UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA ELECTRÓNICA Y REDES DE COMUNICACIÓN

“PLAN DE CONTINGENCIA PARA LA UNIDAD DE SISTEMAS Y TECNOLOGÍA DE INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO ANTONIO ANTE EN BASE A LA NORMA ISO/IEC 27002.”

PROYECTO PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

KARINA ALEXANDRA MÉNDEZ LUNA

DIRECTOR: ING. DAVID NARVÁEZ

Ibarra, Enero 2015

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1003175831		
APELLIDOS Y NOMBRES:	Méndez Luna Karina Alexandra		
DIRECCIÓN:	Luis Felipe Borja y Simón Rodríguez 1-54		
EMAIL:	Kary_3040@yahoo.es		
TELÉFONO FIJO:	062-631226	**TELÉFONO MÓVIL:**	0982872820

DATOS DE LA OBRA	
TÍTULO:	PLAN DE CONTINGENCIA PARA LA UNIDAD DE SISTEMAS Y TECNOLOGÍA DE INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO ANTONIO ANTE EN BASE A LA NORMA ISO/IEC 27002.
AUTORA:	Méndez Luna Karina Alexandra
FECHA:	20 de Abril 2015
PROGRAMA:	PREGRADO
TITULO POR EL QUE OPTA:	Ingeniera en Electrónica y Redes de Comunicación
DIRECTOR:	Ing. David Narváez

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Karina Alexandra Méndez Luna con cédula de identidad Nro. 1003175831, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrollo sin violar derechos de autores de terceros, por lo tanto la obra es original, y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 9 días del mes de mayo del 2015

Firma.....

Nombre: Karina Alexandra Méndez Luna

Cédula: 1003175831

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, **Karina Alexandra Méndez Luna**, con cédula de identidad Nro. 1003175831, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor (es) de la obra o trabajo de grado denominado: **PLAN DE CONTINGENCIA PARA LA UNIDAD DE SISTEMAS Y TECNOLOGÍA DE INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO ANTONIO ANTE EN BASE A LA NORMA ISO/IEC 27002**, que ha sido desarrollado para optar por el título de: **Ingeniera en Electrónica y Redes de Comunicación**, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, a los 9 días del mes de mayo del 2015

Firma .....

Nombre: Karina Alexandra Méndez Luna

Cédula: 1003175831

DECLARACIÓN

Yo, **Karina Alexandra Méndez Luna,** declaro bajo juramento que el trabajo aquí escrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte - Ibarra, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

.....

Firma:

CI: 1003175831

CERTIFICACIÓN

En calidad de tutor del trabajo de grado titulado: "PLAN DE CONTINGENCIA PARA LA UNIDAD DE SISTEMAS Y TECNOLOGÍA DE INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO ANTONIO ANTE EN BASE A LA NORMA ISO/IEC 27002.", certifico que el presente trabajo fue desarrollado por la señorita **Karina Alexandra Méndez Luna**, bajo mi supervisión.

Ing. David Narváez
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Mi más ferviente agradecimiento a mis Padres Rodrigo y Graciela, por haber estado junto a mí cada momento de mi vida brindándome su cariño infinito que me ha dado la fortaleza necesaria para la culminación de este trabajo.

A mi director de tesis el Ing. David Narváez, por sus valiosos consejos, su paciencia y apoyo hacia mi persona, por permitirme robar parte de su tiempo para realizar este proyecto.

De igual modo a la Universidad Técnica del Norte, institución prestigiosa que nos permitió formarnos. A todas aquellas personas que de una u otra manera han hecho posible terminar este proyecto de grado.

Al Gobierno Autónomo Descentralizado de Antonio Ante por permitirme realizar este proyecto de titulación, especialmente al Ing., Francisco Arteaga por brindarme su ayuda en el desarrollo del mismo.

A todos ellos muchas gracias.

Karina

DEDICATORIA

Con mucho cariño y amor a mis padres y hermanos, porque ellos son mi pilar fundamental y una bendición en mi vida, por su comprensión y apoyo incondicional a lo largo de mi vida para alcanzar esta meta.

A mis compañeros por llenar de momentos agradables mi vida, a los docentes de profesión y corazón para que mantengan encendida la llama de voluntad y amor por enseñar.

"Vive como si fueras a morir mañana
Y aprende como si fueras a vivir para siempre"

Karina

CONTENIDO

DECLARACIÓN i
CERTIFICACIÓN ii
AGRADECIMIENTOS iii
DEDICATORIA iv
CONTENIDO v
ÍNDICE DE FIGURAS x
ÍNDICE DE DIAGRAMAS xi
ÍNDICE DE TABLAS xii
RESUMEN xiii
ABSTRACT xiv
PRESENTACIÓN xv
1 CAPÍTULO I 1
1.1 DESCRIPCIÓN DEL PROBLEMA 1
1.2 OBJETIVOS 2
1.2.1 OBJETIVO GENERAL 2
1.2.2 OBJETIVO ESPECÍFICOS 2
1.3 ALCANCE 3
1.4 JUSTIFICACIÓN 5
2 CAPÍTULO II 7
2.1 ANÁLISIS DE LA NORMA TÉCNICA ECUATORIANA NTE UNEN-ISO/IEC 27002 7
2.1.1 ALCANCE 8
2.1.2 ESTRUCTURA DEL ESTÁNDAR 8
2.1.3 EVALUACIÓN Y TRATAMIENTO DEL RIESGO 9
2.1.4 POLÍTICAS DE SEGURIDAD 9
2.1.5 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 10
2.1.6 GESTIÓN DE ACTIVOS 11
2.1.7 SEGURIDAD DE LOS RECURSOS HUMANOS 11
2.1.8 SEGURIDAD FÍSICA Y DEL ENTORNO 11
2.1.9 GESTIÓN DE COMUNICACIONES Y OPERACIONES. 12
2.1.10 CONTROLES DE ACCESO 14

2.1.11 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 14
2.1.12 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN 15
2.1.13 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 15
2.1.14 CUMPLIMIENTO 16
2.2 MARCO LEGAL 16
2.2.1 ANÁLISIS DEL ARTÍCULO 410-11 DE LA LEY DE CONTROL INTERNO DEL ECUADOR 17
2.3 QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN 18
2.4 SISTEMAS DE INFORMACIÓN 20
2.5 QUÉ ES UN PLAN DE CONTINGENCIA 21
2.6 OBJETIVOS DEL PLAN DE CONTINGENCIA 22
2.7 IMPORTANCIA DEL PLAN DE CONTINGENCIA 23
2.8 TIPOS DE CONTINGENCIAS 23
2.9 CARACTERÍSTICAS DE UN PLAN DE CONTINGENCIA 24
2.10 PLAN DE RESPALDO 25
2.11 PLAN DE EMERGENCIA 25
2.12 PLAN DE RECUPERACIÓN 25
2.13 FASES DE UN PLAN DE CONTINGENCIA PARA EL SISTEMA DE INFORMACIÓN. 26
2.13.1 PLANIFICACIÓN 26
2.13.2 IDENTIFICACIÓN DE ESCENARIOS DE CONTINGENCIA INFORMÁTICOS 26
2.13.2.1 Identificación de Amenazas 27
2.13.2.2 Definición de eventos Controlables y No Controlables 33
2.13.3 EVALUACIÓN DE RIESGOS INFORMÁTICOS 34
2.13.3.1 Identificación de vulnerabilidades tecnológicas 35
2.13.3.2 Valoración de Activos 37
2.13.3.3 Análisis de Riesgo 39
a) Probabilidad de Riesgo. 39
b) Evaluación de Probabilidad de Riesgo 39
c) Impacto del Riesgo 40
d) Determinación del Riesgo 41
2.13.3.4 Tipos de análisis Riesgos 42

2.13.4 IDENTIFICACIÓN DE CONTROLES PREVENTIVOS 43
2.13.4.1 Estrategias de protección tecnológica 44
2.13.5 DOCUMENTACIÓN DEL PROCESO 45
2.13.6 REALIZACIÓN DE PRUEBAS Y VALIDACIÓN DE LOS PLANES DE CONTINGENCIA 46
2.13.6.1 Evaluación de resultados y pruebas 47
2.13.6.2 Métodos para las pruebas de los Planes de Contingencia. 47
2.13.6.3 Retroalimentación del plan de acción 48
3 CAPÍTULO III 49
3.1 PLANIFICACIÓN 49
3.1.1 ALCANCE 50
3.2 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL 50
3.2.1 DEPARTAMENTOS DEL MUNICIPIO DE ANTONIO ANTE 51
a) Dirección Administrativa Financiera 52
b) Contabilidad 53
c) Tesorería y Rentas 53
d) Sistemas y Tecnología 53
e) Turismo Cultura Seguridad y Deportes 54
f) Dirección de Planificación Territorial 54
g) Avalúos y Catastros 54
h) Planificación y Urbanismo 55
i) Dirección de Servicios Municipales 55
j) Recursos Humanos 55
3.2.2 SERVICIOS PRESTADOS POR EL GAD DE ANTONIO ANTE 56
3.2.3 SERVICIOS CONSUMIDOS POR EL GAD DE ANTONIO ANTE 56
3.2.4 ACTIVOS DE INFORMACIÓN 57
3.2.5 RED DE DATOS 58
3.2.6 CUARTO DE TELECOMUNICACIONES 60
3.2.6.1 Descripción de los equipos de Red 61
3.2.7 ACTIVOS SOFTWARE 66
3.2.8 ACTIVOS HARDWARE 66
3.2.9 SERVICIOS DEL DEPARTAMENTO INFORMÁTICO 71
3.2.10 PERSONAL 71
3.3 EVALUACIÓN DE RIESGOS Y ESCENARIOS DE CONTINGENCIA ... 72

3.3.1 EVALUACIÓN DE LOS ACTIVOS EN EL GAD DE ANTONIO ANTE 73
3.3.2 EVALUACIÓN DE LAS AMENAZAS 75
3.3.3 MATRIZ DE CONTINGENCIA 78
3.4 IDENTIFICACIÓN DE CONTROLES PREVENTIVOS 80
3.4.1 Propuesta del Orgánico Estructural para el Departamento de Sistemas y Tecnología del GAD de Antonio Ante. 80
a) Dirección TICS 81
b) Análisis Desarrollo y Aplicaciones 82
c) Administrador de Sistemas 82
d) Administrador Redes 83
3.4.2 FORMACIÓN DE GRUPOS Y ASIGNACIÓN DE ROLES EN CASO DE UNA CONTINGENCIA 83
3.4.3 PRIORIZACIÓN DE RECURSOS TECNOLÓGICOS 85
3.4.4 ESTRATEGIAS DE PROTECCIÓN TECNOLÓGICAS 88
3.4.4.1 Manejo de la información 88
3.4.4.2 Obtención de copias de seguridad de la información 89
3.4.4.3 Seguridad en redes 89
3.4.4.4 Seguridad física 91
3.4.4.5 Códigos maliciosos 92
3.4.4.6 Fallas en hardware o software 93
3.4.4.7 Sabotaje o daños accidentales 93
3.4.5 TIEMPO DE RECUPERACIÓN E IMPACTO GENERADO SI FALLAN LOS ACTIVOS CRÍTICOS 94
4 CAPITULO IV 96
4.1 OBJETO 98
4.2 ALCANCE 98
4.3 DEFINICIONES 99
4.4 REFERENCIAS 100
4.5 RESPONSABILIDADES 100
4.6 EJECUCIÓN 101
4.6.1 PLAN DE RECUPERACIÓN Y RESPALDO 101
4.6.1.1 ACTIVIDADES PREVIAS: 102
4.6.1.2 ACTIVIDADES DURANTE: 107

4.6.1.3 ACTIVIDADES DESPUÉS: 111
4.6.2 DOCUMENTACIÓN DEL PROCESO 115
4.6.2.1 DESASTRES NATURALES 115
4.6.3 CORTES DE ENERGÍA 120
4.6.4 FALLAS EN LA RED DE DATOS 123
4.6.5 FALLAS EN EL HARDWARE O SOFTWARE 125
4.6.6 SABOTAJE O DAÑO ACCIDENTAL 128
5 CONCLUSIONES Y RECOMENDACIONES 132
6 BIBLIOGRAFÍA 134
7 ANEXOS 137
8 GLOSARIO 152

ÍNDICE DE FIGURAS

Figura 2.1 Seguridad de la información según la norma ISO/IEC 17799 20
Figura 2.2 Proceso de un Sistema de Información 21
Figura 2.3. Proceso de evaluación del riesgo de la seguridad de la información 35
Figura 2.4 Niveles del riesgo 42
Figura 3.1. Diagrama organizacional del GAD de Antonio Ante 52
Figura 3.2 Topología física de la red inalámbrica del GAD de Antonio Ante 60

ÍNDICE DE DIAGRAMAS

Diagrama 2.1. Riesgos para la seguridad de la información 27
Diagrama 3.1 Estructura organizacional de IT 81
Diagrama 4.1 Diagrama de respuesta en caso de desastres naturales 118
Diagrama 4.2 Diagrama de respuesta a cortes de energía 121
Diagrama 4.3 Diagrama de respuesta a fallas en la red de datos..... 124
Diagrama 4.4 Diagrama de respuesta a fallas en Hardware o Software..... 127
Diagrama 4.5 Diagrama de Sabotaje o daños accidentales 130

ÍNDICE DE TABLAS

Tabla 2.1 Criterios de Evaluación de Vulnerabilidades 36
Tabla 2.2 Valoración de activos 37
Tabla 2.3 Probabilidad de Ocurrencia 40
Tabla 2.4. Prioridades de evaluación del impacto 41
Tabla 3.1 Servicios utilizados 57
Tabla 3.2 Activos de Información 58
Tabla 3.3 Redes de Comunicación de GAD de Antonio Ante 59
Tabla 3.4. Equipos activos de Red 61
Tabla 3.5. Activos Software 66
Tabla 3.6. Activos Hardware 67
Tabla 3.7. Personal de la unidad de sistemas y Tecnología del GAD de Antonio Ante 72
Tabla 3.8. Valoración de los activos del GAD de Antonio Ante 73
Tabla 3.9. Evaluación de las Amenazas a activos del GAD de Antonio Ante 75
Tabla 3.10. Evaluación de las Amenazas a activos físicos 78
Tabla 3.11 Asignación de roles y responsabilidades en caso de una contingencia 84
Tabla 3.12. Requerimientos de Seguridad 86
Tabla 3.13. Tiempos de recuperación máxima de los activos críticos del GAD de Antonio Ante 95
Tabla 7.1 Activos de mayor relevancia 138
Tabla 7.2 Requerimientos de Seguridad 140
Tabla 7.3 Vulnerabilidades 142
Tabla 7.4 Cálculo del riesgo en los activos críticos 150

RESUMEN

El presente trabajo analiza una metodología para el desarrollo de un plan de contingencia para los sistemas de información, que no es más que un conjunto de procedimientos que serán ejecutados para restablecer los procesos críticos lo antes posible con un mínimo impacto, y en el menor tiempo posible resolver el incidente cuando se presente una contingencia Un plan de contingencia define acciones generales para asegurar la adecuada recuperación de información y de los servicios, esta metodología comprende el análisis e identificación de riesgos, identificación y evaluación de amenazas y vulnerabilidades, estimaciones de impacto, la probabilidad de ocurrencia, evaluación de escenarios de contingencia, las protecciones necesarias, así como también la definición soluciones y estrategias que permitan garantizar la continuidad de las actividades en caso de materializarse dichas amenazas. Es necesario contar con un modelo de referencia adecuado para lograr evaluar de manera eficiente, tanto desde el punto técnico como económico, la solución más viable para contrarrestar los riesgos que afecten a la seguridad de la información, y que además provea la seguridad necesaria para la institución.

ABSTRACT

This research analyzes a methodology for the development of a plan of contingency for information systems, it is a set of procedures that will be executed to restore critical processes as soon as possible with minimal impact, and in the shortest possible time to resolve the incident when it appears. A contingency plan defines general actions to ensure adequate recovery of information and services, this methodology includes the analysis and identification of risks, identification and evaluation of threats and vulnerabilities, estimates of impact, probability of occurrence, evaluation of contingency scenarios, the necessary protections, as well as defining solutions and strategies to ensure the continuity of the activities if these threats are materialized. It is necessary to have a proper reference model to evaluate efficiently, both technical as economically, the most viable solution to counteract the risks affecting the security of the information, and also provide the necessary security for the institution.

PRESENTACIÓN

El Gobierno Autónomo descentralizado de Antonio Ante es una institución de carácter público que maneja información de gran importancia por lo que es necesario que los recursos de la red sean gestionados de manera eficaz.

La implementación de un plan de contingencia informático nace ante la necesidad de contar con un proceso sistemático, que sea conocido por toda la institución y que debe contener la documentación necesaria para el manejo de eventos imprevistos en caso de una emergencia.

Un plan de contingencia informático es un conjunto de actividades que nos permiten realizar acciones para minimizar los riesgos en caso de algún desastre de origen natural o humano, manteniendo la operatividad de las actividades a un mínimo nivel hasta que se pueda recuperar las totalidad de los sistemas y recursos; un plan de contingencia se encuentra conformado por tres acciones fundamentales que son: prevención, detección y recuperación.

CAPÍTULO I

ASPECTOS GENERALES

En el presente capítulo se explica la problemática de la investigación junto los objetivos a alcanzarse y la justificación de la importancia que tiene disponer de un plan de contingencia informático dentro de la institución.

1.1 DESCRIPCIÓN DEL PROBLEMA

Actualmente el Gobierno Autónomo Descentralizado de Antonio Ante es una institución de administración pública, cuya misión principal es promover el desarrollo integral de la ciudad brindando servicios eficientes oportunos y de calidad; el Departamento de Sistemas y Tecnología es el encargado de administración y gestión de la red de datos, el almacenamiento de la información, dar soporte técnico y mantener actualizada el área de tecnología, teniendo como labor principal salvaguardar su integridad, disponibilidad y operatividad que hoy en día es de vital importancia y que se debe proteger como un bien activo invaluable del municipio; entre los servicios proporcionados por este departamento dentro de la institución tenemos: elaboración de reportes, cobro de impuestos, manejo de registros de propiedad, el sistema general de administración municipal, sistema de contabilidad de la institución, emisión de permisos de funcionamiento, entre otros.

Hoy en día todas las redes de información se encuentran expuestas a múltiples riesgos que pueden causar problemas críticos en la red como por ejemplo; el factor humano, desastres naturales, fallos o robo de equipos, corrupción de las bases de datos, incendios, fallas eléctricas, son algunos de los eventos que pueden dañar la integridad física y lógica. Estas eventualidades ocasionan pérdidas de datos, que para el municipio de Antonio Ante representaría daños considerables en tiempo y dinero, disminuyendo la efectividad y dificultaría el desempeño de las actividades de los departamentos de la municipalidad que brindan servicios a la ciudadanía ocasionando malestar al no poder

realizar sus transacciones de manera oportuna, además se vería afectada la confianza de la institución; por todo estos acontecimientos es importante contar con un plan de contingencia Informático que permita el restablecimiento inmediato de los servicios en caso de algún incidente inesperado.

La falta de reglas y documentos en una institución hace que los procesos de salvaguardar la información y sus componentes informáticos sea de manera empírica y produce la desorganización de recursos, por consiguiente, se creará un plan de contingencia que garantice la continuidad del funcionamiento de la infraestructura de red el mayor tiempo posible en caso de emergencia, brindando una oportuna respuesta a una situación de cualquier origen que se presente, garantizando la seguridad de la información y equipos que se considere de alto nivel de sensibilidad para la institución.

1.2 OBJETIVOS

1.2.1 OBJETIVO GENERAL

- Diseñar un plan de contingencia que permita garantizar la integridad, disponibilidad y operatividad de recursos lógicos y físicos en la unidad de Sistemas y Tecnología del Gobierno Autónomo Descentralizado de Antonio Ante en base a la norma ISO/IEC 27002.

1.2.2 OBJETIVO ESPECÍFICOS

- Analizar la metodología de la norma ISO/IEC 27002 y la Ley de Control Interno de la Contraloría General del Ecuador el artículo 410-11 que permita establecer lineamientos adecuados para el desarrollo del plan de contingencia.

- Realizar el levantamiento de información de la situación actual del GAD de Antonio Ante, para la identificación de escenarios de contingencia, riesgos lógicos, físicos y de índole ambiental que comprometan la seguridad de la información.

- Definir los procedimientos de acción y reacción, personal encargado, de la ejecución antes, durante y después de una emergencia, de tal forma que podamos asegurar la mayor disponibilidad de la red a través de políticas de seguridad y control.

- Establecer un plan de recuperación y respaldo de la información, mediante un manual de procedimientos, para mantener la disponibilidad, integridad y operatividad de la red en caso de un evento inesperado.

1.3 ALCANCE

El presente proyecto tiene como finalidad la elaboración de un plan de contingencia para el Gobierno Autónomo Descentralizado de Antonio Ante, con el propósito de proveer procedimientos que permitan mantener la disponibilidad integridad y operatividad de la red en caso de presentarse un evento externo o interno que inhabilite las funciones parciales o totales de la infraestructura tecnológica, minimizando pérdidas económicas y malestar en los usuarios que diariamente son atendidos por esta entidad.

Para el inicio del proyecto se realizará la revisión de fundamentos teóricos y lineamientos de la norma ISO/IEC 27002; como también el respectivo análisis de la Ley de Contraloría General del Estado el artículo 410-11 acerca de la implementación de un plan de contingencia para la Unidad de Tecnología de Información, que toda institución pública debe tener.

Posteriormente se procederá al levantamiento de información mediante la realización de inventarios de todos los activos importantes, su documentación se realizará de acuerdo a su importancia, donde se incluirá características de los equipos:

tipo, formato, ubicación información de respaldo, licencias actuales, el responsable de los equipos las revisiones periódicas, el nivel de protección, la prioridad, confidencialidad, son algunos de los parámetros para la clasificación.

Los tipos de activos a inventariar son: información, software, físicos y servicios, a continuación se describe cada uno.

- **Información**: bases de datos y archivos, contratos, acuerdos, documentación del sistema, información de investigaciones, manuales de usuario, materiales de capacitación, procedimientos operacionales o de soporte, rastros de auditorías e información archivada.

- **Software**: software de aplicación, software del sistema, herramientas de desarrollo y utilidades.

- **Físicos**: equipos de cómputo, equipo de comunicación, medios removibles.

- **Servicios**: servicios de computación y comunicación, servicios generales: calefacción, iluminación, energía y aire acondicionado.

Para la identificación de los posibles escenarios de contingencia que pueden causar interrupciones en el procesamiento de información se considerará lo siguiente: fallas en equipos, errores humanos, robo, fuego, desastres naturales, todos seguidos por una evaluación de riesgo para determinar la probabilidad e impacto de dichas interrupciones, en términos de tiempo, escala del daño y período de recuperación.

De acuerdo a los riesgos identificados y los impactos que producen dichas interrupciones y sus consecuencias se definirán procedimientos de control, políticas de seguridad, planes de mantenimiento; se definirán grados de responsabilidad para que en el momento de presentarse un evento imprevisto todos los presentes sepan que actividades realizar, antes durante y después para asegurar la operatividad de la red.

Finalmente se establecerá un plan de recuperación y respaldo de la información que contendrá procedimientos para mantener la continuidad de las comunicaciones y los requerimientos de seguridad tras ocurrir una interrupción o fallas en sus procesos, tanto a nivel físico como lógico o desastre natural de tal forma que aseguraremos la disponibilidad, integridad de la información. El plan de contingencia debe estar orientado a restaurar servicios de comunicación específicos a los clientes en un tiempo aceptable, se identificará y priorizará recursos críticos, periodos de desabastecimiento permitidos y prioridades de recuperación; este documento será socializado conjuntamente con el administrador de la red a los usuarios.

1.4 JUSTIFICACIÓN

La información de una institución es un recurso invaluable que debe ser protegida en su totalidad es por ello que el Gobierno Autónomo Descentralizado de Antonio Ante en su calidad de institución pública debe protegerla por su alto nivel de sensibilidad al manejar información de cientos de personas que diariamente acuden a las instalaciones a realizar transacciones fundamentales para el progreso económico y social de cantón.

Mediante la estructura de datos del GAD Municipal de Antonio Ante se transmite información utilizada en diferentes software aplicativos, los mismos que son usados para brindar servicios a la comunidad; si esta información es corrupta o sufre algún tipo de falla o daño se tendría una enorme pérdida, no solo de información sino también una pérdida económica.

Siendo un punto clave en la seguridad de información la prevención de daños, el GAD de Antonio Ante requiere la elaboración de un plan de contingencia que permitirá realizar el análisis de los procesos críticos, interrupciones importantes o desastres naturales, a los que se encuentra expuesta la red y los sistemas de información, de manera que podamos minimizar el impacto y reducir pérdidas de información.

Un plan de contingencia nos permite mantener controles preventivos y de recuperación, nos ayudan a la reanudación oportuna de las actividades principales, para restablecer los servicios de manera inmediata o en el menor tiempo posible luego de haberse producido una emergencia o suspensión procesos, de forma que nos permite garantizar la integridad y disponibilidad de la información.

Por otro lado la ley de control interno de la Contraloría General del Estado ecuatoriano en el artículo 410-11 determina que toda institución pública debe contar con un plan de contingencia que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado, para salvaguardar la información. En caso de un desastre es importante tener un tratamiento más riguroso para evitar de cualquier forma las amenazas y riesgos que se encuentra expuesta la red.

CAPÍTULO II

FUNDAMENTO TEÓRICO

En este capítulo se realiza el análisis de la norma técnica INEN ISO/IEC 27002 y el análisis del artículo 410-11 de la Ley de Control Interno del Ecuador, además los fundamentos teóricos necesarios para la mejor comprensión y desarrollo de un Plan de Contingencia Informático

2.1 ANÁLISIS DE LA NORMA TÉCNICA ECUATORIANA NTE UNEN-ISO/IEC 27002

ISO (Internacional Organization For Stadarization) e IEC (Commission Electrotechnique International) son organizaciones no gubernamentales y sin fines de lucro que se encargan de publicar estándares internacionales para las tecnologías de información con la única finalidad de facilitar la coordinación y unificación de estándares. (NTE INEN-ISO/IEC 27002, 2009)

Estas dos organizaciones han determinado un comité que se encarga de todos estos asuntos de las tecnologías de la información, se conforma por subcomités y cada uno de estos cumple diferentes funciones, el subcomité SC 27 es el encargado de las técnicas de la seguridad de las tecnologías de la información que ha venido desarrollando sistemas de gestión y seguridad del al información, gestión de riesgos, medición y lineamientos de implementación de sistemas de seguridad de la información, el estándar ISO/IEC 27002 es la nueva edición de la ISO/IEC 17799. (NTE INEN-ISO/IEC 27002, 2009)

Este estándar cuenta con 15 secciones que permiten gestionar la seguridad de la información a un nivel aceptable de disponibilidad para las organizaciones, a continuación se analizará cada uno de las secciones de manera general resaltando las ideas más significativas, haciendo énfasis en el sección 14 que trata acerca de la Gestión

de la Continuidad de Negocio que tomaremos como guía para el desarrollo del plan de contingencia. (NTE INEN-ISO/IEC 27002, 2009)

2.1.1 ALCANCE

Este estándar está orientado a las Técnicas y Prácticas para la Gestión de la seguridad de la información en empresas y organizaciones, con la finalidad de minimizar las probabilidades de sufrir daños por robos o pérdidas de información que dificulten las actividades operativas de las organizaciones.

2.1.2 ESTRUCTURA DEL ESTÁNDAR

La norma (NTE INEN-ISO/IEC 27002, 2009) se encuentra conformada por 11 secciones sobre controles de seguridad de la información, cada una de estas secciones contiene un objetivo de control y uno o más controles que se pueden aplicar para alcanzar el objetivo de control.

1. Política de seguridad.
2. Organización de la seguridad de la información.
3. Gestión de activos.
4. Seguridad de los recursos humanos.
5. Seguridad física y del entorno.
6. Gestión de operaciones y comunicaciones
7. Control de acceso.
8. Adquisición, desarrollo y mantenimiento de los sistemas de información.
9. Gestión de incidentes en la seguridad de la información.
10. Gestión de la continuidad del negocio.
11. Cumplimiento.

2.1.3 EVALUACIÓN Y TRATAMIENTO DEL RIESGO

Para la evaluación de riesgo se debe identificar, cuantificar y priorizar los riesgos a los que se encuentra expuesta la organización, los resultados no permitirán determinar los procedimientos adecuados para disminuir la probabilidad de que ocurran y los efectos negativos al no disponer de una adecuada seguridad. (NTE INEN-ISO/IEC 27002, 2009).

La reducción o tratamiento de riesgos debe ser un proceso que permita seguir medidas adecuadas y eficientes, se considerará los requerimientos y restricciones de la legislación, las regulaciones nacionales e internacionales, objetivos organizacionales, bienestar de usuarios, empleados, costos de implementación y operación. (NTE INEN-ISO/IEC 27002, 2009).

Es necesario señalar que por más controles de seguridad que se implementen no se conseguirá brindar una seguridad completa, sin embargo nos permitirá reducir al máximo los riesgos que afecten la seguridad de la organización. (NTE INEN-ISO/IEC 27002, 2009).

2.1.4 POLÍTICAS DE SEGURIDAD

Su objetivo es proveer soporte para la seguridad de la información, de acuerdo a los reglamentos y requisitos que la organización necesite en concordancia con los requerimientos comerciales, las leyes y regulaciones.

Debe existir con un documento con políticas de seguridad de la información aprobado debidamente por la dirección de la organización y difundido a todos los empleados, este documento debe ser claro, conciso y constar con definiciones como seguridad de la información, objetivos, alcance, importancia, estructuras de evaluación y gestión de riesgos, la explicación de las políticas o principios de la organización,

definición de responsabilidades etc., las políticas de seguridad de la información no deben mantenerse estáticas por el contrario siempre debe estar sujetas a cambios de acuerdo a las condiciones y en concordancia con los cambios tecnológicos. (NTE INEN-ISO/IEC 27002, 2009)

2.1.5 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Básicamente la organización de la seguridad de la información se puede dar de dos maneras: organización Interna y Partes Externas.

En cuanto a la organización interna nos permite manejar la seguridad de la información dentro de la organización, es importante contar con el apoyo de la dirección y que tenga el conocimiento de la las responsabilidades. Es fundamental que la dirección entienda que la seguridad es un aspecto con mucha relevancia que requiere inversión económica y que no representa un gasto innecesario para la empresa. (NTE INEN-ISO/IEC 27002, 2009).

Otros aspectos a considerar son los acuerdos de confidencialidad y la asignación de responsabilidades que no es más que nombrar a un encargado de los diferentes activos de esta forma en caso de problemas exista una persona claramente designada de manera verbal y escrita responda por sus actos y por lo que estaba a su cargo. (NTE INEN-ISO/IEC 27002, 2009).

La organización en partes externas se fundamenta en brindar la seguridad de la información y de los servicios de procesamiento donde se tiene acceso desde el exterior, para ello se procederá con la identificación de los riesgos de las partes externas e implementar controles necesarios. (NTE INEN-ISO/IEC 27002, 2009)

2.1.6 GESTIÓN DE ACTIVOS

La finalidad de este control es mantener una protección de los activos de mayor relevancia, mediante la asignación de un responsable, se debe contar con un inventario actualizado de todos los activos con los que se cuenta, quien es el encargado, así como también el uso para el que fueron adquiridos, y la clasificación de la información. (NTE INEN-ISO/IEC 27002, 2009)

2.1.7 SEGURIDAD DE LOS RECURSOS HUMANOS

El objetivo es afirmar que los empleados, contratistas y clientes comprendan sus responsabilidades y puedan reducir el riesgo de robo o fraude. Se definen claramente cuáles son los roles que va a cumplir cada empleado, las responsabilidades y obligaciones deberán ser establecidas como parte del contrato o acuerdo laborar que tiene cada empleado, debe existir capacitaciones periódicas para concientizar a los empleados. (NTE INEN-ISO/IEC 27002, 2009)

2.1.8 SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad física y del entorno se encuentra dividida en áreas seguras y seguridad de los equipos. Las áreas seguras nos permiten definir un perímetro limitado para proteger zonas donde se encuentra la información y los medios de procesamiento a fin de evitar el acceso no autorizado a las instalaciones o equipos sensibles, en la seguridad física también considera las amenazas externas y de origen natural como por ejemplo incendios, terremotos, inundaciones o actos terroristas, etc. Las instalaciones deben contar con medidas de seguridad que garanticen la protección de los equipos y el personal que trabaja en la organización. (NTE INEN-ISO/IEC 27002, 2009).

En cuanto a la seguridad de los equipos hay que evitar la pérdida, daños o robos de los activos a la interrupción de las actividades de la organización, todos los equipos deben ser protegidos contra las amenazas físicas y ambientales. (NTE INEN-ISO/IEC 27002, 2009).

Se debe controlar la temperatura adecuada para los equipos, seguridad del cableado, servicios de suministro, mantenimiento de equipos, etc. Para cumplir con estos requerimientos se necesita de personal técnico especializado para el cuidado y mantenimiento de los mismos así mismo la ubicación de los equipos debe ser la adecuada a fin de minimizar los riesgos. De igual forma se debe verificar y controlar el tiempo de vida útil de los equipos para que trabajen en condiciones óptimas. (NTE INEN-ISO/IEC 27002, 2009)

2.1.9 GESTIÓN DE COMUNICACIONES Y OPERACIONES.

Con la implementación de esta cláusula se pretende asegurar la correcta operación de los servicios y medios de procesamiento de la información, se establecen responsabilidades y procedimientos de gestión de procedimientos apropiados, todo procedimiento debe ser documentado y autorizado por la dirección. Otro aspecto importante es la gestión de cambios pues todo procedimiento debe documentado de esta manera podemos controlar los cambios en los servicios y los sistemas de información. (NTE INEN-ISO/IEC 27002, 2009)

- La adquisición de nuevos sistemas se debe tomar en cuenta la calidad de software para ello se debe tener personal capacitado que pueda evaluar y afirmar o negar la aceptación del nuevo sistema, tomando en consideración actualizaciones, versiones nuevas, realización de pruebas adecuadas. (NTE INEN-ISO/IEC 27002, 2009)

- La protección contra códigos maliciosos debe servir para proteger la integridad del software, los sistemas y tecnologías con que se cuenta. Además se debe tener controles de detección, prevención y recuperación. (NTE INEN-ISO/IEC 27002, 2009)

- Los respaldos de información son vitales y deben realizarse con una frecuencia razonable, a fin de evitar pérdidas de información de gran impacto negativo. (NTE INEN-ISO/IEC 27002, 2009)

- En cuanto a las redes, es necesario asegurar la protección de la información que se transmite y la protección de la infraestructura de soporte. Los servicios de red tienen que ser seguros. (NTE INEN-ISO/IEC 27002, 2009)

- Los sistemas tienen que estar muy bien documentados, detalle a detalle, incluyendo por supuesto la arquitectura de red con la que se cuenta. (NTE INEN-ISO/IEC 27002, 2009)

- Se tienen que establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación. Además de las medidas directas para proteger el adecuado intercambio de información. (NTE INEN-ISO/IEC 27002, 2009)

- Se debe recordar al personal el tomar las precauciones adecuadas, como no revelar información confidencial (NTE INEN-ISO/IEC 27002, 2009)

- Igualmente para los mensajes electrónicos se deben tomar medidas adecuadas, para evitar así cualquier tipo de problema que afecte la seguridad de la información. (NTE INEN-ISO/IEC 27002, 2009)

- Debe haber un continuo monitoreo para detectar actividades de procesamiento de información no autorizadas. Las auditorías son también necesarias. (NTE INEN-ISO/IEC 27002, 2009)

- Las fallas deben ser inmediatamente corregidas, pero también registradas y analizadas para que sirvan en la toma de decisiones. (NTE INEN-ISO/IEC 27002, 2009)

2.1.10 CONTROLES DE ACCESO

Toda organización o empresa debe controlar el acceso a la información y a los procesos críticos, esto se lo realiza en base a los requisitos de seguridad de cada institución, para la implementación se toma en consideración las políticas de seguridad que son las encargadas de minimizar las probabilidades de ser atacados, contar con un registro de usuarios, gestión de privilegios y la autentificación de usuarios y contraseñas. (NTE INEN-ISO/IEC 27002, 2009)

También es importante mantener el control de acceso a la red y a los diferentes sistemas operativos y aplicaciones que se manejan en las instituciones, para todo esto es necesario contar con registros y bitácoras de acceso. (NTE INEN-ISO/IEC 27002, 2009)

2.1.11 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Se contemplan requisitos de seguridad para la adquisición de sistemas de información a fin de garantizar que la seguridad es la parte principal en los sistemas de información, servicios y aplicaciones desarrolladas para los usuarios, se realiza un análisis y especificaciones de los requisitos de seguridad, todos estos procesos van de la mano con una validación adecuada tanto al ingreso como a la salida de datos, de forma que mantendremos el control del procesamiento interno de las aplicaciones. (NTE INEN-ISO/IEC 27002, 2009)

Mediante la implementación de controles criptográficos podemos proteger la confidencialidad, autenticidad e integridad de la información que viaja a través de la red, para esto se desarrollan políticas de seguridad acordes a la organización. Garantizar la seguridad de los archivos del sistema es fundamental, por lo que se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos de tecnologías de información y las actividades de soporte para evitar robos, alteraciones, o la aplicación de ingeniería inversa por parte de personas no autorizadas. (NTE INEN-ISO/IEC 27002, 2009)

Deben establecerse procedimientos para el control de la instalación del software en los sistemas operacionales. Con esto por ejemplo se evita el riesgo de realizar instalaciones ilegales o sin las respectivas licencias. (NTE INEN-ISO/IEC 27002, 2009)

2.1.12 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Para mantener una buena gestión en cualquier proceso es fundamental contar con una adecuada comunicación, entre todos los procesos, para ello se debe trabajar mediante reportes de vulnerabilidades y debilidades en seguridad de la información de tal forma que nos permitirá tomar una acción correctiva. (NTE INEN-ISO/IEC 27002, 2009)

Establecer mecanismos que nos permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información, nos ayudan a aprender de los errores que ya se cometieron. (NTE INEN-ISO/IEC 27002, 2009)

2.1.13 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Los daños causados por desastres naturales, fallas en equipos, fallas en la seguridad de la información, pérdida de servicios, son algunos de las eventualidades a las que

todas las organizaciones se encuentran expuestas y que deben ser analizadas para conocer el impacto negativo que generan en la organización y la forma de desarrollar e implementar planes de continuidad del negocio que nos permitan asegurar la reanudación de las actividades en el menor tiempo posibles y con las mínimas perdidas. Es importante contar con un plan de continuidad del negocio pues nos ayudan a la identificación y reducción de riesgos, la probabilidad de ocurrencia de dichas interrupciones y garantizar la disponibilidad de la información en los diferentes procesos del negocio. (NTE INEN-ISO/IEC 27002, 2009)

2.1.14 CUMPLIMIENTO

El cumplimiento de los requisitos legales evita cualquier tipo de violación a la ley, regulación o cualquier requerimiento de seguridad, protección de datos y privacidad de la información personal, prevención del uso indebido de los recursos de tratamiento de la información, y a regulaciones de los controles criptográficos. Todo sistema debe estar bajo monitoreo para garantizar el cumplimiento de los estándares de la implementación de la seguridad de la información. (NTE INEN-ISO/IEC 27002, 2009)

2.2 MARCO LEGAL

Es política del estado ecuatoriano que mediante los acuerdos ministeriales Nº 804 y 837 de 29 de julio y el 19 de agosto del 2011, respectivamente, la secretaria Nacional de la Administración Publica creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, dentro de sus atribuciones tiene a establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado; en el acuerdo Nº 166 publicado en septiembre 23 del 2013 la Secretaria de Administración Publica dictamina que es importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en

diferentes medios y formatos de las entidades de la administración Publica Central Institucional. (ACUERDO No. 166, 2013)

Además el registro oficial del acuerdo Nro. 039-CG de las Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos privados, en la sección Tecnología de la Información incluye aspectos con respecto a un plan de contingencia Informático en el artículo 410-11.

2.2.1 ANÁLISIS DEL ARTÍCULO 410-11 DE LA LEY DE CONTROL INTERNO DEL ECUADOR

La Ley de Control Interno es un documento que alberga un conjunto de disposiciones legales y normativas en diferentes sectores como: ambiental, eléctrico, administrativo, talento humano, información pública moderna, entre otras; este reglamento permite la regulación del funcionamiento del sistema de control público. En el artículo 410 de La Ley de Control Interno del Ecuador (2009, pág. 48) trata acerca de tecnologías de la información, se toma en consideración algunos aspectos de gran importancia tales como: la organización informática, segregación de funciones, planes informáticos estratégicos de tecnología, políticas y procedimientos, modelo de información organizacional, administración de proyectos tecnológicos, desarrollo y adquisición de software aplicativo, adquisiciones de infraestructura tecnológica, mantenimiento y control de la infraestructura tecnológica, seguridad en la tecnología de información, planes de contingencia, monitoreo y evaluación de procesos y servicios, sitios web, servicios de internet e intranet, comité informático y firmas electrónicas.

De este conjunto de secciones se analizará de manera sustancial artículo 410-11 Plan de contingencias (Registro Oficial Nro. 039-CG, 2009, pág. 52) que da una idea clara de cómo mantener la continuidad de las actividades dentro de la organización y los procesos que se debe realizar:

- Es indispensable que se cuente con un documento donde conste la asignación de responsabilidades dentro del área de tecnología de información, este documento debe ser claro, preciso, además debe describir escenarios de contingencias a los que se encuentra expuesto y como realizar una adecuada gestión de riesgos a fin de salvaguardar la seguridad de la información.

- Debe contar con procedimiento de control que ayuden a mantener la continuidad de las actividades en caso de presentarse una emergencia, de estar actualizado y acorde a las necesidades de la organización.

- Se debe de tener contemplado la posibilidad de contar con un centro de cómputo alterno que permita la recuperación de respaldos y la reanudación de las actividades en caso de sufrir grandes daños en el infraestructura física y se imposible restablecer las actividades desde el centro de datos principal.

- Los planes de recuperación ante desastres constarán de actividades previas, durante y después del desastre y deben ser dirigidas a través de un comité previamente asignado que ponga en funcionamiento el plan de recuperación en caso de una emergencia.

- Este documento será de carácter confidencial y su puesta en funcionamiento ayudará a la recuperación de las operaciones.

2.3 QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN

Existen diversas definiciones acerca de la seguridad de la información, podemos definir que la seguridad de la información no es más que un conjunto de reglas, controles y procedimientos que adoptan las organizaciones para salvaguardar la información de forma que se encuentre protegida de las diferentes amenazas como

fraudes, espionajes, vandalismos, incendios, inundaciones, software maliciosos, ataques de terceros, negación de servicios, etc.

De acuerdo con la NTE INEN-ISO/IEC 27002, (2009) la información es considerada como un bien activo para cada una de las organizaciones, es de vital importancia contar con una adecuada protección, con el propósito de disminuir los riesgos para el negocio y maximizar el retorno de inversiones y oportunidades. La información la podemos encontrar de diferentes formas, en papel o de manera digital, de cualquiera forma la información siempre debe contar con medidas de seguridad a fin de evitar pérdidas o modificación de datos que puedan poner en riesgo la continuidad de las actividades de la organización.

Una gestión eficiente de la seguridad de la información nos permite asegurar la confidencialidad, integridad y disponibilidad el mayor tiempo posible. (Correa García, 2009)

Entendiendo como:

Confidencialidad: que solo el personal autorizado tiene acceso a la información.
Integridad: asegurando que los información llegue completa y sin modificaciones.
Disponibilidad: que siempre se pueda acceder a ella el mayor tiempo posible.

En la figura 2.1 observamos los pilares fundamentales para bridar una eficiente seguridad de la información.

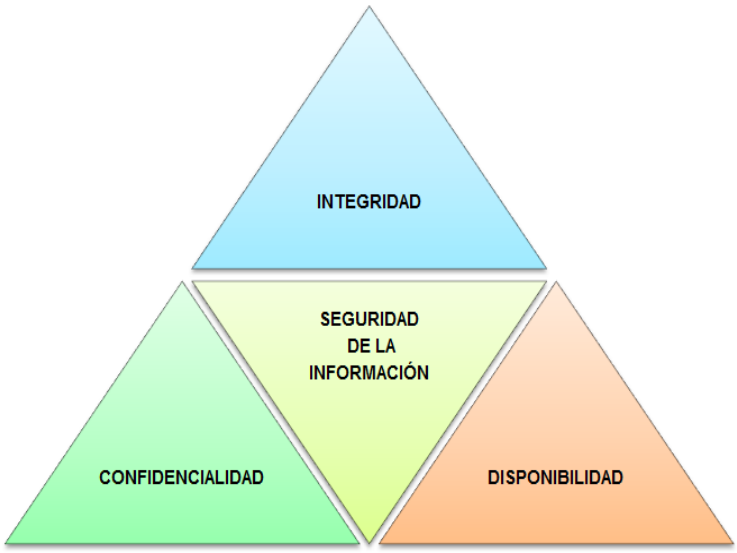


Figura 2.1 *Seguridad de la información según la norma ISO/IEC 17799*
Fuente*: http://cursohispano.com/conceptos-basicos-en-seguridad-de-la-informacion/sgsi/*

2.4 SISTEMAS DE INFORMACIÓN

Según Laudon, K & Laudon, J. (2004) un sistema de información se encuentra conformado por tres elementos como son: la información, recursos humanos y equipos computacionales que operan en conjunto para realizar actividades de administración, almacenamiento, procesamiento, transmisión o recepción datos e información con el único propósito de cumplir con los objetivos de la organización.

Para que un sistema de información genere los datos que las organizaciones necesitan, se requiere tomar decisiones, controlar las operaciones, analizar problemas y crear nuevos servicios:

En la figura 2.2 podemos apreciar de manera gráfica el proceso que realiza el sistema de información.

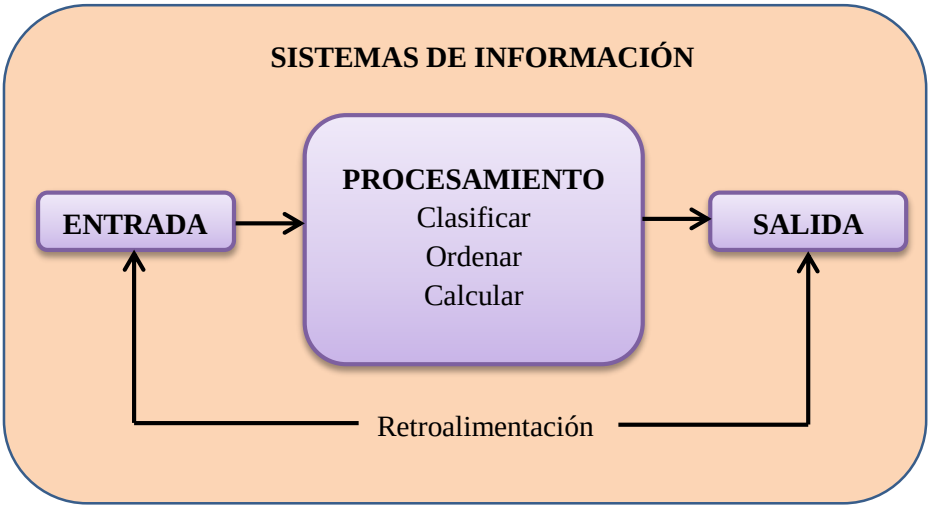


Figura 2.2 *Proceso de un Sistema de Información*

Fuente: *http://biblioteca.itson.mx/oa/dip_ago/introduccion_sistemas/p4.htm*

Entrada: captura de datos tanto desde el interior como del exterior del sistema de información.

Procesamiento: convertir datos e información de una manera más significativa para el negocio

Salida: transferir la información ya procesada a los usuarios para que desarrollen sus actividades diarias.

2.5 QUÉ ES UN PLAN DE CONTINGENCIA

Para HERNÁNDEZ, José (2005) un plan de contingencia informático es un proceso de medidas técnicas, humanas y organizativas, que nos permite contrarrestar las interrupciones que puedan limitar las actividades de la organización, es una herramienta de gestión que nos permite establecer procedimientos preventivos para proteger los procesos críticos, fallas en los sistemas de información de cualquier eventualidad que pueda presentarse, asegurando una recuperación oportuna de manera inmediata hasta un nivel aceptable en un menor costo.

Un plan de contingencia permite a las organizaciones continuar operando a pesar de fallas en los sistemas de información, se encuentra sujeto a tres acciones: prevención detección y recuperación.

Prevención: como su nombre lo indica son acciones que nos ayudan a prevenir cualquier eventualidad que afecte las actividades de las organizaciones de manera total o parcial a fin de reducir los impactos producidos.

Detección: son todos los daños que aún no se han considerado tanto de origen natural como otras eventualidades a fin de que en un futuro podamos prevenirlos y dar pronta solución ante la emergencia.

Recuperación: es el mantenimiento y recuperación de todos los recursos que fueron afectados por el desastre ya sean físicos o lógicos dentro de las organizaciones.

2.6 OBJETIVOS DEL PLAN DE CONTINGENCIA

Una vez analizado la norma NTE INEN-ISO/IEC 27002 y el registro oficial Nro. 039 GG, (2009) un plan de contingencia informático debe cumplir con los siguientes objetivos:

- Mantener la continuidad de los procesos considerados como críticos en un nivel aceptable en caso de una contingencia.

- Definir acciones y procedimientos que permitan mantener la operatividad de los sistemas de información en caso de una emergencia.

2.7 IMPORTANCIA DEL PLAN DE CONTINGENCIA

Toda institución debe contar con un plan de contingencia de información, permite minimizar el impacto de los desastres agilizando una recuperación pronta, por pérdida de activos de información, es importante identificar los procesos críticos para la organización mediante un análisis de impacto. Es de vital importancia que en el plan de contingencia esté establecido de manera clara quien es el encargado de tomar las decisiones durante el período de recuperación del desastre. (Hernández, 2005)

Entendiendo como desastre la interrupción prolongada de los recursos informáticos: la falta de acceso a la información, fallas en los sistemas de información, fallas eléctricas, procesamiento de datos, etc. Que dificulten las actividades normales de la organización.

2.8 TIPOS DE CONTINGENCIAS

Un plan de contingencia informático permite mantener la seguridad de la información, la protección del personal, las instalaciones y equipos, mediante procedimientos preventivos en caso de una emergencia en el área de sistemas, minimizando el tiempo de recuperación y evitando sustanciales pérdidas económicas.

La reanudación de las actividades del área informática puede llegar a ser un gran reto dependiendo de la magnitud de la emergencia a la que se enfrente, la preparación ante un desastre empieza con disponer de los datos suficientes para iniciar con la recuperación de las actividades. De acuerdo al grado de afectación sufrido por las diferentes contingencias se puede categorizarlas de la siguiente manera:

Bajo.- Cuando los daños solo afectan a las actividades diarias y se puede reparar el daño en el trascurso del día.

Medio.- Cuando las instalaciones se ven afectadas pero se puede reanudar las actividades.

Alto.- Cuando los daños afectan a las instalaciones y a las operaciones pero no es necesario trasladarse a instalaciones alternas.

Crítico.- Los daños afectan tanto a las instalaciones como a las operaciones de la institución y el tiempo de recuperación es más largo, es imposible seguir en las mismas instalaciones.

2.9 CARACTERÍSTICAS DE UN PLAN DE CONTINGENCIA

Un plan de contingencia eficaz, minimiza los daños ocasionados a la organización producto de la materialización de las amenazas de origen natural o por errores humanos, por consiguiente debe cumplir con las siguientes características: aprobación, flexibilidad, mantenimiento, costo-efectividad, respuesta organizada, responsabilidad y pruebas. A continuación se define cada una de estas características.

a) **Aprobación**: Debe ser aprobado por la dirección y los usuarios.
b) **Flexibilidad**: Debe poder adaptarse a cualquier contingencia, no debe ser específico para un solo desastre.
c) **Mantenimiento**: Ser preciso, evitar detalles innecesarios para que pueda ser actualizado.
d) **Costo-efectividad:** Las medidas aplicadas en cada una de las eventualidades deberán ser evaluadas con relación a las ventajas que nos brindan, deben ser razonables.
e) **Respuesta organizada:** Contar con una lista de las acciones y servicios que deben recibir prioridad.
f) **Responsabilidad**: Contendrá el nombre de los responsables que deben asumir las diferentes funciones en caso de una emergencia.

g) **Pruebas:** Se realizarán pruebas con inventarios de tiempo y procedimientos de respaldo, debe tener una metodología.

2.10 PLAN DE RESPALDO

Contiene todas las medidas y procedimientos preventivos para asegurar la reanudación de las actividades antes de que la amenaza se materialice, el plan de respaldo es el más importante, permite disminuir y mitigar la probabilidad de ocurrencia de desastres. (Instituto del Mar de Perú, 2012)

2.11 PLAN DE EMERGENCIA

Son las acciones que se deben tomar durante o inmediatamente después de la materialización de la amenaza a fin de disminuirla, es un mecanismo que nos permitirá seguir proporcionando funciones de procesamiento de la información cuando la actividad principal no esté disponible. (Instituto del Mar de Perú, 2012)

2.12 PLAN DE RECUPERACIÓN

Se definen los procesos o lineamientos que se deben seguir después de haber controlado la amenaza, en este plan se realiza la restauración de los equipos y actividades a su estado inicial antes de materializarse la amenaza. (Instituto del Mar de Perú, 2012)

2.13 FASES DE UN PLAN DE CONTINGENCIA PARA EL SISTEMA DE INFORMACIÓN.

Para el diseño del plan de contingencia informático, se realizó el análisis de la norma técnica (NTE INEN-ISO/IEC 27002, 2009), y el reglamento de la Ley de Control Interno del Ecuador, se procedió a definir las siguientes fases: planificación, identificación de escenarios de contingencia, evaluación de riesgos, identificación de controles preventivos, estrategias de protección tecnológica, plan de recuperación, pruebas, mantenimiento y monitoreo del plan de contingencia informático.

2.13.1 PLANIFICACIÓN

Dentro de esta fase se procederá a realizar el respectivo diagnóstico de la institución que comprende las siguientes actividades: el diseño de soluciones propuestas para un problema determinado, diagnóstico de la estructura organizacional, servicios que brindan a la ciudadanía, servicios consumidos, materiales utilizados y el inventario de los recursos informáticos, haciendo uso de herramientas automatizadas o de forma manual mediante la recopilación de información, así como también la delimitación del alcance de nuestro plan de contingencia (Moncada, 2001)

2.13.2 IDENTIFICACIÓN DE ESCENARIOS DE CONTINGENCIA INFORMÁTICOS

Para la identificación de los escenarios de contingencia se debe contar con la información necesaria de los riesgos críticos, identificarlos, conocer las causas y el impacto que generarían para la organización si llegaran a materializarse. (Moncada, 2001)

Todas las instituciones están expuestas a daños producto de desastres naturales o interrupciones en los sistemas, estas actividades producen pérdidas para la organización, en el siguiente diagrama 2.1 se observa los posibles escenarios de contingencia que pondrían en riesgo la seguridad de la información.

2.13.2.1 Identificación de Amenazas

Amenaza: cualquier acción o evento que se dé fuera del sistema y pueda interrumpir las operaciones y funcionamiento de la red o de los sistemas, las amenazas pueden ser accidentales o de manera intencional.

a) **Desastres naturales:** terremotos, incendios, inundaciones o filtraciones de agua.
b) **Desastres por falta de servicios:** fallas en el sistema de energía, ventilación y en el sistema de seguridad, en la red de datos, los equipos de networking y servidores.
c) **Fallas por terceros:** errores humanos, denegación de servicios, software malicioso virus informáticos, vandalismos, espionajes, suspensión en el procesamiento de información.

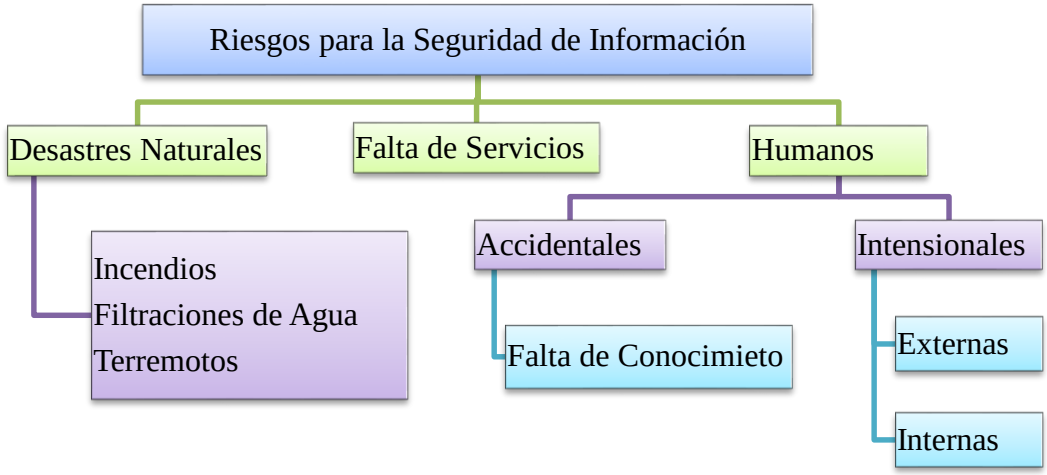


Diagrama 2.1. *Riesgos para la seguridad de la información*

Autora*: Karina Méndez*

El plan de contingencia debe realizar el análisis de todas las contingencias, realizar la evaluación de los mismos y ver el impacto que causaría en la organización, para ello es indispensable que tanto la gerencia como el personal a cargo de TI y los usuarios finales tengan el debido conocimiento.

a) Terremoto

Si el terremoto no produce daños graves en la estructura del edificio, lo datos no se verían afectados de ninguna forma, sin embargo por seguridad del personal que trabaja en las instalaciones se procedería a evacuar las instalaciones fuera del edificio hasta que el reingreso sea seguro, el impacto que tendría para el GAD de Antonio Ante este siniestro sería menor pues las actividades solo se paralizarían unas horas.

Por otra parte si el terremoto fuera de magnitudes mayores interrumpiría de manera prolongada las operaciones de la municipalidad, al sufrir daños físicos en el edificio también tendríamos perdidas de información en el centro de datos que se encuentra en las instalaciones de la institución y no se cuenta con un centro de datos alterno. Para esta situación se necesitaría que las medidas de emergencia y recuperación funcionen de manera adecuada.

Consecuencias.

- Daños en la infraestructura del edificio.
- Daños en la infraestructura de tecnológica.
- Daños en los equipos e indisponibilidad de los servicios
- Pérdidas de información.

b) Incendio

Si el fuego que se produce es grave y se origina dentro del área de sistemas causaría importantes pérdidas tanto de información como en los equipos, puesto que en esta área se encuentra ubicado el centro de datos donde están almacenados los servidores y equipos de networking por lo que de sufrir este siniestro se interrumpe la operatividad y disponibilidad de la red; por otro lado si el fuego es ocasionada en otra área o a su vez es controlado rápidamente no se vería afectada de manera significativa la disponibilidad de la red.

Consecuencias

- Daños en la infraestructura del edificio.
- Daños en la infraestructura de red
- Daños en los equipos e indisponibilidad en los servicios
- Pérdidas de información

c) Filtraciones de Agua

Si bien es cierto por su ubicación la municipalidad no corre riesgo de verse afectada por inundaciones, sin embargo, si se pueden presentar problemas de humedad por filtraciones de agua y esto provocaría serios daños en los dispositivos electrónicos que se encuentren expuestos.

Consecuencias

- Daños en la infraestructura del edificio.
- Daños en la infraestructura tecnológica e indisponibilidad de servicios.
- Pérdidas de información

d) Cortes de Energía

Según antecedentes, los cortes de energía en el municipio no son muy frecuentes; en caso de que se produzca un corte de energía en el exterior del municipio dependiendo del daños se obstaculizarían las actividades puesto que únicamente se cuenta con un UPS de 6KVA instalado en el cuarto de telecomunicaciones para proteger los servidores y equipos de networking, sin embargo, el resto de la red no funcionaría pues no se cuenta con un generador que brinde energía para el resto de la institución; por otro lado, si el corte de energía es producto de una mala práctica dentro del municipio los daños ocasionados serían graves, tendríamos afectaciones como: daños físicos en los equipos, daños en el cableado de las instalaciones eléctricas, disponibilidad parcial de la red, pérdidas de información.

Consecuencias

- Daños en la red eléctrica.
- Daños en los equipos.
- Pérdidas de información
- Indisponibilidad de los servicios.

e) Fallas de la Red de Datos

Las fallas en la red de datos pueden ser producto de no contar con un diseño físico adecuado que cumpla con las normas y estándares internacionales de instalación del sistema de cableado estructurado(SCE), el municipio tiene una red cableada categoría 6a, se encuentra debidamente instalada; otro problema que enfrenta es la falta de administración en los recursos de la red que trae como consecuencia la interrupción de los servicios y afecta a la disponibilidad de la información, posibles causas: ataques de DoS, errores lógicos o físicos, etc.

- **Denegación de servicios (DoS):** Es un ataque al sistema de red que evita el acceso a servicios o recursos dentro de la red haciéndolos inaccesibles para los usuarios, generalmente se produce por la saturación de los puertos haciendo que el servidor se sobrecargue con solicitudes.

- **Errores lógicos:** Se producen cuando las aplicaciones se encuentran en funcionamiento y en ocasiones son el resultado por mal manejo del usuario.

- **Errores físicos:** Se producen cuando existe una conexión errónea o cables en mal estado.

Consecuencias:

- Interceptación o pérdida de datos comprometería la confidencialidad de información y de las comunicaciones, las causas: la falta de procedimientos de seguridad, ingeniería social, robo de equipos que contengan información sensible, en conversaciones telefónicas al revelar información confidencial.

- Modificación o alteración de la información que afectaría la integridad de los datos, las causas: programas maliciosos o personal mal intencionado.

f) Fallas en el Hardware y Software

Las fallas producto de daños en software y hardware causadas por variaciones de voltaje, falta de mantenimiento en los equipos, falta de procedimientos para la instalaciones, fallas por desgaste de los equipos, códigos maliciosos, errores en los sistemas de arranque, saturación de los servicios, errores de programación y diseño, etc., el tiempo de recuperación variaría de acuerdo al daño ocasionado.

Códigos maliciosos como por ejemplo: virus, troyanos, gusanos, bombas lógicas, etc.

Virus: software malicioso que tiene por objetivo infiltrarse en el equipo para alterar el funcionamiento, se propagan a través de otro software para ejecutarse y tomar el control de los servicios básicos del sistema operativo.

Troyanos: programa que generalmente es inofensivo pero al ejecutarse crea un acceso remoto en el equipo infectando abriendo una entrada en la seguridad.

Gusanos: software malicioso que tiene la propiedad de propagarse por sí mismo, este tipo de software afecta el rendimiento de la red.

Bombas lógicas: son fragmentos de códigos de programa que se ejecutan en un momento determinado, por ejemplo una fecha o al ejecutar comando.

Consecuencias

- Daños físicos y lógicos en los equipos.
- Pérdidas y/o modificación de la información.
- Indisponibilidad de los servicios.

g) Accidentales - Falta de Conocimiento

Este tipo de riesgos se presentan normalmente por la falta de conocimiento en el uso de equipos, usuarios inconscientes o curiosos y virus electrónicos, generalmente no son conscientes de sus acciones pueden causar daños a la organización.

h) Intencionales

Hechos inesperados cuyo impacto es perjudicial entre estos tenemos: suplantación de identidad, modificación o alteración de la información, accesos no autorizados, fraudes, vandalismo, sabotajes, espionaje, ataques, robos y hurtos de información.

Ingeniería Social: Son ataques donde se intenta ganar el acceso no autorizado al sistema de computadores médiate el engaño a usuarios, para hacerles creer algo que no es cierto aprovechándose de su credulidad.

Suplantación de identidad: Actividad maliciosa donde el atacante se hace pasar por un usuario legítimo con el fin de cometer fraude, robos de información.

Modificación o alteración de la información: Intento de modificar información no autorizada, este tipo de ataques afectan la integridad de la información.

Accesos no autorizados: Intento de obtener información sin autorización del administrador de red, este tipo de ataques se dirige contra la confidencialidad de la información.

Vandalismo y Manifestaciones: Son actos vandálicos, que por menores que sean pueden llegar a causar daños a los equipos, periféricos, servidores e infraestructura de red, todos estos actos provocarían pérdida de información y como consecuencia las actividades se suspenderían de manera parcial o total dependiendo del daño causado.

2.13.2.2 Definición de eventos Controlables y No Controlables

Para la identificación de riesgos se procede a la categorización de los mismos, es imposible predecirlos con anticipación sin embargo los podemos clasificar de la siguiente manera:

Eventos Controlables: Cando al identificarlos se pueden tomar acciones preventivas que disminuyan el impacto y minimicen su ocurrencia.

Eventos No Controlables: Sucesos impredecibles que solo se pueden tomar acciones para minimizar el impacto.

2.13.3 EVALUACIÓN DE RIESGOS INFORMÁTICOS

Entendiendo como Riesgo: una vulnerabilidad explotada por una o varias amenazas que al materializarse provocan daños e interrupciones de los servicios y procesos de información, las consecuencias se presentan luego que ocurre un evento inesperado.

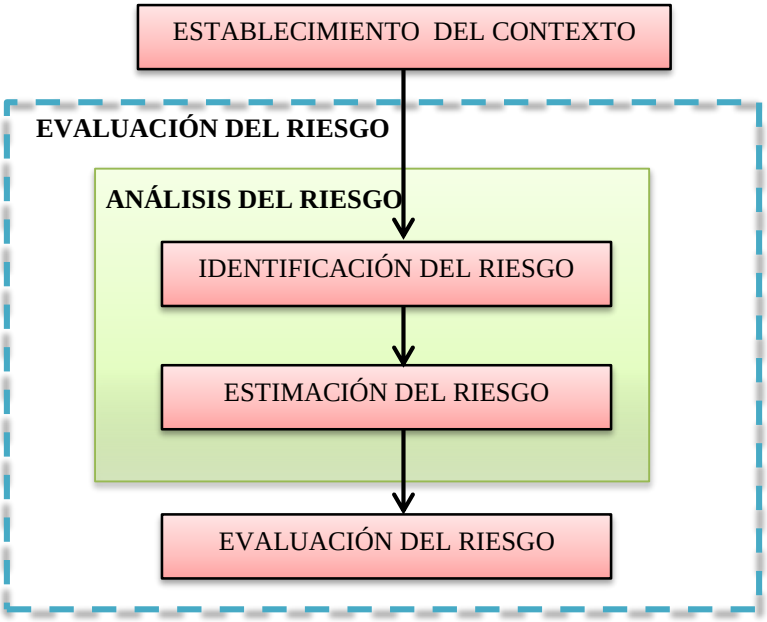
Dentro de la evaluación de riesgos se debe identificar, cuantificar y priorizar los riesgos dentro de la organización, estos resultados deben proporcionarnos la suficiente información para realizar una adecuada gestión de riesgo mediante la implementación de controles de protección.

Se debe realizar una evaluación periódica de los riesgos que puedan afectar a la organización, por consiguiente se tomará como guía de referencia NTC-ISO 27005, que nos proporciona directrices para la seguridad de la tecnología de información, mediante una serie de metodologías y ejemplos para realizar la evaluación de riesgos en los diferentes sistemas y componentes de la información. Para la evaluación de riesgos y consecuencias producto de la materialización de una o varias amenazas, se debe realizar el siguiente proceso:

a) Identificación de riesgos.
b) Evaluar los riesgos en términos de impacto y probabilidad de ocurrencia.
c) Establecer un orden adecuado de prioridad en el tratamiento de los riesgos.
d) Identificar el tiempo máximo de interrupción permitida en los servicios y procesos críticos.
e) Definir la designación de roles de trabajo y obligaciones al personal en caso de emergencia.

f) Realizar un monitoreo continuo de los riesgos.

En la figura 2.3 se observa el proceso para la gestión de riesgos.



F*igura 2.3.* *Proceso de evaluación del riesgo de la seguridad de la información*

***Fuente**: https://es.scribd.com/doc/124454177/ISO-27005-espanol*

En el proceso de identificación de riesgos es importante conocer los puntos críticos dentro de la organización, para brindarle la debida atención a cada proceso, no toda la información ni todo proceso van a tener la misma importancia para la organización. (Moncada, 2001)

2.13.3.1 Identificación de vulnerabilidades tecnológicas

Vulnerabilidad: Es una debilidad en la seguridad de la información que se puede dar lugar por diferentes causas como por ejemplo la falta de mantenimiento, falta de conocimiento en el personal, desactualizaciones de los sistemas críticos, etc.

Para realizar esta actividad se hace uso de la lista de los activos y los controles existentes dentro de la organización, las vulnerabilidades se pueden encontrar en las siguientes áreas:

a) Organización.
b) Procesos y procedimientos.
c) Rutinas de gestión.
d) Personal.
e) Ambiente físico.
f) Configuración del sistema de información.
g) Hardware, software o equipos de comunicaciones.

Evaluación de Vulnerabilidades

Para la evaluación de las vulnerabilidades técnicas se puede aplicar diferentes métodos por ejemplo la utilización de herramientas de software de exploración automática, entrevistas, cuestionarios, inspecciones físicas entre otros; todo dependerá de la importancia del sistema de tecnología de información y los recursos disponibles. (NTC-ISO 27005)

Los criterios para la evaluación de las vulnerabilidades de establecen de la siguiente manera:

Tabla 2.1 *Criterios de Evaluación de Vulnerabilidades*

Autora*: Karina Méndez*

Características / Denominacion	Facilidad de explotación	Capacidad de Detección	Costo de recuperación
Alta	Probable	Difícil	Alto
Media	Posible	Posible	Alto
Baja	Posible	Posible	Mínimo
Mínima	Poco probable	Probable	Mínimo

2.13.3.2 Valoración de Activos

Una vez identificado los activos de mayor relevancia, se procede a la definición de una escala de valoración para cada uno de los activos críticos, puede ser de forma cuantitativa o cualitativa. En concordancia con el departamento de informática se hará uso de la siguiente tabla 2.2 de valoración de los activos:

Tabla 2.2 *Valoración de activos*

Fuente*: http://www.slideshare.net/mmujica/mi-defensa*

VALORACIÓN DE LOS ACTIVOS				
Valor	**Denominación**	**Disponibilidad**	**Integridad**	**Confidencialidad**
4	Critico	La información, instalaciones y recursos siempre debe estar disponibles Su pérdida es considerada como catastrófica para la Institución.	Toda información, instalación o recurso donde la integridad es importante y debe garantizarse Su pérdida seria catastrófica.	Abarca toda información, instalación o recurso calificado como de uso confidencial. Solo puede ser utilizado con autorización explícita
3	Alto	Toda información, instalación o recurso cuya disponibilidad puede estar detenida por algunas horas.	Abarca toda información, instalación o recurso en el cual la integridad es muy importante y debe garantizarse.	Toda información, instalación o recurso calificado como de uso restringido. Solo puede ser utilizado por personal autorizado.

VALORACIÓN DE LOS ACTIVOS				
Valor	**Denominación**	**Disponibilidad**	**Integridad**	**Confidencialidad**
2	Medio	Toda información, instalación o recurso cuya disponibilidad puede estar detenida por 24 horas máximo.	Todo recurso, información o instalación en el cual la integridad es de importancia media y debe garantizarse.	Información, instalación o recurso calificado como de uso semi-restringido. Solo puede ser utilizado por personal interno.
1	Bajo	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 48 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad no es muy importante pero debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso interno. Solo puede ser utilizado por personal interno o usuarios/clientes.

Los criterios que se considerará para la asignación de los valores a los activos será:

a) El costo original del activo.
b) El valor acumulado por pérdida de confidencialidad, integridad, disponibilidad.
c) El impacto generado para la organización por daños o suspensión de los servicios.

2.13.3.3 Análisis de Riesgo

Existen varias razones para aplicar el análisis de riesgos dentro de una organización, permite identificar activos, controles de seguridad, criterios para el diseño y evaluación de planes de contingencia, en general permite mejorar la seguridad de todos nos niveles de la infraestructura tecnológica; se fundamenta en toda la información recopilada en la etapa de realización de inventarios de los activos de mayor relevancia para la organización.

Esta etapa se encuentra comprendida por tres elementos que nos permite dar un valor a los riesgos: la probabilidad de ocurrencia, el impacto y la determinación de riesgo. (NTC-ISO 27005)

a) Probabilidad de Riesgo.

La probabilidad de ocurrencia de una amenaza se debe establecer bajo qué circunstancias el activo tendrá valor o necesitará protección. (NTC-ISO 27005), se determinará en base a estadísticas recogidas a lo largo de la administración, además se tomará en consideración lo siguiente:

- La importancia del activo para la organización.
- La facilidad de explotación de una vulnerabilidad del activo.
- La susceptibilidad técnica de la vulnerabilidad a la explotación.

b) Evaluación de Probabilidad de Riesgo

La evaluación de la probabilidad de ocurrencia se realiza mediante la identificación de las amenazas, los activos afectados y las vulnerabilidades, también se tomará en cuenta la frecuencia con la que ocurren las amenazas. (NTC-ISO 27005)

En la tabla 2.3 se define las cuantificaciones para la designación de frecuencia de cada uno de las vulnerabilidades encontradas.

Tabla 2.3 *Probabilidad de Ocurrencia*

Autora*: Karina Méndez*

NIVEL	DENOMINACIÓN	DESCRIPCIÓN
76-100%	Muy Frecuente	Eventos repetitivos
51-75%	Frecuente	Eventos aislados
26-50%	Ocasional	Sucede alguna vez
0-25%	Remoto	Improbable que suceda

c) Impacto del Riesgo

Un eventualidad en la seguridad de la información de puede afectar a más de un activo dentro de la organización, estos impactos pueden ser inmediatos a en el futuro que provocaría pérdidas financieras. El impacto inmediato puede ser directo o indirecto. (NTC-ISO 27005)

Directo: Se denomina impacto directo cuando se necesita el remplazo del activo perdido, configuración, instalación o copia de soporte, el costo de las operaciones suspendidas debido al incidente hasta volver a las actividades normales. (NTC-ISO 27005)

Indirecto: Cuando la afectación genera pérdida de oportunidades por los daños en los equipos o cuando se utilizaron recursos que pudieron usarse en otra parte y los costos por interrupción de las actividades. (NTC-ISO 27005)

Existen diferentes criterios para realizar la valoración de los impactos causados por los diferentes riesgos, depende únicamente de cada organización el definir las consideraciones necesarias para llevar a cabo esta actividad. (NTC-ISO 27005)

- El grado de afectación o el costo que implicaría para la organización si se produce algún daño o la interrupción de un proceso crítico.
- De acuerdo a la importancia de los activos de la institución.
- Las brechas de seguridad que existen tanto a nivel de lógico como físico.
- Las operaciones que se realizan tanto al interior como al exterior.
- El valor financiero para la organización si sufre alguna emergencia.

Tabla 2.4. *Prioridades de evaluación del impacto*

Autora. *Karina Méndez*

IMPACTO	VALOR	DESCRIPCIÓN
Bajo	1	Cuando no afectan las actividades y los sistemas principales trabajan de forma normal.
Medio	2	Cuando los daños son parciales y se dan en los sistemas, no afecta a las operaciones.
alto	3	Cuando se ven afectadas de manera directa las operaciones y funciones, los usuarios y los sistemas informáticos.
critico	4	Pérdida de información crítica, daños severos en los equipos, Suspensión de funciones

d) Determinación del Riesgo

La determinación del riesgo de un sistema se establece mediante el impacto de las amenazas sobre el valor acumulado de cada uno de los activos más relevantes y la probabilidad de ocurrencia.

En la ecuación 2.1 se observa la forma del cálculo del riesgo.

Riesgo *= V. Activo* Impacto * Probabilidad ocurrencia*

Ecuación 2.1 *Cálculo del riesgo*

Los riesgos que tengan alto nivel en probabilidad de ocurrencia y gran impacto dentro de la organización son los que debemos considerar al momento de la elaboración del plan de contingencia. En la figura 2.4 podemos observar el nivel de riesgo.

PROBABILIDAD				
4	**A**	**A**	**C**	**C**
3	**M**	**M**	**A**	**C**
2	**B**	**M**	**M**	**A**
1	**B**	**B**	**M**	**A**
	1	2	3	4

IMPACTO

Figura 2.4 *Niveles del riesgo*

Fuente*: http:// Www.Gestiopolis.Com/Administracion-Estrategia/Riesgo-En-La-Estrategia-Administrativa.Htm*

- El rojo nos indica los riesgos críticos (C)
- El naranja no indica que son riesgos altos (A)
- El amarillo son riesgos medios (M)
- El verde no indica los riesgos bajos (B)

2.13.3.4 Tipos de análisis Riesgos

La estimación del riesgo se define de acuerdo a diferentes niveles de detalle dependiendo de la criticidad de los activos y vulnerabilidades conocidas. La estimación de riesgos se puede realizar de dos formas: cuantitativo y cualitativo.

a) **Cualitativo:** Cuando usamos adjetivos calificativos como alta, media, baja, mediante estos podemos describir las consecuencias o probabilidades de ocurrencia de un riesgo, su aplicación es más sencilla e intuitiva, se refiere a una estimación de pérdidas. (NTC-ISO 27005)

b) **Cuantitativo:** La estimación cuantitativa nos permite dar valores numéricos tanto para las consecuencias como para la probabilidad de ocurrencia, utiliza como fuente datos de incidentes anteriores. (NTC-ISO 27005)

En todo proceso de evaluación de riesgo es primordial que tanto directores como personal operativo estén al tanto de todas las actividades a realizarse en caso de una emergencia para disminuir posibles daños potenciales, se recomienda llevar una documentación de los resultados de las actividades desarrolladas dentro del proceso de gestión de riesgo y dentro de la seguridad de la información. (NTC-ISO 27005)

Para realizar la asignación de un valor a los riesgos encontrados en la seguridad de la información es importante considerar lo siguiente:

1. Objetivos estratégicos de la organización, políticas.
2. Las funciones y estructura de la organización.
3. Políticas de seguridad de la información que tiene la institución.
4. Enfoque general de la organización hacia la gestión de los riesgos.
5. Los activos de información.
6. La ubicación y sus características.

2.13.4 IDENTIFICACIÓN DE CONTROLES PREVENTIVOS

El objetivo en esta fase es bridar alternativas eficientes que minimicen la aparición de vulnerabilidades, estos procedimientos deben ser documentados junto con las causas que lo provocaron y las acciones tomadas. (Moncada, 2001)

Para desarrollar las expectativas propuestas consideraremos algunas las siguientes actividades:

- La formación de equipos que brinden soporte en caso de una contingencia.
- La asociación de soluciones con cada riesgo identificado.
- Determinar procesos críticos y el impacto para la organización si estos fallan.
- Identificar una perdida aceptable de información y servicios.
- Mantener actualizado el documento donde se encuentras las soluciones y reglas de implementación.

2.13.4.1 Estrategias de protección tecnológica

Qué hacer si a pesar de todas las medidas de seguridad tomadas para garantizar la continuidad de las operaciones dentro de la organización ocurre algún evento imprevisto, es importante tener nuestro plan de contingencia informático que nos permita estar preparados para reaccionar y actuar ante una emergencia para mantener el funcionamiento normal de las actividades. (Hernández, 2005)

Se debe definir una estrategia de recuperación que contenga una guía de procedimientos para la recuperación ante el desastre, la elección de la misma se determinará de acuerdo a la criticidad de los procesos o aplicaciones, tiempo de recuperación y la seguridad requerida. (Hernández, 2005)

HERNÁNDEZ, J (2005) nos dice que, de acuerdo al tipo de organización existen diferentes tipos de centros de recuperación:

Hot sites: Son centros de procesos que son totalmente compatibles con el centro primario tanto en software como en hardware, se encuentran bien equipados, configurados y listos para entrar en funcionamiento a poco tiempo que sea declarado el desastre, el costo de instalación es medio alto. (Hernández, 2005)

Warm sites: Centros parcialmente configurados para desempeñar las operaciones del centro primario, contiene la mayor parte del hardware periférico, pero no tienen respaldo de los equipos centrales, de costo de instalación es moderado, el tiempo para la recuperación es mayor al del Hot sites, pues únicamente reconstruye el ordenador central pero no se lo puede usar al inmediatamente. (Hernández, 2005)

Cold sites: Centros con la infraestructura básica, electricidad, salas para instalar equipos, mesa, sillas, no cuenta con equipamiento de hardware ni de telecomunicaciones, este centro únicamente se encuentra preparado para recibir equipamiento del centro primario, el costo de instalación de este centro es bajo, el tiempo de que entre en funcionamiento es relativamente largo. (Hernández, 2005)

Centro duplicado: Son centros diseñados para entrar en funcionamiento al instante de haberse declarado la emergencia, actúan como un reflejo del centro primario, el costo de instalación es alto, estos centros pueden tener duplicado de total o únicamente de los procesos críticos. (Hernández, 2005)

2.13.5 DOCUMENTACIÓN DEL PROCESO

Después de haber realizado el análisis de los riesgos y elaborar una serie de recomendaciones en caso de alguna eventualidad o desastres se procede a la documentación de lo descrito anteriormente en las fases. Este documento debe ser redactado en un lenguaje simple y entendible para todos.

Debe contener la siguiente información:

- Conocer la situación previa al desastre.
- Contar con información de los riesgos.
- Identificar procesos y recursos de Infraestructura de telecomunicaciones que se debe recuperar.

- Designación de responsabilidades y soluciones a realizar en caso de contingencias.

Se debe realizar una revisión continua del plan de contingencia establecido, pues tanto la tecnología como el negocio crecen, evolucionan y lo que en este momento es útil más adelante será obsoleto. Para contar con un buen mantenimiento del plan de contingencia es importante tener en consideración lo siguiente:

- Las necesidades del negocio.
- La adquisición de nuevo hardware o desarrollo de nuevas aplicaciones de software.
- Los procesos críticos cambian de acuerdo a las necesidades del negocio.

2.13.6 REALIZACIÓN DE PRUEBAS Y VALIDACIÓN DE LOS PLANES DE CONTINGENCIA

La realización de pruebas en el Plan de Contingencia permite asegurar que tanto el equipo de recuperación como el resto del personal deben conocer sus responsabilidades para el restablecimiento de la operatividad de la red y la seguridad de la información; las pruebas deben contemplar la siguiente información:

a) Verificar que la información del plan este correcta y completa.
b) Evaluación del personal involucrado.
c) Evaluación de la coordinación entre el equipo de emergencia y componentes externas.
d) Evaluación de la capacidad de recuperación.
e) Evaluación del rendimiento general de la organización después de la recuperación.

2.13.6.1 Evaluación de resultados y pruebas

Luego de haber concluido las operaciones de recuperación de los sistemas que se vieron afectados por el siniestro, se debe evaluar de forma objetiva las actividades realizadas, que tan eficientes fueron y en qué tiempo se resolvieron; estos resultados generados darán las pautas necesarias para la retroalimentación del plan de recuperación y la perdida generada por el desastre. (Hernández, 2005)

Niveles de pruebas para un plan de contingencia:

- Pruebas en pequeñas unidades funcionales o divisiones.
- Pruebas en unidades departamentales.
- Pruebas interdepartamentales o con otras bodegas.

2.13.6.2 Métodos para las pruebas de los Planes de Contingencia.

Es importante que al desarrollar un plan de contingencia se realicen pruebas que garanticen el desempeño real del proyecto. A continuación se presentan 3 métodos:

Pruebas específicas: Se refiere a realizar pruebas de una sola actividad, capacitando al personal en una función específica, y basándose en los procedimientos definidos en el plan de contingencia, estas pruebas pueden ser realizadas en los recursos y servicios del proveedor, o garantizando una recuperación técnica de manera eficiente.

Pruebas sobre papel: Se basa en un conjunto de preguntas que va dirigido al equipo de recuperación de las contingencias donde se pone a prueba las habilidades de del equipo y sus responsabilidades, se evalúan en varios escenarios y realizando interrupciones a los diferentes sistemas.

Simulacro en tiempo real: Estas pruebas son con un simulacro real, en un determinado departamento, y están dirigidas a una situación de contingencia por un

tiempo de periodo definido, estas pruebas permiten evaluar habilidades coordinativas y de trabajo en equipo de los grupos asignado para afrontar las contingencias.

2.13.6.3 Retroalimentación del plan de acción

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente, la evaluación con respecto al costo que representaría para la institución el no contar con un plan de contingencia. (Hernández, 2005).

CAPÍTULO III

PLAN DE CONTINGENCIA INFORMÁTICO PARA EL MUNICIPIO DE ANTONIO ANTE

El presente capítulo explica cada una de las fases para la elaboración de un Plan de Contingencia Informático para el Departamento de Sistemas y Tecnología de Información del Municipio de Antonio Ante, conformado de la siguiente forma: alcance del Plan de Contingencia, el diagnóstico inicial de la institución respecto a los recursos informáticos que actualmente mantiene, escenarios de contingencia, evaluación de los riesgos e identificación de controles que ayuden a disminuir los riesgos.

3.1 PLANIFICACIÓN

Toda institución pública o privada debe contar con un Plan de Contingencia Informático, y tener la capacidad de afrontar cualquier eventualidad que disminuya el rendimiento de las actividades; la organización debe estar involucrada con los planes de prevención, ejecución y recuperación ante desastres o interrupción de servicios, será definido por un grupo responsable de la elaboración, validación y mantenimiento del mismo.

Para que la recuperación ante un desastre sea eficaz y lo más eficiente posible es necesario que el grupo de trabajo se encuentre bien distribuido y sus funciones bien establecidas.

3.1.1 ALCANCE

El diseño de este Plan de Contingencia Informático incluye los sistemas de información, equipos, infraestructura de red, formación de grupos de trabajo que permitirán minimizar los riesgos.

Este proyecto de titulación se presentó al Jefe del Departamento de Sistemas del GAD de Antonio Ante, se estipuló que, en la elaboración de este Plan de Contingencia no se realizará el desarrollo de la fase de pruebas y validación del plan de contingencia, así como tampoco la implementación del mismo, por consiguiente queda a cargo de las autoridades del municipio y del Departamento de Sistemas de Información una vez terminado este proyecto de titulación proceder al desarrollo de las mismas.

3.2 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

El Gobierno Autónomo Descentralizado de Antonio Ante actualmente cuenta con una red de datos la cual es administrada y gestionada a través del Departamento de Sistemas y Tecnología del municipio. La infraestructura tecnológica se encuentra conformada por una red LAN por donde se envía y recibe gran cantidad de información diariamente, la red no tiene los suficientes mecanismos de seguridad de la información que garanticen la integridad de la misma.

El Departamento de Sistemas maneja ciertos mecanismos de seguridad básicos como: control de acceso a la información con la protección de Windows, manejo de claves para la autentificación de usuarios para el acceso a la información de los servidores, realización de respaldos de la información más relevante dos veces al día; sin embargo estos procesos no son suficientes para responder ante un desastre natural o interrupción de los servicios.

La institución se encuentra sujeta a cambios constantes, tanto en software como en hardware, por lo que es indispensable manejar una documentación de los diferentes procesos que se realizan, así como también se debe realizar un análisis continuo de los riesgos que pueden afectar a los sistemas críticos, su nivel de tolerancia; se debe establecer prioridades de recuperación de los activos más relevantes dentro de la institución, manejar un proceso continuo de verificación del estado de las comunicaciones y servicios dentro de la red, mejorar el control de acceso con las debidas restricciones.

Con la implementación de un plan contingencia informático se proveerá de objetivos de recuperación de información basados en periodos de tiempo, cuando va a entrar en operación el centro de respaldo, manteniendo un nivel aceptable la disponibilidad de la red mientras se restablecen completamente las actividades luego de haber sido afectado por un incidente.

3.2.1 DEPARTAMENTOS DEL MUNICIPIO DE ANTONIO ANTE

El cantón de Antonio Ante se encuentra ubicado al noreste de la provincia de Imbabura, con un total de 45.184 habitantes según el censo del 2010 realizado el INEC (Instituto Nacional de Estadísticas y Censos).

A fin de mejorar el servicio a la colectividad la municipalidad de Antonio Ante se encuentra conformada por varios departamentos, cada uno desempeña funciones importantes que permiten brindar diferentes servicios; diariamente manejan gran cantidad de información y debe contar con un adecuado tratamiento tratando de preservar la integridad y confidencialidad de los datos

En la figura 3.1 se observa el orgánico estructural del GAD de Antonio Ante y posteriormente la descripción breve de cada uno de los departamento de la institución.

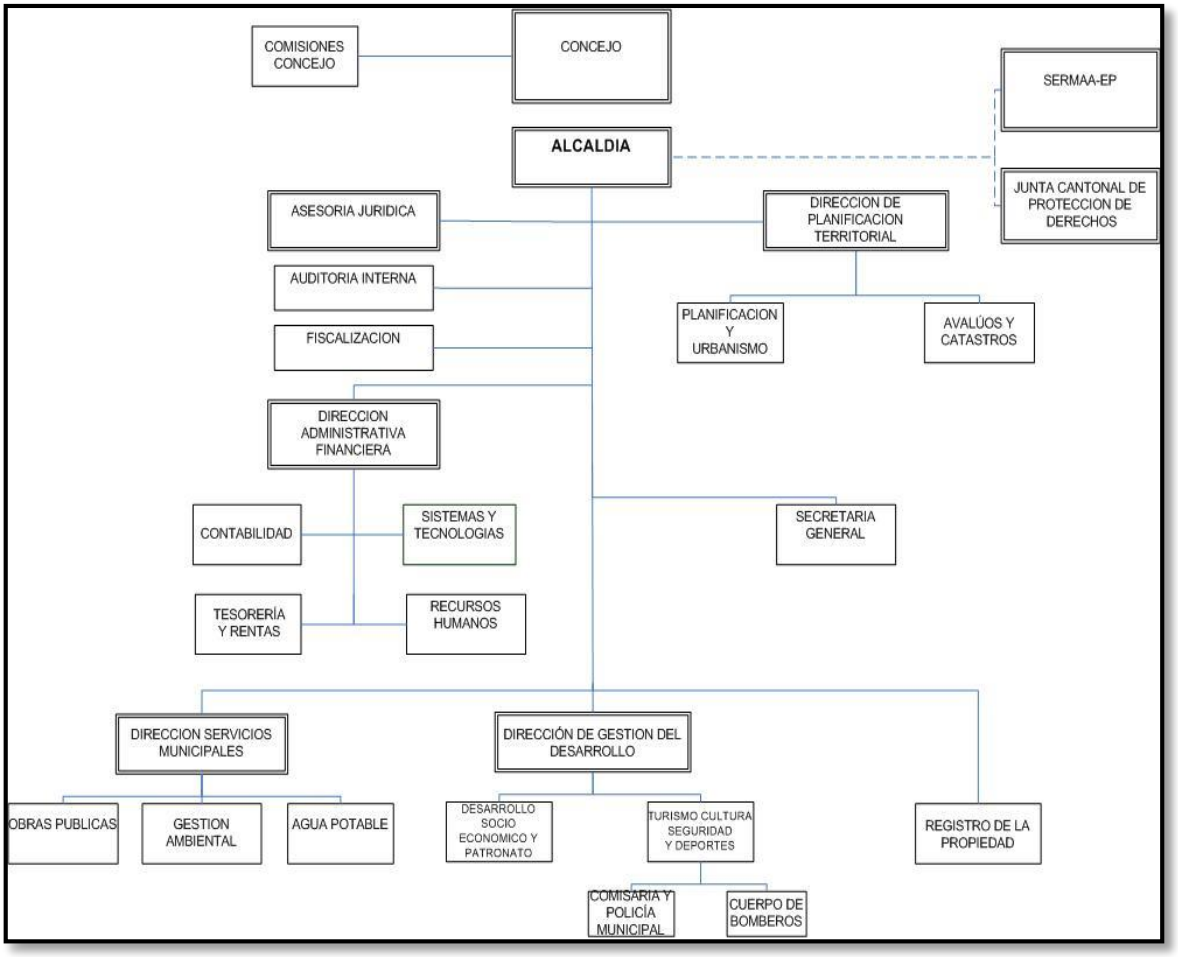


Figura 3.1. *Diagrama organizacional del GAD de Antonio Ante*

Fuente*: http://www.antonioante.gob.ec/web/?page_id=45*

a) Dirección Administrativa Financiera

Entre las funciones principales que desarrolla el Departamento de Dirección Administrativa y Financiera es realizar la implementación de esquemas de control financiero, elaboración de normas técnicas, normas y reglamentos de control interno dentro de la municipalidad, elaboración de proyectos y ordenanzas, dirección de la administración tributaria de la municipalidad, organizar, suministrar y controlar los servicios de mantenimiento en los equipos, automóviles, bienes muebles e instalaciones, así como también los sistemas de seguridad y vigilancia, administración de pólizas de seguros de los diferentes activos de la institución. (Gobierno Municipal de Antonio Ante, 2014)

b) Contabilidad

Este departamento se encarga de llevar la contabilidad automatizada de la municipalidad a través de del sistema integrado contable de tal manera que tiene a disposición los estados financieros de manera confiable y oportuna, presentación de informes periódicos, registros de ingresos y egresos, además se encarga de la coordinación y control del proceso contable. (Gobierno Municipal de Antonio Ante, 2014)

c) Tesorería y Rentas

Es el encargado de organizar supervisar ejecutar tareas de supervisión, optimización de servicios y la recuperación de cartera, preparación de reportes de recaudación y saldos. (Gobierno Municipal de Antonio Ante, 2014)

d) Sistemas y Tecnología

Se encarga de brindar soporte técnico en el área informática y a las diferentes unidades administrativas dentro de la municipalidad con el fin de mantenerse siempre a la vanguardia en tecnología. Entre las principales funciones que realiza son: administración, diseño e implementación de la red informática, instalación y configuración de software y equipos de cómputo, desarrollo de sistemas informáticos de acuerdo a las necesidades presentadas y la actualización de respaldos de los diferentes sistemas de información del municipio. (Gobierno Municipal de Antonio Ante, 2014)

e) Turismo Cultura Seguridad y Deportes

Las actividades desarrolladas por este departamento es la planificación, ejecución de proyectos para el desarrollo turístico, cultural y deportivo del cantón, la supervisión de la prestación de los servicios de la comisaria, policía municipal y el cuerpo de bomberos. (Gobierno Municipal de Antonio Ante, 2014)

f) **Dirección de Planificación Territorial**

Desarrollar acciones y liderar el proceso cantonal de planificación del desarrollo y ordenamiento territorial, coordinar la planificación estratégica institucional en función de la planificación cantonal y la elaboración de los presupuestos participativos territoriales, mmantener actualizada la información geo referencial con indicadores económicos, sociales, servicios básicos, coordinar la elaboración de presupuestos participativos parroquiales, y mantener un inventario de proyectos. (Gobierno Municipal de Antonio Ante, 2014)

g) **Avalúos y Catastros**

Organización, coordinación y supervisión de labores técnicas de avalúos y catastros urbanos y rurales, velar por el cumplimiento de la Ley y más normas a efectos de determinar los tributos, estudiar y analizar las ordenanzas y reglamentos vigentes relativos a la propiedad inmobiliaria y sugerir si fuere el caso su actualización, la elaboración anual de inventarios de solares no edificados y propiedades horizontales. (Gobierno Municipal de Antonio Ante, 2014)

h) Planificación y Urbanismo

Establecer las políticas, planes de desarrollo estratégico en materia urbana territorial. Planear, organizar y dirigir el ordenamiento urbano y parroquial, supervisar y controlar el crecimiento ordenado del Cantón participar en los estudios de racionalización del tránsito y transporte terrestre, tanto urbano como rural, así como los proyectos de terminales y relativas a las zonas de estacionamiento. (Gobierno Municipal de Antonio Ante, 2014)

i) Dirección de Servicios Municipales

Consolidar y fortalecer las acciones de las diferentes secciones dentro de la municipalidad, dando valor agregado a la productividad de los mismos, encargado de dar cumplimiento a las normas, políticas, objetivos estratégicos y el aseguramiento de la calidad en los productos y servicios finales que entregan a los clientes. Entre sus funciones principales se encuentran: velar por la regularidad y continuidad de servicios públicos, garantizar la seguridad, comodidad y salubridad de los usuarios, aseguramiento y abastecimiento de agua potable, servicios de alcantarillado, entre otros. (Gobierno Municipal de Antonio Ante, 2014)

j) Recursos Humanos

Realizar actividades para armonizar el ambiente de trabajo dentro de las instalaciones, conseguir un cumplimiento optimo y oportuno de los servicios de los usuarios internos y externos, evaluar y monitorear los diferentes procesos y subprocesos de su área de trabajo, gestionar el régimen disciplinario, manejo de todos los movimientos de personal relacionados con los trámites del Seguro Social Ecuatoriano, tales como aportes, fondos de reserva, préstamos, retiros, jubilaciones, enfermedad, etc. (Gobierno Municipal de Antonio Ante, 2014)

3.2.2 SERVICIOS PRESTADOS POR EL GAD DE ANTONIO ANTE

El Gobierno Autónomo Descentralizado de Antonio Ante al ser una entidad pública brinda diferentes servicios a la ciudadanía para el desarrollo del cantón.

A continuación se enlista los diferentes servicios:

1) Administración de mercados.
2) Control de alimentos.
3) Administración de la central hidroeléctrica.
4) Saneamiento.
5) Permisos de funcionamiento para establecimientos de carácter comercial o institucional.
6) Consultorías y asesorías jurídicas.
7) Servicios de bandas libres de redes inalámbricas en lugares públicos.
8) Consultas, tramites, transacciones.
9) Pagos de impuestos.
10) Agua potable.
11) Recolección procesamiento y disposición final de desechos sólidos.
12) Pavimentación, apertura y construcción de vías, aceras y cercas.
13) Obras de alcantarillado y canalización.

3.2.3 SERVICIOS CONSUMIDOS POR EL GAD DE ANTONIO ANTE

Para el desarrollo diario de las actividades dentro del GAD de Antonio Ante es indispensable contar con los siguientes servicios, a continuación en la tabla 3.1 se puede observar el proveedor de los servicios y el número de contacto al que se puede recurrir en caso de una emergencia.

Tabla 3.1 *Servicios utilizados*

Fuente*: Información recopilada de GAD de Antonio Ante*

EMPRESA	SERVICIO	TELÉFONO
EMELNORTE	Electricidad	062-997100
Empresa Pública de Agua Potable	Agua Potable	062-906 823
IEES	Seguridad Social	062-605592
Policía Municipal	Seguridad	
Bomberos	Emergencias	911
Energy Gas	Combustible	
SINFOTECNIA	Soluciones de Redes de Comunicación y cableado estructurado	062-957127
Correos del Ecuador	Mensajería	06-2991320

3.2.4 ACTIVOS DE INFORMACIÓN

Siendo la información uno de los activos más importantes para la institución se debe contar con un adecuado almacenamiento a fin de evitar pérdidas, la información se encuentra almacenada de diferentes maneras en formato impreso, en unidades digitales y discos extraíbles en cada uno de los respectivos departamentos, y de manera global en los servidores que se encuentran en el cuarto de telecomunicaciones de la municipalidad, dentro de estos servidores se encuentran almacenados las diferentes bases de datos, ahí se almacena la información que diariamente es receptada a través de los diferentes sistemas.

En la tabla 3.2 se describe el nombre da cada una de las bases de datos, el sistema operativo con el que cuenta y el nombre del sistema de cual almacena la información.

Tabla 3.2 *Activos de Información*

Fuente: *Información recopilada del Dpto. de Sistemas del GAD de Antonio Ante*

DATOS	DESCRIPCIÓN
BBDD Contable Financiero	Microsoft Windows SQL server 2000 Sistema Contable Olympo.
BBDD Sistema de Administración Municipal	Microsoft Windows SQL server 2000 Sistema de Actividades Económicas Sistema de Recaudación y Facturación. Sistema de Control de Asistencia.
BBDD Sistema de Registro de la Propiedad	Microsoft Windows SQL server 2000 Sistema de Avalúos y Catastros Sistema de información Geográfica (SIG) Sil Antonio Ante
BBDD Agua Potable	Microsoft Windows SQL server 2000 Sistema de Agua Potable
Servidor Web	Microsoft Windows Internet Information server Sitio oficial de la municipalidad.

3.2.5 RED DE DATOS

El GAD de Antonio Ante cuenta con una red interna cableada y una inalámbrica que brinda servicio de intranet e internet a los diferentes departamentos de la institución, tiene un enlace de 5 Mbps que se distribuye a través de cada uno de los departamentos de la institución.

Tabla 3.3 *Redes de Comunicación de GAD de Antonio Ante*

Fuente*: Información recopilada del Dpto. de Sistemas del GAD de Antonio Ante*

RED	DESCRIPCIÓN
Red Local	Es la red cableada categoría 6a, es una red totalmente plana.
Red Wireless	Es la red inalámbrica corporativa, los puntos de acceso se encuentran distribuidos en diferentes espacios de la municipalidad.

La topología física de la red cableada está configurada en estrella, es decir que todas las estaciones de trabajo se encuentran conectadas en un punto central, esta topología es usada normalmente en las redes LAN, entre sus ventajas es que, si se inhabilita un una estación de trabajo el resto de la red sigue operando con normalidad, además de su fácil configuración, cuando se refiere a aumentar o quitar un estación de trabajo sin afectar al resto de equipos.

El proveedor del servicio de internet es CNT EP que suministra el servicio mediante cable de fibra óptica monomodo de 6 hilos, la red existente es de clase C, es una red totalmente plana. La Figura 3.2 Representa la topología física de la red inalámbrica del GAD de Antonio Ante

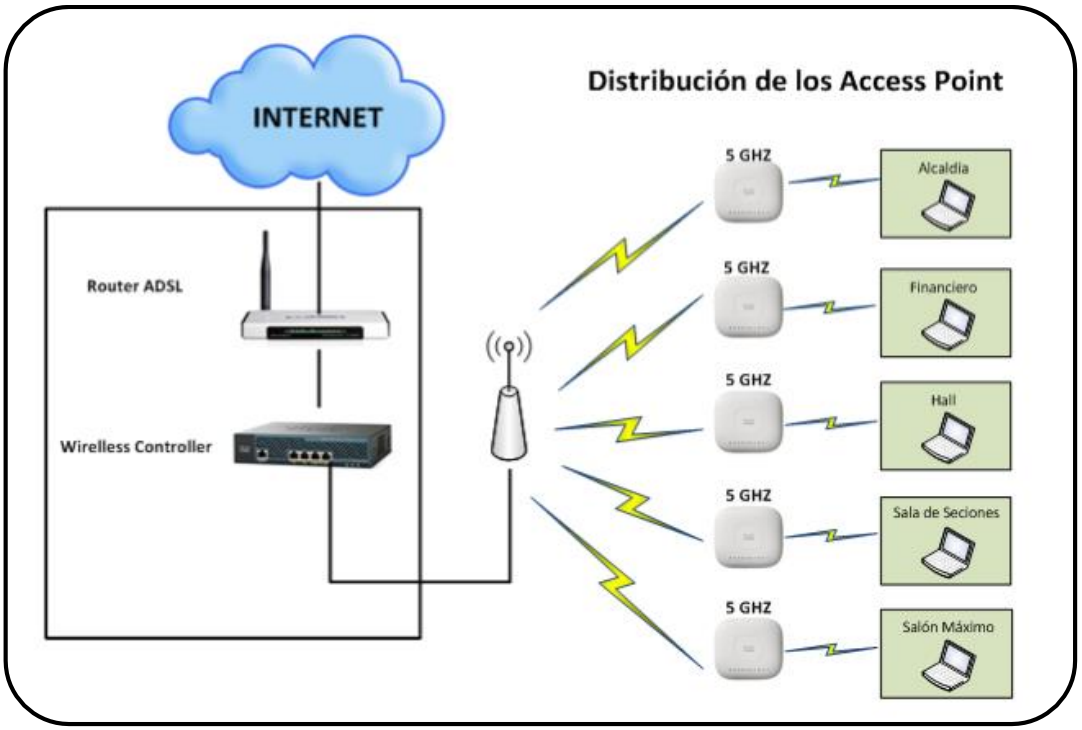


Figura 3.2 *Topología física de la red inalámbrica del GAD de Antonio Ante*

Autora: *Karina Méndez*

3.2.6 CUARTO DE TELECOMUNICACIONES

El área del Datacenter es de 3x4m^2 cuenta con un gabinete de piso para el alojamiento de los equipos de networking, un armario de servidores que aloja 5 servidores 4 tipo torre y uno tipo rack, un UPS de 6KVA no administrable, piso falso por donde se realiza la distribución de los cables de red hacia las distintas dependencias de la municipalidad, equipo de aire acondicionado, sistema de protección eléctrica, cámara de video vigilancia, sistema de seguridad física, y el sistema de iluminación. Además cuenta con una central telefónica análoga Panasonic, actualmente maneja 40 extensiones.

3.2.6.1 Descripción de los equipos de Red

Los equipos de networking que actualmente tiene la municipalidad son de gama 2 y 3 los servidores son de gama media y baja, se encuentran alojados en el cuarto de telecomunicaciones. A continuación en la tabla 3.4 se detallan los equipos que comprenden la parte activa de la red del Municipio de Antonio Ante.

Tabla 3.4. *Equipos activos de Red*

Fuente*: Información recopilada del Dpto. de Sistemas del GAD de Antonio Ante*

CANTIDAD	DESCRIPCIÓN	ESTADO
1	Router CISCO 8211	activo
2	Router Inalámbrico TP-LINK TL WR542G 54M	activo
1	Switch Gigabit de 48 puertos Cisco SGE2010	activo
1	Switch Cisco SG200-50 (SLM2048T) Gigabit 48 Puertos	activo
1	ROUTER LINKSYS BEFSR41	activo
1	Wirelless controller cisco 2500	activo
5	Antenas AIR LAP-1041ª-K9	activo
2	Quest FO-5002	activo
2	Transceiver TP LINK N/C 100 CM	activo
1	Servidor HP ML 150 2 º Generación	activo
1	Servidor HP Prolain G150 3º generación	activo
1	Servidor HP Prolain ML 150 6º generación	activo
1	Servidor HP Prolain DL380E 8º generación	activo

- **ROUTER INALÁMBRICO TP-LINK TL WR542G 54M**

- La velocidad de transmisión de 54Mbps
- Adopta la tecnología de rango extendido 2x a 3x para mayor cobertura inalámbrica
- Frecuencia de operación de 2.4-2.4835GHz
- Puente WDS inalámbrico
- Seguridad inalámbrica 64/128/152-bit WEP/WPA/WPA2, WPA-PSK/WPA2-PSK
- IPQoS asegura la utilización óptima del ancho de banda
- Es compatible con PPPoE, IP dinámica, IP estática, L2TP, PPTP y acceso a Internet por cable BigPond
- Firewall integrado, soporta direcciones IP/MAC y filtrado en el dominio para controlar el acceso de red determinada.

- **SWITCH GIGABIT DE 48 PUERTOS CISCO SGE2010**

- Cuarenta y ocho puertos Ethernet 10/100/1000
- Capacidad de conmutación de almacenamiento y de 96 Gbps sin bloqueos
- Gestión de QoS simplificada utilizando DiffServ o tipo de servicio ToS compatibles con 802.1p
- ACL para ofrecer seguridad granular e implementación de QoS
- Gestión remota segura del switch mediante cifrado SSH y SSL
- Las VLAN basadas en 802.1Q para la segmentación de redes
- Seguridad a nivel de puerto de usuario / red mediante autenticación 802.1X y filtrado basado en MAC
- Aumento del ancho de banda y redundancia de enlace con el protocolo de control de adición de enlace LACP
- Compatible con el protocolo de gestión de red simple SNMP

- **SWITCH CISCO SG200-50 (SLM2048T) GIGABIT 48 PUERTOS**

- Switch capa 2
- Algoritmo de seguridad: 802.1x RADIUS, MD5, MAC, filtro de direcciones
- Protocolos de gestión: IGMPv1/2
- Protocolos de red admitidos: IPv4/IPv6, HTTP, SNTP, TFTP, DNS, ICMP
- Soporta VLAN 256
- Tecnología de cableado: 10/100/1000 Base-T(X)
- QoS integrada para dar prioridad al tráfico sensible a demoras
- Seguridad de red integrada de puertos IEEE 802.1X
- Proporciona seguridad automatizada y configuración de puertos con QoS
- Tasa de transferencia (máx): 1 Gbit/s
- Capacidad de conmutación: 100 Gbit/s

- **ROUTER LINKSYS BEFSR41**

- Un puerto 10/100 RJ-45 para módem de banda ancha
- Cuatro: Puertos conmutados 10/100 RJ-45
- Protocolos de red: TCP/IP
- Compatible con el sistema Universal Plug-and-Play para una configuración más sencilla
- Priorización QoS en función del puerto o el tipo de servicio
- Admite el paso a través PPTP e IPSec
- Posibilidad de administrar y actualizar el router de forma remota en Internet
- Se puede configurar como servidor DHCP de la red
- Funciones avanzadas de administración de seguridad para filtrado de puertos, filtrado de direcciones MAC y asignación de DMZ

- **WIRELESS CONTROLLER CISCO 2500**

- Cuatro puertos Gigabit Ethernet
- Un puerto de consola
- Conexión inalámbrica de normas: IEEE 802.11a, 802.11b, 802.11g, 802.11d, 802.11h, 802.11n
- Diseñado para su uso con el sistema de control inalámbrico
- Web-based: HTTP / HTTPS administrador de dispositivos individuales
- Interfaz de línea: Telnet, SSH, puerto serial
- Gestión centralizada: permite a los administradores de red gestionar las políticas de seguridad del sistema
- Escalabilidad: El controlador soporta hasta 500 clientes y un máximo de 50 puntos de acceso a través de actualizaciones de licencia sumador

- **ANTENAS AIR LAP-1041-K9**

- Con la tecnología 2x2 múltiple entrada múltiple salida MIMO
- Conexiones inalámbricas seguras y fiables.
- Gestión de recursos radio.
- BandSelect mejora las conexiones de cliente 5-GHz en entornos clientes mixtos
- VideoStream
- Ofrece un rendimiento 802.11n con estándar 802.3af Power over Ethernet

- **TRANSCEIVER TP LINK N/C 100 CM**

- Cumple con 802.3u 10 / 100Base-TX, estándares 100Base-FX
- Enlace Fault Passthrough y Far End Fault minimizan la pérdida causada por falla en el enlace oportuna
- Proporciona configuración del switch de modo de transferencia Half-Duplex / Full-Duplex para el puerto FX
- Amplía la distancia de fibra de hasta 2km

- **SERVIDOR HP ML150 2º GENERACIÓN**

ÍTEM	CARACTERÍSTICA
Procesador	1 Procesador Pentium
Memoria	2 GB de RAM
Disco Duro	Disco interno de 300 GB
Sistema Operativo	Windows server

- **SERVIDOR HP PROLIANT G150 3º GENERACIÓN**

ÍTEM	CARACTERÍSTICA
Procesador	1 Procesador Intel 1.6 Ghz
Memoria	4GB de RAM
Disco Duro	Disco interno de 160 GB
Sistema Operativo	Windows server

- **SERVIDOR HP ML150 6º GENERACIÓN**

ÍTEM	CARACTERÍSTICA
Procesador	1 Procesador Intel Celeron2.6 Ghz
Memoria	2GB de RAM
Disco Duro	Disco interno de 75 GB
Sistema Operativo	Windows server

- **SERVIDOR HP PROLIANT DL380E 8º GENERACIÓN**

ÍTEM	CARACTERÍSTICA
Procesador	1 Procesador Intel 2.2 Ghz
Memoria	54 GB de RAM
Disco Duro	Disco interno de 3 TB
Sistema Operativo	Windows server

3.2.7 ACTIVOS SOFTWARE

A continuación en la siguiente tabla 3.5 se describe el tipo de software que es usado en los diferentes departamentos de acuerdo a las funciones que se desempeñan, la mayoría del software utilizado se encuentra licenciado o a su vez son aplicaciones realizadas por el Departamento de Sistemas y Tecnología de la municipalidad de acuerdo a los requerimientos presentados por los usuarios.

Tabla 3.5. *Activos Software*

Fuente: *Información recopilada del Dpto. de Sistemas del GAD de Antonio Ante*

APLICACIÓN	DESCRIPCIÓN
Antivirus	Eset Smart Security 4
Microsoft Windows Professional	Equipos licenciados
Microsoft Office	Equipos con licencia
ArcGIS, gvSIG	Licenciado
Visual Studio .NET	Licenciado
NetBeans IDE 6.9.1	Versión gratuita
Developer Express, SQL Server 7	
Autocad	
Adobe Pothoshop CS4/CS6	
Firefox	

3.2.8 ACTIVOS HARDWARE

En los departamentos del GAD de Antonio Ante se encuentran distribuido el siguiente equipamiento de activos físicos con respecto a tecnología, en la tabla 3.6 se muestra el equipamiento tecnológico de acuerdo a cada departamento.

***Tabla 3.6**. Activos Hardware*

***Fuente:** Información recopilada del Dpto. de Sistemas del GAD de Antonio Ante*

DEPARTAMENTO	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
Recaudación	5	HP Pro 3130 MT Intel Core i3 HP Pro 3130 MT Intel Core i3 CPU ATX P4 Intel Pentium 4 CPU ATX P4 Intel Core 2 Duo E7500 CPU ATX P4 Intel Pentium 4	4 Epson FX-890 UPS Marca CDP UPR505120VAC UPS TrippLite
Rentas	1	CPU ATX P4 Intel Core 2 Duo	Epson FX-890 UPS CDP
Turismo cultura y deportes	1	Vostro 3460 Intel Core i7 Modelo 3612QM a 2.10 Ghz 6 Mb Caché L3	Samsung ML-2240 Samsung SCX-4828FN Notebook Computer Look Taurus
Recursos humanos	3	HP Compaq 6000 Pro Micro Tower Intel Core 2 Quad HP Compaq 6200 Pro MT Procesador Intel Core i7-2600/ 8 Mb Caché L3 CPU ATX P4 Intel Core 2 Quad	HP Laser Jet Pro 400 Color MFP UPS TrippLite Interactive Office
Registro de la propiedad	1 8	Inspiron N4110 Intel Core i5- 2410M HP Compaq 6200 Pro MT Procesador Intel Core i7-2600/ 8 Mb Caché L3	Epson LX-300+II UPS CDP Samsung ML-1610 Regulador TDE ProNet Samsung ML-2240 UPS THOR Voltage Regulator Lexmark X466
Comisaria municipal	2	HP Compaq 6200 Pro MT Procesador Intel Core i7-2600 / 8 Mb Caché L3 Dell Inspiron 600M Pentium M	Samsung ML-1610
Patronato	1	Dell Vostro 3460 Intel Core i7 Modelo 3612QM a 2.10 Ghz 6 Mb Caché L3	Notebook Computer Look Taurus
Dirección de participación ciudadana	2	ProBook 4420S XL370LT#AC8 Intel Core i3 M370 CPU Clon ATX P4 Intel Pentium 4	Notebook Computer Look Taurus HP Desjket 3940 Regulador TrippLite

DEPARTAMENTO	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
Gestión de desarrollo	3	HP Compaq 6200 Pro MT Procesador Intel Core i7-2600/ 8 Mb Caché L3 CPU Clon ATX P4 Intel Pentium 4 CPU Clon SP Intel Core 2Quad Q8400	HP DeskJet F2280 Copiadora/Impresora Xerox Workcentre 5020 Regulador Tripp Lite Samsung ML− 2010
Coordinador de proyectos	1	Pro Book 4420S XL370LT#AC8 Intel Core i3 M370	
Fiscalización	4	Dell Inspiron N4010 14" Intel Core i5 M480 Clon ATX P4 Intel Pentium 4 CPU ATX P4 Intel Core 2 Duo 6550	Samsung CLP-610ND Láser HP Laser Jet Pro 400 Color MFP Samsung ML1610 Regulador CDP
Sistemas y tecnologías	4	Dell Inspiron N4010 14" Intel Core i5 480 Clon ATX P4 Intel Core 2 Quad Q9550 Clon ATX P4 Intel Pentium 4 HP Compaq 6200 Pro MT Procesador Intel Core i7-2600 / 8 Mb Caché L3	Regulador Tripp Lite Cortapicos Color Blanco Samsung ML-2010 2 UPS Tripp Lite Smart 1000 LCD
	2	HP Compaq 6000 Pro Microtower Intel Core 2 Quad Q9550	
UGA	4	Dell Inspiron N4010 Intel Core i5 Optiplex 745Intel Pentium D Optiplex 745 Intel Pentium D Clon ATX P4 Intel Pentium 4	Samsung ML-2010 HP Deskjet 1280 HP Lasér Jet 3055 3 UPS Tripp Lite
Bodega	2	HP Compaq 6200 Pro MT Procesador Intel Core i7-2600/8 Mb Caché L3 Acer Aspire 56102556 Genuine Intel	Samsung ML-1610 Epson LX-300+ II Samsung SCX- 4521F Zebra TLP 2844 Regulador Tripp Lite
Dirección de planificación	2	Pavilion 14 Notebook PC Intel Core i7 Modelo 4702MQ Inspiron N4010 14R Intel Core i5 M480	Samsung ML1740 Samsung ML-2010 Switch Encore de Sistema Samsung ML-2010
Planificación	8	HP Compaq 6000 Pro Microtower Intel Core 2Quad Q9550 HP Compaq 6200 Pro MT Procesador Intel Core i7-2600/ 8 Mb	Regulador Samsung ML-2165 Regulador ALTEK Samsung ML− 2240

DEPARTAMENTO	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
		Caché L3 CPU ATX P4 Intel Core 2 Duo E6550 HP Compaq 6000 Pro Microtower Intel Core 2Quad Q 550 CPU ATX P4 Intel Pentium 4 HP Compaq 6200 Pro MT Procesador Intel Core i7-2600/ 8 Mb Caché L3 Clon ATX P4 Intel Core 2 Duo E6750 CPU ATX P4 Intel Pentium 4	Plotter HP DesignJet 500 Samsung ML− 1665 4 Regulador Tripp Lite UPS TRIPP
Planificación y urbanismo	1	Tecra A11- SP5003L Intel Core i5 M450	Samsung ML-1610 Lexmark X464de FCC Regulador TrippLite
Avalúos y catastros	6	Clon ATX P4 Intel Core i7 870 Toshiba Tecra A11-SP5003L Intel Core i5 M450 HP Compaq 6000 Pro Microtower Intel Core 2 Quad Q9550 HP Compaq 6000 Pro Microtower Intel Core 2 Quad Q9550 Clon ATX P4 Intel Core i7 870 CPU ATX P4 Intel Core 2 Quad Q9550	2 Epson FX-890 Samsung ML 2010 Ploter HP DesingJet 130 Samsung SCX-4828FN 3 Regulador UPS Forza
Secretaria general	2	ProBook 4420S XL370LT# AC8 Intel Core i3 M370 CPU ATX P4 Intel Pentium Dual Core E2180	Samsung Modelo CLP-620ND Epson FX-890 Samsung SCX-4521F
Archivo	1	CPU ATX P4 Pentium 4	Epson FX-890
Asesoría de imagen	3	CPU ATX P4 Intel Core 2 Quad Touch Smart tx2 Notebook PCtx2-380LA AMD Turion x2 Dual Core Mobile RM-77 Mac Book Pro6.2 Intel Core i7	Samsung ML− 1740 HP Office Jet Pro K8600 Regulador Modelo: AVR 1500N
Auditoria	2	Probook 4410s Intel Core 2 Duo T6670 Clon ATX P4 Intel Core 2 Duo E7500	Samsung SCX-4300 UPS Thor 600
Compras publicas	3	Dell Inspiron 3420 Intel Core i3 Modelo 3110M a 2.40 Ghz CPU ATX P4 Intel Core 2 Duo E6550 HP 435AMD E-300 APU HD Graphic	Lexmark X466de S/N: 35P88DX

DEPARTAMENTO	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
Servicios públicos	7	Toshiba Tecra A11-SP5003L Intel Core i5 M450 HP Compaq 6000 Pro Microtower Intel Pentium Dual Core E5500 CPU ATX P4 Intel Pentium 4 Dell Inspiron 410 Intel Core i5 Apex Intel Pentium 4 CPU ATX P4 Intel Core 2Quad Q9550 CPU ATX P4 Intel Pentium 4	Toshiba E-Studio 232 HP Laser Jet Pro 400 Color MFP Samsung ML-2010 HP Color LaserJet 2600n Lexmark X466de Samsung ML− 1740 HP Deskjet 9800 UPS TRIPP LITE Switch Dlink 8 Puertos
Asesoría jurídica	5	HP Pro 3130Intel Core i3 550 HP Compaq 2230S Intel Core 2 Duo Dell Vostro 3460 Intel Core i7 Modelo 3612QM a 2.10 Ghz 6 Mb Caché L3 HP Compaq 6200 Pro MT Procesador Intel Core i7-2600/ 8 Mb Caché L3 CPU ATX P4 Intel Core 2 Duo	Samsung ML-2010 Mono Laser Notebook Computer Look Taurus Lexmark X466d 2 Regulador
Dirección administrativa y financiera	1	Dell Latitude E6430 Intel Core i7 Modelo 3520M	Epson FX-890 Samsung SCX-4828FN
Dirección administrativa	3	HP Compaq 6200 Pro MT Procesador Intel Core i7-2600/8 Mb Caché L3 CPU ATX P4 Intel Core 2 Duo E7500 HP Compaq 6000 Pro Microtower Intel Dual Core E5500	Samsung Láser Color C6220 UPS Forza Lexmark X464 Regulador CDP
Tesorería	3	Probook 4410S Intel Core 2 Duo T6670 Toshiba Tecra A11- SP5003L Intel Core i5 M450 CPU ATX P4 Intel Pentium 4	Samsung SCX-4300 UPS TrippLite
contabilidad	4	HP Compaq 6000 Pro Microtower Intel Core 2QUAD Q9550 Clon ATX P4 Intel Core 2 Duo E6550 HP Compaq 6000 Pro Microtower Intel Core 2QUAD Q9550 HP Compaq 6000 Pro Microtower	HP LáserJet P2035 Epson FX-890 Lexmark X466de Regulador Apex 1200M Switch TrendNET 8 Puertos Samsung SCX-4521F

DEPARTAMENTO	CPU	DESCRIPCIÓN	OTROS DISPOSITIVOS
Empresa de agua potable	5	Intel Core 2Quad Q9550 Pavilion DV4-1525LA Intel Core 2 Duo T6600 Clon ATX P4 Intel Pentium 4 Dell Inspiron N401014R Intel Core i5 M480 HP Compaq 6000 Pro Microtower Intel Core 2 Quad Q9550 HP Compaq 6000 Pro Microtower Intel Core 2 Quad Q9550	Samsung ML-1740 HUB Usb Omega 4 Puertos UPS TrippLite LS606X Epson FX-890 Samsung SCX-4828FN

3.2.9 SERVICIOS DEL DEPARTAMENTO INFORMÁTICO

Los servicios que brinda el departamento de Sistemas y Tecnología del GAD de Antonio ante son:

- Soporte de las aplicaciones de Software.
- Mantenimiento correctivo de los equipos de computación
- Soporte por fallas de conexión a internet
- Soporte en la red inalámbrica y la red Lan.

3.2.10 PERSONAL

Dentro del Departamento de Sistemas se encuentran trabajando 5 personas, en la tabla 3.7 se muestra el cargo y las funciones que realizan diariamente.

Tabla 3.7. *Personal de la unidad de sistemas y Tecnología del GAD de Antonio Ante*

Fuente*: Información recopilada del Dpto. de Sistemas del GAD de Antonio Ante*

CARGO	ENCARGADO	DESCRIPCIÓN
Jefe del departamento de Sistemas	Ing. Francisco Arteaga	Es el encargado de supervisar el correcto funcionamiento de todos los procesos
Analista de Sistemas	Tecnóloga Nuvia Guevara	Responsable del sitio web, administración del sistema Olympo, sistema de RRHH, y realizar los respectivos respaldos de las BBDD.
Asistente de Sistemas	Técnico Javier Suárez	Mantenimiento de equipos Soporte a Usuarios
Programadores	Ing. David Bargas Ing. Diego Michilena	Desarrollo de Software.

3.3 EVALUACIÓN DE RIESGOS Y ESCENARIOS DE CONTINGENCIA

En lo últimos años la municipalidad de Antonio Ante ha ido aumentando el número de usuarios y servicios que brinda a la ciudadanía, este crecimiento ha dado como resultado la ampliación de la infraestructura tecnología y con ello a la implementación de nuevas medidas de protección para la información; por tanto se procede a realizar un análisis de riesgos y amenazas para desarrollar un plan de contingencia informático que permita mitigar los posibles riesgos potenciales que afecten las actividades de la institución.

Tomando como referencia la NTC-ISO 27005, en conjunta concordancia con el jefe del departamento de Sistemas de la municipalidad de Antonio Ante y de acuerdo a las actividades de la institución se obtiene los siguientes criterios para la evaluación de los riesgos:

1. Evaluación de los activos disponibilidad, confidencialidad e integridad de las operaciones.
2. Evaluación de las amenazas
3. Evaluación de las vulnerabilidades
4. Los activos que se verían afectados con la interrupción de este proceso.

3.3.1 EVALUACIÓN DE LOS ACTIVOS EN EL GAD DE ANTONIO ANTE

El análisis de los activos se realizará en base a tres aspectos como son: Disponibilidad (D), Integridad (I), Confidencialidad (C). No todos los activos están sujetos a la evaluación bajo estos criterios, en este caso si no cumple con algún aspecto tiene valor nulo y se representa mediante un guion medio (-)

La determinación del valor de cada uno de los activos en la tabla 3.8 se realizó de acuerdo a las consideraciones de la tabla 2.2 (*Valoración de activos)*, donde se explica cada una de las denominaciones y los criterios que se tomaran en consideración para su respectiva valoración.

Tabla 3.8. *Valoración de los activos del GAD de Antonio Ante*

Fuente: *Información recopilada del Dpto. de Sistemas del GAD de Antonio Ante*

CANT.	DESCRIPCIÓN	V. PROPIO			V. ACUMULADO
		D	I	C	
1	BBDD Contable Financiero	4	-	-	4
1	BBDD Sistema de Administración Municipal	4	-	-	4
1	BBDD Sistema de Registro de la Propiedad	4	-	-	4
1	BBDD Agua Potable	4	-	-	4
1	Servidor Web	1	-	-	1

CANT.	DESCRIPCIÓN	V. PROPIO			V. ACUMULADO
1	Sistema de Actividades Económicas	2	2	2	2
1	Sistema de Recaudación y Facturación	4	3	-	3.5
1	Sistema de Avalúos y Catastros	3	3	-	3
1	Router CISCO 8211	4	-	-	4
2	Router Inalámbrico TP-LINK TL WR542G	4	-	-	4
1	Switch Gigabit de 48 puertos Cisco SGE2010	4	-	-	4
1	Switch Cisco SG200-50 SLM2048T	4	-	-	4
1	ROUTER LINKSYS BEFSR41	4	-	-	4
1	Wirelless controller cisco 2500	4	-	-	4
5	Antenas AIR LAP-1041ª-K9	3	-	-	3
5	servidores	4	-	-	4
53	Computadores de escritorios completos	3	-	-	3
1	Ups central	4	-	-	4
60	Impresoras	1	-	-	1
	Infraestructura de red	4	-	-	4

Los resultados arrojados por las encuestas y de acuerdo con la valoración de los activos de mayor importancia para el municipio dieron como resultado lo siguiente:

1) La información que se encuentra almacenada en las diferentes bases de datos.
2) Los sistemas de Recaudación, facturación, Avalúos y Catastros fueron determinados de mayor importancia pues son los que aportan ingresos económicos al municipio, además si llegaran a fallar producirían perdidas de información y reputación, pues al ser el municipio una entidad que brinda servicios a la colectividad la suspensión de estas actividades provocaría disconformidad.

3) Servidores: contable financiero, administración municipal, archivos, correo y web son donde se encuentra almacenada toda la información y los sistemas que ayudan al desempeño de las actividades.
4) El sistema de cableado estructurado categoría 6ª que conecta todos los departamentos del municipio.
5) El Data Center junto con sus instalaciones eléctricas, protecciones y sistemas de respaldo de energía, aire acondicionado, sistema de control de acceso, sistemas de alertas contra incendio.
6) El equipamiento de networking que se encuentra en el Data Center.
7) Los CPU de los usuarios finales.

3.3.2 EVALUACIÓN DE LAS AMENAZAS

La evaluación de las amenazas se realiza mediante el análisis de las vulnerabilidades en los activos críticos, para la definición de la probabilidad de ocurrencia se hace referencia a la tabla 2.3; los criterios de evaluación a considerar son:

- La importancia del activo para la organización.
- La facilidad de explotación de una vulnerabilidad del activo.
- La susceptibilidad técnica de la vulnerabilidad a la explotación.

Tabla 3.9*. Evaluación de las Amenazas a activos del GAD de Antonio Ante*

Fuente*: Información recopilada del Dpto. de Sistemas del GAD de Antonio Ante*

Nro.	AMENAZA	ACTIVO	VULNERABILIDAD	PROBABILIDAD
1	Terremotos /Interrupción de servicios	Cuarto de telecomunicaciones	La toda información se encuentra almacenada en un mismo lugar	Remoto
2	Incendio /Interrupción de servicios		Sobrecargas en el sistema eléctrico	Remoto
3	Fallas en		No se tiene definido	Ocasional

Nro.	AMENAZA	ACTIVO	VULNERABILIDAD	PROBABILIDAD
	hardware		periodos de limpieza	
4	Cortes de energía eléctrica	Equipos de Networking	Variaciones de voltaje	Frecuente
5	Humedad /interrupción de servicios		Falta mantenimiento de equipos de enfriamiento	Ocasional
6	Desgaste /daños físicos		Equipos con muchos años de servicio	Ocasional
7	Interrupción de servicios	Servidores	Ineficiente conexión de los cables de red	Ocasional
8	Espionaje remoto		Problemas de transferencia de contraseñas sin autorización	Ocasional
9	Fallas de software		Errores de compilación	Frecuente
10	Software maliciosos (virus)		Trafico sensible sin protección	Muy Frecuente
11	Interrupción de servicios		Personas mal intencionadas Ataques	Frecuente
12	Fallas de energía	PC	Daños en el sistema de alimentación del equipo	Frecuente
13	Fallas en el hardware		Falta de mantenimiento en los equipos	Muy Frecuente
14	Fallas en el software		Insuficiencias de pruebas en el software	Ocasional
15	Fallas en el software		Utilización de errónea de aplicaciones de software	Frecuente
16	Códigos maliciosos		Descarga y uso no controlado de software	Frecuente
17	Errores físicos	Red de Datos	La infraestructura de red de cat 5e no cumple con las normas y estándares de SCE	Ocasional
18	Ataques a los principales servicios		No existe segmentación de la red	Frecuente
19	Presencia de			

Nro.	AMENAZA	ACTIVO	VULNERABILIDAD	PROBABILIDAD
	interferencias electromagnéticas		Fallas en el diseño de red	Frecuente
20	Interceptación de información		falta de pruebas del envió o la recepción de mensajes	Frecuente
21	Interceptación de información		Las líneas de comunicación sin protección	Frecuente
22	Modificación o alteración de la información		Él envió de tráfico sensible a través de la red es inseguro	Frecuente
23	Cumplimiento parcial objetivos del departamento	Estructura organizacional	Falta de personal en el departamento informático	Muy Frecuente
24	Abuso de derechos		Falta de monitoreo de los recursos de procesamiento de la red	Frecuente
25	Negación de servicios		Faltan procedimientos de identificación y evaluación de riesgos.	Frecuente
26	Interrupción de servicios		Falta de planes de continuidad	Frecuente
27	Descuido mal uso del servicio		Falta políticas sobre el uso de correo electrónico	Frecuente
28	Negación de servicios	Información	Saturación de las BBDD	Ocasional
29	Modificación o alteración de información		Errores de duplicidad	Frecuente
30	Ingeniería social		Falta de cultura de la seguridad de la información	Frecuente
31	Accesos no autorizados		Falta de controles para la habilitación de servicios	Muy Frecuente
32	Suplantación de identidad	Software	Falta de mecanismos de identificación y autentificación de usuario	Muy Frecuente

3.3.3 MATRIZ DE CONTINGENCIA

En la tabla 3.10 se observa la evaluación de los activos físicos tecnológicos, para la obtención del porcentaje del riesgo los cálculos se adjuntan en el anexo D, en la categorización de cada uno de los posibles eventos a materializarse se utiliza la siguiente nomenclatura: (NC) para eventos no controlables y (C) para eventos controlados.

Tabla 3.10. *Evaluación de las Amenazas a activos físicos*

Fuente*: Información recopilada del Dpto. de Sistemas del GAD de Antonio Ante*

Nro.	Amenaza	Probabilidad	Impacto	Riesgo %	Alerta	Categoría
Activo :Centro de Datos						
1	Terremotos/Interrupción de servicios	1	4	16		NC
2	Incendio/Interrupción de servicios	1	4	16		NC
3	Fallas en hardware	2	4	32		C
26	Daños físicos en el UPS central	1	3	12		NC
Activo: Equipos de Almacenamiento (servidores)						
7	Ineficiente conexión de los cables de red	2	3	24		C
8	Espionaje remoto	2	3	24		NC
9	Fallas de software	3	3	36		C
10	Software maliciosos (virus)	4	4	64		C
11	Personas mal intencionadas	2	3	24		C
Activo: PCs. Hardware y Software						
13	Fallas en el hardware	4	2	24		C
14	Fallas en el software	2	1	6		C

Nro.	Amenaza	Probabilidad	Impacto	Riesgo %	Alerta	Categoría
15	Utilización errónea de aplicaciones	3	1	9		C
16	Códigos maliciosos	3	2	18		C
23	Suplantación de identidad	4	2	18,67		C
24	Descuido o mal uso del servicio(correo electrónico)	3	1	3		C
25	Daños físicos en dispositivos de multimedia	2	1	2		C
Activo: Red de datos						
17	Errores físicos	2	3	24		C
18	Presencia de interferencias electromagnéticas	3	1	12		C
19	Interceptación de información	3	3	36		C
5	Equipos Networking Humedad/interrupción de servicios	2	3	24		C
6	Equipos Networking Desgaste/daños físicos	2	3	24		NC
	Accesos no autorizados	3	4	48		
Activo: Información						
20	Modificación o alteración de información	3	3	36		C
21	Ingeniería social	3	2	24		C
22	Accesos no autorizados	4	2	32		C

3.4 IDENTIFICACIÓN DE CONTROLES PREVENTIVOS

Como parte fundamental de esta fase es necesario realizar la asignación de roles y responsabilidades que deben cumplir cada uno de los miembros del departamento de informática en caso de presentarse una emergencia.

3.4.1 Propuesta del Orgánico Estructural para el Departamento de Sistemas y Tecnología del GAD de Antonio Ante.

Los trabajos realizados por el personal del Departamento Informático son de gran importancia para el desarrollo de las actividades del municipio, exigiendo una alta preparación técnica para cada uno de sus cargos. Entre sus objetivos principales son la implantación de nuevos sistemas de información, mantenimiento de los diferentes aplicativos de software existentes, controles de calidad, programación, soporte en redes, asistencia técnica a los usuarios, obtención de respaldos de información y sistemas, elaboración de manuales de procesos y procedimientos, implementación de nuevas tecnologías.

Actualmente el Departamento Informático cuenta con cinco miembros para brindar soporte a las diferentes dependencias del municipio, se propone la contratación de tres personas adicionales, debido a que el equipo de trabajo es insuficiente y tomando en consideración el crecimiento de la municipalidad se propone el siguiente orgánico a fin de mejorar el trabajo en equipo. En el diagrama 3.1 se observa los respectivos cargos y responsabilidades que deberían cumplir cada uno de los miembros del departamento.

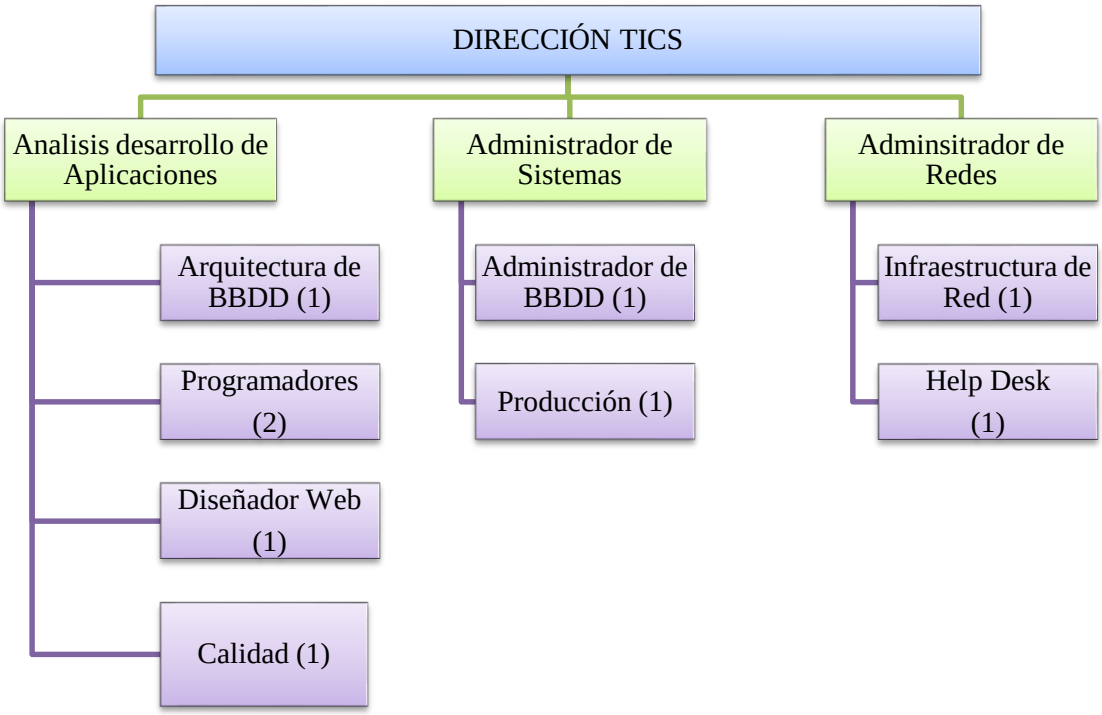


Diagrama 3.1 *Estructura organizacional de IT*

Autor*: Karina Méndez*

De acuerdo con el orgánico propuesto a continuación se describe las responsabilidades que tendrá cada cargo.

a) Dirección TICS

El responsable del área deberá estar en la capacidad de identificar las necesidades de la institución y del departamento, establecer planes de gestión y monitoreo de los recursos de IT, definir estructuras internas, establecer metas, definir políticas y procedimientos de operación junto con el resto del equipo y promover el entrenamiento constante del talento humano.

b) Análisis Desarrollo y Aplicaciones

Aquí se realizan todos los programas e implementaciones que solicitan los usuarios, también se realiza el mejoramiento de las diferentes bases de datos; el personal debe estar capacitado en las siguientes áreas:

- **Arquitectura de BBDD:** Es el encargado del diseño de estrategias para los sistemas de base de datos, la integración de los nuevos sistemas implementados con las estructuras de almacenamiento ya existentes en la organización mejorando el desempeño del sistema.

- **Programadores:** Cumplen con funciones como: depurar, mantener y mejorar el código fuente de los programas dentro de la institución, también son los encargados del desarrollo de software de acuerdo a las necesidades de la organización.

- **Diseñador Web:** El encargado de mantener, crear y mejorar las web de la institución para que estén actualizadas.

- **Calidad**: Encargado de revisar que los diferentes aplicativos de software funcionen de acuerdo a las necesidades de los usuarios.

c) Administrador de Sistemas

El encargado de esta sub área debe realizar actividades como: implementar controles que permitan garantizar que el software desarrollado de calidad, brindar soluciones a las necesidades de los usuarios a través creación de nuevo software que faciliten el trabajo de los usuarios.

- **Administrador de las BBDD:** Debe realizar el mantenimiento de las BBDD, las respectivas copias de seguridad de todos los sistemas y datos que se almacenan diariamente, consultas, reportes, respaldos de integridad.

- **Producción:** Encargado de la instalación de los sistemas principales, y aplicativos de software necesarios para mantener el acceso a la información.

d) Administrador Redes

- **Infraestructura de red:** Entre las funciones que debe desempeñar se tiene: mantenimiento y monitoreo de los equipos de networking, mantenimiento del sistema de cableado estructurado, asignación de direcciones IP, configuraciones de protocolos de ruteo, configuración de autentificación y autorización de servicios a los usuarios, asegurarse que la red sea usada eficientemente.

- **Help Desk**: Se encarga de brindar soporte a los usuarios tanto a nivel físico lógico reduciendo significativamente tiempos y recursos, realizar un registro de control y mantener la documentación actualizada del soporte técnico ofrecido.

3.4.2 FORMACIÓN DE GRUPOS Y ASIGNACIÓN DE ROLES EN CASO DE UNA CONTINGENCIA

Para la formación de grupos en caso de presentarse una contingencia debe contar con un coordinador principal quien será el encargado de reportar de manera diaria el avance de la recuperación y en caso de ser necesario reportar de manera inmediata al jefe a cargo de plan de contingencias general.

La recuperación se realizará en dos etapas la primera la restauración del servicio usando los recursos del área alternativa de respaldo, o haciendo uso de los recursos y lugares propios del sistema de información, siendo la solución más rápida y eficiente para no perjudicar el buen servicio y la imagen institucional.

En la tabla 3.11 se describe los roles y las responsabilidades a desarrollar por los miembros del grupo en caso de una emergencia. (Plan de Contingencia Sistemas Informaticos)

Tabla 3.11 *Asignación de roles y responsabilidades en caso de una contingencia*

Autor: *Karina Méndez*

ROLES	PUESTO	RESPONSABILIDADES
Coordinador principal	Director TICS	Verificar que se realizan reuniones periódicas para la actualización del plan o realización de pruebas.
		Encargado de tomar las decisiones importantes en caso de emergencias.
		Coordinar las etapas para la ejecución del plan de contingencia.
		Llevar un registro de las reuniones que se realizan para evaluar los procesos críticos y el tipo de evento.
		Responsable de dar por concluida la declaración de contingencia
Coordinador de Redes y comunicaciones	Administrador de Red	Responsable de los procedimientos en caso de que la contingencia afecte a las comunicaciones, servicios de internet, correo electrónico, red cableada, daños en los equipos de networking
		Mantener un inventario actualizado de los equipos de telecomunicaciones.
		Llevar a cabo pruebas de operatividad en caso de que se produzca la interrupción parcial o total de los servicios.
		Mantener una lista actualizada de proveedores y usuarios de los servicios.
Coordinador de sistemas	Administrador de Sistemas	Responsable de determinar los sistemas críticos
		Realización de pruebas cuando se realiza una nueva configuración de sistemas
		Mantener actualizados los manuales técnicos y de usuario.

ROLES	PUESTO	RESPONSABILIDADES
Coordinador de respaldos	Administrador de BBDD	Encargado mantener las copias de seguridad actualizadas.
		Mantener seguras las copias de respaldo en una ubicación externa.
Coordinador de soporte técnico	Help Desk	Llevar un inventario de los Pcs, software, impresoras, faxes, etc.
		Determinar las características necesarias de los equipos para dar continuidad a las operaciones.
		Coordinar con los usuarios la realización de respaldos de información.
		Mantener actualizado el directorio de proveedores de equipos, garantías, servicio de mantenimiento
		Responsable de restablecer el servicio a la brevedad posibles sea cual sea el daño en los equipos

3.4.3 PRIORIZACIÓN DE RECURSOS TECNOLÓGICOS

Luego de identificar los riesgos de seguridad en la matriz de contingencia se procede a la identificación de los requerimientos necesarios para mejorar la seguridad de la información en cada uno de los activos, en la tabla 3.12 se determina el activo y los requerimientos de seguridad.

Tabla 3.12. *Requerimientos de Seguridad*

Autora: *Karina Méndez*

ACTIVO	REQUERIMIENTOS
Información	Este activo se encuentra conformado por datos de las siguientes bases de datos: contable, administración municipal, agua potable, registro de la propiedad y es considerado uno de los más importantes para el desarrollo de las actividades municipales por lo que es fundamental que se encuentre siempre disponible. Debe tener procedimientos para la realizaciones copias de seguridad de los datos. Las copias de seguridad deben estar almacenadas en oficinas externas al edificio principal.
Software	Para el municipio de Antonio Ante se considera como críticos los siguientes sistemas: recaudación, financiero contable, facturación, avalúos y catastros. • Siempre deben mantenerse en funcionamiento • Deben contar con procedimientos de contingencias • Funcionan de manera conjunta con el hardware y el software. • Solo el personal autorizado debe tener acceso a estos sistemas. • Los datos que son ingresados a través de estos sistemas deben ser íntegros.
Servidores	Estos dispositivos de almacenamiento contienen información y sistemas de gran importancia para el municipio por lo que deben mantenerse siempre activos y disponibles. • Deben contar con un proceso de autentificación de usuarios. • Políticas de perfiles de usuarios. • La información almacenada en estos dispositivos únicamente debe ser vista o modificada únicamente por el personal autorizado y debe permanecer completa y exacta. • Debe contar con procedimientos para la recuperación de respaldos de la información residente en los servidores.

ACTIVO	REQUERIMIENTOS
Red de datos	• Debe mantenerse siempre disponible, puesto que por aquí se transporta gran cantidad de información para ser almacenada en los servidores. • Mantener procedimientos de seguridad en la red. • Contar con políticas de protección contra desastres. • Realizar la configuración de todos los equipos de networking para administrar de mejor manera la red. • Mantener procedimientos de control de acceso. • Debe contar con políticas de respaldo de todas las configuraciones de los dispositivos de red. • La manipulación de los equipos debe ser únicamente por personal capacitado.
Centro de Datos	Debe mantener un manual de contingencia en caso de producirse desastres en los sistemas que se encuentran albergados en su interior como: iluminación, control de acceso, ventilación, energía. Se debería contar un centro alterno con características similares para la pronta reanudación de las actividades.
PCs	• Es el principal medio de trabajo para los trabajadores del municipio por lo que deben funcionar correctamente el mayor tiempo posible para que puedan desempeñar sus actividades diarias. • Deben contar con un proceso de autentificación. • La información aquí almacenada únicamente debe ser modificada por el personal autorizado y debe ser únicamente para el desarrollo de las actividades laborables • Debe contar un software para evitar los daños producidos por códigos maliciosos.

3.4.4 ESTRATEGIAS DE PROTECCIÓN TECNOLÓGICAS

Las estrategias de protección se encuentran orientadas a proveer mayor seguridad a la información y a los activos críticos, o en caso de necesitar una solución inmediata en respuesta a un evento imprevisto. Áreas en las que se deben definir estrategias de protección.

a) Manejo de la información.
b) Obtención de respaldos de información.
c) Seguridad en la red.
d) Seguridad física.
e) Controles contra códigos maliciosos.
f) Mantenimiento de los equipos.
g) Sabotaje o daño accidental.

3.4.4.1 Manejo de la información

1) Restringir el acceso al personal no autorizado a las instalaciones donde se almacena información sensible o critica. (NTE INEN-ISO/IEC 27002, 2009)
2) Realizar pruebas a la los respaldos de información para verificar que se encuentra en buen estado. (NTE INEN-ISO/IEC 27002, 2009)
3) Debe estar debidamente etiquetada en todos los medios almacenados y su nivel de sensibilidad. (NTE INEN-ISO/IEC 27002, 2009)
4) Debe contar con procedimientos de protección al momento de intercambiarla a través de la red pública. (NTE INEN-ISO/IEC 27002, 2009)
5) Uso te técnicas de encriptación para proteger la confidencialidad, la integridad y la autenticidad de la información (NTE INEN-ISO/IEC 27002, 2009)
6) Responsabilidades a los empleados de no comprometer a la organización a través de difamación acoso suplantación de identidad etc. (NTE INEN-ISO/IEC 27002, 2009)

7) Implementar precauciones sobre métodos de robo de información con la ingeniería social. (NTE INEN-ISO/IEC 27002, 2009)
8) Procedimientos y policías para la protección de la información en los sistemas que usan información compartida (NTE INEN-ISO/IEC 27002, 2009)

3.4.4.2 Obtención de copias de seguridad de la información

1) Implementación de políticas y proceso de copias de respaldo de la información y software (NTE INEN-ISO/IEC 27002, 2009)
2) Realizar registros exactos y completos de las copias de respaldo. (NTE INEN-ISO/IEC 27002, 2009)
3) Contar con procedimientos de restauración pruebas que funcionen de la información (NTE INEN-ISO/IEC 27002, 2009)
4) La información de respaldo debe ser almacenada en un lagar externo a las instalaciones principales para evitar ser afectada por cualquier desastre que pueda presentarse. (NTE INEN-ISO/IEC 27002, 2009)

3.4.4.3 Seguridad en redes

1) Los sistemas la red eléctrica y de telecomunicaciones deben estar protegidos contra interceptaciones o daños (NTE INEN-ISO/IEC 27002, 2009)
2) El cableado debe estar bebidamente protegido para evitar posibles daños o interceptaciones no autorizadas. (NTE INEN-ISO/IEC 27002, 2009)
3) Tanto equipos como cables deben estar debidamente etiquetados para evitar errores en el manejo, o conexiones erróneas en la red. (NTE INEN-ISO/IEC 27002, 2009)
4) Contar con un plano del cableado de la red para ubicar rápidamente algún segmento dela red que se encuentre afectado. (NTE INEN-ISO/IEC 27002, 2009)
5) Realizar un reconocimiento en las instalaciones físicas en busca de dispositivos conectados sin autorización. (NTE INEN-ISO/IEC 27002, 2009)

6) Solo el personal autorizado y capacitado puede realizar el mantenimiento de los equipos de red. (NTE INEN-ISO/IEC 27002, 2009)
7) Llevar un registro del manteamiento preventivo y correctivo realizado a los equipos. (NTE INEN-ISO/IEC 27002, 2009)
8) Definir los controles necesarios para salvaguardar la confidencialidad e integridad de los datos través de las redes públicas e inalámbricas (NTE INEN-ISO/IEC 27002, 2009)
9) Se recomienda el uso de herramientas para implementar algoritmos de encriptación para proteger las comunicaciones por correo electrónico donde se envíe información confidencial. (NTE INEN-ISO/IEC 27002, 2009)
10) Crear políticas para la protección contra riesgos con la obtención de archivos y software desde o a través de redes externas.
11) Deshabilitar de los equipos los servicios que no sean necesarios y verificar los posibles puertos que se encuentren abiertos y no se estén utilizando para cerrarlos. (NTE INEN-ISO/IEC 27002, 2009)
12) Se recomienda implementar Vlans para la segmentación de la infraestructura física de la red. (NTE INEN-ISO/IEC 27002, 2009)
13) Gestionar y optimizar la distribución apropiada del ancho de banda para la red cableada y la red inalámbrica. (NTE INEN-ISO/IEC 27002, 2009)
14) Realizar un monitoreo de la red, detectar y corregir vulnerabilidades para proteger la infraestructura y la red de ataques. (NTE INEN-ISO/IEC 27002, 2009)
15) Solicitar permisos de autentificación al momento de conectarse a la red ya sea inalámbrica o cableada médiate claves de acceso. (NTE INEN-ISO/IEC 27002, 2009)
16) Identificar las seguridades necesarias para el acceso a servicios niveles de seguridad (NTE INEN-ISO/IEC 27002, 2009)
17) Para la protección del acceso no autorizado a nivel lógico se sugiere la habilitación de un firewall y proxy que impida el ingreso desde redes externas hacia la red interna del municipio. (NTE INEN-ISO/IEC 27002, 2009)

3.4.4.4 Seguridad física

1) Restringir el acceso al centro de datos mediante la utilización de llaves, tarjetas de identificación y sistemas biométricos. (NTE INEN-ISO/IEC 27002, 2009)
2) El acceso al centro de datos debe ser únicamente por el personal autorizado. (NTE INEN-ISO/IEC 27002, 2009)
3) Controlar el acceso a las áreas donde se procesa o almacena la información sensible, se debería implementar un registro con fecha y hora de ingreso y salida a los visitantes, los mismos que siempre deben ser supervisados por el personal encargado. (NTE INEN-ISO/IEC 27002, 2009)
4) Cuando se cuenta con servicios de soporte de terceros se debe tener el acceso restringido y solo si es necesario se debe autorizar el acceso y llevar el respectivo monitoreo. (NTE INEN-ISO/IEC 27002, 2009)
5) Contar con vigilancia para realizar un constante monitoreo de posibles sospechosos que quieran atentar con la integridad de los equipos, infraestructura. (NTE INEN-ISO/IEC 27002, 2009)
6) Se recomienda la contratación o implementación de oficinas alternas y procedimientos de protección en casos de desastres naturales o manifestaciones sociales. (NTE INEN-ISO/IEC 27002, 2009)
7) Evitar el uso de quipos de grabaciones de videos, fotográficas sin la respectiva autorización. (NTE INEN-ISO/IEC 27002, 2009)
8) Evitar que la información sensible se encuentre a simple vista de forma de reducir el riesgo por visualización de la información por personas no autorizadas. (NTE INEN-ISO/IEC 27002, 2009)
9) Realizar un monitoreo constante de las condiciones ambientales dentro del centro de datos para evitar fallas ocasionadas estos equipos que afectaría al procesamiento de la información (NTE INEN-ISO/IEC 27002, 2009)
10) Procedimientos de revisión en los de iluminación electricidad agua, ventilación para garantizar el adecuado funcionamiento. (NTE INEN-ISO/IEC 27002, 2009)
11) Debe contar con un UPS para el cierre ordenado de los equipos o el funcionamiento continuo de las operaciones criticas (NTE INEN-ISO/IEC 27002, 2009)

3.4.4.5 Códigos maliciosos

1) Realizar procesos de concientización a usuarios sobre códigos maliciosos y la importancia de la seguridad de la información dentro de la institución.
2) Llevar a cabo revisiones regulares de software y el contenido de datos de los sistemas, se debe investigar la presencia de archivos no aprobados o modificaciones no autorizadas. (NTE INEN-ISO/IEC 27002, 2009)
3) Usar software de fuentes conocidas y de confianza, de tal forma que se evite copias falsificadas que puedan ser objetivos de un atacante al no contar con las debidas garantías que provee un software oficial. (NTE INEN-ISO/IEC 27002, 2009)
4) Para la detección de códigos maliciosos se recomienda la utilización de un software que permita detectarlos y en caso de ser necesario reparar archivos que se vean afectados por estos códigos maliciosos, este software debe estar en continuo actualización.
5) Para mayor eficiencia se considera contar con un antivirus para los equipos de usuario y otro para los servidores, de esta manera es más difícil la propagación de los virus al contar con la diversificación de antivirus, es importante que estos dos software escogidos sean compatibles para evitar fallas dentro del sistema operativo.
6) A fin de evitar que códigos maliciosos ingresen al sistema se prohíbe la instalación de programas sin el permiso del administrador de red. (NTE INEN-ISO/IEC 27002, 2009)
7) La instalación de software debe ser realizada únicamente por el personal del departamento de sistemas y tecnología, se recomienda contar con una lista del software, este será seleccionado por la gerencia y del departamento de sistemas y tecnologías. (NTE INEN-ISO/IEC 27002, 2009)
8) Contar con información actualizada sobre seguridad de la información y acerca de los nuevos códigos maliciosos. (NTE INEN-ISO/IEC 27002, 2009)
9) Procedimientos y responsabilidades para la gestión de para la verificación de códigos maliciosos en medios extraíbles, correos electrónicos páginas web, archivos enviados por la red. (NTE INEN-ISO/IEC 27002, 2009)

3.4.4.6 Fallas en hardware o software

1) Se recomienda que al menos dos veces al año se realice el mantenimiento preventivo de todos los equipos tanto de redes como PCs, y llevar un control de los daños encontrados, y el desgaste de los mismos. (NTE INEN-ISO/IEC 27002, 2009)
2) Se sugiere contar con uno o más empleados debidamente capacitados que brinden el mantenimiento preventivo y correctivo a todos los equipos de la organización. (NTE INEN-ISO/IEC 27002, 2009)
3) Los equipos de computación deben tener un regulador de voltaje para evitar daños por variaciones de voltaje.
4) Implementar herramientas sistematizadas para controlar el inventario de Hardware y Software de la compañía. (NTE INEN-ISO/IEC 27002, 2009)
5) Realizar actualizaciones de seguridad para los sistemas operativos, una herramienta que nos puede resultar útil es WSUS puesto que en toda la institución los equipos trabajan en Mirosoft. El procedimiento a seguir sería la configuración del servidor para que se descarguen las actualizaciones y se almacenen en el disco duro y luego de manera automática los usuarios podrán descargar las actualizaciones de manera segura
6) También es indispensable que se actualice los parches de seguridad de las otras aplicaciones como por ejemplo Sql server, Oracle, etc.

3.4.4.7 Sabotaje o daños accidentales

Aunque no existe protección absoluta contra el robo de la información podemos minimizar el impacto haciendo uso de algunas herramientas:

1) Contar con políticas de seguridad de información dentro de la organización
2) Designar responsabilidades a cada uno de los empleados. (NTE INEN-ISO/IEC 27002, 2009)
3) Solicitar la debida autentificación y permisos por parte del administrador para el acceso y modificación de datos. (NTE INEN-ISO/IEC 27002, 2009)

4) Solicitar permisos de administrador para la copia de información en cualquier tipo de dispositivo extraíble por parte de las estaciones de trabajo. (NTE INEN-ISO/IEC 27002, 2009)
5) Establecer medidas drásticas con empleados que atentan con la integridad de la institución.

3.4.5 TIEMPO DE RECUPERACIÓN E IMPACTO GENERADO SI FALLAN LOS ACTIVOS CRÍTICOS

A causa de amenazas como desastres naturales, fallas en los equipos, daños provocados por terceros, la información e infraestructura de red se verían comprometidos en integridad y disponibilidad.

Si el daño es producto de desastres naturales el impacto producto de la materialización de estas amenazas seria crítico, generaría perdidas económicas.

Si la materialización de amenazas se presenta en los sistemas principales o en los equipos críticos, el impacto para la institución seria alto, se suspenderían las actividades diarias, generaría pérdidas económicas, molestias en los usuarios.

Si los daños se producen en el centro de datos en los sistemas informáticos, los daños serian parciales y el impacto sería medio pues las actividades podrían continuar de manera parcial.

Cuando los daños se producen en los equipos de usuario final el impacto sería normal pues no interrumpiría con las actividades de la institución y el costo de recuperación sería menor.

En la tabla 3.13 se estable de acuerdo a cada uno de los activos el tiempo máximo que pueden estar inhabilitados, este tiempo fue determinado y analizado por parte del jefe del Departamento de Sistemas y Tecnología de Información del GAD de Antonio Ante.

Tabla 3.13. *Tiempos de recuperación máxima de los activos críticos del GAD de Antonio Ante*

Fuente*: Departamento de Sistemas de GAD de Antonio Ante*

INDICADORES	TIEMPO DE RECUPERACIÓN
Activo: Información y servidores	Registro de la propiedad máximo 6 horas Recaudación máximo 1 día contable, agua potable avalúos y catastros máximo 3 días
Activo: equipos de networking	El switch de core máximo 2 horas Switch secundarios máximo 1 día
Activo: red de datos	Inhabilitada máximo 3 horas
Activo: software	Sistema Registro de la propiedad máximo 5 horas Sistema de recaudación máximo 1 día Sistema contable, agua potable avalúos y catastros máximo 2 días
Activo: centro de datos	Los sistemas de energía máximo 3 horas Sistema de enfriamiento máximo 48 horas

CAPITULO IV

En el presente capitulo se desarrolla un manual de procedimientos que permita la pronta reanudación de las operaciones en el menor tiempo posible luego de haberse presentado un evento que dificulte el desarrollo normal de las actividades en la institución.

El documento se encuentra conformado por una caratula, objetivo y el alcance del mismo, además se describe los roles y funciones a realizar por cada uno de los miembros del departamento de Sistemas y los procedimientos a ejecutarse para cada una de las amenazas.

GOBIERNO MUNICIPAL DE ANTONIO ANTE 	PLAN DE RECUPERACIÓN Y RESPALDO MANUAL DE PROCEDIMIENTOS DE LA UNIDAD DE SISTEMAS Y TECNOLOGÍA	Revisión:

CONTENIDO

OBJETO
ALCANCE
DEFINICIONES
REFERENCIAS
RESPONSABILIDAD
EJECUCIÓN

ELABORADO	REVISADO	APROBADO
Cargo: Nombre:	Cargo: Nombre:	Cargo: Nombre:
Fecha: Firma:	Fecha: Firma:	Fecha: Firma:

4.1 OBJETO

Reanudar las operaciones de la municipalidad de Antonio Ante lo más pronto posible luego de haberse presentado una situación de contingencia.

4.2 ALCANCE

El presente manual de procedimientos se aplica para la Unidad de Sistemas y Tecnología del Gobierno Municipal de Antonio Ante, consta de procedimientos de recuperación global en caso de fallas o interrupciones tecnológicas.

Este documento no proporciona procedimientos específicos en caso de contingencia en cualquiera de los otros departamentos del municipio por lo que es de responsabilidad del encargado de cada departamento desarrollarlos.

Se considera los siguientes puntos:

1. Restablecimiento de equipos y sistemas vitales para la continuación de las actividades del municipio.
2. Restablecimiento de las áreas vitales de la red de computadores.
3. El departamento de sistemas tiene como responsabilidad:

- Dar soporte a la red local de datos
- Mantener actualizado el plan de contingencia y de recuperación de desastres
- Mantener contratos con proveedores conforme lo requiera
- Entran al personal para llevar a cabo las funciones definidas
- Notificar a usuarios de aplicaciones críticas que lleven a una situación de desastre.

Y no está considerado:

- Emergencias en los edificios y procedimientos de evacuación.

4.3 DEFINICIONES

Sistemas de información: conjunto de procesos, persona y equipos capaces de recibir datos y producir información. Pueden ser aplicaciones de todo tipo de proceso de datos automatización de oficinas y sistemas.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Integridad: Se refiere a la capacidad de proteger la información de transmisiones o alteraciones no autorizadas, la información debe mantenerse intacta, precisa y fiable.

Incidente: Cuando un suceso inesperado se materializa, como por ejemplo fallas en los sistemas básicos: iluminación, eléctrico, o cuando de forma accidental se pierde información.

Plan de recuperación: Se definen los procesos o lineamientos que se deben seguir después de haber controlado la amenaza, en este plan se realiza la restauración de los equipos y actividades a su estado inicial antes de producirse la amenaza.
Activo: a aquello que tiene algún valor para la organización y por tanto debe protegerse.

Interrupción de servicios: es una suspensión temporal o total de la ejecución de un proceso.

Evento: La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información.

Riesgo: Es la explotación de las debilidades de un activo de información por una amenaza se valora en función del impacto, amenaza, vulnerabilidad y la probabilidad de un ataque exitoso.

Servidores: es un ordenador o máquina informática que brinda servicios y suministra información a otras máquinas denominadas clientes.

Red: es un sistema o medio de comunicación utilizado para el envío y recepción de la información.

4.4 REFERENCIAS

- Norma NTE INEN-ISO/IEC 27002:2009

4.5 RESPONSABILIDADES

Coordinador General: es el responsable de la elaboración del presente documento, así como de la ejecución, supervisión y designación de actividades a cada uno de los miembros del grupo de contingencia, así como también las tareas relacionadas a su área de alcance.

Coordinador de Redes y Comunicaciones: encargado de ejecutar las labores que sean designadas por el coordinador general, del correcto funcionamiento de las comunicaciones, servicios de internet, correo electrónico, red cableada e inalámbrica y los daños ocasionados en los equipos de networking.

Coordinador de Sistemas: responsable de realizar las tareas designadas por el coordinador general, verificar el funcionamiento correcto de los sistemas

considerados críticos, optimización de recursos, pruebas de funcionamiento de los sistemas en caso de configuración de nuevos equipos.

Coordinador de Respaldos: encargado de mantener las copias de seguridad actualizadas y en un lugar seguro.

Coordinador de soporte técnico: encargado de realizar las tareas designadas por el por el coordinador de redes, brindar mantenimiento a los PCs, impresoras, faxes, etc., y restablecer el servicio a la brevedad posibles sea cual sea el daño en los equipos.

4.6 EJECUCIÓN

El manejo adecuado de las tecnologías de información (IT) se basas en un marco referencial de buenas prácticas orientadas a la seguridad, consistencia, disponibilidad, y eficiencia de los procesos involucrados y relacionados con las mismas. Dichas actividades están orientadas a garantizar el correcto funcionamiento de los siguientes servicios de IT.

4.6.1 PLAN DE RECUPERACIÓN Y RESPALDO

El plan de recuperación y respaldo es un documento debidamente planificado con procedimientos que permiten brindar de forma oportuna una respuesta, ante la presencia de un evento inesperado, siga operando al mínimo de su capacidad.

Para que este plan tenga éxito se necesita la colaboración de todos los involucrados en el incidente a fin de fortalecer y cumplir con las acciones descritas.

4.6.1.1 ACTIVIDADES PREVIAS:

a) Incendio

- Contar con equipos de emergencia como extintores apropiados para los departamentos con mayor probabilidad de provocarse un incendio.
- Contar con señalización de rutas de escape en toda la municipalidad.
- Realizar simulacro de incendio con los empleados al menos una vez al año para que estén capacitados en caso de presentarse un incendio.
- Sistemas de detección de incendios, mismo que brinda alertas tanto para los empleados como para el cuerpo de bomberos.
- Contratar pólizas de seguros para todo el equipo informático del municipio, a fin de proteger los activos.
- Las paredes del centro de datos deben estar cubiertas con pintura especializada que retrase la propagación del fuego.
- Evitar el almacenamiento de productos inflamables.
- Revisar continuamente que los cables de los equipos eléctricos se encuentren en perfectas condiciones.
- Evitar las sobrecargas en los circuitos eléctricos en los contactos múltiples.
- Contar con los números telefónicos de emergencia a la vista y un botiquín.

b) Sismos

- Identificar las zonas seguras y vías de evacuación dentro del municipio.
- Ubicar lugares seguros cercanos para la concentración de los empleados.
- Realizar simulacros preventivos por lo menos una vez al año para capacitar a los empleados.
- Realizar una revisión continua de instalaciones eléctricas a fin de evitar corto circuitos y posibles incendios.
- Verificar de manera periódica el estado de las instalaciones de agua.
- Se debe contar con un botiquín de primeros auxilios, debe estar ubicado en un lugar de fácil acceso y visible.

- Identificar los lugares donde existe gran peligro en este tipo de desastres: pasillos, ascensores, laboratorios, centro de datos.
- Asegurar las líneas eléctricas y telefónicas, coordinando con las instituciones pertinentes.
- Mantener un inventario de materiales, herramientas y equipos necesarios para enfrentar situación de emergencia.
- Crear un Comité de Seguridad Sísmica.
- Organizar grupos que trabajará en las brigadas de emergencia, primeros auxilios y búsqueda y rescate.
- Contar con un listado de números telefónicos de emergencia.

c) Filtraciones de Agua

- Mantener limpios los sistemas de desagüe y verificar que estén funcionando adecuadamente.
- Contar con pólizas de seguros para los equipos de forma que dicha empresa responda por los daños producidos por el agua.
- Todo contacto o interruptor debe tener su taba debidamente aislada.

d) Cortes o Sobrecarga de energía

- Se debe contar con la documentación necesaria tanto del cableado de la red y el eléctrico.
- Todos los equipos que se encuentren en el centro de datos han de estar debidamente conectados a un UPS, para evitar que se apaguen por cortes de energía eléctrica.
- Verificar el correcto funcionamiento y estado de cada uno de los puntos eléctricos y la conexión a tierra.
- Todas las estaciones de trabajo deben contar con un regulador de voltaje a fin de evitar los daños en los equipos por variaciones de voltaje.

- Para evitar que las actividades del municipio se suspendan cuando existen cortes de energía eléctrica la institución debe contar con energía eléctrica suministrada por otra fuente (generador eléctrico u otro proveedor de electricidad).

e) Ataques Internos a la red

- Tener habilitados únicamente los puntos que se encuentran utilizados por los usuarios y solo si es necesario habilitarlos con autorización del encargado de la administración de la red.
- Desactivar los servicios que no son necesarios de acuerdo a cada departamento de la institución.
- Contar con un diseño de red físico, lógico y jerarquizado, se debe contar con una lista de todas las direcciones IP de las estaciones de trabajo de la institución y a quién le pertenece.
- Realizar monitoreo constantes en busca de conexiones no autorizadas.

f) **Problemas de conectividad de la red**

- Verificar si las tarjetas de red de cada computador se encuentran conectados de manera correcta tanto físicamente y si el controlador del dispositivo se encuentra instalado correctamente.
- Verificar si el ptach cord que conecta la estación de trabajo con el punto de usuario final se encuentra en buen estado.
- Verificar si el patch cord se encuentre bien conectado al punto de red y en el computador.
- Verificar si desde el punto de usuario final hasta la conexión al switch no tenga problemas.
- Comprobar el estado y el funcionamiento del switch.

- El equipo de telecomunicaciones debería tener al menos dos rutas de conexión con el proveedor de servicios en caso de fallas en la red

g) Robos

- Observar que en las instalaciones no se encuentre algún individuo sospechoso, esta labor se encontrara a cargo del personal de seguridad municipal de la institución.
- El personal debe contar con su respectiva identificación para tener acceso a determinados lugares (datacenter, bodega).
- Mantener la información crítica resguardada, debe almacenarse en servidores centralizados y no en los discos de almacenamiento de los computadores personales; la información debe contar con un almacenamiento espejo en un centro de datos externo a la institución.
- Contar con vigilancia permanente a través de cámaras de seguridad tanto en el interior de las instalaciones del municipio como en el centro de almacenamiento externo donde se encuentre el respaldo de la información crítica.
- Se debe contar con pólizas de seguros de los activos más importantes.
- Instalación de alarmas de seguridad.

h) Errores de Hardware y Software

- Cada computador debe contar con un regulador de voltaje.
- Realizar un mantenimiento preventivo por lo menos dos veces al año para evitar acumulación de polvo en los equipos lo que provocaría fallas en la fuente de poder o en la memoria RAM.
- Verificar si los ventiladores del computador se encuentran funcionando correctamente, la falla de estos puede producir un sobrecalentamiento en los dispositivos internos del computador.

- Se debe mantener un inventario actualizado de los equipos, sus características y su estado.
- Adquirir pólizas de seguros comerciales para la protección de los activos más importantes de la institución en caso de daños.
- Se debe contar con una adecuada señalización de equipos de mayor importancia de acuerdo a su contenido o servicios que brinda.
- El encargado de sistemas debe realizar un seguimiento de todos los equipos de computación para identificar las posibles fallas en los equipos.

i) Códigos maliciosos

- Los computadores deben estar protegidos con un buen antivirus, contar con las respectivas actualizaciones.
- De igual forma los servidores deben estar protegidos con antivirus actualizado, firewall, proxy.
- No abrir mensajes de correo de desconocidos.
- Evitar el uso de software ilegal.
- Realizar copias de seguridad constantemente.
- Realizar el escaneo de todos los dispositivos extraíbles a través del antivirus antes de abrirlos en el computador.

j) Pérdidas de información

- Realizar copias de seguridad continuas de los datos.
- Realizar copias del software considerado como crítico en caso de posibles fallas.
- Contar con un backup del sistema operativo, programas desarrollados dentro de la organización, software Base- paquetes y/o lenguajes de programación.

- Al realizar las respectivas de copias de seguridad, se debe tomar en cuenta el uso de herramientas de encriptación con el fin que la información únicamente pueda ser recuperada por quien la genero.
- Se recomienda mantener respaldos en el interior de sitio para mayor facilidad de recuperación y de igual forma otro respaldo fuera de las instalaciones de la organización.

4.6.1.2 ACTIVIDADES DURANTE:

a) Incendios

- Alertar al cuerpo de bomberos sobre la situación de incendio.
- El personal deberá salir con calma y dirigirse a los sitios designados como seguros para la reunión.
- Los empleados escogidos con anterioridad para la utilización de extinguidores pondrán en marcha su responsabilidad en ese momento.
- Si es que es posible el responsable de cada departamento terminará las sesiones iniciadas por los usuarios que hayan estado utilizando el sistema en ese momento y procederá a apagar los servidores.
- La última persona en salir de cada uno de los departamentos debe comprobar si todos los dispositivos electrónicos se encuentran debidamente apagados.
- El personal de bomberos tratará de salvaguardar la integridad tanto del personal como de la infraestructura física de la institución.
- Después que los Bomberos declaren el fin de la emergencia y si las condiciones lo permiten, el personal regresara a su área de trabajo.

b) Sismos

- Conservar la calma y ayudar que los otros hagan lo mismo, evita correr, gritar o empujar de esta manera evitas accidentes durante la evacuación.
- Retirarse de las ventanas y objetos que puedan caerse, colócate bajo escritorio, mesa fuertes o marcos de las puertas para protegerte.
- Si te es posible desconecta equipos electrónicos, elimina fuentes de incendio
- Evitar el uso de elevadores
- Ubicarse en zonas de seguridad
- Localizar las rutas de evacuación

c) Filtraciones de Agua

- Apagar los equipos de computación de manera correcta y desconectarlos para evitar corto circuitos.
- Dar aviso al departamento de sistemas para que verifique si el o los equipos no fueron afectados por el agua o la humedad.
- Dar aviso de evento al encargado del departamento para que de aviso al personal pertinente para realizar las respectivas reparaciones.
- Evitar que las instalaciones eléctricas tengan contacto con el agua.

d) Cortes o Sobrecarga de energía

- Si se produce cortes del suministro de energía el encargado de sistemas debe informar de dicho suceso al técnico para que corrija el problema y evitar que vuelva a suceder.

- Verificar que el fallo no haya dañado los equipos de computación, revisar fuentes de poder, tarjetas de red, equipos de multimedia, equipos de networking, servidores, etc.
- Si el corto circuito se produce en el interior del municipio el personal técnico realizará las debidas evaluaciones para corregir el daño y comprobar los puntos eléctricos y las conexiones que se vean afectados en ese circuito.

e) Ataques Internos a la red

- Bloquear el equipo que no se encuentra autorizado para las acciones que se encuentra realizando.
- Restringir el acceso al usuario que esté realizando el ataque.
- El administrador de red debe verificar nuevamente los puntos de red

f) Problemas de conectividad de la red

- Dar aviso al help desk local.
- Revisar el entorno de la red
- Si no se cuenta con el acceso (internet) reportar al proveedor local.
- Si se demora por más de 6 horas dar aviso a los usuarios.

g) Robos

- Si el robo de información es interno se deberá hacer un seguimiento al empleado mal intencionado para tener evidencia y tomar acciones respectivas.
- Se prohíbe revelar información confidencial de la organización o del personal.
- Mantener la calma: no oponerse a los atacantes de manera especial si estos se encuentran armados o bajo el efecto de las drogas.

- Si es posible activar las alarmas de seguridad para alertar a la policía de lo que está sucediendo.

h) Errores de Hardware y Software

- Si el daño se produce en los equipos de computación se comunica al encargado para que evalué los posibles causas.
- Contactar Help Desk.
- Si fuera necesario instalar un nuevo equipo hasta la reparación del otro.
- Realizar procedimientos de recuperación de la información.

i) Códigos maliciosos

- Si se observa que somos víctimas de una infección pro un software malicioso dar aviso al departamento de sistemas de lo ocurrido y este pueda actuar antes que el virus infecte más estaciones de trabajo.
- El encargado procederá la desinfectar el equipo y luego examinar si más equipos dentro de la red fueron infectados incluyendo los servidores.

j) Perdidas de información

- Dara aviso al help desk local.
- Examinar el servidor de archivos.
- Revisar el tipo de búsqueda que se realiza.
- Proveer de soporte técnico para la realización de copias de respaldo de las aplicaciones.
- Coordinar redes, líneas, terminales, módems y otras comunicaciones.
- Realizar trabajos de recuperación.

4.6.1.3 ACTIVIDADES DESPUÉS:

a) Incendios

- El responsable de cada departamento será el encargado de solicitar un informe al cuerpo de bomberos el estado de las instalaciones, informará al encargado de sistemas para que realice una evaluación de los daños a los equipos de computación.
- Los responsables de cada departamento realizarán una investigación de las pérdidas físicas y lógicas, considerando la posibilidad de recuperación parcial o total de los equipos e información.
- Si se determina que el área es segura y se encuentra en buenas condiciones para la reanudación de las actividades, se procede a la instalación de equipo de computación ya sean estos de propiedad de la municipalidad o nuevos.

Con relación al respaldo de información

- El responsable debe almacenar la información de mayor importancia en un lugar diferente del edificio, en dispositivos extraíbles, unidades Dvd, etc., y almacenarlos en un sitio seguro.
- Se debe realizar la inmediata restauración de las actividades del municipio, para ello de se debe contar con los respaldos de información.
- El encargado debe restaurar las bases de datos, sistemas de mayor prioridad y la información recuperada, debe emitir las debidas notificaciones a los usuarios que ya pueden volver a utilizar los diferentes sistemas.
- El responsable de cada departamento debe analizar cómo se originó el incendio y las posibles causas, a fin de poder actualizar las políticas de seguridad y los controles preventivos.

b) Sismos

- Salir de las instalaciones y permanecer fuera durante un tiempo considerable o hasta que sea declarado oficialmente que puedes volver a ingresar.
- Revisar los daños externos e internos antes de ingresar nuevamente a las instalaciones.

Con relación al respaldo de información

- El responsable debe almacenar la información de mayor importancia en un lugar diferente del edificio, en dispositivos extraíbles, unidades Dvd, etc., y almacenarlos en un sitio seguro.
- Se debe realizar la inmediata restauración de las actividades del municipio, para ello de se debe contar con los respaldos de información
- El encargado debe restaurar las bases de datos, sistemas de mayor prioridad y la información recuperada, debe emitir las debidas notificaciones a los usuarios que ya pueden volver a utilizar los diferentes sistemas.
- El responsable de cada departamento debe analizar cómo se originó el incendio y las posibles causas, a fin de poder actualizar las políticas de seguridad y los controles preventivos.

c) Filtraciones de Agua

- El responsable de cada departamento debe realizar una investigación de las pérdidas de los equipos y la posibilidad de su recuperación parcial o total de los mismos.
- Revisar si las instalaciones se encuentran en buenas condiciones y no existe peligro de que vuelva a producirse el daño.
- Volver a instalar los equipos ya sea nuevos o de propiedad de la municipalidad.
- El responsable debe realizar una investigación de los daños en los equipos de networking y de almacenamientos si la filtración se realizó en el centro de datos.

- Se debe llevar a cabo la restauración de las aplicaciones proporcionadas por él AME (Asociación de Municipalidades Ecuatorianas) y el resto de aplicaciones adquiridas y desarrolladas por la municipalidad.
- Realizar las respectivas notificaciones acerca de los sistemas restaurados así como también de las bases de datos para que los usuarios puedan volver a usarlos.
- El encendido de los equipos se realizará únicamente luego de la revisión realizada por el designado del departamento de sistemas.
- Los responsables de cada departamento y autoridades del municipio deben darle seguimiento a este evento a fin de evitar la ocurrencia del mismo.

d) Cortes o Sobrecarga de energía

- El técnico encargado realizará una investigación sobre las posibles causas de los eventos y emitirá un informe a las autoridades pertinentes.
- Se procederá al cambio y/o reparación de las instalaciones afectadas cada uno de los puntos eléctricos.
- Una vez superado la contingencia y verificado su correcto funcionamiento el encargado procederá a la reinstalación del equipo.

e) Ataques Internos a la red

- Realizar un informe de los eventos ocurridos y las acciones realizadas para contar con un seguimiento de los incidentes y evitar el evento no vuela a ocurrir.
- Si el evento tiene incidencia el administrador de red podrá determinar quién es el responsable y tomar medidas correctivas de acuerdo al caso.
- Una vez terminada la investigación se informara a las autoridades pertinentes para que tomen las decisiones respecto a este evento.

f) Problemas de conectividad de la red

- Evaluar las posibles causas del evento
- Realizar un informe de los daños ocasionados por la interrupción del servicio de internet y/o acceso a la red interna.

g) Robos

- Los responsables de cada departamento deben realizar un inventario del sustraído
- La persona encargada debe informar a las autoridades de dichos hechos.
- Si es qué los equipos se encuentra asegurados comunicarse con el responsable para hacer uso del servicio.
- El responsable de cada departamento y el responsable de la seguridad física de la institución deben revisar las políticas de seguridad.

h) Errores de Hardware y Software

- Realizar una investigación de las posibles causas y las acciones tomadas al momento de evento.
- Evaluar los daños ocasionados, los sistemas afectados, que equipos ha dejado de funcionar y el tiempo de recuperación.

i) Códigos maliciosos

- Verificar la calidad e integridad de la información existente, esto lo realizamos mediante pruebas sobre los programas que antes el desastre funcionaban con normalidad.
- La calidad e integridad de la información de respaldo
- En lo posible volver al estado inicial antes de verse afectados por el software malicioso.

j) Perdidas de información

- Realizar una investigación de la información perdida y las posibles causas que origino este evento.
- Revisar los debidos procedimientos de copias de seguridad para evitar incidencias de este tipo

4.6.2 DOCUMENTACIÓN DEL PROCESO

Finalmente se realizó la documentación de todo el proceso que hemos venido desarrollando a lo largo del documento.

4.6.2.1 DESASTRES NATURALES

Si los daños fueron causados por sismos, incendios o filtraciones de agua y hace imposible la prestación de los servicios a los clientes en el mismo edificio, se toma en consideración lo siguiente:

Procedimiento:

1) Comunicar inmediatamente al coordinador general sobre el desastre que acaba de suceder, el coordinador será el encargado de determinar si el evento es considerado como un riesgo potencial y dará la orden de trasladar las actividades a las oficinas alternas designadas.

2) Cuando el daño ha sido significativo en las instalaciones del municipio lo que imposibilita la continuación de las actividades se debe hacer uso de las oficinas alternas y se procede a la instalación de los equipos para restablecer las operaciones, por otro lado se evaluará la probabilidad de regresar a las instalaciones principales, o establecerlas en un nuevo sitio. Se considera daños mayores cuando la afectación impide la utilización de equipos y no tenga reparación o necesite un tiempo prolongado para su recuperación.

3) Implementar los procedimientos de recuperación para el restablecimiento de las actividades.

a) Transportar los respaldos de la información, programas, manuales, etc., de donde se encontraban almacenadas a las oficinas alternativas, estos respaldos de información serán transportados con la debida seguridad
   Responsable: Coordinador de respaldos.

b) Restaurar la información de las bases de datos y programas en los equipos alternos.
c) Comprobar que la información se encuentre integra y completa hasta el punto antes del incidente.
   Responsable: Coordinador de sistemas junto con el coordinador de redes que es el encargado de preparar los equipos donde se va a restablecer los sistemas.

d) Dar aviso para reanudar las operaciones por parte del coordinador de sistemas al coordinador general, quien será el encargado de informar a las autoridades y a los usuarios.

Si los daños son menores y no es necesario el uso de las oficinas alternas se realizará las siguientes actividades:

a) Evaluar los daños encontrados e informar al personal encargado para que empiece el proceso de tramitar las garantías de los equipos dañados o comprar nuevos equipos indispensables para la continuidad de las operaciones.
   Responsable: Coordinador general.

b) Trasportar la información de respaldo, programas, manuales, etc., de donde se encuentra almacenada y se procede a la instalación del sistema operativo
   Responsable: Coordinador de respaldos.

c) Restaurar la información de las bases de datos y programas en los equipos alternos
d) Comprobar que la información se encuentre integra y completa hasta el punto antes del incidente.
   Responsable: Coordinador de sistemas.

e) Dar aviso para reanudar las operaciones por parte del coordinador de sistemas al coordinador general, quien será el encargado de informar a las autoridades y a los usuarios.

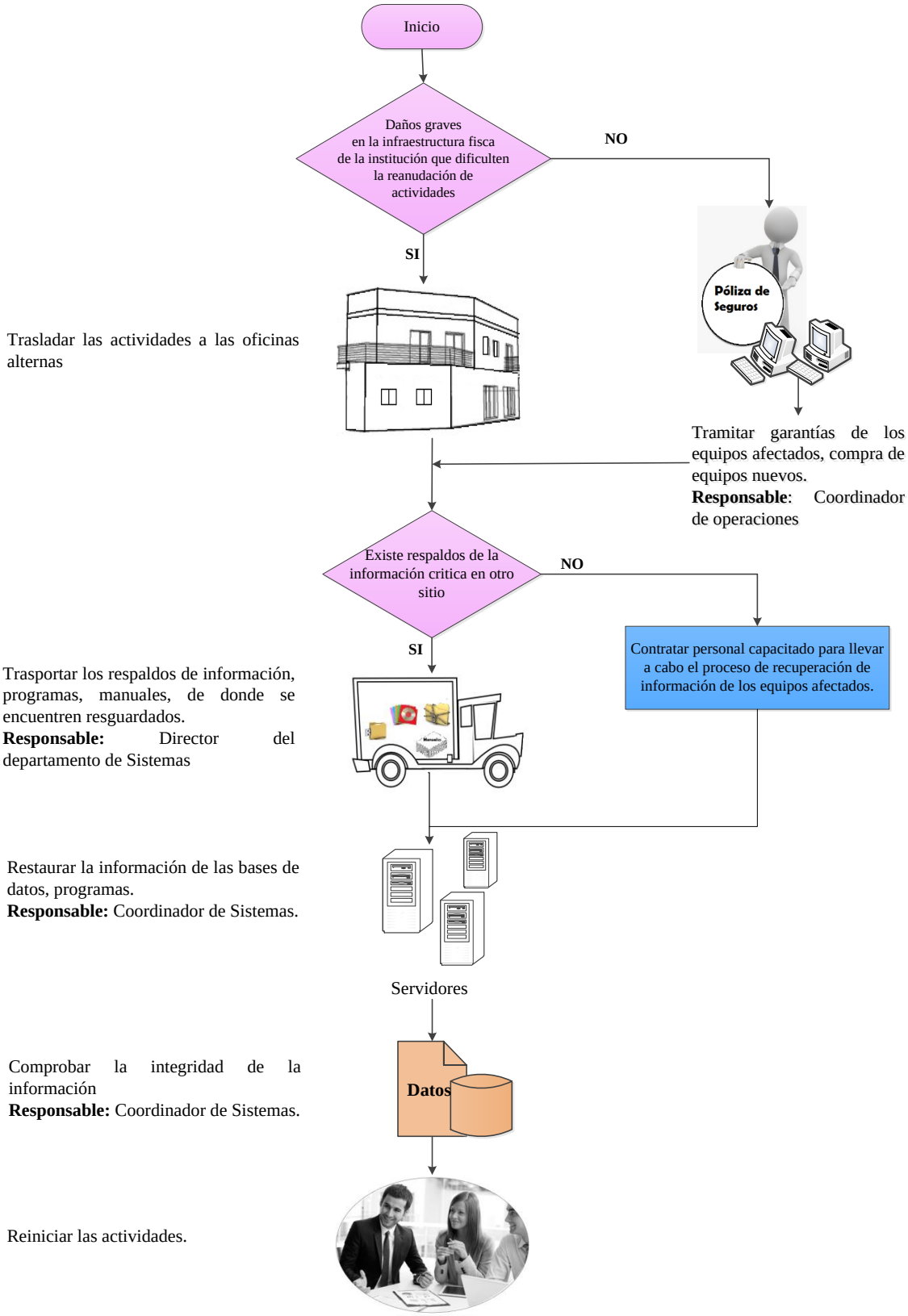


Diagrama 4.1 *Diagrama de respuesta en caso de desastres naturales*
Autora*: Karina Méndez*

4) Luego de haber puesto nuevamente operativa la infraestructura de red se procede a realizar la primera evaluación de daños de la infraestructura tecnológica, se realiza con la colaboración de todos los miembros del grupo de contingencia informático.

5) Comunicarse con los números de los proveedores de equipos y servicios necesarios para la reactivación de actividades en las oficinas alterna.

6) Comunicar oportunamente a las autoridades del incidente mediante la formulación de informes realizados por el coordinador en colaboración con el resto de miembros del grupo de contingencia. La investigación debe contener las causas del incidente, la naturaleza, la magnitud de los daños, los nombres y números telefónicos de las personas que fueron parte del incidente, y si es posible se debe tomar fotos, grabaciones, dibujos o cualquier tipo de información, las acciones que se tomaron en respuesta al incidente, los daños de los activos de la institución, comunicar las pérdidas por interrupción de servicios.

Revisión de la crisis:

1) Revisar si las acciones tomadas fueron efectivas al momento de contrarrestar la emergencia y si la utilización de recursos fue correcta.

2) Con que rapidez se obtuvo la disponibilidad de los recursos claves al momento de la gestión de riesgo.

3) Que tan efectivo fue el grupo para la contención del riesgo.

4.6.3 CORTES DE ENERGÍA

La activación de este procedimiento se realizará cuando los cortes de energía se produzcan en las instalaciones internas del municipio, y los daños interrumpan las actividades operativas.

Para la protección de los equipos que se encuentran en el interior del centro de datos el municipio cuenta con un UPS, sin embargo no es suficiente para continuar con las actividades del municipio y si el corte de electricidad es prolongado las actividades del municipio se verían afectadas. Aunque la probabilidad de que se presente un corte de energía prolongado es baja a continuación se describe el siguiente procedimiento.

Procedimiento:

- Comunicar inmediatamente al coordinador general sobre el incidente que acaba de suceder, el coordinador será el encargado de determinar si el evento es considerado como un riesgo potencial.

- Informar al personal encargado del manteamiento eléctrico de la institución para que evalué los daños, e inmediatamente implementar los procedimientos de recuperación en caso de cortes de energía.

  a) Verificar si el sistema eléctrico automático está funcionando correctamente por parte del personal encargado del mantenimiento eléctrico.
  b) Verificar el estado de los equipos del cuarto de telecomunicaciones
     Responsable: Coordinador de redes.

  c) Y si el corte afecto a los equipos de usuario el encargado de verificar el estado de los equipo será el encargado de Help desk
  d) Comprobar que la información se encuentre integra y completa hasta el punto antes del incidente.
     Responsable: Coordinador de sistemas.

e) Dar aviso para reanudar las operaciones por parte del coordinador de sistemas al coordinador general, quien será el encargado de informar a las autoridades y a los usuarios.

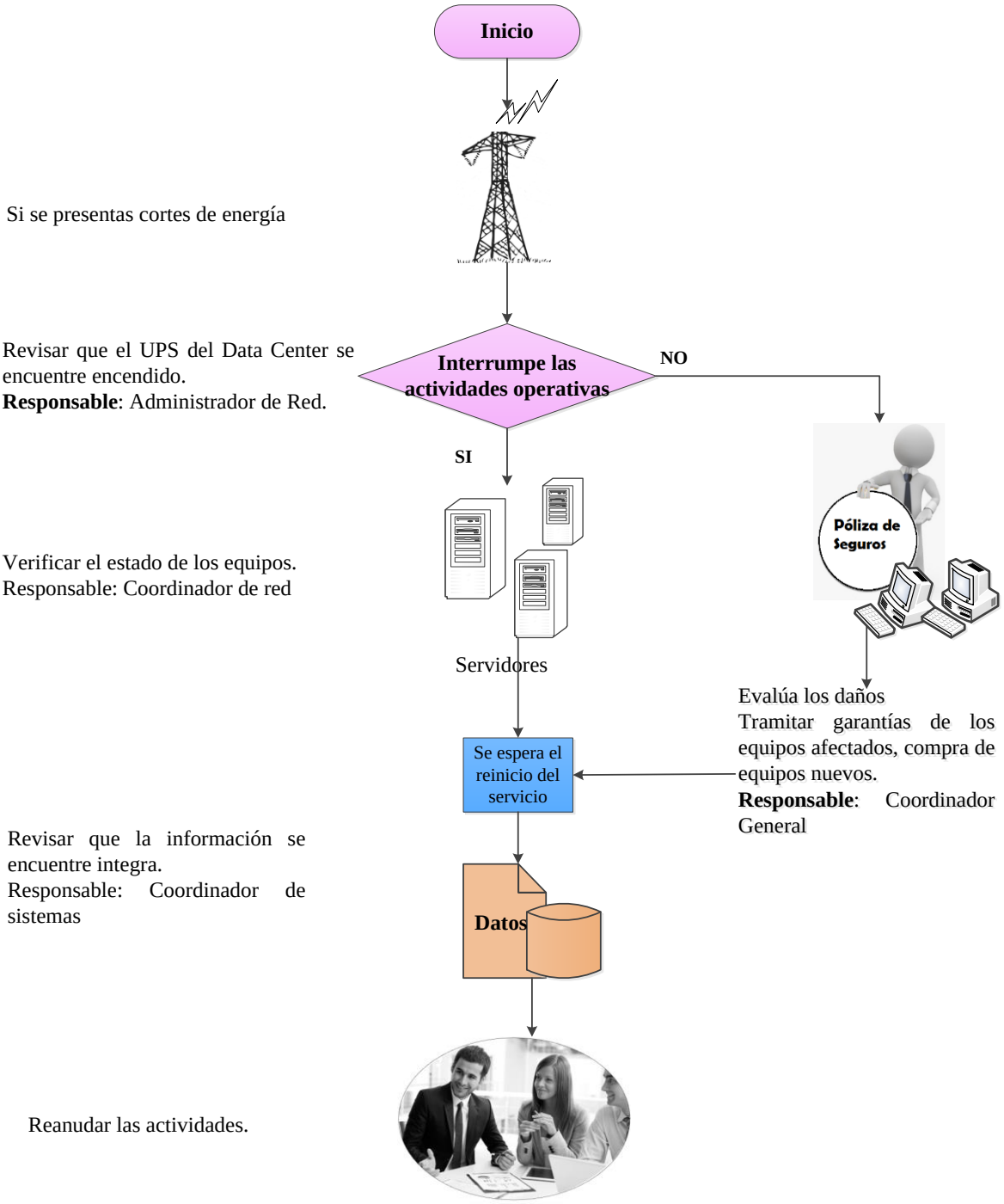


Diagrama 4.2 *Diagrama de respuesta a cortes de energía*

***Autora**: Karina Méndez*

- Realizar la primera estimación de daños ocasionados por el incidente.

- Si los daños no son considerados graves posterior a la evaluación del incidente por parte del coordinador de red, el coordinador general procede a tramitar garantizas en caso de ser necesario.

- Comunicar oportunamente a las autoridades del incidente mediante la formulación de informes realizados por el coordinador en colaboración con el resto de miembros del grupo de contingencia. La investigación debe contener las causas del incidente, la naturaleza, la magnitud de los daños, los nombres y números telefónicos de las personas que fueron parte del incidente, y si es posible se debe tomar fotos, grabaciones, dibujos o cualquier tipo de información, las acciones que se tomaron en respuesta al incidente, los daños de los activos de la institución, comunicar las pérdidas por interrupción de servicios.

Revisión de la crisis:

1) Revisar si las acciones tomadas fueron efectivas al momento de contrarrestar la emergencia y si la utilización de recursos fue correcta.

2) Con que rapidez se obtuvo la disponibilidad de los recursos claves al momento de la gestión de riesgo.

3) Que tan efectivo fue el grupo para la contención del riesgo.

4.6.4 FALLAS EN LA RED DE DATOS

Existe varios factores para que se produzcan fallas en la red, estos pueden ser por daños en los equipos de red, daños físicos en el sistema de cableado estructurado, lo primero que se debe hacer es evaluar las causas de que originó las fallas en la red.

Cuando la red de datos se encuentre afectada y sea imposible continuar con las actividades dentro del municipio este procedimiento entrará en acción bajo las siguientes circunstancias:

Procedimiento

1) Comunicar inmediatamente al coordinador general sobre el incidente que acaba de suceder.

2) El coordinador general dará la orden al coordinador de redes que proceda con las acciones para recuperar la disponibilidad de red.

3) El coordinador de redes procederá a la evaluación del incidente y determinara donde se encuentra el daño.

a) Si la falla procede por mal funcionamiento del equipo se procede al remplazo inmediato o remitirse al uso de la póliza de seguro.
b) De lo contrario los daños son en el SCE se procede a buscar una ruta alternativa para proveer de servicios al departamento afectado.
c) Revisar y probar la integridad de la información y las comunicaciones.
d) Todas estas actividades serán realizadas por el coordinador de redes.
e) Comprobar que la información se encuentre integra y completa hasta el punto antes del incidente.
f) Responsable: Coordinador de sistemas
g) Dar aviso para reanudar las operaciones por parte del coordinador de sistemas al coordinador general, quien será el encargado de informar a las autoridades y a los usuarios.

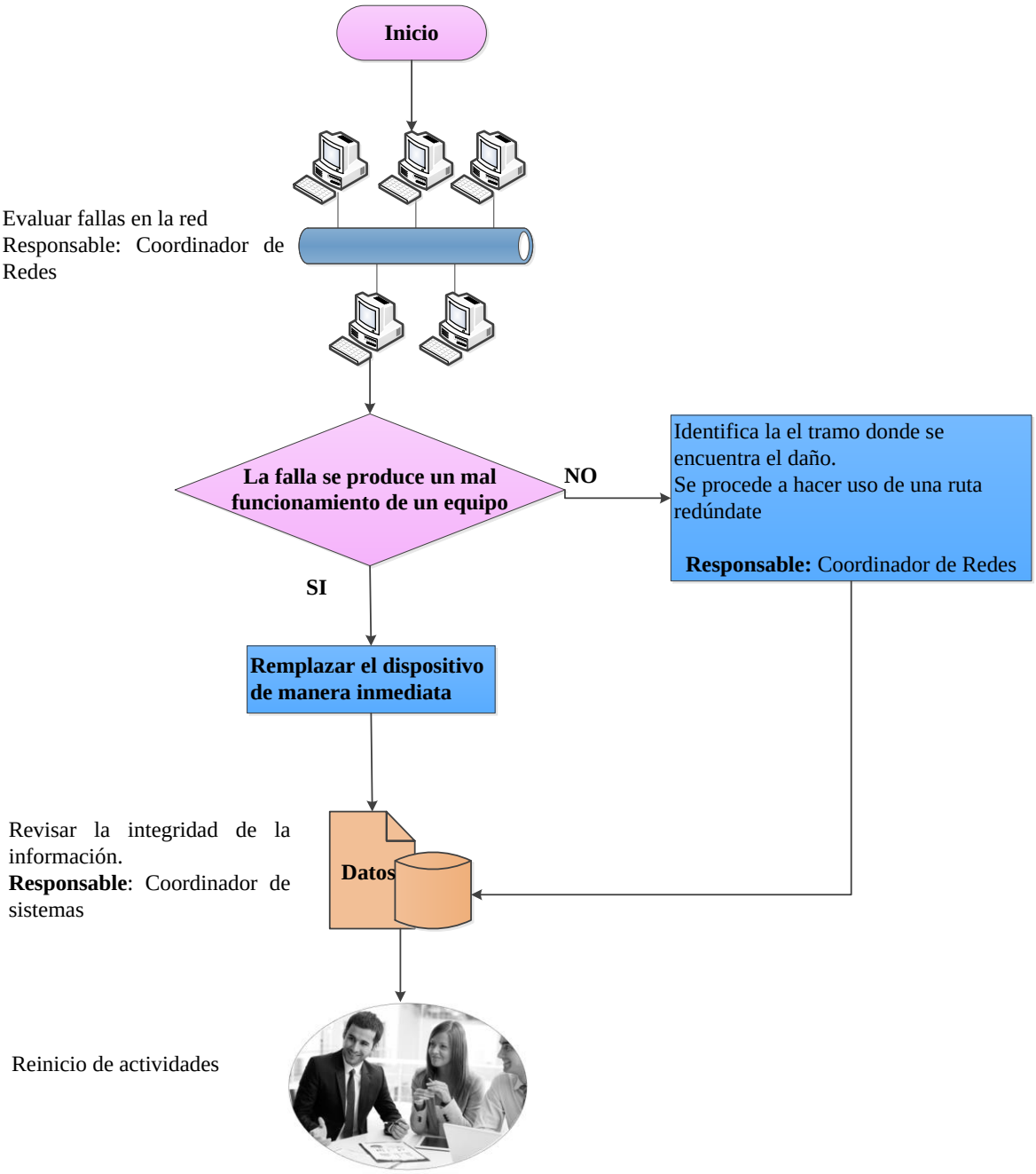


Diagrama 4.3 *Diagrama de respuesta a fallas en la red de datos*

Autora*: Karina Méndez*

4) Se realizará la entrega de un informe por parte del coordinador de redes sobre las causas, la magnitud de los daños, se debe tomar fotos para evidenciar los hechos, se describe las acciones que se tomaron en respuesta al incidente, las perdidas por la interrupción de las actividades.

Revisión de la crisis:

1) Revisar si las acciones tomadas fueron efectivas al momento de contrarrestar la emergencia y si la utilización de recursos fue correcta.

2) Con que rapidez se obtuvo la disponibilidad de los recursos claves al momento de la gestión de riesgo.

4.6.5 FALLAS EN EL HARDWARE O SOFTWARE

Este proceso entra en funcionamiento cuando los daños en los servidores sean críticos y las operaciones se vean afectadas por tanto se hace inicio de las siguientes actividades:

Procedimiento

1) Comunicar inmediatamente al coordinador general sobre el desastre que acaba de suceder.

2) El coordinador general dará la orden al coordinador de redes que proceda con las acciones para recuperar la disponibilidad de los servicios.

3) El coordinador de redes procederá a la evaluación del incidente y determinará la naturaleza del incidente y procederá a ejecutar las siguientes actividades.

    a) Informará al coordinador de respaldos para que proceda a trasportar la información, programas, manuales del sitio externo de donde se encuentran almacenados.

    b) Si las fallas proceden por daños en los equipos se procede a remplazo del equipo remitirse a la póliza de mantenimiento
    Responsable: Coordinador de Redes.

c) Instalar el sistema operativo (si es que es necesario)

Responsable: Coordinador de Redes

d) Restablecer la información de las bases de datos y programas
e) Verificar la integridad de la información

Responsable: Coordinador de Sistemas.

f) Dar aviso para reanudar las operaciones por parte del coordinador de sistemas al coordinador general, quien será el encargado de informar a las autoridades y a los usuarios.

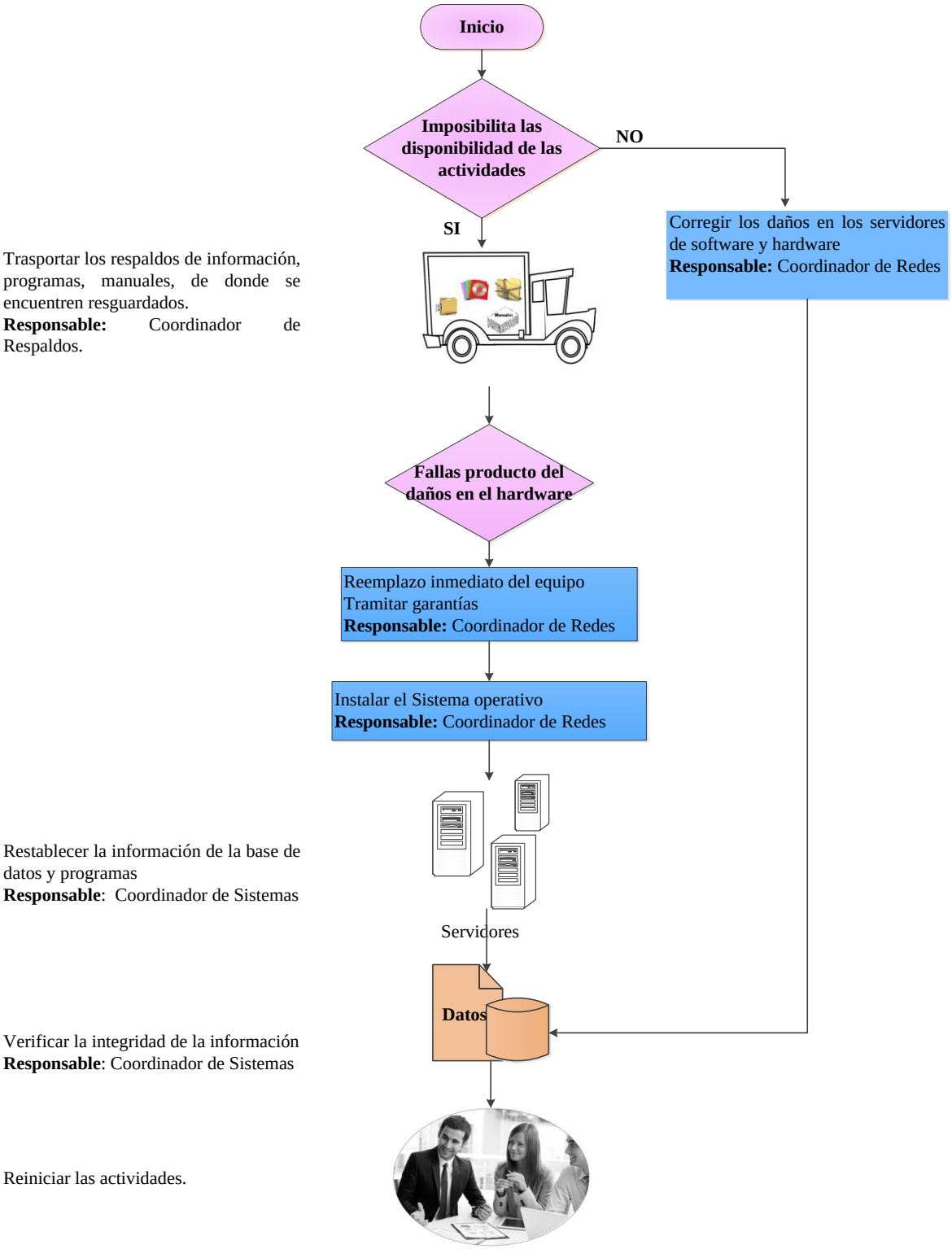


Diagrama 4.4 *Diagrama de respuesta a fallas en Hardware o Software*

Autora*: Karina Méndez*

4) El coordinador general será el encargado de comunicar oportunamente a las autoridades sobre el incidente presentado.

5) Se realizará la entrega de un informe por parte del coordinador de redes sobre las causas, la magnitud de los daños, se debe tomar fotos para evidenciar los hechos, se describe las acciones que se tomaron en respuesta al incidente, las perdidas por la interrupción de las actividades.

Revisión de la crisis:

1) Revisar si las acciones tomadas fueron efectivas al momento de contrarrestar la emergencia y si la utilización de recursos fue correcta.

2) Con que rapidez se obtuvo la disponibilidad de los recursos claves al momento de la gestión de riesgo.

4.6.6 SABOTAJE O DAÑO ACCIDENTAL

Este proceso se activara cuando las pérdidas de información son grandes y el tiempo para su recuperación es demasiado largo y las actividades del municipio no pueden estar suspendidas tanto tiempo por lo que lo más óptimo es recurrir a los respaldos con los que cuenta la institución y únicamente se procede a la recuperación de los datos del día y las actividades no se verían afectadas. El procedimiento a seguir en caso de que la pérdida de información, fallas en el procesamiento de datos, falta de acceso a los sistemas, será:

Procedimiento

1) Comunicar inmediatamente al coordinador general sobre el desastre que acaba de suceder.
2) El coordinador general dará la orden al coordinador de sistemas que proceda con las acciones para recuperar la información.

3) El coordinador de sistemas procederá a la evaluación del incidente y determinará la naturaleza del incidente

a) Informar al coordinador de respaldos para que proceda a trasportar los respaldos de información, programas, manuales del lugar de donde se encuentren almacenados.

b) Considerar el cambio del equipo por otro alterno para continuar con las actividades
c) Restaurar la información en los servidores de las bases de datos y programas.
d) Verificar la integridad de la información.

Responsable: Coordinador de Sistemas

e) Si los daños o pérdidas de información se dan en los PCs encargado de brindar soporte es el coordinador de Help Desk.

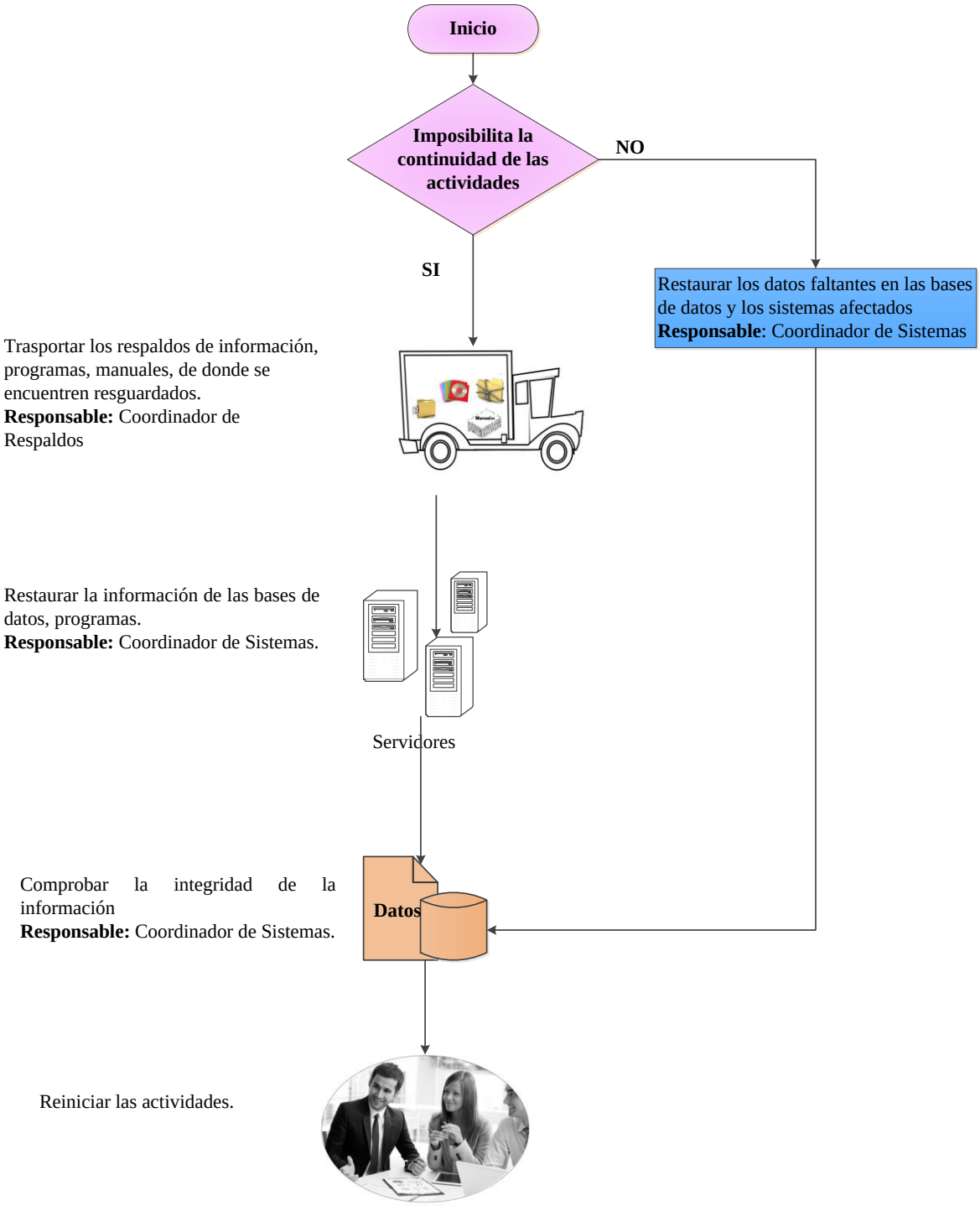


Diagrama 4.5 *Diagrama de Sabotaje o daños accidentales*

Autora*: Karina Méndez*

4) Dar aviso para reanudar las operaciones por parte del coordinador de sistemas al coordinador general, quien será el encargado de informar a las autoridades y a los usuarios.

5) Se realizará la entrega de un informe por parte del coordinador de sistemas sobre las causas, la magnitud de los daños, se debe tomar fotos para evidenciar los hechos, se describe las acciones que se tomaron en respuesta al incidente, las perdidas por la interrupción de las actividades.

Revisión de la crisis:

1) Revisar si las acciones tomadas fueron efectivas al momento de contrarrestar la emergencia y si la utilización de recursos fue correcta.

2) Con que rapidez se obtuvo la disponibilidad de los recursos claves al momento de la gestión de riesgo.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- El desarrollo del diseño de un plan de contingencia informático permite conocer las vulnerabilidades latentes en infraestructura de red y servicios dentro de la institución, y pone a consideración de las autoridades los respectivos correctivos a fin de minimizar los riesgos.

- La identificación, evaluación de los riesgos y escenarios de contingencia en los activos considerados críticos para la institución se realizó en base a perfiles de amenazas, considerando el impacto ocasionado si llegan a materializarse dichos riesgos.

- Se definen recomendaciones para el control y administración de la red de la institución que permitan asegurar la operatividad de la red al mínimo de su capacidad con la finalidad de minimizar pérdidas económicas y de reputación.

- La formación de grupos de emergencia en el departamento informático permitirá mayor organización al momento de dar una respuesta ante una incorrupción de servicios.

- Con las estrategias propuestas para el mejoramiento de la seguridad de la información y la reducción de amenazas en los activos críticos se mejorará la eficiencia y administración de la red y los servicios proporcionados por el departamento de sistemas del GAD de Antonio Ante.

- Finalmente se concluye que, una institución provista de un plan de contingencia informático va a estar preparada para eventos inesperados, tomar medidas oportunas y soluciones eficientes.

RECOMENDACIONES:

- Según, la Ley de Control Interno para Organismos del sector público del Ecuador determina que: se debe realizar pruebas y evaluaciones del Plan de Contingencia de forma trimestral o mínimo 2 al año. Para determinar la aparición de nuevos riesgos, el grado de afectación y las respectivas medidas preventivas.

- Definir políticas y procedimientos de seguridad de la información, socializarlas y mantenerlas debidamente documentadas.

- Llevar registros de control de los procedimientos que se realizan dentro del departamento informático al momento de brindar soporte.

- Realizar campañas de sensibilización, dirigidas al personal para fomentar la cultura sobre la seguridad de la información y los peligros latentes con el avance de la tecnología.

- Se recomienda contar con un almacenamiento externo de la información crítica del municipio de Antonio Ante, con características parecidas al del equipo principal para evitar pérdidas de información en caso de un desastre.

- Realizar auditorías dentro del departamento para mejorar la eficiencia de los sistemas informáticos.

- Difundir con todo el personal los planes de contingencia para que sepan cómo actuar en caso de emergencia.

- Concientizar a los usuarios sobre deberes responsabilidades que tienen con la institución acerca de la seguridad de la información.

BIBLIOGRAFÍA

ACUERDO No. 166. (09 de 2013). ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN(EGSI). Quito, Ecuador.

Areitio, J. (2008). *Seguridad de la Información (Redes Informáticas y Sistemas de Información).* Madrid: Learminig paraninfo sa.

Contraloria General de la República. (2009). *Normas Tecnicas en Tecnologías de Información y Comunicaciones.* Obtenido de http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/Normas%20t%C3%A9c%20en%20TI%20y%20comunics.pdf

Correa García, C. A. (2009). *Seguridad de la Información*. Obtenido de http://info-segur.blogspot.com/2009/12/los-pilares-de-la-seguridad-de-la.html: http://info-segur.blogspot.com/2009/12/los-pilares-de-la-seguridad-de-la.html

Correa, J., Pons, J., & Moreira, M. (2010). *Políticas Educativas y Buenas Prácticas con TIC.* España: Grao de irif, s.l.

Gobierno Municipal de Antonio Ante. (Noviembre de 2014). *http://www.antonioante.gob.ec/web/?page_id=100*. Obtenido de http://www.antonioante.gob.ec/web/?page_id=100

Gómez López, J. (2012). *Seguridad en Sistemas Operativos Windows y GNU/Linux.* Madrid.

Hernández, I. J. (Diciembre de 2005). *Métodos y Políticas de Respaldo en Planes de Contingencia*. Obtenido de http://benjamin.davy.free.fr/Auditoria/ContingenciaybackupenSI.pdf

Herrero, R. (2010). Planes de Contingencia y su Auditoría.

Indra. (s.f.). Plan de Contingencias Informáticas.

Instituto del Mar de Perú. (2012). Plan de Contingencia Informático.

Instituto Nacional de Estadísticas y Censos . (s.f.). *Instituto Nacional de Estadísticas y Censos (INEC).* Obtenido de http://www.ecuadorencifras.gob.ec/wp-content/descargas/Manu-lateral/Resultados-provinciales/imbabura.pdf

Instituto Nacional de Tecnologías de la Comunicación(INTECO). (s.f.). *Guía Avanzada para la Gestion de Riesgos.* Obtenido de https://www.incibe.es/file/TnOIvX7kM5r8OY-S8r9Bmg

Katz, M. (2013). *Redes y Seguridad.* Alfaomega.

Lau C., O. (s.f.). Gestión de Riesgos de la Información.

Laudon, K., & Laudon, J. (2004). *Sistemas de Información Gerencial*. Obtenido de http://biblioteca.itson.mx/oa/dip_ago/introduccion_sistemas/p3.htm

Moncada, G. (Febrero de 2001). Guía Práctica para el Desarrollo de Planes de Contingencia de Sistemas de Información. Lima, Perú.

Nacional Institute of Standars and Technology. (mayo de 2010). Contingency Planning Guide for Federal Information Systems.

National Institute of Standards and Technology Special Publication 800-30. (s.f.). *Risk Management Guide for Information Technology Systems.* Obtenido de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

NTC-ISO 27005. (s.f.). *http://es.scribd.com/doc/124454177/ISO-27005-espanol.* Obtenido de http://es.scribd.com/doc/124454177/ISO-27005-espanol

NTE INEN-ISO/IEC 27002. (2009). TECNOLOGÍA DE LA INFORMACIÓN-TÉCNICAS DE LA SEGURIDAD-CÓDIGO DE PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. Quito, Ecuador.

Plan de Contingencia Sistemas Informaticos. (s.f.). *http://es.scribd.com/doc/43714047/Plan-de-contingencia-sistemas-informaticos#scribd.* Obtenido de http://es.scribd.com/doc/43714047/Plan-de-contingencia-sistemas-informaticos#scribd.

PLAN DE CONTINGENCIAS SISTEMAS DE INFORMACIÓN. (Diciembre de 2009). Bogota DC, Colombia.

Registro Oficial Nro. 039-CG. (14 de 12 de 2009). NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS. Quito, Ecuador.

SeguridadPC.NET. (Noviembre de 2014). *http://www.seguridadpc.net/gusanos.htm*. Obtenido de http://www.seguridadpc.net/gusanos.htm

SNGR/ECHO/UNISDR. (2012). Referencias Básicas para la Gestión de Riesgos. Quito, Ecuador.

Vergara, K. (s.f.). *Redes y Comunicaciones*. Obtenido de http://www.bloginformatico.com/topologia-de-red.php

ANEXOS

Anexo A: Encuesta dirigida a los 5 miembros que actualmente trabajan en el departamento de informática del GAD de Antonio Ante.

UNIVERSIDAD TÉCNICA DEL NORTE
ENCUESTA TÉCNICA

Con la finalidad de tener un criterio respecto a los activos de información más relevantes de la municipalidad se realizará la siguiente encuesta que permitirá conocer su valoración respecto a los activos más importantes y las seguridades que poseen para salvaguardarlos.

1. **¿Conoce Ud. la importancia de la seguridad de la información dentro de la institución?**

   La mayoría de los encuestados saben de la importancia de la seguridad de la información, sin embargo comentan que no se han tomado las medidas necesarias.

2. **¿Conoce Ud. Que dentro de la institución se da la debida importancia a la seguridad de la información por parte de los altos directivos?**

   La mayoría de los encuestados comentan que no se da la debida importancia a la seguridad de la información por parte de autoridades por falta de conocimiento.

3. **¿Cuáles son los activos más importantes para en GAD de Antonio Ante?**

Considere:

- Información
- Software
- Hardware
- Servicios
- Personas

Tabla 7.1 *Activos de mayor relevancia*

Autora*: Karina Méndez*

Activos Importantes	Razón
Información	Toda la información que se ingresa diariamente debe ser tratada de manera adecuada y sobre todo debe mantenerse protegida.
Servidores para almacenamiento de datos y de aplicaciones.	Se lo considera un activo muy importante para la organización pues en estos equipos se encuentra almacenada gran cantidad de información de la ciudadanía Anteña, además de los diferentes aplicativos que permite el desarrollo de las actividades diarias del municipio.
Sistemas de Recaudación y Facturación, Avalúos y Catastros, Agua Potables, contable-financiero.	Los tres primeros sistemas son de gran importancia debido a que son el ingreso económico principal para la municipalidad. El sistema contable financiero es también muy importante debido que a través de este ser realizan actividades económicas del municipio.
La red cableada y equipos de networking	Mediante estos activos se mantiene todas las comunicaciones con todos los departamentos del municipio, así como también se distribuye el uso de los diferentes servicios como internet, mensajería, consultas, etc.
Datacenter con los servicios de iluminación,	Es importante pues se necita contar con un lugar adecuado para el procesamiento de toda la información

Activos Importantes	Razón
sistemas de respaldo de energía eléctrica (UPS) aire acondicionado, sistemas de control de incendios.	que diariamente ingresa a través de los diferentes aplicativos de software; además todos los equipos de red que se encuentran almacenados en el interior deben estar bajo ciertas condiciones ambientales para su correcto desempeño
Otros: • Estaciones de trabajo de escritorio, portátiles, dispositivos de entrada y salida. • Equipos de multimedia como: impresoras, faxes, copiadores, plotter. • Aplicaciones de seguridad para los usuarios y copias de seguridad.		

4. **¿Cuáles cree Ud. que son los escenarios en que los activos mencionados anteriormente se verían amenazados?**

- Terremotos
- Incendios
- Filtraciones de agua
- Fallas o cortes de energía
- Daños físicos o lógicos en los equipos
- Daños físicos en la red de datos
- Sabotaje o robos de equipos.

5. **¿Qué impactos traería para la municipalidad si los escenarios se llegaran a ocurrir?**

Las consecuencias por la materialización de cualquiera de estos escenarios antes mencionados traerían pérdidas económicas, demora en la ejecución de las actividades diarias que realiza la institución, pérdida de credibilidad por parte de los usuarios, perdida de disponibilidad de los diferentes servicios que brinda la institución a la ciudadanía.

6. **¿Cuáles de los siguientes requerimientos de seguridad de la información son más importantes para cada uno de los activos de información?**

- Confidencialidad
- Integridad
- Disponibilidad
- Otros

Tabla 7.2 *Requerimientos de Seguridad*

Autora*: Karina Méndez*

ACTIVO	REQUERIMIENTO DE SEGURIDAD
Información	Disponible
Sistemas	Disponible, integridad
Red de datos y equipos de networking	Disponibilidad
Datacenter	Disponibilidad
servidores	Disponibilidad

7. **¿Del literal anterior indique cuál de los requerimientos es más importante para Ud.?**

   Se considera que el requerimiento de mayor importancia es la disponibilidad debido a que es una institución dedicada a la prestación de servicios por lo que considera necesario que siempre estén disponible todos los datos y aplicaciones dentro de la municipalidad.

8. **¿Conoce Ud. si existen políticas específicas, estrategias y procedimientos que sean únicos para los activos de mayor importancia para la institución? ¿Cuáles son?**

No existen políticas específicas para cada uno de los activos más importantes de la institución, únicamente se realizan procedimientos generales y no están documentados.

CONCLUSIÓN:

- Luego de haber realizado las encuestas se concluyó que la mayoría de los encuestados conocen la importancia de la seguridad de la información, pero que sin embargo se requiere mayor socialización para contar con mayor apoyo por parte de las autoridades para mejorar las salvaguardas que actualmente existen.

- Se definieron los activos de mayor relevancia para la institución y los respectivos requerimientos de seguridad para cada uno de los activos y los posibles escenarios de contingencia que pueden estar expuestos.

Anexo B: Entrevista realizada en el GAD de Antonio Ante al Jefe del departamento de Sistemas y Tecnología de Información.

UNIVERSIDAD TÉCNICA DEL NORTE
ENTREVISTA TÉCNICA

Objetivo: La presente entrevista tiene como finalidad conocer las posibles vulnerabilidades a las que se encuentra expuesta la institución desde el punto de vista del jefe del departamento.

Tabla 7.3 *Vulnerabilidades*

Autora*: Karina Méndez*

Indicadores	**Si**	**No**
Organización		
¿Se cuenta con suficiente personal en el departamento informático para cumplir con todos los procesos de seguridad de la información?		X
¿Existe falta de procesos de manera formal para la revisión de los derechos de acceso?	X	
¿Existen suficientes disposiciones respecto a la seguridad de la información?		X
¿Existen procedimientos de monitoreo de los recursos de procesamiento de la red?		X
¿Falta de auditorías regulares?	X	
¿Cuentan con procedimientos de identificación y evaluación de riesgos?		X
¿Manejan reportes sobre fallas incluidos en los registros de administradores y operador?		X
¿Es adecuada la respuesta al momento de dar mantenimiento a algún servicio?	X	
¿Existen procedimientos de control de cambios en la administración de la red?		X

¿Considera Ud. Que es adecuado el proceso de autorización para el acceso a la información?		X
¿Es adecuada la asignación de responsabilidades en la seguridad de la información?		X
¿Falta de planes de continuidad?	X	
¿Existen políticas sobre el uso de correo electrónico?		X
¿Existe control de inventarios de software, hardware y medios de almacenamiento de datos?	X	
¿Se realiza una documentación adecuada de registros en las bitácoras de administrador y operario?		X
¿Existe procedimientos para el manejo de información clasificada?		X
¿Existen procesos disciplinarios definidos en el caso de incidentes de seguridad de la información?		X
¿Existen políticas formales sobre la utilización de computadores portátiles y dispositivos móviles?		X
¿Existe control de los activos que se encuentran fuera de las instalaciones?		X
¿Falta de mecanismos de monitoreo establecido para las brechas en la seguridad?	X	
¿Los procesos de aprobación, adquisición e instalación de servicios para Tecnologías de Información en relación a seguridad son claros?	X	
¿En la Institución hay una cultura de apoyo a la seguridad informática?		X
Software		
¿Existe falta o insuficiencia de la prueba de software?		X
¿Existe un control sobre la instalación de software en los equipos de los usuarios?	X	
¿Existe conocimiento por parte de los usuarios los riegos a los que se exponen al no "terminación de sesión" cuando se abandona la estación del trabajo?		X
¿Existen pruebas de auditoria?		X
¿La interface de un software desarrollado es amigable con usuario?	X	
¿Es documentado cada proceso de desarrollo de software de forma adecuada?	X	
¿Existen controles para la habilitación de servicios?	X	

¿Falta de mecanismos de identificación y autentificación de usuario?	X	
¿Especificaciones incompletas o no claras para los desarrolladores?		X
¿Existe descarga y uso no controlado de software?		X
¿Se realiza un adecuado control de copias de seguridad de la información?	X	
Hardware		
¿Es suficiente el mantenimiento de los medios de almacenamiento?		X
¿Se cuenta con esquemas de reemplazo periódico, susceptibilidad a la humedad, polvo y suciedad?		X
¿Existe un control de cambio de configuración eficiente?		X
¿Existe susceptibilidad a las variaciones de tensión?	X	
¿Existe susceptibilidad a las variaciones de temperatura?		X
¿El almacenamiento de información cuenta con la suficiente protección?		X
¿Existe el debido cuidado en la disposición final de la información?	X	
Red		
¿Existe falta de pruebas del envió o la recepción de mensajes?	X	
¿Las líneas de comunicación se encuentran protegidas?		X
¿Él envió de tráfico sensible a través de la red se encuentra protegido?		X
¿Es eficiente la conexión de los cables de red?	X	
¿Existe problemas de transferencia de contraseñas sin autorización?	X	
¿Es adecuada la gestión de red?		X
¿Los puntos de usuario final se encuentran en buen estado?	X	
¿Conexión a la red pública se encuentra protegida?		X
Infraestructura		
¿Existe un control adecuado de acceso físico a las edificaciones y los recintos?	X	
¿Existen problemas con la red energética?	X	
¿Se cuenta con seguridad para la protección de la institución?	X	
¿La ubicación del cuarto de telecomunicaciones se encuentra en un área susceptible de inundación?		X
¿Los Sistemas de Computo son ubicados pensando en su protección ante posibles amenazas ambientales (incendio, inundación, terremoto)?	X	
¿El personal sabe que procesos de seguridad de la información se deben seguir en caso de una emergencia (incendio)?		X

Personal		
¿Ausencia del personal?		X
¿Existe falta de personal?	X	
¿Se cuenta con una persona encargada de la seguridad de la información?		X
¿Esta explícitamente definido la responsabilidad individual o compartida de seguridad sobre los procesos?	X	
¿Entrenamiento insuficiente de seguridad de la información?	X	
¿Uso incorrecto de software y hardware?		X
¿Falta de conciencia acerca de la seguridad en los usuarios?		X
Falta de mecanismos de monitoreo	X	
¿El trabajo del personal externo o de limpieza es supervisado?	X	
¿Falta de políticas para el uso correcto de los medios e comunicaciones y mensajería?	X	
¿Se vigila el comportamiento del personal de la del departamento informático a fin de evitar un posible fraude?	X	

RESULTADOS:

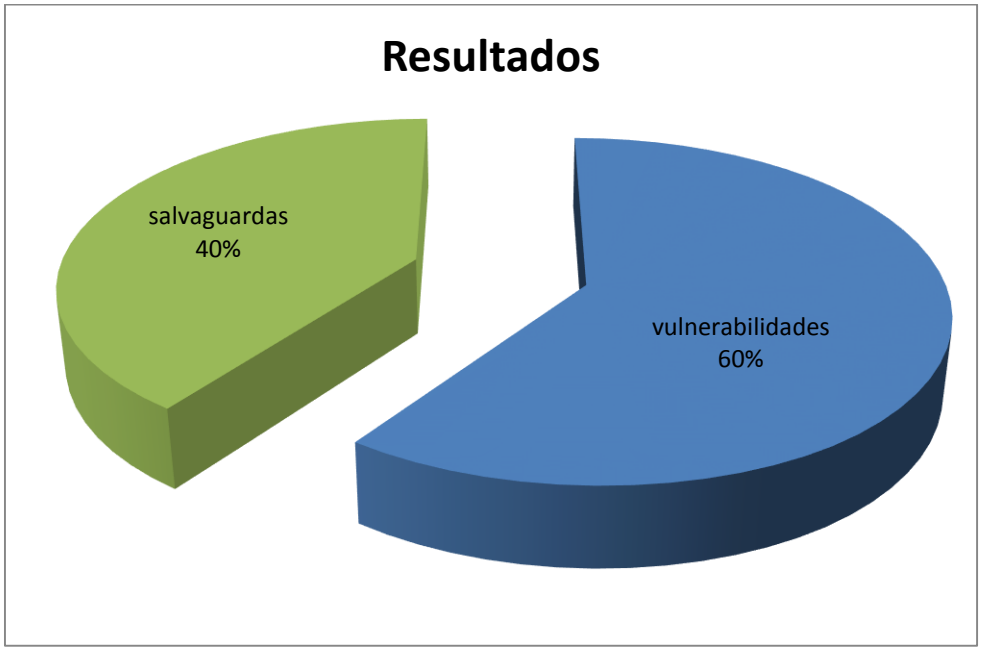


Figura 7.1 *Resultados de las vulnerabilidades existentes en le GAD de Antonio Ante*

Autor*: Karina Méndez*

Como podemos apreciar en la figura 7.1 el porcentaje de medidas de seguridad representa únicamente el 40% mientras que las vulnerabilidades existentes representa el 60% por lo que es de gran importancia poner a consideración de las autoridades los resultados obtenidos a fin de tomar medidas preventivas lo más pronto posible y evitar la materialización de posibles riesgos.

Anexo C: Vulnerabilidades encontradas en los servidores de la institución.

Las herramientas a utilizar se encuentran basadas en software libre y otras en versión evaluativo por lo que se detallará de manera general las vulnerabilidades encontradas.

El software utilizado en cada uno de los dispositivos es:

- Nmap
- CAIN Y ABEL V4.9.43
- Nessus

Pruebas realizadas:

- Escaneo de vulnerabilidades. Herramientas automatizadas
- Se escanearon 65535 puertos
- Denegación de servicios
- Man in the Middle

Servicios activos en cada uno de los servidores

PUERTO	SERVICIO
22	SSH
25	Smtp
53	Domain
80	http
110	Pop3
139	Netbios sesión service
143	Imap
433	http
443	https

1029	Often used by Microsoft DCOM services
2222	DirectAdmin administración de los sitios web
2179	Vmrdp
3128:	http-proxy
10000	Webmin (Administración remota web)
27000	VMWare servidor de licencias

VULNERABILIDADES ENCONTRADAS

Por motivos de confidencialidad se describirá de manera general las vulnerabilidades encontradas dentro de los servidores de la institución a continuación se enumeran algunos de los servicios y los posibles ataques que se pueden presentar.

SERVICIOS	**ATAQUES**
SSHield	Denegación de servicios
OpenSSH	Agotamiento de la conexión
Sendmail	Errores en la memoria
Oracle	Obtención de privilegios
SQL	Daños a través de códigos maliciosos
HTTP	Divulgación de información.
POP3	Ataques remotos con mensajes falsos
IMAP	Denegación de servicios
Microsoft Windows TLS / SSL	Accesos no autorizados a clientes AAA
	Ataques a la confidencialidad e integridad
	Inyección de SQL
	Ataques de envenenamiento de cache
	Inyección HTML
	atacantes man-in-te-mídele a servidores
	Ataques de fuerza bruta
	Suplantación de identidad

CONCLUSIÓN:

- Dentro de los servidores de la institución se observa gran número de vulnerabilidades que pueden ser explotadas a través de herramientas de software, y causan pérdidas o daños en la integridad de la información, falsificación de identidad, accesos no autorizados, etc., en los diferentes sistemas que se encuentran almacenados actualmente.

Anexo D: Cálculo del riesgo de los activos materiales

Tabla 7.4 *Cálculo del riesgo en los activos críticos*

Autora*: Karina Méndez*

Activo: Cuarto de telecomunicaciones	
Terremotos/Interrupción de servicios	*Riesgo*= 4*1*4 *Riesgo*= 16
Incendio/Interrupción de servicios	*Riesgo*= 4*1*4 *Riesgo*= 16
Fallas en hardware	*Riesgo*= 4*2*4 *Riesgo*= 32
Daños físicos UPS central	*Riesgo*= 4*1*3 *Riesgo*= 12
Activos: información	
Modificación o alteración de información	*Riesgo*= 4*3*3 *Riesgo*= 36
Ingeniería social	*Riesgo*= 4*3*2 *Riesgo*= 24
Accesos no autorizados	*Riesgo*= 4*4*2 *Riesgo*= 32
Activo: servidores	
Ineficiente conexión de los cables de red	*Riesgo*= 4*2*3 *Riesgo*= 24
Espionaje remoto	*Riesgo*= 4*2*3 *Riesgo*= 24
Fallas de software	*Riesgo*= 4*3*3 *Riesgo*= 36
Software malicioso (virus)	*Riesgo*= 4*4*4 *Riesgo*= 64

Personal mal intencionado	*Riesgo*= 4*2*3 *Riesgo*= 24
Activo: PCs Hardware y Software	
Fallas en el hardware	*Riesgo*= 3*4*2 *Riesgo*= 24
Fallas en el software	*Riesgo*= 3*2*1 *Riesgo*= 6
Utilización errónea de aplicaciones	*Riesgo*= 3*3*1 *Riesgo*= 9
Códigos maliciosos	*Riesgo*= 3*3*2 *Riesgo*= 18
Suplantación de identidad	*Riesgo*= 2.34*4*2 *Riesgo*= 18.67
Descuido o mal uso del servicio (correo electrónico)	*Riesgo*= 1*3*1 *Riesgo*= 3
Daños físicos en dispositivos de multimedia	*Riesgo*= 1*2*1 *Riesgo*= 2
Activo: Red de datos	
Errores físicos	*Riesgo*= 4*2*3 *Riesgo*= 24
Presencia de interferencias electromagnéticas	*Riesgo*= 4*3*1 *Riesgo*= 12
Interceptación de información	*Riesgo*= 4*3*3 *Riesgo*= 36
Accesos no autorizados	*Riesgo*= 4*4*3 *Riesgo*= 48
Equipos de Networking Humedad/interrupción de servicios	*Riesgo*= 4*2*3 *Riesgo*= 24
Equipos de Networking Desgaste/daños físicos	*Riesgo*= 4*2*3 *Riesgo*= 24
Modificación o alteración de la información	*Riesgo*= 4*3*3 *Riesgo*= 36

GLOSARIO

- **Privacidad**: Es la protección de los datos que una organización determina para los sistemas informáticos, el derecho a quien o quienes pueden tener acceso a la información y cuanta de la misma puede ser modificada o trasmitida.
- **Seguridad**: Son las medidas o controles que se toman para salvaguardar la integridad de la información cuando de manera no autorizada sean modificados o destruidos de manera ilegal.
- **Datos**: Cualquier tipo de información que se encuentre almacenada en los servidores o equipos personales dentro de la organización.
- **Base De Datos (BBDD):** Es el conjunto de datos que se encuentran relacionados entre sí y se encuentran almacenados, su procedencia es de diferentes fuentes o programas que las utilizan, entre algunas características de las bases de datos tenemos: nos brida seguridad a los datos, se encuentran almacenados de manera ordenada.
- **Ataques**: Evento que interfiere con el funcionamiento de los sistemas informáticos o el acceso no autorizado para obtener información sin contar con permisos suficientes.
- **Autenticación**: Es la confirmación de la identidad de un usuario mediante login y password, o la procedencia de la información mediante parámetros como quien lo elaboró la fecha de creación etc.
- **Golpes**: El quebrantamiento de las medidas de seguridad de la red o de los sistemas de información, cuando el atacante tiene éxito en el robo de información o de equipos.
- **Cifrado**: un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido.
- **Contraseña**: es una forma de autentificación que utiliza información para controlar el acceso hacia algún recurso.
- **Autorización**: son los permisos que se dan los recursos del sistema.
- **acceso**: es el resultado positivo de una autentificación, para que el acceso dure un tiempo predeterminado.
- **Firewall**: Es un mecanismo de seguridad contra ataques de Internet, filtra y controla todas las comunicaciones que pasan a través de la red.

- **Evento**: La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad
- **Contingencia**: evento que permite prevenir la materialización de un riesgo o amenaza que inhabilite las actividades de la institución.
- **Continuidad**: se refiere al requerimiento de la disponibilidad de la información y por tanto de los sistemas que la tratan y su entorno.
- **Desastre**: La interrupción prolongada de los recursos informáticos y de comunicación de una organización, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.
- **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **ISO** (International Standard Organization): Organización Internacional de Estandarización. Organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.
- **IEC** (International ElectrotechnicalCommission): Comisión Electrotécnica Internacional. organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas.
- **GAD** (Gobierno Autónomo Descentralizado)
- **INEN:** (Instituto Ecuatoriano de Normalización)
- **IT** (information technology) Tecnologías de Información son herramientas y métodos empleados para recabar, retener, manipular o distribuir información.
- **CNT EP.:** Corporación Nacional de Telecomunicaciones, Empresa Pública proveedora de soluciones de telecomunicaciones.
- **LAN** (Local Area Network): Red de área Local. Es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros.
- **OSI:** (Open System Interconnection) Es un modelo de interconexión de sistemas abiertos creado como marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

- **SCE:** Sistema de cableado estructurado.
- **WSUS** (Windows Server Update Services) gestiona la distribución de actualizaciones para el sistema operativo de Windows que se encuentran en la red.
- **WDS:** (Wireless Distribution System) Un Sistema de Distribución Inalámbrico que permite la interconexión inalámbrica de múltiples puntos de acceso en una red IEEE 802.11, sin la necesidad de un cable troncal que los conecte.
- **WEP:** (Wired Equivalent Privacy) es un estándar de seguridad de la red inalámbrica que permite cifrar la información que se transmite a nivel 2
- **WPA:** (Wi-Fi Protected Access) es un sistema para proteger las redes inalámbricas
- **PSK:** (Phase Shift Keying) modulación por desplazamiento de fase, es una forma de modulación angular que consiste en hacer variar la fase de la portadora entre un número de valores discretos.
- **IP:** (Internet Protocol): Protocolo de Internet no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos.
- **QoS:** (Quality of Service) Calidad de servicio es el conjunto de técnicas para manejar los recursos de red.
- **PPPoE:** (Point-to-Point Protocolover Ethernet): Protocolo Punto a Punto sobre Ethernet es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayoritariamente para proveer conexión de banda ancha mediante servicios de cable módem y xDSL
- **L2TP:** (Layer 2 TunnelingProtocol): utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado
- **PPTP:** (Point to Point TunnelingProtocol): Es un protocolo de comunicaciones desarrollado para implementar redes privadas virtuales.
- **MAC:** (media access control) Control de Acceso al medio es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red, conocida como dirección física.
- **DiffServ:** (Servicios diferenciados) proporcionan un método que garantiza la calidad de servicio en redes de gran tamaño, analiza varios flujos de datos en vez de conexiones únicas o reservas de recursos.
- **ToS:** (Type of Service) Campo de ocho bits en el encabezado del datagrama IP que identifica la prioridad relativa de un paquete respecto a otro y colocarlos en diferentes colas en caso necesario.

- **ACL:** (Access control list) lista de control de acceso especifica qué usuarios o procesos del sistema se concede el acceso a los objetos.
- **SSH:** (Secure Shell) Protocolo de conexión punto a punto que permite obtener acceso seguro a un computador remoto.
- **SSL:** (Secure Sockets Layer) Protocolo que garantiza seguridad y privacidad en comunicaciones de internet.
- **VLAN:** (Red de área local virtual) es un método de crear redes lógicamente independientes dentro de una misma red física.
- **LACP:** (Link Aggregation Control Protocol) métodos para combinar múltiples conexiones de red en paralelo con el fin de aumentar el rendimiento que una sola conexión podría sostener, y para proporcionar redundancia en caso de que uno de los enlaces falle.
- **SNMP:** (Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.
- **RADIUS:** (Remote Authentication Dial-In User Service) protocolo que permite la autenticación centralizada y la contabilización del acceso a la red.
- **MD5:** es un algoritmo de reducción criptográfico de 128 bits.
- **IGMP:** (Internet Group Management Protocol) protocolo de red que se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores.
- **IPv6**: (Protocolo de Internet versión 6) es una versión del protocolo Internet Protocol (IP), diseñada para reemplazar a IPv4, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.
- **HTTP:** (Hypertext Transfer Protocol): Protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la World Wide Web.
- **SNTP:** (Simple Network Time Protocol) permite sincronizar el reloj de software con el servidor de tiempo NTP
- **TFTP:** (Trivial file transfer Protocol) protocolo de transferencia muy simple se utiliza para transferir pequeños archivos entre ordenadores en una red.
- **DNS:** (Domain Name System) su función es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.
- **ICMP:** (Internet Control Message Protocol) sub protocolo de control y notificación de errores del Protocolo de Internet (IP). se usa para enviar mensajes de error,

indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

- **TCP/IP**: es un modelo de descripción de protocolos de red específicos que permiten que un equipo pueda comunicarse en una red, provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.
- **IPSec**: Estandar de seguridad de internet, proporcionan directivas generales basadas en un mecanismo de seguridad de la capa IP.
- **DHCP:** (Dynamic Host Configuration Protocol) protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.
- **DMZ:** (demilitarized zone) Zona desmilitarizada el propósito de una DMZ es agregar una capa adicional de seguridad al de una organización de la red de área local (LAN)
- **WAN:** (wide-area network): sistema de redes lan conectadas entre ellas.
- **RAM: (**Random Access Memory**):** es una memoria volátil, es decir, que pierde sus datos cuando deja de recibir energía
- **TELNET**: protocolo de red que nos permite viajar a otra máquina para manejarla remotamente.
- **MIMO**: (Multiple-input Multiple-output): Múltiple entrada múltiple salida, se refiere a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos.