede medir mediante criterios de frecuencia, de acuerdo con su respectivo nivel de evaluación según varios factores como pueden ser internos y externos que pueden ocasionar un riesgo.

En la Tabla 2.7 se puede observar la probabilidad de ocurrencia acorde al nivel de frecuencia de cada una de las vulnerabilidades encontradas en la institución.

NIVEL	FRECUENCIA	PROBABILIDAD	DESCRIPCIÓN
5	81-100%	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias. Probabilidad muy alta.
4	61-80%	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias. Probabilidad alta.
3	41-60%	Posible	El evento podría ocurrir en algún momento. Probabilidad media.
2	21-40%	Improbable	El evento puede ocurrir en algún momento. Probabilidad baja.
1	0-20%	Raro	El evento puede ocurrir solo en circunstancias excepcionales. Probabilidad muy baja.

Tabla 2.7: Probabilidad de ocurrencia

Fuente: Elaborado por el autor a partir de [35]

**Parámetros de impacto:** Se entiende como un incidente en el que puede afectar múltiples activos dentro de la municipalidad, los impactos pueden ocurrir de forma inmediata o en futuros, mismos que ocasionarían la interrupción de las actividades y como resultado pérdidas financieras causando malestar en la población.

El impacto se lo mide de acuerdo con el grado de consecuencias que podrían dañar al G.A.D. Municipal, si llegase a presentar el riesgo. Con la finalidad de ubicar con mayor precisión la escala del impacto, se considera las variables (Nivel, Valor impacto, Frecuencia, Nivel de impacto, Descripción, Usuario, Operación, Imagen, Pérdidas económicas), mismas que permitirán tener una percepción concisa de tipo cualitativo sobre el activo amenazado. En la Tabla 2.8 se define el análisis sobre los parámetros de impacto.

NIVEL	VALOR IMPACTO	FRECUENCIA	NIVEL IMPACTO	DESCRIPCIÓN	USUARIO	OPERACIÓN	IMAGEN	PÉRDIDAS ECONÓMICAS
1	1	0-20%	Insignificante	El evento puede ocurrir solo en circunstancias excepcionales. Probabilidad muy baja.	No se ven afectados los usuarios.	No hay interrupción de las operaciones del G.A.D. Municipal.	No se ve afectada la imagen o credibilidad del G.A.D. Municipal.	Pérdidas económicas mínimas.
2	2	21-40%	Menor	El evento puede ocurrir en algún momento. Probabilidad baja.	Baja afectación a los usuarios.	Interrupción de las operaciones del G.A.D. Municipal por algunas horas, menor a un día.	Imagen o credibilidad institucional afectada internamente.	Pérdidas económicas menores.
3	5	41-60%	Moderado	El evento podría ocurrir en algún momento. Probabilidad media.	Afectación a un grupo reducido de usuarios.	Interrupción de las operaciones del G.A.D. Municipal por un (1) día.	Imagen o credibilidad institucional afectada localmente.	Pérdidas económicas moderadas.
4	10	61-80%	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.	Afectación en la práctica del proceso que repercute en los usuarios.	Interrupción de las operaciones del G.A.D. Municipal por más de dos (2) días.	Imagen o credibilidad del G.A.D. Municipal afectada en la región.	Pérdidas económicas mayores.
5	20	81-100%	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.	Afectación en la práctica del proceso que repercute en la mayoría de los usuarios.	Interrupción de las operaciones del G.A.D. Municipal por más de cinco (5) días.	Imagen o credibilidad del G.A.D. Municipal afectada a gran escala.	Pérdidas económicas significativas.

Tabla 2.8: Parámetros de impacto

Fuente: Elaborado por el autor a partir de [36]

**Niveles de aceptabilidad:** La calificación del riesgo se establece mediante la evaluación de la probabilidad de ocurrencia y el impacto que tendría al materializarse el riesgo. Es importante considerar los parámetros previamente descritos en la Tabla 2.7 y la Tabla 2.8, identificando así los niveles que apliquen al análisis de riesgo y ejecutar su calificación a partir del cruce entre estas dos variables sobre la matriz de 5x5 (probabilidad eje “Y” e impacto eje “X”), como se muestra en la Figura 2.5, acorde al rango estimado por los expertos.

**Calificación del riesgo = Probabilidad x Impacto**

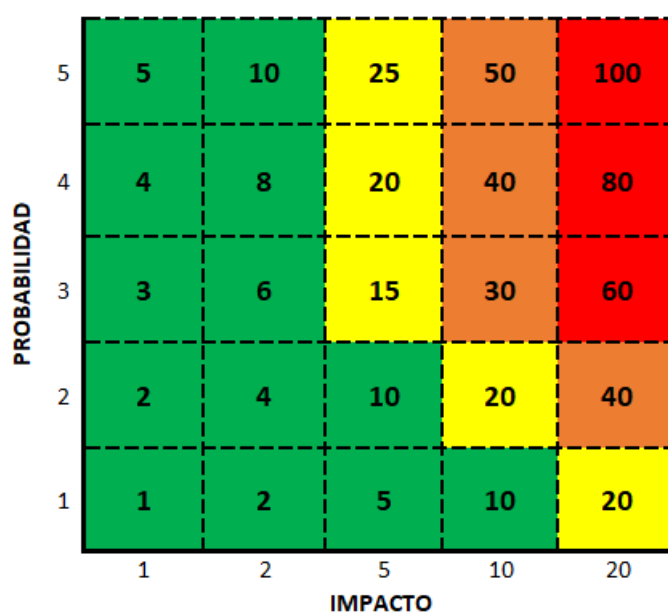


Figura 2.5: Matriz de calificación de riesgos operativos  
Fuente: Elaborado por el autor a partir de [36]

La calificación del riesgo muestra un valor numérico entre (1 y 100), el cual se ubica en los rangos establecidos por los niveles de aceptabilidad los cuales se encuentran asociados a un código de color tipo semáforo, donde se puede observar la gravedad del riesgo al que está expuesto un determinado activo, de esta manera tenemos una mejor percepción sobre las acciones que se deben tomar para gestionarlo y el valor de vulnerabilidad al que se encuentra expuesto el G.A.D. Municipal del cantón Salcedo.

VALOR	NIVEL DE ACEPTABILIDAD	ACCIÓN	VALOR VULNERABILIDAD
Entre 1 y 10	BAJO	Los riesgos en esta zona se encuentran en un nivel que puede reducirse fácilmente con los controles establecidos en la institución. <b>Ello requiere asumir los riesgos. Riesgos aceptables.</b>	Vulnerabilidad inferior al 10%
Entre 15 y 25	MODERADO	Deben tomarse las medidas necesarias para llevar los riesgos a la Zona de riesgo baja. <b>Riesgos moderados.</b>	Vulnerabilidad entre el 15 y el 25%
Entre 30 y 50	ALTO	Deben tomarse las medidas necesarias para llevar los riesgos a la zona de riesgo moderada o baja. <b>Riesgos importantes.</b>	Vulnerabilidad entre el 30 y el 50%
Entre 60 y 100	EXTREMO	Los riesgos en la zona de riesgo extrema requieren de un tratamiento prioritario. Se deben implementar los controles orientados a reducir la posibilidad de ocurrencia del riesgo o disminuir el impacto de sus efectos. <b>Riesgos inaceptables.</b>	Vulnerabilidad mayor al 60%

Tabla 2.9: Niveles de aceptabilidad del riesgo

Fuente: Elaborado por el autor a partir de [36]

**Vulnerabilidad:** La vulnerabilidad se refiere al grado de exposición que se encuentra el G.A.D. Municipal hacia los riesgos identificados, conforme a los niveles de aceptabilidad determinados en la Institución. Donde se muestra el estado de inseguridad ante el riesgo en una escala porcentual que va desde (1% al 100%), considerando que la vulnerabilidad más baja es del (1%) misma que contempla los riesgos con probabilidad (1) Raro e impacto (1) Insignificante, contrario a que la vulnerabilidad más alta que corresponde al (100%) de acuerdo con los riesgos con probabilidad (5) Casi seguro e impacto (20) Catastrófico.

Anteriormente se mencionó el libro (INFORMATION SECURITY), en el que se plantea un ejemplo acerca del paradigma de la seguridad de la información, ALE es una fórmula algebraica que multiplica la (expectativa de pérdida individual o SLE) por su expectativa de probabilidad de ocurrencia (ARO), esto representa la pérdida monetaria que puede representar para la institución si se materializa una o más amenazas. En conjunto con el tutor se a considerado tomar el valor del activo más la perdida monetaria por hora (PH), en el caso que un activo deje de brindar un determinado servicio. Y de esta manera contemplar un análisis cuantitativo e identificar de mejor manera las acciones requeridas para su tratamiento.[34]

Se define mediante la siguiente fórmula:

$$ALE = SLE \times ARO$$

$$SLE = FE \times (VA+PH)$$

**Donde:**

- **ALE:** Expectativa de Pérdida Anual.
- **SLE:** Expectativa de Pérdida Individual.
- **ARO:** Tasa de Ocurrencia Anualizada.
- **FE:** Factor de Exposición.
- **VA:** Valor del activo.
- **PH:** Valor de la pérdida por hora.

Fuente: [34]

## **EVALUACIÓN DEL RIESGO**

La etapa de evaluación del riesgo se encuentra enfocado en confrontar los resultados de su análisis. Es necesario considerar los puntos de control de seguridad ya existentes en la municipalidad para de esta manera avanzar con la gestión. La finalidad de la evaluación del riesgo es dar la habilidad en la toma de disposiciones en la municipalidad, respaldándose en el análisis de resultados sobre cuáles riesgos combatir, brindando así un tratamiento adecuado y por ende dar la prioridad del caso para su posterior implementación. Para llevar a cabo esta comparación del nivel de riesgo observado hay que considerar la etapa del contexto.

Por otra parte, hay que tomar en cuenta los controles pertinentes acorde a las medidas de probabilidad e impacto que recaen sobre la amenaza.

### **Controles de probabilidad**

En esta parte el principal objetivo es evitar que un determinado riesgo se materialice, por lo que se enfoca en atacar las causas detectadas en el análisis.

### **Controles de impacto**

Se enfoca en el activo amenazado, donde se busca reducir las consecuencias de la materialización del riesgo.

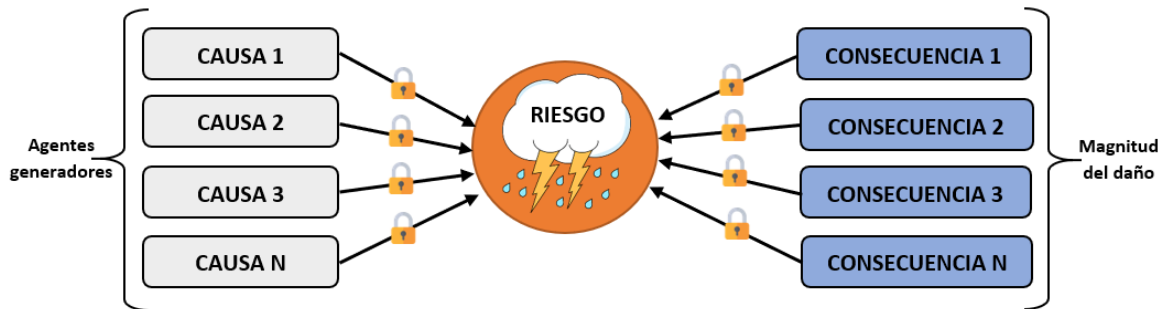


Figura 2.6: Identificación de riesgos en esquema de corbatín (bow tie)  
Fuente: Elaborado por el autor a partir de [32]

### Valoración de los controles

En esta parte se dejará planteado el análisis para conocimiento del departamento de TI, sobre cómo se procederá a medir la eficiencia del control ya en la práctica. Se enuncian las características donde se asignará una puntuación desde el más eficiente al menos eficiente, acorde al diseño de los controles con sus correspondientes tipologías. Las Tablas 2.10 y 2.11 se la construyeron a partir de un proyecto realizado por la Universidad de Colombia (UN), misma que realiza una guía para la administración de riesgos operativos de procesos en la UN, en la que también hacen uso del (ciclo PDCA).

Por esta razón se tomó como guía este proceso, por consiguiente la valoración de los controles queda a cargo de las autoridades y de quienes conforman el departamento de TI de la institución.

CÓDIGO	CARACTERÍSTICA	TIPOLOGÍA	DESCRIPCIÓN	VALOR
MA	Acorde al momento en el que actúa el control	Preventivo	Controles que actúan antes o al inicio de una actividad/proceso.	3
		Detectivo	Controles que actúan durante el proceso y que permite corregir las deficiencias.	2
		Correctivo	Controles que actúan una vez que el proceso ha terminado.	1
C	Acorde a su cobertura	Total	Controles que se aplican a todos los eventos sin importar sus características.	2
		Parcial	Controles que se aplican de manera parcial a discreción de una persona o una tecnología específica.	1
		Nulo	El control no está siendo aplicado sobre los objetos de control.	0
AUT	Nivel de automatización del control	Automático	Controles embebidos en la infraestructura tecnológica y/o los sistemas de información.	2
		Manual	Controles que no involucran el uso de tecnologías de información.	1
PER	De acuerdo a la periodicidad en la que se aplica el control	Permanente	Controles que actúan durante todo el proceso, sin intermitencia.	3
		Periódico	Controles que se aplican en ciertos periodos de tiempo.	2
		Ocasional	Controles que no se aplican de forma constante y de manera ocasional.	1

Tabla 2.10: Evaluación del diseño (eficiencia) del control

Fuente: Elaborado por el autor a partir de [36]

CÓDIGO	CARACTERÍSTICA	TIPOLOGÍA	DESCRIPCIÓN	VALOR
MAD	De acuerdo a la madurez del control	Información documentada, implementado socializado y con seguimiento.	Información documentada, hace parte del hacer cotidiano del proceso, es conocido y aplicado por las personas involucradas y se realiza seguimiento para la toma de decisiones.	5
		Información documentada, implementado y socializado	Información documentada, hace parte del hacer cotidiano del proceso, conocido y aplicado por las personas involucradas.	4
		Información documentada e implementado	Información documentada hace parte del hacer cotidiano del proceso.	3
		Definido y con información documentada	Control hace parte de la información documentada del proceso.	2
		Definido	Controles se encuentran operando de manera informal.	1
DES	De acuerdo a la desagregación del control	Control institucional	Control realizado por una instancia externa al proceso (Auditoría interna y demás instancias externas)	3
		Control de Gestión	Controles que permiten evaluar el desempeño del proceso (Informes de gestión, autoevaluación de procesos).	2
		Autocontrol	Control que ostenta cada servidor público, adecuado cumplimiento de los resultados.	1

Tabla 2.11: Evaluación del diseño (eficiencia) del control

Fuente: Elaborado por el autor a partir de [36]



Como máxima calificación del control tenemos 18 puntos los que equivalen a una eficiencia del 100 %, el valor se obtiene seleccionando un valor que va desde el más eficiente al menos eficiente de acuerdo a cada código de las tablas anteriormente mostradas, se debe tener en cuenta que para cada control identificado se calcula el porcentaje de eficiencia.

Se define mediante la siguiente fórmula:

**Donde:**

- **MA:** Momento de actuación.
- **C:** Cobertura.
- **ART:** Automatización.
- **PER:** Periodicidad.
- **MAD:** Madurez.
- **DES:** Desagregación.

$$\% \text{ DE EFICIENCIA DEL CONTROL} = (MA + C + AUT + PER + MAD + DES) / (\sum (\text{Máximo valor por categoría})) \times 100$$

Fuente: [36]

El resultado se encuentra ubicado en la Tabla 2.12 para comprobar la disminución en la variable probabilidad o impacto según se aplique y calcular el riesgo residual.

Calificación de la eficiencia del control	Rango de eficiencia	Color	Descripción	Disminución de la Probabilidad o el Impacto
<b>ALTO</b>	>= 80%		El control presenta un diseño eficiente.	2
<b>MEDIO</b>	Entre el 60% y el 79%		El control presenta un buen diseño susceptible de ser mejorado.	1
<b>BAJO</b>	<= 59%		El control presenta deficiencias en su diseño, definir acciones de mejora.	0

Tabla 2.12: Rangos de eficiencia del control

Fuente: Elaborado por el autor a partir de [36]

Para mayor entendimiento al método de evaluación sobre la eficiencia de controles se ha planteado un ejemplo donde podemos apreciar los siguientes valores:

- **MA:** Preventivo = 3.
- **C:** Parcial = 1.
- **ART:** Manual = 1.
- **PER:** Permanente = 3.
- **MAD:** Información documentada, implementado y socializado = 5.
- **DES:** Control institucional = 3.

Acorde con la fórmula el porcentaje de eficiencia se calcularía así:

$$\% \text{ eficiencia del control} = ((3+1+1+3+5+3)/18) \times 100 = 88.88 \%$$

Con el resultado anteriormente obtenido se puede concluir que con la aplicación del control se puede disminuir la probabilidad del riesgo 2 casillas, ya que se encuentra en el rango de eficiencia en la Tabla 2.12.

### **2.2.2.3. Etapa de tratamiento del riesgo**

Cabe destacar que todos los riesgos conllevan un mismo nivel crítico en la que su gestión involucra costos, tiempo y esfuerzos en los que debe incurrir la municipalidad por parte de las autoridades y encargados del departamento de TI, de ahí la importancia de establecer cuáles riesgos son “inadmisibles” y así saber por cuales empezar a gestionarlos.

En el caso del G.A.D. Municipal del cantón Salcedo, los riesgos que se encuentran en zonas de calificación moderada, alta y extrema requieren tratamiento con el propósito de llevarlos a la zona de calificación baja, sin embargo los que están ubicados en zona baja se recomienda ser monitoreados dándole la importancia del caso para evitar que se materialicen en un futuro.

De la misma manera se debe hacer un análisis sobre los costos que implica el amparo sobre las medidas de protección que permitan contrastar los riesgos ante su materialización y de esta manera tomar decisiones sobre implementarlas o no.

**Plan de tratamiento de riesgos** Como resultado de esta etapa de tratamiento se concreta en el diseño de un plan de contingencia, donde se toma las medidas necesarias para adoptar y modificar los niveles de riesgo identificado. Estas medidas de tratamiento deben adaptarse a las necesidades del G.A.D. Municipal del cantón Salcedo.

Es importante resaltar los tiempos en los cuales el plan de tratamiento de riesgos tomará las medidas pertinentes como es el antes, durante y después. Se debe considerar que las actividades específicas tendrán designado su responsable de ejecutar una determinada tarea.

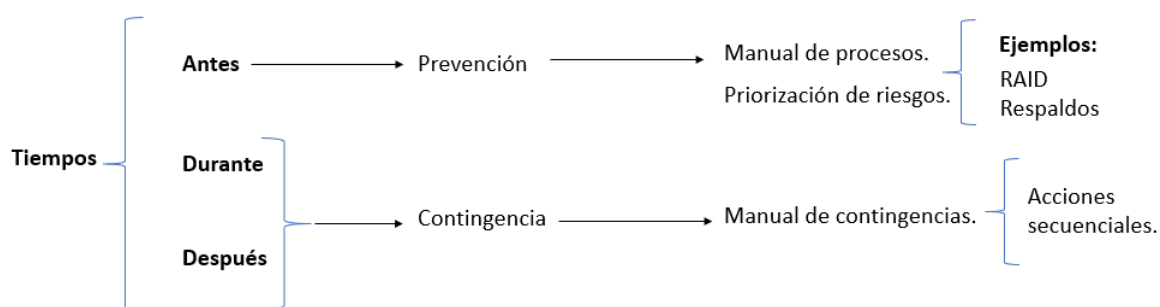


Figura 2.7: Tiempos ante el diseño del plan de contingencia  
Fuente: Elaborado por el autor

#### 2.2.2.4. Etapa de comunicación y consulta

Establecer una buena comunicación entre el personal responsable de su ejecución y demás autoridades de la municipalidad deben ser permanentes en las distintas etapas del proceso para una correcta gestión de riesgos, dado a las diversas variaciones sobre las percepciones de los riesgos desde el punto de vista del personal encargado de los procesos. Mismos que tienen sus propios criterios, preocupaciones que los llevan a hacer juicios ante los riesgos basándose en la experiencia y conocimiento adquirido durante su vida laboral en la institución. Como principal objetivo de esta etapa es tomar en cuenta la comunicación mediante el intercambio de información, analizar los resultados e interpretarlos para conseguir información confiable y consistente considerando los puntos de vista del personal, el correcto desarrollo de esta etapa permitirá:

- Identificar de manera correcta los riesgos.
- Valorar los riesgos en función a las consecuencias para el G.A.D. Municipal del cantón Salcedo.
- Comprender su probabilidad e impacto, que un riesgo se materialice.
- Establecer prioridades para su correcto tratamiento.

- Difundir la información para que se involucren tanto las autoridades como personal de la institución.
- Monitorear frecuentemente la eficiencia sobre el tratamiento.
- Inspeccionar con regularidad el proceso de gestión de riesgo para identificar las mejoras correspondientes.
- Fomentar en el G.A.D. Municipal el pensamiento sobre la prevención de riesgos.

Fuente: [36]

#### **2.2.2.5. Etapa de monitoreo y revisión**

Esta etapa consiste en analizar la información de manera minuciosa observando el desarrollo de la gestión del riesgo, con el propósito de que se cumplan los objetivos para una correcta toma de decisiones futuras. Para tener mejor resultados se sugiere supervisar en la práctica permitiendo realizar correcciones si fuera el caso. Tener una revisión acerca de los cambios del entorno se incluye en esta etapa, realimentando así la etapa del establecimiento del contexto.

Dado a que los riesgos no son estáticos y pueden cambiar de forma radical es importante considerar una supervisión continua para así:

- Garantizar la eficiencia de los controles establecidos para mitigar los riesgos.
- Comprobar el grado de cumplimiento en la ejecución de los planes de tratamiento propuestos.
- Adquirir experiencia en el transcurso del tiempo a partir de los eventos, los cambios sucedidos en la institución.
- Identificar riesgos emergentes.
- Tratar los riesgos materializados.

Fuente: [36]

Esta etapa será llevada a cabo tanto por las autoridades como quienes forman parte del equipo de trabajo del departamento de Tecnologías de la Información TI, en conjunto con los líderes y colaboradores de los demás departamentos de la institución, se recomienda realizar este proceso al menos una vez al año en las fechas que establezca la autoridad mayor en este caso el señor alcalde.

#### **2.2.2.6. Etapa de seguimiento**

Mediante esta etapa los procesos de gestión de riesgos deben demostrar que están cumpliendo con la normativa y que están obteniendo los resultados anhelados conforme a los compromisos adquiridos por parte del G.A.D. Municipal del cantón Salcedo, para obtener una adecuada gestión de riesgos.

El seguimiento permite conocer si la gestión del riesgo se cumple, mediante las siguientes actividades:

- Comprobar la aplicación de la metodología para la administración de riesgos operativos adoptada para G.A.D. Municipal del cantón Salcedo.
- Comprobar la correcta identificación sobre los controles asociados a los riesgos operativos.
- Verificar la efectividad de los controles y los tratamientos propuestos.
- Confirmar si se han materializado riesgos operativos emergentes.
- Corregir o eliminar controles innecesarios, complejos o que no aporten de una manera adecuada al tratamiento de los riesgos correspondientes.

Fuente: [36]

La investigación esta enfocada en averiguar detenidamente la problemática por la ausencia de un plan de contingencia informático para ello se llevará acabo las siguientes modalidades:

#### **2.2.3. Modalidad de la Investigación**

El presente proyecto está basado en la investigación aplicada dado a la importancia de la colaboración entre los conocimientos adquiridos en la universidad y el sector público donde se pondrá en práctica dichos conocimientos para así dar solución a los problemas que sean detectados acorde al objetivo planteado en la investigación.

#### **Investigación bibliográfica**

Este método va a permitir a la investigación entender de mejor manera definiciones, basadas en resultados de investigaciones ya existentes referentes al tema por medio de la lectura con la finalidad de dar un aporte teórico, que servirá

como base a la investigación apoyandose en distintos autores de libros, artículos científicos, repositorios, tesis de grado, enlaces bibliográficos, que han expresado sus diferentes conclusiones del problema.

### **Investigación de campo**

Generalmente la presente modalidad es considerada debido a que es necesario asistir al lugar donde se desarrollan las actividades que involucran la parte informática dentro del G.A.D. Municipal del cantón Salcedo, para así entender de mejor manera la problemática en dicho lugar, lo que generará una recolección de datos reales que servirán como respaldo a la investigación.

### **Investigación aplicada**

Permitirá resolver el problema planteado con el diseño de un plan de contingencia informático en el G.A.D. Municipal del cantón Salcedo ante una posible amenaza y dar respuesta de manera inmediata para evitar eventualidades que provoquen una paralización en las actividades de la institución.

#### **2.2.4. Recolección de Información**

Las personas que proporcionarán la información serán: Administrativos de la institución, jefe del departamento de Sistemas. Para recabar la información se utilizarán técnicas como la observación y la entrevista con sus respectivos instrumentos que son el registro de datos, entrevistas, también se contará con el apoyo de organismos especializados y finalmente el método Delphi.

#### **2.2.5. Procesamiento y Análisis de Datos**

Como primera parte es indispensable recopilar información de manera correcta acorde al tema de investigación, para el procedimiento y análisis de datos, análisis estadístico descriptivo, entrevistas, cuestionarios, que permitan la ejecución de un plan de contingencia, tomando en cuenta el análisis de tiempos ante los posibles riesgos que se puedan presentar y a su vez mostrar resultados basados en datos reales.

### **2.2.6. Desarrollo del Proyecto**

Para el desarrollo del proyecto se ha tomado en cuenta lo siguiente:

- Analizar la situación actual de los sistemas informáticos y sus políticas internas.
- Evaluar los sistemas informáticos.
- Categorizar los riesgos y procesos.
- Establecer responsables de los procesos.
- Definir tiempos de respuesta para solventar dichas problemáticas.
- Diseñar un plan de contingencia informático.
- Brindar una capacitación al personal de la institución.

## **CAPÍTULO 3**

### **RESULTADOS Y DISCUSIÓN**

#### **3.1. Análisis y discusión de los resultados**

##### **3.1.1. Desarrollo de la propuesta**

El presente capítulo establece tiempos que serán llevados por fases las mismas que contribuyen al diseño de un plan de contingencia informático para el área de TI en el Gobierno Autónomo Descentralizado Municipal del cantón Salcedo, acorde a lo detallado anteriormente en el proceso para la gestión de riesgos operativos, donde se ha hecho un análisis entre algunas metodologías disponibles y elegido a la que más se adapte a la institución, previo al desarrollo del proyecto en el que se ha tomado como referente la norma NTC-ISO/IEC 27005 para una mejor sustentabilidad hacia la Norma 410-11 de la C.G.E. del Ecuador, dicho proceso se encuentra compuesto por (5) etapas del proceso de gestión de riesgo como se observa en la Figura 2.2.

De acuerdo con explicado anteriormente y con sustento de las metodologías a continuación se realiza el desarrollo de la propuesta.

##### **3.1.2. Etapa de establecimiento del contexto**

###### **3.1.2.1. Consideraciones iniciales del G.A.D. Municipal del cantón Salcedo**

###### **El objetivo principal**

El GAD Municipal de Salcedo para su gestión establece los siguientes objetivos estratégicos:

- a) Planificar, coordinar y ejecutar el ordenamiento territorial del Cantón, mediante la implementación de planes de construcción, mantenimiento, aseo, embellecimiento y reglamentación vial, de ornamentación y embellecimiento, de dotación de servicios públicos y de ordenamiento del tránsito y transporte terrestres.
- b) Planificar, coordinar y ejecutar el desarrollo económico del Cantón, a través de planes de desarrollo turístico y el apoyo a microempresas, pequeña industria



e industria en actividades productivas.

c) Planificar, coordinar y ejecutar el desarrollo social, cultural y recreativo en coordinación con las organizaciones públicas o privadas del Cantón.

d) Planificar, coordinar y ejecutar el desarrollo ambiental del Cantón, armonizando el uso sostenible y sustentable de los recursos naturales a fin de contar con un ambiente sano y saludable.

Fuente: [37]

### **Misión**

El G.A.D. Municipal del cantón Salcedo, es responsable de impulsar el buen vivir, a través del desarrollo territorial, económico, sociocultural y ambiental del cantón; a fin de que, Salcedo sea un espacio de equidad y participación en armonía con su cultura y con su naturaleza.[38]

### **Visión**

El G.A.D. Municipal de Salcedo fortalece su sistema de gestión organizacional, a fin de que éste se artifice del desarrollo cantonal, de la participación ciudadana y del uso sostenible y sustentable de sus recursos.[38]

### **Políticas**

Las políticas que rigen al G.A.D. Municipal del Cantón Salcedo son las siguientes: Legalizar, aplicar y fomentar ordenanzas y reglamentos que faciliten las iniciativas privadas, públicas e institucionales.[38]

Dentro de la administración del departamento de Tecnologías de la Información se encontró la documentación sobre los principales artículos pertenecientes a las políticas de seguridad del G.A.D. Municipal del Cantón Salcedo.

**Art. 1.** Los servicios de la red institucional son de exclusivo uso técnicos y para gestiones administrativas, cualquier cambio en la normativa de uso de los mismos, será expresa y adecuada como política de seguridad en este documento.

**Art. 2.** La Unidad de Informática dará seguimiento al cumplimiento de la normativa y propiciará el entorno necesario para crear un Sistema de Gestión de Seguridad de la Información (SGSI) el cual tendrá entre sus funciones:

- a) Velar por la seguridad de los activos informáticos.
- b) Gestión y procesamiento de información.
- c) Cumplimiento de políticas.

- d) Elaboración de planes de seguridad.
- e) Capacitación de usuarios en temas de seguridad.
- f) Gestionar y coordinar esfuerzos, por crear un plan de contingencia, que dé sustento o solución, a problemas de seguridad dentro de la institución. El mismo orientará y guiará a los empleados, la forma o métodos necesarios para salir adelante ante cualquier eventualidad que se presente.
- g) Informar sobre problemas de seguridad.
- h) Poner especial atención a los usuarios de la red institucional sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.

El comité de seguridad estará integrado por los siguientes miembros:

- I. Alcalde.
- II. Gestor de Seguridad.
- III. Unidad de Informática.
- IV. Responsable de Activos.

**Art. 3.** La Unidad de Informática es el encargado de mantener en buen estado los servidores dentro de la red institucional.

**Art. 4.** Todo usuario de la red institucional gozará de absoluta privacidad sobre su información, o la información que provenga de sus acciones, salvo en casos, en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional.

**Art. 5.** Los usuarios tendrán el acceso a Internet previo a una autorización por escrito de la Autoridad Máxima y en el cual se detallen las actividades a realizar; siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la unidad de informática, además este servicio puede ser permanente o momentáneo de acuerdo con las actividades.

**Art. 6.** Las actividades Administrativas, tienen la primera prioridad por lo que a cualquier usuario utilizando otro servicio (por ejemplo: Internet, Juegos o “Chat”) sin estos fines, se le podrá solicitar salir o desconectar automáticamente los servicios, si así, fuera necesario.

Fuente: [39]

### **Estructura organizacional**

La estructura organizacional del Gobierno Autónomo Descentralizado Municipal del cantón Salcedo se alinea con su misión, y se sustenta en la ética profesional y el enfoque hacia los servicios y procesos, con el objetivo de establecer su ordenamiento Orgánico. Figura 3.2

Los procesos y servicios que se cumplen en el Gobierno Autónomo Descentralizado del cantón Salcedo se ordenan y clasifican en función de su grado de contribución para el cumplimiento de la misión institucional.

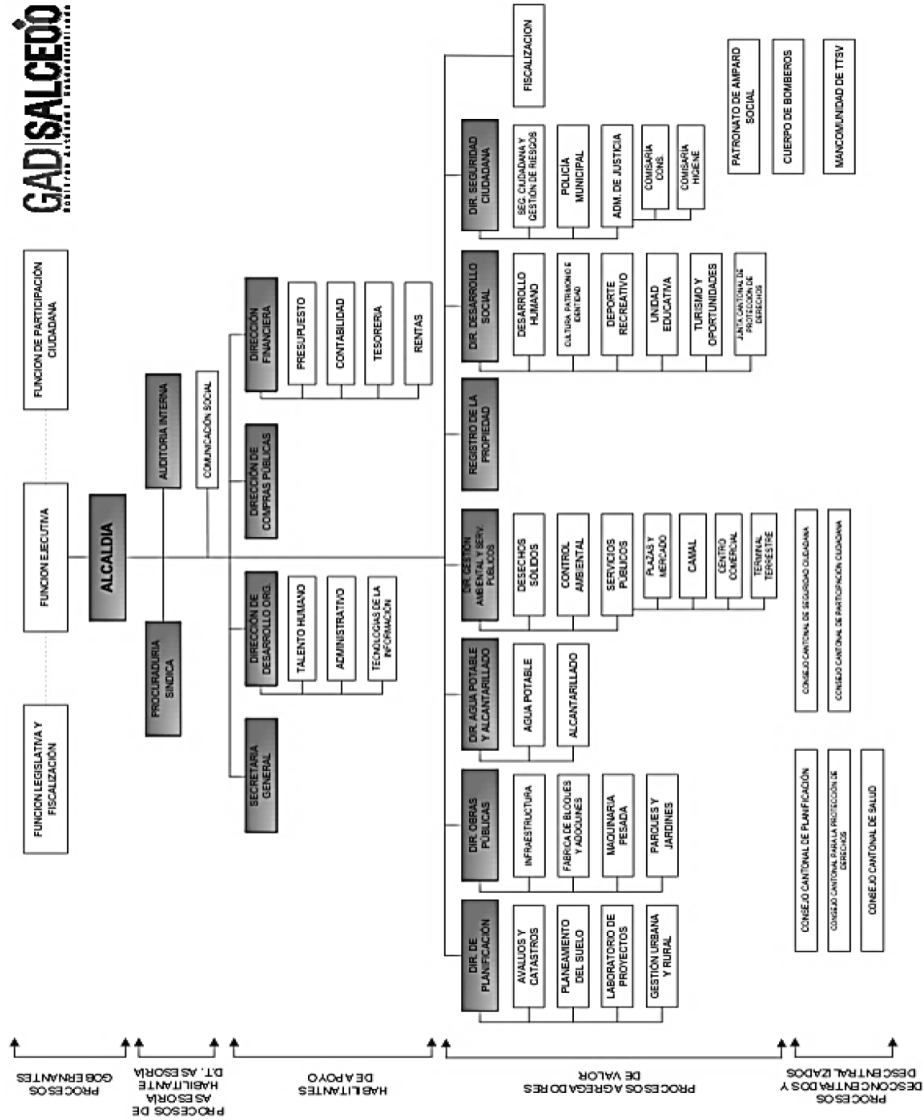


Figura 3.1: Organigrama G.A.D Municipal del cantón Salcedo  
Fuente: Elaborado por el G.A.D Municipal

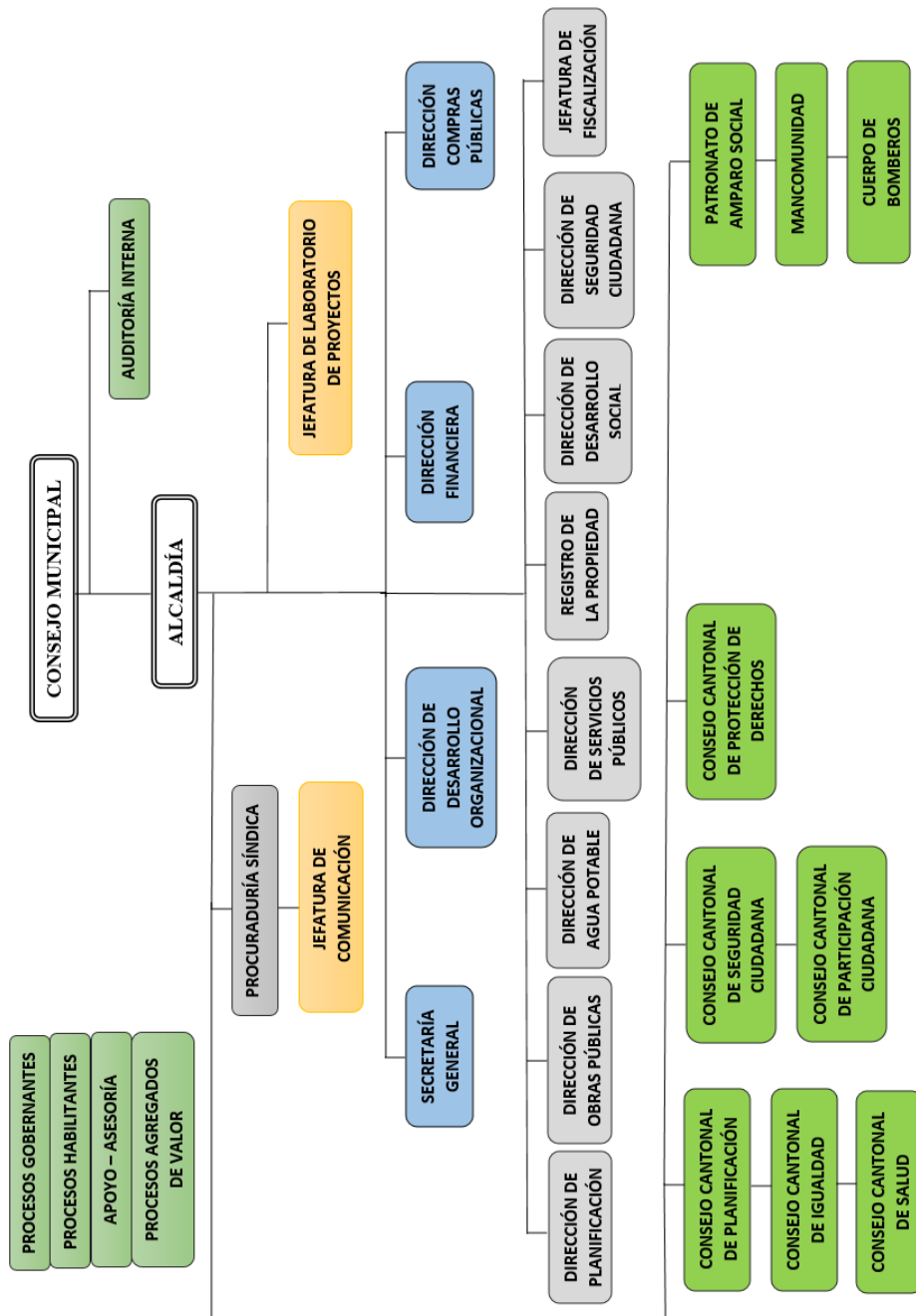


Figura 3.2: Actualización del organigrama G.A.D Municipal del cantón Salcedo  
Fuente: Elaborado por el autor a partir la última auditoría a la institución

### Red de datos

El G.A.D. Municipal del cantón Salcedo cuenta con un sistema de red LAN con topología en cascada, el cual interconecta a todos los equipos de cómputo que existen en la Municipalidad. La principal ventaja que ofrece el uso de esta topología en cascada es su velocidad y fácil desarrollo. El proveedor de servicio de internet que colabora con la Municipalidad es la Corporación Nacional de Telecomunicaciones CNT EP, que brinda el respaldo y garantiza acceso a internet a través de fibra óptica. La red de la Municipalidad se encuentra distribuidos según las instalaciones que se muestra a continuación.

### Las instalaciones

Es imprescindible contar con un diagrama sobre los departamentos dentro del G.A.D. Municipal, y tener una perspectiva más clara del lugar donde se desarrolla el proyecto.

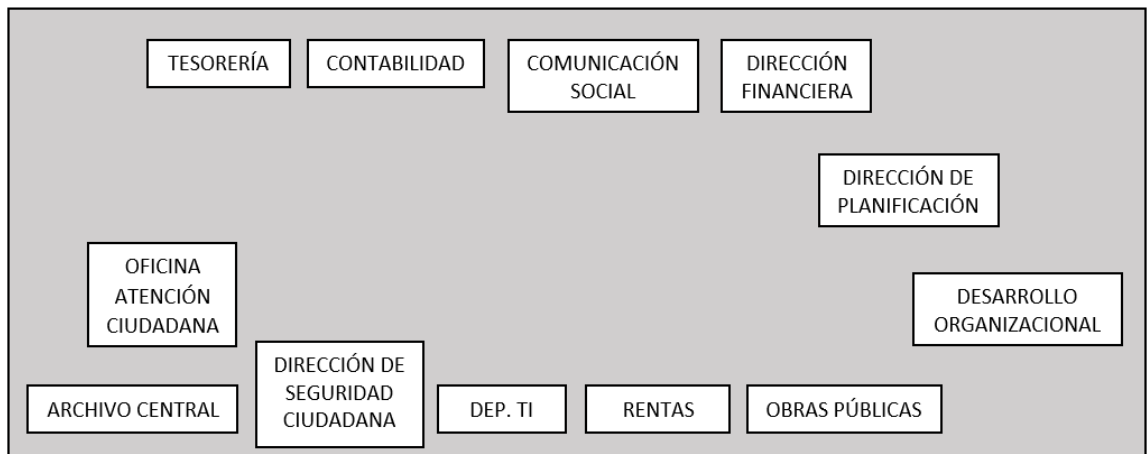


Figura 3.3: Primera planta edificio antiguo y nuevo  
Fuente: Elaborado por el autor

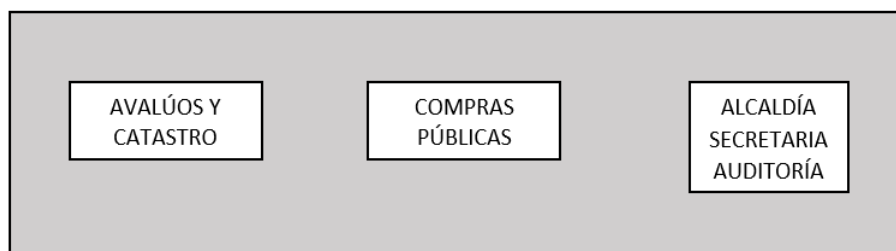


Figura 3.4: Segunda planta edificio nuevo  
Fuente: Elaborado por el autor

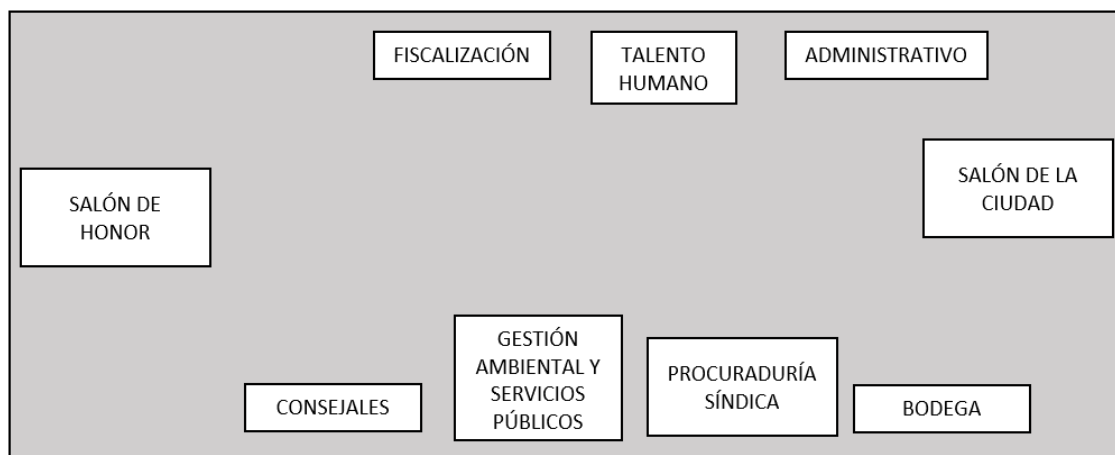


Figura 3.5: Segunda planta edificio antiguo y tercera planta del edificio nuevo  
Fuente: Elaborado por el autor

### Los funcionarios y sus roles en la organización

A continuación en la Tabla 3.1, se detalla los Cargos del personal del departamento de Tecnologías de la Información del G.A.D. Municipal del Cantón Salcedo según sus funcionarios (Esta información se encuentra actualizado hasta el 30 de junio de 2020):

CARGO	FUNCIONARIO	FUNCIÓN
<b>Jefe de Sistemas</b>	Ing. Enrique Arcos	Dirigir el departamento de tecnologías de la información.
<b>Analista de Sistemas</b>	Ing. Paulina Villalba	Soporte informático y mantenimiento a los aplicativos de la institución.
<b>Técnico de Sistemas</b>	Tec. Juan Córdoba	Soporte Técnico.

Tabla 3.1: Cargos del personal del departamento de Tecnologías de la Información del G.A.D. Municipal del Cantón Salcedo

Fuente: Elaborado por el autor en colaboración con el departamento de TI

De la misma manera es importante conocer los representantes o el personal que se encuentra a cargo de los distintos departamentos y el rol que desempeña dentro del G.A.D. Municipal, con quienes se puede gestionar un determinado procedimiento a tomar en caso de materializarse un determinado riesgo. Esta información se encuentra actualizado hasta el 30 de junio de 2020.

DEPARTAMENTO	CARGO	FUNCIONARIO
Tesorería	Jefe tesorería	Srta./Sra. Katty González
Contabilidad	Jefe contabilidad	Srta./Sra. Mariana de la Vega
Rentas	Jefe de rentas	Sr. Fernando Peralta
Avalúos y catastros	Jefe de avalúos y catastros	Sr. Francisco Villagómez
Obras públicas	Director de obras públicas	Sr. Diego Soria
Agua potable	Director de agua potable	Sr. Patricio Avilés
Archivo	Auxiliar de documentación y archivo	Sr. Juan Vizcaíno
Informática	Jefe del departamento TI	Sr. Enrique Arcos
Comunicación social	Jefe de comunicación social	Sr. Juan Candonga
Compras públicas	Director de compras	Srta./Sra. Margare Guerrero
Dirección financiera	Directora de dirección financiera	Srta./Sra. Gabriela Arias
Planificación	Director de planificación	Sr. Álvaro Villota
Presupuesto	Jefe del área de presupuesto	Srta./Sra. Salazar María

Tabla 3.2: Cargos del personal primera planta (edificio antiguo y nuevo)

Fuente: Elaborado por el autor en colaboración de los distintos departamentos del G.A.D. Municipal.

DEPARTAMENTO	CARGO	FUNCIONARIO
Administrativo	Jefe del departamento administrativo	Srta./Sra. Fernando Navas
Alcaldía	Secretaria de alcaldía	Srta./Sra. Jaqueline Chano
Secretaría general	Secretaría general	Sr. Tarquino Naranjo
Procuraduría	Procuraduría	Srta./Sra. Cecilia Guaigua Srta./Sra. Natalia Santamaria
Desarrollo organizacional	Directora del departamento organizacional	Sin funcionario
Talento humano	Jefe de talento humano	Sr. Fernando Vásquez
Gestión ambiental	Jefe de gestión ambiental	Sin funcionario
Servicios públicos	Jefe servicios públicos	Sin funcionario
Archivo financiero	Director de archivo financiero	Sr. Luis Rodríguez
Concejales	Secretaria de consejo	Srta./Sra. Ana Santa Fe
Fiscalización	Jefe de fiscalización	Srta./Sra. Mónica Velastegui
Bodega	Guarda almacén	Sr. William Velastegui
Dirección de seguridad ciudadana	Director de seguridad ciudadana	Sr. Santiago Vásquez

Tabla 3.3: Cargos del personal segunda planta (edificio antiguo y nuevo)

Fuente: Elaborado por el autor en colaboración de los distintos departamentos del G.A.D. Municipal.

DEPARTAMENTO	CARGO	FUNCIONARIO
Cultura y patrimonio	Director de cultura y patrimonio / desarrollo humano	Sr. Francisco Paredes
Desarrollo humano	Especialista en desarrollo humano	Sr. Marcelo Córdova
Turismo	Dirección de turismo	Srta./Sra. Inés Carrillo

Tabla 3.4: Cargos del personal Casa Yerovy Mackuart

Fuente: Elaborado por el autor en colaboración de los distintos departamentos del G.A.D. Municipal.



DEPARTAMENTO	CARGO	FUNCIONARIO
Registro de la propiedad	Director del Registro de la propiedad	Sr. Guillermo Pérez
Operación Mercantil	Operador Mercantil	Sr. Luis Tutasig

Tabla 3.5: Cargos del personal Terminal terrestre

Fuente: Elaborado por el autor en colaboración de los distintos departamentos del G.A.D. Municipal.

### **Análisis de la situación actual del área de TI**

En 1897 mediante la Convención Nacional de la época se presentó la creación del cantón Salcedo, pero en ese instante no se dio paso, luego de 22 años el Congreso Nacional concede la cantonización el 19 de septiembre de 1919, publicado en el Registro Oficial N° 899 el 22 de septiembre de 1919. Mediante votación se elige al presidente titular del Concejo el señor Alejandro Dávalos donde se declaró legalmente inaugurado, el Concejo Municipal de Salcedo para el año de 1920. El nombre de Salcedo se debió al sacerdote Manuel Antonio Salcedo.[40]

El Congreso de la República del Ecuador en el Art, 1 se constituye el cantón Salcedo con las parroquias: San Miguel que será la cabecera, Panzaleo, Cusubamba, Mulalillo, Mulliquindil las parroquias, los límites serán los mismos que tiene las parroquias que forman, al norte Latacunga y Pujilí, al sur provincia de Tungurahua, al este Napo y al oeste Pujilí. El alcalde es la máxima autoridad tanto administrativa como política del cantón Salcedo. Se encuentra dividido en parroquias que pueden ser urbanas o rurales representadas por los Gobiernos Parroquiales.[40]

Ecuador es un Estado constitucional donde destaca los derechos y justicia, social, intercultural, pluricultural, democrático, independiente. Se encuentra organizado en forma de república gobernando de manera descentralizada, en conformidad con el Art. 1 de la Constitución de la República. La Municipalidad del cantón Salcedo de la misma manera que las demás del país, conforme al Art. 238 de la (Constitución de la Republica del Ecuador, 2008), se los denomina “Gobiernos Autónomos Descentralizados”, en la que tienen autonomía administrativa, política, financiera, acogidos a los principios de la equidad intercultural, participación ciudadana, protección.[41]

El (Código Orgánico de Organización Territorial), COOTAD señala que “Cada gobierno regional, provincial, metropolitano y municipal tendrá la estructura administrativa que requiera para el cumplimiento de sus fines y el ejercicio de sus competencias y funcionará de manera desconcentrada”. [42]

El G.A.D. Municipal del cantón Salcedo está ubicado actualmente en las calles Bolívar y Sucre frente al parque Central 19 de Septiembre. La historia de la Institución asido una muestra de lucha y perseverancia para el resto de GAD's, la ardua labor de su población para el desarrollo socioeconómico mismo que resalta a nivel cantonal, siendo un ejemplo a seguir a nivel nacional.

El G.A.D. Municipal del cantón Salcedo cuenta con su propia página web, la misma que pone a disposición de la ciudadanía, servicios modernos que permiten a los contribuyentes realizar consultas sobre sus planillas, comprobantes electrónicos a través de la opción de servicios. Las planillas se pueden consultar mediante el número de cédula como usuario y la contraseña viene dada en la carta de pago de la persona interesada.

Se hace una observación, en la página web de la municipalidad hay algunos campos que carecen de la información respectiva y actualmente contienen links que no se enlazan correctamente y están en mantenimiento.

## **DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN**

El departamento de TI de la municipalidad del cantón Salcedo, se encuentra constituido como una área abarcado por la Dirección de Desarrollo Organizacional, el cual impone nuevos desafíos para mejor significativamente la calidad de servicio que se brinda al usuario.

### **Misión del departamento de TI**

Buscar soluciones a todos los problemas relativos a la administración, distribución y almacenamiento de la información necesaria para la gestión técnica y administrativa del G.A.D. Municipal del Cantón Salcedo, con un enfoque simétrico e integral, utilizando los recursos disponibles en forma eficaz y eficiente, ejerciendo sus funciones de apoyo técnico y supervisión de las políticas de desarrollo de las tecnologías de la información.[39]

### **Visión del departamento de TI**

Lograr que el G.A.D. Municipal del Cantón Salcedo sea una entidad cuya gestión esté basada en un adecuado soporte de tecnologías de información costo-efectivas, que apoye los procesos de producción con información adecuada, confiable y oportuna y que se vincule efectivamente con su entorno (Ciudadanía, Funcionarios, Comunidad, Estado) aprovechando las posibilidades que brindan estas tecnologías.[39]

## Análisis FODA del departamento de Tecnologías de la Información del G.A.D. Municipal

Con la colaboración del equipo de trabajo del departamento de TI del G.A.D. Municipal y junto con la documentación perteneciente a la misma sobre un (Plan integral informático), donde destaca los escenarios y la gestión municipal de los últimos años, se hace un análisis FODA con respecto al departamento de TI, identificando las principales fortalezas, oportunidades, debilidades y amenazas existentes.

EVALUACIÓN INTERNA	EVALUACIÓN EXTERNA
<b>FORTALEZAS</b> <ul style="list-style-type: none"> <li>• Red de área local (LAN).</li> <li>• Servicio de Internet.</li> <li>• Cuarto frío para servidores.</li> <li>• Sistemas realizados con software libre (Oficios, Memorándums, Personal, Ordenes de Pago, Coactivas, etc).</li> <li>• Personal técnico del departamento de TI con la capacidad y conocimiento necesario para resolver problemas informáticos.</li> <li>• Departamento de TI tiene el control sobre los sistemas y programas desarrollados en la institución.</li> <li>• No existe costo adicional sobre los sistemas y programas desarrollados en la institución.</li> </ul>	<b>OPORTUNIDADES</b> <ul style="list-style-type: none"> <li>• Se cuenta con el respaldo de la plataforma tecnológica (AME), permitiendo el manejo de información catastral Urbana y Rural de igual forma la recaudación de estos rubros.</li> <li>• Atención oportuna a los usuarios que recurren al departamento de TI.</li> </ul>
<b>DEBILIDADES</b> <ul style="list-style-type: none"> <li>• Falta de capacitación del personal de TI.</li> <li>• Poco o ningún control en sistemas o programas dotados por otras instituciones (AME).</li> <li>• No se ha establecido funciones, competencias y responsabilidades para cada usuario de sistemas implantados en la institución.</li> <li>• Los datos personales almacenados en las bases de datos de los sistemas se encuentran incompletos (no cumple con estándares mínimos: dos nombres, dos apellidos, cédula, dirección exacta).</li> <li>• La institución no dispone de licencias de paquetes utilitarios.</li> <li>• Espacio físico insuficiente para un mejor desempeño del personal.</li> <li>• Falta de personal que brinde apoyo en las diferentes actividades encomendadas al departamento de TI.</li> </ul>	<b>AMENAZAS</b> <ul style="list-style-type: none"> <li>• El avance de la tecnología en relación con el software y hardware demandan continua capacitación de personal, así como actualización de equipos informáticos.</li> <li>• Ningún control en sistemas contratados.</li> <li>• Cambios en la Ley o disposiciones legales requieren cambios de manera segura en los sistemas.</li> </ul>

Tabla 3.6: Análisis FODA del departamento de TI

Fuente: Elaborado por el autor en colaboración con el equipo de trabajo del departamento de TI

### 3.1.2.2. Criterios básicos

#### Principales activos de información involucrados

El departamento de Tecnologías de la Información tiene bajo su responsabilidad 7 siete servidores, en los cuales se encuentran alojados diversos servicios, en la Tabla 3.7 se muestra una breve descripción de los servidores.

Nº SERVIDOR	NOMBRE DEL SERVIDOR	DESCRIPCIÓN
Servidor 1	Servidor ZIMBRA	Brinda el Servicio de correo electrónico y almacena cuentas de correo electrónico interno.
Servidor 2	Servidor SAMBA	Almacena las bases de datos de los sistemas internos y provee de los enlaces para las computadoras a través de la red interna. (Permite el manejo de varios servicios).
Servidor 3	Servidor de Internet	Distribuye el servicio de internet a las computadoras de la institución.
Servidor 4	Servidor de Antivirus	Almacena la consola de la plataforma ESET ENDPOINT SECURITY. Provee de protección a las computadoras de la institución. Realiza actualizaciones de antivirus constantemente.
Servidor 5	Servidor de Facturación Electrónica	Apoya con el servicio de Facturación Electrónica. Brinda el servicio de Video vigilancia (ZONEMINDER).
Servidor 6	Servidor Intranet	Almacena las bases de datos de los sistemas internos y provee de los enlaces para las computadoras a través de la red interna. (Permite el manejo de varios servicios).
Servidor 7	Servidor AME	Almacena las bases de datos para el manejo de los sistemas dotados por AME.

Tabla 3.7: Principales servidores del G.A.D. Municipal del cantón Salcedo

Fuente: Elaborado por el autor

En coordinación con el equipo de trabajo del departamento de TI se a visto en la necesidad de realizar un inventario general sobre equipos tecnológicos que forman parte de las herramientas necesarias para el desempeño de las actividades encomendadas al departamento.

Nº	CARGO	FUNCIONARIO	RANGO IP	COSTO ESTIMADO DEL EQUIPO	DESCRIPCIÓN DEL EQUIPO	LICENCIA
1	Jefe del departamento de TI	Ing. Enrique Arcos	10.10.1.8	\$ 1.000,00	LAPTOP PERSONAL	ACTIVA
2	Analista de sistemas	Ing. Paulina Villalba	10.10.0.9	\$ 900,00	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM	ACTIVA
3	Técnico de sistemas	Tec. Juan Córdoba	10.10.1.9	\$ 1.200,00	Microsoft Windows 10 Pro- Intel(R) Core™ i7 - 8550 CPU 1.80GHz / 16,00 GB - RAM	ACTIVA

Tabla 3.8: Principales computadores a cargo de los funcionarios del departamento de TI

Fuente: Elaborado por el autor

SERIE	DESCRIPCIÓN DEL EQUIPO	TIPO DE IMPRESORA	MODELO DE IMPRESORA	TINTA O TONER	VALOR DEL EQUIPO
CNBJN93233	HP LASER JET P2015DN	IMPRESORA A NEGRO	53A HP LASERJET	TONER NEGRO	\$ 200,00
53YX552512	EPSON L355	MULTIFUNCIONAL	54a HP LASERJET	TINTA ORIGINAL EPSON	\$ 250,00
JPRCD351CS	HP COLOR LASERJET CP6015DN	MULTIFUNCIONAL A4 Y A3	HP COLOR LASERJET CB380A	CARTUCHO DE TONER A COLOR	\$ 800,00

Tabla 3.9: Informe de las impresoras de tinta y toner dentro del departamento de TI

Fuente: Elaborado por el autor

CANTIDAD	EQUIPO	COSTO ESTIMADO DE LOS EQUIPOS	DESCRIPCIÓN DEL EQUIPO
1	Regletas para Bastidor para Rack	\$ 1.200,00	Nexxt Solutions para Rack AW220NXT95
1	Tripp Lite Rack Console 1URM	\$ 600,00	KVM Switch, 19" LCD 1080p Rackmount TAA
1	Cisco Router	\$ 600,00	4 Ports - Management Port / Slots Gigabit Ethernet
1	Switch	\$ 600,00	24 Puertos QP-AVP24S QPCOM
1	Switch	\$ 600,00	24 Puertos Giga QPCOM QP-G240R
1	Central Telefónica con voz sobre IP	\$ 1.000,00	Teléfonos Grandstream BT200
5	UPS Departamento de TI	\$ 800,00	UPS
8	Gabinete para Cableado de Alta Densidad y Servidores	\$ 2.000,00	Marca Quest International S.A.

Tabla 3.10: Principales equipos informáticos dentro del departamento de TI

Fuente: Elaborado por el autor

Tomando en consideración la importancia de los servidores y los servicios que estos brindan se hace necesario realizar un análisis minucioso de estos y así entender de mejor manera sus características principales como se aprecia en la Tabla 3.11, servidores y sus características en la que se añadió la pérdida por hora de suspensión para en lo posterior mitigar los riesgos según el nivel de impacto que tendría hacia la institución si dejara de funcionar alguno de ellos. Se ha visto necesario hacer un estudio sobre los servicios que se encuentran alojados dentro de estos servidores como se observa en los Anexos en las Tablas B.2, B.3 y B.4 donde se puede observar una breve descripción, también el servicio o sistema ya sea elaborado de manera interna o externa, entre otras características.

Nº SERVIDOR	TIPO (RACK/TORRE)	SISTEMA OPERATIVO	MARCA	MODELO	CAPACIDAD EN DISCO (STORAGE)	VALOR DEL SERVIDOR	PERDIDA POR HORA DE SUSPENSIÓN	MECANISMOS DE RESPALDO	DESCRIPCIÓN	SERVICIOS
<b>Servidor 1</b>	RACK	Linux Centos	HP	Proliant DL360 G10	4 X 600 Gb	\$ 3.000,00	\$ 500,00	Externo	Servidor ZIMBRA	Servicio de correo electrónico. Sistema de recaudación del rubro Agua Potable. Sistema de recaudación de Activos y Patentes Sistema de recaudación del Impuesto al Juego Sistema de recaudación de Locales Comerciales Sistema de recaudación del Puestos en el mercado y Plazas Sistema de recaudación Especial de Mejoras Sistema de recaudación del Rubro Predio Urbano y años anteriores Sistema de recaudación del Rubro Predio Rural y años anteriores Reloj Biométrico (Control de asistencia de empleados y trabajadores) Servicio de internet en la institución y aplicaciones web Actualización de contenidos de la página web institucional Servidor dedicado de Antivirus (Eset Endpoint Security) Servicio de Facturación Electrónica Servicio de Video vigilancia (ZONEMINDER)
<b>Servidor 2</b>	RACK	Linux Centos	HP	Proliant DL320 G8	250 Gb	\$ 2.500,00	\$ 2.500,00	Externo	Servidor SAMBA	Sistema de Gestión de contenidos (WORDPRESS) Sistema (GUÍA RÁPIDA) Publicación de documentos Sistema de gestión de proyectos (COLLABTIVE) Sistema para compartir videos para aulas virtuales (PHPMOTION) Gestor de mensajería instantánea (INTRAMESSENGER) Administración de Base de Datos MySQL (phpMyAdmin) Sistema de emisión de memorandos (Comunicaciones internas) Sistema de recepción de oficios externos y guía de trámites Sistema de permisos de personal (Institucionales) Registro de Actas y Denuncias en la Comisaría (Administración) Registro de Vales pagados Registro de Profesionales (Obra civil) Registro de Ordenanzas, Reformas, Actas Registro y emisión de ordenes de pago Reportes de citaciones y Autos de pago de Coactiva Registro de personal Institucional Sistema de inventario de equipos de computo institucionales Sistema de sugerencias para el departamento de sistemas (Buzón) Sistema Integral de Catastros (Sistema AME predio Urbano) Sistema Integral de Catastros (Sistema AME predio Rural) Sistema Integral de Gestión Administrativa Financiera
<b>Servidor 3</b>	RACK	Linux Centos	HP	Proliant DL380 G7	250 Gb	\$ 2.000,00	\$ 1.500,00	Externo	Servidor de internet	
<b>Servidor 4</b>	RACK	Linux Centos	HP	Proliant DL120 G7	250 Gb	\$ 2.000,00	\$ 500,00	Externo	Servidor de Antivirus	
<b>Servidor 5</b>	TORRE	Linux Centos	HP	Proliant ML150 G5	160 Gb	\$ 1.500,00	\$ 1.000,00	Externo	Servidor de Facturación Electrónica	
<b>Servidor 6</b>	TORRE	Linux Centos	HP	Proliant ML150 G6	160 Gb	\$ 1.500,00	\$ 3.000,00	Externo	Servidor intranet	
<b>Servidor 7</b>	TORRE	Windows Server 2012	HP	Proliant ML150 G6	160 Gb	\$ 1.500,00	\$ 2.000,00	Externo	Servidor AME	

Tabla 3.11: Principales servidores de la institución y sus principales servicios

Fuente: Elaborado por el autor

## La importancia de la disponibilidad, integridad y confidencialidad para las operaciones.

Con este esquema podremos evaluar el riesgo en función de los niveles de confidencialidad (C), integridad (I) y disponibilidad (D). Las partes interesadas pueden acceder a estos datos con facilidad y tener más claro la situación como se encuentran los activos de la empresa y tomar decisiones rápidamente. A continuación, en la Tabla 3.12 se muestra la valoración acorde a la denominación (3 Alto, 2 Medio, 1 Bajo).

VALORACIÓN DE LOS ACTIVOS				
Valor	Denominación	Disponibilidad	Integridad	Confidencialidad
		Asegurando que los usuarios autorizados tienen acceso a la información y los activos asociados cuando se requiera	La cualidad de la información para no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones.	Asegurar que la información sea accesible solo para aquellos autorizados para tener acceso
3	Alto	Se podría esperar que la interrupción del acceso o uso del sistema de información tenga un efecto adverso severo o catastrófico en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la modificación o destrucción no autorizada de información tenga un efecto adverso severo o catastrófico en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la divulgación no autorizada de información tenga un efecto adverso severo o catastrófico en las operaciones de la organización, los activos de la organización o las personas.
2	Medio	Se podría esperar que la interrupción del acceso o uso del sistema de información tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la modificación o destrucción no autorizada de información tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la divulgación no autorizada de información tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.
1	Bajo	Se podría esperar que la interrupción del acceso o uso de la información o un sistema de información tenga un efecto adverso limitado o bajo en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la modificación o destrucción no autorizada de la información tenga un efecto adverso limitado en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la divulgación no autorizada de información tenga un efecto adverso limitado en las operaciones de la organización, los activos de la organización o las personas.

Tabla 3.12: Impacto potencial

Fuente: Elaborado por el autor a partir de [43]

Acorde con el esquema de valoración de los activos en la Tabla 3.12, misma que fue expuesta y analizada tanto por la autoridad mayor (Alcaldía Municipal) como miembros del departamento de Tecnologías de la Información se procede con la

primera etapa de valoración que corresponde a cada activo informático en la que podemos apreciar en que grado de disponibilidad, integridad y confidencialidad se encuentran.

En las Tablas 3.13 y 3.14 se muestran la valoración de los activos, que se la realizó en conjunto con la colaboración del departamento de TI.

CANTIDAD	EQUIPO	DESCRIPCIÓN	Disponibilidad	Integridad	Confidencialidad
1	<b>Servidor 1</b>	Servidor ZIMBRA	3	3	3
1	<b>Servidor 2</b>	Servidor SAMBA	3	3	3
1	<b>Servidor 3</b>	Servidor de Internet	3	3	3
1	<b>Servidor 4</b>	Servidor de Antivirus	3	3	3
1	<b>Servidor 5</b>	Servidor de Facturación Electrónica	3	3	3
1	<b>Servidor 6</b>	Servidor Intranet	3	3	3
1	<b>Servidor 7</b>	Servidor AME	3	3	3
2	<b>Switch</b>	24 PUERTOS QP-AVP24S QPCOM	3	3	3
2	<b>Switch</b>	24 PUERTOS GIGA QPCOM QP-G240R	2	3	3
1	<b>Regletas para Bastidor para Rack</b>	Nexxt Solutions para Rack AW220NXT95	2	-	-
1	<b>Tripp Lite Rack Console 1URM</b>	KVM Switch, 19" LCD 1080p Rackmount TAA	2	2	2
1	<b>Cisco Router</b>	4 Ports - Management Port / Slots Gigabit Ethernet	3	3	3
1	<b>Central Telefónica con voz sobre IP</b>	Teléfonos Grandstream BT200	3	2	2
5	<b>UPS de TI</b>	UPS	3	-	-
1	<b>Gabinete para Cableado de Alta Densidad y Servidores</b>	Marca Quest International S.A.	2	-	-

Tabla 3.13: Valoración de los activos acorde a la disponibilidad, integridad y confidencialidad

Fuente: Elaborado por el autor



CANTIDAD	EQUIPO	DESCRIPCIÓN	Disponibilidad	Integridad	Confidencialidad
2	Computadoras de escritorio completas	Intel(R) Core™ i7 - 870 CPU 2.93GHz & Intel(R) Core™ i7 - 8550 CPU 1.80GHz	2	2	2
2	Laptops personales	Laptops personales	2	2	2
1	HP LASER JET P2015DN	53A HP LASERJET	2	-	-
1	EPSON L355	54a HP LASERJET	2	-	-
1	HP COLOR LASERJET CP6015DN	HP COLOR LASERJET CB380A	2	-	-
1	Aire acondicionado	Cuarto de Telecomunicaciones	3	-	-
-	Infraestructura de red	Conexiones de red	3	-	-
-	Red WIRELESS	WIFI	2	2	2
-	Red LOCAL	LAN	3	3	3

Tabla 3.14: Valoración de los activos acorde a la disponibilidad, integridad y confidencialidad

Fuente: Elaborado por el autor

De acuerdo con los resultados obtenidos anteriormente podemos apreciar un panorama general sobre aspectos importantes que deben ser tomados en cuenta, para así en lo posterior analizar que ocurre con cada activo e identificar el impacto que tendría la falta de disponibilidad, integridad o bien la confidencialidad de los activos. Esta evaluación contribuye en gran parte a identificar que, dado a la interrupción del acceso, la modificación o destrucción no autorizada de información tanto como la divulgación de la misma cause un efecto adverso limitado, grave o catastrófico.

### 3.1.2.3. Alcance y límites

#### Definir el alcance y los límites de la gestión del riesgo de la seguridad de la información

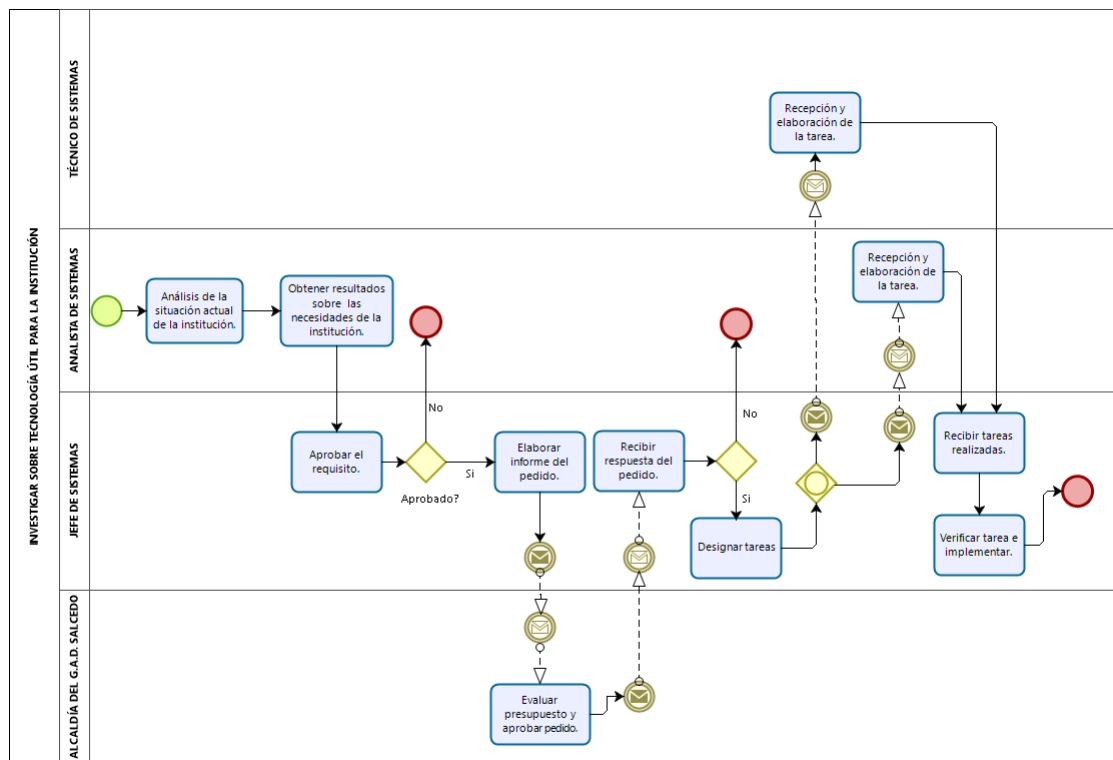
La presente investigación no sólo de limitará a elaborar un análisis y evaluación sobre los principales activos informáticos, sino que proporcionará un enfoque sobre las pérdidas y el costo que implicaría el mal funcionamiento de los activos hacia la institución, a través del diseño de un Plan de contingencia Informático, el mismo que es presentado al Alcalde del G.A.D. Municipal del cantón Salcedo, quien mostró interés por la propuesta junto con el departamento de Tecnologías de la Información, dicho plan de contingencia tiene como principal propósito

ayudar a gestionar la Seguridad de la Información. Este proyecto se limitará al desarrollo de la fase de pruebas y validación del Plan de Contingencia, de la misma manera no será implementado, por consiguiente, queda a cargo de las autoridades y del Departamento de Sistemas de la Municipalidad una vez completado con el proyecto de titulación proceder al desarrollo del mismo.

## Procesos de la organización

### Investigar sobre tecnología útil para la institución

El objetivo de este proceso es investigar nuevas tecnologías que sean útiles para el desarrollo de la institución que mejoren la administración, utilizando software libre y aplicaciones gratuitas, garantizando el buen uso tanto de los sistemas transaccionales como equipos informáticos. Figura 3.6



Powered by  
**bizagi**  
Modeler

Figura 3.6: Investigar sobre tecnología útil para la institución.  
Fuente: Elaborado por el autor a partir de una entrevista en el departamento de TI.

### Determinar necesidades de automatización

El objetivo de este proceso es planificar nuevas aplicaciones que mejoren el servicio brindado por los diferentes departamentos y de esta manera automatizar los procesos usando nueva tecnología. Es necesario brindar una capacitación continua a los encargados de utilizar las nuevas aplicaciones desarrolladas. Figura 3.7

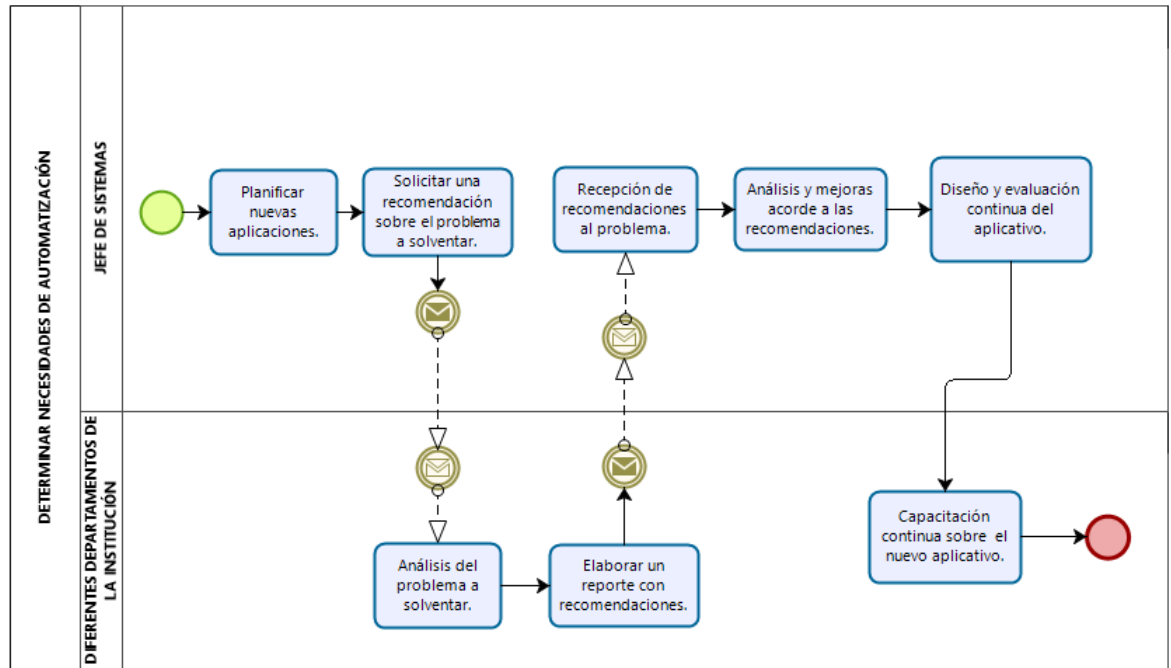


Figura 3.7: Determinar necesidades de automatización.

Fuente: Elaborado por el autor a partir de una entrevista en el departamento de TI.

### Elaborar planes informáticos

El objetivo de este proceso es elaborar un análisis de la situación actual del área informática que permita diseñar planes informáticos como el de contingencia, mantenimiento preventivo y correctivo. Se debe tomar en cuenta las normas de control interno y ordenanzas, leyes, etc. Relacionadas con el área de sistemas. Figura 3.8

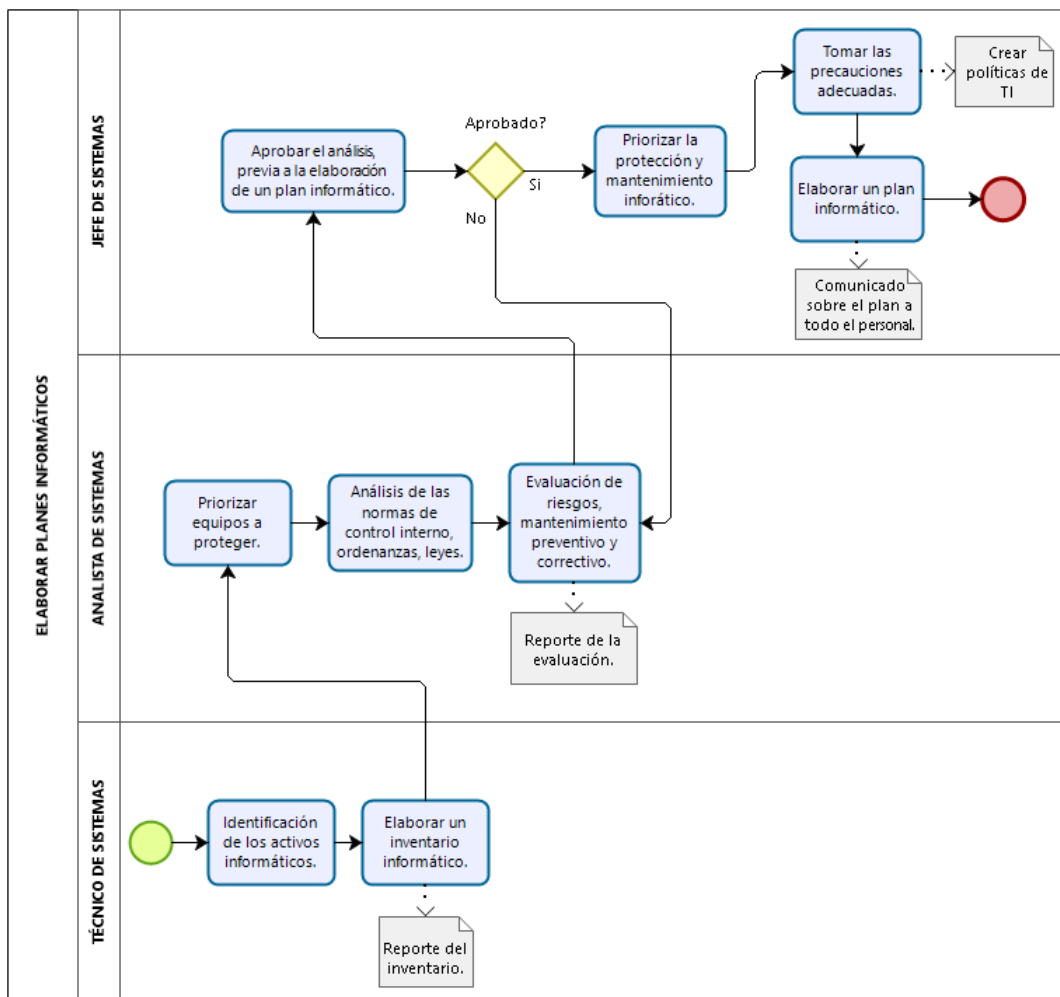
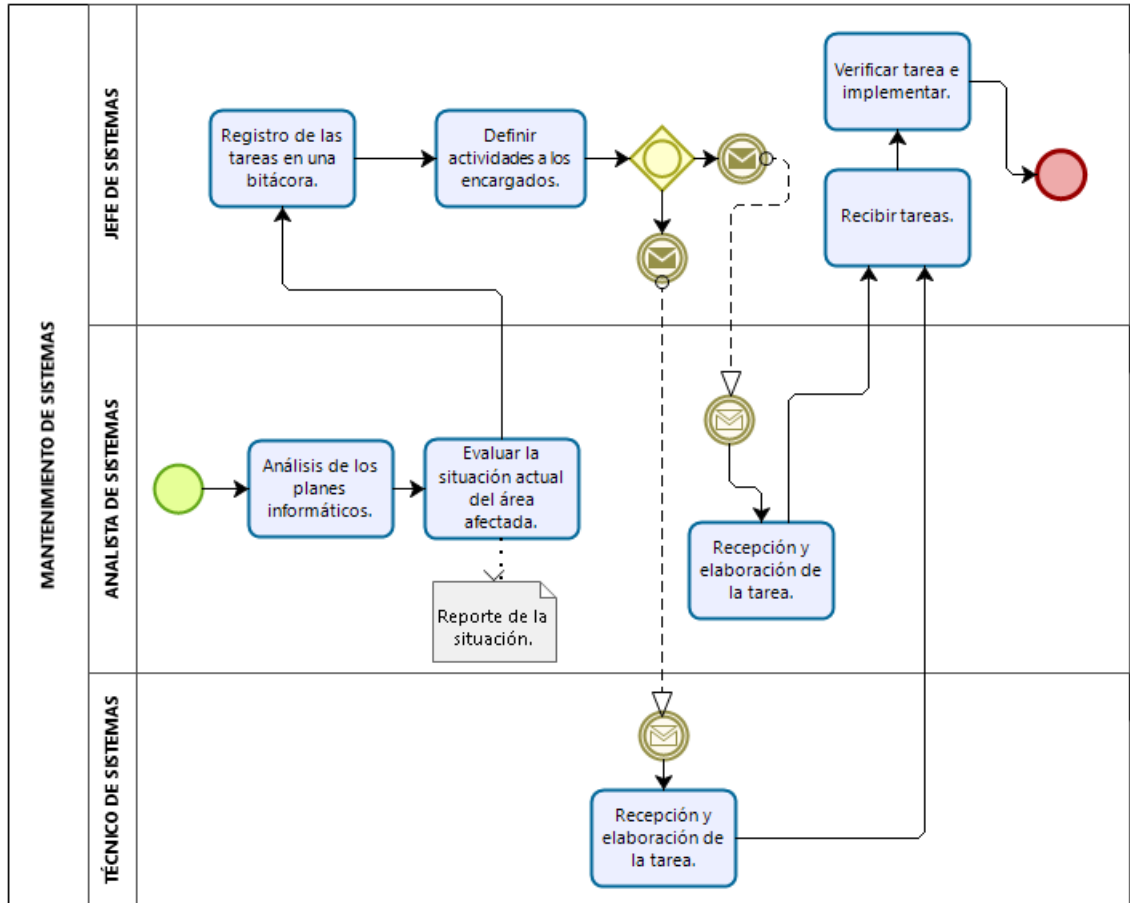


Figura 3.8: Elaborar planes informáticos.

Fuente: Elaborado por el autor a partir de una entrevista en el departamento de TI.

## Mantenimiento de sistemas

El objetivo de este proceso es dar un mantenimiento tanto preventivo como correctivo en las distintas áreas que contengan equipos y sistemas informáticos, mediante una evaluación continua apoyándose en los planes y manuales informáticos. Es necesario tener una bitácora de todo lo realizado. Figura 3.9



Powered by  
**bizagi**  
Modeler

Figura 3.9: Mantenimiento de sistemas.

Fuente: Elaborado por el autor a partir de una entrevista en el departamento de TI.

### Asesoramiento institucional

El objetivo de este proceso es la administración de contratos relacionados con el área de sistemas acorde a un análisis de las necesidades en los diferentes departamentos y solventar de una manera eficiente los requerimientos como es la adquisición de sistemas informáticos e instalación de equipos técnicos e informáticos. Figura 3.10

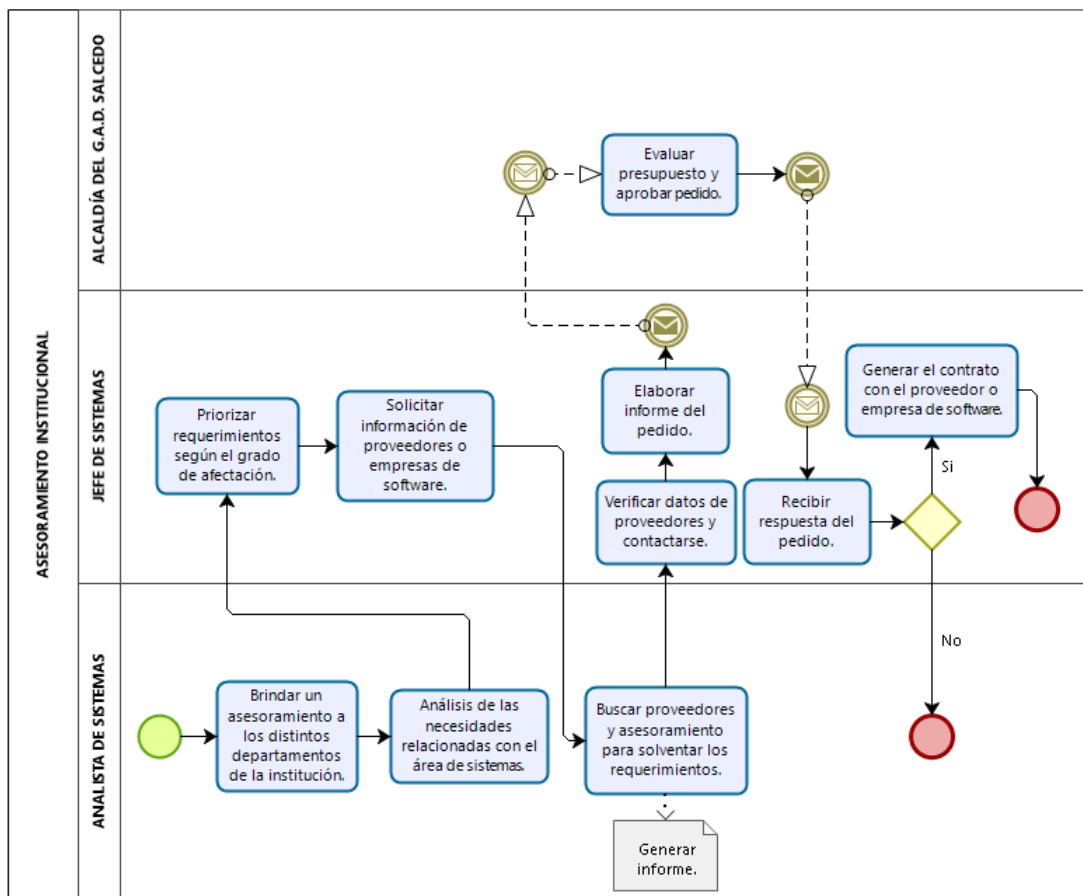


Figura 3.10: Asesoramiento institucional

Fuente: Elaborado por el autor a partir de una entrevista en el departamento de TI.

## Red de área local (LAN)

El objetivo de este proceso es mantener una correcta conectividad física de los equipos a través de las redes conectadas dentro de la institución. Determinando las necesidades de los departamentos y solventando problemas en una determinada área de la red. Figura 3.11

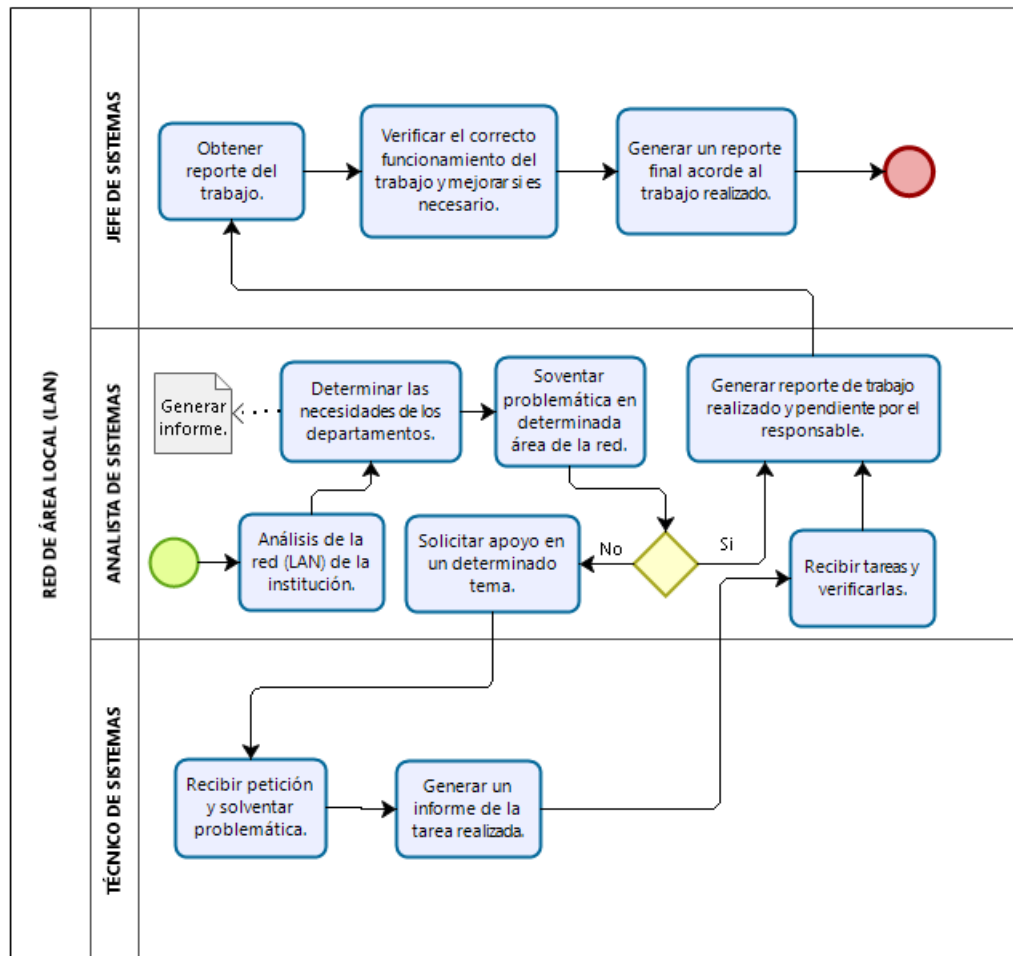


Figura 3.11: Red de área local (LAN)

Fuente: Elaborado por el autor a partir de una entrevista en el departamento de TI.

## Ubicación geográfica de la organización

El G.A.D. Municipal del cantón Salcedo se encuentra ubicado en la Calle Bolívar entre, Calle Sucre y Calle 24 de Mayo. Figura 3.12

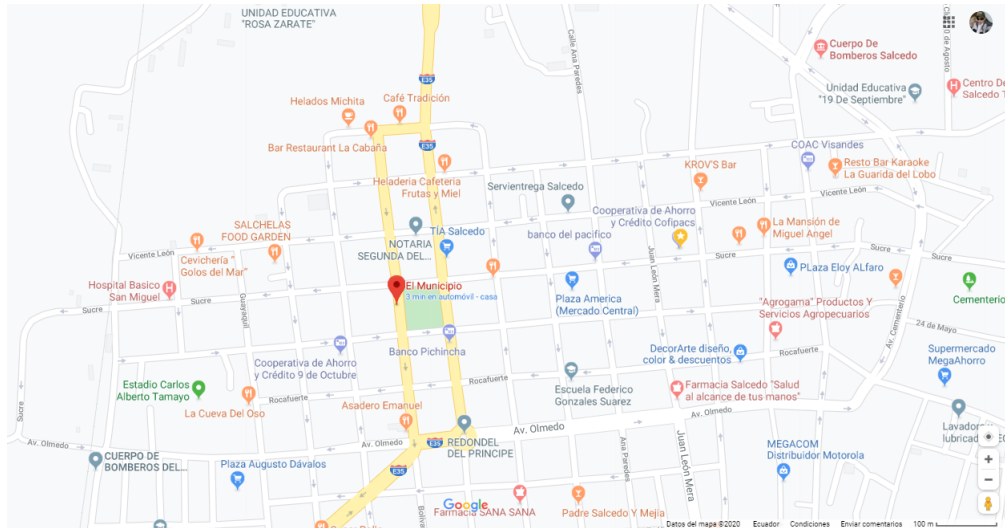


Figura 3.12: Vista Satelital ubicación geográfica de G.A.D. Municipal del cantón Salcedo

Fuente: Página Google Maps.

### 3.1.2.4. Organización para la gestión del riesgo de seguridad de la información

**Establecer una recomendación sobre el proceso de gestión del riesgo y la seguridad de la información**

Considerando que el término riesgo se refiere a los efectos que pueden ocasionar una amenaza si esta se convierte en un desastre y causen daño a una determinada organización. La gestión del riesgo hace énfasis a las actividades coordinadas en la que se pueda controlar y administrar una organización acorde al riesgo. El proceso de gestión de riesgo hace referencia a la aplicación sistemática de procedimientos y prácticas de gestión a las actividades de: comunicación y consulta, establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo. Acotando la seguridad de la información misma que toma las medidas tanto preventivas como correctivas permitiendo resguardar la información y mantener la disponibilidad, integridad y la confidencialidad de los datos. Como una breve recomendación y teniendo claro los principales conceptos es necesario llevar un correcto orden sistemático en el que nos permita evidenciar de manera clara la evaluación del riesgo acorde a los niveles que se designen dentro de esta investigación y así poder gestionar el riesgo correctamente.



### 3.1.3. Etapa de valoración del riesgo

#### 3.1.3.1. Identificación del riesgo

La siguiente etapa trata sobre la identificación del riesgo debe ser considerada de forma permanente e interactiva, con el respaldo del análisis del contexto correspondiente. Las siguientes etapas dependerán de una correcta identificación del riesgo. Con la colaboración de los encargados del departamento de TI de la municipalidad, se procedió a identificar las fuentes de riesgo que amenazan al G.A.D. Municipal del cantón Salcedo, sus causas y consecuencias potenciales. Como objetivo principal de esta etapa se realiza una lista de riesgos con base en aquellos eventos que podrían materializarse. Se ha hecho un análisis sobre los escenarios de contingencia recolectando información verás, clasificándola acorde a las posibles causas que pueden originar un riesgo como pueden ser: desastres naturales, falta de servicios y provocadas por el humano como podemos observar en la Figura 3.13.

#### Identificación de escenarios de contingencia y amenaza.

Se obtiene de la información recolectada de los riesgos críticos identificados en la municipalidad, es importante conocer las causas y el impacto que afectaría a la organización si llegarán a materializarse. En la Figura 3.13 se representa los posibles escenarios de contingencia que se pueden presentar ante la seguridad de la información.

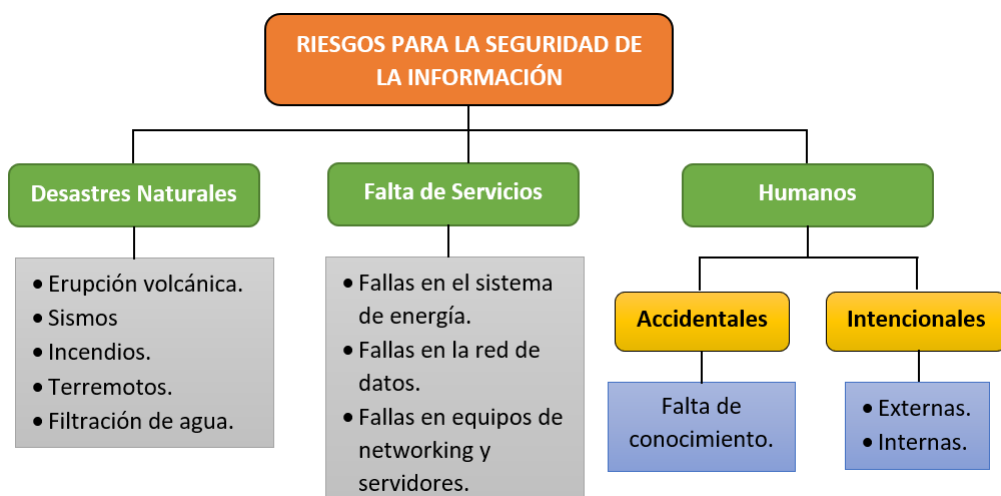


Figura 3.13: Riesgos para la seguridad de la información.

Fuente: Elaborado por el autor a partir de [36]

### Principales capas concéntricas del planeta Tierra

En los últimos 50 años, estudios de geofísica y geoquímica en todo el mundo han demostrado que el planeta Tierra se encuentra compuesto por tres grandes capas concéntricas que son: la Corteza con un espesor variable de entre 10 y 100 km, el Manto tiene un espesor de 2900 km y el Núcleo uno de 3500 km. Figura 3.14 El Manto arrastra en diferentes direcciones a la delgada Corteza que se encuentra sobre, lo que provoca que la superficie de la Tierra esté dividida en grandes segmentos conocidos como “Placas tectónicas”. [44]

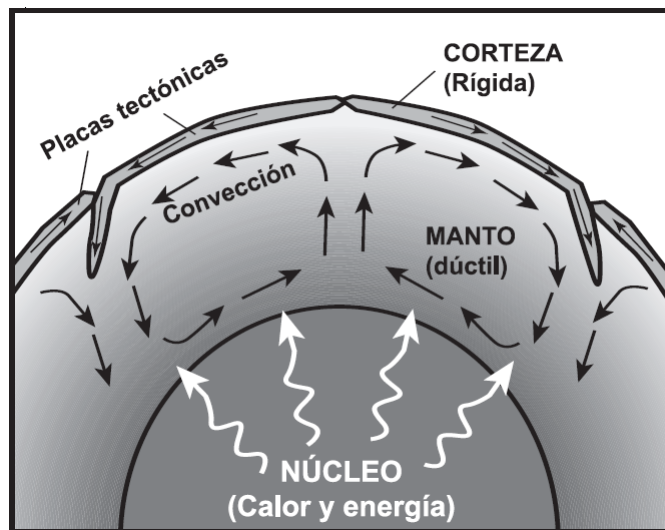


Figura 3.14: Principales capas concéntricas del planeta Tierra  
Fuente: Libro “Los peligros volcánicos asociados con el Cotopaxi” [44]

En la Figura 3.15, muestra las diferentes “placas tectónicas” donde las líneas gruesas representan los límites de las placas. 1) Límite de divergencia (las placas Sudamericana y Africana se separan una de la otra); 2) Límite de transurrencia (la placa del Pacífico se desliza junto a la placa de Norteamérica); y, 3) Límite de convergencia (la placa Nazca choca con la Sudamericana). [44]

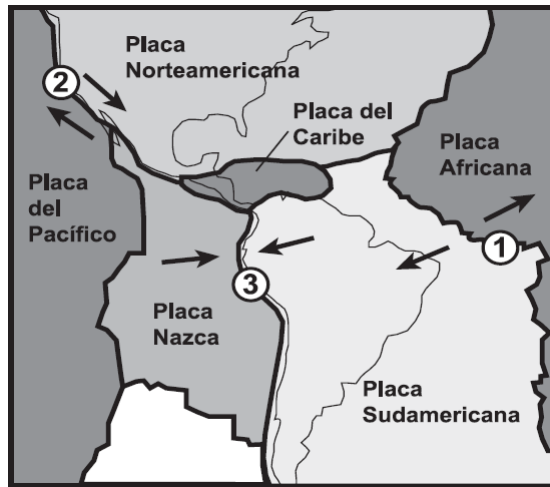


Figura 3.15: Representación de las diferentes “placas tectónicas”  
 Fuente: Libro “Los peligros volcánicos asociados con el Cotopaxi” [44]

Ecuador está ubicado en una zona donde dos placas tienen un límite de convergencia: las placas de Nazca y de Sudamérica. Esto ocasiona que la placa de Nazca choque y luego se sumerja bajo la placa Sudamericana, entrando poco a poco al Manto terrestre, dando lugar a la formación de magmas.[44]  
 Los magmas forman volcanes al llegar a la superficie provocando sismos y erupciones volcánicas. Como se puede apreciar en la Figura 3.16

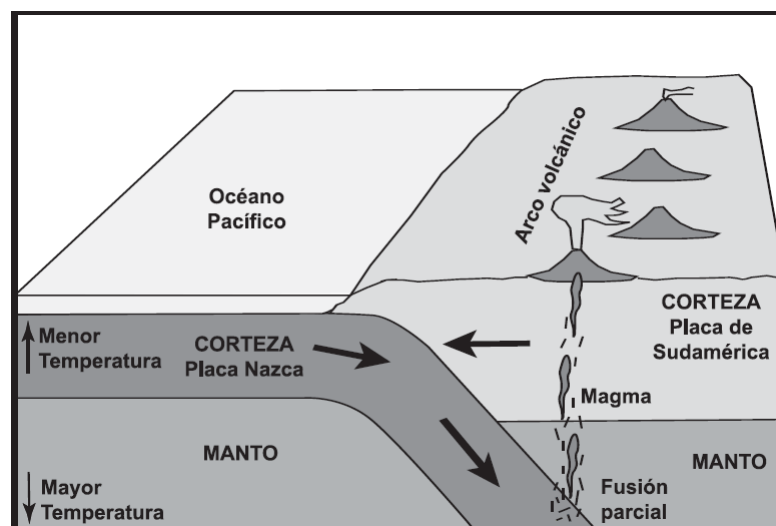


Figura 3.16: Subducción de la placa Nazca bajo la Sudamericana  
 Fuente: Libro “Los peligros volcánicos asociados con el Cotopaxi” [44]

## Peligro Volcánico

El cantón Salcedo perteneciente a la Provincia de Cotopaxi, ubicado en la Cordillera Real de los Andes del Ecuador, sector propenso a varios fenómenos naturales, como es el caso del volcán Cotopaxi mismo que es un gran estratovolcán activo, a 60 km al sureste de Quito y a 45 km al norte de Latacunga.[45]

El Cotopaxi ha presentado cinco ciclos eruptivos en los años: 1532-1534, 1742-1744, 1766-1768, 1853-1854 y 1877-1880. Cerca de trece erupciones graves ocurrieron dentro de estos cinco ciclos, los fenómenos volcánicos que provocaron estas erupciones fueron:

1. Caída de ceniza, pómez y escoria.
2. Flujos de lava.
3. Flujos piroclásticos.
4. Flujos de lodo y escombros (lahares)

Fuente: [45]

Estos fenómenos volcánicos afectaron gravemente el área alrededor del volcán, causando daños significativos a la propiedad, especialmente al sector agrícola, víctimas y crisis económica regional.

## Principales amenazas provocadas por la erupción del volcán Cotopaxi

Para entender mejor las amenazas a las cuales el cantón Salcedo y sus alrededores se encontraron expuestos se hace un análisis de las últimas erupciones registradas en los años 1877-1880. A continuación, en la Tabla 3.15 se registran datos acordes a las principales amenazas que se suscitaron, tomando en cuenta la frecuencia, intensidad, magnitud, daños provocados.

PONDERACIÓN DE AMENAZAS IDENTIFICADAS													
AÑO	Amenaza / Evento	FRECUENCIA			Recurrencia	INTENSIDAD			MAGNITUD			DAÑOS	
		LARGO PLAZO	MEDIANO PLAZO	CORTO PLAZO		ALTO	MEDIO	BAJO	LARGO	MEDIANO	CORTO	HUMANOS	MATERIALES
1877 1880	Sismos volcánicos			X	VARIAS VECES			X		X		X	X
1877 1880	Gases volcánicos			X	VARIAS VECES			X		X		X	
1877 1880	Lluvia de ceniza y piroclastos	X			VARIAS VECES	X			X			X	X
1877 1880	Flujo de lodos y escombros (lahares)	X			VARIAS VECES		X			X		X	X

Tabla 3.15: Matriz de ponderación de amenazas identificadas

Fuente: Elaborado por el autor a partir de [44] [45]

El G.A.D. Municipal del cantón Salcedo se encuentra dentro de la zona de riesgo de flujos de lodo y escombros (lahares) como se puede ver en la Figura 3.17

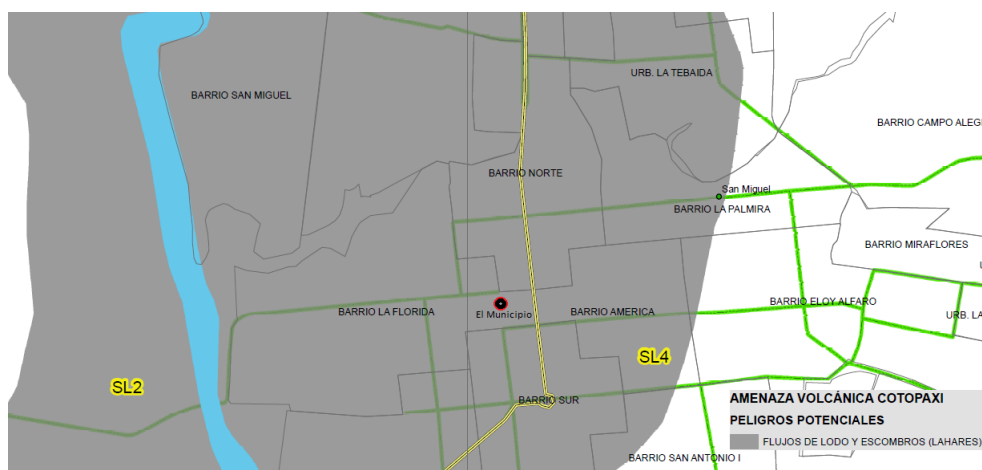


Figura 3.17: Mapa de rutas de evacuación y zonas seguras de Salcedo  
Fuente: Servicio Nacional de Gestión de Riesgos y Emergencias Ecuador [46]

### **Peligro Sísmico**

El cantón Salcedo está ubicado en la Cordillera Real de los Andes del Ecuador y se encuentra propenso a una alta incidencia sísmica, debido a que la placa Nazca se mueve a una velocidad relativa de 9 cm/año donde choca y luego se sumerja bajo la placa Sudamericana como se observó en la Figura 3.16, este choque produce deformación en las placas dando lugar a una liberación repentina de energía acumulada en fallas en la corteza ubicadas en zonas de fricción provocando daños humanos y materiales.[44]

### **Peligros Naturales**

Otros peligros naturales a los cuales el cantón Salcedo está expuesto son: erupción volcánica, sismos, filtración de agua, humedad. Estas amenazas son propensas a materializarse y afectar el correcto funcionamiento de la institución.

### **Falta de servicios**

Una de las principales preocupaciones de todas las entidades públicas y privadas que brindan servicios y atención a la ciudadanía pueden originarse por diversos factores como son:

- Fallas en el sistema de energía.
- Fallas en la red de datos.
- Fallas en equipos de networking y servidores.

El G.A.D. Municipal no cuenta con un generador eléctrico que permita abastecer el flujo normal de la electricidad, causando detener el normal funcionamiento de las actividades y una pérdida económica significativa. Las fallas en la red de datos dependen de varios factores como el deterioro por el uso así como el ambiente húmedo al cual está expuesto tanto el cableado de red como sus equipos de networking y servidores.

### **Riesgos originados por el Humano**

En un estudio realizado por Ponemon Institute – The Human Factor in Data Protection (2012), muestra que “el 78 % de las organizaciones se han visto expuestas a incidentes de seguridad debido a empleados negligentes o maliciosos. La investigación fue realizada sobre 709 encuestados en EE.UU. dentro del área de TI a cargo de la protección de la información”. Como podemos darnos cuenta en las estadísticas muestran un gran número de incidentes ocasionados por el factor humano. El caso de los ciberdelincuentes a nivel mundial sostiene un tema muy delicado dado a las brechas que la información se ve expuesta ya sea por cambios en las telecomunicaciones, Internet, almacenamiento de datos en medios como la nube, redes sociales, etc.[47]

## **LISTA DE LOS PRINCIPALES RIESGOS BASADOS EN EVENTOS QUE PUEDEN LLEGAR A SUCEDER**

Continuando con el desarrollo de la propuesta en esta parte se muestra un listado de los posibles riesgos que pueden llegar a materializarse, esta etapa está fundamentada en el análisis del contexto, así como eventos considerados por la colaboración del departamento de “Dirección de Seguridad ciudadana” de la institución en la que se compartió varios criterios sobre la seguridad a la que se encuentra expuesto el G.A.D. Municipal. Para completar la identificación sobre estos riesgos se basa en la experiencia que tienen los encargados del “Departamento de TI”, con el manejo de los equipos, así como documentación sobre las normas y políticas de seguridad informática, un plan integral informático mismos que fueron de gran apoyo para un mejor estudio del caso.

En conjunto con el departamento de TI se desarrolló el listado que se muestra en la Tabla 3.16, en el que se a tomado de manera organizada los riesgos que tienen mayor impacto, así como aquellos que ya se han materializado, y afectan el normal funcionamiento de los equipos e interrumpiendo las actividades en la institución, dichos riesgos tienen sus causas y consecuencias que posteriormente se los identificará.

Nº RIESGO	IDENTIFICACIÓN
R1	Flujo de lodos y escombros (lahares)
R2	Lluvia de ceniza y piroclastos
R3	Sismos (volcánicos/repentinos)
R4	Interrupción del servicio de energía eléctrica
R5	Filtración de agua
R6	Incendio
R7	Daño en el ventilador
R8	Daño en fuente de poder
R9	Falla de disco duro SATA/IDE
R10	Falla de Tarjeta de Red
R11	Fallas de Software/Configuración
R12	Falla de cableado y conectores
R13	Acceso no autorizado (Robo o alteración de información)
R14	Ataques DoS o denegación de servicio
R15	Falla de Hardware
R16	Error Humano (Falta de conocimiento)
R17	Robo de dispositivos
R18	Atasco de papel en la impresora
R19	El dispositivo (PC) no reconoce la impresora
R20	Presencia de interferencias electromagnéticas
R21	Ingeniería social

Tabla 3.16: Listado de los posible riesgos que pueden materializarse

Fuente: Elaborado por el autor

Una vez redactado correctamente el riesgo operativo, se procede a asociar sus causas y consecuencias, para esto se ha realizado un listado de las causas y consecuencias respectivamente las mismas que serán asociadas usando la técnica denominada "análisis de corbata" (bow tie analysis).

**Causas:** Se relacionan con el riesgo a través de expresiones como:

- Puesto que ...
- Debido a ...

Y se clasifican según las siguientes categorías:

COD	EXTERNAS	COD	INTERNAS
E1	Erupción volcánica.	I1	Incorrecto mantenimiento por parte de las autoridades.
E2	Ubicación geográfica.	I2	Incendios eléctricos.
E3	Imperfecciones del suministro eléctrico.	I3	Utilizar cigarrillos y fósforos.
E4	Mantenimiento de la planta eléctrica.	I4	Líquidos inflamables.
E5	Exceso de Lluvias.	I5	Falta de orden y aseo.
E6	Humedad.	I6	Incendios provocados.
E7	Ciberatacantes a los recursos.	I7	Superficies calientes.
E8	Manipulación psicológica del personal.	I8	Acumulación de polvo.
E9	Correos electrónicos de phishing.	I9	Falta de mantenimiento.
		I10	Deterioro por el tiempo.
		I11	Sobretensión.
		I12	Exceso de temperatura.
		I13	Apagado incorrecto.
		I14	Virus o malware.
		I15	Desgaste o la corrosión.
		I16	Problema en los (controladores).
		I17	Problema físico en la placa.
		I18	Mal configuración de la tarjeta.
		I19	Archivos del sistema dañados.
		I20	Falta de actualizaciones del equipo.
		I21	Desinstalaciones realizadas incorrectamente.
		I22	Falta de seguridad en la institución.
		I23	Ausencia de cámaras de seguridad.
		I24	Empleado desleal cómplice.
		I25	Antivirus desactualizado.
		I26	Empleado desleal cómplice.
		I27	Acceso a sitios web y redes sociales de carácter peligroso.
		I28	USB o Dispositivos insertados con virus.
		I29	Falta de capacitación.
		I30	Negligencia laboral.
		I31	El papel no está cargado correctamente en la bandeja.
		I32	Cables conectados incorrectamente.
		I33	Instalaciones eléctricas cerca del cableado de red.

Tabla 3.17: Clasificación de causas

Fuente: Elaborado por el autor

**Consecuencias:** Se relacionan con el riesgo a través de expresiones como:

- Así que ...
- De manera que ...

Se clasifican según las siguientes categorías:



COD	CONSECUENCIAS
C1	Pérdidas materiales.
C2	Pérdidas económicas.
C3	Daños a la integridad física.
C4	Pérdida de información.
C5	Interrupción del trabajo.
C6	Infraestructura.
C7	Apagados frecuentes en el equipo.
C8	Presenta lentitud en el equipo.
C9	No enciende el equipo.
C10	Problemas en la detección de conexiones.
C11	Desestabilización institucional.
C12	Denegación de servicio.
C13	Pérdida de la conectividad de la red.
C14	Equipo funcione mucho más lento de lo normal.
C15	Sistema muestre pantallas azules de la muerte.

Tabla 3.18: Clasificación de consecuencias

Fuente: Elaborado por el autor

**Análisis de corbata (bow tie analysis):** Esta técnica es recomendada para el desarrollo de esta fase, en el análisis se utiliza el esquema de corbatín donde de forma sencilla podemos analizar el trayecto del riesgo empezando de las causas a las consecuencias. Al notar una similitud entre algunas consecuencias según el tipo de riesgo se ha considerado contar con una precalificación, para complementar el esquema se ha visto necesario colocar un parámetro adicional (Grado de negatividad), en el cual nos permite diferenciar entre las distintas consecuencias según el grado de afectación de los riesgos al que estará expuesto el G.A.D. Municipal.

Y de esta manera identificar que riesgo tiene mayor consecuencia según los parámetros (muy severo, grave, moderado y leve). Para esta precalificación sobre las consecuencias se a contado con el apoyo del personal del departamento de TI y documentación interna de la municipalidad.

La Tabla 3.19 nos ayuda con esta clasificación inicial que servirá como complemento para el análisis del riesgo posteriormente.

GRADO DE NEGATIVIDAD	DESCRIPCIÓN	TRATAMIENTO
<b>Muy Severo</b>	Consecuencias en la zona de riesgo extrema o inaceptables.	Correctivo prioritario
<b>Grave</b>	Consecuencias en la zona de riesgos importantes.	Correctivo inmediato
<b>Moderado</b>	Consecuencias en la zona de riesgos moderados.	Correctivo moderado
<b>Leve</b>	Consecuencias en la zona de riesgos aceptables o baja.	Preventivo

Tabla 3.19: Clasificación inicial según el grado de negatividad

Fuente: Elaborado por el autor

CAUSA (S)		ESCENARIO DE RIESGO	CONSECUENCIA (S)		GRADO DE NEGATIVIDAD
Determino las causas que pueden llevar a que se presente el escenario de riesgo. <b>ESCENARIO DE RIESGO DEBIDO A:</b>		Describe claramente el riesgo teniendo en cuenta los eventos que pueden llegar a ocurrir y el activo/proceso que puede afectar.	EFECTO	CONSECUENCIA	VALORACIÓN
COD	CAUSA	RIESGO	COD	CONSECUENCIA	VALORACIÓN
E1	Erupción volcánica	Flujo de lodos y escombros (lahares)	C1	Pérdidas materiales	Muy Severo
E2	Ubicación geográfica		C2	Pérdidas económicas	Muy Severo
E1	Erupción volcánica		C3	Daños a la integridad física	Muy Severo
E2	Ubicación geográfica		C4	Pérdida de información	Muy Severo
E1	Erupción volcánica		C5	Interrupción del trabajo	Muy Severo
E2	Ubicación geográfica		C6	Infraestructura	Muy Severo
E1	Erupción volcánica	Lluvia de ceniza y piroclastos	C1	Pérdidas materiales	Grave
E2	Ubicación geográfica		C2	Pérdidas económicas	Grave
E1	Erupción volcánica		C3	Daños a la integridad física	Grave
E2	Ubicación geográfica		C6	Interrupción del trabajo	Grave
E1	Erupción volcánica	Sismos (volcánicos/repentinos)	C1	Pérdidas materiales	Grave
E2	Ubicación geográfica		C2	Pérdidas económicas	Grave
E1	Erupción volcánica		C3	Daños a la integridad física	Grave
E2	Ubicación geográfica		C4	Pérdida de información	Grave
E1	Erupción volcánica		C5	Interrupción del trabajo	Grave
E2	Ubicación geográfica		C6	Infraestructura	Grave
E3	Imperfecciones del suministro eléctrico	Interrupción del servicio de energía eléctrica	C1	Pérdidas materiales	Moderado
E4	Mantenimiento de la planta eléctrica		C2	Pérdidas económicas	Moderado
E4	Mantenimiento de la planta eléctrica		C4	Pérdida de información	Leve
E4	Mantenimiento de la planta eléctrica		C5	Interrupción del trabajo	Moderado

Tabla 3.20: Identificación de riesgos en esquema de corbatín (bow tie)

Fuente: Elaborado por el autor

CAUSA (S)		ESCENARIO DE RIESGO	CONSECUENCIA (S)		GRADO DE NEGATIVIDAD
Determino las causas que pueden llevar a que se presente el escenario de riesgo. <b>ESCENARIO DE RIESGO DEBIDO A:</b>		Describa claramente el riesgo teniendo en cuenta los eventos que pueden llegar a ocurrir y el activo/proceso que puede afectar.	Efecto que podría llegar a tener la ocurrencia del escenario de riesgo en el G.A.D. Municipal del cantón Salcedo.		Muestra el grado de negatividad según el tipo de riesgo.
COD	CAUSA		COD	CONSECUENCIA	
I1	Incorrecto mantenimiento por parte de las autoridades	Filtración de agua	C1	Pérdidas materiales	Grave
E5	Exceso de Lluvias		C2	Pérdidas económicas	Grave
I10	Deterioro por el tiempo		C4	Pérdida de información	Muy Severo
I2	Incendios eléctricos		C5	Interrupción del trabajo	Grave
I3	Utilizar cigarrillos y fósforos		C1	Pérdidas materiales	Muy Severo
I4	Líquidos inflamables	Incendio	C2	Pérdidas económicas	Muy Severo
I5	Falta de orden y aseo		C3	Daños a la integridad física	Muy Severo
I6	Incendios provocados		C4	Pérdida de información	Muy Severo
I7	Superficies calientes		C5	Interrupción del trabajo	Muy Severo
I8	Acumulación de polvo		C6	Infraestructura	Muy Severo
I9	Falta de mantenimiento	Daño en el ventilador	C7	Apagados frecuentes en el equipo	Moderado
I10	Deterioro por el tiempo		C5	Interrupción del trabajo	Grave
I10	Deterioro por el tiempo		C8	Presenta lentitud en el equipo	Moderado
I11	Sobretensión	Daño en fuente de poder	C9	No enciende el equipo	Moderado
I12	Exceso de temperatura		C5	Interrupción del trabajo	Grave
I8	Acumulación de polvo		C2	Pérdidas económicas	Muy Severo
E3	Imperfecciones del suministro eléctrico	Falla de disco duro SATA/IDE	C4	Pérdida de información	Muy Severo
I13	Apagado incorrecto		C5	Interrupción del trabajo	Grave
I14	Virus o malware		C9	No enciende el equipo	Grave
I15	Desgaste o la corrosión				
I10	Deterioro por el tiempo				

Tabla 3.21: Identificación de riesgos en esquema de corbatín (bow tie)

Fuente: Elaborado por el autor

CAUSA (S)		ESCENARIO DE RIESGO	CONSECUENCIA (S)		GRADO DE NEGATIVIDAD
Determino las causas que pueden llevar a que se presente el escenario de riesgo. <b>ESCENARIO DE RIESGO DEBIDO A:</b>		Describe claramente el riesgo teniendo en cuenta los eventos que pueden llegar a ocurrir y el activo/proceso que puede afectar.	Efecto que podría llegar a tener la ocurrencia del escenario de riesgo en el G.A.D. Municipal del cantón Salcedo.		Muestra el grado de negatividad según el tipo de riesgo.
COD	CAUSA	RIESGO	COD	CONSECUENCIA	VALORACIÓN
I16	Problema en los (controladores)	<b>Falla de Tarjeta de Red</b>	C10	Problemas en la detección de conexiones	Moderado
I17	Problema físico en la placa		C2	Pérdidas económicas	Moderado
I18	Mal configuración de la tarjeta		C5	Interrupción del trabajo	Moderado
I19	Deterioro por el tiempo		C2	Pérdidas económicas	Muy Severo
I20	Archivos del sistema dañados		C4	pérdida de información	Muy Severo
I21	Falta de actualizaciones del equipo		C5	Interrupción del trabajo	Muy Severo
I14	Virus o malware		C7	Apagados frecuentes en el equipo	Grave
I10	Deterioro por el tiempo		C8	Presenta lentitud en el equipo	Moderado
I25	Antivirus desactualizado		C9	No enciende el equipo	Grave
I27	Acceso a sitios web y redes sociales de carácter peligroso		C4	Pérdida de información	Grave
I28	USB o Dispositivos insertados con virus	C5	Interrupción del trabajo	Moderado	
I21	Desinstalaciones realizadas incorrectamente	C2	Pérdidas económicas	Moderado	
E6	Humedad	C1	Pérdidas materiales	Grave	
I10	Deterioro por el tiempo	C2	Pérdidas económicas	Grave	
I22	Falta de seguridad en la institución	C4	Pérdida de información	Grave	
I23	Ausencia de cámaras de seguridad	C5	Interrupción del trabajo	Grave	
I24	Empleado desleal cómplice	C11	Desestabilización institucional	Grave	
I29	Falta de capacitación	C12	Denegación de servicio	Muy Severo	
E7	Ciberatacantes a los recursos	C13	Pérdida de la conectividad de la red	Grave	
I25	Antivirus desactualizado	C2	Pérdidas económicas	Grave	
I26	Empleado desleal cómplice	C4	Pérdida de información	Muy Severo	
		C5	Interrupción del trabajo	Grave	
		C11	Desestabilización institucional	Muy Severo	
			<b>Ataques DoS o denegación de servicio</b>		
			<b>Acceso no autorizado (Robo o alteración de información)</b>		
			<b>Falla de cableado y conectores</b>		

Tabla 3.22: Identificación de riesgos en esquema de corbatín (bow tie)

Fuente: Elaborado por el autor

CAUSA (S)		ESCENARIO DE RIESGO	CONSECUENCIA (S)		GRADO DE NEGATIVIDAD
Determino las causas que pueden llevar a que se presente el escenario de riesgo. <b>ESCENARIO DE RIESGO DEBIDO A:</b>		Describe claramente el riesgo teniendo en cuenta los eventos que pueden llegar a ocurrir y el activo/proceso que puede afectar.	Efecto que podría llegar a tener la ocurrencia del escenario de riesgo en el G.A.D. Municipal del cantón Salcedo.		Muestra el grado de negatividad según el tipo de riesgo.
COD	CAUSA	RIESGO	COD	CONSECUENCIA	VALORACIÓN
E3	Imperfecciones del suministro eléctrico	<b>Falla de Hardware</b>	C2	Pérdidas económicas	Grave
E6	Humedad		C4	Pérdida de información	Grave
I8	Acumulación de polvo		C5	Interrupción del trabajo	Grave
I9	Falta de mantenimiento		C14	Equipo funcione mucho más lento de lo normal	Grave
I10	Deterioro por el tiempo		C15	Sistema muestre pantallas azules de la muerte	Grave
I11	Sobretensión	<b>Error Humano (Falta de conocimiento)</b>	C2	Pérdidas económicas	Moderado
I13	Apagado incorrecto		C4	Pérdida de información	Moderado
I29	Falta de capacitación		C5	Interrupción del trabajo	Moderado
I30	Negligencia laboral	<b>Robo de dispositivos</b>	C1	Pérdidas materiales	Grave
I23	Ausencia de cámaras de seguridad		C2	Pérdidas económicas	Grave
I22	Falta de seguridad en la institución		C4	Pérdida de información	Muy Severo
I24	Empleado desleal cómplice		C5	Interrupción del trabajo	Grave
I10	Deterioro por el tiempo		C11	Desestabilización institucional	Grave
I9	Falta de mantenimiento	<b>Atasco de papel en la impresora</b>	C2	Pérdidas económicas	Moderado
I29	Falta de capacitación		C5	Interrupción del trabajo	Leve
I31	El papel no está cargado correctamente en la bandeja		C2	Pérdidas económicas	Leve
I16	Problema en los (controladores)	<b>El dispositivo no reconoce la impresora</b>	C5	Interrupción del trabajo	Leve
I32	Cables conectados incorrectamente		C2	Pérdidas económicas	Leve
I10	Deterioro por el tiempo	<b>Presencia de interferencias electromagnéticas</b>	C2	Pérdidas económicas	Moderado
I33	Instalaciones eléctricas cerca del cableado de red		C4	Pérdida de información	Moderado
E8	Manipulación psicológica del personal		C4	Pérdida de información	Grave
E9	Correos electrónicos de phishing	<b>Ingeniería social</b>	C5	Interrupción del trabajo	Grave
			C11	Desestabilización institucional	Grave

Tabla 3.23: Identificación de riesgos en esquema de corbatín (bow tie)

Fuente: Elaborado por el autor

### 3.1.3.2. Análisis del riesgo

Una vez identificado el escenario de riesgo junto con sus causas y consecuencias, se procede a realizar el análisis que dependerá de la información obtenida en la identificación de los riesgos acorde al activo informático que se encuentre expuesto. Es decir, la calificación del riesgo es subjetiva y depende del conocimiento y experiencia de las personas que participan en su análisis. Considerando el método de evaluación (Annualized Loss Expectancy o ALE por sus siglas en inglés) anteriormente explicado, se calificará los riesgos utilizando los parámetros expuestos en las Tablas 2.7 y 2.8, tomando como referencia los parámetros de impacto en la Tabla 2.8, en la que se encuentra relacionado con el impacto que tendría con respecto al: usuario, la interrupción de las operaciones de la institución, su imagen o credibilidad se vean afectadas y las pérdidas económicas.

Como primera parte se obtuvo los datos subjetivos de acuerdo con los conocimientos y experiencia por parte del personal encargado, mismos que con ayuda de la herramienta Excel de Microsoft se logró tener un orden adecuado consiguiendo un promedio sobre las opiniones del personal (jefe del departamento de TI, analista de Sistemas, y técnico de TI) con quienes se cuenta con la participación para este análisis, como respaldo a este procedimiento se cuenta con la técnica Delphi donde se sugiere aplicarla mínimo a 3 o 4 personas.

Para el análisis se ha diseñado un esquema que contendrá los resultados sobre la evaluación realizada por los expertos, los parámetros correspondientes de los esquemas se muestran a continuación:

- **Nº RIESGO:** Código del riesgo respectivamente.
- **RIESGO:** Listado de los riesgos identificados que afectan a un determinado equipo.

### ANÁLISIS

En esta parte se puede encontrar varios parámetros los cuales son de gran relevancia, ya que son los resultados del promedio general luego de aplicar la técnica Delphi, donde se muestra los datos subjetivos por parte del personal encargado del departamento de TI. Se puede apreciar el parámetro (VA), mismo que en conjunto con el tutor se ha visto optimo sumarle el valor del activo junto con la perdida por hora, la cual nos ayuda a tener una respuesta clara sobre cual activo tomar las medidas correctivas de manera inmediata en el caso de que estas dejen de funcionar y evitar pérdidas económicas significativas para el G.A.D. Municipal.

- **VA:** Valor del activo + Valor de pérdida por hora (PH).
- **ARO:** Tasa de Ocurrencia Anualizada (Probabilidad de ocurrencia).
- **FE:** Factor de Exposición (Impacto).

## **UBICACIÓN EN LA MATRIZ**

Para conseguir la ubicación en la matriz de riesgos se ha hecho una relación que va desde los parámetros (ARO y FE), mismos que nos ayudan con la ubicación sobre la matriz de 5x5 (probabilidad eje “Y” e impacto eje “X”) respectivamente. Como primera parte se toma como referencia la Tabla 2.7, correspondiente a la probabilidad de ocurrencia y el impacto en la Tabla 2.8. En estas tablas se muestra el parámetro correspondiente al nivel, mismo que será tomado de acuerdo con la valoración de la frecuencia sobre (ARO y FE).

## **PARÁMETRO IMPACTO**

Considerando la valoración establecida por la Tabla 2.8, en relación con la escala determinada anteriormente en la ubicación del riesgo en la matriz por el impacto en el eje “X”, se presenta la Tabla 2.8 en la que se muestra dicha relación.

## **ACEPTABILIDAD DEL RIESGO**

Para determinar el valor de aceptabilidad del riesgo se considera la multiplicación entre la probabilidad por el parámetro de impacto ya relacionado, en la que se genera una matriz como se muestra en la Figura 2.5. Los resultados de este producto se ven correspondidos a un código de color tipo semáforo, donde se puede observar la gravedad del riesgo en la Tabla 2.9.

## **ALE**

Para un mejor análisis en conjunto con el tutor se ha tomado como referencia el libro (INFORMATION SECURITY), mismo que hace uso de una fórmula algebraica que multiplica la (expectativa de pérdida individual o SLE), por su expectativa de probabilidad de ocurrencia (ARO), anteriormente explicado en el apartado de la metodología capítulo 2 sobre el análisis del riesgo.

Es así que con la herramienta Excel de Microsoft se ha logrado simplificar los cálculos permitiendo valorar las vulnerabilidades que afecten tanto a la seguridad de los equipos informáticos como de la información, se a representado en cuadros donde se puede apreciar ya los resultados e identificar que equipo dar el tratamiento pertinente con mayor prioridad, como se puede apreciar en las siguientes tablas:

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ		PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I			
Servidor 1	R1	Flujo de lodos y escombros (lahares).	\$ 3.500,00	37%	100%	2	5	20	40%	\$ 1.283,33
	R2	Lluvia de ceniza y piroclastos.	\$ 3.500,00	63%	93%	4	5	20	80%	\$ 2.068,89
	R3	Sismos (volcánicos/repentinos).	\$ 3.500,00	83%	87%	5	5	20	100%	\$ 2.527,78
	R4	Interrupción del servicio de energía eléctrica.	\$ 3.500,00	47%	73%	3	4	10	30%	\$ 1.197,78
	R5	Filtración de agua.	\$ 3.500,00	97%	97%	5	5	20	100%	\$ 3.270,56
	R6	Incendio.	\$ 3.500,00	63%	97%	4	5	20	80%	\$ 2.142,78
	R7	Daño en el ventilador.	\$ 3.500,00	27%	43%	2	3	5	10%	\$ 404,44
	R8	Daño en fuente de poder.	\$ 3.500,00	33%	50%	2	3	5	10%	\$ 583,33
	R9	Falla de disco duro SATA/IDE.	\$ 3.500,00	33%	73%	2	4	10	20%	\$ 855,56
	R10	Falla de Tarjeta de Red.	\$ 3.500,00	17%	43%	1	3	5	5%	\$ 252,78
	R11	Fallas de Software/Configuración.	\$ 3.500,00	70%	93%	4	5	20	80%	\$ 2.286,67
	R12	Falla de cableado y conectores.	\$ 3.500,00	60%	47%	3	3	5	15%	\$ 980,00
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 3.500,00	30%	77%	2	4	10	20%	\$ 805,00
	R14	Ataques DoS o denegación de servicio.	\$ 3.500,00	33%	97%	2	5	20	40%	\$ 1.127,78
	R15	Falla de Hardware	\$ 3.500,00	57%	97%	3	5	20	60%	\$ 1.917,22
	R16	Error Humano (Falta de conocimiento).	\$ 3.500,00	23%	53%	2	3	5	10%	\$ 435,56
	R17	Robo de dispositivos.	\$ 3.500,00	20%	100%	1	5	20	20%	\$ 700,00
<b>\$22.839,44</b>										

Tabla 3.24: Análisis del riesgo sobre el (Servidor 1)

Fuente: Elaborado por el autor



EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Servidor 2	R1	Flujo de lodos y escombros (lahares).	\$ 5.000,00	37%	100%	2	5	20	40%	\$ 1.833,33	
	R2	Lluvia de ceniza y piroclastos.	\$ 5.000,00	63%	93%	4	5	20	80%	\$ 2.955,56	
	R3	Sismos (volcánicos/repentinos).	\$ 5.000,00	83%	87%	5	5	20	100%	\$ 3.611,11	
	R4	Interrupción del servicio de energía eléctrica.	\$ 5.000,00	47%	83%	3	5	20	60%	\$ 1.944,44	
	R5	Filtración de agua.	\$ 5.000,00	97%	97%	5	5	20	100%	\$ 4.672,22	
	R6	Incendio.	\$ 5.000,00	63%	97%	4	5	20	80%	\$ 3.061,11	
	R7	Daño en el ventilador.	\$ 5.000,00	43%	57%	3	3	5	15%	\$ 1.227,78	
	R8	Daño en fuente de poder.	\$ 5.000,00	33%	77%	2	4	10	20%	\$ 1.277,78	
	R9	Falla de disco duro SATA/IDE.	\$ 5.000,00	33%	100%	2	5	20	40%	\$ 1.666,67	
	R10	Falla de Tarjeta de Red.	\$ 5.000,00	17%	67%	1	4	10	10%	\$ 555,56	
	R11	Fallas de Software/Configuración.	\$ 5.000,00	70%	93%	4	5	20	80%	\$ 3.266,67	
	R12	Falla de cableado y conectores.	\$ 5.000,00	60%	57%	3	3	5	15%	\$ 1.700,00	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 5.000,00	30%	77%	2	4	10	20%	\$ 1.150,00	
	R14	Ataques DoS o denegación de servicio.	\$ 5.000,00	33%	97%	2	5	20	40%	\$ 1.611,11	
	R15	Software malicioso.	\$ 5.000,00	40%	100%	2	5	20	40%	\$ 2.000,00	
	R16	Error Humano (Falta de conocimiento).	\$ 5.000,00	23%	63%	2	4	10	20%	\$ 738,89	
	R17	Robo de dispositivos.	\$ 5.000,00	20%	100%	1	5	20	20%	\$ 1.000,00	
										\$ 34.272,22	

Tabla 3.25: Análisis del riesgo sobre el (Servidor 2)

Fuente: Elaborado por el autor

EQUIPO	Nº RIESGO	IDENTIFICACIÓN RIESGO	ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
			VA	ARO	FE	P	I				
Servidor 3	R1	Flujo de lodos y escombros (lahares).	\$ 3.500,00	37%	100%	2	5	20	40%	\$ 1.283,33	
	R2	Lluvia de ceniza y piroclastos.	\$ 3.500,00	63%	93%	4	5	20	80%	\$ 2.068,89	
	R3	Sismos (volcánicos/repentinos).	\$ 3.500,00	83%	87%	5	5	20	100%	\$ 2.527,78	
	R4	Interrupción del servicio de energía eléctrica.	\$ 3.500,00	47%	73%	3	4	10	30%	\$ 1.197,78	
	R5	Filtración de agua.	\$ 3.500,00	97%	97%	5	5	20	100%	\$ 3.270,56	
	R6	Incendio.	\$ 3.500,00	63%	97%	4	5	20	80%	\$ 2.142,78	
	R7	Daño en el ventilador.	\$ 3.500,00	27%	50%	2	3	5	10%	\$ 466,67	
	R8	Daño en fuente de poder.	\$ 3.500,00	33%	50%	2	3	5	10%	\$ 583,33	
	R9	Falla de disco duro SATA/IDE.	\$ 3.500,00	33%	80%	2	4	10	20%	\$ 933,33	
	R10	Falla de Tarjeta de Red.	\$ 3.500,00	17%	83%	1	5	20	20%	\$ 486,11	
	R11	Fallas de Software/Configuración.	\$ 3.500,00	70%	93%	4	5	20	80%	\$ 2.286,67	
	R12	Falla de cableado y conectores.	\$ 3.500,00	60%	47%	3	3	5	15%	\$ 980,00	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 3.500,00	30%	77%	2	4	10	20%	\$ 805,00	
	R14	Ataques DoS o denegación de servicio.	\$ 3.500,00	53%	97%	3	5	20	60%	\$ 1.804,44	
	R15	Software malicioso.	\$ 3.500,00	57%	97%	3	5	20	60%	\$ 1.917,22	
	R16	Error Humano (Falta de conocimiento).	\$ 3.500,00	23%	53%	2	3	5	10%	\$ 435,56	
	R17	Robo de dispositivos.	\$ 3.500,00	20%	100%	1	5	20	20%	\$ 700,00	
										\$ 23.889,44	

Tabla 3.26: Análisis del riesgo sobre el (Servidor 3)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Servidor 4	R1	Flujo de lodos y escombros (lahares).	\$ 2.500,00	37%	100%	2	5	20	40%	\$ 916,67	
	R2	Lluvia de ceniza y piroclastos.	\$ 2.500,00	63%	93%	4	5	20	80%	\$ 1.477,78	
	R3	Sismos (volcánicos/repentinos).	\$ 2.500,00	83%	87%	5	5	20	100%	\$ 1.805,56	
	R4	Interrupción del servicio de energía eléctrica.	\$ 2.500,00	47%	73%	3	4	10	30%	\$ 855,56	
	R5	Filtración de agua.	\$ 2.500,00	97%	97%	5	5	20	100%	\$ 2.336,11	
	R6	Incendio.	\$ 2.500,00	63%	97%	4	5	20	80%	\$ 1.530,56	
	R7	Daño en el ventilador.	\$ 2.500,00	27%	50%	2	3	5	10%	\$ 333,33	
	R8	Daño en fuente de poder.	\$ 2.500,00	33%	50%	2	3	5	10%	\$ 416,67	
	R9	Falla de disco duro SATA/IDE.	\$ 2.500,00	33%	80%	2	4	10	20%	\$ 666,67	
	R10	Falla de Tarjeta de Red.	\$ 2.500,00	17%	83%	1	5	20	20%	\$ 347,22	
	R11	Fallas de Software/Configuración.	\$ 2.500,00	57%	70%	3	4	10	30%	\$ 991,67	
	R12	Falla de cableado y conectores.	\$ 2.500,00	60%	47%	3	3	5	15%	\$ 700,00	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 2.500,00	50%	77%	3	4	10	30%	\$ 958,33	
	R14	Ataques DoS o denegación de servicio.	\$ 2.500,00	43%	97%	3	5	20	60%	\$ 1.047,22	
	R15	Falla de Hardware	\$ 2.500,00	57%	97%	3	5	20	60%	\$ 1.369,44	
	R16	Error Humano (Falta de conocimiento).	\$ 2.500,00	23%	53%	2	3	5	10%	\$ 311,11	
	R17	Robo de dispositivos.	\$ 2.500,00	20%	100%	1	5	20	20%	\$ 500,00	
<b>\$16.563,89</b>											

Tabla 3.27: Análisis del riesgo sobre el (Servidor 4)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Servidor 5	R1	Flujo de lodos y escombros (lahares).	\$ 2.500,00	37%	100%	2	5	20	40%	\$ 916,67	
	R2	Lluvia de ceniza y piroclastos.	\$ 2.500,00	63%	93%	4	5	20	80%	\$ 1.477,78	
	R3	Sismos (volcánicos/repentinos).	\$ 2.500,00	83%	87%	5	5	20	100%	\$ 1.805,56	
	R4	Interrupción del servicio de energía eléctrica.	\$ 2.500,00	47%	73%	3	4	10	30%	\$ 855,56	
	R5	Filtración de agua.	\$ 2.500,00	97%	97%	5	5	20	100%	\$ 2.336,11	
	R6	Incendio.	\$ 2.500,00	63%	97%	4	5	20	80%	\$ 1.530,56	
	R7	Daño en el ventilador.	\$ 2.500,00	27%	70%	2	4	10	20%	\$ 466,67	
	R8	Daño en fuente de poder.	\$ 2.500,00	33%	50%	2	3	5	10%	\$ 416,67	
	R9	Falla de disco duro SATA/IDE.	\$ 2.500,00	33%	80%	2	4	10	20%	\$ 666,67	
	R10	Falla de Tarjeta de Red.	\$ 2.500,00	17%	43%	1	3	5	5%	\$ 180,56	
	R11	Fallas de Software/Configuración.	\$ 2.500,00	70%	93%	4	5	20	80%	\$ 1.633,33	
	R12	Falla de cableado y conectores.	\$ 2.500,00	60%	47%	3	3	5	15%	\$ 700,00	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 2.500,00	53%	97%	3	5	20	60%	\$ 1.288,89	
	R14	Ataques DoS o denegación de servicio.	\$ 2.500,00	33%	97%	2	5	20	40%	\$ 805,56	
	R15	Falla de Hardware	\$ 2.500,00	57%	97%	3	5	20	60%	\$ 1.369,44	
	R16	Error Humano (Falta de conocimiento).	\$ 2.500,00	23%	53%	2	3	5	10%	\$ 311,11	
	R17	Robo de dispositivos.	\$ 2.500,00	20%	100%	1	5	20	20%	\$ 500,00	
<b>\$17.261,11</b>											

Tabla 3.28: Análisis del riesgo sobre el (Servidor 5)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Servidor 6	R1	Flujo de lodos y escombros (lahares).	\$ 4.500,00	37%	100%	2	5	20	40%	\$ 1.650,00	
	R2	Lluvia de ceniza y piroclastos.	\$ 4.500,00	63%	93%	4	5	20	80%	\$ 2.660,00	
	R3	Sismos (volcánicos/repentinos).	\$ 4.500,00	83%	87%	5	5	20	100%	\$ 3.250,00	
	R4	Interrupción del servicio de energía eléctrica.	\$ 4.500,00	47%	100%	3	5	20	60%	\$ 2.100,00	
	R5	Filtración de agua.	\$ 4.500,00	97%	97%	5	5	20	100%	\$ 4.205,00	
	R6	Incendio.	\$ 4.500,00	63%	97%	4	5	20	80%	\$ 2.755,00	
	R7	Daño en el ventilador.	\$ 4.500,00	50%	73%	3	4	10	30%	\$ 1.650,00	
	R8	Daño en fuente de poder.	\$ 4.500,00	57%	70%	3	4	10	30%	\$ 1.785,00	
	R9	Falla de disco duro SATA/IDE.	\$ 4.500,00	60%	100%	3	5	20	60%	\$ 2.700,00	
	R10	Falla de Tarjeta de Red.	\$ 4.500,00	33%	83%	2	5	20	40%	\$ 1.250,00	
	R11	Fallas de Software/Configuración.	\$ 4.500,00	70%	93%	4	5	20	80%	\$ 2.940,00	
	R12	Falla de cableado y conectores.	\$ 4.500,00	60%	47%	3	3	5	15%	\$ 1.260,00	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 4.500,00	57%	77%	3	4	10	30%	\$ 1.955,00	
	R14	Ataques DoS o denegación de servicio.	\$ 4.500,00	33%	97%	2	5	20	40%	\$ 1.450,00	
	R15	Falla de Hardware	\$ 4.500,00	57%	97%	3	5	20	60%	\$ 2.465,00	
	R16	Error Humano (Falta de conocimiento).	\$ 4.500,00	23%	87%	2	5	20	40%	\$ 910,00	
	R17	Robo de dispositivos.	\$ 4.500,00	20%	100%	1	5	20	20%	\$ 900,00	
<b>\$35.885,00</b>											

Tabla 3.29: Análisis del riesgo sobre el (Servidor 6)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Servidor 7	R1	Flujo de lodos y escombros (lahares).	\$ 3.500,00	37%	100%	2	5	20	40%	\$ 1.283,33	
	R2	Lluvia de ceniza y piroclastos.	\$ 3.500,00	63%	93%	4	5	20	80%	\$ 2.068,89	
	R3	Sismos (volcánicos/repentinos).	\$ 3.500,00	83%	87%	5	5	20	100%	\$ 2.527,78	
	R4	Interrupción del servicio de energía eléctrica.	\$ 3.500,00	47%	83%	3	5	20	60%	\$ 1.361,11	
	R5	Filtración de agua.	\$ 3.500,00	97%	97%	5	5	20	100%	\$ 3.270,56	
	R6	Incendio.	\$ 3.500,00	63%	97%	4	5	20	80%	\$ 2.142,78	
	R7	Daño en el ventilador.	\$ 3.500,00	50%	77%	3	4	10	30%	\$ 1.341,67	
	R8	Daño en fuente de poder.	\$ 3.500,00	57%	73%	3	4	10	30%	\$ 1.454,44	
	R9	Falla de disco duro SATA/IDE.	\$ 3.500,00	33%	97%	2	5	20	40%	\$ 1.127,78	
	R10	Falla de Tarjeta de Red.	\$ 3.500,00	17%	83%	1	5	20	20%	\$ 486,11	
	R11	Fallas de Software/Configuración.	\$ 3.500,00	70%	93%	4	5	20	80%	\$ 2.286,67	
	R12	Falla de cableado y conectores.	\$ 3.500,00	60%	47%	3	3	5	15%	\$ 980,00	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 3.500,00	30%	77%	2	4	10	20%	\$ 805,00	
	R14	Ataques DoS o denegación de servicio.	\$ 3.500,00	33%	97%	2	5	20	40%	\$ 1.127,78	
	R15	Falla de Hardware	\$ 3.500,00	57%	97%	3	5	20	60%	\$ 1.917,22	
	R16	Error Humano (Falta de conocimiento).	\$ 3.500,00	23%	83%	2	5	20	40%	\$ 680,56	
	R17	Robo de dispositivos.	\$ 3.500,00	20%	100%	1	5	20	20%	\$ 700,00	
										\$25.561,67	

Tabla 3.30: Análisis del riesgo sobre el (Servidor 7)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS				UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I					
PCs del departamento de Tecnologías de la Información	R1	Flujo de lodos y escombros (lahares).	\$ 3.600,00	37%	100%	2	5	20	40%	\$ 1.320,00		
	R2	Lluvia de ceniza y piroclastos.	\$ 3.600,00	63%	93%	4	5	20	80%	\$ 2.128,00		
	R3	Sismos (volcánicos/repentinos).	\$ 3.600,00	83%	87%	5	5	20	100%	\$ 2.600,00		
	R4	Interrupción del servicio de energía eléctrica.	\$ 3.600,00	47%	60%	3	3	5	15%	\$ 1.008,00		
	R5	Filtración de agua.	\$ 3.600,00	97%	97%	5	5	20	100%	\$ 3.364,00		
	R6	Incendio.	\$ 3.600,00	63%	97%	4	5	20	80%	\$ 2.204,00		
	R7	Daño en el ventilador.	\$ 3.600,00	27%	57%	2	3	5	10%	\$ 544,00		
	R8	Daño en fuente de poder.	\$ 3.600,00	27%	47%	2	3	5	10%	\$ 448,00		
	R9	Falla de disco duro SATA/IDE.	\$ 3.600,00	33%	97%	2	5	20	40%	\$ 1.160,00		
	R10	Falla de Tarjeta de Red.	\$ 3.600,00	23%	57%	2	3	5	10%	\$ 476,00		
	R11	Fallas de Software/Configuración.	\$ 3.600,00	40%	90%	2	5	20	40%	\$ 1.296,00		
	R12	Falla de cableado y conectores.	\$ 3.600,00	33%	43%	2	3	5	10%	\$ 520,00		
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 3.600,00	30%	70%	2	4	10	20%	\$ 756,00		
	R14	Ataques DoS o denegación de servicio.	\$ 3.600,00	33%	90%	2	5	20	40%	\$ 1.080,00		
	R15	Falla de Hardware	\$ 3.600,00	43%	87%	3	5	20	60%	\$ 1.352,00		
	R16	Error Humano (Falta de conocimiento).	\$ 3.600,00	23%	77%	2	4	10	20%	\$ 644,00		
	R17	Robo de dispositivos.	\$ 3.600,00	20%	100%	1	5	20	20%	\$ 720,00		
<b>\$21.620,00</b>												

Tabla 3.31: Análisis del riesgo sobre las (PCs del departamento de TI)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Impresoras del departamento de Tecnologías de la Información	R1	Flujo de lodos y escombros (lahares)	\$ 680,00	37%	100%	2	5	20	40%	\$ 249,33	
	R2	Lluvia de ceniza y piroclastos	\$ 680,00	63%	93%	4	5	20	80%	\$ 401,96	
	R3	Sismos (volcánicos/repentinos)	\$ 680,00	83%	87%	5	5	20	100%	\$ 491,11	
	R4	Interrupción del servicio de energía eléctrica	\$ 680,00	47%	73%	3	4	10	30%	\$ 232,71	
	R5	Filtración de agua	\$ 680,00	97%	97%	5	5	20	100%	\$ 635,42	
	R6	Incendio	\$ 680,00	63%	97%	4	5	20	80%	\$ 416,31	
	R11	Fallas de Software/Configuración	\$ 680,00	60%	43%	3	3	5	15%	\$ 176,80	
	R12	Falla de cableado y conectores	\$ 680,00	60%	47%	3	3	5	15%	\$ 190,40	
	R15	Falla de Hardware	\$ 680,00	67%	87%	4	5	20	80%	\$ 392,89	
	R16	Error Humano (Falta de conocimiento)	\$ 680,00	43%	33%	3	2	2	6%	\$ 98,22	
	R17	Robo de dispositivos	\$ 680,00	23%	73%	2	4	10	20%	\$ 116,36	
	R18	Atasco de papel en la impresora	\$ 680,00	63%	77%	4	4	10	40%	\$ 330,18	
	R19	El dispositivo no reconoce la impresora.	\$ 680,00	73%	53%	4	3	5	20%	\$ 265,96	
											\$ 3.997,64

Tabla 3.32: Análisis del riesgo sobre las (Impresoras del departamento de TI)

Fuente: Elaborado por el autor



EQUIPO	IDENTIFICACIÓN		ANÁLISIS				UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I					
Tripp Lite Rack Console IURM	R1	Flujo de lodos y escombros (lahares).	\$ 790,00	37%	100%	2	5	20	\$ 289,67			
	R2	Lluvia de ceniza y piroclastos.	\$ 790,00	63%	93%	4	5	20	\$ 466,98			
	R3	Sismos (volcánicos/repentinos).	\$ 790,00	83%	87%	5	5	20	\$ 570,56			
	R4	Interrupción del servicio de energía eléctrica.	\$ 790,00	47%	63%	3	4	10	\$ 233,49			
	R5	Filtración de agua.	\$ 790,00	97%	97%	5	5	20	\$ 738,21			
	R6	Incendio.	\$ 790,00	63%	90%	4	5	20	\$ 450,30			
	R7	Daño en el ventilador.	\$ 790,00	27%	57%	2	3	5	\$ 119,38			
	R8	Daño en fuente de poder.	\$ 790,00	27%	47%	2	3	5	\$ 98,31			
	R9	Falla de disco duro SATA/IDE.	\$ 790,00	27%	63%	2	4	10	\$ 133,42			
	R10	Falla de Tarjeta de Red.	\$ 790,00	23%	37%	2	2	2	\$ 67,59			
	R11	Fallas de Software/Configuración.	\$ 790,00	27%	33%	2	2	2	\$ 70,22			
	R12	Falla de cableado y conectores.	\$ 790,00	27%	37%	2	2	2	\$ 77,24			
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 790,00	20%	43%	1	3	5	\$ 68,47			
	R14	Ataques DoS o denegación de servicio.	\$ 790,00	33%	67%	2	4	10	\$ 175,56			
	R15	Falla de Hardware	\$ 790,00	27%	60%	2	3	5	\$ 126,40			
	R16	Error Humano (Falta de conocimiento).	\$ 790,00	20%	53%	1	3	5	\$ 84,27			
	R17	Robo de dispositivos.	\$ 790,00	20%	43%	1	3	5	\$ 68,47			
<b>\$ 3.838,52</b>												

Tabla 3.33: Análisis del riesgo sobre el (Tripp Lite Rack Cpnsole IURM)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Cisco Router	R1	Flujo de lodos y escombros (lahares).	\$ 600,00	37%	100%	2	5	20	40%	\$ 220,00	
	R2	Lluvia de ceniza y piroclastos.	\$ 600,00	63%	93%	4	5	20	80%	\$ 354,67	
	R3	Sismos (volcánicos/repentinos).	\$ 600,00	83%	87%	5	5	20	100%	\$ 433,33	
	R4	Interrupción del servicio de energía eléctrica.	\$ 600,00	47%	73%	3	4	10	30%	\$ 205,33	
	R5	Filtración de agua.	\$ 600,00	97%	97%	5	5	20	100%	\$ 560,67	
	R6	Incendio.	\$ 600,00	63%	90%	4	5	20	80%	\$ 342,00	
	R11	Fallas de Software/Configuración.	\$ 600,00	57%	77%	3	4	10	30%	\$ 260,67	
	R12	Falla de cableado y conectores.	\$ 600,00	53%	47%	3	3	5	15%	\$ 149,33	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 600,00	27%	67%	2	4	10	20%	\$ 106,67	
	R14	Ataques DoS o denegación de servicio.	\$ 600,00	43%	73%	3	4	10	30%	\$ 190,67	
	R15	Falla de Hardware	\$ 600,00	27%	83%	2	5	20	40%	\$ 133,33	
	R16	Error Humano (Falta de conocimiento).	\$ 600,00	23%	47%	2	3	5	10%	\$ 65,33	
	R17	Robo de dispositivos.	\$ 600,00	20%	43%	1	3	5	5%	\$ 52,00	
											\$ 3.074,00

Tabla 3.34: Análisis del riesgo sobre el (Cisco Router)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Switches	R1	Flujo de lodos y escombros (lahares).	\$ 600,00	43%	100%	3	5	20	60%	\$ 260,00	
	R2	Lluvia de ceniza y piroclastos.	\$ 600,00	53%	93%	3	5	20	60%	\$ 298,67	
	R3	Sismos (volcánicos/repentinos).	\$ 600,00	87%	90%	5	5	20	100%	\$ 468,00	
	R4	Interrupción del servicio de energía eléctrica.	\$ 600,00	57%	73%	3	4	10	30%	\$ 249,33	
	R5	Filtración de agua.	\$ 600,00	90%	87%	5	5	20	100%	\$ 468,00	
	R6	Incendio.	\$ 600,00	63%	70%	4	4	10	40%	\$ 266,00	
	R11	Fallas de Software/Configuración.	\$ 600,00	33%	47%	2	3	5	10%	\$ 93,33	
	R12	Falla de cableado y conectores.	\$ 600,00	33%	47%	2	3	5	10%	\$ 93,33	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 600,00	37%	47%	2	3	5	10%	\$ 102,67	
	R14	Ataques DoS o denegación de servicio.	\$ 600,00	40%	33%	2	2	2	4%	\$ 80,00	
	R15	Falla de Hardware	\$ 600,00	37%	73%	2	4	10	20%	\$ 161,33	
	R16	Error Humano (Falta de conocimiento).	\$ 600,00	23%	40%	2	2	2	4%	\$ 56,00	
	R17	Robo de dispositivos.	\$ 600,00	23%	33%	2	2	2	4%	\$ 46,67	
											\$ 2.643,33

Tabla 3.35: Análisis del riesgo sobre (Switches)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Red de datos	R1	Flujo de lodos y escombros (lahares).	\$ 600,00	50%	100%	3	5	20	60%	\$ 300,00	
	R2	Lluvia de ceniza y piroclastos.	\$ 600,00	60%	93%	3	5	20	60%	\$ 336,00	
	R3	Sismos (volcánicos/repentinos).	\$ 600,00	77%	90%	4	5	20	80%	\$ 414,00	
	R4	Interrupción del servicio de energía eléctrica.	\$ 600,00	73%	77%	4	4	10	40%	\$ 337,33	
	R5	Filtración de agua.	\$ 600,00	90%	80%	5	4	10	50%	\$ 432,00	
	R6	Incendio.	\$ 600,00	73%	83%	4	5	20	80%	\$ 366,67	
	R11	Fallas de Software/Configuración.	\$ 600,00	47%	47%	3	3	5	15%	\$ 130,67	
	R12	Falla de cableado y conectores.	\$ 600,00	47%	47%	3	3	5	15%	\$ 130,67	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 600,00	47%	40%	3	2	2	6%	\$ 112,00	
	R14	Ataques DoS o denegación de servicio.	\$ 600,00	53%	40%	3	2	2	6%	\$ 128,00	
	R15	Falla de Hardware	\$ 600,00	43%	73%	3	4	10	30%	\$ 190,67	
	R16	Error Humano (Falta de conocimiento).	\$ 600,00	40%	40%	2	2	2	4%	\$ 96,00	
	R17	Robo de dispositivos.	\$ 600,00	37%	37%	2	2	2	4%	\$ 80,67	
	R20	Presencia de interferencias electromagnéticas.	\$ 600,00	33%	37%	2	2	2	4%	\$ 73,33	
	<b>\$ 3.054,67</b>										

Tabla 3.36: Análisis del riesgo sobre (Switches)

Fuente: Elaborado por el autor

EQUIPO	IDENTIFICACIÓN		ANÁLISIS			UBICACIÓN EN LA MATRIZ			PARÁMETRO IMPACTO	ACEPTABILIDAD DEL RIESGO	ALE
	Nº RIESGO	RIESGO	VA	ARO	FE	P	I				
Información	R11	Fallas de Software/Configuración.	\$ 1.000,00	60%	97%	3	5	20	60%	\$ 580,00	
	R13	Acceso no autorizado (Robo o alteración de información).	\$ 1.000,00	60%	100%	3	5	20	60%	\$ 600,00	
	R14	Ataques DoS o denegación de servicio.	\$ 1.000,00	60%	93%	3	5	20	60%	\$ 560,00	
	R15	Falla de Hardware	\$ 1.000,00	43%	73%	3	4	10	30%	\$ 317,78	
	R16	Error Humano (Falta de conocimiento).	\$ 1.000,00	67%	47%	4	3	5	20%	\$ 311,11	
	R21	Ingeniería social.	\$ 1.000,00	30%	53%	2	3	5	10%	\$ 160,00	
											\$ 2.368,89

Tabla 3.37: Análisis del riesgo sobre (Switches)

Fuente: Elaborado por el autor

## NIVELES DE ACEPTABILIDAD

Los niveles de aceptabilidad están basados en los resultados sobre la evaluación de la probabilidad de ocurrencia y el impacto, ubicando los riesgos sobre la matriz de calificación de riesgos operativos en la que podemos observar su calificación a partir del cruce entre estas dos variables sobre la matriz de 5x5. En esta parte podemos observar el comportamiento de los riesgos los cuales se encuentran asociados a un código de color tipo semáforo, donde se puede observar la gravedad del riesgo al que está expuesto el activo como se muestra a continuación:

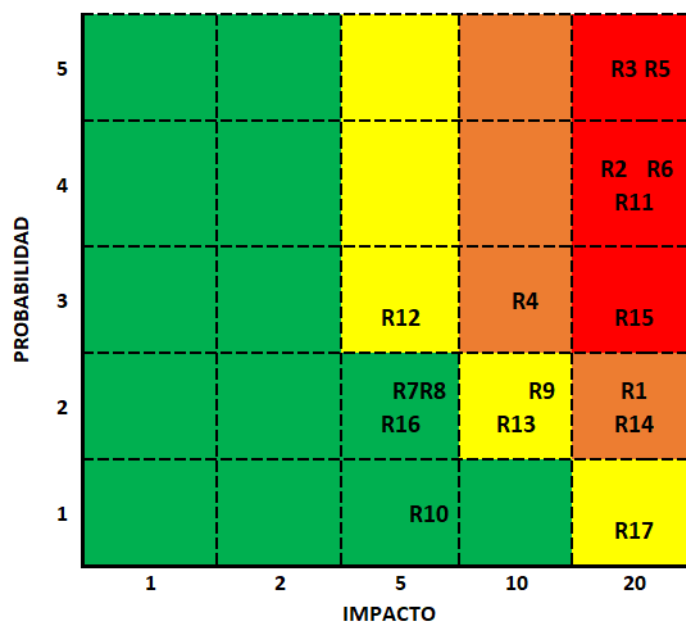


Figura 3.18: Matriz de calificación de riesgos operativos (Servidor 1)  
Fuente: Elaborado por el autor

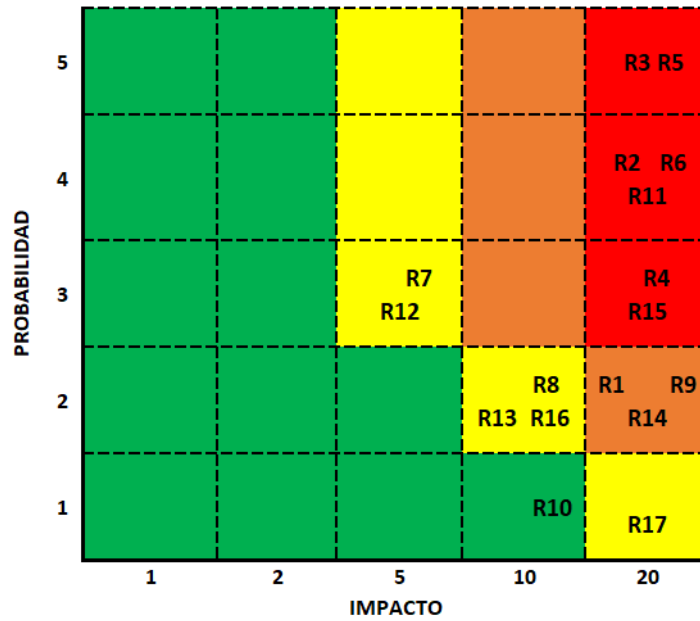


Figura 3.19: Matriz de calificación de riesgos operativos (Servidor 2)  
Fuente: Elaborado por el autor

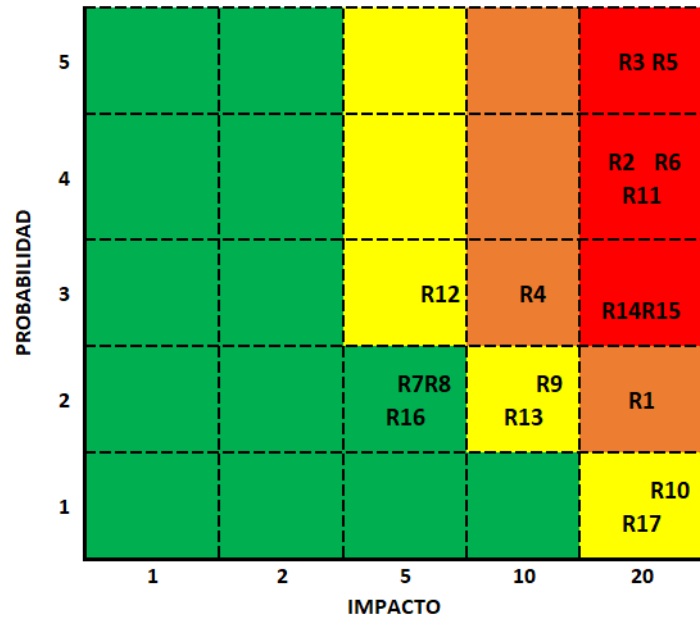


Figura 3.20: Matriz de calificación de riesgos operativos (Servidor 3)  
Fuente: Elaborado por el autor

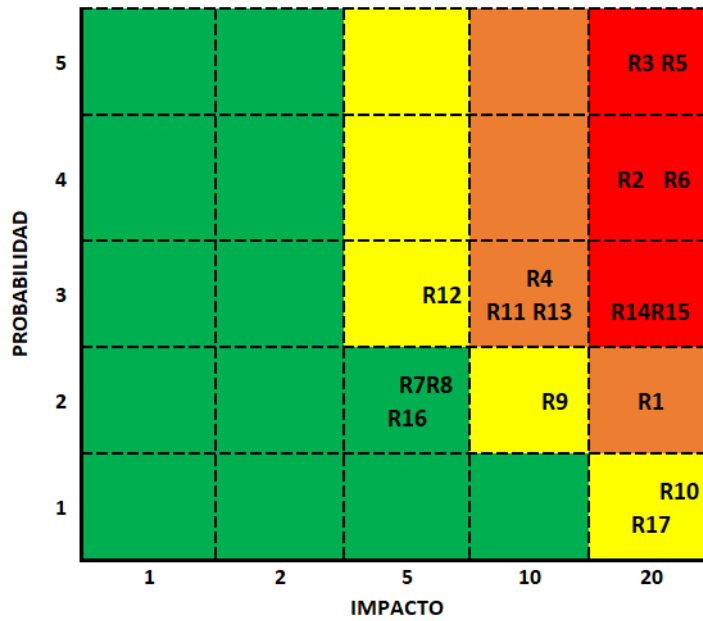


Figura 3.21: Matriz de calificación de riesgos operativos (Servidor 4)  
Fuente: Elaborado por el autor

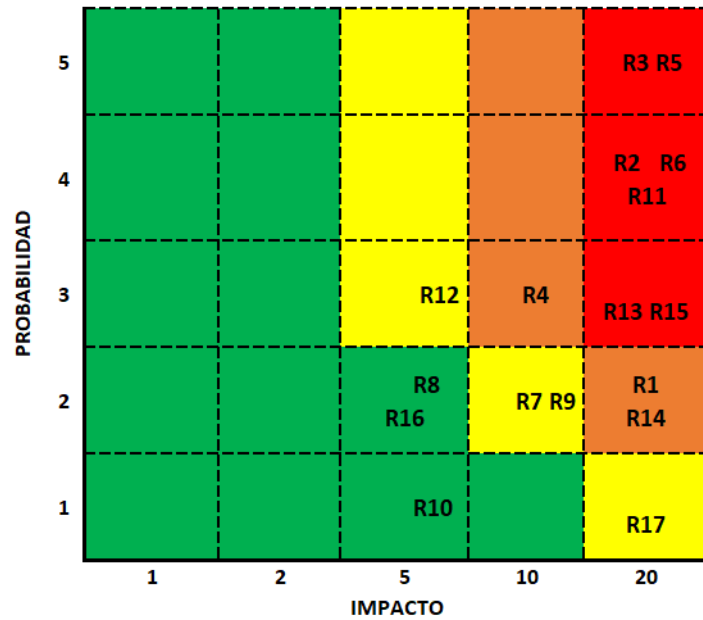


Figura 3.22: Matriz de calificación de riesgos operativos (Servidor 5)  
Fuente: Elaborado por el autor



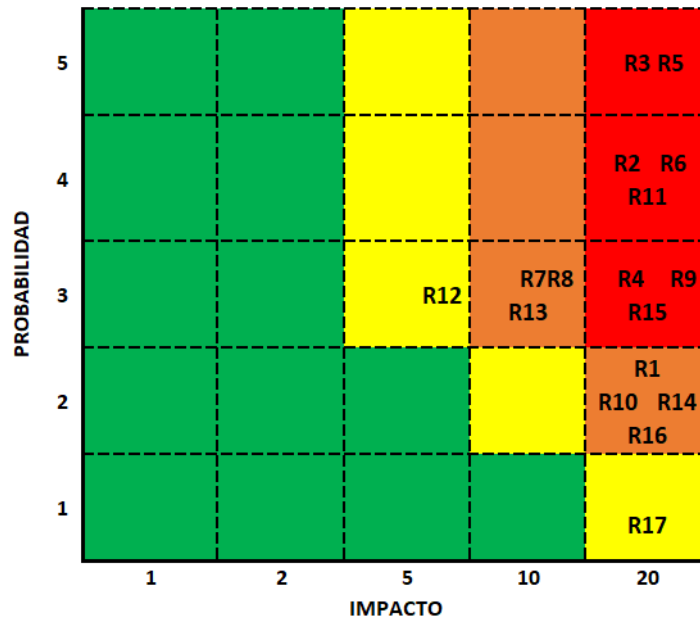


Figura 3.23: Matriz de calificación de riesgos operativos (Servidor 6)  
Fuente: Elaborado por el autor

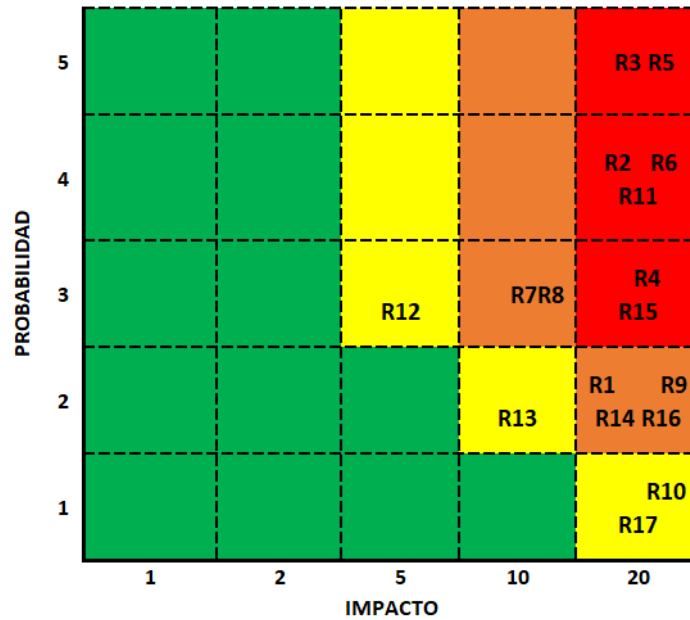


Figura 3.24: Matriz de calificación de riesgos operativos (Servidor 7)  
Fuente: Elaborado por el autor

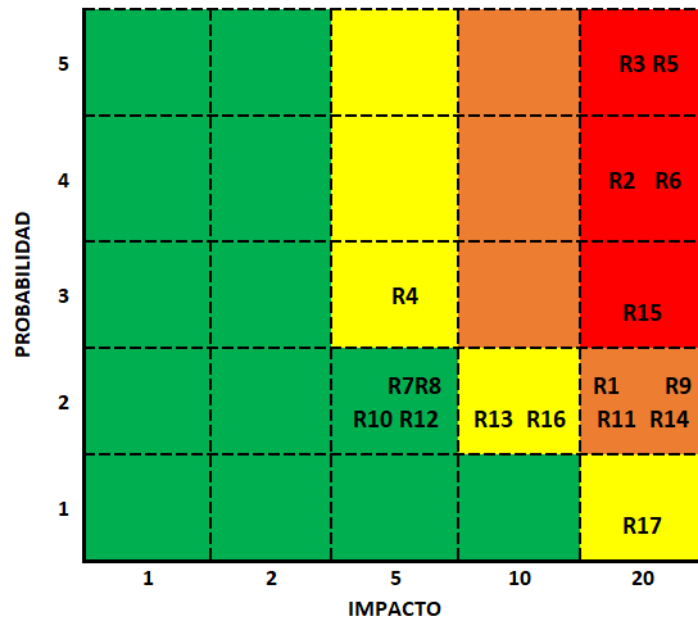


Figura 3.25: Matriz de calificación de riesgos operativos (PCs TI)  
Fuente: Elaborado por el autor

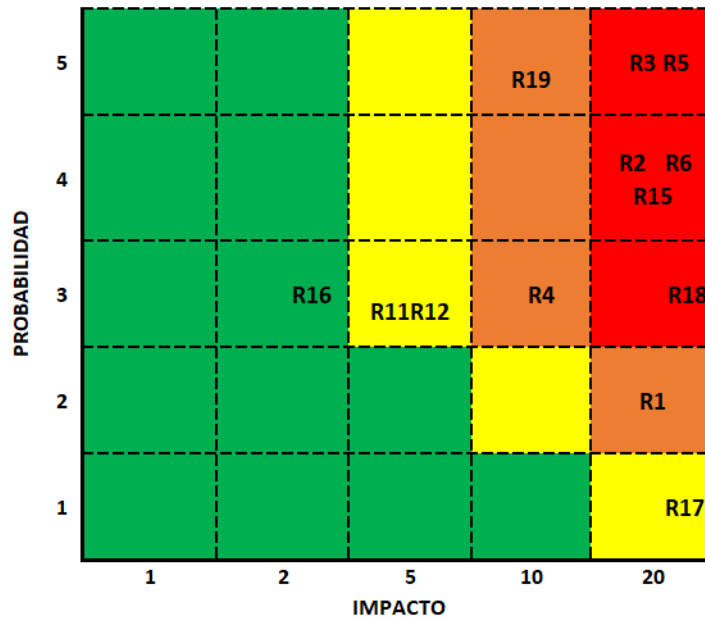


Figura 3.26: Matriz de calificación de riesgos operativos (Impresoras TI)  
Fuente: Elaborado por el autor

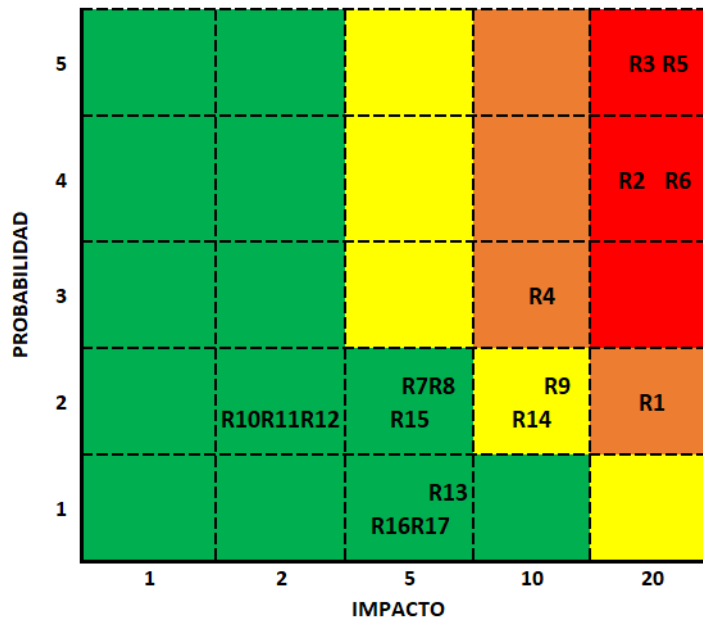


Figura 3.27: Matriz de calificación de riesgos operativos (Tripp Lite Rack Console)

Fuente: Elaborado por el autor

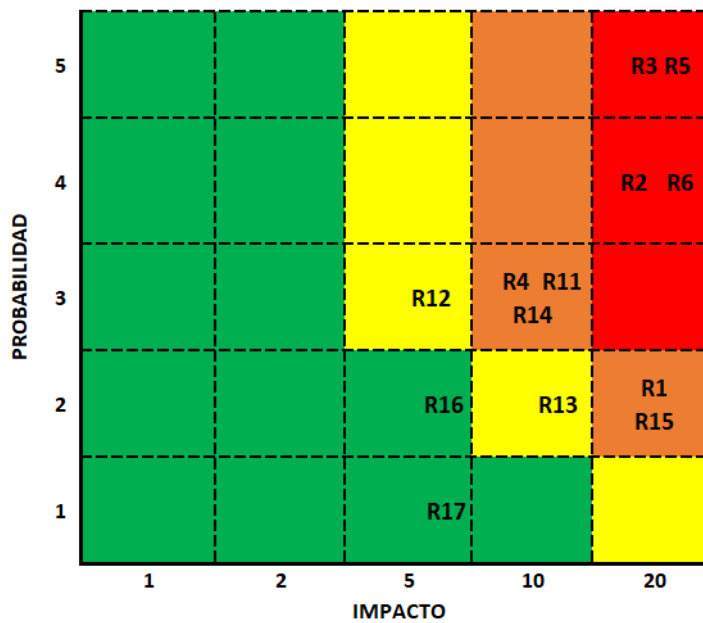


Figura 3.28: Matriz de calificación de riesgos operativos (Cisco Router)

Fuente: Elaborado por el autor

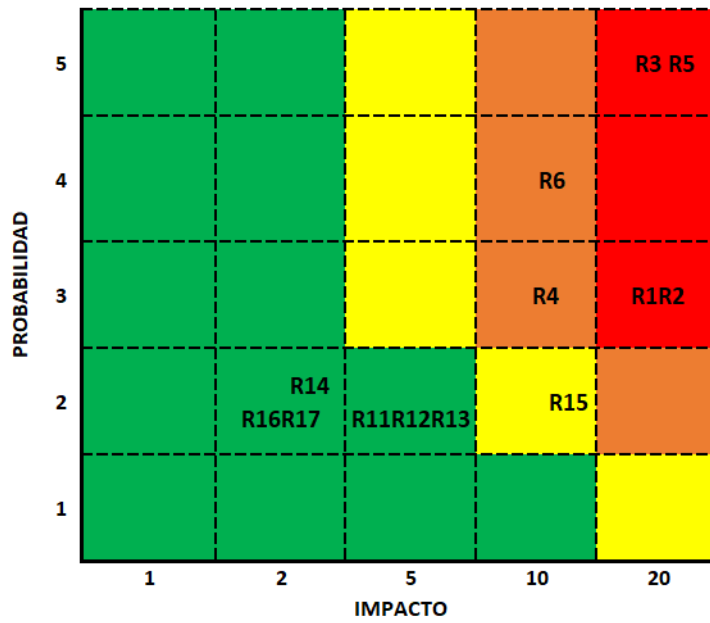


Figura 3.29: Matriz de calificación de riesgos operativos (Switches)  
Fuente: Elaborado por el autor

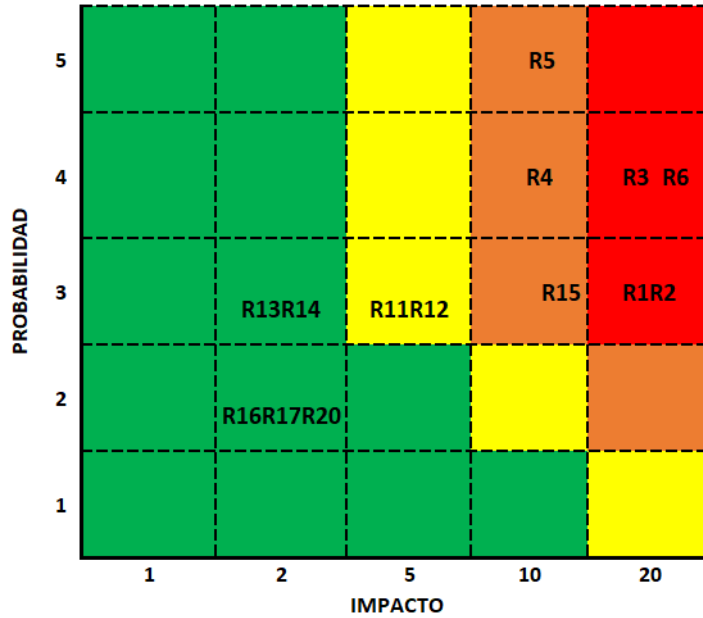


Figura 3.30: Matriz de calificación de riesgos operativos (Red de datos)  
Fuente: Elaborado por el autor

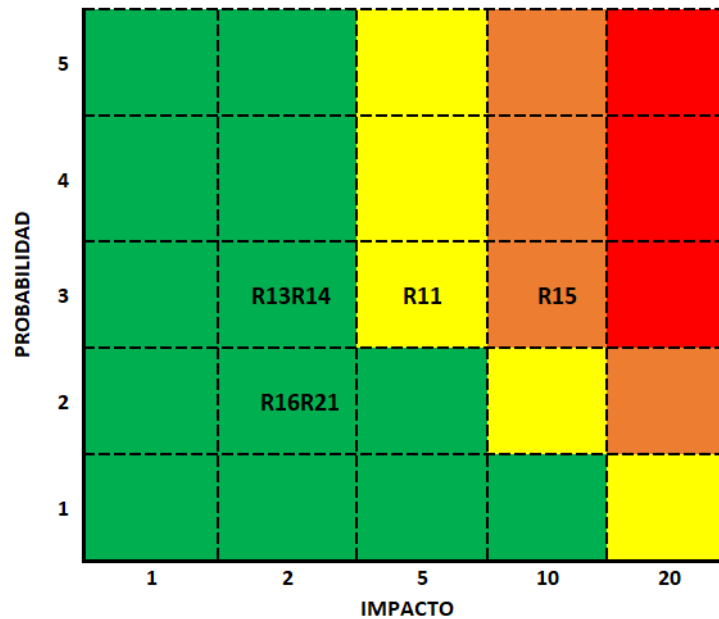


Figura 3.31: Matriz de calificación de riesgos operativos (Información)  
Fuente: Elaborado por el autor

### 3.1.3.3. Evaluación del riesgo

Esta etapa corresponde principalmente a confrontar los resultados del análisis considerando los puntos de control de seguridad realizados previamente, brindando así un tratamiento adecuado y la prioridad del caso para su posterior implementación por el personal encargado y las autoridades pertinentes. Es necesario llevar la etapa del contexto actualizada de manera periódica, cada año según lo recomienda la metodología.

#### Identificación de controles

Los controles corresponden a las acciones sobre el tratamiento que permiten contrarrestar el riesgo actuando sobre alguna de las dos variables de su evaluación (probabilidad o impacto), ya sea para identificarlo a tiempo (impedir que se materialice) o reducirlo (minimizar las consecuencias).

- **Controles de probabilidad:**

Es importante comprender que en esta parte el principal objetivo es evitar que el riesgo se materialice, para lograrlo es necesario enfocarse en atacar las causas descubiertas en la etapa de identificación del riesgo.

- **Controles de impacto:**

Se centra en el activo amenazado, para de esta manera reducir las consecuencias o efectos en caso de materializarse el riesgo.

Considerando la importancia sobre la identificación de los controles y para evitar redundancia, las actividades a realizarse en este paso estarán incluidas en el Plan de Contingencia Informático de la Municipalidad de cantón Salcedo.

### **Valoración de los controles**

Como se explicó anteriormente en el apartado de la metodología, el proceso de valoración de los controles queda a cargo de las autoridades y de quienes conforman el departamento de TI de la institución. Dado a que estos resultados serán identificados ya en la práctica y al transcurrir el tiempo se visualizará la eficiencia del control misma que será expuesta a una calificación donde se tendrá rangos de eficiencia como se plantea en la Tabla 2.12, acorde a la discusión de la probabilidad o del impacto.

### **Planificación**

En la actualidad es importante contar con un Plan de Contingencia Informático actualizado, ya que se lo considera como una herramienta valiosa la misma que esta basada en un análisis de riesgo donde se cuente con un conjunto de procedimientos alternativos que brinden apoyo al funcionamiento normal de cada institución ya sean publicas o privadas.

### **Capacidades de las estructuras territoriales de los G.A.D. para la respuesta ante un desastre**

Las capacidades de los G.A.D. cantonales de la provincia de Cotopaxi son limitadas en términos de personal y equipamiento; No todos los municipios tienen unidades de GR. La demanda de la población excede las capacidades de las estructuras de los G.A.D. y requiere el apoyo de los cantones o provincias vecinas. La funcionalidad de las estructuras municipales puede verse limitada debido a las afectaciones de sus empleados.[48]



### **3.2. Plan de contingencia informático**

El Plan de Contingencia Informático es un instrumento orientado a gestionar las medidas de seguridad ante los posibles riesgos a los cuales puede estar expuesto el departamento de TI de la municipalidad y sus recursos informáticos. Este manual aplica medidas de seguridad para precautelar y proteger ante una contingencia o desastre de cualquier magnitud y afrontar este tipo de evento inesperado de manera oportuna garantizando la continuidad del servicio que presta a la ciudadanía del cantón Salcedo. Al tener siempre la posibilidad de que se materialice un determinado riesgo, pese a las medidas de seguridad, es importante considerar que el plan de contingencia incluya las actividades durante y después de materializarse un determinado desastre para así restaurar el normal funcionamiento de la institución de manera rápida y eficiente.

En cuanto a costos de recuperación en caso de ocurrir desastre severos, como por ejemplo los de un terremoto de gran magnitud que destruya completamente el interior de la infraestructura de la municipalidad y sus instalaciones, estará directamente relacionado con el valor de los equipos informáticos como son servidores, computadoras, impresoras, equipos de red, información, entre los más destacados, dado a la importancia del tema en el presente proyecto se ha hecho un análisis de costos que servirían como base para oportunamente actualizar la información en relación a los equipos informáticos asegurados que obra en poder de la institución de seguros que cuenta el G.A.D. Municipal del cantón Salcedo.

El plan de restablecimiento de las actividades para retomar nuevamente el control del funcionamiento normal de la institución será abordado en la etapa de las actividades posteriores al desastre. Como primera parte en el desarrollo del plan contra desastres, se enfoca en la identificación de los principales integrantes o personas que estarán al frente de coordinar la emergencia y activar el plan de contingencia ante un evento adverso institucional. Estas personas estarán conformadas por el presidente del Comité de Operaciones de Emergencia (COE) del cantón Salcedo, junto con el director de seguridad ciudadana de gestión de riesgos, integrantes del departamento de TI de la institución también se contará con el respaldo de actores institucionales operativos del G.A.D. Salcedo que apoyan al bienestar del cantón.

### 3.2.1. Contenidos

	<b>GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SALCEDO</b>	
<b>PLAN DE CONTINGENCIA INFORMÁTICO PARA EL DEPARTAMENTO DE TI</b>		
<b>3.2.1 CONTENIDO.</b>		
<b>3.2.2 OBJETIVO.</b>		
<b>3.2.3 ALCANCE.</b>		
<b>3.2.4 DEFINICIONES.</b>		
<b>3.2.5 COMITÉ DE ROLES.</b>		
<b>3.2.6 CLASES DE RIESGOS QUE AMENAZAN A LA INSTITUCIÓN.</b>		
<b>3.2.7 ACTIVIDADES GENERALES PREVIAS AL DESASTRE.</b>		
<b>3.2.8 ACTIVIDADES GENERALES DURANTE EL DESASTRE.</b>		
<b>3.2.9 ACTIVIDADES GENERALES DESPÚES DEL DESASTRE.</b>		
<b>3.2.10 ACCIONES ESPECÍFICAS FRENTE A LOS TIPOS DE RIESGO (ANTES, DURANTE Y DESPUÉS).</b>		

### 3.2.2. Objetivo

Disponer de un plan de contingencia informático, y dar la continuidad a las actividades en la municipalidad, mediante información de primera mano ante cualquier situación adversa que afecte al departamento de TI.

### 3.2.3. Alcance

Este plan de recuperación y respaldo de la información será abordado previo al desarrollo de la investigación en el que se detallan los procesos de recuperación en beneficio de la institución si llegara a materializarse algún tipo de desastre en el área de TI. Ante la existencia de un posible desastre, es necesario contar con un Plan de Contingencia Informático que indique las acciones que deben tomarse antes, durante y después de un desastre. El proyecto se limitará al desarrollo de la fase de pruebas y validación del Plan de Contingencia, no será implementado, por consiguiente, queda a cargo de las autoridades y del Departamento de TI.



### 3.2.4. Definiciones

**Sistema de información (SI):** Se refiere a un grupo de recursos entre los cuales se encuentran: recursos humanos, recursos informáticos, actividades, datos, con el objetivo de administrar estos datos y generar información útil para los distintos procesos en una institución.[49]

**Plan de contingencia:** Es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garantizan la continuidad del servicio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto.[8]

**Integridad:** Cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.[11]

**Confidencialidad:** Hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada.[12]

**Disponibilidad:** Recursos los cuales deben estar disponibles cuando sean requeridos en cualquier instante de tiempo.[13]

**Riego:** Hace relación a cualquier evento en la que se puedan presentar resultados no planificados, se consideran cómo aquellas circunstancias que afectan de manera negativa a la institución.[36]

**Activo:** Componente de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización”.[15]

**Amenaza:** Fenómeno que tiene el potencial de afectar negativamente a los seres humanos.[16]

**Vulnerabilidad:** Grado de exposición que se encuentra una organización, fallos de los sistemas de seguridad o en los propios que el usuario utiliza para desarrollar las actividades que genera un problema.[17]

**Ataque:** Aquellas acciones deliberadas por actores internos o externos que afectan un sistema informático, redes de datos alámbricas o inalámbricas, estos ataques pueden ser propiciados por una o más personas para causar un perjuicio hacia las infraestructuras tecnológicas.[18]

**Impacto** Puede ser expresado por las consecuencias o daños que afectan a un activo, atendado contra la integridad o la pérdida de disponibilidad de un negocio.[19]

**Servidor:** Es un ordenador de gran potencia que se encarga de (prestar el servicio) de transmitir la información pedida por sus clientes a otros ordenadores, dispositivos móviles, impresoras, personas, etc.[50]

### 3.2.5. Comité de roles

#### Principales integrantes del Plan de Contingencia ante un evento adverso institucional

	ACCIONES OPERATIVAS DEL RESPONSABLE/ DETALLE	DATOS
ALCALDE DEL CANTÓN SALCEDO	ACTIVACIÓN DE LA EMERGENCIA	<b>MSc. Willan Polivio Naranjo Torres</b>
	OPERACIONES	0998763870
	LOGÍSTICA	032700420 ext. 101
	COMUNICACIÓN	
	RESPUESTA	willan.naranjo@salcedo.gob.ec
	EVALUACIÓN	wilycolon3@hotmail.com
DIRECTOR DE SEGURIDAD CIUDADANA Y GESTIÓN DE RIESGOS	ACTIVACIÓN DE LA EMERGENCIA	<b>Ing. Santiago Vásquez Esquivel</b>
	OPERACIONES	0958710222
	LOGÍSTICA	032700420 ext. 127
	COMUNICACIÓN	
	RESPUESTA	santiago.vasquez@salcedo.gob.ec
	EVALUACIÓN	austinsan@outlook.com

Tabla 3.38: Principales integrantes del Plan de Contingencia institucional

Fuente: Elaborado por el autor

ROLES	DATOS	ACCIONES OPERATIVAS	PRINCIPALES RESPONSABILIDADES / DETALLE
JEFE DEL DEPARTAMENTO DE TI	Ing. Enrique Arcos 0987872441  enrique.arcos@salcedo.gob.ec	COORDINADOR DE LA EMERGENCIA	Coordinar con los directivos y jefes de cada uno de los departamentos las operaciones, así mismo las garantías de equipos informáticos, ante una emergencia.
		OPERACIONES	Aprobar y desarrollar sistemas y aplicaciones necesarias para la institución garantizando su funcionalidad.
		LOGÍSTICA	
		COMUNICACIÓN	
		RESPUESTA	Crear respaldos de las bases de datos, sistemas y aplicaciones creadas, delegar y supervisar el proceso de Backups.
		EVALUACIÓN	Coordinar la prioridad y rescate de los equipos informáticos en una emergencia.
ANALISTA DE SISTEMAS	Ing. Paulina Villalba 0984555067  paulina.villalba@salcedo.gob.ec	APOYO ANTE LA EMERGENCIA	Supervisar y aprobar el trabajo realizado por el analista y el técnico de TI.
		OPERACIONES	Administrar los sistemas y aplicaciones, así mismo los equipos informáticos de la institución, garantizando su correcto funcionamiento.
		LOGÍSTICA	Proponer el desarrollo e instalación de nuevo software necesarios en la institución.
		COMUNICACIÓN	Monitorear el estado de la red, así como verificar el Firewall, ante posibles ataques.
		RESPUESTA	Colaborar con el proceso Backups así como recuperar, restaurar y verificar el funcionamiento de los respaldos del sitio externo alojado.
		EVALUACIÓN	Comunicación con el proveedor externo de aplicaciones y sistemas como es AME.
TÉCNICO DE SISTEMAS	Tec. Juan Córdoba 0983561124  juan.cordoba@salcedo.gob.ec	APOYO ANTE LA EMERGENCIA	Garantizar el cumplimiento de las políticas internas de la municipalidad.
		OPERACIONES	Mantenimiento y reparación de equipos informáticos, instalación de impresoras en los equipos de la institución.
		LOGÍSTICA	Instalación y mantenimiento de puntos de red de la institución.
		COMUNICACIÓN	Colaborar en funciones delegadas por el jefe del departamento de TI.
		RESPUESTA	Mantener un inventario de los equipos informáticos y sistemas de la institución.
		EVALUACIÓN	En caso de una emergencia coordinar las garantías de los equipos informáticos.

Tabla 3.39: Principales integrantes del departamento de TI y sus acciones operativas

Fuente: Elaborado por el autor

## Actores institucionales operativos del G.A.D. SALCEDO

INSTITUCIÓN	ACCIONES OPERATIVAS DEL RESPONSABLE/ DETALLE	DATOS
<b>DIRECCIÓN DISTRICTAL 05D06 SALCEDO SALUD</b>	ACTIVACIÓN DE LA EMERGENCIA	<b>Mgs. Yadira García Tello</b>
	OPERACIONES	0992680668
	LOGÍSTICA	
	COMUNICACIÓN	yadigt_88@yahoo.es
	RESPUESTA	
<b>DISTRITO DE POLICÍA SALCEDO</b>	ACTIVACIÓN DE LA EMERGENCIA	<b>Tncl. Herbie Olaf Guamani Silva</b>
	OPERACIONES	0996397707
	LOGÍSTICA	
	COMUNICACIÓN	serviciorural77@hotmail.com
	RESPUESTA	
<b>CUERPO DE BOMBEROS (SALCEDO)</b>	ACTIVACIÓN DE LA EMERGENCIA	<b>Sub. Of. Luis Pailacho</b>
	OPERACIONES	0999794920
	LOGÍSTICA	032729434
	COMUNICACIÓN	luis_alberto100@gmail.com
	RESPUESTA	
<b>SALA DE SITUACIÓN PROVINCIAL DE LA SGR</b>	ACTIVACIÓN DE LA EMERGENCIA	<b>Ing. Byron Yachimba</b>
	OPERACIONES	0992946810
	LOGÍSTICA	
	COMUNICACIÓN	byron.yachimba@gestionde riesgos.gob.ec
	RESPUESTA	direccion_zonal3@gestionderiesgos .gob.ec
	EVALUACIÓN	

Tabla 3.40: Actores institucionales operativos del G.A.D. SALCEDO

Fuente: Elaborado por el autor

### 3.2.6. Clases de riesgos que amenazan a la institución

Dentro del análisis de riesgo se ha obtenido una evaluación independiente sobre los equipos informáticos del departamento de TI, mismos que son de apoyo para establecer un promedio general dentro de los parámetros de (probabilidad e impacto), que permita determinar el grado de peligro a los cuales están expuestos los equipos de computo y sistemas de información de la institución. En la Tabla 2.3 se puede apreciar los resultados promedio que alzaron cada uno de los riesgos en relación a los equipos informáticos de la institución, gracias al conocimiento y experiencia de las personas que participaron en la evaluación del riesgo, se cuenta con datos veraces que ocurren en el G.A.D. Municipal del cantón Salcedo.

Nº RIESGO	IDENTIFICACIÓN	PROMEDIO GENERAL	
	RIESGO	PROBABILIDAD	IMPACTO
R1	Flujo de lodos y escombros (lahares).	40%	100%
R2	Lluvia de ceniza y piroclastos.	62%	93%
R3	Sismos (volcánicos/repentinos).	81%	87%
R4	Interrupción del servicio de energía eléctrica.	49%	75%
R5	Filtración de agua.	94%	95%
R6	Incendio.	62%	93%
R7	Daño en el ventilador.	36%	57%
R8	Daño en fuente de poder.	38%	57%
R9	Falla de disco duro SATA/IDE.	36%	86%
R10	Falla de Tarjeta de Red.	24%	64%
R11	Fallas de Software/Configuración.	57%	76%
R12	Falla de cableado y conectores.	52%	43%
R13	Acceso no autorizado (Robo o alteración de información).	36%	71%
R14	Ataques DoS o denegación de servicio.	41%	83%
R15	Software malicioso.	47%	87%
R16	Error Humano (Falta de conocimiento).	29%	56%
R17	Robo de dispositivos.	22%	79%
R18	Atasco de papel en la impresora	63%	77%
R19	El dispositivo no reconoce la impresora.	73%	53%
R20	Presencia de interferencias electromagnéticas.	33%	37%
R21	Ingeniería social.	30%	53%

Tabla 3.41: Promedio general del análisis de los riesgos sobre los equipos informáticos

Fuente: Elaborado por el autor

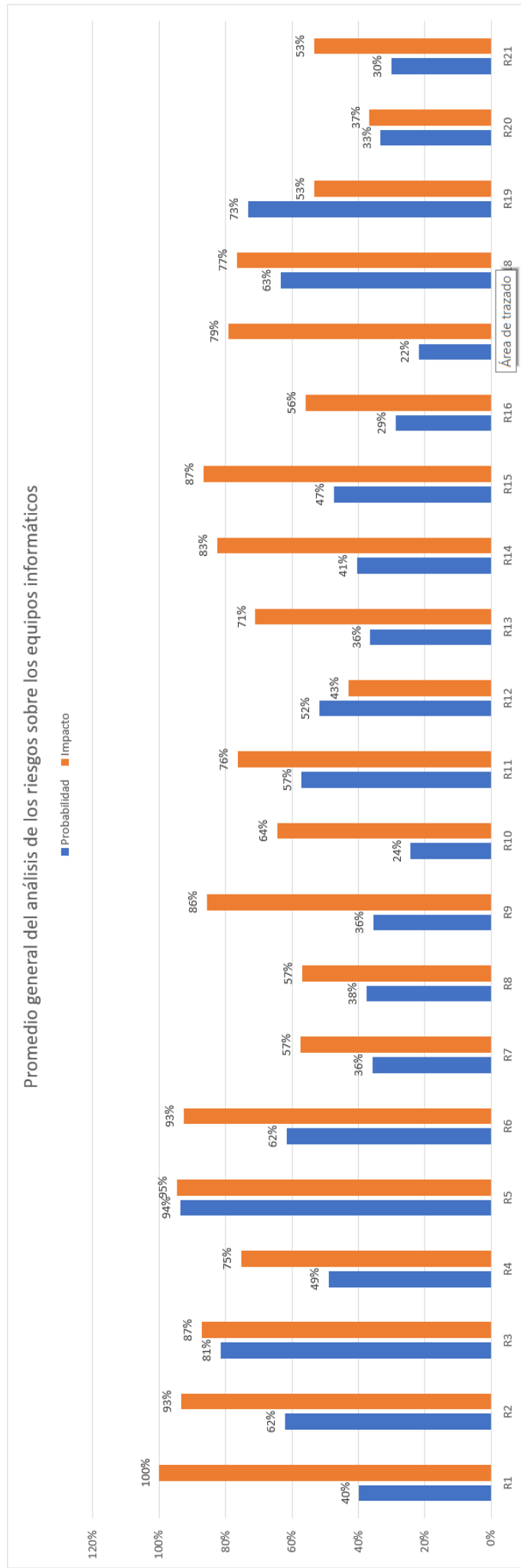


Figura 3.32: Promedio general del análisis de los riesgos sobre los equipos informáticos  
Fuente: Elaborado por el autor

### **3.2.6.1. Flujo de lodos y escombros (lahares).**

**Análisis:** En la última década no se ha registrado contingencias debido a fenómenos naturales como erupciones volcánicas que generen flujo de lodos y escombros (lahares), en vista que el volcán Cotopaxi se caracteriza por ser un estratovolcán activo. Además, de acuerdo con la ubicación de la institución se encuentra dentro de la zona de riesgo de flujos de lodo y escombros (lahares) como se observa en la Figura 3.17.

**Interpretación:** Se tiene como resultados altos índices de impacto con un promedio de 100 % correspondiente a catastrófico y a una probabilidad de ocurrencia del 40 % correspondiente a improbable, según los resultados de la evaluación promedio expuestos en la Figura 3.32. En la Tabla 3.15 se registran datos acordes a las principales amenazas por la erupción del volcán Cotopaxi que se suscitaron, tomando en cuenta la frecuencia, intensidad, magnitud, daños provocados.

#### **Consecuencias:**

- Pérdidas materiales. (Muy Severo)
- Pérdidas económicas. (Muy Severo)
- Daños a la integridad física. (Muy Severo)
- Pérdida de información. (Muy Severo)
- Interrupción del trabajo. (Muy Severo)
- Infraestructura. (Muy Severo)

### **3.2.6.2. Lluvia de ceniza y piroclastos.**

**Análisis:** La ceniza siendo un polvo compuesta por partículas de roca y mineral muy finas mismas que pueden transportarse fácilmente a largas distancias con ayuda del viento y llegar a lugares como puede ser la Municipalidad del cantón Salcedo, y por ende al departamento de TI donde esta ubicado los equipos informáticos que pueden sufrir daños severos si se ven expuestos al contacto con este polvo volcánico. Así también es el caso de los piroclastos que pueden alcanzar grandes distancias según sea la magnitud de la erupción volcánica.

**Interpretación:** Este tipo de riesgo al tener una frecuencia a largo plazo, una intensidad y magnitud alta, daños tanto materiales como humanos según la

ponderación indicada en la Tabla 3.15, de la misma manera como en el caso anterior se tiene resultados con altos índices de impacto promedio de 93 % correspondiente a catastrófico y a una probabilidad de ocurrencia del 62 % correspondiente a probable, de acuerdo a los resultados de la evaluación promedio expuestos en la Figura 3.32.

**Consecuencias:**

- Pérdidas materiales. (Grave)
- Pérdidas económicas. (Grave)
- Daños a la integridad física. (Grave)
- Interrupción del trabajo. (Grave)

**3.2.6.3. Sismos (volcánicos/repentinos).**

**Análisis:** Los sismos pueden ser provocados por una erupción volcánica o repentinos, dado a que Ecuador esta ubicado en una zona donde dos placas tienen un límite de convergencia, estas son las placas de Nazca y de Sudamérica como se muestra en la Figura 3.15, ocasionando que la placa Nazca choque y luego se sumerja bajo la placa Sudamericana, dando lugar a la formación de magmas por ende los magmas forman volcanes que al llegar a la superficie provocan sismos y erupciones volcánicas.

**Interpretación:** Como resultados se tiene un impacto promedio del 87 % correspondiente a mayor y una probabilidad de ocurrencia del 81 % correspondiente a casi seguro, si llegase a presentar este tipo de riesgo la institución se encontraría con un alto índice de pérdidas con daños físicos en la edificación y por ende al departamento de TI, afectando de manera grave la operatividad del G.A.D. Municipal.

**Consecuencias:**

- Pérdidas materiales. (Grave)
- Pérdidas económicas. (Grave)
- Daños a la integridad física. (Grave)
- Pérdida de información. (Grave)
- Interrupción del trabajo. (Grave)
- Infraestructura. (Grave)



#### **3.2.6.4. Interrupción del servicio de energía eléctrica.**

**Análisis:** La instalación eléctrica es un factor fundamental para la operación y seguridad de los equipos informáticos ya que una mala instalación provocaría fallas frecuentes, cortos circuitos y hasta provocar que los equipos se quemen. Los reguladores de voltaje son de gran importancia ya que estas interrupciones pueden quemar los equipos o de la misma manera las variaciones de energía eléctrica. La institución no cuenta con un generador de energía eléctrica que brinde la capacidad para retomar las actividades mientras esta retorna.

**Interpretación:** Factores como imperfecciones del suministro eléctrico y mantenimientos de la planta eléctrica de manera repentina han hecho que se obtenga resultados correspondientes a un impacto promedio de 75 % definido como mayor y una probabilidad de ocurrencia del 49 % correspondiente a posible que el evento llegue a ocurrir.

#### **Consecuencias:**

- Pérdidas materiales. (Moderada)
- Pérdidas económicas. (Moderada)
- Pérdida de información. (Leve)
- Interrupción del trabajo. (Moderada)

#### **3.2.6.5. Filtración de agua.**

**Análisis:** En la provincia de Cotopaxi se ha tenido épocas de fuertes lluvias que causan estragos en viviendas de material rústico, como es el caso del G.A.D. Municipal del cantón Salcedo ya que las instalaciones no están adecuadamente protegidas ante este tipo de riesgo.

**Interpretación:** Dado a que el departamento de TI se encuentra en el antiguo edificio de la institución, en el que por el pasar del tiempo ha venido deteriorándose considerablemente, potencialmente existe un alto impacto promedio del 95 % correspondiente a catastrófico y una probabilidad de ocurrencia del 94 % correspondiente a casi seguro de sufrir filtración de agua debido a las lluvias que ocurren en épocas de invierno.

**Consecuencias:**

- Pérdidas materiales. (Grave)
- Pérdidas económicas. (Grave)
- Pérdida de información. (Muy Severo)
- Interrupción del trabajo. (Grave)

**3.2.6.6. Incendio o Fuego.**

**Análisis:** El incendio, conforme con su acción calorífica, es capaz de destruir los equipos informáticos con gran facilidad como dispositivos de almacenamiento tales como CD's, DVD's, discos duros, perdiendo información importante y de esta manera interrumpiendo la operatividad de la institución. El departamento de TI al ubicarse en el edificio antiguo de la municipalidad y al encontrarse con una infraestructura considerable de madera, eleva el factor de riesgo ante un posible incendio. Esta información permite resaltar el tema sobre el sitio donde almacenar los respaldos.

**Interpretación:** Con un promedio general correspondiente a una probabilidad de 62 % correspondiente a probable, se puede determinar que el riesgo indica una alta ocurrencia en la mayoría de las circunstancias, también se considera que el impacto promedio es de 93 % correspondiente a catastrófico, por lo que se puede determinar que el área de TI tendría desastrosas consecuencias si llegara a presentarse este tipo de riesgo.

**Consecuencias:**

- Pérdidas materiales. (Muy Severo)
- Pérdidas económicas. (Muy Severo)
- Daños a la integridad física. (Muy Severo)
- Pérdida de información. (Muy Severo)
- Interrupción del trabajo. (Muy Severo)
- Infraestructura. (Muy Severo)

### 3.2.6.7. Daño en el ventilador.

**Análisis:** El ventilador como parte importante del hardware de algunos equipos informáticos como son, los computadores utilizados por el personal así como los servidores que se encuentran en constante uso ya que mantener la temperatura idónea a los componentes electrónicos del equipo es la razón que hay un alto índice de deterioro al permanecer encendidos, así mismo la acumulación de polvo es un factor predominante ya que la falta de mantenimiento hace que los equipos empiecen a fallar.

**Interpretación:** Se obtiene resultados correspondientes a un impacto promedio del 57 % definido como moderado y una probabilidad de ocurrencia del 36 % en donde el evento puede ocurrir en algún momento con baja probabilidad.

#### **Consecuencias:**

- No enciende el equipo. (Moderado)
- Interrupción del trabajo. (Grave)

### 3.2.6.8. Daño en fuente de poder.

**Análisis:** La fuente de poder es un componente del computador encargado de transformar la corriente eléctrica alterna en una corriente eléctrica continúa brindando la corriente necesaria para que los demás dispositivos del ordenador funcionen. Al encontrarse expuesto a altos y bajos picos de corriente eléctrica ocasionan un mal funcionamiento llevándolo a una sobretensión. El deterioro por el tiempo también es un factor por considerar ya que en el transcurso de su vida útil también ha ido acumulando polvo y dañando el dispositivo. Al ser elementos que permanecen gran cantidad de tiempo encendidos por el mismo hecho de ser un componente primario pueden llegar a elevar la temperatura y quemar dicho componente.

**Interpretación:** Como resultados se ha obtenido un impacto del 57 % definido como moderado y una probabilidad de ocurrencia del 38 % en donde el evento puede ocurrir en algún momento con baja probabilidad.

#### **Consecuencias:**

- No enciende el equipo. (Moderado)
- Interrupción del trabajo. (Grave)

### **3.2.6.9. Falla de disco duro SATA/IDE.**

**Análisis:** Es importante aclarar que el comportamiento de este componente es impredecible ya que en cualquier momento puede presentar una falla, el disco puede tener varios años en uso, como haber sido adquirido recientemente y puede fallar o aun mas grave dañarse de forma irreparable. Los discos duros, dado a su estructura o construcción pueden presentar diversos daños por factores como: imperfecciones del suministro eléctrico, apagado incorrecto, virus o malware, desgaste o la corrosión, y el deterioro por el tiempo.

**Interpretación:** Como resultados se ha obtenido un impacto del 86 % definido como catastrófico y una probabilidad de ocurrencia del 36 % en donde el evento puede ocurrir en algún momento con baja probabilidad.

#### **Consecuencias:**

- Pérdidas económicas. (Muy Severo)
- Pérdida de información. (Muy Severo)
- Interrupción del trabajo. (Grave)
- No enciende el equipo. (Grave)

### **3.2.6.10. Falla de Tarjeta de Red.**

**Análisis:** La tarjeta de red es un dispositivo indispensable que nos permite acceder a una determinada red de computadoras en la que podemos compartir recursos (como archivos, discos duros enteros, impresoras, servicios e internet). En la institución tener acceso a la red es importante ya que así se mantiene el normal funcionamiento de las actividades que interactúan con la ciudadanía. Problemas como es el caso de los controladores o pequeños programas que se encuentran con una mala configuración de la tarjeta es común presenciarlos, si no es el caso podría tratarse de alguna falla física en la placa o en si por el deterioro del tiempo.

**Interpretación:** De acuerdo con los resultados promedio se tiene un impacto del 64 % que correspondería a mayor si el hecho llegará a presentarse, tendría altas consecuencias y una probabilidad de ocurrencia del 24 % que corresponde a un evento improbable.

#### **Consecuencias:**

- Problemas en la detección de conexiones. (Moderado)

- Pérdidas económicas. (Moderado)
- Interrupción del trabajo. (Moderado)

#### **3.2.6.11. Fallas de Software/Configuración.**

**Análisis:** Las fallas de software son bastante comunes debido a diversos factores entre ellos el deterioro por el tiempo que también afectan a los sistemas dañando sus archivos o cuando se desinstala aplicaciones de manera incorrecta. Otro factor para considerar es la falta de actualizaciones del sistema así mismo como del antivirus que permiten el acceso a virus o malware hacia el equipo si este se encuentra conectado a la red de internet y se accede a sitios web o redes sociales de carácter peligroso, no obstante también se corre peligro al hacer uso de dispositivos externos como son USB o cualquier otro dispositivo de almacenamiento con virus, provocando fallas de software o una mala configuración en el sistema operativo principal y así deteniendo las actividades en la institución.

**Interpretación:** Como resultados de la evaluación se ha obtenido un impacto del 76 % definido como mayor ya que si llegase a ocurrir, tendría altas consecuencias o efectos sobre la entidad, y una probabilidad de ocurrencia del 57 % en donde la probabilidad es media y podría llegar a ocurrir en algún momento. Gran parte de los servicios que brinda la institución son desarrollados internamente por lo que es necesario darles un mantenimiento preventivo para evitar fallas en los sistemas.

#### **Consecuencias:**

- Pérdidas económicas. (Muy Severo)
- Pérdida de información. (Muy Severo)
- Interrupción del trabajo. (Muy Severo)
- Apagados frecuentes en el equipo. (Grave)
- Presenta lentitud en el equipo. (Moderado)
- No enciende el equipo. (Grave)

#### **3.2.6.12. Falla de cableado y conectores.**

**Análisis:** Tanto el cableado como los conectores hacia los equipos deben permanecer a una temperatura considerable para que esta no genere fallas o roturas, la instalación del cableado eléctrico es una parte importante ya que

implica crear un circuito exclusivo desde el punto de entrega de la empresa distribuidora de electricidad hacia el departamento de TI. En cuanto al cableado de red se puede apreciar en varios departamentos que no se cumple con una correcta distribución dejando a la intemperie este tipo de cableado. Al paso del tiempo el cableado y diferentes conectores tienden a deteriorarse perdiendo la efectividad de su uso generando fallas.

**Interpretación:** Como resultados se tiene un impacto promedio del 43 % que corresponde a moderado, y una probabilidad de ocurrencia del 52 % refiriéndose a posible el hecho de que ocurra alguna falla de este tipo.

**Consecuencias:**

- Interrupción del trabajo. (Moderado)
- Pérdidas económicas. (Moderado)

**3.2.6.13. Acceso no autorizado (Robo o alteración de información).**

**Análisis:** La institución cuenta con un control de acceso al Sistema de Red mediante una “cuenta” o “login” con su respectiva clave, a cada usuario de red se le designa un acceso a un sitio respectivo de trabajo para el manejo de archivos o información según sea el caso. Cuando el personal abandona sus funciones y/o es designado a otra área, se le redefinen los accesos y autorizaciones, bloqueando la primera designación y dejándola sin acceso. También se forman grupos de usuarios, a los cuales se establecen accesos por conjuntos, mejorando la administración de los recursos.

En el G.A.D. Municipal se acostumbra a confiar la clave de acceso (uso personal) a los trabajadores de cada departamento, sin medir la implicación en el caso de acceso no autorizado. En varios casos los trabajadores suelen escribir su contraseña en sitios visibles por no tener una correcta capacitación sobre la confidencialidad de sus contraseñas. La falta de seguridad en la instrucción es otro factor para considerarse ya que la ausencia de cámaras de seguridad eleva el factor de riesgo. La revelación o deslealtad por parte de algunos malos trabajadores en beneficio propio venden la información de carácter confidencial a personas ajenas a la institución.

**Interpretación:** Como resultados de la evaluación se tiene un impacto promedio del 71 % que corresponde a mayor dado a que si el hecho llegase a ocurrir tendría altas consecuencias y una probabilidad de ocurrencia del 36 % refiriéndose a una probabilidad baja pero que puede ocurrir en algún momento.

### **Consecuencias:**

- Pérdidas materiales. (Grave)
- Pérdidas económicas. (Grave)
- Pérdida de información. (Grave)
- Interrupción del trabajo. (Grave)
- Desestabilización institucional. (Grave)

#### **3.2.6.14. Ataques DoS o denegación de servicio.**

**Análisis:** Este ataque de denegación del servicio conocido también como ataque DoS (Denial-of-service attack), es el que busca quitar a los usuarios el acceso a los equipos y a su red. La falta de disponibilidad de todos los servicios de red y conectividad es su característica principal. La institución maneja gran cantidad de información confidencial la misma que es ansiada por los ciberatacantes para luego venderla o bien dejar a la institución sin operar. Para ello el G.A.D. Municipal cuenta con un Software Antivirus corporativo que se lo actualiza anualmente. Todo software es manejado por el personal de TI, quienes son los encargados de su instalación en los computadores. La municipalidad cuenta con firewall que permite bloquear las paginas web evitando cualquier tipo de amenaza. Se cuenta con un programa permanente de bloqueo de acciones como cambiar configuraciones de red, acceso a servidores, etc. Así como es el caso de empleados cómplices o desleales que quieran dañar la buena imagen de la institución.

**Interpretación:** Como resultados de la evaluación se tiene un impacto promedio del 83 % dentro de la categoría de catastrófico, si el hecho llegara a presentarse se tendría desastrosas consecuencias en cuanto a la probabilidad que esto ocurra es del 41 % categorizándolo como una probabilidad media, podría ocurrir en algún momento.

### **Consecuencias:**

- Denegación de servicio. (Muy Severo)
- Pérdida de la conectividad de la red. (Grave)
- Pérdidas económicas. (Grave)
- Pérdida de información. (Muy Severo)

- Interrupción del trabajo. (Grave)
- Desestabilización institucional. (Muy Severo)

#### **3.2.6.15. Falla de Hardware.**

**Análisis:** Un error de hardware es un fallo en las piezas físicas que componen un equipo informático, diversos factores pueden ser los causantes entre los más comunes suelen ser: imperfecciones del suministro eléctrico, humedad, acumulación de polvo, falta de mantenimiento, deterioro por el tiempo, sobretensión y apagado incorrecto. Principalmente los servidores pueden sufrir algún tipo de daño físico ya que por el hecho de permanecer encendidos gran parte del tiempo se ven expuestos a un alto deterioro en el que es necesario darle un mantenimiento adecuado cada cierto tiempo. El departamento de TI de la Municipalidad cuenta con un técnico de sistemas que se encarga de dar mantenimiento a los equipos y dar soporte en el caso de ocurrir algún tipo de falla.

**Interpretación:** Como resultados de la evaluación se ha obtenido un impacto del 87% correspondiente a catastrófico, si el hecho llegara a ocurrir tendría desastrosas consecuencias por otra parte la probabilidad de ocurrencia es de 47% con una probabilidad media.

#### **Consecuencias:**

- Pérdidas económicas. (Grave)
- Pérdida de información. (Grave)
- Interrupción del trabajo. (Grave)
- Equipo funcione mucho más lento de lo normal. (Grave)
- Sistema muestre pantallas azules de la muerte. (Grave)

#### **3.2.6.16. Error Humano (Falta de conocimiento).**

**Análisis:** El error humano es uno de los problemas que originalmente suceden por la falta de conocimiento o la negligencia laboral. Se debe considerar cuanto saben los empleados de computadoras o redes para una mejor eficiencia en sus labores. Durante el tiempo que dure las vacaciones de los empleados, se debe capacitar correctamente al reemplazo para que este sustituya mientras el empleado regrese de sus vacaciones.



**Interpretación:** Como resultados de la evaluación se ha obtenido un impacto del 56 % correspondiente a moderado si llegase a presentarse tendría consecuencias medianas por otra parte la probabilidad de ocurrencia es de 29 % con una probabilidad baja.

**Consecuencias:**

- Pérdidas económicas. (Moderado)
- Pérdida de información. (Moderado)
- Interrupción del trabajo. (Moderado)

**3.2.6.17. Robo de dispositivos.**

**Análisis:** En el G.A.D. Municipal existe vigilancia permanente, pero no se verifica si el personal de seguridad cumple con la inspección de los usuarios, sobre su obligación de cerrar puertas y ventanas al finalizar su jornada. Es relativamente fácil remover un disco duro del case, un CD-DVD ROM, tarjetas, etc., y no darse cuenta del faltante hasta días después, situaciones de este tipo no se han presentado en la institución pero es importante mantenerse alerta, por lo que la ausencia de cámaras de seguridad en varios departamentos es un factor de riesgo ya que varios empleados desleales pueden generar perdidas de equipos si así lo proponen, así que es mejor ser cautelosos y establecer medidas de seguridad.

**Interpretación:** Como resultados de la evaluación se ha obtenido un impacto del 79 % correspondiente a mayor si el hecho llegara a presentarse, tendría altas consecuencias mientras que la probabilidad de ocurrencia es del 22 % con una probabilidad baja.

**Consecuencias:**

- Pérdidas materiales. (Grave)
- Pérdidas económicas. (Grave)
- Pérdida de información. (Muy Severo)
- Interrupción del trabajo. (Grave) Desestabilización institucional. (Grave)

**3.2.6.18. Atasco de papel en la impresora.**

**Análisis:** El atasco de papel es uno de los problemas mas comunes ya que detiene todo el proceso de impresión independientemente del tipo de

impresora que se utilice. La mayoría de los atascos de papel se deben a simples problemas mecánicos. La falta de capacitación del personal sobre como manipular correctamente es otro factor relevante ya que no colocan el papel de manera correcta en la bandeja causando problemas mecánicos. El deterioro por el tiempo y la falta de un mantenimiento preventivo hacen que empiece a fallar.

**Interpretación:** Como resultados de la evaluación se ha obtenido un impacto del 77 % correspondiente a mayor si el hecho llegara a presentarse, tendría altas consecuencias mientras que la probabilidad de ocurrencia es del 63 % con una probabilidad alta.

**Consecuencias:**

- Pérdidas económicas. (Moderado)
- Interrupción del trabajo. (Leve)

**3.2.6.19. El dispositivo no reconoce la impresora.**

**Análisis:** En el G.A.D. Municipal los equipos de impresión son de gran utilidad en los diferentes departamentos ya que la gran mayoría de tramites necesitan ser firmados y verificados con el personal encargo de cada área, en donde suele presentarse un problema en el dispositivo (computador) dado a que no reconoce la impresora, esta falla se relaciona con un problema en los controladores, cables conectados de manera incorrecta, o deterioro por el tiempo de uso.

**Interpretación:** Como resultados de la evaluación se ha obtenido un impacto del 53 % correspondiente a moderado si el hecho llegara a presentarse tendría medianas consecuencias mientras que la probabilidad de ocurrencia es del 73 % con una probabilidad alta.

**Consecuencias:**

- Pérdidas económicas. (Leve)
- Interrupción del trabajo. (Leve)

**3.2.6.20. Presencia de interferencias electromagnéticas.**

**Análisis:** La instalación eléctrica es un factor fundamental ya que debe cumplir con varias medidas, entre ellas mantener una distancia considerable entre las instalaciones eléctricas y los cableados de red para que justamente no exista interferencias electromagnéticas que causes fallas en la conectividad de la red.

**Interpretación:** Como resultados de la evaluación se tiene un impacto promedio del 37 % dentro de la categoría de menor, si el hecho llegara a presentarse se tendría un bajo impacto en cuanto a la probabilidad que ocurra es del 33 % categorizándolo como una probabilidad baja, dado a que el evento puede ocurrir en algún momento y se lo debe considerar.

**Consecuencias:**

- Pérdidas económicas. (Moderado)
- Pérdida de información. (Moderado)

**3.2.6.21. Ingeniería social.**

**Análisis:** La Ingeniería Social se refiere a la manipulación psicológica del personal, para que estos entreguen información confidencial entre ellos las contraseñas personales para acceder a sus cuentas y robar o alterar información o simplemente instalar software malicioso para desestabilizar a una institución. Los engaños a los empleados también suelen ser con correos electrónicos de phishing suplantando la identidad de la institución para obtener información, para ellos de debe capacitar al personal para evitar este tipo de riesgos.

**Interpretación:** Como resultados de la evaluación se tiene un impacto promedio del 53 % dentro de la categoría de moderado, si el hecho llegara a presentarse se tendría medianas consecuencias en cuanto a la probabilidad que ocurra es del 30 % categorizándolo como una probabilidad baja, dado a que el evento puede ocurrir en algún momento y se lo debe considerar.

**Consecuencias:**

- Pérdida de información. (Grave)
- Interrupción del trabajo. (Grave)
- Desestabilización institucional. (Grave)

### **3.2.7. Actividades generales previas al desastre**

En esta parte se considera una etapa de planteamiento, preparación y ejecución de actividades de resguardo de la información, y de los equipos informáticos en el que se asegure un proceso de recuperación con el menor tiempo posible evitando así grandes pérdidas de dinero para la municipalidad.

#### **Establecimiento del Plan de Acción**

En esta etapa de planteamiento se establece los procedimientos relativos a:

##### **3.2.7.1. Equipos Informáticos**

En este apartado se detallan de forma general las actividades que se debe tomar para prevenir los equipos informáticos. El G.A.D. Municipal del cantón Salcedo deberá tener actualizado el inventario de los equipos informáticos con los que cuenta. Para el presente proyecto de titulación se ha realizado un inventario de los principales equipos informáticos entre ellos servidores, equipos de cómputo, impresoras, hardware de red, para complementar con la información adquirida por el departamento de TI. Se detalla en el Anexo A para informe del inventario de la institución.

Para tener una adecuada identificación y protección en los equipos informáticos se debe considerar los siguientes puntos:

- Como parte de la protección institucional se debe contar con pólizas de seguros comerciales, que brinden un seguro a los activos informáticos, teniendo en cuenta una restitución por equipos de mayor tecnología, considerando el avance tecnológico al paso del tiempo.
- Etiquetar los equipos informáticos acorde a su categoría en importancia de contenido y valor monetario que representa su pérdida, con el objetivo de dar prioridad en caso de evacuación por emergencia y salvaguardar el equipo sin que esto represente riesgo de exponer su vida. Se podría considerar: etiquetar con un color rojo a los servidores, color amarillo los computadores con información importante, y con color verde los demás equipos de uso cotidiano que no representen mayor pérdida para la municipalidad.
- Realizar un mantenimiento preventivo a los equipos informáticos de manera periódica y así conservar su buen funcionamiento.

- Dependiendo del tipo de problema en el equipo informático, los jefes de cada departamento deben comunicar el incidente al departamento de TI, para que este de una pronta solución.

### **3.2.7.2. Sistemas e Información**

Se debe tener en cuenta un inventario de los principales Sistemas de Información con los que cuenta la institución, tanto los de desarrollo interno, como los desarrollados por empresas externas. Se detalla en el Anexo B para informe del inventario de la institución.

### **3.2.7.3. Obtención y almacenamiento de los respaldos de Información**

En esta parte se redacta de manera general las instrucciones de los backups de los principales elementos de software necesarios para restablecer las actividades normales de la institución en caso de ocurrir un desastre, donde los datos originales estarán a salvo en un lugar distinto a la institución afectada. Los backups de seguridad que se deben tomar en cuenta son:

1. **Backup del Sistema Operativo:** Se debe tener un respaldo de todas las versiones de los sistemas operativos instalados en la red.
2. **Backup del Software Base:** Tener un respaldo de los lenguajes de programación utilizados en el desarrollo de los aplicativos de la municipalidad.
3. **Backup del Software Aplicativo:** Considerar backups de los programas fuentes (código fuente) y programas ejecutables de la municipalidad.
4. **Backup de las Bases de datos:** Un respaldo de la base de datos, índices, triggers, password y demás archivos necesarios para la correcta ejecución del software aplicativo de la municipalidad.
5. **Backup del Hardware:** En esta parte de puede considerar dos modalidades externa o interna:

**Modalidad Externa:** Esta parte se refiere al convenio que puede tener la municipalidad con otra institución donde tenga equipos similares o superiores con la capacidad y seguridad suficiente para procesar la información y ser puesta a la disposición de la institución en caso de ocurrir un siniestro. Definir un convenio

claro es la clave de esta modalidad al tener sus condiciones bien definidas ya que se debe considerar la cantidad de equipos, periodos de tiempo, los ambientes, etc., donde la entidad mantenga un Plan de Seguridad de Hardware en relación a las pólizas de seguros que respalden estos equipos.

**Modalidad Interna:** En el caso del G.A.D. Municipal del cantón Salcedo dispone de un sitio en el que podría ser usado para almacenar equipos de respaldo para luego ser utilizados ante una emergencia, en este caso podría ser el Terminal terrestre del cantón que cuenta con instalaciones nuevas donde actualmente funcionan varios departamentos de la institución, es este lugar en donde se puede aprovechar para procesos de restauración de información que posibiliten el funcionamiento normal de los procesos y actividades de la municipalidad.

#### 3.2.7.4. Políticas (normas y procedimientos de respaldos)

Para la obtención de los “Backups” es necesario establecer normas y procedimientos, los mismos que fueron tomados en consideración por los miembros del departamento de TI, según las medidas de seguridad tomadas por la institución para precautelar la información. Entre las principales actividades mencionadas en las políticas internas de la municipalidad que debe realizar el personal capacitado del departamento de TI se encuentran:

NOMBRE DEL RECURSO	DESCRIPCIÓN	TIPO DE BACKUP	RESPONSABLE
<b>SIG-AME: Sistema de Integral de Gestión. Su módulo Sistema Administrativo Financiero.</b>	Diario en el servidor	Backup progresivo o incremental	Ing. Enrique Arcos Ing. Paulina Villalba
<b>SIC-AME: Sistema Integral de Catastros.</b>	Diario en el servidor	Backup progresivo o incremental	Ing. Enrique Arcos Ing. Paulina Villalba
<b>Sistemas desarrollados en la institución.</b>	Diario en el servidor	Backup progresivo o incremental	Ing. Enrique Arcos Ing. Paulina Villalba
<b>Sistema de Control Biométrico de Recursos Humanos.</b>	Cada 15 días en el computador del Analista Informático y cada mes a Recursos Humanos.	Backup completo	Ing. Enrique Arcos Ing. Paulina Villalba
<b>Sistemas internos y externos de la municipalidad.</b>	Backup automático, días no laborables, feriados, etc.	Backup completo	Ing. Enrique Arcos Ing. Paulina Villalba

Tabla 3.42: Tipos de Backups y responsables

Fuente: Elaborado por el autor

- Se debe llevar un control obligatorio con el uso de un formulario del programa de Backups diarios, semanales y mensuales, este control será implementado por el departamento de TI de tal manera que lleven un registro diario sobre los resultados de los backups realizados como se muestra en el Anexo C F.1.
- Ejecutar el proceso de almacenamiento de los Backups en condiciones ambientales apropiadas, considerando el medio magnético empleado.
- No se realiza remplazos de los backups, pero si se realiza copias de estas, tomando en cuenta que no se puede predecir exactamente el periodo de vida útil del dispositivo o equipo donde se ha realizado el backup.
- Realizar los Backups en lugares distintos de donde reside la información primaria y así evitar su pérdida en caso de la destrucción del lugar de origen. En la institución se tiene distribuidos los backups de la siguiente manera: una copia reside en el departamento de TI, y una segunda copia reside en la oficina que genera la información (RR.HH. y OO.PP.).
- Verificar la funcionalidad de los Backups realizando pruebas periódicas (Restore), mediante los sistemas y resultados anteriormente confiables de la primera y segunda copia realizada.

### **3.2.7.5. Formación de equipos operativos**

En cada departamento de la institución en donde se almacene información y sirva para la operatividad de la institución, se deberá designar responsables de la seguridad de los equipos informáticos, así como de la información, y la integridad física de los miembros del departamento al que pertenezcan, puede ser el jefe del departamento o sus funcionarios que estén prestos a colaborar con actividades extras para prevenir una emergencia, entre las principales acciones que tendrán se tiene:

- Mantener una capacitación adecuada para conservar el control y la calma al resto del personal dentro del departamento al cual pertenezca (se incluye el departamento de TI), ante cualquier tipo de riesgo físico que pueda presentarse.
- Tener identificado los equipos con mayor importancia de contenido de acuerdo con la etiqueta con su categoría previamente realizado como se

menciona en el apartado (3.2.7.1). Esta actividad debe realizarse dentro del departamento de TI así como en los demás departamentos que se maneje información.

- Realizar simulacros de acuerdo con las medidas para salvaguardar los principales equipos informáticos con mayor importancia considerando la ruta más segura para hacerlo y llegar a un sitio seguro durante una emergencia, (si la situación lo amerita y no representen riesgo de exponer la vida).
- Conocer las rutas de evacuación y áreas seguras establecidas previamente por la administración (avalúos y catastros) de la municipalidad que sirvan como puntos de encuentro del personal.
- Responsabilizarse de verificar la fecha de caducidad del extintor y notificar a quien corresponda para su recargo y mantener listo ante cualquier tipo de emergencia que requiera su uso.
- En el caso del jefe de cada departamento debe proporcionar las facilidades del caso (procedimientos, técnicas) para que el personal encargado del departamento de TI, realice los Backus de acuerdo con las políticas internas de la municipalidad mencionadas anteriormente en el apartado (3.2.7.4).

### **3.2.8. Actividades generales durante el desastre**

Si la contingencia o emergencia se presenta se debe ejecutar las siguientes actividades previamente descritas.

#### **3.2.8.1. Plan de Emergencias**

En esta parte se redacta las actividades a desarrollarse durante un desastre o siniestro, considerando la probabilidad de ocurrencia durante el día, noche o madrugada. El plan incluye la participación de todas y cada una de las personas que puedan encontrarse presentes en el lugar de ocurrencia del siniestro. Las acciones correspondientes al resguardo de los equipos informáticos durante predomine un determinado siniestro serán llevadas acabo sin que esta situación atente con exponer la vida. Durante ocurra la actividad del siniestro si el personal no está debidamente capacitado previamente será difícil para las personas enfrentar esta situación, dado a que no se encuentran con los conocimientos de seguridad respectivos, por este motivo en esta etapa se dedica a brindar una



ayuda inmediata evitando que la acción misma del siniestro cause más daños o destrucciones.

El personal de toda la institución debe conocer lo siguiente:

- **Plan de Evacuación Personal:** En el G.A.D. Municipal el personal ha recibido periódicamente instrucciones para la evacuación ante siniestros, mediante simulacros, con el apoyo de la Defensa Civil de la localidad con programas de seguridad, que instruyen al personal a utilizar las vías de escape.
- **Localización de vías de Escape o Salidas de Emergencia:** Conocer las vías de escape o salida en la institución ya que estas señales son de gran ayuda ante una emergencia, para que el personal actúe de forma adecuada y ordenada, solicitando apoyo de inmediato..
- **Ubicación y señalización de elementos contra un siniestro:** Estos elementos pueden ser extintores, una iluminación adecuada, zonas de seguridad debidamente señalizadas como son salidas de emergencia.
- **Listado de llamadas en caso de siniestro:** Tener a la mano lista de teléfonos de instituciones como son: Compañía de bomberos, Hospitales, Centro de Salud, Ambulancia, Seguridad, como se muestra en las Tablas 3.38, 3.39, 3.40.

### **3.2.8.2. Formación de Equipos**

La formación de equipos de trabajo se refiere a realizar determinadas actividades que serán desarrolladas en el caso de ocurrir un desastre en la institución.

Si la situación lo amerita y al encontrarse cercano al área de los equipos informáticos en peligro y al inicio de un desastre que podría ser controlable, considerando siempre las medidas de no exponer la vida, se debe actuar conforme dos equipos de personal que se realizó previo a una emergencia.

Actuar responsablemente durante un determinado siniestro, el primer equipo se encarga de combatir dicho siniestro y el otro para el rescate de los equipos informáticos, según los lineamientos de prioridades según el equipo.

### **3.2.8.3. Entrenamiento**

Contar con una presentación de actividades que den lucha contra los distintos tipos de siniestros de forma periódica es necesario. En estas practicas se asignan

roles con actividades precisas según los planes de evacuación del personal y equipos informáticos, y así minimizar las pérdidas para la institución. En estos programas de charlas también se muestra el uso de extintores y la manera correcta de utilizarlos.

Es importante concientizar al personal sobre los siniestros que pueden llegar a suceder como son, (incendios, terremotos, erupción volcánica, inundaciones, apagones, etc.); estos son algunos de los siniestros que podrían llegar a materializarse, es por este motivo que se debe tomar con la seriedad y responsabilidad que esto amerita, de allí la importancia de los entramientos, se debe contar con la participación de los directivos de la municipalidad.

### **3.2.9. Actividades generales después del desastre**

Luego de ocurrir un desastre las actividades a cumplir inmediatamente son las siguientes:

#### **3.2.9.1. Evaluación de daños**

Como principal objetivo se debe evaluar la dimensión de los daños producto de algún tipo de desastre, identificando que equipos se encuentran inoperativos y por ende que sistemas o servicios se hallaran suspendidos, y cuales se pueden restablecer y en que tiempo.

Con respecto al G.A.D. Municipal del cantón Salcedo se debe dar prioridad a los procesos de contabilidad, tesorería, área administrativa, avalúos y catastros, para que estos vuelvan a estar operativos dado a que representan gran importancia estratégica para la institución. Por ende brindar una pronta recuperación y puesta en marcha de estos servidores que alojan dichos sistemas o servicios, es prioritario.

#### **3.2.9.2. Priorizar Actividades del Plan de Acción**

Una vez evaluados los daños se tendrá como resultado un grupo de actividades con el objetivo de contrarrestar las perdidas, con propuestas estratégicas y urgentes que necesita la municipalidad. Estas actividades servirán de apoyo para la puesta en marcha tanto de los equipos informáticos afectados como de los servicios alojados en estos, reposición de equipos y accesorios dañados, etc.

#### **3.2.9.3. Ejecución de actividades**

Para esta parte involucra la creación de grupos de trabajo para de esta manera ejecutar actividades anteriormente planificadas en el Plan de Acción. Estos grupos

de trabajo contarán con un coordinador los cuales darán un reporte del avance de estos grupos de recuperación, en el caso de presentarse un problema se debe notificar al jefe o coordinador del Plan de Contingencia a cargo.

Para la recuperación de los trabajos se contará con dos partes:

- La restauración de los servicios en la institución se los realizará utilizando recursos de la institución o el local de respaldo si es el caso.
- Como segundo punto sería volver a contar con los recursos que sufrieron algún daño o fueron afectados retomando su lugar propio en la institución, esta etapa debe ser lo suficientemente rápida para evitar en lo posible grandes pérdidas económicas por falta de operatividad institucional. Garantizar un buen servicio a la colectividad del cantón Salcedo y mantener la buena imagen de la institución son los principales objetivos.

#### **3.2.9.4. Evaluación de los resultados**

Una vez terminadas las labores de recuperación de los equipos y sistemas perjudicados por el siniestro, es importante proceder con la evaluación de todas las actividades realizadas, y conocer con que eficiencia se ejecutaron, el tiempo que tomo, que circunstancias aceleraron y cuales entorpecieron el proceso con respecto al Plan de Acción, cual fue el comportamiento de los equipos de trabajo, etc.

#### **3.2.9.5. Retroalimentación del Plan de Acción**

De esta evaluación de resultados podemos conseguir una retroalimentación para el Plan de Contingencias y Seguridad de la Información, junto con recomendaciones para minimizar los riesgos. Se debe optimizar el Plan de Acción original, perfeccionando las actividades que tuvieron algún tipo de dificultad y reforzando aquellas actividades que funcionan adecuadamente. Un aspecto importante es evaluar cual hubiera sido el costo si no se contaba con un Plan de Contingencia en el G.A.D. Municipal del cantón Salcedo.

#### **3.2.10. Acciones específicas frente a los tipos de riesgo**

Este tipo de riesgos son aquellos que fueron tomados en conjunto con los miembros del departamento de TI, en el que se realizó un análisis previo a su correspondiente evaluación basándose en una recolección de información sobre los riesgos que pueden afectar a la institución, así como la experiencia que el personal del

departamento de TI ha ido adquiriendo. Estas acciones serán complementadas en conjunto con un diagrama de respuesta, que serán actividades de primera mano que estarán a disposición de todo el personal para su correspondiente conocimiento en caso de materializarse algún tipo de riesgo.

### 3.2.10.1. Clase de Riesgo: Flujo de lodos y escombros (lahares)

Dado a que producto de una erupción volcánica se generan: flujos de lodos y escombros acompañados de lluvia de ceniza y piroclastos, en el que también se presentan movimientos sísmicos, estas actividades serán compartidas entre estas clases de riesgos que son de gran importancia para ser consideradas.

El G.A.D. Municipal del cantón Salcedo cuenta con un Plan de Contingencia cantonal ante una erupción del volcán Cotopaxi, mismo que fue compartido para considerarse en el presente Plan de Contingencia Informático, en la Tabla 3.43 se puede apreciar la coordinación operativa ante este tipo de riesgo que lleva la institución, mismo que será complementado con acciones necesarias para sobrellevar una emergencia en caso de presentarse.

RIESGO IDENTIFICADO	ACCIONES DE PRIMERA RESPUESTA	RESPONSABLES O DE APOYO EN LA PRIMERA RESPUESTA
FLUJO DE LODOS Y ESCOMBROS (LAHARES)	<b>Fase de prevención:</b> Publicar boletines de prensa, afiches, cartillas entre otros y difundir a través de medios de comunicación los daños que traerá consigo la erupción y el riesgo al que está expuesta la ciudadanía que se encuentran ubicados en zonas de riesgos.	<ul style="list-style-type: none"> <li>* DIRECCIÓN DE SEGURIDAD CIUDADANA Y UGR G.A.D. SALCEDO.</li> <li>* CUERPO DE BOMBEROS.</li> <li>* POLICIA NACIONAL.</li> <li>* ÁREA DE SALUD DE SALCEDO.</li> <li>* ECU 911.</li> <li>* SNGRE. Servicio Nacional de Gestión de Riesgos y Emergencias.</li> <li>* CRUZ ROJA.</li> </ul>
	<b>Fase de atención de la emergencia:</b> Recibir el aviso del IGM y asistir a los lugares donde sea necesario el salvamento de personas que se encuentren atrapada en viviendas, escuelas, colegios, instituciones entre otras por la presencia de lodo y lava (lahares).	
	<b>Fase de rehabilitación:</b> Evaluar daños en nuestra jurisdicción a causa de los flujos de lava.	

Tabla 3.43: Coordinación operativa en la atención de la emergencia (Flujo de lodos y escombros, lahares)

Fuente: Elaborado por el autor, a partir del Plan de contingencia cantonal ante una erupción del volcán Cotopaxi [45]

## ACTIVIDADES ANTES

### Medidas Humanas

- Tener a la mano los números telefónicos de emergencia, los responsables de la activación de la emergencia, así como de los actores institucionales operativos como se muestra en las Tablas. 3.38, 3.39, 3.40, de esta manera tendremos comunicación directa con el personal de estas entidades y dar cualquier tipo de aviso y solicitar apoyo.
- Organizarse mediante la formación de equipos operativos para un mejor control y orden como se indica en el literal (3.2.7.5).
- El equipo del Comité de Operaciones de Emergencia (C.O.E.) cantonal de Salcedo, cuenta con la señalética de emergencia y rutas de evacuación correspondiente a la municipalidad.
- Coordinar con a la UPC del cantón para brindar una capacitación y realizar simulacros preventivos a todo el personal incluido los directivos, ante una posible emergencia que llegue afectar la institución gravemente. Así mismo ejecutar programas de capacitación acerca del uso de elementos sobre seguridad y la manera correcta de dar primeros auxilios, a todo el personal de la municipalidad.
- Al encontrarse dentro la zona de peligro ante una erupción volcánica se debe buscar un asesoramiento sobre cómo proceder y acatar las órdenes para precautelar la vida de quienes trabajan en la municipalidad.
- Ubicar un botiquín de primero auxilios en un lugar visible dentro de cada departamento de la institución.
- Colocar un extintor cargado en un lugar visible dentro del departamento donde están ubicados los servidores en la institución. De igual manera en todos los departamentos ubicar extintores debidamente cargados y en cuanto al personal capacitar sobre la manera correcta de uso.
- En cuanto a los equipos informáticos se debe seguir una serie de lineamientos y pólizas estipuladas por la municipalidad del cantón entre algunas mencionadas en el apartado (3.2.7.1) para estar prevenidos ante una emergencia de este tipo.

- La institución debe contar con pólizas de seguros comerciales, que brinden un seguro a los activos informáticos como se menciona en el apartado (3.2.7.1) de los equipos informáticos.

### **Medidas Técnicas**

- Buscar asesoría de un ingeniero civil, arquitecto, para identificar sitios con mayor vulnerabilidad en la municipalidad y los más seguros para poder protegerse ante un riesgo de grandes dimensiones.
- Realizar revisiones periódicas, y reparar si fuera el caso, las instalaciones eléctricas, de gas si existiera y así mantenerlos en buen estado, capacitar el personal sobre como desconectar los suministros de electricidad y gas para evitar que el riesgo se pueda incrementar.
- Actualizar periódicamente el inventario de los equipos informáticos para tener un respaldo tanto para un correcto funcionamiento de las actividades como para el conocimiento de la institución de seguros que brinda el apoyo a la institución ante posibles desastres.
- Etiquetar los equipos informáticos acorde a su categoría en importancia de contenido y valor monetario que representa su pérdida como se menciona en el apartado (3.2.7.1) de los equipos informáticos.
- Elaborar un plan para la evacuación de hardware, que permita coordinar al los equipos operativos transportar los equipos informáticos a un sitio seguro en el menor tiempo posible, para esto se debe considerar su categoría en importancia de contenido y valor monetario que representa su pérdida (si la situación lo amerita y no representen riesgo de exponer la vida).
- La información con carácter crítico debe contar con una copia de seguridad en espejo (MIRROR BACKUP) en otro sitio alternativo, manteniendo así una copia exacta de los datos originales en caso de ocurrir un desastre.
- Mantener de manera periódica Backus de los principales elementos de software necesarios para restablecer las actividades normales de la institución, como se menciona en el apartado (3.2.7.3).

## ACTIVIDADES DURANTE

### Medidas Humanas

- Ante todo, se recomienda conservar la calma, ya que de esto repercute las acciones tomadas durante la emergencia.
- En ese instante de la erupción volcánica cualquier actividad que se esté realizando en los equipos informáticos, se deberá suspender guardando la información que se haya trabajado y cerrar la sesión de usuario.
- No utilizar los ascensores, descender por las escaleras con las manos sobre la cabeza protegiéndose ante la caída de algún objeto, al descender pegarse a la pared en donde posee mayor resistencia, recuerde: No gritar, No empujar, No correr, y dirigirse a una zona de seguridad.
- Cada departamento de la institución debidamente evacuado siempre manteniendo la calma, los jefes o encargados del área procederán a cerrar sus puertas y colocar una tela blanca en la entrada indicando que se evacuó facilitando así el trabajo de las brigadas de auxilio.
- En el refugio temporal es necesario registrarse y atender a las recomendaciones que se le indiquen.
- El personal de la institución debe actuar de acuerdo con un plan de emergencia ante este tipo de desastres mismo que la municipalidad cuenta con un estudio por las autoridades competentes de la municipalidad, para complementar se menciona en el apartado (3.2.8.1) algunas medidas que estarán tomadas en cuenta.

### Medidas Técnicas

- Apagar los equipos informáticos y desconectar los servidores y equipos de red (OFF) en la caja principal de corriente, (si la situación lo amerita y no representen riesgo de exponer la vida).
- En los grupos formados previo a una emergencia se procederá a realizar las actividades encomendadas, (Sin que estas acciones representen riesgo de exponer la vida) entre ellas se encuentran:
  - El primer equipo se encarga de combatir dicho siniestro como es desconectar el suministro eléctrico y de gas si existiera.

- El segundo equipo se encarga del rescate de los principales equipos informáticos (servidores), trasladándolos a un lugar seguro, y así limitar los daños.
- Un tercer equipo debe asegurarse de cerrar el acceso al departamento, asegurándose que no exista personal en su interior.

## **ACTIVIDADES DESPUÉS**

### **Medidas Humanas**

- Las autoridades del (COE) cantonal son los encargados de evaluar la situación de la institución en colaboración con los bomberos del cantón, y personal de seguridad, para declarar por finalizado la emergencia.
- Ya con los resultados del (COE) cantonal las autoridades de la municipalidad procederán a informar al personal que pueden retornar a su departamento de trabajo de manera segura.
- Realizar una reunión con las autoridades de la institución para hacer un recuento de los daños y tomar las medidas del caso.
- En caso de un daño severo de las instalaciones, trasladar las operaciones a otras oficinas alternas.
- Proceder al trámite pertinente de las garantías de los equipos afectados por el desastre, o a su vez comprar los equipos indispensables para retomar las operaciones.

### **Medidas Técnicas**

- Identificar los principales equipos informáticos afectados para su pronto reemplazo.
- Se debe hacer un testeo de la infraestructura de la red para verificar cualquier tipo de avería causada por la emergencia.
- Recoger los Backups, programas, manuales del sitio alternativo en donde se encuentran resguardados.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.
- Brindar el soporte pertinente a la restauración para verificar y probar la integridad de los datos.



- Iniciar las operaciones, sin pasar por alto las medidas de seguridad establecidas por las políticas internas de la municipalidad.

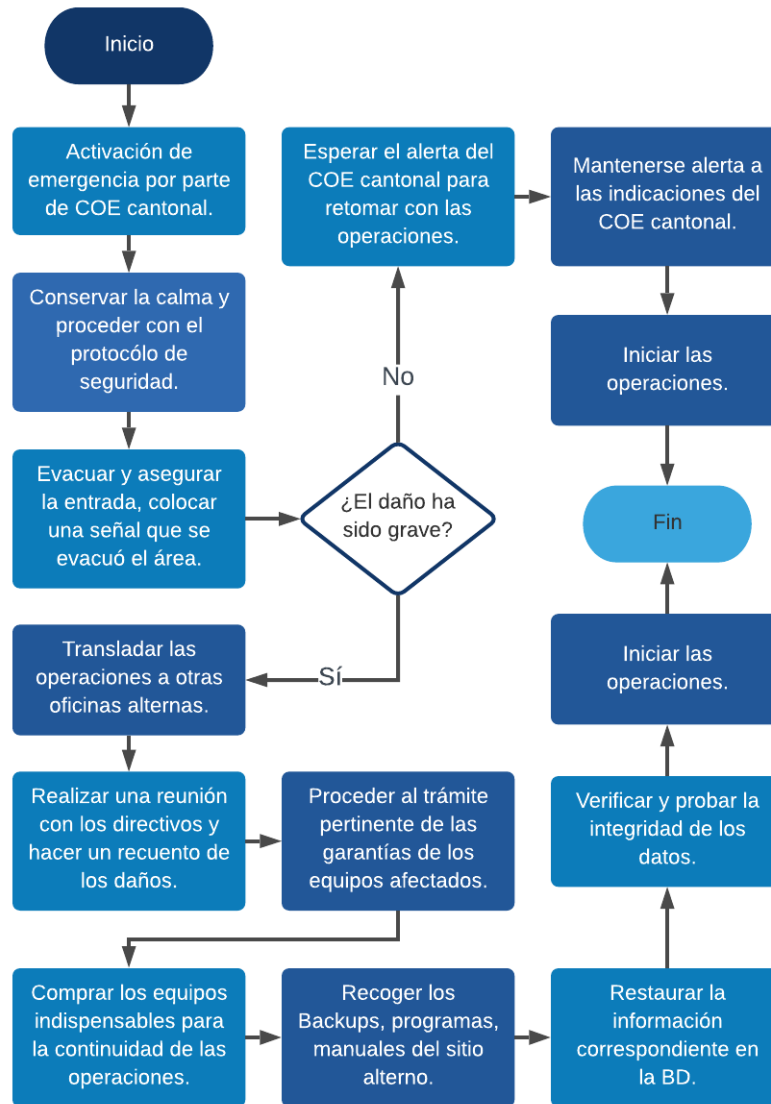


Figura 3.33: Acciones frente al flujo de lodos y escombros (lahares)  
Fuente: Elaborado por el autor

### 3.2.10.2. Clase de Riesgo: Lluvia de ceniza o piroclastos

Este riesgo puede presentarse en erupciones volcánicas, así es el caso en el que la acumulación de ceniza en los techos podría ocasionar su colapso dando lugar a pérdidas humanas y materiales que se encuentren bajo el techo. La infraestructura de la Municipalidad del cantón Salcedo correspondiente al edificio antiguo es de teja propenso a sufrir este tipo de riesgo. Las actividades que se presentan a

continuación comparten este tipo de riesgo de flujo de lodos y escombros (lahares) en el punto anterior al presentarse en una erupción volcánica.

El G.A.D. Municipal del cantón Salcedo cuenta con un Plan de Contingencia cantonal ante una erupción del volcán Cotopaxi, mismo que fue compartido para considerarse en el presente Plan de Contingencia Informático, en la Tabla 3.44 se puede apreciar la coordinación operativa ante este tipo de riesgo que lleva la institución, mismo que será complementado con acciones necesarias para sobrellevar la emergencia.

RIESGO IDENTIFICADO	ACCIONES DE PRIMERA RESPUESTA	RESPONSABLES O DE APOYO EN LA PRIMERA RESPUESTA
LLUVIA DE CENIZA Y PIROCLASTOS	<b>Fase de prevención:</b> A través de cursos prácticos impartir conocimientos sobre erupciones volcánicas.	* DIRECCIÓN DE SEGURIDAD CIUDADANA Y UGR G.A.D. SALCEDO. * CUERPO DE BOMBEROS.
	<b>Fase de atención de la emergencia:</b> Recibir el aviso del IGM y asistir a los lugares donde existieron destrucción por la caída de ceniza.	* POLICIA NACIONAL. * ÁREA DE SALUD DE SALCEDO. * ECU 911. * SNGRE. Servicio Nacional de Gestión de Riesgos y Emergencias.
	<b>Fase de rehabilitación:</b> Evaluar daños en nuestra jurisdicción a causa de la caída de ceniza.	* CRUZ ROJA.

Tabla 3.44: Coordinación operativa en la atención de la emergencia (Lluvia de ceniza y piroclastos)

Fuente: Elaborado por el autor, a partir del Plan de contingencia cantonal ante una erupción del volcán Cotopaxi [45]

## ACTIVIDADES ANTES

### Medidas Humanas

- El equipo del Comité de Operaciones de Emergencia (C.O.E.) cantonal de Salcedo, cuenta con la señalética de emergencia y rutas de evacuación correspondiente a la municipalidad.
- Coordinar con a la UPC del cantón para brindar una capacitación y realizar simulacros preventivos a todo el personal incluido los directivos, ante una posible emergencia que llegue afectar la institución gravemente. Así mismo ejecutar programas de capacitación acerca del uso de elementos sobre seguridad y la manera correcta de dar primeros auxilios, a todo el personal de la municipalidad.

- Organizarse mediante la formación de equipos operativos para un mejor control y orden como se indica en el literal (3.2.7.5).
- El equipo del Comité de Operaciones de Emergencia (C.O.E.) cantonal de Salcedo, cuenta con la señalética de emergencia y rutas de evacuación correspondiente a la municipalidad.
- En cuanto a los equipos informáticos se debe seguir una serie de lineamientos y pólizas estipuladas por la municipalidad del cantón entre algunas mencionadas en el apartado (3.2.7.1) para estar prevenidos ante una emergencia de este tipo.
- Tener a la mano los números telefónicos de emergencia, los responsables de la activación de la emergencia, así como de los actores institucionales operativos como se muestra en las Tablas. 3.38, 3.39, 3.40, de esta manera tendremos comunicación directa con el personal de estas entidades y dar cualquier tipo de aviso y solicitar apoyo.
- Solicitar a la UPC del cantón brindar una capacitación a todo el personal incluido los directivos, ante un posible riesgo que llegue afectar la institución gravemente.
- Verificar si las ventanas tienen algún tipo de rotura o ranura que permita la entra de ceniza hacia las instalaciones.
- Dar un mantenimiento previo a las tejas del edificio antiguo de la municipalidad para que estas no colapsen en el caso de acumulación de ceniza en el techo.
- Ubicar un botiquín de primero auxilios en un lugar visible dentro de cada departamento de la institución.
- La institución debe contar con pólizas de seguros comerciales, que brinden un seguro a los activos informáticos como se menciona en el apartado (3.2.7.1) de los equipos informáticos.

### **Medidas Técnicas**

- Limpiar la caja exterior de los equipos informáticos con un trapo húmedo, o algún producto antipolvo.
- Realizar un mantenimiento periódico al interior de los equipos informáticos evitando la acumulación de polvo o ceniza en el interior ya que el polvo acumulado hace que disminuya la refrigeración de los componentes.

- Actualizar periódicamente el inventario de los equipos informáticos para tener un respaldo tanto para un correcto funcionamiento de las actividades como para el conocimiento de la institución de seguros que brinda el apoyo a la institución ante posibles desastres.
- Etiquetar los equipos informáticos acorde a su categoría en importancia de contenido y valor monetario que representa su pérdida como se menciona en el apartado (3.2.7.1) de los equipos informáticos.
- Elaborar un plan para la evacuación de hardware, que permita coordinar al los equipos operativos transportar los equipos informáticos a un sitio seguro en el menor tiempo posible, para esto se debe considerar su categoría en importancia de contenido y valor monetario que representa su pérdida (si la situación lo amerita y no representen riesgo de exponer la vida).
- Mantener de manera periódica Backus de los principales elementos de software necesarios para restablecer las actividades normales de la institución.
- La información con carácter crítico debe contar con una copia de seguridad en espejo (MIRROR BACKUP) en otro sitio alternativo, manteniendo así una copia exacta de los datos originales en caso de ocurrir un desastre.
- Mantener de manera periódica Backus de los principales elementos de software necesarios para restablecer las actividades normales de la institución, como se menciona en el apartado (3.2.7.3).
- Verificar que exista una correcta ventilación en el lugar que se encuentren los servidores y equipos informáticos verificando que se encuentren funcionando los ventiladores de enfriamiento del cuarto.

## **ACTIVIDADES DURANTE**

### **Medidas Humanas**

- Ante todo, se recomienda conservar la calma, ya que de esto repercute las acciones tomadas durante la emergencia.
- Mantener el uso de las mascarillas y gafas de protección mientras dure la emergencia y sea comunicado por las autoridades de la institución.

- Cerrar todas las ventanas y puertas de las oficinas, y colocar un aviso que se esta trabajando normalmente, mantenerse de esta manera hasta que dure la emergencia y sea comunicado por las autoridades de la institución.
- Al momento de realizar limpieza de los distintos departamentos tomar las medidas de precaución utilizando mascarillas y gafas de protección ya que este tipo de polvo volcánico puede ser perjudicial para la salud.
- Realizar la limpieza de los departamentos en horas no laborables por sus funcionarios.
- Si la caída de ceniza se mantiene es necesario evaluar la institución ante posibles colapsos del techo de la municipalidad.
- Cada departamento de la institución debidamente evacuado siempre manteniendo la calma, los jefes o encargados del área procederán a cerrar sus puertas y colocar una tela blanca en la entrada indicando que se evacuó facilitando así el trabajo de las brigadas de auxilio.
- En el refugio temporal es necesario registrarse y atender a las recomendaciones que se le indiquen.

### **Medidas Técnicas**

- Mantener las puertas del bastidor o rack cerradas para evitar el ingreso de polvo mientras dure la emergencia.
- Proteger a los equipos informáticos ante el ingreso de polvo o ceniza donde estos se encuentran ya que pueden causar graves daños a sus piezas internas.
- Realizar un mantenimiento periódico al interior de los equipos informáticos evitando la acumulación de polvo o ceniza en el interior ya que el polvo acumulado hace que disminuya la refrigeración de los componentes.
- Limpiar la caja exterior con un trapo húmedo, o algún producto antipolvo.
- Al limpiar el interior de los equipos se puede utilizar un spray antipolvo, mismos que no dañan los componentes electrónicos (hacerlo lejos de otros equipos ya que este polvo puede ir a parar a otros equipos cercanos).
- En los grupos formados previo a una emergencia en caso de una evacuación, se procederá a realizar las actividades encomendadas, (Sin que estas acciones representen riesgo de exponer la vida) entre ellas se encuentran:

- El primer equipo debe desconectar los servidores y equipos de red (OFF) en la caja principal de corriente.
- El segundo equipo se encarga del rescate de los principales equipos informáticos (servidores), trasladándolos a un lugar seguro, y así limitar los daños.
- El tercer equipo debe asegurarse de cerrar el acceso al departamento, asegurándose que no exista personal en su interior.

## **ACTIVIDADES DESPUÉS**

### **Medidas Humanas**

- Las autoridades del (COE) cantonal son los encargados de evaluar la situación de la institución en colaboración con los bomberos del cantón, y personal de seguridad, para declarar por finalizado la emergencia.
- Ya con los resultados del (COE) cantonal las autoridades de la municipalidad procederán a informar al personal que pueden retornar a su departamento de trabajo de manera segura.
- Realizar una reunión con las autoridades de la institución para hacer un recuento de los daños y tomar las medidas del caso.
- En caso de un daño severo de las instalaciones, trasladar las operaciones a otras oficinas alternas.
- Proceder al tramite pertinente de las garantías de los equipos afectados por el desastre, o a su vez comprar los equipos indispensables para retomar las operaciones.

### **Medidas Técnicas**

- Proteger a los equipos informáticos ante el ingreso de polvo o ceniza donde estos se encuentran ya que pueden causar graves daños a sus piezas internas.
- Realizar un mantenimiento preventivo o correctivo al interior de los equipos informáticos evitando la acumulación de polvo o ceniza en el interior.
- En el caso de avería en los equipos se procederá a recoger los Backups, programas, manuales del sitio alternativo en donde se encuentran resguardados.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.

- Brindar el soporte pertinente a la restauración para verificar y probar la integridad de los datos.
- Iniciar las operaciones, sin pasar por alto las medidas de seguridad establecidas por las políticas internas de la municipalidad.

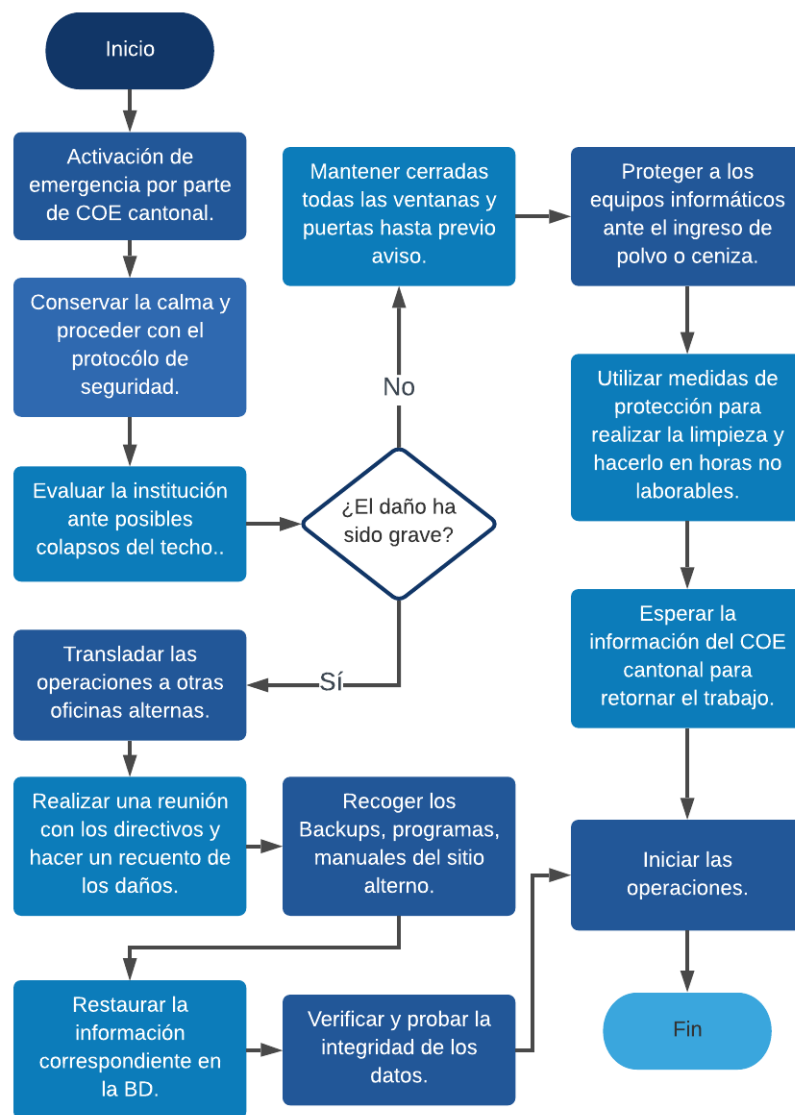


Figura 3.34: Acciones frente a la lluvia de ceniza y piroclastos  
Fuente: Elaborado por el autor

### **3.2.10.3. Clase de Riesgo: Sismos (volcánicos/repentinos)**

El cantón Salcedo está ubicado en la Cordillera Real de los Andes del Ecuador y se encuentra propenso a una alta incidencia sísmica, debido a que la placa Nazca se mueve a una velocidad relativa de 9 cm/año donde choca y luego se sumerja bajo la placa Sudamericana. La institución se encuentra propensa a este tipo de riesgos por lo que a continuación se muestran acciones que se deben tomar al materializarse este desastre.

## **ACTIVIDADES ANTES**

### **Medidas Humanas**

- Coordinar con a la UPC del cantón para brindar una capacitación y realizar simulacros preventivos a todo el personal incluido los directivos, ante una posible emergencia que llegue afectar la institución gravemente. Así mismo ejecutar programas de capacitación acerca del uso de elementos sobre seguridad y la manera correcta de dar primeros auxilios, a todo el personal de la municipalidad.
- Organizarse mediante la formación de equipos operativos para un mejor control y orden como se indica en el literal (3.2.7.5).
- El equipo del Comité de Operaciones de Emergencia (C.O.E.) cantonal de Salcedo, cuenta con la señalética de emergencia y rutas de evacuación correspondiente a la municipalidad.
- Tener a la mano los números telefónicos de emergencia, los responsables de la activación de la emergencia, así como de los actores institucionales operativos como se muestra en las Tablas. 3.38, 3.39, 3.40, de esta manera tendremos comunicación directa con el personal de estas entidades y dar cualquier tipo de aviso y solicitar apoyo.
- Ubicar un botiquín de primero auxilios en un lugar visible dentro de cada departamento de la institución.
- Colocar un extintor cargado en un lugar visible dentro del departamento donde están ubicados los servidores en la institución. De igual manera en todos los departamentos ubicar extintores debidamente cargados y en cuanto al personal capacitar sobre la manera correcta de uso.



- Al encontrarse dentro la zona de peligro sísmico se debe buscar un asesoramiento sobre cómo proceder y acatar las órdenes para precautelar la vida de quienes trabajan en la municipalidad.
- La institución debe contar con pólizas de seguros comerciales, que brinden un seguro a los activos informáticos como se menciona en el apartado (3.2.7.1) de los equipos informáticos.

### **Medidas Técnicas**

- Buscar asesoría de un ingeniero civil, arquitecto, para identificar sitios con mayor vulnerabilidad en la municipalidad y los más seguros para poder protegerse ante un riesgo de grandes dimensiones.
- Realizar revisiones periódicas, y reparar si fuera el caso, las instalaciones eléctricas y de gas si existiera y así mantenerlos en buen estado, capacitar el personal sobre como desconectar los suministros de electricidad y gas para evitar que el riesgo se pueda incrementar.
- Etiquetar los equipos informáticos acorde a su categoría en importancia de contenido y valor monetario que representa su pérdida, con el objetivo de dar prioridad en caso de evacuación por emergencia y salvaguardar el equipo sin que esto represente riesgo de exponer su vida.
- Actualizar periódicamente el inventario de los equipos informáticos para tener un respaldo tanto para un correcto funcionamiento de las actividades como para el conocimiento de la institución de seguros que brinda el apoyo a la institución ante posibles desastres.
- La información con carácter crítico debe contar con una copia de seguridad en espejo (MIRROR BACKUP) en otro sitio alternativo, manteniendo así una copia exacta de los datos originales en caso de ocurrir un desastre.
- Mantener de manera periódica Backus de los principales elementos de software necesarios para restablecer las actividades normales de la institución, como se menciona en el apartado (3.2.7.3).

## ACTIVIDADES DURANTE

### Medidas Humanas

- Ante todo, se recomienda conservar la calma, ya que de esto repercute las acciones tomadas durante la emergencia.
- No utilizar los ascensores, descender por las escaleras con las manos sobre la cabeza protegiéndose ante la caída de algún objeto, al descender pegarse a la pared en donde posee mayor resistencia, recuerde: No gritar, No empujar, No correr, y dirigirse a una zona de seguridad.
- Cada departamento de la institución debidamente evacuado siempre manteniendo la calma, los jefes o encargados del área procederán a cerrar sus puertas y colocar una tela blanca en la entrada indicando que se evacuó facilitando así el trabajo de las brigadas de auxilio.
- En el refugio temporal es necesario registrarse y atender a las recomendaciones que se le indiquen.

### Medidas Técnicas

- Apagar los equipos informáticos y desconectar los servidores y equipos de red (OFF) en la caja principal de corriente, (si la situación lo amerita y no representen riesgo de exponer la vida).
- En los grupos formados previo a una emergencia se procederá a realizar las actividades encomendadas, (Sin que estas acciones representen riesgo de exponer la vida) entre ellas se encuentran:
  - El primer equipo se encarga de combatir dicho siniestro como es desconectar el suministro eléctrico y de gas si existiera.
  - El segundo equipo se encarga del rescate de los principales equipos informáticos (servidores), trasladándolos a un lugar seguro, y así limitar los daños.
  - Un tercer equipo debe asegurarse de cerrar el acceso al departamento, asegurándose que no exista personal en su interior.

## ACTIVIDADES DESPUÉS

### Medidas Humanas

- Las autoridades del (COE) cantonal son los encargados de evaluar la situación de la institución en colaboración con los bomberos del cantón, y personal de seguridad, para declarar por finalizado la emergencia.
- Ya con los resultados del (COE) cantonal las autoridades de la municipalidad procederán a informar al personal que pueden retornar a su departamento de trabajo de manera segura.
- Realizar una reunión con las autoridades de la institución para hacer un recuento de los daños y tomar las medidas del caso.
- En caso de un daño severo de las instalaciones, trasladar las operaciones a otras oficinas alternas.
- Proceder al trámite pertinente de las garantías de los equipos afectados por el desastre, o a su vez comprar los equipos indispensables para retomar las operaciones.

### Medidas Técnicas

- Identificar los principales equipos informáticos afectados para su pronto reemplazo.
- Se debe hacer un testeo de la infraestructura de la red para verificar cualquier tipo de avería causada por la emergencia.
- Recoger los Backups, programas, manuales del sitio alterno en donde se encuentran resguardados.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.
- Brindar el soporte pertinente a la restauración para verificar y probar la integridad de los datos.
- Iniciar las operaciones, sin pasar por alto las medidas de seguridad establecidas por las políticas internas de la municipalidad.

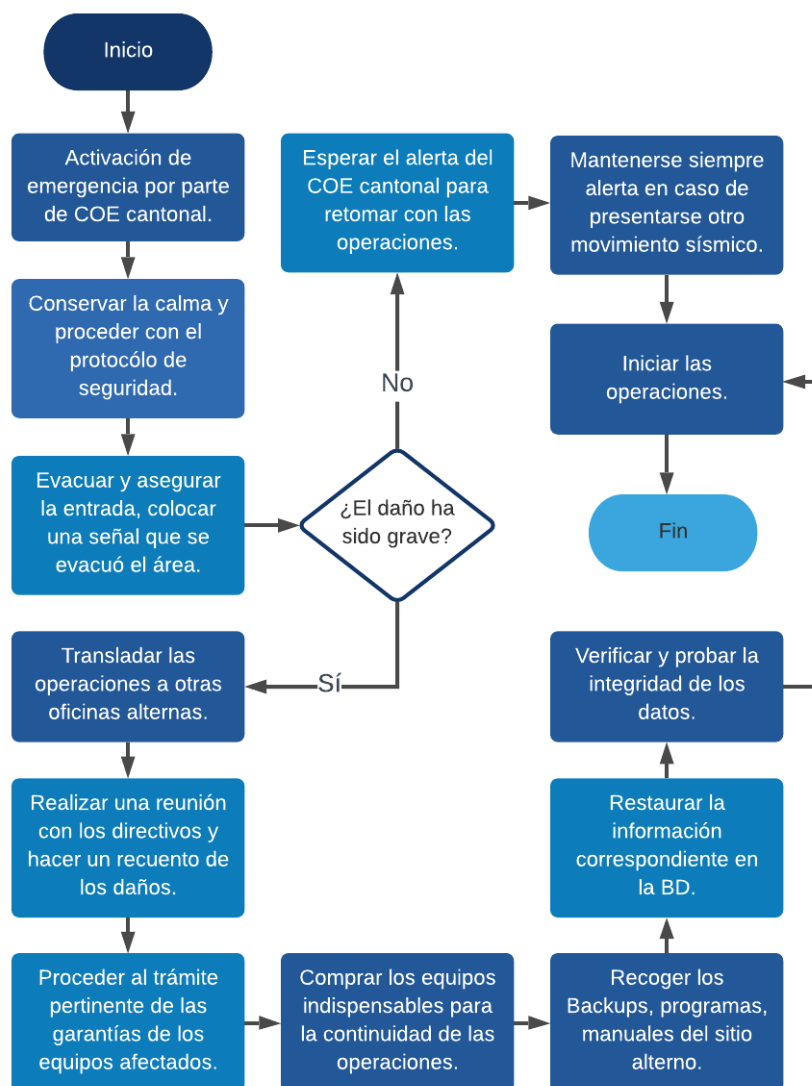


Figura 3.35: Acciones frente a sismos volcánicos o repentinos

Fuente: Elaborado por el autor

#### 3.2.10.4. Clase de Riesgo: Interrupción del servicio de energía eléctrica

La instalación eléctrica representa un factor importante para el funcionamiento y seguridad de los equipos informáticos, una mala instalación podría provocar fallas frecuentes, cortos circuitos y causar que se quemen los equipos interrumpiendo la operatividad de la institución. A pesar de que la Empresa Eléctrica Provincial de Cotopaxi, trabaja arduamente para mantener un servicio sin interrupciones se debe considerar las siguientes actividades para una correcta coordinación en la institución en caso de suscitarse un corte del servicio eléctrico:

## ACTIVIDADES ANTES

### Medidas Humanas

- El personal de la municipalidad debe utilizar una línea independiente para servicios, ya sea para limpieza o cualquier otro trabajo (aspiradora, taladro, pulidora, etc.), dentro del departamento de TI y sus áreas próximas a este involucra no conectar estos dispositivos en la misma línea eléctrica que utiliza los componentes informáticos y evitar perturbaciones electromagnéticas que pudieran ocasionar, afectando el trabajo que realizan los servidores, computadores, equipos de red.
- Tener a la mano los números telefónicos de la Empresa Eléctrica Provincial de Cotopaxi, para solicitar una pronta solución en caso de ocurrir un corte del servicio eléctrico.

### Medidas Técnicas

- Verificar que la instalación eléctrica para el departamento de TI sea un circuito exclusivo tomado de la sub-estación o acometida desde el punto de entrega de la empresa eléctrica distribuidora.
- Se debe construir una toma a tierra física exclusiva para el departamento de TI, misma que se conecte mediante un cable con cubierta aislante al centro de carga del departamento de TI.
- Como medida de seguridad se deberá instalar en un lugar próximo a la puerta un control para suspender la energía a todo el equipo informático del departamento, para cualquier situación de emergencia, mismo que deberá estar correctamente señalizado.
- El espacio donde se encuentra el control de interruptores debe encontrarse libre de obstáculos para una fácil operación.
- La protección contra casos como golpes de tensión (exceso de corriente eléctrica en un instante), ya sea por un mal servicio de la red eléctrica, o por ejemplo la caída de un rayo, se debe utilizar interruptores electromagnéticos que protejan los equipos interrumpiendo el paso de la corriente cuando detecte algún problema.
- Todos los interruptores deben estar correctamente rotulados para una correcta operación por parte del personal respetable.

- Es indispensable proteger de fallas de energía eléctrica y evitar pérdidas de información por un apagado imprevisto en el que algún trabajo se estaba realizando y no pudo ser guardado, para esto se requiere un UPS que abastezca eléctricamente a cada equipo informático dándole el tiempo necesario para guardar cualquier tipo de información.
- Asegurarse de que los equipos informáticos dentro del departamento de TI así como en los demás departamentos de la institución cuenten con un UPS debidamente funcionando y conectados a los equipos.
- Utilizar conexiones a contactos polarizados 125 VCA, y utilizar con un estándar de código de colores:
  - **FASE:** Negro, rojo, o azul.
  - **NEUTRO:** Blanco o gris.
  - **TIERRA FÍSICA:** Verde.

## **ACTIVIDADES DURANTE**

### **Medidas Humanas**

- Si los equipos informáticos se encuentran conectados a sus correspondientes UPS, se procede a almacenar la información que se estaba trabajando y posteriormente apagar los equipos de manera correcta mientras la energía eléctrica regresa.
- En el caso en que la suspensión sea de manera general en el sector, comunicarse con la institución que brinda el servicio eléctrico y notificar lo sucedido para que den solución al conflicto con la brevedad posible.
- Se recomienda aprovechar el tiempo mientras dure el corte de energía, realizando otras actividades como son entrega o firma de documentos.
- Mantenerse informado por las autoridades de la institución sobre si ya se puede retomar las operaciones normalmente.

### **Medidas Técnicas**

- Si el problema se presenta en una determina área un técnico capacitado verificará el daño y procederá con la reparación respectiva.

- Personal del departamento de TI, procederá a guardar el trabajo que se haya estado realizando y apagar los equipos informáticos de manera correcta como son los servidores, equipos de red, computadores, etc, mientras regrese la energía eléctrica o el daño sea solventado.

## **ACTIVIDADES DESPUÉS**

### **Medidas Humanas**

- Realizar una reunión con las autoridades de la institución para hacer un recuento de la pérdida que ocasionó la falla del suministro eléctrico y de acuerdo al tiempo que se dejó de laborar.
- En el caso de existir algún equipo con avería luego del corte de energía eléctrica notificar al departamento de TI el incidente.

### **Medidas Técnicas**

- Si el daño fue interno el técnico capacitado en el área que revisó y reparó la avería del suministro eléctrico deberá informar a las autoridades de la institución cual fue dicho problema para en lo posterior evitar este tipo de incidentes.
- El equipo técnico del departamento de TI, procederá a reanudar la operatividad de los equipos informáticos como son los servidores, equipos de red, computadores, etc.
- Se realizará una verificación del normal funcionamiento de los equipos informáticos.
- Realizar una verificación detenida sobre cada uno de los sistemas informáticos una vez reiniciado sus procesos.

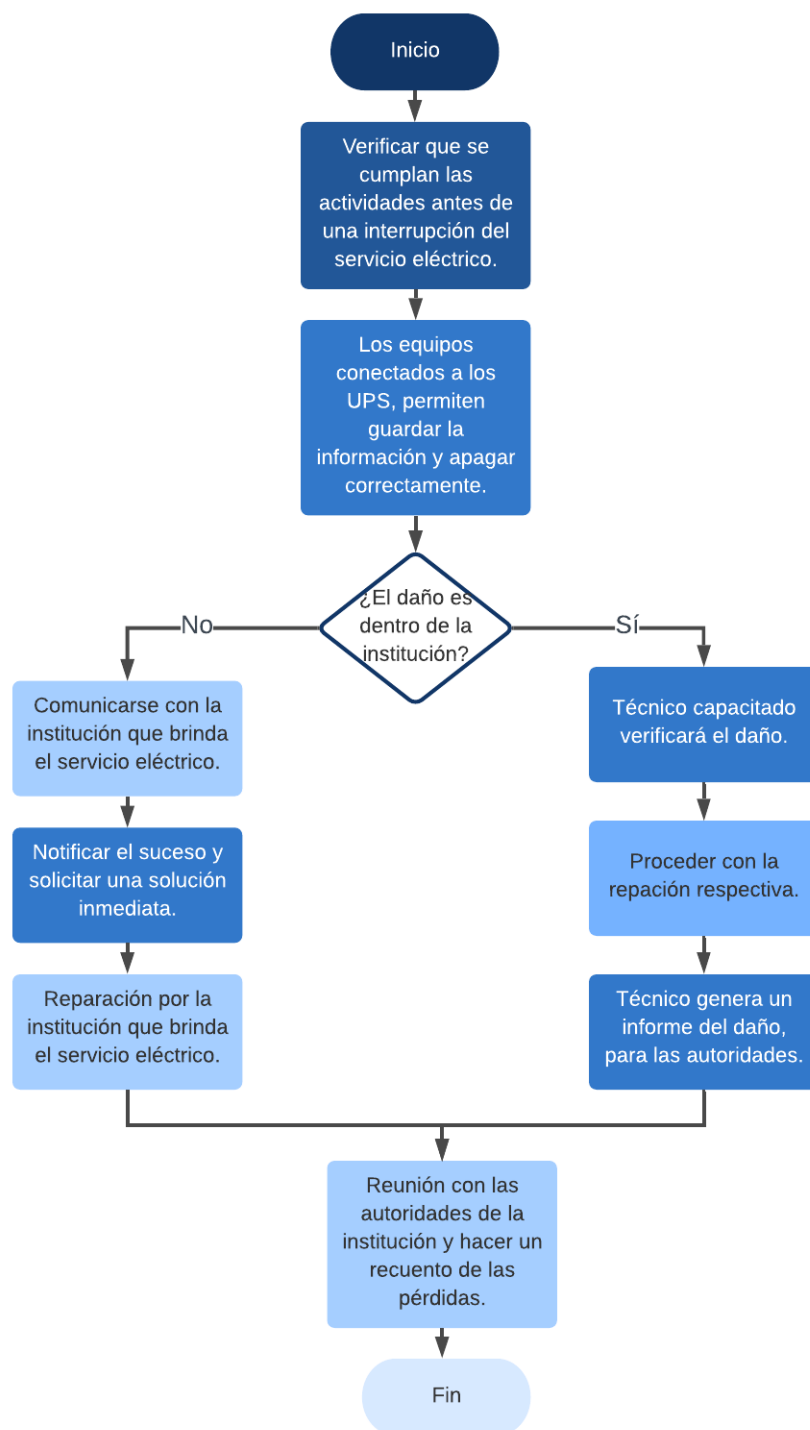


Figura 3.36: Acciones frente a la interrupción del servicio de energía eléctrica  
 Fuente: Elaborado por el autor



### **3.2.10.5. Clase de Riesgo: Filtración de agua**

Lamentablemente hay una gran probabilidad de sufrir inundaciones debido a lluvias que ocurren en épocas de invierno donde pueden ocasionar estragos en construcciones con techos de material rustico como es el caso de la municipalidad.

## **ACTIVIDADES ANTES**

### **Medidas Humanas**

- Los interruptores en medida de lo posible deberán estar instalados a una altura razonable.
- Verificar que las conexiones de las mangueras de flujo de agua se encuentren debidamente conectadas a los servicios higiénicos donde es importante evitar alguna filtración de agua que podría ocasionar problemas en los equipos informáticos.
- Verificar y reemplazar las mangueras de flujo de agua en caso de presentarse algún tipo de agrietamiento.
- Se recomienda contar con un contratista de techos capacitado que verifique y repare el techo deteriorado o dañado en caso de estarlo.

### **Medidas Técnicas**

- Para evitar este tipo de inconvenientes la filtración de agua e inundaciones se recomienda ubicar los servidores a una altura de 50 cm.
- Las canaletas, aleros y bajantes deben encontrarse libres de algún obstáculo que interrumpa el libre desagüe del agua, dichos bajantes deben estar ubicados lejos del edificio y evitar daños a los cimientos, que pueden ser afectados por el exceso de agua.
- Verificar que no exista alguna grieta en el contorno de las ventanas, ya que permiten el ingreso de agua de las lluvias hacia las oficinas donde están ubicados los servidores y equipos de red que pueden sufrir cortocircuitos en el caso de contacto con el cableado eléctrico, interruptores cerca de las ventanas.
- La información con carácter crítico debe contar con una copia de seguridad en espejo (MIRROR BACKUP) en otro sitio alterno, manteniendo así una copia exacta de los datos originales en caso de ocurrir un desastre.

- Mantener de manera periódica Backus de los principales elementos de software necesarios para restablecer las actividades normales de la institución, como se menciona en el apartado (3.2.7.3).

## **ACTIVIDADES DURANTE**

### **Medidas Humanas**

- Las autoridades deben comunicarse con un técnico capacitado en solvente la filtración de agua que repare el daño con la brevedad posible.
- Comunicar el incidente a las respectivas autoridades de la institución, para que el problema sea solventado a la brevedad posible.

### **Medidas Técnicas**

- Apagar los equipos informáticos y desconectar los servidores y equipos de red (OFF) en la caja principal de corriente, (si la situación lo amerita y no representen riesgo de exponer la vida).
- Mover de inmediato los equipos informáticos y demás equipos electrónicos a un lugar seguro ya que pueden causar un cortocircuito al encontrarse expuesto a una filtración de agua.

## **ACTIVIDADES DESPUÉS**

### **Medidas Humanas**

- Las autoridades de la institución deben dar la orden para reanudar las actividades.
- Realizar una reunión con los directivos para hacer un recuento de los daños materiales si fuera el caso.
- Proceder al trámite pertinente de las garantías de los equipos afectados por el incidente, o a su vez comprar los equipos indispensables para retomar las operaciones.

### **Medidas Técnicas**

- El técnico capacitado que revisó y reparó la avería de la filtración de agua deberá informar a las autoridades de la institución cual fue dicho problema para en lo posterior evitar este tipo de incidentes.

- El equipo técnico del departamento de TI, procederá a reanudar la operatividad de los equipos informáticos como son los servidores, equipos de red, computadores, etc.
- Se realizará una comprobación del normal funcionamiento de los equipos informáticos.
- Realizar una verificación detenida sobre cada uno de los sistemas informáticos una vez reiniciado sus procesos.

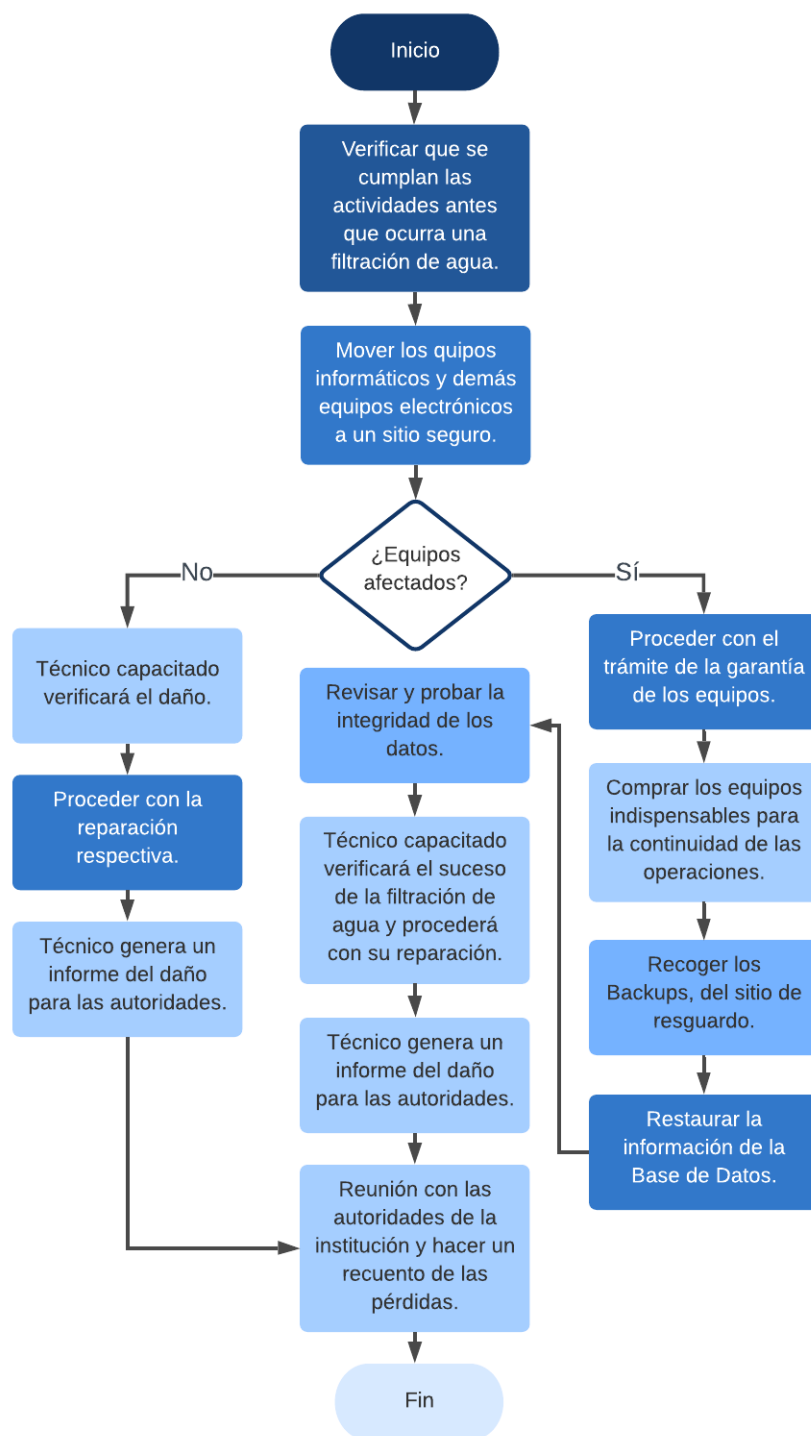


Figura 3.37: Acciones frente a una filtración de agua  
 Fuente: Elaborado por el autor

### 3.2.10.6. Clase de Riesgo: Incendio

#### ACTIVIDADES ANTES

##### Medidas Humanas

- El equipo del Comité de Operaciones de Emergencia (C.O.E.) cantonal de Salcedo, cuenta con la señalética de emergencia y rutas de evacuación correspondiente a la municipalidad.
- Coordinar con a la UPC del cantón para brindar una capacitación y realizar simulacros preventivos a todo el personal incluido los directivos, ante una posible emergencia que llegue afectar la institución gravemente. Así mismo ejecutar programas de capacitación acerca del uso de elementos sobre seguridad y la manera correcta de dar primeros auxilios, a todo el personal de la municipalidad.
- Ubicar un botiquín de primero auxilios en un lugar visible dentro de cada departamento de la institución.
- Colocar un extintor en un lugar visible dentro de cada departamento de la institución y capacitar debidamente al personal sobre la manera correcta de uso.
- Verificar periódicamente la fecha de caducidad de los extintores.
- Está prohibido fumar dentro de institución ya que puede provocar un incendio.
- No dejar al alcance de terceras personas productos inflamables.
- Por ninguna circunstancia tener derramado agua en los distintos departamentos, se debe tener en cuenta que el agua es un buen conductor de energía eléctrica.
- Si se manifiesta cualquier tipo de anomalía en las instalaciones eléctricas, notificar de manera inmediata a Seguridad de la municipalidad.
- Es necesario tener siempre un área de trabajo limpia y ordenada, ya que no hacerlo podría provocar la caída de sustancias líquidas en equipos electrónicos y causar incendios.

- La institución debe contar con pólizas de seguros comerciales, que brinden un seguro a los activos informáticos como se menciona en el apartado (3.2.7.1) de los equipos informáticos.

### **Medidas Técnicas**

- En el departamento de TI, no se cuenta con la instalación de sistemas de detección de humo y aspersión automática en el cuarto de servidores y comunicaciones, por lo que sería factible coordinar su implementación.
- Verificar periódicamente que las instalaciones eléctricas estén en buen estado, evitando así posibles cortocircuitos.
- En el departamento de TI, las paredes deben estar recubiertas con pintura especializada contra la propagación del fuego, esto contribuye a reducir la gravedad de los daños.
- No exceder las conexiones en contactos múltiples, evitar sobrecargar los circuitos eléctricos.
- Se debe construir una toma a tierra física exclusiva para el departamento de TI, misma que se conecte mediante un cable con cubierta aislante al centro de carga del departamento de TI.
- Como medida de seguridad se deberá instalar en un lugar próximo a la puerta un control para suspender la energía a todo el equipo informático del departamento, para cualquier situación de emergencia, mismo que deberá estar correctamente señalizado.

## **ACTIVIDADES DURANTE**

### **Medidas Humanas**

- Ante todo, se recomienda conservar la calma, ya que de esto repercute las acciones tomadas durante la emergencia.
- Si el fuego todavía es controlable, utilizar los conocimientos adquiridos en las capacitaciones sobre el uso del extintor, quitar el seguro para proceder a sofocar el fuego, si el fuego es de una magnitud considerable solicitar apoyo.
- Si el fuego está fuera de control, comunicarse con el departamento de bomberos del cantón y proceder de inmediato con la evacuación del inmueble acogiéndose a las medidas de seguridad ante este tipo de emergencia.

- No utilizar los ascensores, descender por las escaleras, pegados a la pared en donde posee mayor resistencia, recuerde: No gritar, No empujar, No correr, y dirigirse a una zona de seguridad.
- En el caso de encontrarse atrapado por el incidente y hay mucho humo, mantenerse al ras del piso, cubriendo la boca y nariz si tiene agua a su alcance remojar un pañuelo y respirar a través de este, intente trasladarse a pisos superiores mientras llegue el ayuda.
- Si es posible y está a su alcance de hacerlo mojar la ropa, ya que ayuda a evitar quemaduras.
- Al momento de abrir las puertas verificar si estas están calientes, en el caso de estarlas buscar otra salida.
- Las personas que se hallen en los últimos pisos procederán abrir las ventanas permitiendo que el humo salga liberando el ambiente, así como las escaleras para que tanto el personal de rescate como personas atrapadas en el edificio no se asfixien.

### **Medidas Técnicas**

- En ese momento del incendio, cualquier actividad que se esté realizando en los equipos informáticos, se deberá (si la situación lo amerita y no representen riesgo de exponer la vida) “Apagar los equipos” y desconectar los Servidores y equipos de red (OFF) en la caja principal de corriente.
- En los grupos formados previo a una emergencia se procederá a realizar las actividades encomendadas, (Sin que estas acciones representen riesgo de exponer la vida) entre ellas se encuentran:
  - El primer equipo se encarga de combatir dicho siniestro con el uso del extintor para tratar de sofocar el fuego.
  - El segundo equipo se encarga del rescate de los principales equipos informáticos (servidores), trasladándolos a un lugar seguro, y así limitar los daños.
  - Un tercer equipo debe asegurarse de cerrar el acceso al departamento afectado para evitar se propague el fuego, asegurándose que no exista personal en su interior.

## ACTIVIDADES DESPUÉS

### Medidas Humanas

- Retirarse de manera inmediata del área de incendio ya que esta puede desplomarse y presenta un gran peligro, dirigirse a una zona segura externa y esperar las indicaciones de las autoridades.
- No obstruir las labores del personal especializado, dejar que los profesionales que encarguen de apagar el fuego.
- Un personal especializado verificará la estructura física del inmueble afectado y emitirá un informe sobre las condiciones sobre si este puede ser utilizado normalmente.
- Personal de la municipalidad realizará una reunión con los directivos para hacer un recuento de los daños, en el se emitirá un informe al jefe del departamento de TI, que pueda tomar las medidas correctivas del caso.
- Proceder al trámite pertinente de las garantías de los equipos afectados por el desastre, o a su vez comprar los equipos indispensables para retomar las operaciones.

### Medidas Técnicas

- Personal del departamento de TI, realizará un análisis detenido sobre las posibles causas que originaron el incendio para actualizar así el plan de contingencia y adjuntar las nuevas medidas para prevenir.
- Se procederá a realizar un inventario sobre los equipos informáticos afectados por el incidente y proceder con su reemplazo respectivo, con la brevedad posible.
- El equipo técnico del departamento de TI, procederá a reanudar la operatividad de los equipos informáticos como son los servidores, equipos de red, computadores, etc.
- Se realizará una comprobación del normal funcionamiento de los equipos informáticos.
- Realizar una verificación detenida sobre cada uno de los sistemas informáticos una vez reiniciado sus procesos.



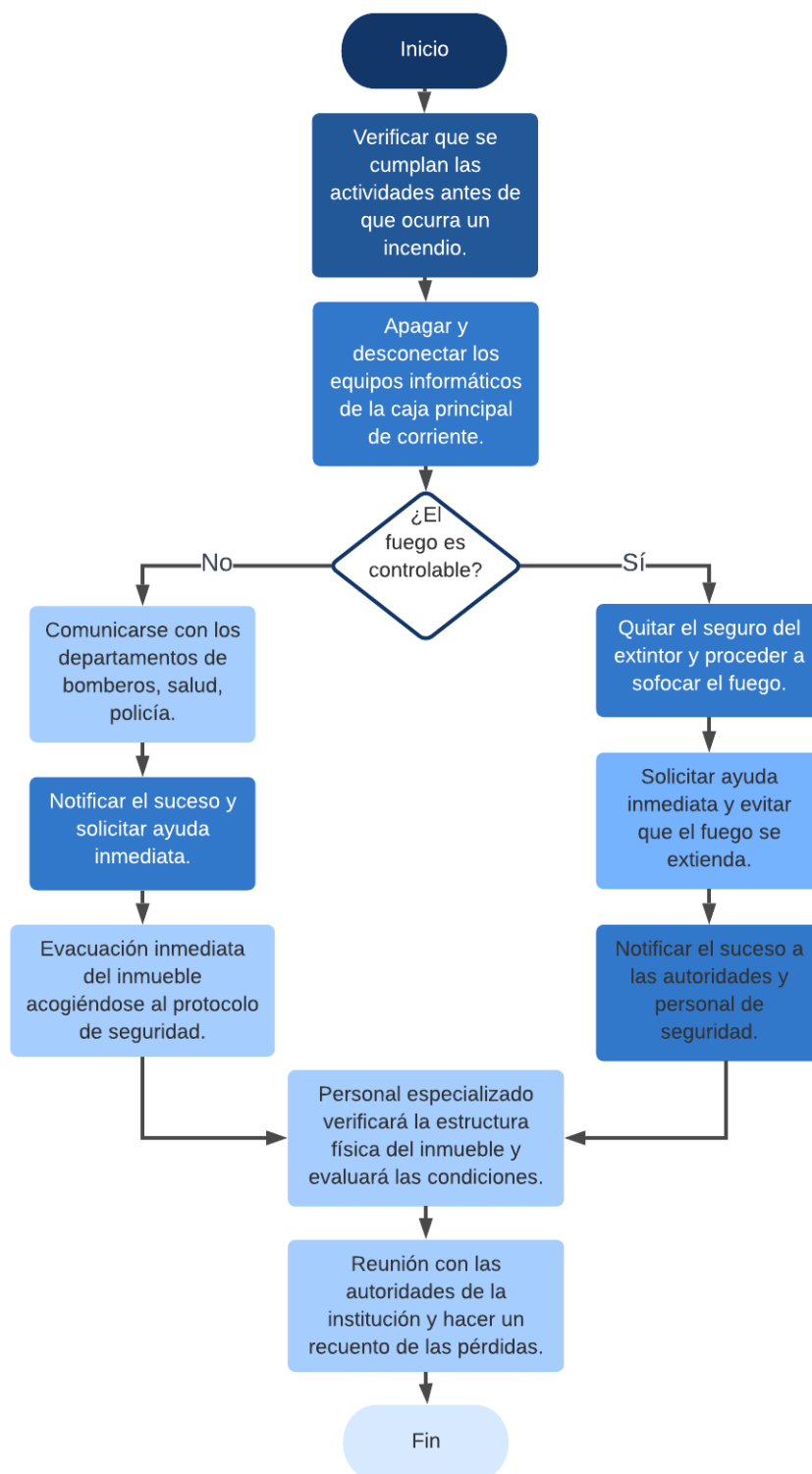


Figura 3.38: Acciones frente a un incendio  
 Fuente: Elaborado por el autor

### **3.2.10.7. Clase de Riesgo: Daño en el ventilador**

El ventilador es un componente electrónico interno de los equipos informáticos que ayuda a mantener una temperatura ideal y así evitar un sobrecalentamiento, dado a que, dentro de una PC, laptops, Servidores, generan altas temperaturas en sus componentes, el daño de estos componentes es muy frecuente dado a la falta de mantenimiento del hardware.

## **ACTIVIDADES ANTES**

### **Medidas Técnicas**

- Realizar una limpieza preventiva en los ventiladores de los equipos informáticos, ya que la acumulación de polvo en los componentes electrónicos siempre se lo encontrará.
- Verificar que los equipos informáticos se mantengan en un área despejada y remover cualquier obstáculo que impida el correcto flujo de aire.
- Mantener cerradas las carcasas de las computadoras, servidores, en todo momento para evitar el ingreso de polvo.
- No mantener abierta la puerta del cuarto frío donde se encuentren los servidores.
- En cuanto al sistema de refrigeración del cuarto frío del departamento de TI, se debe realizar un mantenimiento preventivo periódico para que equipo de ventilación se encuentre funcionamiento adecuadamente.

## **ACTIVIDADES DURANTE**

### **Medidas Humanas**

- Si el personal de los diferentes departamentos, nota algún ruido extraño dentro del computador, o el equipo se está reiniciando, debe apagar el equipo y comunicarse con el departamento de TI para notificar el problema.

### **Medidas Técnicas**

- Al notar un ruido fuerte al encender el equipo puede tratarse de una falla en el ventilador.
- Si el equipo empieza apagarse de manera repentina simultáneamente puede ser un signo de que el ventilador este fallando.

- Si observa que las aspas del ventilador no se encuentran en movimiento definitivamente el ventilador ha dejado de funcionar.
- Para realizar cualquier tipo de chequeo por parte del técnico del departamento de TI, es importante utilizar una manilla antiestática y evitar daños en los componentes internos de los equipos.
- El técnico verificará si hay obstrucciones en los ventiladores o los orificios de ventilación.
- El técnico deberá verificar que el cable de alimentación se encuentre conectado al ventilador de la placa base.
- El técnico revisará si el ventilador dejó de funcionar, ya que estos cumplen con un tiempo de uso.
- El técnico verificará si los controladores de dispositivos y BIOS se encuentran desactualizados.

## **ACTIVIDADES DESPUÉS**

### **Medidas Técnicas**

- Liberar la acumulación de polvo en los orificios o en los ventiladores.
- Luego de un chequeo y no obtener resultados proceder con el cambio del ventilador.
- Proceder al trámite de identificación del tipo de ventilador y generar una petición a quien corresponda para su adquisición.
- Verificar que ventilador adquirido sea la indicado.
- Proceder con el cambio del ventilador utilizando medidas de seguridad.
- Emitir un informe del daño que se solvento al jefe del departamento de TI.

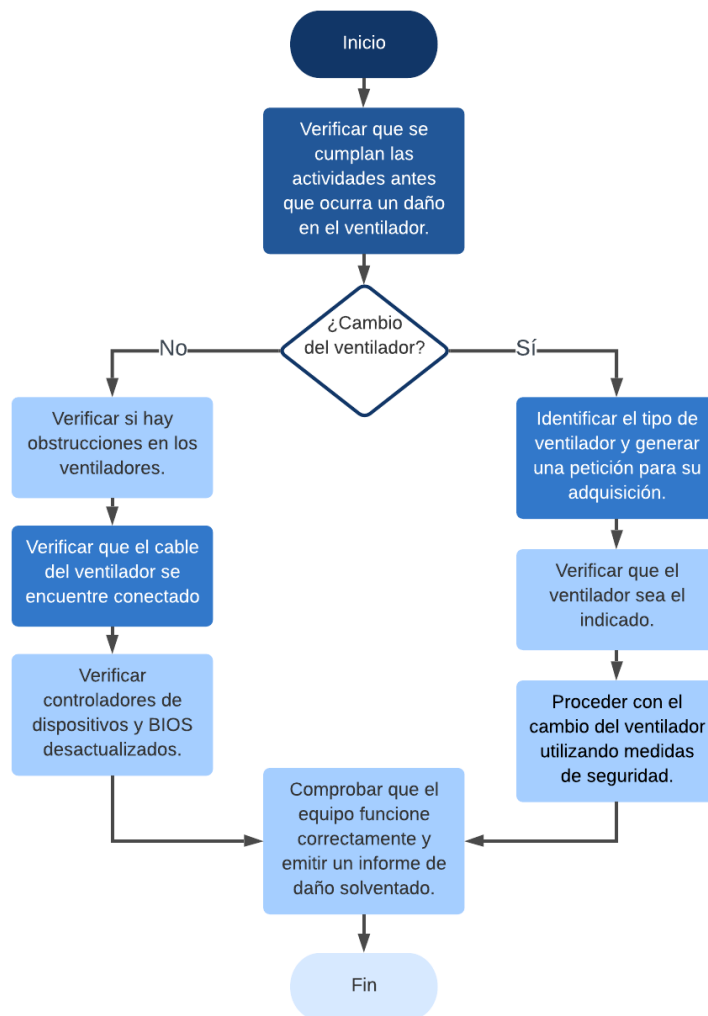


Figura 3.39: Acciones frente a un daño de ventilador.  
Fuente: Elaborado por el autor

### **3.2.10.8. Clase de Riesgo: Daño en la fuente de poder**

#### **ACTIVIDADES ANTES**

##### **Medidas Humanas**

- Si observa la presencia de cucarachas u otro tipo de insectos cerca del departamento de TI, o en sus demás departamentos de la municipalidad, de preferencia comunicarse con un experto en control de plagas para que fumigue el lugar (estos insectos pueden ingresar a los equipos y ocasionar daños).

##### **Medidas Técnicas**

- Cuando se realice un mantenimiento del equipo por parte del técnico del departamento de TI de la municipalidad, se debe también sopletear la fuente de poder con aire comprimido, y de esta manera evitar la acumulación de polvo.
- Asegurarse de tener la conexión con tierra física en los tomacorrientes que se está utilizando y evitar una sobretensión, en el caso de no tenerlo comunicarse con un electricista capacitado.
- Verificar que no se encuentren obstruidas las entrada de aire al ventilador de la fuente o del CPU, ya que al estar cubiertos de algún modo, es el motivo por la cual se calientan y llegan a quemarse.

#### **ACTIVIDADES DURANTE**

##### **Medidas Técnicas**

- Para realizar cualquier tipo de chequeo por parte del técnico del departamento de TI de la municipalidad, es importante utilizar una manilla antiestática y evitar daños en los componentes internos de los equipos.
- Si el computador se reinicia constantemente es necesario verificar si el ventilador de la fuente de poder se encuentre fallando, recalentando sus componentes y provocando inestabilidad al equipo.
- El técnico capacitado verificará los voltajes de la fuente de poder de sus conectores en el caso de encontrar alguna anomalía, es necesario hacer un chequeo más interno (condensadores en mal estado).

- En el caso que el equipo no encienda y no se muestre ninguna actividad eléctrica el técnico capacitado deberá verificar los voltajes de la fuente, revisar un chequeo más interno (revisar si el fusible está en mal estado, si es así cambiarlo).
- El técnico deberá verificar si la fuente de poder funciona en otro equipo en buen estado, al no detectar problemas en la fuente puede tratarse de un problema en la tarjeta madre.

## **ACTIVIDADES DESPUÉS**

### **Medidas Técnicas**

- Luego de un chequeo técnico proceder con su reparación o cambio de la fuente de poder.
- Proceder al trámite de identificación del tipo de fuente de poder y generar una petición a quien corresponda para su adquisición.
- Verificar que la fuente de poder adquirida sea la indicado.
- Proceder con el cambio de la fuente de poder utilizando medidas de seguridad.
- Emitir un informe del daño que se solvento al jefe del departamento de TI.

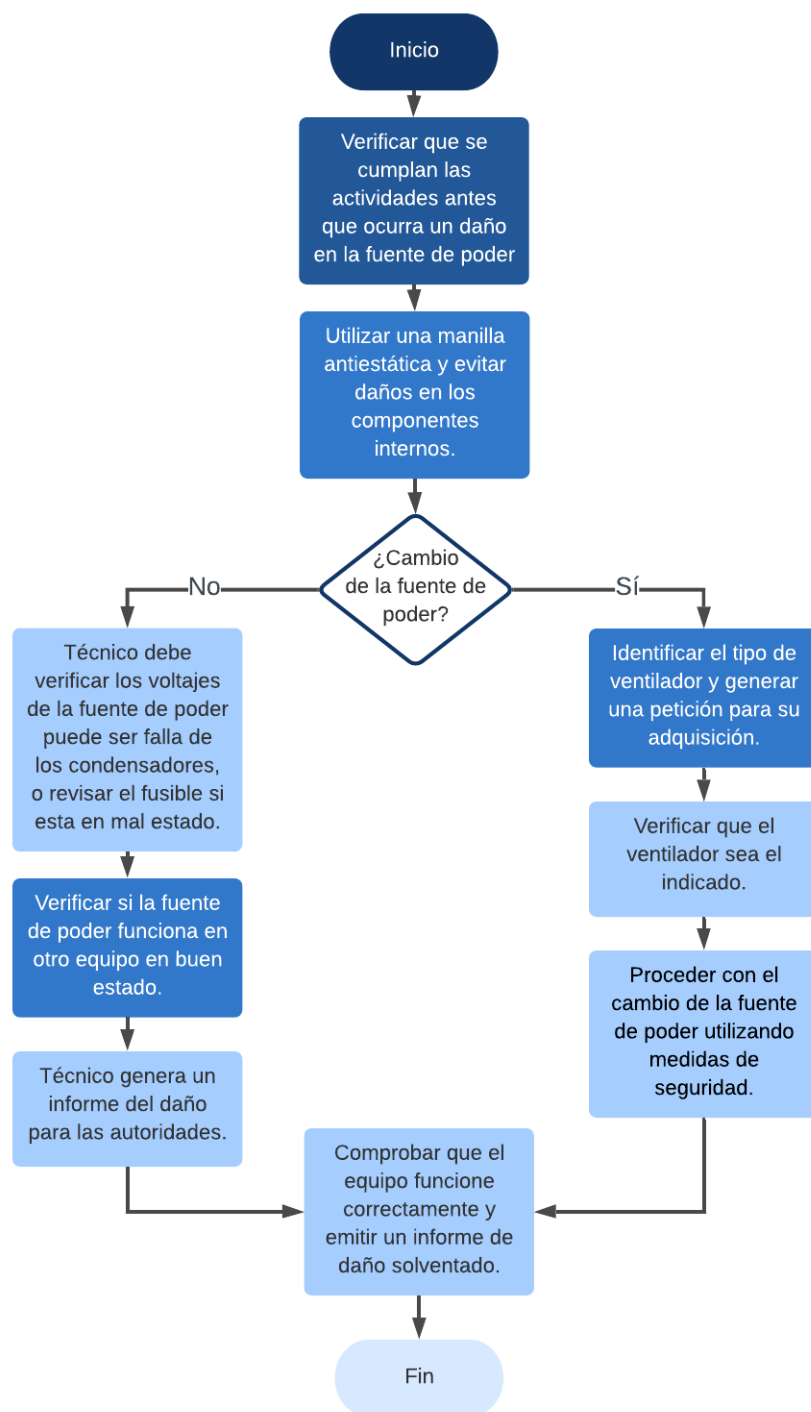


Figura 3.40: Acciones frente a un daño de la fuente de poder  
Fuente: Elaborado por el autor

### **3.2.10.9. Clase de Riesgo: Falla de disco duro SATA/IDE**

Este dispositivo es muy importante ya que en este se almacena información de vital importancia, los discos duros se han ido actualizando a través de los tiempos pueden ser IDE (los más antiguos) o SATA (los más nuevos), en ambas tecnologías giran los discos y tienen lecturas con un cabezal, la diferencia entre ellos es la transferencia de datos, favoreciendo a la tecnología SATA demostrando ser bastante más rápidos.

## **ACTIVIDADES ANTES**

### **Medidas Técnicas**

- El técnico capacitado si va a realizar un mantenimiento preventivo a los equipos es importante comprobar que el disco duro se encuentre correctamente sujetado y libre de suciedad y polvo acumulado.
- Se debe tener mucho cuidado de no golpear los equipos informáticos en caso de trasladarlos a otra área ya que podría estropearse el disco duro.
- Se debe verificar que el espacio de memoria libre en el disco no sea inferior al 10 % de su capacidad total, por lo que se recomienda sacar Backups de la información.
- La fragmentación en el disco duro puede hacerse notable al pasar el tiempo y su uso cotidiano por lo que es necesario desfragmentar el disco en su totalidad, este proceso puede tardar un tiempo considerable, por lo que se recomienda no hacerlo en horas laborables.
- Eliminar los archivos innecesarios de los equipos donde se generan archivos temporales, esto hace que los equipos procesen la información de manera lenta.



## **ACTIVIDADES DURANTE**

### **Medidas Técnicas**

- El técnico debe verificar que el disco duro se encuentre debidamente conectado y libre de polvo y suciedad.
- Luego de hacer un chequeo rápido del problema se procederá a probar el equipo si funciona con normalidad.
- El técnico capacitado luego del chequeo rápido debe proceder con la técnica de mantenimiento del disco duro utilizando sus conocimientos y retomar la operatividad del equipo averiado.

## **ACTIVIDADES DESPUÉS**

### **Medidas Técnicas**

- Proceder al trámite de identificación del tipo de disco duro y generar una petición a quien corresponda para su adquisición.
- Verificar que el disco duro adquirido sea el indicado.
- Proceder con el cambio del disco duro utilizando medidas de seguridad.
- Recoger los Backups, programas, manuales del sitio alterno en donde se encuentran resguardados.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.
- Brindar el soporte pertinente a la restauración para verificar y probar la integridad de los datos.
- Entrega del equipo informático por parte del técnico capacitado.
- Emitir un informe del daño que se solventó al jefe del departamento de TI.

## **Error físico de Disco duro de un Servidor (Sin RAID)**

La falla de un disco duro es un caso crítico, como puede presentarse el caso de no poder repararlo, es necesario tomar las siguientes acciones:

- Identificar el disco duro con la falla o avería.
- Se debe enviar mensajes a los usuarios que deben salir del sistema, se puede hacer uso de mensajes por red y comunicar a los jefes de cada departamento que lo informen con los miembros de cada área.
- Se debe deshabilitar la entrada al sistema para que el personal no reintente su ingreso.
- Se procederá a dar de baja el sistema y apagar el equipo que presenta el problema.
- Retirar el disco duro averiado utilizando medidas de seguridad.
- Proceder al trámite de identificación del tipo de disco duro y generar una petición a quien corresponda para su adquisición.
- Verificar que el disco duro adquirido sea el indicado.
- Proceder con el cambio del disco duro utilizando medidas de seguridad, formatearlo y realizar la partición correspondiente según se necesite.
- Recoger el último Backup, programas, manuales del sitio alternativo en donde se encuentran resguardados.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas, desde esa fecha a la actualidad.
- Brindar el soporte pertinente a la restauración para verificar y probar la integridad de los datos.
- Verificar el correcto estado de los sistemas.
- Habilitar las entradas al sistema al personal de los distintos departamentos de la institución.

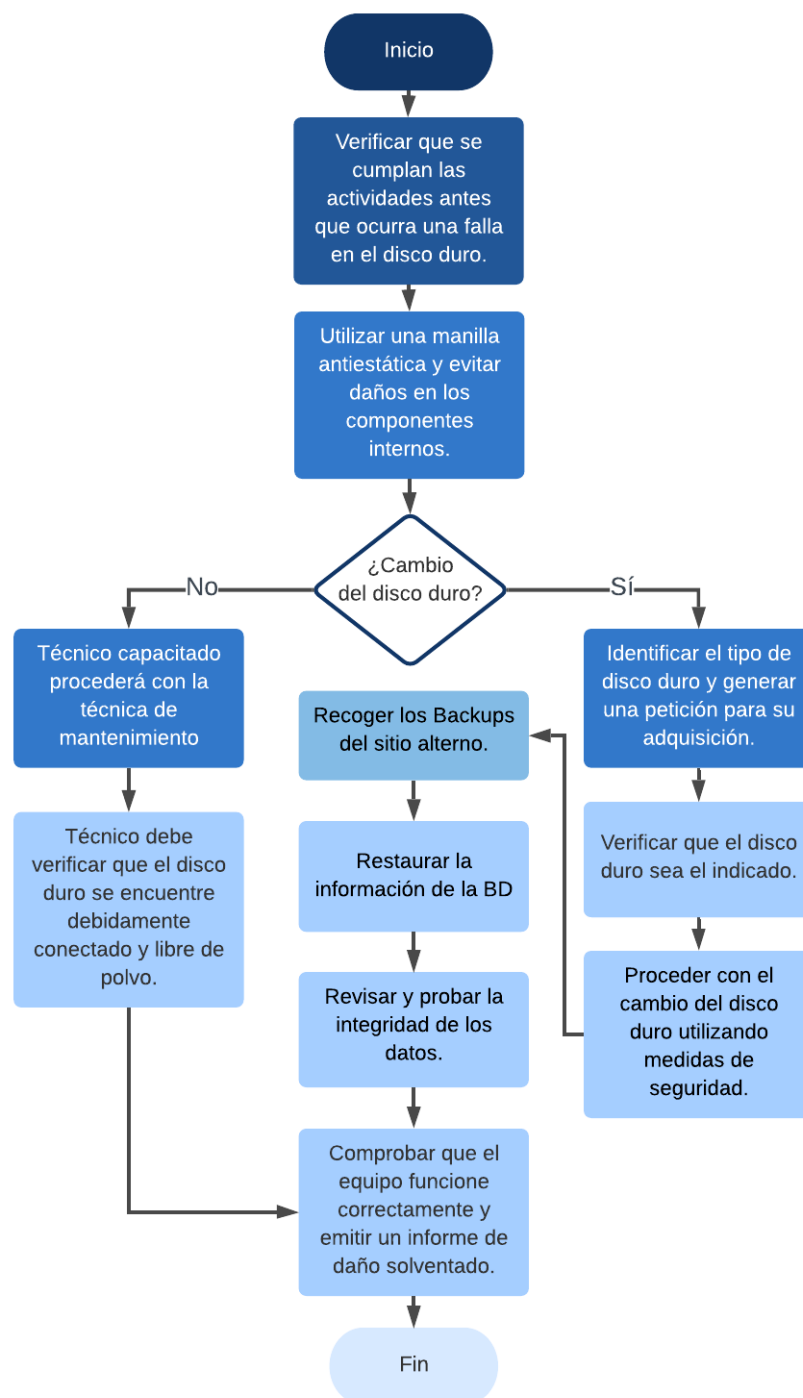


Figura 3.41: Acciones frente a una falla de disco duro SATA/IDE  
 Fuente: Elaborado por el autor

### 3.2.10.10. Clase de Riesgo: Falla de Tarjeta de Red

#### ACTIVIDADES ANTES

##### Medidas Técnicas

- Es importante que el técnico del departamento de TI verifique que los (Drivers) o controladores de los equipos se encuentren correctamente actualizados y evitar posibles fallas.
- Verificar que la tarjeta de red no se encuentre configurada en modo ahorro de energía ya que al no enviar o recibir datos, esta procede apagarse.
- Verificar que la dirección IP fija que fue asignada a la maquina este correctamente asignada.

#### ACTIVIDADES DURANTE

##### Medidas Técnicas

Si existe una falla en la conexión a la red, puede tratarse de un problema en la tarjeta de red, por lo que el técnico capacitado debe revisar que:

- Los (Drivers) controladores estén correctamente actualizados.
- Puede tratarse de un problema en el sistema, dado a una mala configuración del (Firewall) o Cortafuegos, que interrumpa la conexión inalámbrica. Se sugiere deshabilitar el cortafuegos, conviene también tener actualizado el sistema y probar la conexión si se solvento el inconveniente.
- Si el sistema operativo muestra que la red local y el internet esta desconectado y luego conectado sucesivamente, el técnico debe mover el conector y el cable sin mucha fuerza para no estropearlo ninguno de estos, si observa que el indicador se apaga, se debe cortar el cable unos 5 cm y colocar un conector RJ45 usando una crimpadora.
- Si el problema es físico en la misma placa, el técnico debe reinstalar el Driver de red y actualizar los controladores, en el caso de no solucionarse se precedería con el cambio de la placa de red.
- Si el equipo no reconoce la placa de red, el técnico debe verificar que la placa se encuentre colocada correctamente en la ranura PCI.

## ACTIVIDADES DESPUÉS

### Medidas Técnicas

- Luego de un chequeo técnico y no obtener resultados proceder con el cambio de la tarjeta de red, al ser un dispositivo económico y fácil de instalar no habría mayor complicación.
- Proceder al trámite de identificación del tipo de tarjeta de red y generar una petición a quien corresponda para su adquisición.
- Verificar que la tarjeta de red adquirida sea la indicado.
- Proceder con el cambio de la tarjeta de red utilizando medidas de seguridad.
- Emitir un informe del daño que se solvento al jefe del departamento de TI.

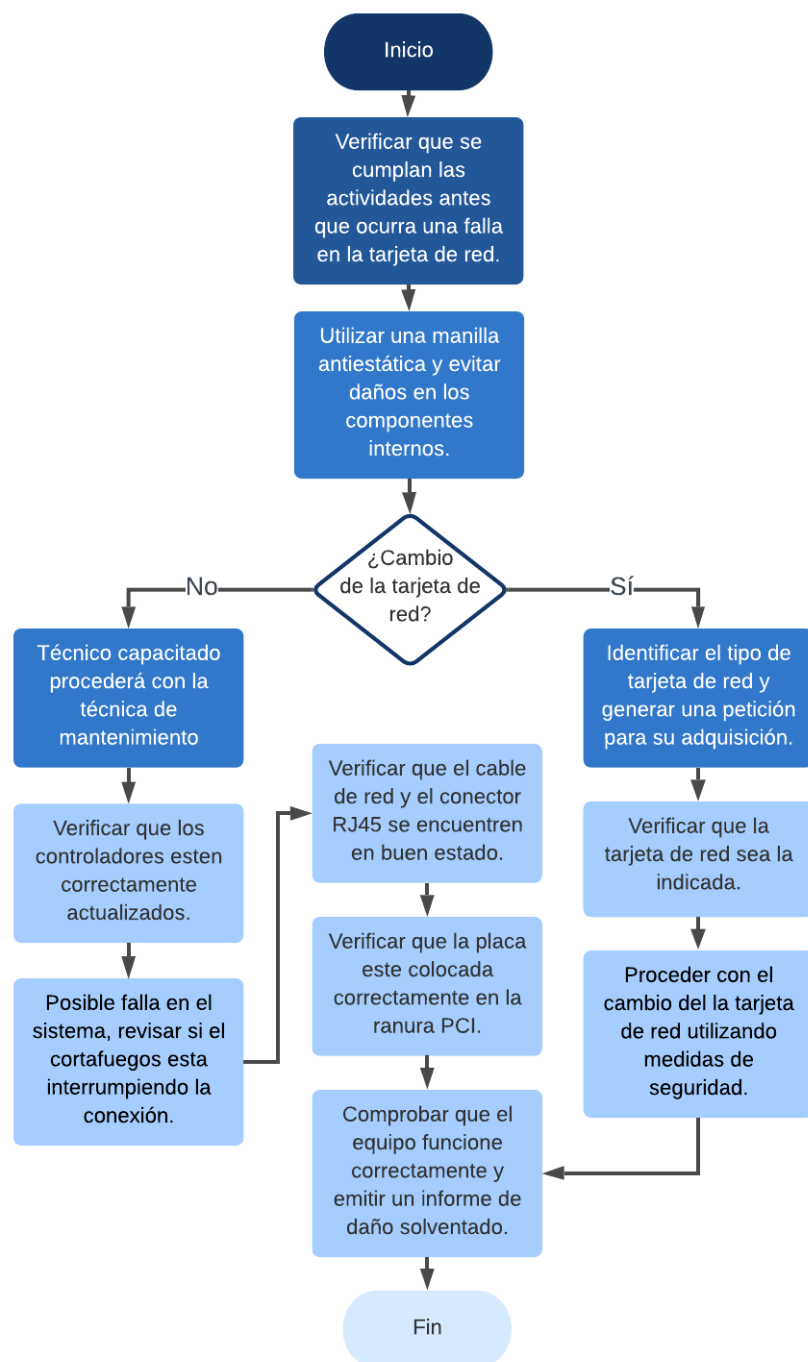


Figura 3.42: Acciones frente a la falla en la tarjeta de red  
Fuente: Elaborado por el autor

### 3.2.10.11. Clase de Riesgo: Fallas de Software/Configuración

#### ACTIVIDADES ANTES

##### Medidas Humanas

Se debe capacitar al personal que hace uso de los equipos informáticos para su trabajo sobre:

- No acceder a sitios Web de carácter peligroso o sospechoso para evitar el ingreso de virus a través de la conexión a internet.
- Si necesita instalar algún tipo de programa determinado, comunicarse con el personal del departamento de TI, ya que esta restringido la instalación de cualquier programa sin autorización.
- Solo si es necesario y necesita conectar algún tipo de almacenamiento externo en los equipos informáticos, se debe informar al jefe del departamento correspondiente para asegurarse de pasarlo por un análisis del antivirus.

##### Medidas Técnicas

El personal encargado de dar el mantenimiento respectivo al software debe asegurarse que se cumpla las siguientes actividades:

- Verificar que el sistema operativo de los equipos se encuentre correctamente actualizado.
- En el caso de requerir un determinado programa, descargarlo solo de sitios confiables.
- Si es necesario desinstalar algún tipo de programa del computar, el técnico debe asegurarse de no dejar restos de los archivos del programa desinstalado ya que podrían ocasionar fallas en el sistema a futuro.
- El equipo de trabajo del departamento de TI debe realizar un chequeo habitual del software referente a los programas desarrolladas internamente, y verificar si están trabajando correctamente, debido a que al pasar el tiempo este suele estropearse o tener algún tipo de falla.
- Existen programas de diagnóstico y reparación del sistema lo que es recomendable ejecutarlo periódicamente y mantener un software del sistema con un correcto mantenimiento, esto evita tener archivos dañados que pueden ocasionar fallas.

## ACTIVIDADES DURANTE

### Medidas Técnicas

En el caso de que el sistema operativo este fallando el técnico debe:

- Verificar si el sistema operativo esta correctamente actualizado.
- Realizar un análisis minucioso con el antivirus.
- Ejecutar un programa de diagnóstico y reparación del sistema, y ver su comportamiento.
- Eliminar archivos temporales del equipo, los que se generan de acuerdo con los programas ejecutados.
- Si el sistema no inicia, verificar las configuraciones de arranque a través de la BIOS, podría tratarse de una falla del disco duro.

En el caso del software desarrollado internamente por el personal del departamento de TI.

- Recoger los Backups, programas, manuales del sitio alternativo en donde se encuentran resguardados.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.

Para el servidor:

- La institución cuenta con un antivirus el mismo que permitirá aislar el virus para su futura inspección.
- Este antivirus mostrará el nombre y tipo de archivo infectado, así como quien lo utilizó.
- Luego de aislar el virus y si el mensaje sobre la existencia de un virus en el sistema persiste, es probable que una de las estaciones sea la que causó la infección, procediendo a retirarla del ingreso al sistema y proceder con un chequeo más detenido.



## ACTIVIDADES DESPUÉS

### Medidas Técnicas

El técnico capacitado del departamento de TI deberá:

- Utilizar los discos con la instalación del sistema operativo igual o de superiores características al computador infectado.
- Luego de instalar el nuevo sistema operativo, se deberá instalar el antivirus de tal manera que permita revisar todos los archivos y no solo los programas ejecutables, en el caso de encontrar algún tipo de virus proceder a eliminarlo, si no es posible hay que eliminar el archivo infectado, tomando nota de estos.
- Recoger los Backups, programas, manuales del sitio alternativo en donde se encuentran resguardados.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.
- Brindar el soporte pertinente a la restauración para verificar y probar la integridad de los datos.
- Entrega del equipo informático por parte del técnico capacitado.
- Emitir un informe del daño que se solventó al jefe del departamento de TI.

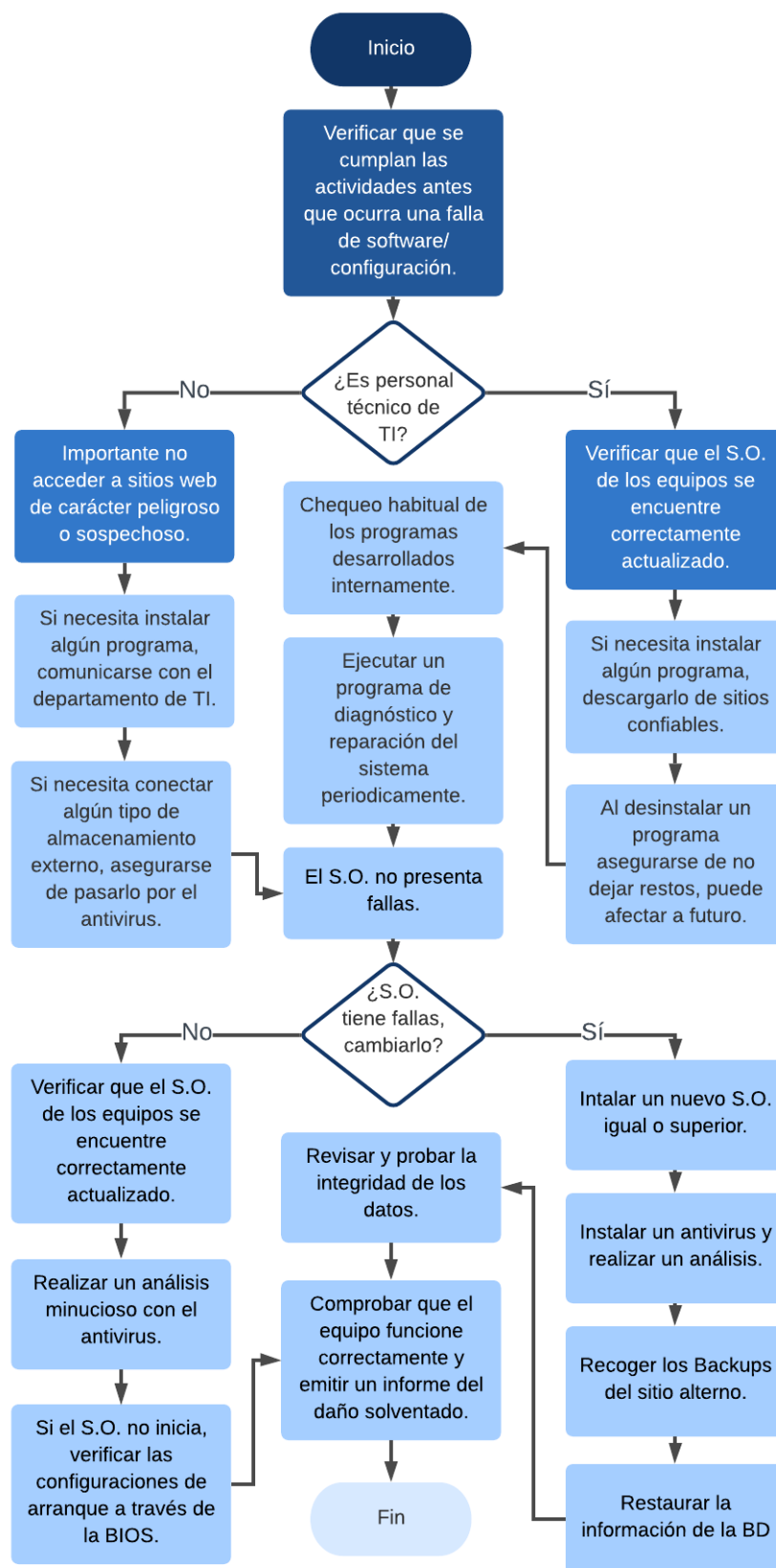


Figura 3.43: Acciones frente a una falla de software/configuración  
 Fuente: Elaborado por el autor

### 3.2.10.12. Clase de Riesgo: Falla de cableado y conectores

#### ACTIVIDADES ANTES

##### Medidas Técnicas

En cuanto al cableado de red y conectores.

- Evitar instalar el cable de red en áreas con filos tipo esquina, puede dañarlo y producir fallas.
- Al momento pasar el cable puede ser una tubería o canaleta, y se encuentre con un paso difícil no intente jalarlo, se debe localizar el punto donde se presenta la falla y repararlo.
- Si utiliza sujetadores de cable tales como amarres, abrazaderas, permitir que el cable tenga un espacio suficiente para permitir un pequeño movimiento, y evitar dañarlo.
- No colocar objetos pesados sobre el cable ya que puede estropearse, en el caso que este haya sufrido algún tipo de daño no intente repararlo con alguna cinta de aislar, se debe remplazar el cable.
- Al realizar una conexión y existiera un sobrante de cable debe cortarlo, bastaría con un diámetro interno del enrollado no menor a un metro.
- Evite dañar o raspar el recubrimiento.
- No torcer el cable sobre su propio eje a que puede causar fallas.
- Evitar dejar un espacio entre la envoltura del cable y conector.
- Los patch cords deben estar identificados en las salidas de los usuarios en cada departamento, así como en el departamento de TI donde están los equipos de redes.
- La mejor forma de gestionar estos cables de red y conectores es utilizando rack y gabinetes así se podrá identificar de mejor manera cada cable y hasta para añadir mas cableado de manera organizada.

En cuanto al cableado de energía eléctrica.

- Crear un circuito exclusivo desde el punto de entrega de la empresa distribuidora de electricidad hacia el departamento de TI.

- Se debe construir una toma a tierra física exclusiva para el departamento de TI, misma que se conecte mediante un cable con cubierta aislante al centro de carga del departamento de TI.
- Utilizar conexiones a contactos polarizados 125 VCA, y utilizar el código de colores:
  - **FASE:** Negro, rojo, o azul.
  - **NEUTRO:** Blanco o gris.
  - **TIERRA FÍSICA:** Verde.
- Los empalmes en el cableado eléctrico deben ser realizado por un personal capacitado, utilizando medidas de seguridad.

## ACTIVIDADES DURANTE

### Medidas Técnicas

En cuanto al cableado de red y conectores.

- Se debe gestionar los cables, para esto hay que dirigirse al rack o gabinetes donde estos se encuentran correctamente señalizados y así identificar cual es la falla, ahorrando tiempo.
- Verificar si el conector RJ45, este correctamente conectado, al notar que este presenta fallas cambiarlo.
- El técnico debe verificar el estado del cable si se encuentra roto en algún tramo de este, y proceder a cambiar el cable si es el caso.
- Verificar si el cableado presenta daño por la humedad, puede que exista una filtración de agua que causa este tipo de problema.

En cuanto al cableado de energía eléctrica.

- Comunicar el incidente a las respectivas autoridades.
- Las autoridades deben comunicarse con un técnico capacitado de la empresa eléctrica.
- Si los equipos informáticos están conectados a los UPS, se procede a guardar la información procesada y apagarlos hasta que el inconveniente se solucione y las autoridades den la orden de retomar las actividades.

- Si se presenta alguna falla en el cableado eléctrico, el técnico capacitado en el área verificará la avería.
- La humedad en la institución es otro factor que se debe considerar por lo que se debe hacer un chequeo del cable y descartar este posible fallo.
- Si el daño es mayor se debe comunicar con la empresa distribuidora de electricidad de la localidad, y evitar que la falla se incremente.

## **ACTIVIDADES DESPUÉS**

### **Medidas Técnicas**

En cuanto al cableado de red y conectores.

- El técnico que solvento el inconveniente con la red debe presentar un informe con el daño solventado al jefe del departamento de TI.
- Considerar el tipo de daño solventado para poder prevenirlo y no ocurra nuevamente a futuro.

En cuanto al cableado de energía eléctrica.

- El técnico que solvento el inconveniente con el cableado de energía eléctrica debe reportarse con los dirigentes de la institución sobre la avería.
- Considerar el tipo de daño solventado para poder prevenirlo y no ocurra nuevamente a futuro.
- Las autoridades de la institución procederán a dar la orden de retomar las actividades con normalidad.

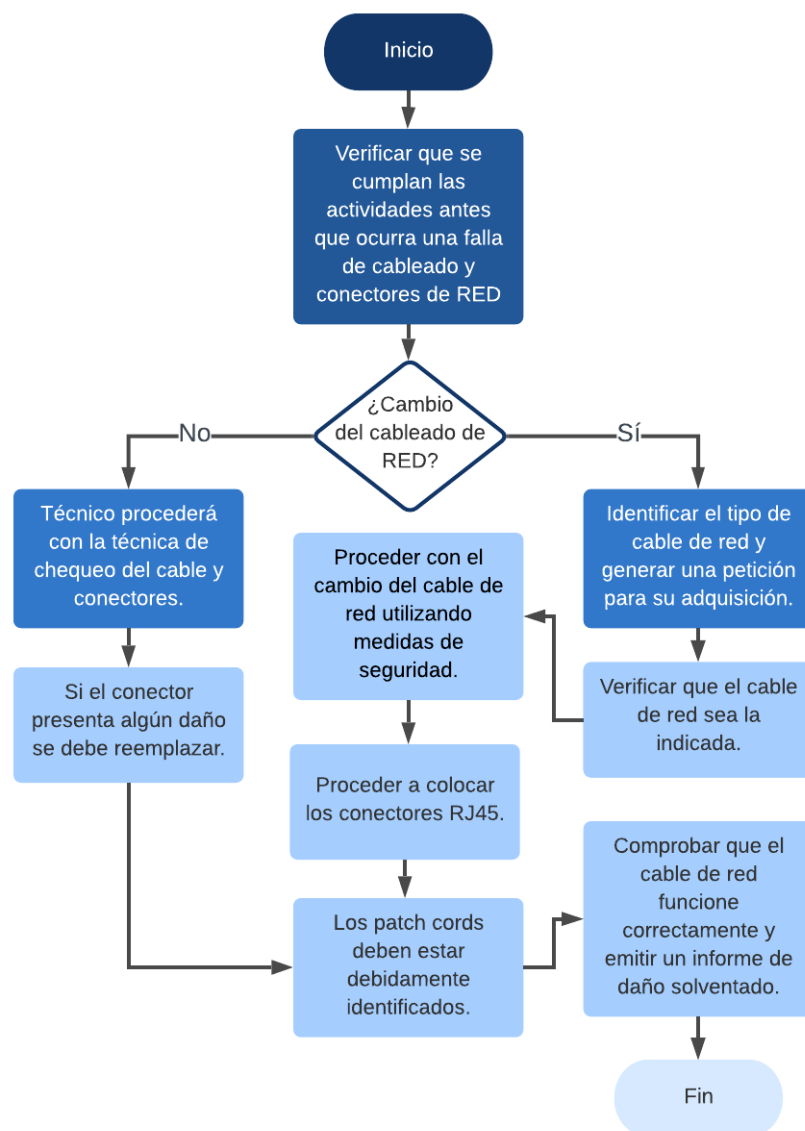


Figura 3.44: Acciones frente a una falla de cableado y conectores de red  
 Fuente: Elaborado por el autor

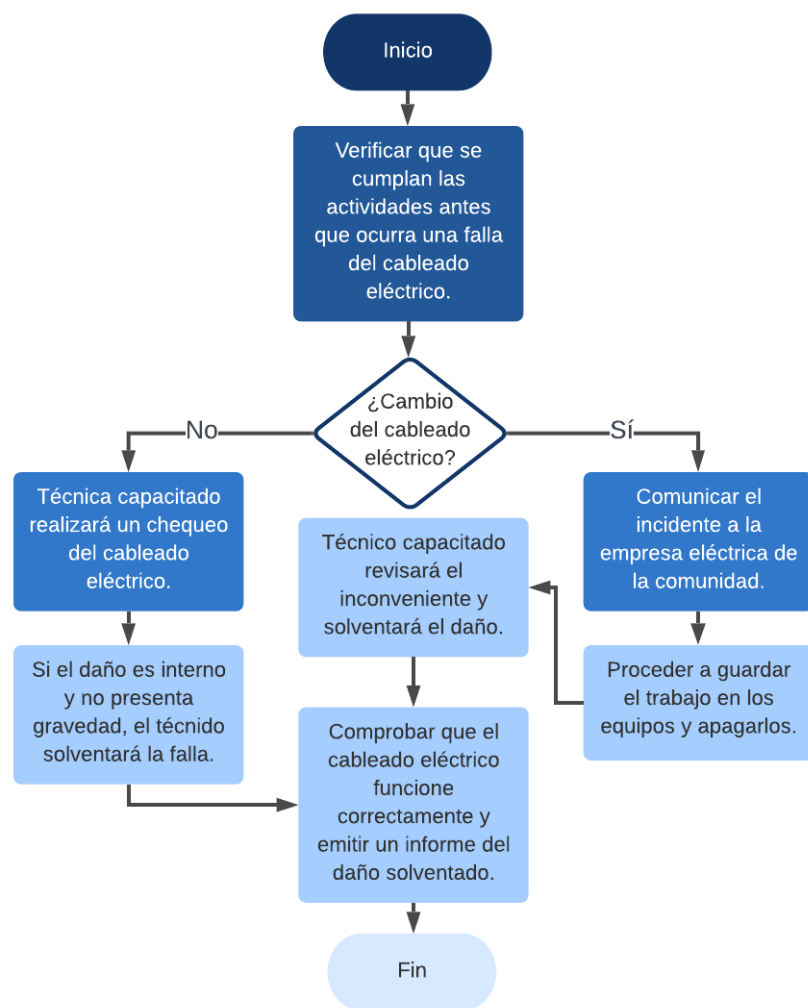


Figura 3.45: Acciones frente a una falla de cableado eléctrico  
 Fuente: Elaborado por el autor

### **3.2.10.13. Clase de Riesgo: Acceso no autorizado (Robo o alteración de información)**

#### **ACTIVIDADES ANTES**

##### **Medidas Humanas**

- Verificar que cualquier persona ajena al departamento al que perezca no tenga acceso directo con ningún equipo informático, en el caso del departamento de TI solo el personal autorizado debe ingresar donde están ubicados los servidores y demás equipos informáticos de la institución.
- Es importante contar con cámaras de seguridad tanto en el departamento de TI como en las estaciones de trabajo para un mejor control y vigilancia ante un robo o alteración de la información dentro de la institución.
- Contar con una buena seguridad física en los departamentos donde se encuentre los principales equipos informáticos, y así controlar que solo el personal autorizado manipule un determinado equipo.
- La capacitación del personal es imprescindible ya que, al dar la importancia del caso a la seguridad de la información, se debe enfatizar temas como las contraseñas y la seguridad que debe tener, esto ayuda a proteger ante posibles robos o alteración de los datos.

##### **Medidas Técnicas**

- Limitar el acceso a la base de datos, los diferentes grupos de trabajo tendrán acceso solo a lo necesario para laborar en su puesto que desempeña. (Acotar los permisos y privilegios)
- Evitar que el servidor que maneja la base de datos tenga acceso directamente desde el internet, y así descartar cualquier tipo de ataque.
- Tener activado el cortafuegos (firewall) en los equipos en todo momento.
- El monitoreo de la base de datos se puede hacer con ayuda de auditorias con registros de estos movimientos sobre los datos, permitiendo conocer quién, cuándo, cómo y que tipo de dato fue manipulado. Esto permite detectar cualquier tipo de acción sospechosa en tiempo real, así se puede controlar algún tipo de empleado cómplice que quiera divulgar la información o alterarla.



- Una vez que un empleado renuncia o es despedido por algún motivo, inmediatamente se debe revocar el acceso a los datos de la red dándole protección ante empleados desleales que quieran dañar la imagen de la institución.
- En el punto de administrador de la red se debe tener una clasificación de los usuarios de la red en grupos de trabajo para un mayor control de acceso permitiéndole adjudicar su nivel de seguridad y perfil adecuado según el departamento que ocupe.
- Ningún usuario final tendrá acceso total como usuario administrador del equipo informático.
- Se debe restringir un tiempo de uso, y tener activado el periodo de inactividad para que los equipos se suspendan y si quiere nuevamente acceder deberá ingresar la contraseña designada al puesto de trabajo y evitar cualquier modificación o alteración de la información por parte de una tercera persona.

## **ACTIVIDADES DURANTE**

### **Medidas Humanas**

- En el caso de que el personal de la institución note alguna situación sospechosa en el sistema que se encuentra a cargo debe informar al personal del departamento de TI.

### **Medidas Técnicas**

- Identificar el equipo que presente algún tipo de problema o sospecha ante un posible acceso no autorizado, se debe retirar el ingreso al sistema y proceder con un chequeo más detenido.
- Técnico procederá con una revisión sobre las actividades de prevención se están cumpliendo.
- Cambiar las credenciales del usuario con el problema o sospecha.
- Si existe una sospecha en la alteración de la información se debe recurrir a gestionar las auditorias de los registros sospechosos y verificar si los movimientos son los adecuados.

- Es importante realizar un análisis detenido con el antivirus y descartar la posibilidad de un posible virus.

## **ACTIVIDADES DESPUÉS**

### **Medidas Humanas**

- Capacitar a los empleados sobre las precauciones que deben tener ante el acceso no autorizado.

### **Medidas Técnicas**

- El técnico y personal encargado del análisis de las auditorias deberá emitir un registro de los últimos movimientos alterados para el jefe del departamento de TI y a las autoridades de la institución para que se encarguen del proceso.
- Una vez descartado cualquier posibilidad o sospecha de robo o alteración de la información se procederá a reactivar el sitio de trabajo y conectarlo nuevamente a la red.
- El equipo técnico del departamento de TI, procederá a reanudar la operatividad de los equipos informáticos que formaron parte del proceso.
- Se realizará una comprobación del normal funcionamiento de los sistemas informáticos, asegurándose que toda la documentación y procesos se encuentren en orden.
- El técnico procederá a entregar las credenciales al usuario, luego de descartar cualquier tipo de problema referente al acceso no autorizado del sistema respectivo.

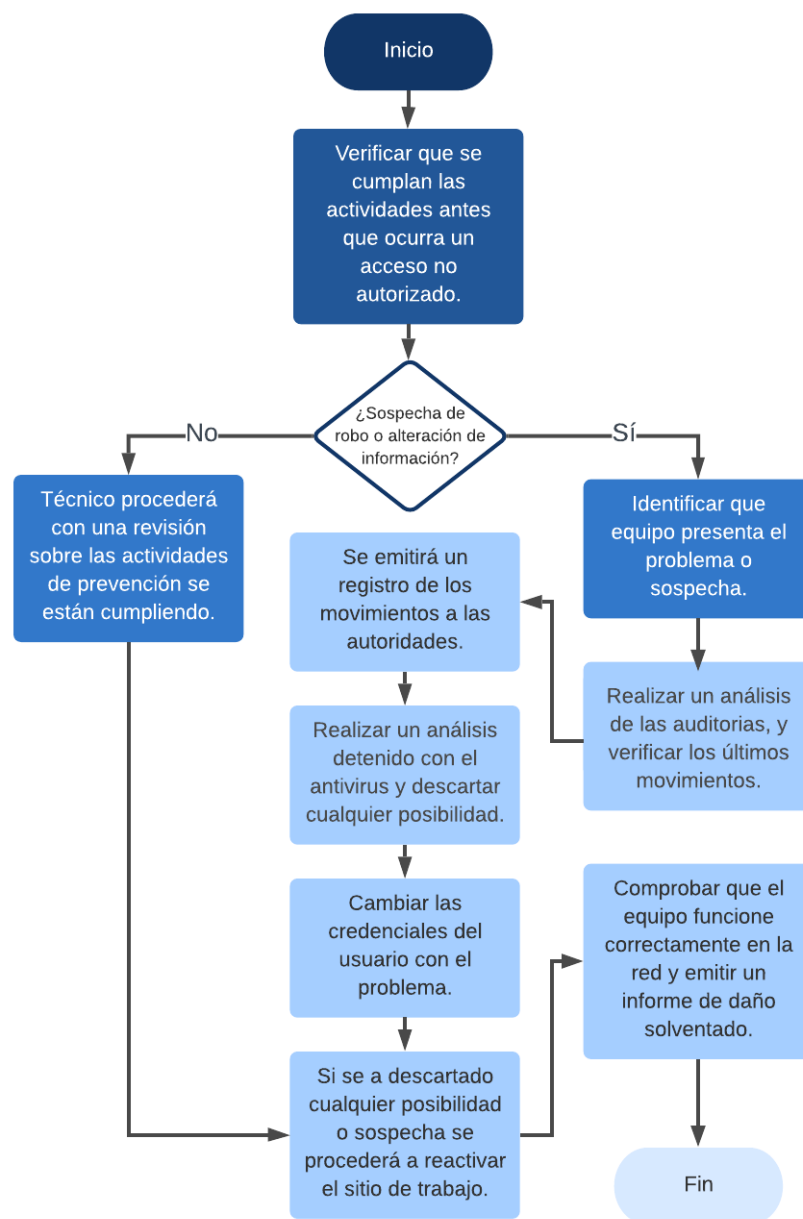


Figura 3.46: Acciones frente al acceso no autorizado (robo o alteración de la información)

Fuente: Elaborado por el autor

### 3.2.10.14. Clase de Riesgo: Ataques DoS o denegación de servicio

#### ACTIVIDADES ANTES

##### Medidas Técnicas

- El personal del departamento de TI debe verificar la configuración de los routers y firewalls para detectar IP's inválidas o falsas, que posiblemente estén dirigidos por atacantes.
- La instalación de un router entre la red interna y el proveedor de servicios de internet (ISP), sería lo ideal para tener una configuración de seguridad como es el caso de una lista de control de acceso (ACL), permitiendo controlar el flujo del tráfico de la red, a manera de un cortafuegos.
- En el caso de un servidor web, aparte de contar con un firewall, es necesario instalar un cortafuegos de aplicaciones web o por sus siglas en inglés Web Application Firewall (WAF), especializado en bloquear y proteger cualquier tipo de acciones que se considere maliciosas, así como “inyección de SQL”.
- La municipalidad al manejar datos de carácter confidencial es necesario contar con el uso del protocolo de Seguridad de la capa de transporte, o por sus siglas en inglés Transport Layer Security (TCL), y así asegurar la confidencialidad de transmisión de la información a través de Internet.
- En los servidores de la municipalidad los puertos que no sean necesarios hay que desactivarlos. Dado el caso que el servicio requerido sea únicamente alojar un servicio de web, los puertos que deberían estar habilitados son 80/TCP u 8080/TCP para realizar peticiones HTTPS. Si se desea alojar un servicio DNS, se puede tener abierto el puerto 53/TCP o 53/UDP.

#### ACTIVIDADES DURANTE

##### Medidas Técnicas

- Identificar qué equipo informático presenta el problema o sospecha de haber sido atacado, denegándole su servicio.
- Se debe aislar el equipo informático víctima del ataque para su correspondiente análisis.
- El técnico debe restablecer los sistemas que han sido afectados.

- Asegurarse de que el firewall se encuentre activado.
- El G.A.D. Municipal al ser víctima de un ataque de denegación de servicio (DoS), dirigido al servicio web de la institución, se hace necesario contar con una copia estática del sitio web donde se muestre información básica como es: números de contactos de la municipalidad, dirección de correo electrónico, y contenido que no necesite grandes procesamientos para ser mostrados a los usuarios y así no dejar en ningún momento de brindar un servicio, mostrando una buena imagen de la municipalidad.
- Realizar un análisis con el antivirus y descartar cualquier posibilidad de presencia de virus.
- Realizar un chequeo de los puertos que se encuentren habilitados y verificar que sean los correspondientes de acuerdo con el servicio requerido.

## **ACTIVIDADES DESPUÉS**

### **Medidas Técnicas**

- Luego de un análisis detenido en el servidor que sufrió el ataque se procederá a emitir un informe a las autoridades sobre los daños que ocasionó el percance.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.
- Brindar el soporte pertinente a la restauración para verificar y probar la integridad de los datos.
- Bloquear los puertos que no sean necesarios para un determinado servicio.
- Entrega del equipo informático por parte del técnico capacitado.
- Verificar si el firewall se encuentra correctamente ejecutándose.
- En el caso que el antivirus se encuentre sin las actualizaciones respectivas es importante descargarlas.
- Capacitar a los empleados sobre los ataques informáticos.

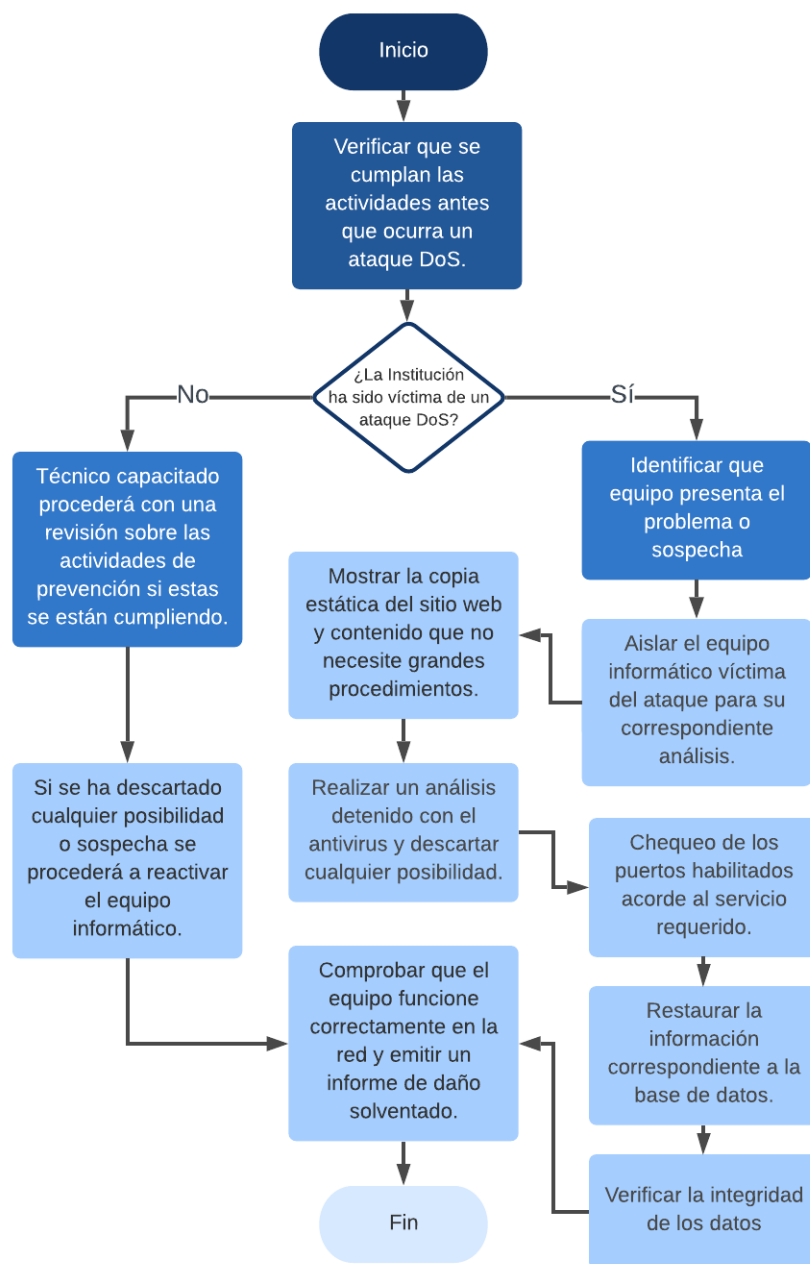


Figura 3.47: Acciones frente a los ataques DoS o denegación de servicio  
 Fuente: Elaborado por el autor

### **3.2.10.15. Clase de Riesgo: Falla de Hardware**

#### **ACTIVIDADES ANTES**

##### **Medidas Humanas**

- Contar con pólizas de seguros comerciales, que brinden un seguro a los activos informáticos.
- Colocar un extintor en un lugar visible dentro de cada departamento de la institución y capacitar debidamente al personal sobre la manera correcta de uso.

##### **Medidas Técnicas**

- El técnico de la institución debe realizar un mantenimiento preventivo a los equipos informáticos de manera periódica y evitar posibles fallas.
- Verificar periódicamente que las instalaciones eléctricas estén en buen estado.
- Asegurarse que los equipos informáticos se encuentren conectados a un UPS, que proteja ante posibles altas y bajas de tensión eléctrica (falla eléctrica).
- Mantener de manera periódica Backus de los principales elementos de software necesarios para restablecer las actividades normales de la institución.
- Actualizar periódicamente el inventario de los equipos informáticos.
- Evitar cualquier movimiento brusco o golpes en los equipos informáticos, ya que podrían ocasionar fallos en las piezas internas.
- No dejar cualquier tipo de líquido (agua, café, líquidos corrosivos, etc.), cerca de los equipos informáticos ya que podrían derramarse y dañar los equipos.

#### **ACTIVIDADES DURANTE**

##### **Medidas Humanas**

- Al presentarse una falla en los equipos el personal de los diferentes departamentos de la institución debe comunicarse con el personal de TI y notificar la falla.

### **Medidas Técnicas**

- Identificar que equipo presenta el problema o falla del hardware.
- El técnico debe realizar un chequeo general del equipo informático averiado y solventarlo en caso de no presentarse mayor gravedad.
- Si el daño es grave, el técnico debe llevar el equipo al departamento de TI para realizar un chequeo más detenido e informar el percance al jefe de dicho departamento.
- En caso de necesitar algún remplazo sobre las piezas internas, se debe realizar el correspondiente pedido, según el protocolo interno de la institución.

## **ACTIVIDADES DESPUÉS**

### **Medidas Técnicas**

- Verificar que la pieza(s) del equipo informático sean las correctas para su correspondiente reemplazo.
- En el caso de ser un problema en el servidor se procede a colocar un nuevo equipo de reemplazo y restaurar la información correspondiente en la Base de Datos y sus respectivos programas.
- Verificar la integridad de los datos.
- Entrega del equipo informático por parte del técnico capacitado.
- Técnico emitirá un informe del daño que se solventó al jefe del departamento de TI.

### **Error de Memoria RAM y Tarjeta(s) Controladora(s) de Disco**

Al presentarse una falla en las memorias RAM, se presentan las siguientes señales:

- Los equipos informáticos y servidores no pueden responder correctamente ya sea por lentitud del equipo en los diferentes procesos al no soportar el ingreso masivo de usuarios que desempeñan en la institución.
- Al presentarse grandes procesos que deben ser respondidos por el servidor estos se congelan.



- Se puede presenciar mensajes de errores en la pantalla.

Para el caso de los servidores es importante contar con una tarjeta RAM ECC (Error-Correcting Code), el cual garantice la integridad de los datos, estas memorias tienen la capacidad de recuperarse de determinados errores identificándolos y corrigiéndolos e incluso recuperando la información.

Cualquier tipo de cambio interno que se requiera realizar en los servidores, se debe realizar fuera del horario de trabajo establecido por la municipalidad, salvo el caso que una falla lo amerite, se debe cambiar cualquier pieza de forma inmediata.

Hay que considerar que ningún proceso de la institución debe quedar suspendido, para el caso de un cambio de las memorias con fallas se debe tomar en cuenta las siguientes acciones:

- Se debe enviar mensajes a los usuarios que deben salir del sistema, se puede hacer uso de mensajes por red y comunicar a los jefes de cada departamento que lo informen con los miembros de cada área.
- El servidor debe encontrarse apagado, teniendo como resultado un apagado de los sistemas o programas alojados en este.
- Proceder al trámite de identificación de las memorias malogradas y generar una petición a quien corresponda para su adquisición.
- Verificar que las memorias adquiridas sean las indicadas.
- Proceder con el reemplazo de las memorias por unas similares utilizando medidas de seguridad.
- Desconectar la conexión a la red del servidor, evitando así que los usuarios ingresen.
- Verificar el funcionamiento del servidor con pruebas locales, deshabilitar las entradas, luego se procederá a conectar a la red de la institución e ir habilitando las entradas paulatinamente para los departamentos en los cuales se ejecutarán las pruebas.
- Probar que los sistemas y programas conectados en la red están funcionando de manera correcta.
- Finalmente después de realizar las pruebas pertinentes y con resultados favorables, se procede habilitar las entradas a los sistemas y programas a los demás usuarios de los demás departamentos.

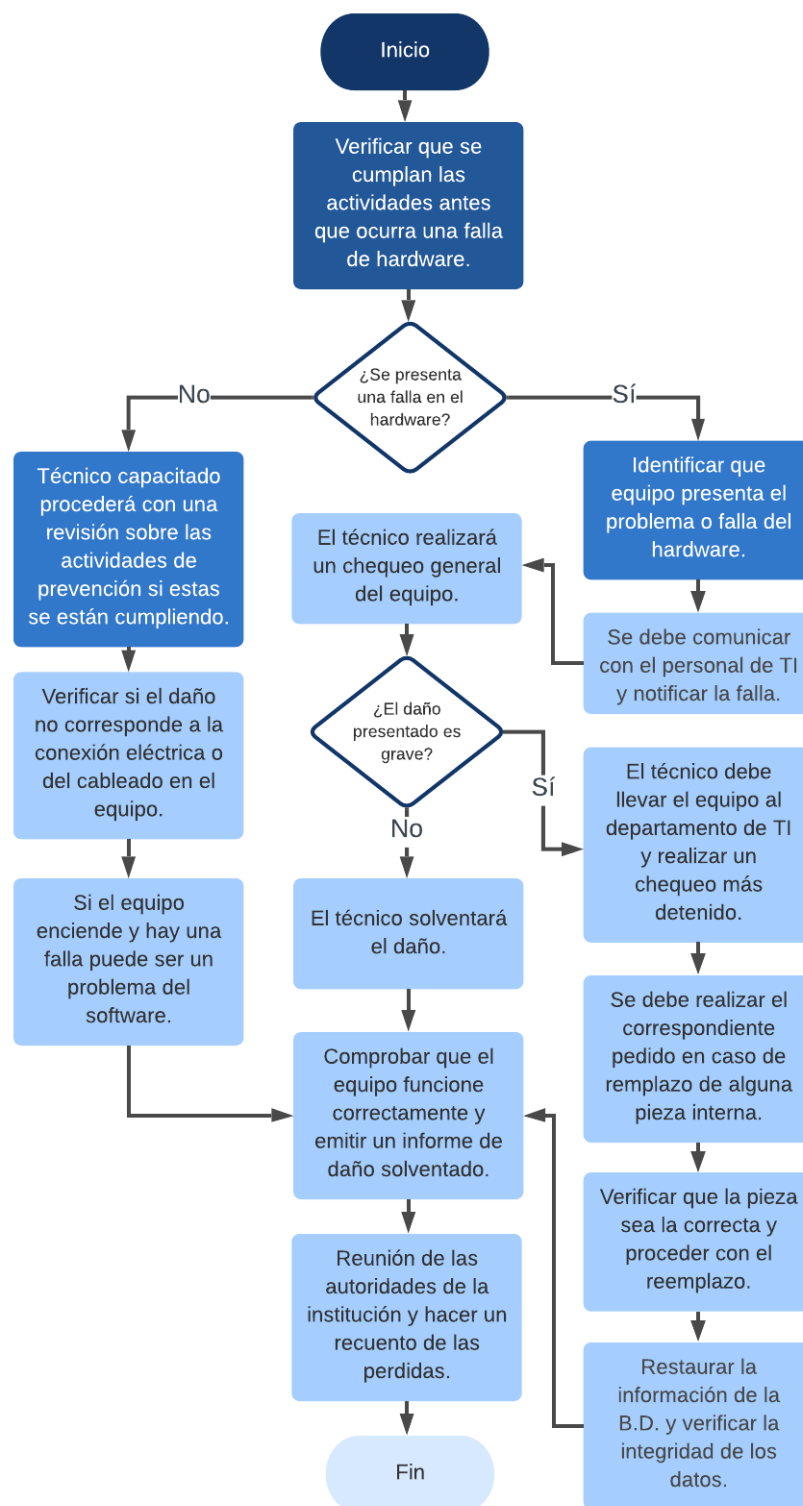


Figura 3.48: Acciones frente a una falla de hardware  
Fuente: Elaborado por el autor

### **3.2.10.16. Clase de Riesgo: Error Humano (Falta de conocimiento)**

#### **ACTIVIDADES ANTES**

##### **Medidas Humanas**

- Mientras un trabajador de la institución toma sus vacaciones anuales, se debe considerar un remplazo que realice las actividades de manera correcta y responsable, procediendo con la capacitación al reemplazo sobre lo que debe cubrir durante un tiempo determinado.
- Reforzar el conocimiento del personal que labora en la institución con capacitaciones frecuentes, cada una sobre su respectiva área desempeñada en la municipalidad.
- Asignar un responsable del control y la protección de los equipos informáticos en los diferentes departamentos, quien será encargado de informar cualquier situación sospechosa o que no esté autorizada por las autoridades competentes.
- Contar con personal capacitado y responsable en la parte de recursos humanos, para tener un buen control administrativo.

##### **Medidas Técnicas**

- Se debe difundir manuales de usuario que permitan manipular de forma correcta el software y programas que maneja la municipalidad para cada departamento a todo el personal que trabaja de manera directa con los equipos informáticos.
- Al seleccionar nuevo personal para la institución se realizará de manera rigurosa tomando en cuenta su preparación y grado de experiencia.
- Mantener de manera periódica Backups de los principales elementos de software necesarios para restablecer las actividades normales de la institución, en el caso que exista algún mal manejo por parte del personal y dañe la información.
- Verificar los respaldos (Backups) funcionen correctamente ejecutando pruebas sobre los servicios de procesamientos de datos.
- Contar con una buena seguridad física en los departamentos donde se encuentre los principales equipos, y así controlar que solo el personal autorizado manipule un determinado equipo informático.

- Se puede hacer uso de auditorías en la base de datos sobre los registros de los movimientos, permitiendo detectar cualquier acción como medida de seguridad.

## **ACTIVIDADES DURANTE**

### **Medidas Técnicas**

- Identificar qué equipo informático presenta el problema o sospecha de haber sufrido un error humano.
- Se debe comunicar al personal de TI (jefe del departamento) el problema.
- Deshabilitar el ingreso al sistema al empleado involucrado en el percance hasta próximo aviso.
- El personal encargado del departamento de TI (técnico capacitado) realizará un chequeo general del problema o falla.
- Realizar un análisis de la causa junto con el personal involucrado en el fallo o error humano a falta de atención o capacitación en el área desempeñada.
- En el caso de ser grave del daño el técnico encargado debe llevar el equipo al departamento de TI para un análisis más detenido.
- Proceder con la identificación de la falla y solventarlo.
- Realizar el respectivo seguimiento tanto al personal responsable como a este tipo de errores presentados en la institución.
- Proceder con las políticas internas de la municipalidad en el caso de ser un error grave y malintencionado que afecte la operatividad de la institución, así como su imagen.

## **ACTIVIDADES DESPUÉS**

### **Medidas Humanas**

- Capacitar el personal del departamento de TI sobre los posibles fallos que pueden presentarse acotando los errores presentados en la institución para que estos no vuelvan a repetirse.
- Emitir un informe del daño que se solventó al jefe del departamento de TI.

- Realizar una reunión con los directivos para hacer un recuento de los daños.

### **Medidas Técnicas**

- Luego de un análisis detenido en el equipo informático afectado se procederá a emitir un informe a las autoridades sobre los daños que ocasionó el percance.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.
- Verificar la integridad de los datos.
- En el caso de identificar que el error no es causa mal intencionada contra la institución se procederá a habilitar el usuario al empleado involucrado y que reanude el trabajo.
- Reforzar el conocimiento del personal que labora en la institución con capacitaciones frecuentes, cada una sobre su respectiva área desempeñada en la municipalidad.

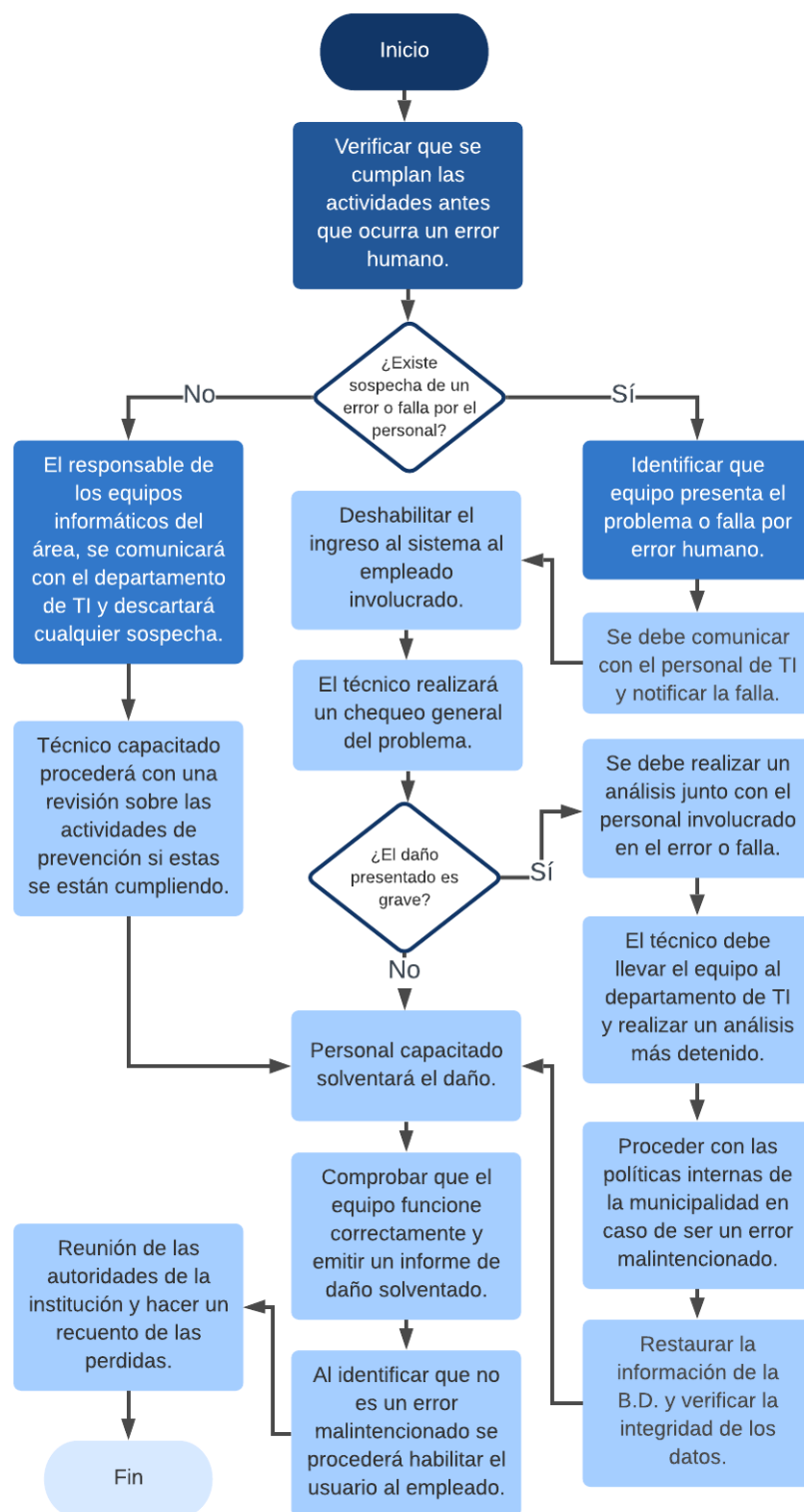


Figura 3.49: Acciones frente a un error humano (falta de conocimiento)  
Fuente: Elaborado por el autor

### **3.2.10.17. Clase de Riesgo: Robo de dispositivos**

#### **ACTIVIDADES ANTES**

##### **Medidas Humanas**

- Si usted se encuentra laborando en la institución e identifica personas con comportamientos extraños fuera de lo usual, inmediatamente debe comunicarse con el jefe de seguridad de la municipalidad o al guardia de seguridad más cercano, describiendo la situación.
- El personal de la institución debe participar en todas las actividades dispuestas para la prevención del riesgo público, y estar preparados ante alguna emergencia.
- Establecer vigilancia mediante cámaras de seguridad tanto en el departamento de TI como en donde se encuentran los servidores, registrando así los movimientos de entrada y salida del personal al área.
- Contar con pólizas de seguros comerciales, que brinden un seguro a los activos informáticos.
- Contar con un guardia de seguridad que brinde vigilancia interna de la institución.
- Mantener una buena relación de trabajo con el departamento de policía del cantón que realice rondas por la institución, salvaguardando la municipalidad.
- Los jefes de cada departamento manejarán la seguridad en cada departamento, estableciendo medidas estrictas del personal que manipule estos equipos informáticos.
- El personal que labora en institución debe conocer los números de llamadas de emergencia como el de la UPC del cantón y otros organismos de seguridad necesarios ante una emergencia.

##### **Medidas Técnicas**

- Proteger el área donde se encuentran los principales equipos informáticos, mantener con la puerta cerrada y con seguro el cuarto frío del departamento de TI.

- Mantener de manera periódica Backups de los principales elementos de software necesarios para restablecer las actividades normales de la institución, en el caso de existir algún robo en lo equipos.
- Mantener los respaldos fuera de la Municipalidad, para en lo posterior reanudar las actividades.
- Actualizar periódicamente el inventario de los equipos informáticos.
- Es recomendable colocar candados de seguridad en la ranura exterior de los equipos ya que pueden sustraerse fácilmente piezas internas de lo equipos como pueden ser tarjetas RAM, etc.

## **ACTIVIDADES DURANTE**

### **Medidas Humanas**

- Si el robo se presenta en horas laborables, el personal debe mantener la calma.
- El personal civil de la institución no debe enfrentarse a este grupo de asaltantes, especialmente si estos se encuentran armados.
- Esperar las indicaciones del personal de seguridad de emergencia interna, externa o de las autoridades de la municipalidad.
- Si es posible y sin poner en riesgo la vida, intente identificar a los agresores, en el caso de ser varios, determinar el número, pero fijarse solo en uno y en sus características.
- No debe intentar nada que pueda empeorar la situación.

### **Medidas Técnicas**

- Al estar activadas las cámaras de seguridad se activará una alerta de emergencia solicitando apoyo al departamento de policía del cantón.

## **ACTIVIDADES DESPUÉS**

### **Medidas Humanas**

- Comunicar el incidente a las respectivas autoridades de la institución.
- No se debe ingresar a la zona que fue afectada por los agresores hasta que las autoridades de la municipalidad lo autoricen.



- Si la situación lo amerita, se debe cerrar las oficinas, departamentos y esperar indicaciones de las autoridades.
- A la brevedad posible, hay que acudir con las autoridades y describir todo lo que pueda ser de importancia como las características del agresor(es) que pueda recordar, actitudes del agresor(es), etc. No fiarse de la memoria por mucho tiempo ya que pueden omitirse detalles de gran importancia para la investigación.
- En el caso de tener la autorización de las autoridades de la municipalidad, se procederá a reanudar las actividades normales de cada departamento.
- Establecer una comunicación directa con la UPC del cantón para dar con los responsables del robo.
- Proceder al trámite pertinente de las garantías de los equipos sustraídos por el robo, o a su vez comprar los equipos indispensables para retomar las operaciones.

### **Medidas Técnicas**

- Las autoridades de la municipalidad deben realizar una reunión con los directivos para hacer un inventario de las perdidas.
- Luego de adquirir los nuevos equipos sustraídos se procederá a restablecer los procesos en los equipos informáticos.
- Recoger los Backups, programas, manuales del sitio alternativo en donde se encuentran resguardados.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.
- Brindar el soporte pertinente a la restauración para verificar y probar la integridad de los datos.
- Iniciar las operaciones, sin pasar por alto las medidas de seguridad establecidas por las políticas internas de la municipalidad.

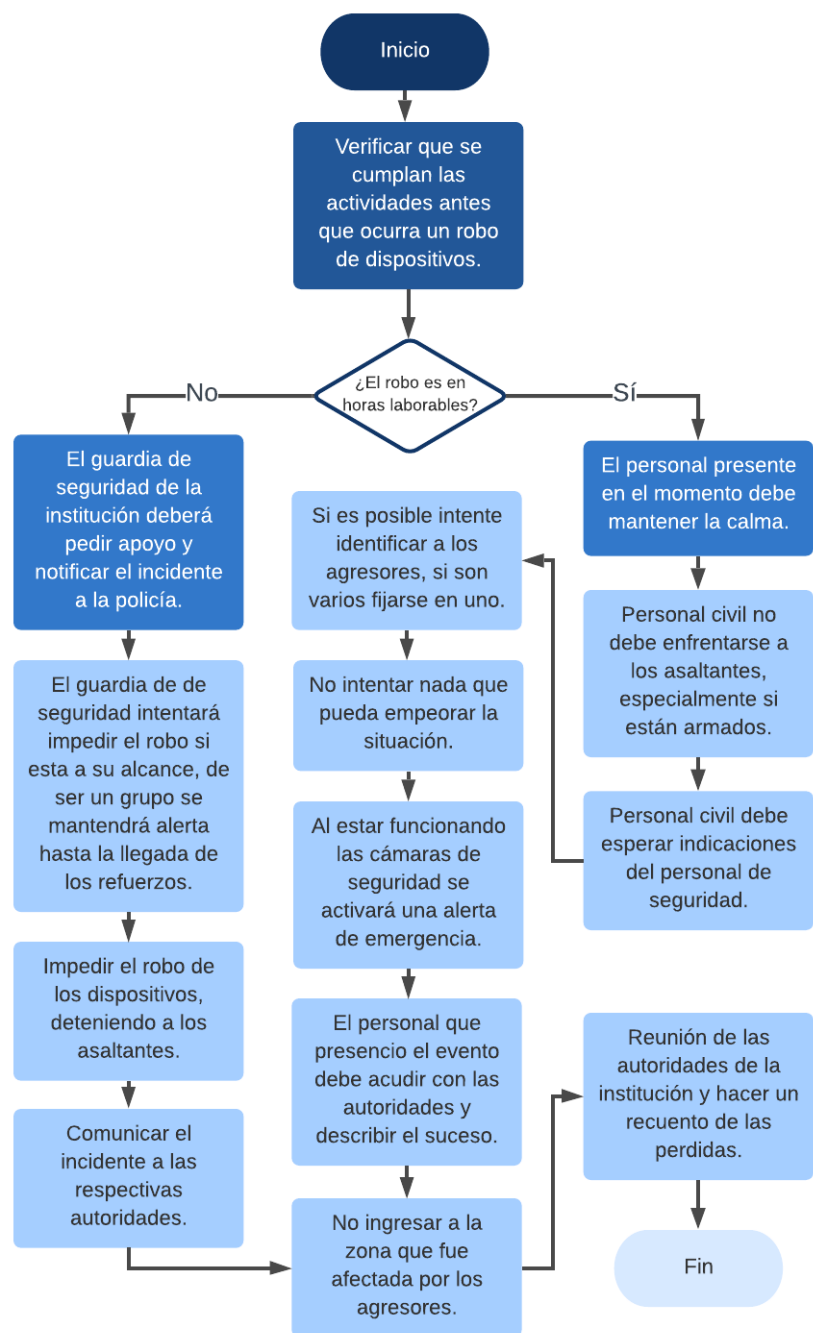


Figura 3.50: Acciones frente a un robo de dispositivos  
 Fuente: Elaborado por el autor

### **3.2.10.18. Clase de Riesgo: Atasco de papel en la impresora**

#### **ACTIVIDADES ANTES**

##### **Medidas Humanas**

- El personal que trabaja con las impresoras normales y multifuncional deben contar con una capacitación sobre el buen manejo de estos equipos que garanticen su funcionalidad.
- El papel que se utiliza en estos equipos debe ser de buena calidad.

##### **Medidas Técnicas**

- Asegurarse que el formato que va a imprimir sea el correcto ya que podría ser causa de un atasco si es un formato inapropiado.
- Se debe llenar las bandejas de papel de las impresoras al llegar al sitio de trabajo, evitando así que el papel este húmedo al pasar toda la noche en la máquina.
- Asegurarse que el papel se encuentre correctamente colocado en el cassette y no se encuentre demasiado lleno.
- Hay que considerar que el papel no se encuentre arrugado o roto y evitar mezclar diferentes tipos de papel en la bandeja de la impresora.

#### **ACTIVIDADES DURANTE**

##### **Medidas Humanas**

- El personal que labora en los diferentes departamentos no debe tratar de solucionar el incidente ya que puede empeorar la falla.
- Si la impresora se atasca en uno de los departamentos de la institución debe comunicar el incidente al técnico del departamento de TI.

##### **Medidas Técnicas**

- El técnico capacitado debe actuar con tranquilidad y paciencia, puesto a que una mala ejecución puede dañar el mecanismo de tracción del papel de la impresora y empeorar la situación.
- Se debe identificar el atasco de papel, algunas tienen la compuerta en la parte frontal y otras en la parte posterior del equipo.

- Seguir las instrucciones mostradas en la pantalla de la impresora (en el caso de tenerla).
- En el caso de no solucionar el inconveniente por el modelo de la impresora, se procede a apagar el equipo.
- Desconectar la impresora de la corriente eléctrica.
- Si el atasco de papel está localizado, se procede a retirar el papel suave y uniformemente utilizando las dos manos, siempre en el sentido de salida del papel ya que el mecanismo está diseñado para girar en un único sentido, forzar a sacarlo al revés haría que los engranajes se dañen.
- Para dar por terminado el proceso hay que asegurarse que no exista pequeños trozos de papel, si hubiera hay que sacarlos y así evitar atascos posteriores.
- Asegurarse que todas las compuertas estén cerradas las mismas que se abrió para solventar el problema.

## **ACTIVIDADES DESPUÉS**

### **Medidas Técnicas**

- El técnico debe hacer una prueba de impresión y verificar que la impresora se encuentre correctamente funcionando.
- Entrega del equipo informático por parte del técnico capacitado.
- Emitir un informe del daño que se solventó al jefe del departamento de TI.

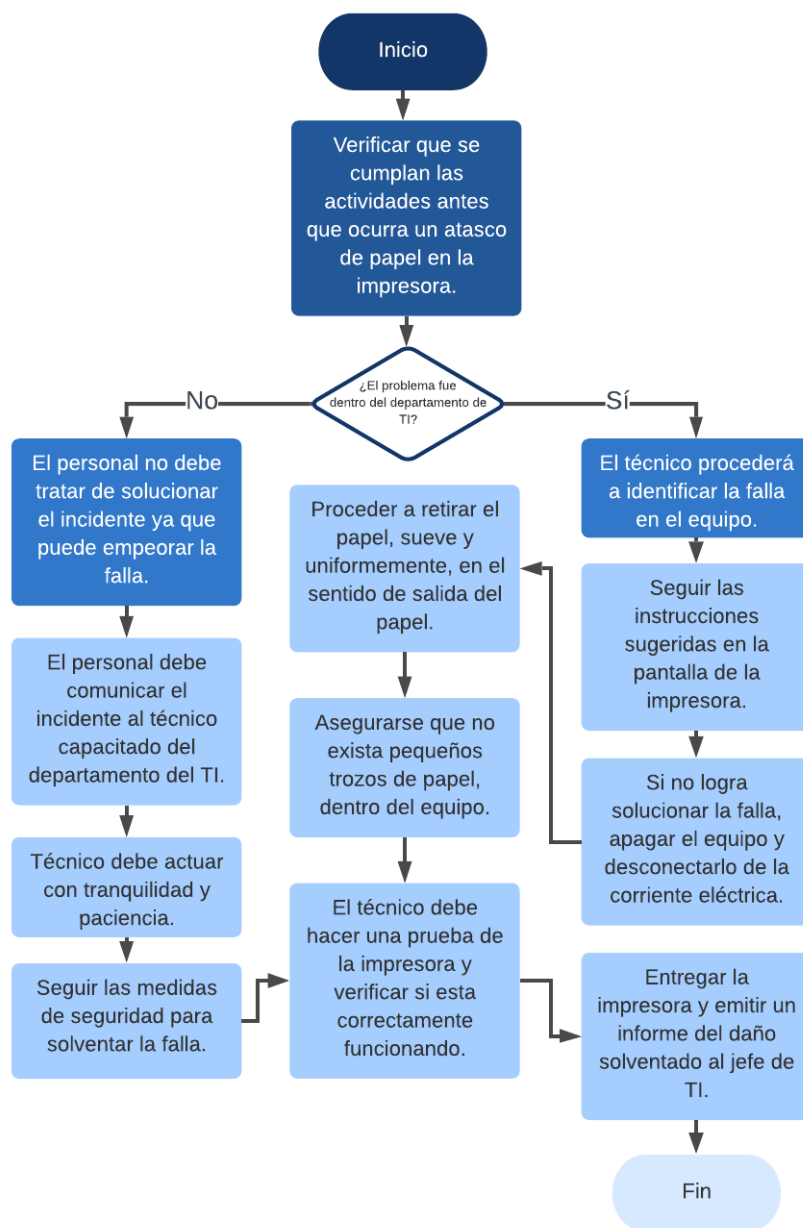


Figura 3.51: Acciones frente a un atasco de papel en la impresora  
 Fuente: Elaborado por el autor

### **3.2.10.19. Clase de Riesgo: El dispositivo (PC) no reconoce la impresora**

#### **ACTIVIDADES ANTES**

##### **Medidas Técnicas**

- El técnico de la institución debe realizar un mantenimiento preventivo a los equipos informáticos de manera periódica y evitar posibles fallas.
- Verificar periódicamente que las conexiones eléctricas entre los dispositivos estén en buen estado.
- Mantener actualizados los controladores (Drivers) de los equipos informáticos para evitar cualquier falla con los dispositivos externos como es el caso de la impresora.

#### **ACTIVIDADES DURANTE**

##### **Medidas Humanas**

- Si la impresora no reconoce en uno de los departamentos de la institución debe comunicar el incidente al técnico del departamento de TI.

##### **Medidas Técnicas**

- El técnico debe verificar que la conexión del equipo a la impresora se encuentre correctamente conectadas.
- El técnico capacitado verificará que los controladores (Drivers) del equipo se encuentren correctamente instalados o si existe alguna actualización disponible tanto en los controladores como en el sistema.
- Si no consigue solventar la falla, desinstale y reinstale el controlador correspondiente al modelo de la impresora correcta.
- Probar cambiando el cableado de conexión por otro que, si este funcionando y verificar si el equipo reconoce a la impresora.
- Si aún no logra solventar el problema probar la impresora con otro computador.

## ACTIVIDADES DESPUÉS

### Medidas Técnicas

- El técnico debe verificar que el dispositivo (PC), reconozca correctamente a la impresora, realizar las pruebas pertinentes con los equipos.
- Entrega del equipo informático por parte del técnico capacitado.
- Emitir un informe del daño que se solvento al jefe del departamento de TI.

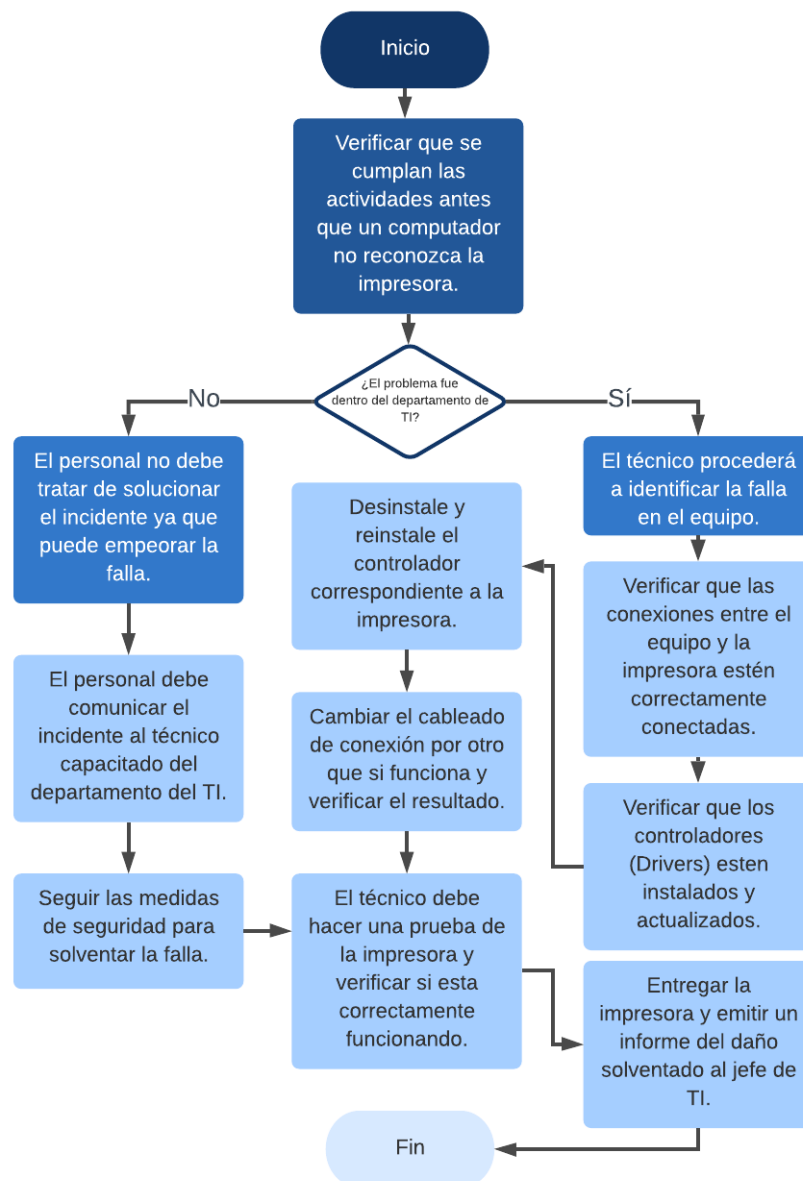


Figura 3.52: Acciones frente a un equipo que no reconoce la impresora  
Fuente: Elaborado por el autor

### **3.2.10.20. Clase de Riesgo: Presencia de interferencias electromagnéticas**

#### **ACTIVIDADES ANTES**

##### **Medidas Humanas**

- Si sospecha que existe algún tipo de interferencia comunicar el problema al departamento de TI, para que un técnico capacitado en el área se encargue de solventar el problema.

##### **Medidas Técnicas**

- Para evitar algún tipo de interferencias en la red se debe contar con un sistema de cableado apantallado que consiste en recubrir con una malla metálica en el cableado de red impidiendo la entrada de radiación hacia el interior.
- La energía apantallada debe tener su salida por lo que ira conectada a tierra, mediante un conector con protección metálica, estos conectores son iguales a los RJ45 con la diferencia que tienen una chapa metálica misma que une el metal del apantallamiento con el metal del conector de la tarjeta que se encuentra conectado a tierra.
- Evitar bucles en los cables de red, lo que se refiere a no dejar extensiones de cable sobrante solo lo necesario. Dado el caso que sobre cableado de red no hay que enrollarlo como si fuera una circunferencia, si no en forma de ocho logrando así que el bucle sea lo más pequeño posible, con esto evitamos que capte interferencias.
- Línea independiente para servicios, ya sea para limpieza o cualquier otro trabajo (aspiradora, taladro, pulidora, etc.), dentro del departamento de TI y sus áreas próximas a este involucra no conectar estos dispositivos en la misma línea eléctrica que utiliza los componentes informáticos y evitar perturbaciones electromagnéticas que pudieran ocasionar, afectando el trabajo que realizan los servidores, computadores, equipos de red.
- Evitar colocar equipos informáticos junto a cajas de energía eléctrica ya que estas pueden generar interferencia y provocar problemas.



## **ACTIVIDADES DURANTE**

### **Medidas Técnicas**

- Si existe pérdidas de la comunicación, corrupción en los datos e incluso ralentización de la transmisión de los mismos, se debe verificar cuales son los motivos que generan esta interferencia.
- El técnico capacitado en el tema debe verificar que las conexiones de red no se encuentren:
  - Con espacios libres entre las envolturas del cable y el conector, esto evitará interferencias.
  - Verificar si el cableado de red se encuentra raspado el recubrimiento.
  - Si el cable de red se encuentra torcido en su propio eje podría causar interferencia.
- El técnico capacitado en el área debe notificar la situación a las autoridades de la institución, así como al departamento de TI.
- Si es necesario cambiar el cableado de red común y colocar cableado apantallado junto con sus conectores respectivos se debe justificar la razón.
- Si el técnico tiene la autorización de las autoridades debe solventar el inconveniente.

## **ACTIVIDADES DESPUÉS**

### **Medidas Técnicas**

- El técnico capacitado debe verificar si existe algún tipo de interferencia en el área y descartar cualquier problema presentado.
- Emitir un informe del daño que se solvento a las autoridades y al jefe del departamento de TI.

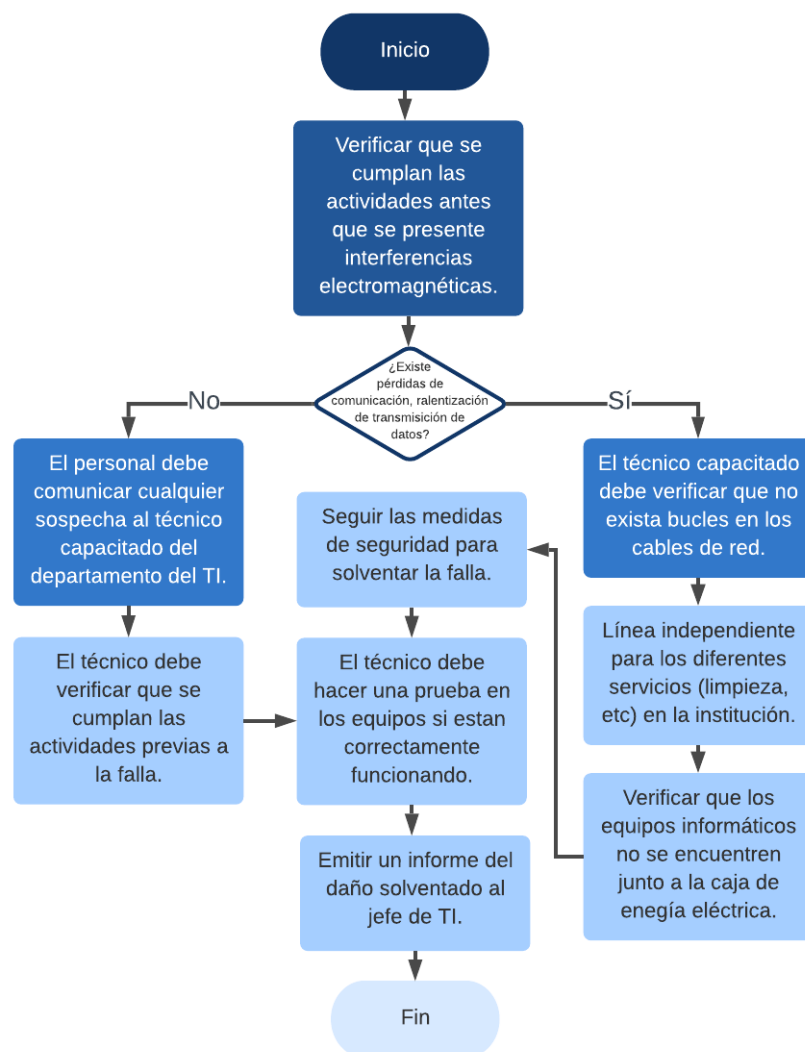


Figura 3.53: Acciones frente a inteferencias electromagnéticas  
Fuente: Elaborado por el autor

### **3.2.10.21. Clase de Riesgo: Ingeniería social**

#### **ACTIVIDADES ANTES**

##### **Medidas Humanas**

- Realizar capacitaciones frecuentes a todo el personal sobre temas de ingeniería social y cómo afectaría a la institución en caso de presentarse este tipo de ataques.

##### **Medidas Técnicas**

- Mantener de manera periódica Backus de los principales elementos de software necesarios para restablecer las actividades normales de la institución.
- Es importante contar siempre actualizado el sistema operativo y el antivirus.
- Colocar claves con letras, números y caracteres especiales para mayor seguridad.
- Se recomienda cambiar las claves de los sistemas y personales de manera periódica.
- Verificar periódicamente que el Firewall de la institución se encuentre activo y funcionando de manera correcta.

#### **ACTIVIDADES DURANTE**

##### **Medidas Humanas**

- Si existe sospecha de algún tipo de fraude o solicitud de información, debe comunicar el incidente al departamento de TI.
- Si no está absolutamente seguro sobre algún tipo de información publicada en internet, nunca de por cierto y acceda a brindar información privada.
- Desconfiar de los mensajes inesperados que son enviados de carácter de urgentes.
- La ortografía en mensajes sospechosos suele estar incorrecta, este es una primera señal de algún tipo de peligro.
- No debe aceptar cualquier tipo de oferta si usted no lo ha solicitado.

- No debe dar clic en ningún enlace que proceda de sitios desconocidos.
- Por ningún motivo revele su contraseña personal de ninguna cuenta o sistema que estén a su cargo.
- Aún siendo mensajes de contactos conocidos, debe tener precaución al descargar archivos adjuntos.

### **Medidas Técnicas**

- El personal del departamento de TI al ser notificados sobre la sospecha de fraude, se procederá a identificar la gravedad de la situación.
- Si la situación lo amerita el técnico cambiará las credenciales del usuario con el problema o sospecha.
- Si existe una sospecha en la alteración de la información se debe recurrir a gestionar las auditorias de los registros sospechosos y verificar si los movimientos son los adecuados.

## **ACTIVIDADES DESPUÉS**

### **Medidas Humanas**

- Si el personal de la institución cree que fue víctima de estafa o robo de información confidencial debe informar al departamento de TI la situación para que procedan a deshabilitar el usuario y restaurar la cuenta así evitar inconvenientes.

### **Medidas Técnicas**

- Realizar un análisis de la situación, y determinar el grado de afectación si se presento algún tipo ingeniería social que afecte a la institución.
- En el caso de sospechar algún tipo de ingreso no autorizado y cambios en los datos de la institución se debe acudir a las auditorias realizadas a la base de datos y verificar en sus registros.
- Recoger los Backups, programas, manuales del sitio alternativo en donde se encuentran resguardados.
- Restaurar la información correspondiente en la Base de Datos y sus respectivos programas.

- Brindar el soporte pertinente a la restauración para verificar y probar la integridad de los datos.
- Emitir un informe del daño que se solvento al jefe del departamento de TI.
- Iniciar las operaciones, sin pasar por alto las medidas de seguridad establecidas por las políticas internas de la municipalidad.

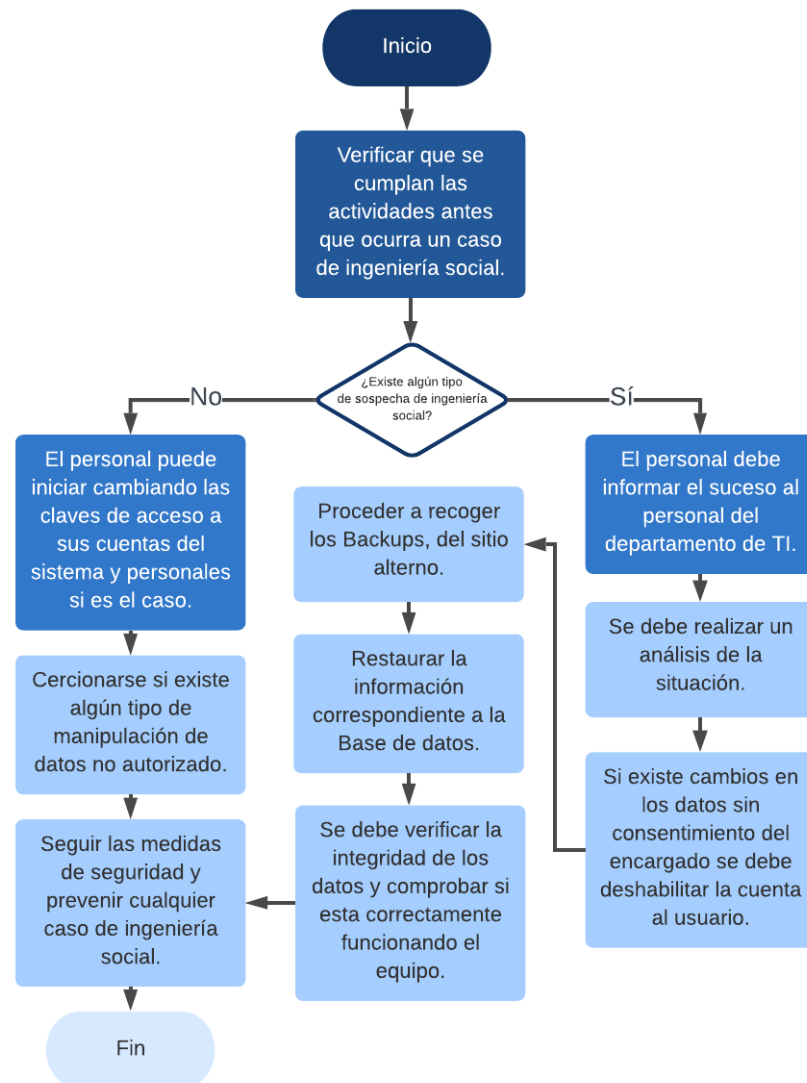


Figura 3.54: Acciones frente a un caso de ingeniería social  
Fuente: Elaborado por el autor

## CAPÍTULO 4

### CONCLUSIONES Y RECOMENDACIONES

#### 4.1. Conclusiones

- El presente proyecto ha permitido diseñar de un Plan de Contingencia Informático para G.A.D. Municipal del cantón Salcedo, estableciendo lineamientos sobre gestión de seguridad acorde con la Norma 410-11 de la C.G.E. (Contraloría General del Estado) del Ecuador, correspondiente a un plan de contingencia, asegurando así una correcta gestión de riesgos.
- Para tener una mayor solidez y respaldo para la elaboración del diseño del Plan de Contingencia Informático se tomó en consideración adicionalmente la metodología NTC-ISO/IEC 27005, en el cual plantea un conjunto de etapas donde se encuentran inmersos los lineamientos de seguridad estipulados en la norma 410-11 de la C.G.E. del Ecuador, garantizando así un adecuado seguimiento a esta norma.
- Se ha identificado los principales riesgos asociadas a sus causas y consecuencias usando la técnica denominada "análisis de corbata" (bow tie analysis), en el que se ha realizado una preevaluación donde se muestra el grado de negatividad según el tipo de riesgo.
- Para el análisis de la situación actual que atraviesa la municipalidad en cuanto al tema informático, se realizó una recolección de la información con la colaboración del personal del departamento de TI, quienes laboran el día a día y conocen sus fortalezas y debilidades de la institución, aplicado la técnica Delphi.
- El diseño del plan de contingencia que se propuso en el proyecto se elaboró de acuerdo con las necesidades del G.A.D. Municipal del cantón Salcedo en el que se detalla los recursos reales que cuenta la institución mejorando así los servicios que estos brindan y por ende contribuyendo con el crecimiento y excelencia de la municipalidad.
- De acuerdo con los resultados de evaluación de la probabilidad de ocurrencia y el impacto, se realizó una categorización mediante una matriz de

calificación de riesgo permitiendo identificar el grado de vulnerabilidad al cual se encuentra dicho activo informático.

- Se ha establecido de manera organizada y general las actividades a ejecutarse antes, durante y después junto con las acciones a realizarse sobre cada riesgo mismas que fueron complementadas con un diagrama de respuesta, que serán acciones de primera mano que servirán si un riesgo se materializa.
- Se cuenta con un análisis costo/perdida en el que se realizó una evaluación sobre las consecuencias que puede acarrear la interrupción de las actividades por hora de acuerdo con el equipo informático afectado, permitiendo tomar la mejor decisión para priorizar el mantenimiento correctivo inmediato, consiguiendo así una mínima afectación posible a la institución.
- El presente plan de contingencia informático realmente permite al departamento de TI y por ende a la municipalidad reaccionar adecuadamente ante posibles situaciones adversas que afecten las operaciones ocasionando una interrupción parcial o total en sus funciones habituales de la institución.

## 4.2. Recomendaciones

- El personal directivo del G.A.D. Municipal del cantón Salcedo en conjunto con el personal encargado del departamento de TI debe realizar un análisis sobre el plan de contingencia informático para su pronta implementación.
- Se debe verificar la efectividad de las acciones propuestas en el plan de contingencia informático, en caso de ocurrir algún tipo de riesgo y tener la seguridad de contar con un método seguro.
- Difundir mediante campañas de capacitación el contenido del presente plan de contingencia informático, con la finalidad de instruir adecuadamente al personal del G.A.D. Municipal del cantón Salcedo, creando de esta manera una cultura de colaboración y asistencia en la seguridad informática.
- Se debe considerar la adecuación del espacio físico al ser la principal fuente propensa a riesgos, para salvaguardar los equipos informáticos donde están alojados servicios e información de la institución.
- Mantener actualizado el plan de contingencia informático como mínimo una vez al año, permitiendo evaluar los equipos informáticos que se vayan adquiriendo, así como la creación y actualización de nuevos servicios o software, permitiendo así detectar la aparición de nuevos posibles riesgos donde se tome las medidas de seguridad pertinentes.



## Bibliografía

- [1] I. G. S. SABINO, *PROPUESTA DE APLICACIÓN DE UNA METODOLOGÍA PARA LA SEGURIDAD INFORMÁTICA EN LA DIVISIÓN DE CIENCIAS BÁSICAS*. Universidad Nacional Autónoma de México, 2009.
- [2] L. F. B. Jorge, *SEGURIDAD INFORMÁTICA ORIENTADA A PARTICULARES*. Universidad de San Carlos de Guatemala, 2015.
- [3] T. P. P. SHIRLEY, *DISEÑO DE UN PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LAS NORMAS ISO/IEC 22301 E ISO/IEC 27031 PARA LA FERRETERÍA CESAR S.A.S EN LA CIUDAD DE VALLEDUPAR*. UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD, 2018.
- [4] M. L. K. Alexandra, *DISEÑO DE UN PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LAS NORMAS ISO/IEC 22301 E ISO/IEC 27031 PARA LA FERRETERÍA CESAR S.A.S EN LA CIUDAD DE VALLEDUPAR*. UNIVERSIDAD TÉCNICA DEL NORTE UTN, 2015.
- [5] D. C. P. POZO, *PROPUESTA DE UN PLAN DE CONTINGENCIA DE TI PARA LA EMPRESA LOGICIEL*. ESCUELA POLITÉCNICA NACIONAL, 2016.
- [6] V. L. A. ALCÍVAR, *PLAN DE CONTINGENCIAS PARA EL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE CTT ESPE CECAI INNOVATIVA MATRIZ SANGOLQUÍ*. ESPE, 2014.
- [7] A. D. O. GUEVARA, *PLAN DE RIESGOS Y CONTINGENCIAS INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO INDUSTRIAL*. UTA, 2018.
- [8] L. P. Aguilera, *SEGURIDAD INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO INDUSTRIAL*. EDITEX SA, 2010.
- [9] RAE, *REAL ACADEMIA ESPAÑOLA*. RAE, 2014.

- [10] U. G. Baca, *SEGURIDAD INFORMÁTICAS BASADO EN UN ACUERDO DE NIVEL DE SERVICIO APLICADA A LA EMPRESA PLASTICAUCHO INDUSTRIAL*. Grupo Editorial Patria, 2016.
- [11] F. E, *FIRMA E*. Consultoría y Desarrollo TI, 2014.
- [12] OCDE, *PROTECCIÓN DE LA INFORMACIÓN*. Consultoría y Desarrollo TI, 2012.
- [13] UMU, *Introducción a la Seguridad Informática*. GESESI, 2017.
- [14] I. 27000, *Términos y definiciones sobre la seguridad de la información*. ISO, 2018.
- [15] C. 2019, *Glosario de Seguridad*. INTECO, 2010.
- [16] U. N. de Luján, *Amenazas a la Seguridad de la Información*. UNLu, 2014.
- [17] I. R. C. Martha, *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. 3ciencias, 2018.
- [18] R. López, *Fundación Universitaria AREANDINA*. 3ciencias, 2017.
- [19] C. Jean-Francois, *La seguridad informática en la PYME*. Grupo Editorial ENI, 2016.
- [20] A. G. C.-M. del Pilar Alegre, *Seguridad Informática - Madrid España*. Editorial Paraninfo SA, 2011.
- [21] S. O. O. y Omar Cervantes Sánchez, *SEGURIDAD INFORMÁTICA*. Eumedt, 2012.
- [22] V. Á. Gómez, *Enciclopedia de la Seguridad Informática 2da edición*. Editorial RA-MA S.A., 2017.
- [23] M. A. Oliva, *CONCEPTOS DE SEGURIDAD*. Universidad de Sevilla, 2006.
- [24] USS, *Seguridad para Empresas*. USS Seguridad, 2019.
- [25] C. J. Alberts and S. G. Behrens, *Operationally Critical Threat Asset and Vulnerability Evaluation OCTAVE*. Networked Systems Survivability Program, 2000.
- [26] G. de España, *MAGERIT versión 3*. Esquema Nacional de Seguridad, 2012.

- [27] E. K. Bezerra, *Gestión del riesgo de las TI NTC 27005*. Escuela Superior de Redes RED CEDIA, 2012.
- [28] J. P. J. y Hugo Llanos, *MEHARI 2010*. CLUSIF, 2010.
- [29] L. F. B. Guerrero, *NORMAS DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO*. CONTRALORIA GENERAL DEL ESTADO, 2009.
- [30] U. C. de Cuenca F M Arévalo, *Agile Methodology for Computer Risk Management*. Revista Killkana Técnica Vol 1 No2 pp 31-42, Mayo-Agosto 2017.
- [31] ICONTEC, *Norma Técnica NTC-ISO/IEC 27005*. Intituto Colombiano de Normas Técnicas y Certificación, 2009.
- [32] B. Hancock, *The Bow Tie analysis*. ERM Initiative, 2016.
- [33] M. R.-Á. y Mercedes Torrado-Fonseca, *El método Delphi*. Universidad de Barcelona REIRE, 2016.
- [34] C. Gallotti, *Information security- Risk Assessment Management Systems-the ISO/IEC 27001- pp. 69*. Massimo Cottafavi and Stefano Ramacciotti, 2019.
- [35] E. R. Taylor, *Guía para la administración del riesgo*. Departamento Administrativo de la Función Pública DAFP, 2009.
- [36] U. N. de Colombia, *Guía para la administración de riesgos operativos de procesos UN*. Sistema Integrado de Gestión Académica Administrativa y Ambiental, 2018.
- [37] B. M. y Chiluisa Sandra, *Auditoría Integral al GAD Salcedo Provincia de Cotopaxi*. ESPEL, 2014.
- [38] G. Salcedo, *Página Web Oficial del GAD Salcedo*. GAD Municipal del cantón Salcedo, 2014.
- [39] G. M. del cantón Salcedo, *Normas y políticas de seguridad informática para el GAD Municipal del cantón Salcedo*. Editorial Municipio del cantón Salcedo, 2019.
- [40] G. Salcedo, *GAD Municipal Salcedo*. Municipal, 2019.

- [41] A. C. D. ECUADOR, *CONSTITUCIÓN DEL ECUADOR*. ASAMBLEA CONSTITUYENTE, 2008.
- [42] COOTAD, *CÓDIGO ORGÁNICO DE ORGANIZACIÓN*. COOTAD, 2015.
- [43] J. Jordan, *ATLANTIC BT*. ATLANTIC, 2018.
- [44] I. G. de la Escuela Politécnica Nacional de Quito, *Los peligros volcánicos en el Ecuador*. Editorial IG-EPN IRD, 2005.
- [45] G. M. del cantón Salcedo, *PLAN DE CONTINGENCIA CANTONAL ANTE UNA POSIBLE ERUPCIÓN DEL VOLCÁN COTOPAXI*. Editorial Municipio del cantón Salcedo, 2019.
- [46] S. N. de Gestión de Riesgos y Emergencias, *Mapas de las rutas de evacuación y zonas seguras para el simulacro Cotopaxi*. Gobierno de la República del Ecuador, 2019.
- [47] T. Micro, *The Human Factor in Data Protection*. Ponemon Institute, 2012.
- [48] L. S. de Gestión de Riesgos, *Plan Nacional de Respuesta SGR del Ecuador*. RESPONDEc, 2018.
- [49] D. Concepto.de, *Sistema de información*. Concepto, 2012.
- [50] R. Content, *Servidor*. Redator Rock Content, 2019.

## **Anexos y Apéndices**

## Anexo A

### Equipos Informáticos de la institución

Nº SERVIDOR	TIPO (RACK/TORRE)	SISTEMA OPERATIVO	MARCA	MODELO	CAPACIDAD EN DISCO (STORAGE)	VALOR DEL SERVIDOR	PERDIDA POR HORA	MECANISMOS DE RESPALDO
Servidor 1	RACK	Linux Centos	HP	Proliant DL360 G10	4 X 600 Gb	\$ 3.000,00	\$ 500,00	Externo
Servidor 2	RACK	Linux Centos	HP	Proliant DL320 G8	250 Gb	\$ 2.500,00	\$2.500,00	Externo
Servidor 3	RACK	Linux Centos	HP	Proliant DL380 G7	250 Gb	\$ 2.000,00	\$1.500,00	Externo
Servidor 4	RACK	Linux Centos	HP	Proliant DL120 G7	250 Gb	\$ 2.000,00	\$ 500,00	Externo
Servidor 5	TORRE	Linux Centos	HP	Proliant ML150 G5	160 Gb	\$ 1.500,00	\$1.000,00	Externo
Servidor 6	TORRE	Linux Centos	HP	Proliant ML150 G6	160 Gb	\$ 1.500,00	\$3.000,00	Externo
Servidor 7	TORRE	Windows Server 2012	HP	Proliant ML150 G6	160 Gb	\$ 1.500,00	\$2.000,00	Externo

Tabla A.1: Servidores del G.A.D. Municipal del cantón Salcedo

Fuente: Elaborado por el autor

CANTIDAD	EQUIPO	DESCRIPCIÓN
2	Switch	24 PUERTOS QP-AVP24S QPCOM
2	Switch	24 PUERTOS GIGA QPCOM QP-G240R
1	Regletas para Bastidor para Rack	Nexxt Solutions para Rack AW220NXT95
1	Tripp Lite Rack Console 1URM	KVM Switch, 19" LCD 1080p Rackmount TAA
1	Cisco Router	4 Ports - Management Port / Slots Gigabit Ethernet
1	Central Telefónica con voz sobre IP	Teléfonos Grandstream BT200
5	UPS de TI	UPS - CA 120 V
1	Gabinete para Cableado de Alta Densidad y Servidores	Marca Quest International S.A.
1	HP LASER JET P2015DN	53A HP LASERJET
1	EPSON L355	54a HP LASERJET
1	HP COLOR LASERJET CP6015DN	HP COLOR LASERJET CB380A
1	Computador de escritorio	Intel(R) Core™ i7 - 870 CPU 2.93GHz
1	Computador de escritorio	Intel(R) Core™ i7 - 8550 CPU 1.80GHz
2	Laptops personales	Laptops personales
1	Aire acondicionado	Cuarto de Telecomunicaciones

Tabla A.2: Principales equipos informáticos del departamento de TI

Fuente: Elaborado por el autor

## Anexo B

### Principales Sistemas de Información de la institución

En la Tabla B.1, se muestra los niveles de prioridad de acuerdo con su puntaje respectivo, que será asignado a los Sistemas de Información de la municipalidad desarrollados tanto por el personal interno del departamento de TI como por terceros o externos a la institución.

PRIORIDAD	PUNTAJE
Baja	1
Media	2
Alta	3

Tabla B.1: Niveles de prioridad de Sistemas de información del G.A.D. Municipal

Fuente: Elaborado por el autor

En las Tablas B.2, B.3, B.4, se muestra un detalle con las principales características de los Sistemas de Información que cuenta la institución en la que se adjuntó la prioridad de restauración basándose en el análisis de riesgos anteriormente evaluados sobre cada uno de los servidores a los que estos sistemas de información pertenecen, complementándolo junto con la experiencia del personal de TI que está a cargo de mantener estos sistemas funcionando, garantizando así una continuidad en la operatividad de la municipalidad ante cualquier tipo de desastre o incidente.

NOMBRE DEL SERVICIO	DESCRIPCIÓN	ELABORACIÓN	CARACTERÍSTICAS ESPECIALES	EQUIPAMIENTO	ESTADO	PRIORIDAD
Servicio de correo electrónico.	Gestor de mensajería instantánea.	INTERNO	ZIMBRA. Open source (Linux, Apache, PHP, MySQL).	Conexión a la red e internet.	FUNCIONANDO	2
Sistema de recaudación del rubro Agua Potable.	Emisión y recaudación del rubro Agua Potable.	INTERNO	Open source (PHP/MySQL).	Conexión a la red local.	FUNCIONANDO	3
Sistema de recaudación de Activos y Patentes	Emisión y recaudación del Impuesto de Activos y Patentes.	INTERNO	Open source (Visual FoxPro/Tablas DBF).	Conexión a la red local.	FUNCIONANDO	3
Sistema de recaudación del Impuesto al Juego	Emisión y recaudación del Impuesto al Juego.	INTERNO	Open source (Visual FoxPro/Tablas DBF).	Conexión a la red local.	FUNCIONANDO	2
Sistema de recaudación de Locales Comerciales	Emisión y recaudación del Impuesto a los Locales Comerciales.	INTERNO	Open source (PHP/MySQL).	Conexión a la red local.	FUNCIONANDO	3
Sistema de recaudación del Puestos en el Mercado y Plazas	Emisión y recaudación de Puestos en el Mercado y Plazas.	INTERNO	Open source (Visual FoxPro/Tablas DBF).	Conexión a la red local.	FUNCIONANDO	3
Sistema de recaudación Especial de Mejoras	Emisión y recaudación de Mejoras.	INTERNO	Open source (PHP/MySQL).	Conexión a la red local.	FUNCIONANDO	2
Sistema de recaudación del Rubro Predio Urbano y años anteriores	Emisión y recaudación del Rubro Predio Urbano y años anteriores.	INTERNO	Open source (Visual FoxPro/Tablas DBF).	Conexión a la red local.	FUNCIONANDO	3
Sistema de recaudación del Rubro Predio Rural y años anteriores	Emisión y recaudación del Rubro Predio Rural y años anteriores.	INTERNO	Open source (Visual FoxPro/Tablas DBF).	Conexión a la red local.	FUNCIONANDO	3
Reloj Biométrico (Control de asistencia de empleados y trabajadores)	Control de asistencia de empleados y trabajadores.	INTERNO	Registro de marcaciones (Sistema del reloj biométrico)	Conexión a la red local.	FUNCIONANDO	1
Servicio de internet en la institución y aplicaciones web	Servicio de internet en la institución.	EXTERNO	Servicio de internet por C.N.T.	Conexión a la red e internet.	FUNCIONANDO	3
Actualización de contenidos de la página web institucional	Información general de la Municipalidad. Gestión Administrativa. Información de interés.	INTERNO	Joomla - HTML - MySQL	Conexión a la red e internet.	FUNCIONANDO	1
Servidor dedicado de Antivirus	Plataforma de control de Antivirus para la Municipalidad.	INTERNO	Panel de control (ESET Endpoint Security)	Conexión a la red local.	FUNCIONANDO	3
Servicio de Facturación Electrónica	Documento que cumple con los requisitos legales y reglamentarios exigibles para todos comprobantes de venta.	EXTERNO	EN EVALUACIÓN PARA USO INSTITUCIONAL	Conexión a la red e internet.	EN EVALUACIÓN	2
Servicio de Video vigilancia (ZONEMINDER)	Aplicaciones que proporcionan una completa solución de video vigilancia.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	3

Tabla B.2: Principales servicios del G.A.D. Municipal alojados en los servidores de la institución

Fuente: Elaborado por el autor



NOMBRE DEL SERVICIO	DESCRIPCIÓN	ELABORACIÓN	CARACTERÍSTICAS ESPECIALES	EQUIPAMIENTO	ESTADO	PRIORIDAD
Sistema de Gestión de contenidos	Sistema de gestión de contenidos o CMS, creación de bitácoras web.	INTERNO	WORDPRESS. Open source (Linux, Apache, MySQL, PHP).	Conexión a la red e internet.	FUNCIONANDO	1
Sistema (GUÍA RÁPIDA) Publicación de documentos	Permite almacenar, editar documentos, como guías de trámites, manuales, etc.	INTERNO	Open source / Servidor web Apache (PHP/MySQL).	Conexión a la red local.	FUNCIONANDO	1
Sistema de gestión de proyectos	Software de gestión de proyectos basado en la web.	INTERNO	COLLABTIVE. Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	EN EVALUACIÓN	1
Sistema para compartir videos para aulas virtuales (PHPMOTION)	Facilidad para subir vídeos directamente desde el computador del usuario.	INTERNO	PHPMOTION. Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	EN EVALUACIÓN	1
Gestor de mensajería instantánea (INTRAMESSENGER)	Gestor de mensajería instantánea.	INTERNO	IntraMessenger. Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	1
Administración de Base de Datos MySQL (phpMyAdmin)	Permite la administración de bases de datos MySQL.	INTERNO	phpMyAdmin. Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	3
Sistema de emisión de memorandos (Comunicaciones internas)	Seguimiento a comunicaciones internas, (memos enviados, memos recibidos).	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	1
Sistema de recepción de oficios externos y guía de trámites	Control de Oficios recibidos, seguimiento a las comunicaciones Externas.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red e internet.	FUNCIONANDO	1
Sistema de permisos de personal (institucionales)	Control de emisión de permisos personales. Autorización de permisos. Informes y reportes de los permisos individual y departamental.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red e internet.	FUNCIONANDO	1
Registro de Actas y Denuncias en la Comisaría (Administración)	Registro de denuncias. Reportes. Emisión de Resoluciones.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	2
Registro de Vales pagados	Facilita la búsqueda de vales pagados.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	1
Registro de Profesionales (Obra civil)	Archivo digital de Registro de Profesionales.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	1
Registro de Ordenanzas, Reformas, Actas	Archivo digital, el usuario puede buscar y descargar la ordenanza digitalizada en PDF.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	2
Registro y emisión de ordenes de pago	Archiva una orden de pago y la imprime para su uso en Rentas.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	2

Tabla B.3: Principales servicios del G.A.D. Municipal alojados en los servidores de la institución

Fuente: Elaborado por el autor

NOMBRE DEL SERVICIO	DESCRIPCIÓN	ELABORACIÓN	CARACTERÍSTICAS ESPECIALES	EQUIPAMIENTO	ESTADO	PRIORIDAD
<b>Reportes de citaciones y Autos de pago de Coactiva</b>	Migra la información de cartera vencida de las bases de datos institucionales hacia la intranet, permitiendo en un formato válido imprimir citaciones y autos de pago de diferentes rubros de recaudación.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red e internet.	FUNCIONANDO	3
<b>Registro de personal Institucional</b>	Registro a todo el personal institucional para el uso de memos, permisos, oficios, etc.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	1
<b>Sistema de inventario de equipos de computo institucionales</b>	Almacena número de serie de cada equipo de cómputo, marca, modelo, color, periféricos.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	1
<b>Sistema de sugerencias para el departamento de sistemas (Buzón)</b>	Archiva sugerencias.	INTERNO	Open source (Linux, Apache, MySQL, PHP).	Conexión a la red local.	FUNCIONANDO	1
<b>Sistema Integral de Catastros (Sistema AME predio Urbano)</b>	Permite el avalúo, emisión, control y recaudación de los predios urbanos y rurales. Registro de usuarios nuevos. Información de los contribuyentes con los datos de los predios. Claves de acceso.	EXTERNO	Control: AME (Motor de base de datos MySQL)	Conexión a la red e internet.	FUNCIONANDO	3
<b>Sistema Integral de Catastros (Sistema AME predio Rural)</b>	Módulo de Catálogos, Módulo Contabilidad, Módulo Presupuesto, Módulo Inventario, Módulo Activos Fijos, Módulo Tesorería, Módulo R.R.H.H. , Módulo Proyectos, Claves de acceso.	EXTERNO	Control: AME (Motor de base de datos MySQL)	Conexión a la red e internet.	FUNCIONANDO	3

Tabla B.4: Principales servicios del G.A.D. Municipal alojados en los servidores de la institución

Fuente: Elaborado por el autor

## Anexo C

### Formato para el inventario de hardware y software de las PC'S de la institución

<b>FORMATO PARA EL INVENTARIO DE HARDWARE Y SOFTWARE DE LAS PC'S DEL G.A.D. MUNICIPAL DEL CANTÓN SALCEDO</b>	
<b>Fecha del inventario:</b>	
<b>Elaborado por:</b>	
<b>Nombre del departamento:</b>	
<b>Anexo para el inventario de los computadores de la institución</b>	
<b>Nombres del funcionario a cargo:</b>	
<b>Rol que desempeña el funcionario:</b>	
<b>Nombre del equipo:</b>	
<b>Dirección IP:</b>	
<b>Mascara de Subred:</b>	
<b>Nombre de Dominio:</b>	
<b>Modelo del Procesador:</b>	
<b>Marca:</b>	
<b>Modelo:</b>	
<b>Número de procesadores:</b>	
<b>Velocidad Procesador:</b>	
<b>Sistema Operativo:</b>	
<b>Versión de Sistema Operativo:</b>	
<b>Memoria RAM:</b>	
<b>Capacidad de Almacenamiento:</b>	
<b>Seriales de los componentes:</b>	
Observaciones: ..... ..... ..... .....	

Tabla C.1: Formato para el inventario de PC'S de la institución

Fuente: Elaborado por el autor en base a los registros del G.A.D. Municipal

## Anexo D

### Formulario de Solicitud de Acceso a Sistemas de Información de la institución

FORMATO PARA SOLICITAR ACCESO A LOS SISTEMAS DE INFORMACIÓN DEL G.A.D. MUNICIPAL DEL CANTÓN SALCEDO	
<b>Datos Generales</b>	
<b>Nombre del departamento:</b>	
<b>Datos del usuario:</b>	
<b>Apellidos y nombres del funcionario:</b>	
<b>Cargo:</b>	
<b>Teléfono:</b>	
<b>Correo electrónico:</b>	
<b>Perfil del funcionario a crear o modificar</b>	
<b>Creación</b>	<b>Modificación</b>
Perfil N°: _____ <input type="checkbox"/>	Eliminación: <input type="checkbox"/>
	Cambio de perfil: <input type="checkbox"/>
<b>Registro de firmas</b>	
_____	_____
<b>Cargo:</b> .....	<b>Cargo:</b> .....
<b>Fecha:</b> .....	<b>Fecha:</b> .....
<b>Solicitante:</b> .....	<b>Autoriza:</b> .....
<b>Aprobación (Uso Interno del Departamento)</b>	
_____	
<b>Jefe del departamento:</b> .....	
<b>Fecha:</b> .....	
Observaciones: .....	
.....	
.....	

Tabla D.1: Formato para solicitar acceso a los sistemas de información

Fuente: Elaborado por el autor en base a los registros del G.A.D. Municipal

## Anexo E

### Formulario para la creación de usuario y responsabilidad de contraseñas de la institución

FORMULARIO PARA LA CREACIÓN DE USUARIO Y RESPONSABILIDAD DE CONTRASEÑAS DENTRO DEL G.A.D. MUNICIPAL DEL CANTÓN SALCEDO	
<b>Datos Generales</b>	
<b>Nombre del departamento:</b>	
<b>Información del funcionario (Solicitante)</b>	
<b>Apellidos y nombres:</b>	
<b>Cargo:</b>	
<b>Teléfono:</b>	
<b>Correo electrónico:</b>	
<b>Perfil del usuario a crear</b>	
<b>Sistema de Información:</b>	
<b>Usuario:</b>	
<b>Contraseña:</b>	
<b>Obligaciones del nuevo usuario</b>	
<ul style="list-style-type: none"> <li>▪ La contraseña es de uso personal e intransferible, no puede ser otorgada a otro funcionario o persona ajena a la institución por ninguna circunstancia.</li> <li>▪ En el caso de requerir cambio en el perfil de usuario, debe comunicarse con el departamento de TI (Tecnologías de la información) del G.A.D. Municipal.</li> <li>▪ Si el funcionario es suspendido temporal o definitivamente de su cargo, se debe comunicar de forma inmediata al administrador de usuarios.</li> <li>▪ El funcionario debe memorizar la contraseña y no tener escrito en ningún o lugar ya que puede ser encontrado por alguna persona ajena.</li> <li>▪ Si el funcionario no se encuentra utilizando es sistema, deberá cerrar su sesión de usuario.</li> </ul>	
<b>Registro de firmas</b>	
_____	_____
<b>Cargo:</b> .....	<b>Cargo:</b> .....
<b>Fecha:</b> .....	<b>Fecha:</b> .....
<b>Solicitante:</b> .....	<b>Autoriza:</b> .....
<b>Observaciones:</b> .....	
.....	
.....	

Tabla E.1: Formato para la creación de usuario y responsabilidad de contraseña

Fuente: Elaborado por el autor en base a los registros del G.A.D. Municipal

## Anexo F

### Formato para la realización de Backups o Copias de Seguridad

Considerando el apoyo del equipo de trabajo del departamento de TI de la institución, se define un formato que se llevará como medida de control ante los backups diarios, semanales y mensuales que se vayan desarrollando en la municipalidad.

<b>FORMATO PARA EL REGISTRO DE BACKUPS DEL G.A.D. MUNICIPAL DEL CANTÓN SALCEDO</b>					
<b>Código:</b>					
<b>Versión:</b>					
<b>Anexo de Periodicidad para la realización de Backups o Copias de Seguridad</b>					
<b>Fecha de actualización:</b>					
<b>Elaborado por:</b>					
<b>Sistema de Información</b>	<b>Tipo de Backup</b>	<b>Periodicidad del Backup</b>	<b>Medio de Almacenamiento</b>	<b>Lugar de Almacenamiento</b>	<b>Persona que lo genera</b>
Observaciones: .....					
.....					
.....					
.....					

Tabla F.1: Formato para el registro de Backups

Fuente: Elaborado por el autor en base a los registros del G.A.D. Municipal

## Anexo G

### Formulario para el registro, tratamiento y valoración de incidentes en la institución.

FORMULARIO PARA EL REGISTRO, TRATAMIENTO Y VALORACIÓN DE INCIDENTES DENTRO DEL G.A.D. MUNICIPAL DEL CANTÓN SALCEDO	
Datos Generales	
Nombre del departamento:	
Elaborado por:	
Nº: de incidente:	
Prioridad:	
Departamento afectado:	
Usuarios afectados:	
Información del Incidente	
Breve descripción:	..... .....
Posible causa:	
Fecha y hora aproximada del inicio del incidente:	
Fecha y hora de detección:	
Fecha y hora de restauración:	
Equipos afectados:	
Sistemas afectados:	
Protocolos atacados (HTTP, POP, etc.):	
Tiempo estimado de suspensión del servicio:	
Costo estimado del incidente:	
Actividades de restauración:	
Resolución:	
Registro de firmas	
_____	_____
Cargo: .....	Cargo: .....
Fecha: .....	Fecha: .....
Solicitante: .....	Autoriza: .....
Observaciones: .....	
.....	
.....	

Tabla G.1: Formato para el registro, tratamiento, y valoración de incidentes

Fuente: Elaborado por el autor en base a los registros del G.A.D. Municipal

## Anexo H

Inventario de los equipos informáticos acorde con su respectivo funcionario y rol desempeñado en la institución (Actualizado hasta el 30 de junio de 2020).

### H.1. PRIMERA PLANTA (EDIFICIO ANTIGUO Y NUEVO)

#### TESORERÍA

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe tesorería	Katty González	10.10.0.91	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/ 8,00 GB - RAM
2	Analista de tesorería	Patricia Bustos	10.10.0.90	Microsoft Windows 7 Professional 7600 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz / 4,00 GB - RAM
3	Auxiliar de tesorería	Alexandra Berrazueta	10.10.0.97	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/ 8,00 GB - RAM
4	Notificador	Ángel Chillagana	10.10.0.183	Microsoft Windows 7 Professional 7600 - Intel(R) Core™ i7 - 870 CPU 2.93GHz / 4,00 GB - RAM
5	Secretaria de Coactivas	Delia Donoso	10.10.0.98	Microsoft Windows 7 Professional 7600 - Intel(R) Core™ i7 - 870 CPU 2.93GHz / 4,00 GB - RAM
6	Recaudador Ventanilla 1	Luis Jiménez	10.10.0.92	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/16,00 GB-RAM
7	Recaudador Ventanilla 2	Estefanía Toro	10.10.0.93	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/8,00 GB-RAM
8	Recaudador Ventanilla 3	Diego Alegría	10.10.0.95	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/4,00 GB-RAM
9	Recaudador Ventanilla 4	Ana Morales	10.10.0.94	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/8,00 GB-RAM

Tabla H.1: Equipos del departamento de tesorería

Fuente: Elaborado por el autor



## CONTABILIDAD

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe contabilidad	Mariana de la Vega	10.10.0.41	Microsoft Windows 7 Professional 7600 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz / 8,00 GB - RAM
2	Jefe contabilidad	Mariana de la Vega	10.10.0.42	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
3	Auxiliar de contabilidad	Guenda Cepeda	10.10.0.43	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/ 8,00 GB - RAM
4	Analista de contabilidad	Fernanda Cevallos	10.10.0.46	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
5	Secretaria de Coactivas	Janeth Chillagana	10.10.0.40	Microsoft Windows XP Professional Service Pack 3 -2600 – Intel Corp. TCIBX10H.86A CPU 2926MHz / 4,00 GB - RAM

Tabla H.2: Equipos del departamento de contabilidad

Fuente: Elaborado por el autor

## RENTAS

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe de rentas	Fernando Peralta	10.10.0.83	Microsoft Windows 7 Professional Intel(R) Core™ i7 - 4790 CPU 3.60GHz / 8,00 GB - RAM
2	Técnico de rentas	Marcos Tonato	10.10.0.82	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/ 8,00 GB - RAM
3	Técnico de rentas	Fernando Cepeda	10.10.0.81	Microsoft Windows 7 Professional Intel(R) Core™ i7 - 4790 CPU 3.60GHz / 8,00 GB - RAM
4	Analista de rentas	Germania Amores	10.10.0.80	Microsoft Windows 7 Professional Intel(R) Core™ i7 - 4790 CPU 3.60GHz / 8,00 GB - RAM

Tabla H.3: Equipos del departamento de rentas

Fuente: Elaborado por el autor

## AVALÚOS Y CATASTROS

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe de avalúos y catastros	Francisco Villagómez	10.10.0.71	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 3.20 GHz/ 8,00 GB - RAM
2	Secretaria de avalúos y catastros	Velastegui Molina	-	MANTENIMIENTO
3	Técnica de avalúos y catastros	Velastegui Ángel	10.10.0.79	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 860 CPU 2.80 GHz/ 4,00 GB - RAM
4	Técnica de avalúos y catastros	Rodrigo Garzón	10.10.0.73	Microsoft Windows 8.1 Pro - Intel(R) Core™ i7 - 4770 CPU 3.40GHz / 8,00 GB - RAM
5	Técnica de avalúos y catastros	Juan Changoluisa	10.10.0.78	Microsoft Windows 7 Professional - Intel(R) Core™ 2 Quad- Q8400 CPU 2.66GHz/ 4,00 GB - RAM
6	Técnica de avalúos y catastros	Juan Quispe	10.10.0.16	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
7	Técnica de avalúos y catastros	Cesar Paredes	10.10.0.77	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
8	Técnica de avalúos y catastros	Luis Jarrin	10.10.0.74	Microsoft Windows XP Professional - Service Pack 3 GenuineIntel- 3392MHz/4GB- RAM
9	Técnica de avalúos y catastros	Juan Córdova	10.10.0.76	Microsoft Windows 7 Professional - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB-RAM
10	Técnico en el área rural en avalúos y catastros	Mónica Gualpa	10.10.0.70	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM

Tabla H.4: Equipos del departamento de avalúos y catastros

Fuente: Elaborado por el autor

## OBRAS PÚBLICAS

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Director de obras públicas	Diego Soria	10.10.0.24	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93 GHz/ 4,00 GB - RAM
2	Secretaria de obras públicas	Cecilia Garcés	10.10.0.27	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
3	Especialista en vialidad	Pedro Silva	10.10.0.115	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93 GHz/ 4,00 GB - RAM
4	Jefe de parques y jardines	Víctor Noroña	10.10.0.26	Microsoft Windows10 - Intel(R) Core™ i7 - 8400 CPU 3.20GHz / 16,00 GB - RAM
5	Gestión Ambiental (Especialista de parques y jardines)	Sin funcionario	10.10.0.21	Microsoft Windows XP - Intel(R) Pentium 4/ CPU 3GHz/ 4GB- RAM
6	Jefe de infraestructura	Diana Pacheco	10.10.0.23	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
7	Infraestructura	Nataly Jiménez	10.10.0.22	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
8	Infraestructura	Luis Salguero	10.10.0.25	Microsoft Windows 10 Pro - Intel(R) Core™ i7 - 7700 CPU 3.60GHz/ 8,00 GB-RAM
9	Especialista en vehicular y maquinaria	Diego Tapia	10.10.0.28	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/8,00 GB-RAM
10	Ayudante de cuadrilla	Cristian Tipanquiza	SIN IP	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM

Tabla H.5: Equipos del departamento de obras públicas

Fuente: Elaborado por el autor

## AGUA POTABLE

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Director de agua potable	Patricio Avilés	-	LAPTOP PERSONAL
2	Secretaria de agua potable	Diana Romero	10.10.0.34	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
3	Inspector de lecturas	Luis Cruz	10.10.0.31	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
4	Catastro	Patricio Tamayo	10.10.0.37	Microsoft Windows 7 Professional - Intel(R) Core™ i7 - 870 CPU 2.93 GHz / 4,00 GB - RAM
5	Analista de agua potable	Marcelo Tigmasa	10.10.0.35	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 7700 CPU 3.60GHz/ 16GB - RAM
6	Ayudante de campo	José Jiménez	10.10.0.36	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3540 CPU 3.00GHz/ 4,00 GB - RAM

Tabla H.6: Equipos del departamento de agua potable

Fuente: Elaborado por el autor

## ARCHIVO

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe secretaria general	Tarquino Naranjo	-	LAPTOP PERSONAL
2	Auxiliar de documentación y archivo	Juan Vizcaíno	10.10.0.68	Microsoft Windows 7 Professional - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
3	Atención ciudadana	Inés Garcés	10.10.0.66	Microsoft Windows XP Professional - Service Pack 3 GenuineIntel- 2833MHz/2GB- RAM

Tabla H.7: Equipos del departamento de archivo

Fuente: Elaborado por el autor

## INFORMÁTICA

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe del departamento de TI	Enrique Arcos	10.10.1.8	LAPTOP PERSONAL
2	Analista de sistemas	Paulina Villalba	10.10.0.9	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
3	Técnico de sistemas	Juan Córdoba	10.10.1.9	Microsoft Windows 10 Pro- Intel(R) Core™ i7 - 8550 CPU 1.80GHz / 16,00 GB - RAM

Tabla H.8: Equipos del departamento de TI

Fuente: Elaborado por el autor

## COMUNICACIÓN SOCIAL

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe de comunicación social	Juan Candonga	10.10.0.51	MacBook Pro - Intel(R) Core™ i7 - CPU 2.9 GHz/ 8,00 GB - RAM
2	Diseñador	Israel Arcos	10.10.0.50	Microsoft Windows 10 Pro- Intel(R) Core™ i7 - 870 CPU 2.93GHz / 12,00 GB - RAM
3	Periodista	Mónica Acosta	10.10.0.49	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i3 - 2100 CPU 3.10GHz/ 8,00 GB - RAM
4	Auxiliar de comunicación social	Francisco Vivas	10.10.0.87	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 8,00 GB - RAM

Tabla H.9: Equipos del departamento de comunicación social

Fuente: Elaborado por el autor

## COMPRAS PÚBLICAS

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Director de compras públicas	Sin funcionario	10.10.0.146	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
2	Director de compras públicas	Margare Guerrero	10.10.0.145	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
3	Asistente de compras	Paola Chilingua	10.10.0.143	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i3 - 2100 CPU 2.80GHz/ 4,00 GB - RAM
4	Sin cargo	Sin funcionario	10.10.0.144	Microsoft Windows 7 Professional - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM

Tabla H.10: Equipos del departamento de compras públicas

Fuente: Elaborado por el autor

## DIRECCIÓN FINANCIERA

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Directora de dirección financiera	Gabriela Arias	10.10.0.96	Microsoft Windows 7 Professional Intel(R) Core™ i7 - 4790 CPU 3.60GHz / 8,00 GB - RAM
2	Analista de dirección financiera	Daisy Viteri	10.10.0.182	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i5 - 2400 CPU 3.10GHz/ 4,00 GB - RAM
3	Secretaria de dirección financiera	Guadalupe Villalba	10.10.0.197	Microsoft Windows 7 Professional Intel(R) Core™ i7 - 4770 CPU 3.40GHz / 6,00 GB - RAM

Tabla H.11: Equipos del departamento financiero

Fuente: Elaborado por el autor

## PLANIFICACIÓN

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Director de planificación	Álvaro Villota	-	LAPTOP PERSONAL
2	Jefe de planeamiento de suelos	Hugo Herrera	10.10.0.126	Microsoft Windows 10 - Intel(R) Core™ i7 - 7700 CPU 3.60GHz / 16,00 GB - RAM
3	Jefe de gestión urbana y rural	Edison Carrillo	10.10.0.120	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
4	Analista de gestión urbana y rural	Blanca Cando	10.10.0.234	Microsoft Windows 7 Ultimate Service Pack 1 - Intel(R) Pentium 4 - CPU 3.00GHz/ 2,00 GB - RAM
5	Topógrafo	Jorge Quispe	10.10.0.121	Microsoft Windows 7 Professional - Intel(R) Core™ i7 - 870 CPU 2.93GHz / 4,00 GB - RAM
6	Secretaria	Leonor Tercero	10.10.0.233	Microsoft Windows 7 Professional - Intel(R) Core™ i3 - 550 CPU 3.20GHz / 2,00 GB - RAM
7	Gestión urbana y rural	Pablo Tapia	10.10.0.123	Microsoft Windows 7 Professional Service Pack 1-Intel(R) Core™ 2 Quad -CPU 2.66GHz/4,00 GB-RAM
8	Técnico de planeamiento de suelos	Diego Villacis	10.10.0.127	Microsoft Windows 8.1 Pro - Intel(R) Core™ i7 - 8700 CPU 3.20GHz/8,00 GB-RAM
9	Gestión urbana y rural, Movilidad	Carolina Freire	169.254.71.210	Microsoft Windows10 - Intel(R) Core™ i5 - 7400 CPU 3.00GHz / 8,00 GB - RAM

Tabla H.12: Equipos del departamento de planificación

Fuente: Elaborado por el autor

## PRESUPUESTO

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe del área de presupuesto	Salazar María Augusta	10.10.0.106	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/ 8,00 GB - RAM
2	Auxiliar de presupuesto	Evelin Jácome	10.10.0.107	Microsoft Windows 8.1 Pro - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/ 8,00 GB - RAM
3	Analista de presupuesto	Mónica Mollocana	10.10.0.105	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM

Tabla H.13: Equipos del departamento de presupuesto

Fuente: Elaborado por el autor

## H.2. SEGUNDA PLANTA (EDIFICIO ANTIGUO Y NUEVO)

### ADMINISTRATIVO

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe del departamento administrativo	Fernanda Navas	10.10.0.186	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4770 CPU 3.40GHz/ 6,00 GB - RAM
2	Jefe del departamento administrativo	Fernanda Navas	10.10.0.189	Microsoft Windows XP Professional - Service Pack 3 GenuineIntel- 2992MHz/2GB- RAM
3	Analista del departamento administrativo	Rosa Ortiz	10.10.0.184	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
4	Analista del departamento administrativo	Olga Teneda	10.10.0.187	Microsoft Windows 7 Starter - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM

Tabla H.14: Equipos del departamento administrativo

Fuente: Elaborado por el autor

### ALCALDÍA

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Secretaria de alcaldía	Jaqueline Chano	10.10.0.166	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4770 CPU 3.40GHz/ 6,00 GB - RAM

Tabla H.15: Equipos del departamento de la alcaldía

Fuente: Elaborado por el autor

### SECRETARÍA GENERAL

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Secretaria general	Tarquino Naranjo	10.10.0.161	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
2	Secretaria de secretaria general	Ana Navas	10.10.0.162	Microsoft Windows XP Professional - Service Pack 3 GenuineIntel- 2992MHz/2GB- RAM

Tabla H.16: Equipos del departamento de secretaría general

Fuente: Elaborado por el autor

## AUDITORÍA - PROCURADURÍA

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Procuraduría	Cecilia Guagua	10.10.0.102	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
2	Procuraduría	Natalia Santamaria	10.10.0.100	Microsoft Windows 10 Pro - - Intel(R) Core™ i7 - 6500 CPU 2.50GHz/ 8,00 GB - RAM

Tabla H.17: Equipos del departamento de auditoría - procuraduría

Fuente: Elaborado por el autor

## DESARROLLO ORGANIZACIONAL

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Director del departamento organizacional	Sin funcionario	10.10.0.114	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
2	Asistente de desarrollo organizacional	Sin funcionario	10.10.0.210	Microsoft Windows 7 Professional - Intel(R) Core™ i7 - 4770 CPU 3.40GHz/ 4,00 GB - RAM

Tabla H.18: Equipos del departamento de desarrollo organizacional

Fuente: Elaborado por el autor

## TALENTO HUMANO

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe de talento humano	Fernando Vásquez	10.10.0.118	Microsoft Windows 8.1 Pro - Intel(R) Core™ i5 - 7400 CPU 3.00 GHz/ 4,00 GB - RAM
2	Jefatura de personal	Maritza Velasco	10.10.0.111	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
3	Analista de talento humano	Cristian Herrera	10.10.0.199	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i5 - 2410 CPU 2.30GHz/ 4,00 GB - RAM
4	Analista de talento humano	Luis Lascano	10.10.0.112	Microsoft Windows10 - Intel(R) Core™ i7 - 8400 CPU 3.20GHz / 16,00 GB - RAM
5	Secretaria	Elsa Fernández	10.10.0.113	Microsoft Windows XP Professional - Service Pack 3 GenuineIntel- 2327MHz/4GB- RAM
6	Técnico seguridad industrial	Alex Guasgua	10.10.1.5	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM

Tabla H.19: Equipos del departamento de talento humano

Fuente: Elaborado por el autor



## GESTIÓN AMBIENTAL Y SERVICIOS PÚBLICOS

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Administrador del cementerio	Wilson Quispe	10.10.0.223	Microsoft Windows 10 Pro - Intel(R) Core™ i7 - 7700 CPU 3.60GHz/ 16,00 GB - RAM
2	Analista de gestión ambiental	Gustavo Caiza	10.10.0.228	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
3	Jefe servicios públicos	Sin funcionario	10.10.0.226	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
4	Analista de gestión ambiental	Jessica Bautista	-	LAPTOP PERSONAL
5	Director de servicios públicos y gestión ambiental	Sin funcionario	10.10.0.220	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
6	Jefe de gestión ambiental	Sin funcionario	10.10.0.225	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
7	Secretaria de gestión ambiental y servicios públicos	Luci Palomo	10.10.0.221	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4400 CPU 2.00GHz/ 2,00 GB - RAM

Tabla H.20: Equipos del departamento de gestión ambiental y servicios públicos

Fuente: Elaborado por el autor

## ARCHIVO FINANCIERO

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Director de archivo financiero	Luis Rodríguez	10.10.0.88	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
2	Analista de archivo financiero	Marco Lara	10.10.0.86	Microsoft Windows XP Professional - Service Pack 3 GenuineIntel- 2394MHz/1GB- RAM

Tabla H.21: Equipos del departamento de archivo financiero

Fuente: Elaborado por el autor

## CONCEJALES

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Concejal	Rodrigo Guillermo	10.10.0.173	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/16,00GB -RAM
2	Concejal	Jiménez Marco	10.10.0.189	Microsoft Windows 7 Professional - Intel(R) Core™ i7 – 4600M CPU 2.90GHz/ 4,00 GB - RAM
3	Concejal	Alfonso Quispe	10.10.0.155	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
4	Concejal	Mariana Espinoza	10.10.0.153	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/16,00GB -RAM
5	Concejal	Gladys Mesías	10.10.0.150	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 2600 CPU 3.40GHz/ 4,00 GB - RAM
6	Vicealcalde	Manuel Jerez	10.10.0.149	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
7	Secretaria de consejo	Ana Santa Fe	10.10.0.151	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 4790 CPU 3.60GHz/ 4,00 GB - RAM

Tabla H.22: Equipos del departamento de los concejales

Fuente: Elaborado por el autor

## FISCALIZACIÓN

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Jefe de fiscalización	Mónica Velastegui	10.10.0.132	Microsoft Windows 10 Pro - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
2	Jefe de fiscalización	Mónica Velastegui	10.10.0.134	Microsoft Windows 8.1 Pro 9600 - Intel(R) Core™ i7 - 6500 CPU 2.50GHz/ 8,00 GB - RAM
3	Secretario de fiscalización	Vinicio Balarezo	10.10.0.135	Microsoft Windows 7 Professional - Intel(R) Core™ i3 - 550 CPU 3.20GHz/ 2,00 GB - RAM
4	Analista de fiscalización	Karina Vega	10.10.0.136	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
5	Analista de fiscalización	Lisette Siza	10.10.0.131	Microsoft Windows XP Professional - Service Pack 3 GenuineIntel- 2926MHz/4GB- RAM

Tabla H.23: Equipos del departamento de fiscalización

Fuente: Elaborado por el autor

## BOEGA

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Guarda almacén	William Velastegui	10.10.0.40	Microsoft Windows 10 Pro - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
2	Asistente de desarrollo organizacional	Karina Velastegui	10.10.0.39	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i5 - 4440 CPU 3.10GHz/ 4,00 GB - RAM

Tabla H.24: Equipos del departamento de bodega

Fuente: Elaborado por el autor

## DIRECCIÓN DE SEGURIDAD CIUDADANA

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Director de seguridad ciudadana	Santiago Vásquez	-	Laptop personal
2	Secretaria de seguridad ciudadana	Esther León	10.10.0.48	Microsoft Windows 8.1 Pro 9600 - Intel(R) Core™ i7 - 6500 CPU 2.50GHz/ 8,00 GB - RAM
3	Comisaria de higiene y salubridad	Santiago Vásquez	10.10.0.135	Microsoft Windows 7 Professional - Intel(R) Core™ i3 - 550 CPU 3.20GHz/ 2,00 GB - RAM
4	Construcciones	Bayrón Jiménez	10.10.0.54	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
5	Gestión de riesgos	Yajaira Mera	10.10.0.141	Microsoft Windows XP Professional - Service Pack 3 GenuineIntel- 2926MHz/4GB- RAM

Tabla H.25: Equipos del departamento de seguridad ciudadana

Fuente: Elaborado por el autor

### H.3. CASA YEROVY MACKUART

#### CULTURA Y PATRIMONIO

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Director de cultura y patrimonio / desarrollo humano	Francisco Paredes	10.10.10.202	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
2	Técnico en cultura y patrimonio	Carmen Villacrés	10.10.10.206	Microsoft Windows 7 Ultimate Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
3	Secretario de cultura y patrimonio	Guillermo Cáceres	10.10.10.204	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i3 - 550 CPU 3.20GHz/ 2,00 GB - RAM
4	Uso común	Uso general del personal	10.10.10.216	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i3 - 550 CPU 3.20GHz/ 2,00 GB - RAM

Tabla H.26: Equipos del departamento de cultura y patrimonio

Fuente: Elaborado por el autor

## DESARROLLO HUMANO

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Especialista en desarrollo humano	Marcelo Cordova	10.10.10.215	Microsoft Windows 7 Professional 7600 - Intel(R) Core™ 2 Duo CPU E4600/ 2.40GHz/ 1,00 GB - RAM
2	Secretario de cultura y patrimonio	Wilson Gualpa	10.10.10.230	Microsoft Windows 7 Starter Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM

Tabla H.27: Equipos del departamento de desarrollo humano

Fuente: Elaborado por el autor

## TURISMO

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Miembro de la junta cantonal	Mónica Pallango	10.10.10.201	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/ 4,00 GB - RAM
2	Miembro de la junta cantonal	Ligia Mogro	10.10.10.200	Microsoft Windows 7 Home Premium 7600 - Intel(R) Core™ i7 2600/ 3.40GHz/ 4,00 GB - RAM
3	Miembro de la junta cantonal	Susana Albán	10.10.10.203	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i3 - 550 CPU 3.20GHz/ 2,00 GB - RAM
4	Turismo	Inés Carrillo	10.10.10.208	Microsoft Windows 7 Starter Service Pack 1 - Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM

Tabla H.28: Equipos del departamento de turismo

Fuente: Elaborado por el autor

#### H.4. TERMINAL TERRESTRE DE SALCEDO

##### TERMINAL

N	CARGO	FUNCIONARIO	RANGOS	DESCRIPCIÓN DEL EQUIPO
1	Tasa Usuario	Moraima Vega Lascano Viviana Clara Caizachana	192.168.10.16	Microsoft Windows 10 Pro - Intel(R) Core™ i5 – 3470S CPU 2.90GHz/ 4,00 GB - RAM
2	Tasa de frecuencia	Oscar Alvear Anival Almeida Luis Minta	192.168.10.15	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i3 - 3240 CPU 3.40GHz/2,00 GB-RAM
3	Director Registro de la propiedad	Guillermo Pérez	10.10.12.150	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i3 - 2100 CPU 3.10GHz/4,00 GB-RAM
4	Secretaria de administración	Ana Tello	10.10.12.152	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i5 - 7400 CPU 3.00GHz/8,00 GB-RAM
5	Asistente Registral	Oswaldo Rodas	10.10.12.158	Microsoft Windows 7 Professional 7600 - Intel(R) Core™ i3 - 2100CPU 3.10GHz / 2,00 GB - RAM
6	Asistente Registral	Carlos Torres	10.10.12.154	Microsoft Windows 7 Professional 7600 - Intel(R) Core™ i3 - 2100CPU 3.10GHz / 2,00 GB - RAM
7	Asistente Mercantil	Viviana Toro	10.10.12.155	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i5 - 7400 CPU 3.00GHz/4,00 GB-RAM
8	Operador Mercantil	Luis Tutasig	10.10.12.156	Microsoft Windows 7 Professional - Intel(R) Core™ i7 - 37700 CPU 3.40GHz/4,00 GB-RAM
9	Servidor	Servidor	10.10.12.141	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i7 - 3770 CPU 3.40GHz/4,00 GB-RAM
10	Secretaria de procuraduría	Lucía Jiménez	10.10.12.148	Microsoft Windows 7 Professional - Intel(R) Core™ i7 - 37700 CPU 3.40GHz/4,00 GB-RAM
11	Servidor público 5	Francisco Teneda	10.10.12.162	COMPUTADOR PERSONAL
12	Recaudador del registro de la propiedad	Sara Pacheco	10.10.12.149	Microsoft Windows 7 Professional Service Pack 1 - Intel(R) Core™ i3 - 2120 CPU 3.30GHz/4,00 GB-RAM

Tabla H.29: Equipos del departamento del terminal

Fuente: Elaborado por el autor

## Anexo I

### Autorización para la valoración de activos y asignación de riesgos



Universidad Técnica de Ambato  
Facultad de Ingeniería en Sistemas, Electrónica e Industrial

**Nota:** La información compartida, es de uso académico para el caso de estudio de acuerdo con la norma desarrollada por ISO (organización internacional de Normalización) con el propósito de ayudar a gestionar la Seguridad de la Información en el G.A.D. Municipal del cantón Salcedo, autorizado por la autoridad mayor (ALCALDÍA MUNICIPAL), MSc. Willan Naranjo Torres.

#### VALORACIÓN DE ACTIVOS Y ASIGNACIÓN DE RIESGOS

Con este esquema podremos evaluar el riesgo en función de los niveles de confidencialidad, integridad y disponibilidad. Por favor lea detenidamente antes de evaluar los activos.

VALORACIÓN DE LOS ACTIVOS				
Valor	Denominación	Disponibilidad	Integridad	Confidencialidad
		Asegurando que los usuarios autorizados tienen acceso a la información y los activos asociados cuando se requiera	La cualidad de la información para no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones.	Asegurar que la información sea accesible solo para aquellos autorizados para tener acceso
3	Alto	Se podría esperar que la interrupción del acceso o uso del sistema de información tenga un efecto adverso severo o catastrófico en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la modificación o destrucción no autorizada de información tenga un efecto adverso severo o catastrófico en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la divulgación no autorizada de información tenga un efecto adverso severo o catastrófico en las operaciones de la organización, los activos de la organización o las personas.
2	Medio	Se podría esperar que la interrupción del acceso o uso del sistema de información tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la modificación o destrucción no autorizada de información tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la divulgación no autorizada de información tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.
1	Bajo	Se podría esperar que la interrupción del acceso o uso de la información o un sistema de información tenga un efecto adverso limitado o bajo en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la modificación o destrucción no autorizada de la información tenga un efecto adverso limitado en las operaciones de la organización, los activos de la organización o las personas.	Se podría esperar que la divulgación no autorizada de información tenga un efecto adverso limitado en las operaciones de la organización, los activos de la organización o las personas.

<https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf>

Figura I.1: Autorización para la valoración de los activos (página 1)

Fuente: Elaborado por el autor



**IMPORTANTE:** Colocar el valor correspondiente a su criterio personal en base a su experiencia en el puesto de trabajo, en el cual desempeña dentro del departamento de “Tecnologías de la Información”.

En base a la tabla de valoración de los activos, colocar el numero correspondiente:

(3 Alto, 2 Medio, 1 Bajo)

CANTIDAD	EQUIPO	DESCRIPCIÓN	Disponibilidad	Integridad	Confidencialidad
1	Servidor 1	Servidor ZIMBRA			
1	Servidor 2	Servidor SAMBA			
1	Servidor 3	Servidor de Internet			
1	Servidor 4	Servidor de Antivirus			
1	Servidor 5	Servidor de Facturación Electrónica			
1	Servidor 6	Servidor Intranet			
1	Servidor 7	Servidor AME			
2	Switch	24 PUERTOS QP-AVP24S QPCOM			
2	Switch	24 PUERTOS GIGA QPCOM QP-G240R			
1	Regletas para Bastidor para Rack	Nexxt Solutions para Rack AW220NXT95			
1	Tripp Lite Rack Console 1URM	KVM Switch, 19" LCD 1080p Rackmount TAA			
1	Cisco Router	4 Ports - Management Port / Slots Gigabit Ethernet			
1	Central Telefónica con voz sobre IP	Teléfonos Grandstream BT200			
5	UPS Departamento de TI	UPS			

CANTIDAD	EQUIPO	DESCRIPCIÓN	Disponibilidad	Integridad	Confidencialidad
2	Computadoras de escritorio completas	Intel(R) Core™ i7-870 CPU 2.93GHz & Intel(R) Core™ i7-8550 CPU 1.80GHz			
2	Laptops personales	Laptops personales			
3	Impresoras	2 HP & 1EPSON			
1	Aire acondicionado	Cuarto de Telecomunicaciones			
-	Infraestructura de red	Conexiones de red			
-	Red WIRELESS	WIFI			
-	Red LOCAL	LAN			

Figura I.2: Autorización para la valoración de los activos (página 2)

Fuente: Elaborado por el autor



**Universidad Técnica de Ambato**  
**Facultad de Ingeniería en Sistemas, Electrónica e Industrial**

**Nota:** La información compartida, es de uso académico para el caso de estudio de acuerdo con la norma desarrollada por ISO (organización internacional de Normalización) con el propósito de ayudar a gestionar la Seguridad de la Información en el G.A.D. Municipal del cantón Salcedo, autorizado por la autoridad mayor (ALCALDÍA MUNICIPAL), **MSc. Willan Naranjo Torres.**

**ANÁLISIS DE EVALUACIÓN**

Un método de evaluación (Annualized Loss Expectancy o ALE por sus siglas en inglés), mencionado en el libro (INFORMATION SECURITY), por Cesare Gallotti, enero 2019, en conjunto con la ISO/IEC 27001 STANDARD, permite modelar el impacto que los riesgos de seguridad pueden tener sobre los activos de una organización.

**(PASO 1)**

Definición del alcance y los activos involucrados en la operación del proceso.

**NOTA:** En el espacio en blanco por favor colocar un valor estimado del equipo.

Nº	CARGO	FUNCIONARIO	RANGOS	COSTO ESTIMADO DEL EQUIPO	DESCRIPCIÓN DEL EQUIPO
1	Jefe del departamento de TI	Ing. Enrique Arcos	10.10.1.8		LAPTOP PERSONAL
2	Analista de sistemas	Ing. Paulina Villalba	10.10.0.9		Microsoft Windows 7 Professional Service Pack 1 Intel(R) Core™ i7 - 870 CPU 2.93GHz/ 4,00 GB - RAM
3	Técnico de sistemas	Tec. Juan Córdoba	10.10.1.9		Microsoft Windows 10 Pro Intel(R) Core™ i7 - 8550 CPU 1.80GHz / 16,00 GB - RAM
4					

Nº SERVIDOR	TIPO (RACK/TORRE)	SISTEMA OPERATIVO	MARCA	MODELO	VALOR ESTIMADO EN EL MERCADO	VALOR ESTIMADO POR LOS ENCARGADOS
Servidor 1	RACK	Linux Centos	HP	Proliant DL360 G10	\$ 1.640,00	
Servidor 2	RACK	Linux Centos	HP	Proliant DL320 G8	\$ 1.409,00	
Servidor 3	RACK	Linux Centos	HP	Proliant DL380 G7	\$ 880,00	
Servidor 4	RACK	Linux Centos	HP	Proliant DL120 G7	\$ 830,00	
Servidor 5	TORRE	Linux Centos	HP	Proliant ML150 G5	\$ 700,00	
Servidor 6	TORRE	Linux Centos	HP	Proliant ML150 G6	\$ 750,00	
Servidor 7	TORRE	Windows Server 2012	HP	Proliant ML150 G6	\$ 750,00	

Information security: The ISO/IEC 27001. Escrito por Cesare Gallotti

Figura I.3: Autorización para la valoración de los activos (página 3)  
Fuente: Elaborado por el autor





Nº	DESCRIPCIÓN DEL EQUIPO	TIPO DE TONER	COSTO ESTIMADO EN EL MERCADO	VALOR ESTIMADO POR LOS ENCARGADOS
1	HP LASER JET P2015DN	53A HP LASERJET	\$ 80,00	
2	EPSON L355	54a HP LASERJET	\$ 150,00	
3	HP COLOR LASERJET CP6015DN	HP COLOR LASERJET CB380A	\$ 450,00	

Nº	EQUIPO	DESCRIPCIÓN	COSTO ESTIMADO EN EL MERCADO	VALOR ESTIMADO POR LOS ENCARGADOS
1	Switch	24 PUERTOS QP-AVP24S QPCOM	\$ 645,00	
2	Switch	24 PUERTOS GIGA QPCOM QP-G240R	\$ 549,00	
3	Cisco Router	4 Ports - Management Port / Slots Gigabit Ethernet	\$ 650,00	
3	Tripp Lite Rack Console 1URM	KVM Switch, 19" LCD 1080p Rackmount TAA	\$ 790,00	

(PASO 2) Identificación de amenazas y probabilidad de ocurrencia.

De la misma manera que en el análisis de riesgos, se definen escenarios de amenaza posibles para los activos.

**ARO: TASA DE OCURRENCIA ANUALIZADA.**

Es la probabilidad de ocurrencia que puede tener una amenaza sobre un determinado activo.

**Importante:** Para la asignación de los valores es necesario colocar el valor en (%) por ejemplo: Si usted considera que una erupción volcánica puede ocurrir con una frecuencia del (10%), estaría dentro del rango remoto como referencia. Los valores de la tabla son una guía de frecuencia, usted es libre de colocar un valor estimado del (0% al 100%)

NIVEL	FRECUENCIA	PROBABILIDAD	DESCRIPCIÓN
4	76-100%	Muy Frecuente	Eventos repetitivos
3	51-75%	Frecuente	Eventos aislados
2	26-50%	Ocasional	Sucede alguna vez
1	0-25%	Remoto	Imposible que suceda

0-25%

76-100%



**FE: FACTOR DE EXPOSICIÓN (IMPACTO).**

El factor de exposición es el porcentaje de pérdida potencial, el impacto que tendrá para un activo, si una amenaza específica se materializa.

**Importante:** Para la asignación de los valores es necesario colocar el valor en (%) por ejemplo:

Si usted considera que los sismos (volcánicos o repentinos) tienen un valor de impacto del (60%), se encontraría dentro del rango alto como referencia. Los valores de la tabla son una guía del impacto que tendrá para un activo, usted es libre de colocar un valor estimado del (0% al 100%).

→ *Valores Empresa*

NIVEL	IMPACTO	VALOR	DESCRIPCIÓN
1	Bajo	0-25%	Cuando no afectan las actividades y los sistemas principales trabajan de forma normal.
2	Medio	26-50%	Cuando los daños son parciales y se dan en los sistemas, no afecta a las operaciones.
3	Alto	51-75%	Cuando se ven afectadas de manera directa las operaciones y funciones, los usuarios y los sistemas informáticos.
4	Critico	76-100%	Pérdida de información crítica, daños severos en los equipos, suspensión de funciones.

**EVALUACIÓN DE LOS ACTIVOS ACORDE A LA PROBABILIDAD E IMPACTO**

**SERVIDOR 1: (Servidor ZIMBRA) Proliant DL360 G10**

Nº SERVIDOR	Nº RIESGO	IDENTIFICACIÓN	VALORACIÓN	
		AMENAZA	PROBABILIDAD %	IMPACTO %
Servidor 1	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R7	Daño en el ventilador		
	R8	Daño en fuente de poder		
	R9	Falla de disco duro SATA/IDE		
	R10	Falla de Tarjeta de Red		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		

Figura I.5: Autorización para la valoración de los activos (página 5)

Fuente: Elaborado por el autor



**SERVIDOR 2:** (Servidor SAMBA) Proliant DL320 G8

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
Servidor 2	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R7	Daño en el ventilador		
	R8	Daño en fuente de poder		
	R9	Falla de disco duro SATA/IDE		
	R10	Falla de Tarjeta de Red		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		

**SERVIDOR 3:** (Servidor de Internet) Proliant DL380 G7

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
Servidor 3	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R7	Daño en el ventilador		
	R8	Daño en fuente de poder		
	R9	Falla de disco duro SATA/IDE		
	R10	Falla de Tarjeta de Red		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		

Figura I.6: Autorización para la valoración de los activos (página 6)  
Fuente: Elaborado por el autor



**SERVIDOR 4:** (Servidor de Antivirus) Proliant DL120 G7

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
Servidor 4	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R7	Daño en el ventilador		
	R8	Daño en fuente de poder		
	R9	Falla de disco duro SATA/IDE		
	R10	Falla de Tarjeta de Red		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		

**SERVIDOR 5:** (Servidor de Facturación Electrónica) Proliant ML150 G5

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
Servidor 5	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R7	Daño en el ventilador		
	R8	Daño en fuente de poder		
	R9	Falla de disco duro SATA/IDE		
	R10	Falla de Tarjeta de Red		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		



**SERVIDOR 6: (Servidor Intranet) Proliant ML150 G6**

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
Servidor 6	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R7	Daño en el ventilador		
	R8	Daño en fuente de poder		
	R9	Falla de disco duro SATA/IDE		
	R10	Falla de Tarjeta de Red		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		

**SERVIDOR 7: (Servidor AME) Proliant ML150 G6**

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
Servidor 7	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R7	Daño en el ventilador		
	R8	Daño en fuente de poder		
	R9	Falla de disco duro SATA/IDE		
	R10	Falla de Tarjeta de Red		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		

Figura I.8: Autorización para la valoración de los activos (página 8)  
Fuente: Elaborado por el autor



**PCs del departamento de Tecnologías de la Información**

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
PCs del departamento de Tecnologías de la Información	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R7	Daño en el ventilador		
	R8	Daño en fuente de poder		
	R9	Falla de disco duro SATA/IDE		
	R10	Falla de Tarjeta de Red		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		

**Impresoras del departamento de Tecnologías de la Información**

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
Impresoras del departamento de Tecnologías de la Información	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		
	R18	Atasco de papel en la impresora		
	R19	El dispositivo no reconoce la impresora.		

Figura I.9: Autorización para la valoración de los activos (página 9)  
Fuente: Elaborado por el autor



**Tripp Lite Rack Console 1URM (KVM Switch, 19" LCD 1080p Rackmount TAA)**

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
Tripp Lite Rack Console 1URM	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R7	Daño en el ventilador		
	R8	Daño en fuente de poder		
	R9	Falla de disco duro SATA/IDE		
	R10	Falla de Tarjeta de Red		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		

**Cisco Router**

Nº SERVIDOR	IDENTIFICACIÓN		VALOR "ARO"	VALOR "FE"
	Nº RIESGO	AMENAZA	PROBABILIDAD %	IMPACTO %
Cisco Router	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		

Figura I.10: Autorización para la valoración de los activos (página 10)

Fuente: Elaborado por el autor



### Red de datos

Nº SERVIDOR	Nº RIESGO	IDENTIFICACIÓN	VALOR "ARO"	VALOR "FE"
		AMENAZA	PROBABILIDAD %	IMPACTO %
Red de datos	R1	Flujo de lodos y escombros (lahares)		
	R2	Lluvia de ceniza y piroclastos (polvo)		
	R3	Sismos (volcánicos/repentinos)		
	R4	Interrupción del servicio de energía eléctrica		
	R5	Filtración de agua		
	R6	Incendio		
	R11	Fallas de Software/Configuración		
	R12	Falla de cableado y conectores		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R17	Robo de dispositivos		
R20	Presencia de interferencias electromagnéticas			

### Información

Nº SERVIDOR	Nº RIESGO	IDENTIFICACIÓN	VALOR "ARO"	VALOR "FE"
		AMENAZA	PROBABILIDAD %	IMPACTO %
Información	R11	Fallas de Software/Configuración		
	R13	Acceso no autorizado (Robo o alteración de información)		
	R14	Ataques DoS o denegación de servicio		
	R15	Software malicioso		
	R16	Error Humano (Falta de conocimiento)		
	R21	Ingeniería social		

#### IMPORTANTE:

La presente evaluación se lleva a cabo en el G.A.D. Municipal del cantón Salcedo, tiene por objetivo mejorar la calidad de gestionar la Seguridad de la Información, misma que permitirá obtener un criterio sobre cuáles son los principales activos de información, vulnerabilidades, amenazas a los cuales se encuentran expuestos y determinar si poseen medidas de seguridad para protegerlos. La información compartida, es de uso académico para el caso de estudio de acuerdo con la norma desarrollada por ISO (organización internacional de Normalización).

Gracias a la colaboración y administración del **MSc. Willan Naranjo Torres** y quienes forman parte del equipo de trabajo del departamento de Tecnologías de la Información se lleva a cabo la elaboración de un Plan de contingencia informático, y mejorar la gestión con resultados y transparencia, como el motor de progreso y transformación para el cantón Salcedo.

GRACIAS POR SU COLABORACIÓN



Figura I.11: Autorización para la valoración de los activos (página 11)

Fuente: Elaborado por el autor



## FRAGMENTOS DE LA VALORACIÓN DE ACTIVOS COMO RESPALDO DE LA EVALUACIÓN REALIZADA AL PERSONAL ENCARGADO DEL DEPARTAMENTO DE TI

Fragmento de la evaluación, firma del Jefe del departamento de TI

### IMPORTANTE:

La presente evaluación se lleva a cabo en el G.A.D. Municipal del cantón Salcedo, tiene por objetivo mejorar la calidad de gestionar la Seguridad de la Información, misma que permitirá obtener un criterio sobre cuáles son los principales activos de información, vulnerabilidades, amenazas a los cuales se encuentran expuestos y determinar si poseen medidas de seguridad para protegerlos. La información compartida, es de uso académico para el caso de estudio de acuerdo con la norma desarrollada por ISO (organización internacional de Normalización).

Gracias a la colaboración y administración del MSc. Willan Naranjo Torres y quienes forman parte del equipo de trabajo del departamento de Tecnologías de la Información se lleva a cabo la elaboración de un Plan de contingencia informático, y mejorar la gestión con resultados y transparencia, como el motor de progreso y transformación para el cantón Salcedo.

GRACIAS POR SU COLABORACIÓN



11

Figura I.12: Respaldo de la valoración, firma del Jefe del departamento de TI

Fuente: Elaborado por el autor

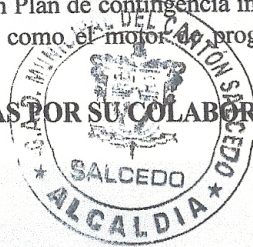
## Fragmento de la evaluación, firma del Analista de Sistemas

### IMPORTANTE:

La presente evaluación se lleva a cabo en el G.A.D. Municipal del cantón Salcedo, tiene por objetivo mejorar la calidad de gestionar la Seguridad de la Información, misma que permitirá obtener un criterio sobre cuáles son los principales activos de información, vulnerabilidades, amenazas a los cuales se encuentran expuestos y determinar si poseen medidas de seguridad para protegerlos. La información compartida, es de uso académico para el caso de estudio de acuerdo con la norma desarrollada por ISO (organización internacional de Normalización).

Gracias a la colaboración y administración del MSc. Willan Naranjo Torres y quienes forman parte del equipo de trabajo del departamento de Tecnologías de la Información se lleva a cabo la elaboración de un Plan de contingencia informático, y mejorar la gestión con resultados y transparencia, como el motor de progreso y transformación para el cantón Salcedo.

GRACIAS POR SU COLABORACIÓN



11

Figura I.13: Respaldo de la valoración, firma del Analista de Sistemas  
Fuente: Elaborado por el autor

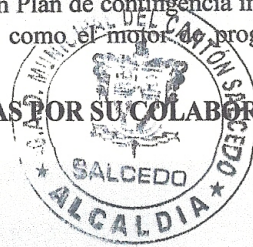
## Fragmento de la evaluación, firma del Técnico de Sistemas

### IMPORTANTE:

La presente evaluación se lleva a cabo en el G.A.D. Municipal del cantón Salcedo, tiene por objetivo mejorar la calidad de gestionar la Seguridad de la Información, misma que permitirá obtener un criterio sobre cuáles son los principales activos de información, vulnerabilidades, amenazas a los cuales se encuentran expuestos y determinar si poseen medidas de seguridad para protegerlos. La información compartida, es de uso académico para el caso de estudio de acuerdo con la norma desarrollada por ISO (organización internacional de Normalización).

Gracias a la colaboración y administración del MSc. Willan Naranjo Torres y quienes forman parte del equipo de trabajo del departamento de Tecnologías de la Información se lleva a cabo la elaboración de un Plan de contingencia informático, y mejorar la gestión con resultados y transparencia, como el motor de progreso y transformación para el cantón Salcedo.

GRACIAS POR SU COLABORACIÓN



11

Figura I.14: Respaldo de la valoración, firma del Técnico de Sistemas