



UNIVERSIDAD ESTATAL DE BOLÍVAR

**FACULTAD DE CIENCIAS ADMINISTRATIVAS GESTIÓN
EMPRESARIAL E INFORMÁTICA**

**ESCUELA DE SISTEMAS
CARRERA DE SISTEMAS**

**TRABAJO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL
TÍTULO DE INGENIERAS EN SISTEMAS COMPUTACIONALES**

TEMA:

**“IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD
INFORMÁTICA PARA FORTALECER LA CONFIDENCIALIDAD
DE LA INFORMACIÓN EN LA INTRANET DEL GOBIERNO
AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA”**

AUTORAS:

**BARRAGÁN PUENTE KARLA BELÉN
REA ROSERO JESSICA SILVANA**

DIRECTOR

ING. RODRIGO DEL POZO DURANGO

PARES ACADEMICOS

ING. DARWIN CARRIÓN

LIC. JUAN MANUEL GALARZA

GUARANDA, 2015.

II. DEDICATORIA

Dedico este trabajo de graduación a Dios por guiar mis pasos, por estar conmigo en todos los momentos buenos y malos y por haberme dado a mi familia quienes son la base fundamental en mi vida, demostrándome su altruismo, amor, paciencia, comprensión, tolerancia incondicional y su apoyo tanto emocional como económico para lograr cumplir con uno de los objetivos de mi vida.

Barragán Karla

Dedico este trabajo de graduación a Dios por mostrarme día a día con humildad, paciencia y sabiduría los pasos que debería seguir para cumplir con mis metas, permitiéndome haber llegado hasta este momento muy importante de mi formación profesional. A mis padres por haberme dado la vida, amor, comprensión y por ser las personas que me apoyaron incondicionalmente en toda mi vida académica dándome una carrera para mi futuro, proporcionándome sus palabras de aliento en los momentos más difíciles de mi vida y mi trayecto estudiantil. A toda mi familia por darme sus valiosos consejos fomentando mi educación y valores.

Rea Jessica.

III. AGRADECIMIENTO

Agradecemos a Dios por habernos acompañado espiritualmente a lo largo de nuestra carrera, por ser nuestra fortaleza en los momentos de debilidad ayudándonos a culminar una meta en nuestra vida

A nuestros padres por ser los pilares fundamentales de nuestra vida ya que son las personas que nos impulsaron a seguir adelante con sus buenos consejos y sabidurías brindándonos su apoyo para tener una excelente educación. Gracias por habernos brindado esta oportunidad de estudiar y adquirir un título profesional.

A nuestro Director por habernos guiado para realizar un buen Trabajo de Graduación brindándonos sus conocimientos para plasmarlos.

A nuestros Pares Académicos por ayudarnos a elaborar nuestro Trabajo de Graduación corrigiéndonos y compartiendo sus conocimientos para el desarrollo del mismo.

A los docentes por habernos compartido sus conocimientos y habernos formado profesionalmente para la vida laboral.

A esta prestigiosa Universidad por habernos abierto las puertas para formarnos como profesionales competentes, humanistas, líderes emprendedores y haber fortalecido nuestros valores.

Barragán Karla, Rea Jessica.

IV. CERTIFICACIÓN DEL DIRECTOR

CERTIFICO

Que, el trabajo de graduación titulado: **“IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA PARA FORTALECER LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA”** de la autoría de las estudiantes Barragán Puente Karla Belén y Rea Rosero Jessica Silvana, previo a la obtención del título de Ingenieras en Sistemas Computacionales, ha sido dirigido y asesorado por mi persona, bajo los lineamientos dispuestos por la Facultad, por lo que se encuentra listo para su defensa.

Guaranda 20 de Julio del 2015.



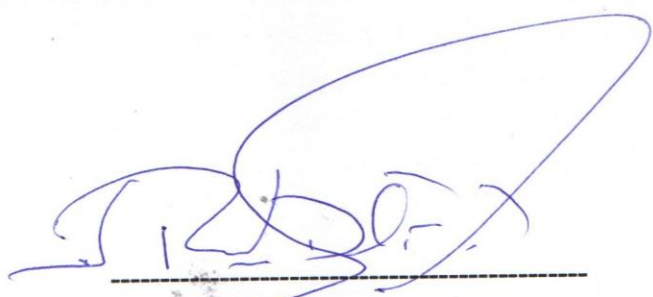
ING. RODRIGO DEL POZO DURANGO
DIRECTOR

IV. CERTIFICACIÓN DEL DIRECTOR

CERTIFICO

Que, el trabajo de graduación titulado: **“IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA PARA FORTALECER LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA”** de la autoría de las estudiantes Barragán Puente Karla Belén y Rea Rosero Jessica Silvana, previo a la obtención del título de Ingenieras en Sistemas Computacionales, ha sido dirigido y asesorado por mi persona, bajo los lineamientos dispuestos por la Facultad, por lo que se encuentra listo para su defensa.

Guaranda 20 de Julio del 2015.



ING. RODRIGO DEL POZO DURANGO
DIRECTOR



Dr. Guido Fierro Barragán
NOTARIO PUBLICO 1ro.
GUARANDA ECUADOR

V. AUTORÍA NOTARIADA



El presente Trabajo de Graduación: **IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA PARA FORTALECER LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA**, es un trabajo original, elaborado con esfuerzo y la dedicación de quienes conformamos el grupo de estudiantes de la Universidad Estatal de Bolívar; **BARRAGÁN PUENTE KARLA BELÉN**, con cédula 020213418-5, y **REA ROSERO JESSICA SILVANA**, con cédula 020209589-9 respectivamente, bajo consultas y referencias bibliográficas.

KARLA BARRAGÁN

JESSICA REA

DOY FE. Que esta copia fotográfica es EXACTA A SU ORIGINAL que me fue exhibida.



Dr. Guido Fierro Barragán
NOTARIO PÚBLICO 1ro.
GUARANDA ECUADOR

ESCRITURA PÚBLICA
DECLARACION JURADA

Señoritas KARLA BELEN BARRAGAN PUENTE y JESSICA SILVANA REA ROSERO

En la ciudad de Guaranda, Capital de la Provincia de Bolívar, República del Ecuador, hoy ~~es~~ MARTES DIECINUEVE DE MAYO DEL DOS MIL QUINCE, ante mí, Doctor GUIDO FABIAN FIERRO BARRAGAN, NOTARIO PÚBLICO PRIMERO DEL CANTÓN GUARANDA, comparecen las señoritas KARLA BELEN BARRAGAN PUENTE y JESSICA SILVANA REA ROSERO. Las comparecientes son de nacionalidad ecuatoriana, mayores de edad, de estado civiles solteras, capaces de contraer obligaciones, domiciliadas en esta ciudad y Cantón, a quienes de conocer doy fe en virtud de haberme exhibido sus cédulas de ciudadanía y papeletas de votación cuya copias adjunto a esta escritura. Advertido por mí el Notario de los efectos y resultados de esta escritura, así como examinado de que comparecen al otorgamiento de la misma sin coacción, amenazas, temor reverencial, ni promesa o seducción, juramentado en debida forma, prevenido de la gravedad del juramento, de las penas del perjurio y de la obligación que tiene de decir la verdad con claridad y exactitud, bajo juramento declaramos lo siguiente: " Previo a la obtención del título de INGENIERAS EN SISTEMAS COMPUTACIONALES, manifiestan que los criterios e ideas emitidas en el presente trabajo de investigación y graduación titulado "IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD INFORMATICA PARA FORTALECER LA CONFIDENCIALIDAD DE LA INFORMACIÓN DE LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA", son de nuestras exclusivas responsabilidad en calidad de autores. Es todo cuanto podemos declarar en honor la verdad." (Hasta aquí la declaración juramentada rendida por los comparecientes, la misma que queda elevada a escritura pública con todo el valor legal). Para el otorgamiento de esta escritura pública se observaron todos los preceptos legales del caso; y leída que le fue a los comparecientes íntegramente por mí el Notario, se ratifica en todo su contenido y firma conmigo en unidad de acto. Incorporo esta escritura pública al protocolo de instrumentos públicos, a mi cargo. De todo lo cual doy fe.-

Señorita. KARLA BELEN BARRAGAN PUENTE

Señorita. JESSICA SILVANA REA ROSERO

DOY FE: Que esta copia fotostática
ES EXACTA A SU ORIGEN.
que me fue exhibido.

Guaranda, 19 de Mayo del 2015



Dr. Guido Fierro Barragán
NOTARIO PÚBLICO 1ro. DEL CANTON GUARANDA

Doctor Guido Fabian Fierro Barragán
NOTARIO PÚBLICO PRIMERO DEL CANTÓN GUARANDA



Dr. Guido Fierro Barragán
NOTARIO PÚBLICO 1ro. DEL CANTON GUARANDA

VI. TABLA DE CONTENIDOS

DEDICATORIA	II
AGRADECIMIENTO	III
CERTIFICACIÓN DEL DIRECTOR	IV
AUTORÍA NOTARIADA	V
TABLA DE CONTENIDOS.....	VI
LISTA DE TABLAS Y GRÁFICOS.....	IX
LISTA DE ANEXOS	XII
RESUMEN EJECUTIVO	XIII
INTRODUCCIÓN	XIV
CAPITULO I.....	2
1.1 Tema	2
1.2 Antecedentes	4
1.3 Problema	6
1.4 Formulación del Problema.....	6
1.5 Justificación	7
1.6 Objetivos	9
1.6.1 General.....	9
1.6.2 Especificos.....	9
1.7 Marco Teorico.....	10
1.7.1 Marco Referencial	10
1.7.2 Marco Georeferencial	11
1.7.3 Marco Legal.....	11
1.7.4 Marco Conceptual.....	19
1.7.5 Teoría Científica	31
1.8 Hipótesis	34
1.9 Variables	34
1.9.1 Variable Independiente.....	34
1.9.2 Variable Dependiente	34
1.9.3 Operacionalización de Variables	35
1.10 Metodología	37

1.10.1 Métodos.....	37
1.11 Tipo de Investigación.....	37
1.11.1 Investigación de Campo.....	37
1.11.2 Investigación Descriptiva.....	37
1.11.3 Investigación Bibliográfica.....	38
1.12 Técnicas e Instrumentos para la obtención de datos.....	38
1.12.1 Entrevista.....	38
1.12.2 Observación Directa.....	38
1.13 Procesamiento de datos.....	39
CAPITULO II.....	40
2.1 Análisis e interpretación de los resultados.....	41
2.2 Selección de la Solución de Seguridad Informática.....	41
2.2.1 Servicio de Directorio.....	41
2.2.2 Estudio Comparativo entre Servicios de Directorio.....	42
2.3 Aplicación de las Técnicas e Instrumentos utilizados.....	55
2.4 Diagramas.....	63
2.5 Requisitos Tecnicos.....	65
2.6 Relación Beneficio – Costo.....	65
2.6.1 Detalle de Costos.....	67
2.6.2 Detalle de Ingresos.....	68
2.7 Conclusiones y Recomendaciones.....	70
2.7.1 Conclusiones.....	70
2.7.2 Recomendaciones.....	71
CAPITULO III.....	72
3.1 Aporte Teorico y / o Práctico.....	73
3.1.1 Comparación entre un Grupo de Trabajo y Controlador de Dominio.....	73
3.2 FASE 1: Levantamiento de información, analisis.....	74
3.2.1 Comprobación de la topología de red y conectividad actual.....	74
3.2.2 Analizar las seguridades perimetrales con las que cuenta la red.....	75
3.2.3 Definir estándares para la creación de usuarios.....	76
3.3 FASE 2: Implementación del directorio activo.....	95
3.3.1 Instalación del Servidor.....	95
3.3.2 Instalación del Servidor de Dominio.....	96
3.3.3 Configuración del Servidor DNS.....	106

3.3.4 Configuración inicial del directorio activo.....	111
3.3.5 Creación de usuarios y políticas de acuerdo al diseño original.....	112
3.3.6 Creación de Políticas de Grupo de Active Directory.....	115
3.3.7 Incorporación de computadores al directorio activo.....	118
3.3.8 Migración de perfiles de usuarios a la nueva estructura de dominio.....	120
CAPITULO IV.....	122
4.1 Pruebas de Funcionamiento y Seguridad.....	123
4.1.1 Pruebas de conectividad hacia y desde el servidor de directorio activo.....	123
4.2 Comprobación de Hipótesis.....	126
4.3 Conclusiones y Recomendaciones.....	128
4.3.1 Conclusiones.....	128
4.3.2 Recomendaciones.....	129
4.4 Bibliografía:.....	130

VII. LISTA DE TABLAS Y GRÁFICOS

TABLAS

Tabla 1 Puntaje para realizar la comparación.	42
Tabla 2 Estudio Comparativo 1 entre servicios de directorio.	45
Tabla 3 Estudio comparativo 2 entre servicios de directorio.	47
Tabla 4 Estudio comparativo entre los costos de los Servicios de Directorio.	49
Tabla 5 Comparación de costos entre los Servicios de Directorio.	50
Tabla 6 Cuadro estadístico de los Costos.	50
Tabla 7 Resultados obtenidos del Estudio Comparativo.	51
Tabla 8 Relación Beneficio \ Costo.	66
Tabla 9 Estructura de Costos.	67
Tabla 10 Detalle de Ingresos.	68
Tabla 11 Estándares para la creación de usuarios.	76
Tabla 12 Políticas de Grupo.	77
Tabla 13 Políticas de Grupo para Sistemas Informáticos.	77
Tabla 14 Usuarios de Administración General.	79
Tabla 15 Usuarios de la Dirección de Comunicación.	80
Tabla 16 Usuarios de Secretaría de Concejo.	81
Tabla 17 Usuarios de la Dirección Procuraduría Sindica.	82
Tabla 18 Usuarios de Auditoría Interna.	83
Tabla 19 Usuarios de C.C. Tambo del Libertador.	83
Tabla 20 Usuarios de la Dirección Administrativa.	85
Tabla 21 Usuarios de la Dirección de Talento Humano.	86
Tabla 22 Usuarios de la Dirección de Desarrollo Comunitario y Gestión Social.	88
Tabla 23 Usuarios de la Dirección de Gestión Ambiental.	90
Tabla 24 Usuarios de la Dirección de Planificación Territorial.	91
Tabla 25 Usuarios de la Dirección de Obras Públicas.	92
Tabla 26 Usuarios de la Unidad Municipal de Tránsito.	93
Tabla 27 Usuarios de Registro de la Propiedad.	94
Tabla 28 Lista de configuraciones.	121

Tabla 29 Control manual y Active Directory.....	127
---	-----

GRÁFICOS

Gráfico 1 Cuadro estadístico sobre Administración.	48
Gráfico 2 Cuadro estadístico de los Costos.....	50
Gráfico 3 Cuadro estadístico sobre los resultados obtenidos.....	52
Gráfico 4 Grupo de Trabajo vs Active Directory.....	54
Gráfico 5 Estructura de un Directorio Activo.	54
Gráfico 6 Plano de la Planta Baja del GAD Municipal.	63
Gráfico 7 Plano de la Planta Alta del GAD Municipal.	64
Gráfico 8 Pruebas de conectividad.....	74
Gráfico 9 Diagrama de la Seguridad Perimetral.	75
Gráfico 10 Panel de Inicio de Windows Server 2012.....	95
Gráfico 11 Cambiar Nombre de Equipo.	96
Gráfico 12 Administrador del Servidor.....	96
Gráfico 13 Servidor Destino.	97
Gráfico 14 Roles de Servidor.....	97
Gráfico 15 Selecciones de Instalación.	98
Gráfico 16 Promover a controlador de dominio.	98
Gráfico 17 Configuración de Implementación.....	99
Gráfico 18 Opciones de Controlador de Dominio.	99
Gráfico 19 Opciones Adicionales.	100
Gráfico 20 Rutas de Acceso.....	100
Gráfico 21 Opciones a configurar.	101
Gráfico 22 Requisitos Previos de Instalación.	101
Gráfico 23 Instalación Completada.....	102
Gráfico 24 Inicio de Sesión del Controlador de Dominio.....	102
Gráfico 25 Administrador del Servidor.....	103
Gráfico 26 Roles de Active Directory activados.....	103
Gráfico 27 Detalle de la configuración de controlador de dominio.....	104
Gráfico 28 Opción Usuarios y características de A.D.	104

Gráfico 29 Controlador de Dominio, usuarios y equipos.	105
Gráfico 30 Pantalla de Panel de Control Windows Server 2012.	106
Gráfico 31 Pantalla del Administrador DNS	106
Gráfico 32 Configuración Zona Directa.	107
Gráfico 33 Política de Caducidad Zonas.....	107
Gráfico 34 Configuración de Caducidad.....	108
Gráfico 35 Reenviadores.....	108
Gráfico 36 Editar Reenviadores.....	109
Gráfico 37 Habilitar Limpieza de registros obsoletos.	109
Gráfico 38 Seguridad.	110
Gráfico 39 Diagrama de la estructura lógica de Active Directory.....	111
Gráfico 40 Panel del Administrador del servidor.	112
Gráfico 41 Controlador del Dominio.....	112
Gráfico 42 Unidades Organizativas.	113
Gráfico 43 Creación de grupos.	113
Gráfico 44 Creación de usuarios.....	114
Gráfico 45 Unión de equipos al dominio.....	114
Gráfico 46 Administración de directivas de grupo.....	115
Gráfico 47 Prohibir propiedades de una conexión LAN.....	115
Gráfico 48 Opciones de Configuración.	116
Gráfico 49 Panel de inicio de Windows Server 2012 – Usuarios y Equipos.....	116
Gráfico 50 Usuario Administrador.....	117
Gráfico 51 Configuración de Hora de Inicio de Sesión.	117
Gráfico 52 Horas de Inicio de Sesión.	118
Gráfico 53 Cambio del nombre de equipo.	119
Gráfico 54 IP para el DNS Preferido.	119
Gráfico 55 Inicio de Sesión.....	124
Gráfico 56 Fondo de Escritorio.....	124
Gráfico 57 Propiedades de Ethernet.....	125
Gráfico 58 Número de conflictos IP.	126

VIII. LISTA DE ANEXOS

ANEXO N° 1 ESTRUCTURA ORGANIZACIONAL.....	134
ANEXO N° 2 MAPA GEOREFERENCIADO.....	135
ANEXO N° 3 ENTREVISTA DE SEGURIDADES INFORMÁTICAS.	136
ANEXO N° 4 FICHA DE OBSERVACIÓN DIRECTA.	139
ANEXO N° 5 CRONOGRAMA DE ACTIVIDADES.....	140
ANEXO N° 6 DETALLE DE COSTOS DE LA UNIDAD DE SISTEMAS INFORMÁTICOS.....	141
ANEXO N° 7 ESTUDIO DEL LOS EQUIPOS DEL RACK.....	143
ANEXO N° 8 CONFIGURACIÓN DEL SERVIDOR.	143
ANEXO N° 9 UNIÓN DE EQUIPOS AL DOMINIO.....	144

IX. RESUMEN EJECUTIVO

El objetivo de esta investigación es realizar la Implementación de una Solución de Seguridad Informática para fortalecer la confidencialidad de la información en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda.

Se realizó el análisis de servicios de directorio existentes tanto de software propietario: Active Directory y software libre: OpenLdap, estableciendo sus ventajas, desventajas y tomando en cuenta las necesidades establecidas por la Institución, optando por Active Directory que es una implementación de servicio de directorio en una red distribuida centralizada que facilita el control, la administración y la consulta de todos los elementos lógicos de una red como pueden ser usuarios, equipos e impresoras.

También se logró definir estándares para la creación de usuarios, estructura de permisos y políticas que fueron implementadas en el directorio activo.

Como resultado se obtuvo un servicio de directorio seguro y confiable debido a que se encuentra centralizando toda la información, gestionando todos los recursos de la red, autenticando y autorizando a los usuarios del GAD Municipal.

Se recomienda acrecentar medidas de seguridad que proporcionen protección a la infraestructura tanto física como lógica de la red de datos, debido a los grandes avances tecnológicos que traen consigo innumerables beneficios como también mayores inseguridades informáticas, provocando cualquier tipo de ataque no previsto afectando así el correcto funcionamiento del Gobierno Autónomo Descentralizado del Cantón Guaranda.

Es muy importante que el personal encargado de la administración del servicio de directorio implementado conozca acerca de su funcionamiento, debido a que puede existir la posibilidad de expansión de la Institución, y las nuevas Unidades Organizativas o equipos se puedan incluir fácilmente en la base de datos de Active Directory.

X. INTRODUCCIÓN

En el presente trabajo de investigación sobre la Implementación de una Solución de Seguridad Informática para fortalecer la confidencialidad de la información en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda, se ha desarrollado en IV capítulos, en los cuales se da a conocer la medida de seguridad que se implementará, mediante un análisis respectivo sobre las necesidades y los recursos con los que cuentan la Institución para adaptar la Solución de Seguridad que se ha definido.

Capítulo I, se presenta un enfoque sobre los antecedentes, los problemas analizados, la justificación para el desarrollo de la investigación, los objetivos planteados, el marco conceptual en donde se detalla todos los conceptos que abarca el presente trabajo haciendo mayor énfasis en la teoría científica que es donde se hace un preámbulo de la Solución de Seguridad y finalmente las metodologías de investigación empleadas.

Capitulo II, se realiza el análisis e interpretación de resultados obtenidos a través de las técnicas utilizadas para la obtención de datos, se establece el estudio comparativo entre los servicios de directorio como es de software propietario a Active Directory y software libre a OpenLdap, presentando sus ventajas y desventajas, estableciendo cual es el más adecuado según las necesidades presentadas, se determina la Relación Beneficio/Costo de la Implementación del Directorio Activo, obteniendo sus beneficios frente a sus costos el cual nos permite establecer los beneficios obtenidos para cubrir los costos empleados, determinado así la factibilidad del trabajo de investigación.

Capítulo III, se ejecuta las fases necesarias para la Implementación de la Solución de Seguridad Informática como el levantamiento de información sobre usuarios, equipos e impresoras del Gobierno Autónomo Descentralizado del Cantón Guaranda, las pruebas técnicas a la red y la definición de las políticas de seguridad que se implementó.

Capitulo IV, se encuentra la fase de pruebas como son de conectividad, de vulnerabilidad la corrección de errores y certificación de pruebas. La Solución de Seguridad funcionando correctamente.

CAPITULO I

1.1 TEMA

IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA PARA FORTALECER LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA.

1.2 ANTECEDENTES

La tecnología es considerada en la actualidad como una herramienta indispensable de trabajo por lo que presenta muchas facilidades en sus servicios, pero al mismo tiempo trae consigo innumerables problemas de seguridad que se deben solucionar para mantener protegida la información que se encuentra almacenada en los equipos del Establecimiento.

El Gobierno Autónomo Descentralizado del Cantón Guaranda, posee una infraestructura de red interna que permite la comunicación entre los diversos departamentos que forman parte de la Institución. Debido al avance tecnológico el Gobierno Autónomo Descentralizado del Cantón Guaranda con la ayuda de los estudiantes de la carrera de Ingeniería en Sistemas de la Universidad Estatal de Bolívar en el año 2010, optaron por implementar la infraestructura de red inalámbrica y una estructura de red LAN, solucionando así la falta de comunicación entre las diferentes dependencias internas y externas que forman parte de la institución.

Con el transcurso de los años los funcionarios del Gobierno Autónomo Descentralizado del Cantón Guaranda han ido adquiriendo mayores conocimientos tecnológicos, volviéndose vulnerable la configuración de los equipos motivo por el cual se presentó los siguientes problemas:

- Inseguridad en su información.
- Poca administración de usuarios.
- Manipulación por medio de los usuarios cambiando el nombre del Grupo de Trabajo.
- En el Grupo de Trabajo se da libre acceso a la información.
- Mala utilización de los recursos de la red.
- Conflictos de direccionamiento IP por manipulación de usuarios.
- Instalación de Programas o aplicaciones no autorizados.
- Infección de Virus.

Por lo tanto, se observó la necesidad de Implementar una Solución de Seguridad Informática, para dar respuesta a los problemas mencionados, con el propósito de

fortalecer la confidencialidad de la información, a la vez que la Institución cumple con sus fines laborales de manera exitosa.

1.3 PROBLEMA

El Gobierno Autónomo Descentralizado del Cantón Guaranda cuenta con una Red Interna que permite la comunicación entre las diferentes oficinas y departamentos que se encuentran dentro del edificio matriz, pero al carecer de Seguridades Informáticas a nivel de software se va acrecentando el nivel de inseguridad de la infraestructura de la intranet. Las redes informáticas crecieron en tamaño, en importancia y seguirán creciendo, así como también las amenazas potenciales en la seguridad por lo que es de suma importancia contar con una Solución de Seguridad Informática, ya que si la seguridad de la red se encuentra afectada, podría tener consecuencias nefastas, como es la pérdida de privacidad, el robo de información e incluso responsabilidad legal.

1.4 FORMULACIÓN DEL PROBLEMA

¿Cómo se podría ver afectada la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda al no contar con un Sistema de Seguridad Informática que proteja la información?

1.5 JUSTIFICACIÓN

La importancia de realizar esta investigación radica en la aplicación de los conocimientos que a lo largo de la carrera de Sistemas se han obtenido, y su ayuda oportuna en la Implementación de una Solución de Seguridad Informática, como una oportunidad para vincular el trabajo educativo con la sociedad, de esta manera colaborando con la Institución en la confidencialidad de la información con la que cuenta, para desempeñarse en sus funciones laborales de manera oportuna.

Con los antecedentes antes mencionados se considera imperativa la Implementación de una Solución de Seguridad Informática en la Red del Gobierno Autónomo Descentralizado del Cantón Guaranda, que brinde protección al bien máspreciado como es la información que es relevante como recurso clave en la gestión de las funciones de la Institución, ya que se podría ver afectada por posibles ataques que se pueden generar en Internet por terceras personas, además para prevenir cualquier tipo de extorsiones, fraudes y peor aún pérdidas irreparables como puede ser la eliminación total de una base de datos de información referente a cualquier aplicación que manejen en el establecimiento que sea de suma importancia para realizar su trabajo, creando la necesidad de realizar un estudio minucioso de las posibles alternativas de seguridad que ofrece el mercado e investigando los casos de éxito de otras instituciones obteniendo así la mejor de ellas para hacer frente a los problemas actuales que se han venido dando como también a los futuros problemas. La Implementación de ésta Solución de Seguridad Informática tiene novedad científica debido a la creciente demanda que existe en la utilización de tecnologías la cual trae consigo problemas de seguridades informáticas, por lo que nos vuelve cada día más vulnerables, es por ello que en nuestra investigación abarcaremos una medida de seguridad dando solución de manera rápida y eficiente a todos los problemas encontrados y que la Institución se encuentre preparada para hacer frente a los futuros ataques de seguridad que se podrían dar en la intranet.

El acceso no autorizado al contenido de cierta información hace que el proceso de administración, organización y control se vuelva vulnerable provocando pérdida de tiempo en las personas encargadas de resolver dichos problemas y creando ineficiencia en el rendimiento laboral de otros usuarios.

La pérdida recursos de la red presenta problemas al personal de trabajo de la Institución debido a que ciertos usuarios se encuentran ocupando ancho de banda ingresando en páginas de entretenimiento u otras actividades que no les corresponde afectando con su jornada laboral. Para lo cual es oportuna la Implementación de una medida de seguridad que nos permita resolver los problemas encontrados.

1.6 OBJETIVOS

1.6.1 GENERAL

Llevar a cabo la Implementación de una Solución de Seguridad Informática en el Gobierno Autónomo Descentralizado del Cantón Guaranda.

1.6.2 OBJETIVOS ESPECÍFICOS

- Analizar los problemas de Seguridad Informática en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda.
- Realizar el análisis de la Solución de Seguridad Informática para la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda.
- Aplicar el análisis planteado de Seguridad para la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda.
- Realizar el análisis Beneficio/Costo de la Solución de Seguridad Informática para la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda.
- Ejecutar la Fase de Pruebas en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda.

1.7 MARCO TEÓRICO

1.7.1 MARCO REFERENCIAL

La presente investigación se la realizará en el Gobierno Autónomo Descentralizado del cantón Guaranda, ubicado en la Convención de 1884 #1018 y García Moreno Provincia Bolívar, País Ecuador.

EVOLUCIÓN HISTÓRICA:

El Palacio Municipal está ubicado en las calles Convención de 1884 y García Moreno, en el centro de la ciudad, frente al Parque el Libertador. La existencia del Palacio Municipal aproximadamente data desde el año 1736, en que llegó a la ciudad de Guaranda el 18 de Mayo la Misión Geodésica Francesa.

Esta casa fue propiedad en primera instancia del señor general José de Unda y Luna, posteriormente pasó a ser propiedad de Don Frenando Echeandía y es ahí donde nació uno de los Próceres guarandeños, Don Manuel de Echeandía.

Fue vivienda y oficina del Corregidor, en su torreón se observa un hermoso reloj que fue puesto en funcionamiento el 14 de Enero 1929, siendo Presidente del Concejo Municipal el Sr. José H Gonzáles Pozo.

En su interior podemos apreciar sus balcones de madera tallada; el patio interior con su piso de piedra sellar, decorado con huesos de vértebras de animales y en el centro una pileta de piedra; en un lugar destacado del patio encontramos una de las imprentas tipográficas más antiguas del país, y su balcón exterior principal con una llamativa vista hacia el Parque Central.

ESTRUCTURA ORGÁNICA

Anexo N° 1.

1.7.2 MARCO GEOREFERENCIAL

Longitud: 79° 0' 4"

Latitud: -1° 35' 30"

Sistema de Referencia: WGS84 Zona 17 Sur.

Anexo N° 2.

1.7.3 MARCO LEGAL

DERECHOS DE PROPIEDAD INTELECTUAL

LEGISLACION NACIONAL - ECUADOR

Ley de la Propiedad Intelectual

Sección V

Disposiciones Especiales sobre ciertas Obras

Parágrafo Primero

De los Programas de Ordenador

Art. 28. Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.

Art. 29. Es titular de un programa de ordenador, el productor, esto es la persona natural o jurídica que toma la iniciativa y responsabilidad de la realización de la obra. Se considerará titular, salvo prueba en contrario, a la persona cuyo nombre conste en la obra o sus copias de la forma usual.

Dicho titular está además legitimado para ejercer en nombre propio los derechos morales sobre la obra, incluyendo la facultad para decidir sobre su divulgación.

El productor tendrá el derecho exclusivo de realizar, autorizar o prohibir la realización de modificaciones o versiones sucesivas del programa, y de programas derivados del mismo.

Las disposiciones del presente artículo podrán ser modificadas mediante acuerdo entre los autores y el productor.

Art. 30. La adquisición de un ejemplar de un programa de ordenador que haya circulado lícitamente, autoriza a su propietario a realizar exclusivamente:

Una copia de la versión del programa legible por máquina (código objeto) con fines de seguridad o resguardo;

Fijar el programa en la memoria interna del aparato, ya sea que dicha fijación desaparezca o no al apagarlo, con el único fin y en la medida necesaria para utilizar el programa; y,

Salvo prohibición expresa, adaptar el programa para su exclusivo uso personal, siempre que se limite al uso normal previsto en la licencia. El adquirente no podrá transferir a ningún título el soporte que contenga el programa así adaptado, ni podrá utilizarlo de ninguna otra forma sin autorización expresa, según las reglas generales.

Se requerirá de autorización del titular de los derechos para cualquier otra utilización, inclusive la reproducción para fines de uso personal o el aprovechamiento del programa por varias personas, a través de redes u otros sistemas análogos, conocidos o por conocerse.

Art. 31. No se considerará que existe arrendamiento de un programa de ordenador cuando éste no sea el objeto esencial de dicho contrato. Se considerará que el programa es el objeto esencial cuando la funcionalidad del objeto materia del contrato, dependa directamente del programa de ordenador suministrado con dicho objeto; como cuando se arrienda un ordenador con programas de ordenador instalados previamente.

Art. 32. Las excepciones al derecho de autor establecidas en los artículos 30 y 31 son las únicas aplicables respecto a los programas de ordenador.

Las normas contenidas en el presente Parágrafo se interpretarán de manera que su aplicación no perjudique la normal explotación de la obra o los intereses legítimos del titular de los derechos.¹

¹ Área de Libre Comercio de las Américas. (2015). Área de Libre Comercio de las Américas. Recuperado de: <http://www.ftaa-alca.org/intprop/natleg/ecuador/L320b.asp#11t1c1s5>

LEY ORGÁNICA DE TELECOMUNICACIONES Y DE SERVICIOS POSTALES

Artículo 1.- Objeto.- La presente ley tiene por objeto establecer el régimen general aplicable a las telecomunicaciones, el establecimiento y explotación de redes para la prestación de servicios públicos de telecomunicaciones incluyendo radiodifusión sonora y televisión, el uso del espectro radioeléctrico, así como las potestades del Estado para su dirección, regulación y control, el régimen de derechos y deberes de los operadores, protección de usuarios, con el fin de garantizar el acceso universal a los servicios de telecomunicaciones y tecnologías de información y comunicación, con calidad, continuidad y tarifas equitativas; a fin de promover el desarrollo tecnológico del país y el avance efectivo hacia la Sociedad de la Información y del Conocimiento.

Artículo 2.- Objetivos Generales.- Los objetivos generales de esta Ley son:

1. Regular, administrar, controlar y gestionar la prestación de los servicios públicos de telecomunicaciones y el acceso a las tecnologías de la información.
2. Favorecer el desarrollo eficiente del sector de telecomunicaciones y el acceso universal a las tecnologías de la información y comunicación y, que todos los ciudadanos tengan derecho a una comunicación libre, intercultural, incluyente, diversa y participativa.
3. Promover la evolución tecnológica del país, a través del desarrollo de redes y servicios de telecomunicaciones, a fin de favorecer la masificación del uso de las tecnologías de información y comunicación y, el avance hacia la Sociedad de la Información y Conocimiento.
4. Garantizar a todos los ciudadanos el derecho a la comunicación y, en consecuencia, el acceso igualitario a redes y servicios de telecomunicaciones, de forma prioritaria en zonas urbano-marginales o rurales.
5. Promover programas y proyectos de investigación y desarrollo, conjuntamente con entes públicos y/o privados.
6. Impulsar el desarrollo y la convergencia de servicios.

7. Promover y controlar la competencia sana y leal entre los operadores de servicios de telecomunicaciones, en atención con el interés público y, colectivo o general y, las políticas públicas.
8. Promover y supervisar el uso efectivo y eficiente de los recursos limitados o escasos de telecomunicaciones y, garantizar la adecuada gestión y administración de tales recursos, evitando el acaparamiento.
9. Regular la delegación del Estado para la prestación de los servicios públicos de telecomunicaciones a empresas mixtas, privadas y a las de economía popular y solidaria.
10. Impulsar la participación protagónica del país en organizaciones o actividades nacionales e internacionales de telecomunicaciones y tecnologías de la información y comunicación, a fin de favorecer la adopción de políticas internas y realizar aportes en el ámbito internacional.
11. Fomentar la inversión nacional e internacional, pública o privada, para el desarrollo de las telecomunicaciones.
12. Controlar que los servicios de telecomunicaciones se presten bajo los principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad.
13. Controlar que las empresas prestadoras de servicios de telecomunicaciones cumplan con la normativa legal vigente y las obligaciones asumidas por el otorgamiento de títulos habilitantes.²

² Ley Orgánica de Telecomunicaciones y de Servicios Postales.

LEY DE COMERCIO ELECTRÓNICO

Título V

DE LAS INFRACCIONES INFORMÁTICAS

Capítulo I

DE LAS INFRACCIONES INFORMÁTICAS

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"**Art.-** El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art.- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."

Art. 59.- Sustitúyase el Art. 262 por el siguiente:

"**Art. 262.-** Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo."

Art. 60.- A continuación del Art. 353, agréguese el siguiente artículo innumerado:

"**Art.- Falsificación electrónica.-** Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

- 1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
- 2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
- 3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo."

Art. 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"**Art.- Daños informáticos.-** El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Art.- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.".

Art. 62.- A continuación del Art. 553, añádanse los siguientes artículos innumerados:

"**Art.-** Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art.- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:

"..... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos."³

³ Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos (Ley No. 2002-67).

1.7.4 MARCO CONCEPTUAL

1.7.4.1 Acceso no autorizado

La persona que de ordinario no tiene derecho a usar los recursos de la compañía hace uso de ellos.⁴

1.7.4.2 Amenaza

“A la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que de tener la oportunidad atacarían al sistema que de tener daños aprovechándose de su nivel de vulnerabilidad.”⁵

1.7.4.3 Ataque Informático

“Es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático.”

- **Actividades de reconocimiento de Sistema.**

Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando para ello un escaneo de puertos para determinar qué servicios se encuentran activos bien un reconocimiento de versiones de Sistemas Operativos y aplicaciones, por citar dos de las técnicas más conocidas. (Vieites, 2011)

- **Análisis del tráfico.**

Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los "sniffers. (Vieites, 2011)

⁴ Raymond McLeod, Jr. (2010). Sistema de información gerencial. México. Printed

⁵ Vieites Gómez, A. (2011). Enciclopedia de la Seguridad Informática. México. AlfaOmega

- **Conexión no autorizada a equipos y servidores.**

Existen varias posibilidades para establecer una conexión no autorizada a otros equipos y servidores, entre las que podríamos destacar las siguientes:

- Violación de sistemas de control de acceso.
- Explotación de "agujeros de seguridad" {"exploits"}.
- Utilización de "puertas traseras" ("backdoors"), conjunto de instrucciones no documentadas dentro de un programa o sistema operativo, que permiten acceder o tomar el control del equipo saltándose los controles de seguridad.

Utilización de "rootkits", programas similares a los troyanos, que se instalan en un equipo reemplazando a una herramienta o servicio legítimo del sistema operativo. (Vieites, 2011)

- **Consecuencias de las conexiones no autorizadas a los sistemas informáticos.**

Las conexiones no autorizadas a los sistemas informáticos pueden acarrear graves consecuencias para la organización afectada por este tipo de ataques e incidentes, entre las que podríamos destacar las siguientes:

- Acceso a información confidencial guardada en un servidor. Los atacantes incluso podrían tener acceso a datos y ficheros que habían sido "borrados" del sistema.
- Utilización inadecuada de determinados servicios por parte de usuarios no autorizados, suponiendo una violación de los permisos establecidos en el sistema.
- Transmisión de mensajes mediante un servidor de correo por parte de usuarios ajenos a la organización ("mail relaying"). Esto podría facilitar el reenvío masivo de mensajes de spam a través de un servidor SMTP configurado de forma inadecuada.

Utilización de la capacidad de procesamiento de los equipos para otros fines, como, por ejemplo, para tratar de romper las claves criptográficas de otros sistemas. (Vieites, 2011)

- **Detección de Vulnerabilidades en el Sistema.**

Este tipo de ataques tratan de detectar y documentación las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como "exploits"). (Vieites, 2011)

- **Modificación del contenido y secuencia de los mensajes transmitidos.**

En estos ataques los intrusos tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque). También se conocen como "ataques de repetición" ("replay attacks"). (Vieites, 2011)

- **Modificaciones del tráfico y las tablas de enrutamiento.**

Los ataques de modificación del tráfico y de las tablas de enrutamiento persiguen desviar los paquetes de datos de su ruta original a través de internet, para conseguir, por ejemplo, que atravesen otras redes o equipos intermedios antes de llegar a su destino legítimo, para facilitar de este modo las actividades de interceptación de datos. (Vieites, 2011)

- **Robo de información mediante la interceptación de mensajes.**

Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.⁶ (Vieites, 2011)

1.7.4.4 Base de Datos

“Es un conjunto de datos estructurados y definidos a través de un proceso específico, que busca evitar la redundancia, y que se almacenará en algún medio de almacenamiento masivo, como un disco”.⁷

⁶ Vieites Gómez, A. (2007). Enciclopedia de la Seguridad Informática. México. AlfaOmega

⁷ Reinoso, E. J; Maldonado, C. A; Muñoz, R. Damiano, L. E y Abrutsky, M. A. (2012).Base de Datos. Argentina. AlfaOmega Grupo Editor Argentina S.A

1.7.4.5 Clasificación de Intrusos

- **Crackers.-** Son individuos que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.
- **“Creadores de Virus y Programas dañinos.-** Son expertos informáticos que pretenden demostrar sus conocimientos construyendo virus u otros programas dañinos, que distribuyen hoy en día a través de internet para conseguir una propagación exponencial y alcanzar así una mayor notoriedad.”
- **“Hackers.-** Son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimiento de los entresijos de internet, pero no pretenden provocar daños en estos sistemas.”
- **“Lamers.-** Son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos y que los utilizan sin tener conocimientos técnicos de cómo funcionan.”
- **Phreakers.** Son individuos que manipula la red telefónica para que realice una función que no está permitida. Un objetivo común del phreaking es ingresar en la red telefónica, por lo general a través de un teléfono público, para realizar llamadas de larga distancia gratuitas.
- **“Piratas Informáticos.-** Son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.”
- **Sniffers.-** Son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como internet.
- **Spammers.-** Son individuos que envían grandes cantidades de mensajes de correo electrónico no solicitado. Por lo general, los spammers utilizan virus para tomar control de computadoras domésticas y utilizarlas para enviar sus mensajes masivos.⁸

⁸ Vieites Gómez, A. (2011). Enciclopedia de la Seguridad Informática. México. AlfaOmega

1.7.4.6 Derecho de autor

Es el sistema jurídico por el cual se concede a los autores derechos morales y patrimoniales sobre sus obras, en cumplimiento a lo dispuesto por la Constitución del Ecuador y la Declaración Universal de los Derechos Humanos. Las obras protegidas comprenden, entre otras, las siguientes: novelas, poemas, obras de teatro, periódicos, programas informáticos, bases de datos, películas, composiciones musicales, coreografías, pinturas, dibujos, fotografías, obras escultóricas, obras arquitectónicas, publicidad, mapas, dibujos técnicos, obras de arte aplicadas a la industria. El Derecho de Autor dura la vida del creador más 70 años después de su muerte. El uso de una obra sin la autorización expresa de su autor es considerado ilegal y puede ser castigado con multas e incluso prisión.⁹

1.7.4.7 Extranet

“Es una mezcla de internet e intranet, y sirve para definir a una red privada virtual que utiliza Internet como medio de transporte de la información entre sus propios nodos.”¹⁰

1.7.4.8 Firewall

“Un firewall (cortafuegos en español) es un sistema de seguridad que protege el equipo y que controla los datos que se transmiten desde el Equipo a Internet y viceversa. De esta manera, le sirve de defensa contra personas o programas (virus y gusanos) que intentan acceder al equipo sin tener autorización. El firewall se encuentra activado por defecto, si un programa debe recibir datos provenientes de internet, le aparecerá una alerta y podrá indicar si autoriza o no la conexión”.¹¹

1.7.4.9 Información

Es un conjunto de datos que tienen relación entre sí, considerado hoy en día como el recurso más valioso de una Organización que permite su correcto funcionamiento.

⁹ Instituto Ecuatoriano de la Propiedad Intelectual. (2015). Instituto Ecuatoriano de la Propiedad Intelectual. Recuperado de <http://www.propiedadintelectual.gob.ec/que-son-derechos-de-autor-y-derechos-conexos/>

¹⁰ Pérez, A. G. (2011). Internet lo Básico que debe saber. España. StarkBook Editorial

¹¹ Daburon B. (2010). Windows 7. España: Ediciones ENI

1.7.4.10 Introducción en el Sistema de Malware.

- **Denegación del Servicio.**

Los ataques de Denegación de Servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticos, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios. Para ello, existen varias posibilidades de conseguirlo:

- Ejecutar algunas actividades que produzcan un elevado consumo de los recursos de las máquinas afectadas: procesador, memoria y/o disco duro, provocando una caída en su rendimiento. Entre ellas podríamos citar el establecimiento de múltiples conexiones simultáneas, el envío masivo de ficheros de gran tamaño o los ataques lanzados contra los puertos de configuración de los routers.
- Provocar el colapso de redes de ordenadores mediante la generación de grandes cantidades de tráfico, generalmente desde múltiples equipos.
- Transmisión de paquetes de datos malformados o que incumplan las reglas de un protocolo, para provocar la caída de un equipo que no se encuentre preparado para recibir este tipo de tráfico malintencionado.
- Sabotajes mediante routers "maliciosos", que se encarguen de proporcionar información falsa sobre tablas de enrutamiento que impidan el acceso a ciertas máquinas de la red.
- Activación de programas "bacteria", cuyo objetivo es replicarse dentro de un sistema informático, consumiendo la memoria y la capacidad del procesador hasta detener por completo al equipo infectado. (Vieites, 2011)

- **Fraudes, Engaños y Extorsiones.**

“Los fraudes y estafas financieros a través de Internet se han hecho muy frecuentes en estos últimos años. Se utiliza el término de "phishing" para referirse al tipo de ataques que tratan de obtener los números de cuenta y las claves de acceso a servicios bancarios, para realizar con ellos operaciones fraudulentas que perjudiquen a los legítimos propietarios. Generalmente, se utilizan páginas Web

falsas que imitan a las originales de los servicios bancarios que pretenden suplantar.

Estos datos podrían ser utilizados para realizar ataques del tipo "salami", consistentes en la repetición de gran cantidad de pequeñas operaciones, como transferencias bancarias de importe reducido, que podrían pasar inadvertidas a nivel individual, pero que en conjunto ocasionan un importante daño económico. (Vieites, 2011)

- **Virus Informáticos Troyanos y Gusanos**

Entendemos por código malicioso o dañino ("malware") cualquier programa, documento o mensaje susceptible de causar daños en las redes y sistemas informáticos. Así, dentro de esta definición estarían incluidos los virus, troyanos, gusanos, bombas lógicas, etcétera. (Vieites, 2011) ¹²

1.7.4.11 Intranet

Es una red de área local, es decir, es de uso exclusivo de una determinada organización, por lo que solamente los equipos informáticos de esta pueden acceder a ella; la intranet es una herramienta que puede ayudar en la comunicación, y lo que es mejor, con un coste muy bajo. ¹³

1.7.4.12 Protocolo

Es un conjunto de reglas para un tipo de comunicación determinada. ¹⁴

1.7.4.13 Redes

“También conocidas como redes de comunicación de datos o de transmisión de datos, representan el resultado lógico de la evolución de dos de las ramas científicas y tecnológicas más importantes de la civilización moderna: las tecnologías de las computadoras y de las telecomunicaciones.” ¹⁵

¹² Vieites Gómez, A. (2011). Enciclopedia de la Seguridad Informática. México. AlfaOmega

¹³ Sanchez Estella, O. y Herrero Domingo, R. (2014). Aplicaciones básicas de ofimática. España. Paraninfo

¹⁴ Anderruthy, J. Gaumé, S. (2011). Mantenimiento y Reparación de un Pc en red. Barcelona. ENI

¹⁵ Olifer, N. y Olifer, V. (2009). Redes de Computadoras. México. Litográfica Ingramex

1.7.4.14 Servidor

Es aquel equipo que no necesariamente debe tener características superiores, para brindar servicios a los diferentes clientes (nodos de la red) permitiéndoles realizar sus funciones de manera eficiente.

1.7.4.15 Tipos de Redes

- Según el tamaño de la red, distinguimos Lan, Man, y Wan
 - LAN: red de área local se conectan varios equipos con un alcance limitado por los cables o por la potencia de las antenas inalámbricas.
 - MAN: red área metropolitana. Red formada por un conjunto de redes LAN en las que se conectan equipos.
 - WAN red de área amplia interconectan equipos en un entorno muy amplio, como un país usando la red telefónica

- Según el medio físico que utilicen para su conexión nos encontramos con diferentes tipos de redes en función de del medio físico utilizado para transmitir la información así tenemos: (Enrique José Reinoso, Damiano, & Abrutsky, 2012)
 - Redes alámbricas: que utilizan los cables que serán de pares trenzados y normalmente con conectores RJ45, así utilizaremos cables paralelos para conectar el ordenador al switch y cables cruzados para conectar ordenadores entre sí
 - Redes inalámbricas: La conexión inalámbrica se realiza mediante las ondas electromagnéticas que se propagan entre una antena emisora y una receptora. Para conectar un ordenador a una red wifi es necesario por tanto una antena receptora y el software adecuado.

- Según topología de la red:
 - Bus o lineal: tiene un cable central con derivaciones.

- Estrella: todos los ordenadores están conectados a un concentrador o Hub central y no están conectados entre sí.
- Anillo: todos se conectan describiendo un anillo, la información llega a un ordenador si no la necesita la pasa al siguiente.
- Malla: cada ordenador está conectado al resto de los equipos con más de un cable. ¹⁶

1.7.4.16 Vulnerabilidad

“Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.” ¹⁷

1.7.4.17 Tipos de Vulnerabilidades

▪ Vulnerabilidades que afectan a equipos

- Cámaras web y servidores de vídeo

Los fallos detectados en este tipo de dispositivos permitirían el control remoto de la cámara por parte de un usuario malicioso o la ejecución de un ataque de Denegación de Servicio contra el dispositivo vulnerable. (Vieites, 2011)

- Router y cables-módems

Las vulnerabilidades detectadas en estos dispositivos permiten acceder a los equipos y redes conectadas por los routers y módems afectados, o facilitan la ejecución de ataques de Denegación de Servicio que tengan como consecuencia el bloqueo total o parcial de las redes de ordenadores conectadas a través de estos dispositivos. (Vieites, 2011)

¹⁶ Garrido Herrera,P.M; López Caballero,M.E; Zarandieta Morán, F. (2009). Tipos de redes de ordenadores. Redes LAN, MAN y WAN. Clasificación. Tecnología Interactiva 3 E.S.O. Recuperado de http://contenidos.educarex.es/mci/2009/43/TEMA7/tipos_de_redes_de_ordenadores_redes_lan_man_y_wan_clasificacin.html

¹⁷ Roldán Santana, C. (2012, 09 de Septiembre). Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. [CODEJOBS Aprende a programar].Recuperado de: <http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#sthash.y6IIwI9F.dpbs>

- **Vulnerabilidades en otros equipos conectados a una red: impresoras, escáner, faxes, fotocopiadoras.**

Las vulnerabilidades en este tipo de dispositivos podrían tener como consecuencia la sustracción de información reservada, la Denegación del Servicio para los usuarios de los dispositivos afectados, el cambio de configuración para provocar un funcionamiento incorrecto, etc. (Vieites, 2011)

- **Vulnerabilidades que afectan a aplicaciones informáticas como:**

Sistemas Operativos, Servidores y Bases de Datos

Navegadores

Aplicaciones ofimáticas como Word y Excel. (Vieites, 2011)¹⁸

1.7.4.18 Seguridad Informática

Se puede definir la Seguridad Informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema. (Vieites, 2011)

1.7.4.19 Servicios de seguridad de la información

- **Auditabilidad**

El servicio de auditabilidad o trazabilidad permite registrar y monitorizar la utilización de los distintos recursos del sistema por parte de los usuarios que han sido previamente autenticados y autorizados. De este modo, es posible detectar situaciones o comportamientos anómalos por parte de los usuarios, además de llevar un control del rendimiento del sistema (tráfico cursado, información almacenada y volumen de transacciones realizadas, por citar algunas de las más importantes). (Vieites, 2011)

¹⁸ Vieites Gómez, A. (2011). Enciclopedia de la Seguridad Informática. México. AlfaOmega

- **Autenticación**

La autenticación garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje. Asimismo, también podemos hablar de la autenticidad de un equipo que se conecta a una red o intenta acceder a un determinado servicio. (Vieites, 2011)

- **Autorización (control de acceso a equipos y servicios)**

Mediante el servicio de autorización se persigue controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos por el sistema informático, una vez superado el proceso de autenticación de cada usuario. Para ello, se definen unas Listas de Control de Acceso (ACL) con la relación de usuarios y grupos de usuarios y sus distintos permisos de acceso a los recursos del sistema. (Vieites, 2011)

- **Confidencialidad**

Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático sólo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, éstas no podrán acceder al contenido del mensaje original. Por lo tanto, este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de backup y/o de los datos transmitidos a través de redes de comunicaciones. (Vieites, 2011)

- **Disponibilidad**

La disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar permanentemente a disposición de los usuarios que deseen acceder a sus servicios. (Vieites, 2011)

- **Integridad**

La función de integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática. De este modo, es posible detectar si se ha añadido o eliminado algún dato en un mensaje o fichero almacenado, procesado o transmitido por un sistema o red informática. (Vieites, 2011)

- **Reclamación de origen**

Mediante la reclamación de origen el sistema permite probar quién ha sido el creador de un determinado mensaje o documento. (Vieites, 2011)

- **Reclamación de propiedad**

Este servicio permite probar que un determinado documento o un contenido digital protegido por derechos de autor (canción, video, Libro) pertenece a un determinado usuario u organización que ostenta la titularidad de los derechos de autor. (Vieites, 2011)¹⁹

¹⁹ Vieites Gómez, A. (2011). Enciclopedia de la Seguridad Informática. México. AlfaOmega

1.7.5 TEORÍA CIENTÍFICA

En la investigación de la Solución de Seguridad Informática se ha visto en la necesidad de detallar a fondo algunos de los protocolos de red más importantes, ya que la Solución amerita la utilización de los mismos para su funcionamiento.

1.7.5.1 Protocolo LDAP (Protocolo Ligero de Acceso a Directorios)

Es un protocolo de aplicación sobre TCP/IP que permite el acceso a un servicio de directorio y que articula mediante un esquema cliente – servidor basado en paso de mensajes.²⁰

1.7.5.2 Protocolo DHCP (Protocolo de Configuración Dinámica de Host)

Es un estándar diseñado para reducir la complejidad de la administración de configuraciones de direcciones mediante el uso de un equipo servidor para administrar de forma centralizada las direcciones IP y otros detalles de configuración de la red.²¹

1.7.5.3 Protocolo DNS (Sistema de Nombres de Dominio)

El protocolo DNS se encarga de establecer unas tablas de equivalencia entre direcciones IP y nombres de dominio. Este protocolo nos permite utilizar el nombre www.google.com en vez de la dirección IP 209.85.229.147, ya que él se encarga de hacer esta traducción.²²

1.7.5.4 Protocolo Kerberos

Es un protocolo de autenticación de red. Está diseñado para ofrecer una autenticación fuerte para aplicaciones cliente – servidor utilizando una clave criptográfica secreta.²³

²⁰ Maciá, F. Mora, F. Gil, J. Iglesias, V. Jorquera, D. Berná, J. Monllor, J. Ramos, H. Albadalejo, A. Hernández, A. (2008). Administración de Servicios de Internet. Murcia. Compobell.

²¹ Perez M. (2009). Windows Server 2008: Instalación, Configuración y Administración. Recuperado de <https://books.google.com.ec/books?id=4FcuYxCbPioC&pg=PA441&dq=que+es+el+protocolo+dhcp&hl=es&sa=X&ei=848EVcisHMWvggSF04PgBw&ved=0CEsQ6AEwCQ#v=onepage&q=que%20es%20el%20protocolo%20dhcp&f=false>

²² Barbancho, J. Benjumea, J. Rivera, O. Romero, M. Roper, J. Sanchez, G. Sivianes, F. (2014). Redes Locales. España. Paraninfo.

²³ Van den Bent, J. Van der Steeg, M. (2012). EXIN Cloud Computing Foundation. Recuperado de https://books.google.com.ec/books?id=8VVeAgAAQBAJ&dq=que+es+protocolo+kerberos&hl=es&source=gbs_navlinks_s

En la aplicación de la Solución de Seguridad Informática nos basaremos en las definiciones de términos técnicos necesarios para la investigación, los cuales citamos a continuación.

1.7.5.5 Árbol

Es el conjunto de uno o más dominios que comparten un espacio de nombres contiguo.²⁴

1.7.5.6 Dominio

Es un conjunto de equipos, usuarios y recursos de una misma red y bajo la misma base de datos de directorio.²⁵

1.7.5.7 El árbol de dominio

Está formado por el dominio raíz y los demás dominios que se forman con el nombre del dominio raíz, es decir que constituyen un espacio contiguo de nombres.²⁶

1.7.5.8 Bosque de arboles

Un bosque de árboles de dominio está formado por un conjunto de árboles de dominio que no forman un espacio de nombres contiguos.²⁷

1.7.5.9 Controlador de dominio

Es un Equipo con Active Directory instalado que gestiona la base de datos de usuarios, grupos y recursos de la red. Cada dominio debe tener un nombre de dominio o DNS (Sistema de nombres de dominio) que lo identifica, y que servirá para denominar a los equipos de la red que pertenezca a ese dominio.²⁸

²⁴ Niño, J. (2011). Sistemas Operativos en Red. Recuperado de <https://books.google.com.ec/books?id=A9vJAwAAQBAJ&pg=PA84&dq=active+directory+como+funciona&hl=es&sa=X&ei=2McBVdyQCsK6ggSn6oHIBA&ved=0CEkQ6AEwBw#v=onepage&q=active%20directory%20como%20funciona&f=false>

²⁵ Alegre, M. García, A. (2011). Sistemas Operativos en Red. Madrid. Paraninfo.

²⁶ Alegre, M. García, A. (2011). Sistemas Operativos en Red. Madrid. Paraninfo.

²⁷ Alegre, M. García, A. (2011). Sistemas Operativos en Red. Madrid. Paraninfo.

²⁸ Alegre, M. García, A. (2011). Sistemas Operativos en Red. Madrid. Paraninfo.

1.7.5.10 Directorio Activo

Almacena y permite buscar información de usuarios, equipos y otros objetos, además se encarga de autenticar a usuarios y equipos.²⁹

²⁹ Niño, J. (2011). Sistemas Operativos en Red. Recuperado de <https://books.google.com.ec/books?id=A9vJAwAAQBAJ&pg=PA84&dq=active+directory+como+funciona&hl=es&sa=X&ei=2McBVdyQCsK6ggSn6oHIBA&ved=0CEkQ6AEwBw#v=onepage&q=active%20directory%20como%20funciona&f=false>.

1.8 HIPÓTESIS

¿Con la Implementación de una Solución de Seguridad Informática se logrará fortalecer la confidencialidad de la Información en la Intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda?

1.9 VARIABLES

1.9.1 VARIABLE INDEPENDIENTE

Solución de Seguridad Informática.

1.9.2 VARIABLE DEPENDIENTE

Fortalecer la confidencialidad de la información.

1.9.3 OPERACIONALIZACIÓN DE VARIABLES

Variable Independiente	Concepto	Dimensiones	Indicadores	Ítems de Indicadores	Instrumentos
Solución de Seguridad Informática.	Es la respuesta a los problemas de amenazas informáticas mediante un conjunto de medidas técnicas de seguridad que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.	Amenazas Informáticas.	Infraestructura de la Red. Sistema Lógico de la Red.	¿Cuál es la topología de red que utiliza? ¿Cuentan con un diseño Lógico de la red?	Entrevista Observación Directa
		Medidas Técnicas de Seguridad.	Seguridad Lógica.	¿Cuentan con un software o equipo que brinde seguridad a la información almacenadas en los diferentes servidores con los que cuenta la Institución?	Entrevista

Variable Dependiente	Concepto	Dimensiones	Indicadores	Ítems de Indicadores	Instrumentos
Confidencialidad de la información.	Es una propiedad de la información mediante la cual se garantizará el acceso a la misma solo por parte de las personas que estén autorizadas.	Información	Atomicidad, Integridad, Legalidad, Disponibilidad	¿Qué medida de seguridad en la intranet está utilizando para evitar el acceso no autorizado a la información?	Entrevista
		Control	Ataques informáticos	¿Qué medida de seguridad está utilizando para prevenir pérdida de recursos en la intranet de la Institución?	Entrevista

1.10 METODOLOGÍA

1.10.1 MÉTODOS.

1.10.1.1 Método Bibliográfico

Nos permitió revisar la bibliografía previamente para iniciar con la investigación de la Implementación de una Solución de Seguridad Informática en el Gobierno Autónomo Descentralizado del Cantón Guaranda., para sustentar la parte del Marco Teórico y Teoría Científica.

1.10.1.2 Método Descriptivo – Deductivo

Estos métodos nos permitieron realizar la observación actual de las Soluciones de Seguridades Informáticas, y seguir un proceso sintético-analítico para detectar las vulnerabilidades en la red partiendo de conceptos, principios, definiciones, leyes o normas generales para Implementar una Solución de Seguridad Informática en el Gobierno Autónomo Descentralizado del Cantón Guaranda.

1.11 TIPO DE INVESTIGACIÓN

En general se determinó todo el enfoque de la investigación incluyendo los instrumentos, y la manera de cómo se analizan los datos recaudados.

1.11.1 Investigación de Campo.

Este tipo de investigación nos permitió aplicar las entrevistas, información de primera mano que se procesa cualitativamente y permite determinar la importancia de una Solución de Seguridad Informática para el Gobierno Autónomo Descentralizado del cantón Guaranda.

1.11.2 Investigación Descriptiva.

Se aplicó para obtener un perfil detallado de la Infraestructura de la Red del Gobierno Autónomo Descentralizado del Cantón Guaranda, mediante fotografías, logrando obtener

una visión metódica, lo cual facilitó la investigación, para obtener datos verídicos del estado actual de la intranet de la Institución.

1.11.3 Investigación Bibliográfica.

La investigación bibliográfica, se realizó recurriendo a las fuentes de investigación secundarias que nos permitió elaborar una base teórica de las Soluciones de Seguridades Informáticas recurriendo a fuentes bibliográficas, fuentes electrónicas, páginas webs, libros, manuales, monografías y demás artículos publicados para la Implementación de una Solución de Seguridad Informática para la Intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda.

1.12 TÉCNICAS E INSTRUMENTOS PARA LA OBTENCIÓN DE DATOS.

Para la recopilación de los datos se utilizó diferentes instrumentos tales como la entrevista y la observación directa.

1.12.1 Entrevista.

Se aplicó esta técnica con preguntas abiertas y cerradas, sin un orden preestablecido, adquiriendo características de conversación. La misma que se realizó a los miembros de la oficina de Sistemas del Gobierno Autónomo Descentralizado del Cantón Guaranda.

1.12.2 Observación Directa.

Esta técnica nos permitió visualizar lo que ocurre en una situación real, clasificando y consignando los acontecimientos pertinentes en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda, que son de nuestro interés.

En la técnica de observación directa, se empleó fichas de observación en donde se registró los siguientes procesos:

- ✓ Arquitectura de la Red.
- ✓ Comprobación de la topología de red y conectividad actual.
- ✓ Análisis de las seguridades perimetrales con las que cuenta la red.
- ✓ Computadoras host y servidores.

- ✓ Dispositivos de interconexión gateway, routers, bridges, repetidores, switches.
- ✓ Software de Monitoreo de la Red.
- ✓ Definir estándares para la creación de usuarios, estructura de permisos y políticas que serán implementadas en la Solución de Seguridad Informática.
- ✓ La información de archivos y bases de datos.

1.13 PROCESAMIENTO DE DATOS

En la investigación se ha empleado como técnica para la obtención de datos la entrevista, la cual la hicimos al Jefe del departamento de Sistemas conjuntamente con sus colaboradores, mediante la misma nos da respuesta a todas las preguntas planteadas que requerimos para realizar la investigación.

CAPITULO II

2.1 ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

En la investigación realizada a la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda, hemos optado por la utilización de dos técnicas como son la entrevista y la ficha de observación técnica, para poder diagnosticar los problemas de inseguridad por los cuales se encuentra atravesando la red.

Para esta investigación hemos contado con el apoyo del Departamento de Sistemas quienes con su conocimiento y experiencia en el manejo de la red nos han dado a conocer los problemas que se están dando en la misma y mostrando cierta inquietud por los problemas que se podrían suscitar, viéndose en la necesidad como en toda empresa la Implementación de una Solución de Seguridad Informática para que sus datos sean confidenciales e intransferibles.

2.2 SELECCIÓN DE LA SOLUCIÓN DE SEGURIDAD INFORMÁTICA

Para la selección de la Solución de Seguridad Informática primero haremos introducción al concepto de un Servicio de Directorio.

2.2.1 Servicio de Directorio

Es una aplicación de software especializada que gestiona la información sobre los recursos disponibles en una red y a la que pueden acceder los usuarios. Sirve de base para facilitar el acceso a esos recursos y asegurar que se detecten e impidan los accesos no autorizados.³⁰

³⁰ The Stationery Office. (2010). Operación del Servicio. Recuperado de <https://books.google.com.ec/books?id=htb2mp3A2WAC&pg=PA108&dq=servicios+de+directorio&hl=es&sa=X&ei=A-UKVeWHHfb7sAT3kYDwBA&ved=0CDIQ6AEwBA#v=onepage&q=servicios%20de%20directorio&f=false>

2.2.2 Estudio Comparativo entre Servicios de Directorio

Para la selección de uno de los servicios de directorio, el cual fortalecerá la confidencialidad de la información en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda de una manera fácil se analizó características de administración y configuración.

Los resultados que permitan la mejor selección del directorio se basa en la siguiente escala de valoración sobre 3 puntos:

Alto	Medio	Bajo
1	2	3

Tabla 1 Puntaje para realizar la comparación.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación.

AD = Puntaje de Active Directory

OL = Puntaje de OpenLdap

T = Total del parámetro de valoración (3)

La valoración definitiva de cada análisis de los Servicios de Directorio se realizara mediante las siguientes funciones.

$$\mathbf{VAD} = \frac{\sum \mathbf{AD}}{\mathbf{VTACTIVE DIRECTORY}} = \mathbf{VAD/VT}$$

$$\mathbf{VOL} = \frac{\sum \mathbf{OL}}{\mathbf{VTOPENLDAP}} = \mathbf{VOL/VT}$$

$$\mathbf{VT} = \sum \mathbf{T}$$

VT Número de variables

VAD Puntaje acumulado de ACTIVE DIRECTORY en el indicador.

VOL Puntaje acumulado de OPENLDAP en el indicador.

VTACTIVE DIRECTORY Calificación total de ACTIVE DIRECTORY en el indicador.

VTOPENLDAP Calificación total de OPENLDAP en el indicador.

CARACTERISTICAS

Índice

- Instalación y configuración del controlador de dominio
- Administración de usuarios y recursos de red
- Sistemas de autenticación y autorización
- Consolidación de directorios
- Infraestructura y aplicaciones habilitadas para el uso de directorios
- Escalabilidad
- Uso de los estándares de Internet (Protocolos)
- Un entorno de desarrollo eficaz
- Replicación
- Supervisión de confianza
- Mantenimiento
- Costo

Valoraciones

Instalación (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto nivel de complejidad en la instalación y configuración del controlador de dominio.

Administración (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto nivel de complejidad en alguna de las siguientes funcionalidades: administración de usuarios, administración de los recursos de la red.

Derechos de Acceso (3): Se penalizará con 1 punto al Servicio de Directorio que no permita: restringir el acceso.

Consolidación de directorios (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto nivel de complejidad en alguna de las siguientes funcionalidades: organizar, simplificar la administración de usuarios, equipos, aplicaciones y dispositivos, y facilitar a los usuarios la búsqueda de la información que necesitan

Infraestructura y aplicaciones habilitadas para el uso de directorios (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto nivel de complejidad en la configuración y administración de las aplicaciones y otros componentes de red habilitados para el uso de directorios.

Escalabilidad (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto nivel de complejidad al que no pueda escalar hasta llegar a tener millones de objetos por cada dominio y utilizar técnicas de replicación avanzadas para aumentar el rendimiento.

Uso de los estándares de Internet (Protocolos) (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto nivel de complejidad en el acceso mediante LDAP y no utilice un espacio de nombres basado en el Sistema de nombres de dominio (DNS).

Un entorno de desarrollo eficaz (3): Se penalizará con 1 punto al Servicio de Directorio que no cuente con una interface amigable.

Replicación (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto nivel de complejidad al copiar y mantener actualizados los datos en varios nodos de bases de datos ya sean estos persistentes o no.

Supervisión de confianza (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto nivel de complejidad

Mantenimiento (3): Se penalizará con 1 punto al Servicio de Directorio que no permita realizar mantenimiento de la información de manera fácil y que no proporcione alternativas de solución a los problemas mediante la utilización de ayudas.

CARACTERISTICAS	ACTIVE DIRECTORY			OPENLDAP		
	Alto	Intermedio	Bajo	Alto	Intermedio	Bajo
Instalación y configuración del controlador de dominio		X		X		
Administración de usuarios y recursos de red			X		X	
Sistemas de autenticación y autorización		X		X		
Consolidación de directorios		X			X	
Infraestructura y aplicaciones habilitadas para el uso de directorios			X	X		
Escalabilidad			X		X	
Uso de los estándares de Internet (Protocolos)	X				X	
Un entorno de desarrollo eficaz			X	X		
Replicación		X			X	
Supervisión de confianza		X		-	-	-
Mantenimiento			X	X		

Tabla 2 Estudio Comparativo 1 entre servicios de directorio.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación.

INTERPRETACIÓN

Instalación: La instalación y configuración del controlador de dominio tiene un nivel medio de complejidad.

Administración: La administración (usuarios y recursos de la red) es administrable en los Servicios de Directorio.

Derechos de Acceso: Los Servicios de Directorio cuentan con sistemas de autenticación y autorización para salvaguardar la confidencialidad de la información

Consolidación de directorios: Los Servicios de Directorio para las funcionalidades: organizar, simplificar la administración de usuarios, equipos, aplicaciones y dispositivos, y facilitar a los usuarios la búsqueda de la información que necesitan, tienen un nivel medio de complejidad para su configuración.

Infraestructura y aplicaciones habilitadas para el uso de directorios: se ha indicado que existe diferencia en el nivel de complejidad entre los Servicios de Directorio en estudio para la configuración y administración de las aplicaciones y otros componentes de red habilitados para el uso de directorios.

Escalabilidad: Los dos Servicios de Directorio pueden escalar hasta llegar a tener millones de objetos por cada dominio y utilizar técnicas de replicación avanzadas para aumentar el rendimiento.

Uso de los estándares de Internet (Protocolos): Los Servicio de Directorio proporcionan el acceso mediante LDAP y utilizan un espacio de nombres basado en el Sistema de nombres de dominio (DNS).

Un entorno de desarrollo eficaz: Uno de los Servicios de Directorio cuentan con una interface amigable.

Replicación: Los Servicios de Directorio permiten copiar y mantener actualizados los datos en varios nodos de bases de datos ya sean estos persistentes o no.

Supervisión de confianza: Establece relaciones de confianza entre dos o más dominios permitiéndoles tener una comunicación segura entre usuarios de un dominio con el otro.

Mantenimiento: Permiten realizar mantenimiento de la información de manera fácil y que proporcionan alternativas de solución a los problemas mediante la utilización de ayudas.

VALORACIÓN

CARACTERISTICAS	ACTIVE DIRECTORY			OPENLDAP		
	Alto	Intermedio	Bajo	Alto	Intermedio	Bajo
Instalación y configuración del controlador de dominio		2		1		
Administración de usuarios y recursos de red			3		2	
Sistemas de autenticación y autorización		2		1		
Consolidación de directorios		2			2	
Infraestructura y aplicaciones habilitadas para el uso de directorios			3	1		
Escalabilidad			3		2	
Uso de los estándares de Internet (Protocolos)	1				2	
Un entorno de desarrollo eficaz			3	1		
Replicación		2			2	
Supervisión de confianza		2		-	-	-
Mantenimiento		2		1		
Costo		2		1		
TOTAL		27			16	

Tabla 3 Estudio comparativo 2 entre servicios de directorio.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación.

$$VT = \sum T = 1+1+1+1+1+1+1+1+1+1+1 = 11$$

$$VAD = \sum 2+3+2+2+3+3+1+3+2+2+2 = 25$$

$$VTACTIVEDIRECTORY = VAD/VT = (25/11) = 2,27$$

$$VOL = \sum 1+2+1+2+1+2+2+1+2+1 = 15$$

$$VTOPENLDAP = VOP/VT = (15/11) = 1,36$$

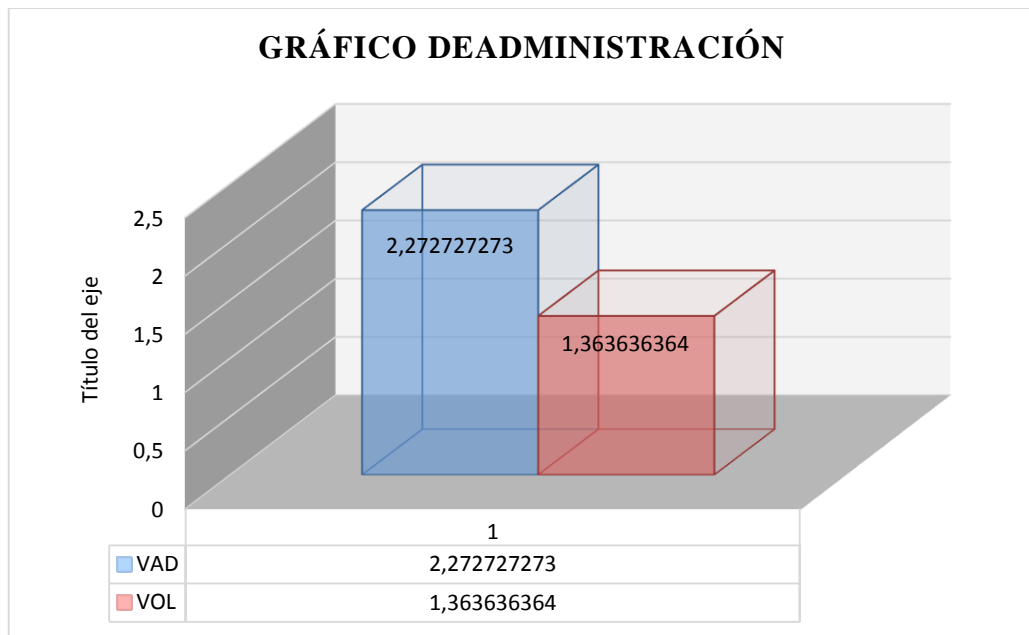


Gráfico 1 Cuadro estadístico sobre Administración.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

COSTOS

Índice

- Costo de Implementación
- Costo de Mantenimiento

Valoraciones

Costo de implementación (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto costo en la instalación y configuración.

Costo de mantenimiento (3): Se penalizará con 1 punto al Servicio de Directorio que proporcione un alto costo de mantenimiento.

COSTOS	ACTIVE DIRECTORY			OPENLDAP		
	Alto	Intermedio	Bajo	Alto	Intermedio	Bajo
Implementación	X					X
Mantenimiento			X	X		

Tabla 4 Estudio comparativo entre los costos de los Servicios de Directorio.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Interpretación

Implementación: La implementación del Servicio de Directorio Active Directory tiene un costo elevado debido a la licencia que se debe adquirir para el Sistema Operativo del Servidor en este caso Windows 2012 Server a diferencia de OpenLdap que es de Distribución libre.

Mantenimiento: El mantenimiento de un Servicio de Directorio en Active Directory es de un costo bajo debido a que toda su configuración se la realiza a nivel gráfico a diferencia de OpenLdap que es a base de comandos e instrucciones a través de una terminal.

VALORACIÓN

COSTOS	ACTIVE DIRECTORY			OPENLDAP		
	Alto	Intermedio	Bajo	Alto	Intermedio	Bajo
Implementación	3					1
Mantenimiento			1	3		

Tabla 5 Comparación de costos entre los Servicios de Directorio.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

$$VT = \sum T = 1 + 1 = 2$$

$$VAD = \sum 3 + 1 = 4$$

$$VT_{ACTIVE\ DIRECTORY} = VAD / VT = (4/2) = 2$$

$$VOL = \sum 1 + 3 = 4$$

$$VT_{OPENLDAP} = VOL / VT = (4/2) = 2$$

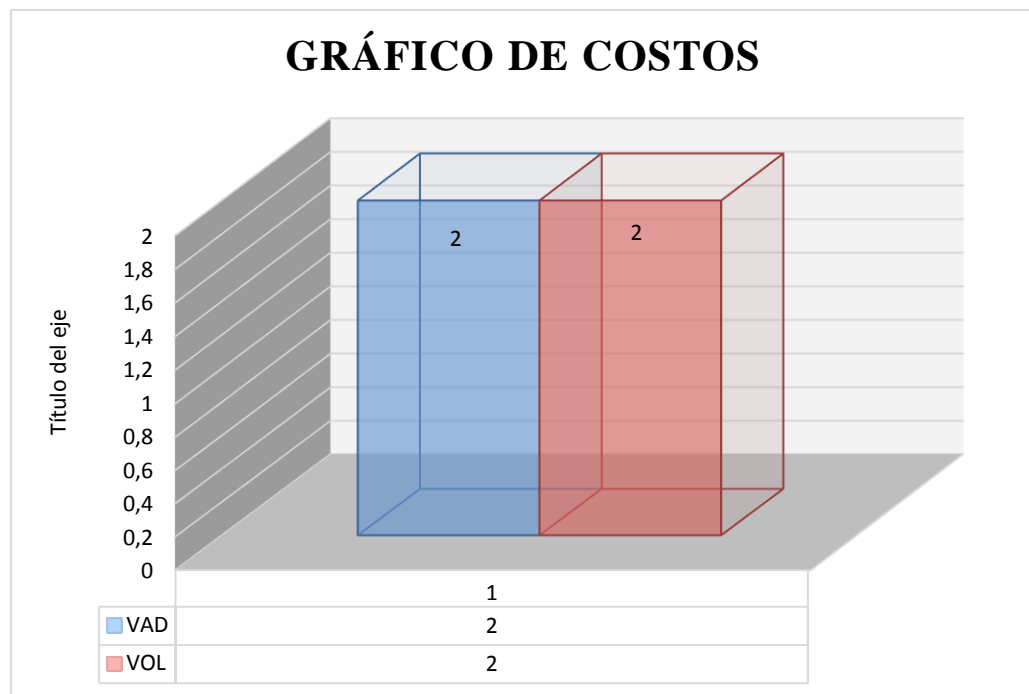


Tabla 6 Cuadro estadístico de los Costos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

RECOPIACIÓN DE RESULTADOS

INDICADOR	ÍNDICE	ACTIVE DIRECTORY	OPENLDAP
Características	Instalación y configuración del controlador de dominio	2	1
	Administración de usuarios y recursos de red	3	2
	Sistemas de autenticación y autorización	2	1
	Consolidación de directorios	2	2
	Infraestructura y aplicaciones habilitadas para el uso de directorios	3	1
	Escalabilidad	3	2
	Uso de los estándares de Internet (Protocolos)	1	2
	Un entorno de desarrollo eficaz	3	1
	Replicación	2	2
	Supervisión de confianza	2	
	Mantenimiento	2	1
	Costos	Implementación	3
Mantenimiento		1	3
Total Sobre 39		29	19
Porcentaje		74,35%	48,71%

Tabla 7 Resultados obtenidos del Estudio Comparativo.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

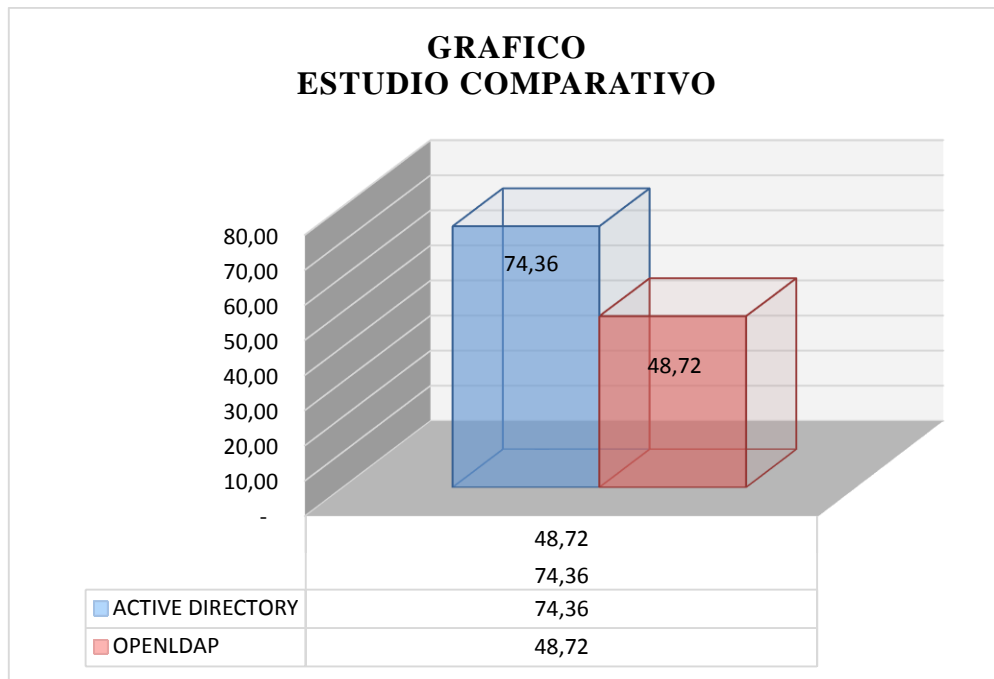


Gráfico 3 Cuadro estadístico sobre los resultados obtenidos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Al realizar el análisis de los Servicios de Directorio OpenLdap y Active Directory se estableció a Active Directory como la solución de seguridad óptima para fortalecer la confidencialidad de la información en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda con el 74,35% un nivel bajo de complejidad en la administración y configuración con respecto a OpenLdap con un 48,72% convirtiéndolo en un Servicio de Directorio complejo para su administración.

Además cabe recalcar que en el Gobierno Autónomo Descentralizado del Cantón Guaranda los equipos con los cuales trabajan los usuarios utilizan software propietario Windows, convirtiéndose en un punto más a favor de **Active Directory** “Que es un servicio de directorio que almacena información acerca de los objetos de una red y la pone a disposición de los usuarios y administradores de la red, nos brinda la posibilidad que desde un solo servidor podamos controlar todos los equipos de la red, sin tener que desplazarnos a los equipos clientes esta medida de seguridad es muy importante debido a que si no tenemos el Directorio Activo y tenemos muchos equipos que administrar, tenemos que desplazarnos a cada equipo para configurar su entorno y los usuarios que pueden usarlo, mientras que con el Directorio Activo esta tarea la realizaremos

exclusivamente desde el servidor”, basándonos en una misma plataforma permitiendo así un buen funcionamiento y una correcta administración de Active Directory.

Presentando a continuación las herramientas para administrar Active Directory.

- **Usuarios y equipos de Active Directory.**

Administra usuarios, equipos, grupos de seguridad y otros objetos.

- **Sitios y Servicios de Active Directory**

Crea sitios para administrar la replicación de la información de los servicios de dominio.

- **Dominios y confianzas de Active Directory**

Sirve para administrar confianzas de dominios, niveles funcionales del bosque o del dominio.³¹

³¹ Niño, J. (2011). Sistemas Operativos en Red. Recuperado de <https://books.google.com.ec/books?id=A9vJAwAAQBAJ&pg=PA84&dq=active+directory+como+funciona&hl=es&sa=X&ei=2McBVdyQCsK6ggSn6oHIBA&ved=0CEkQ6AEwBw#v=onepage&q=active%20directory%20como%20funciona&f=false>.

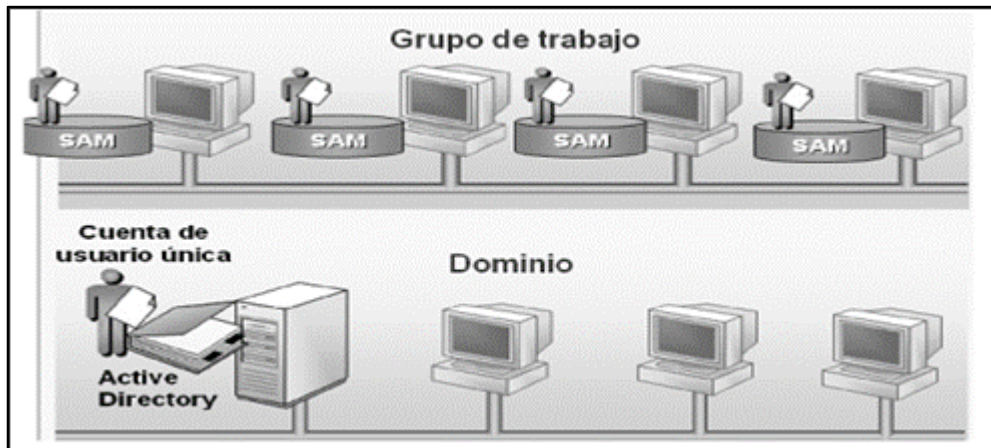


Gráfico 4 Grupo de Trabajo vs Active Directory.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación.

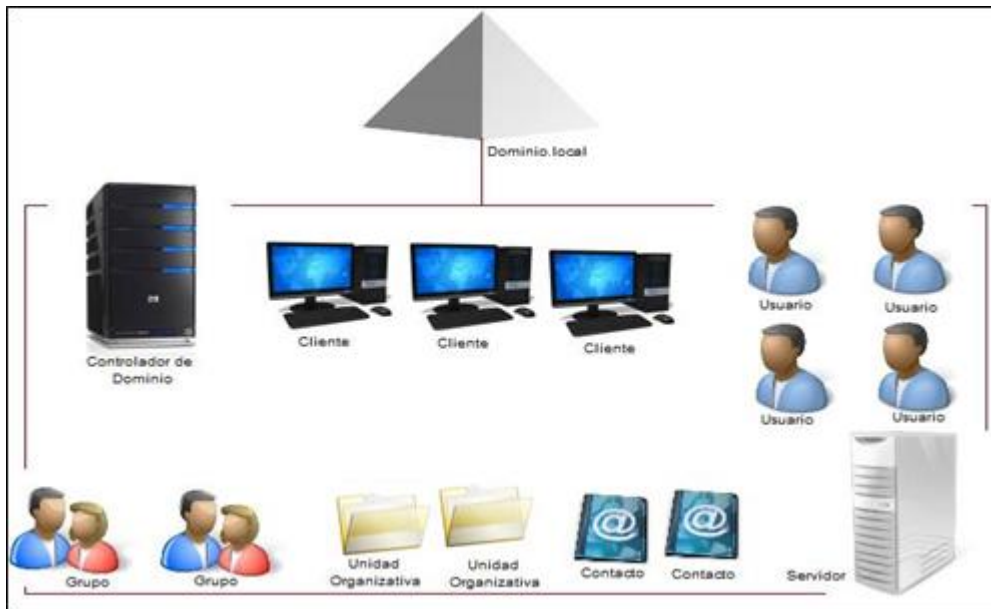


Gráfico 5 Estructura de un Directorio Activo.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación.

2.3 APLICACIÓN DE LAS TÉCNICAS E INSTRUMENTOS UTILIZADOS

En la Implementación de una Solución de Seguridad Informática para fortalecer la confidencialidad de la información en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda, se ha aplicado las siguientes técnicas para la obtención de datos:

ENTREVISTA DE SEGURIDADES INFORMÁTICAS GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA (UNIDAD DE SISTEMAS)
NOMBRE: Ing. Jaime Gaibor. CARGO: Jefe de la Unidad de Sistemas Informáticos. FECHA: 23 de Febrero del 2015. ENTREVISTADORES: Karla Barragán, Jessica Rea.
PREGUNTAS
1. ¿Qué tipo de red utilizan (Diseño de la Red)? En el Gobierno Autónomo Descentralizado del Cantón Guaranda una vez realizada la entrevista a los miembros del Departamento de Sistemas han indicado que están trabajando con una red de datos tipo estrella, en esta topología existe un nodo central, enlazado directamente con todos los demás que controla en tráfico de datos por la red, reenviando los datos a su destino. Cada nodo tiene un enlace punto a punto con el nodo central. ³²
2. ¿Cuál es el medio de conexión que utiliza? En la red de datos del Gobierno Autónomo Descentralizado del Cantón Guaranda como medios guiados cuentan con Fibra Óptica para el Servicio de Internet y cable UTP Cat 6 para la red interna que permite la comunicación entre los diferentes departamentos de la Institución.
3. ¿Con qué tipo de equipos cuentan en su infraestructura de red? <input type="checkbox"/> Capa Dos (Capa Física- No Programables) <input type="checkbox"/> Capa Tres (Capa de Aplicación- Programables)

³² Romero, M. Barbancho, J. Benjumea, J. Rivera, O. Roper, J. Sanchez, G. Sivianes, F. (2010). Redes Locales. Madrid. Paraninfo

En el Gobierno Autónomo Descentralizado del Cantón Guaranda cuentan con equipos de Capa dos no Programables y Equipos de capa tres basándose en el modelo OSI (Interconexión de Sistemas Abiertos) determinado como un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

En los Equipos de Capa Tres tienen el Gateprotect que proporciona seguridad perimetral, cortafuegos (firewall), como control de acceso a redes sociales, control de ancho de banda entre otras funcionalidades, protegiendo así todas las comunicaciones provenientes de internet.

4. ¿Qué conflictos o caídas de sistema ha sufrido su red?

- Ataques ilegales
- Conflicto de direcciones IP
- Ataques de Hackers

En la red de datos el problema que se ha dado con mayor frecuencia es el denominado conflicto de direcciones IP “consiste en que dos o más dispositivos tienen la misma dirección IP lo cual obstaculiza la comunicación a la red inalámbrica a uno de los dispositivos afectados” este problema ocurre debido a la manipulación de los usuarios porque esta opción no se encuentra bloqueada por un administrador de la red, siendo fácilmente manipulable.

5. ¿Qué problemas se han presentado en la administración de la Intranet?

En la Intranet del Gobierno Autónomo Descentralizado del cantón Guaranda se ha presentado los siguientes problemas de seguridad:

- Inseguridad en su información.
- Poca administración de usuarios.
- Manipulación por medio de los usuarios cambiando el nombre del Grupo de Trabajo.
- En el Grupo de Trabajo se da libre acceso a la información.
- Mala utilización de los recursos de la red.
- Conflictos de direcciones IP por manipulación de usuarios.
- Usuarios instalan programas o aplicaciones que no pertenecen al área laboral.
- Virus.

Para lo cual la solución de seguridad que planteamos resolverá todos estos problemas analizados permitiendo la centralización de los recursos y de gestión así como la autenticación y autorización de usuarios.

6. Si usted cuenta con una red inalámbrica ¿qué tipo de seguridad tiene?

- Solo clave
- Clave y configuración

En la configuración de la red inalámbrica han optado por la utilización de una clave de acceso (empleada para que un usuario pueda acceder a un servicio, sistema o programa), para permitir la conexión a la red. La clave de acceso como medida de seguridad para el ingreso a una red, servicio o cuenta de usuario no garantiza la protección completa del medio al que se accede. Debido a que las claves pueden ser descifradas fácilmente con algún programa y una vez conocida la información estaría expuesta a terceras personas con el propósito de robo, extorsión o engaño.

7. ¿Su infraestructura de red cuenta con subredes o VLANS?

En la estructura de la red física del Gobierno Autónomo Descentralizado del Cantón Guaranda utilizan Vlans (Red de Área Local Virtual) consideradas como una red independiente desde el punto de vista lógico, donde los dispositivos no se limitan solo a un segmento físico.³³

8. ¿Cuentan ustedes con algún tipo de Aplicación informática?

- Si
- No

El Gobierno Autónomo Descentralizado del Cantón Guaranda cuenta con las siguientes aplicaciones informáticas:

- Quipux.
- Sistema de Vigilancia.
- Olympo.
- SIM
- PUNNIS V10

³³ Jara, H. Pacheco, F. (2013). Ethical Hacking 2.0. Recuperado de <https://books.google.com.ec/books?id=joMIAU4seLYC&pg=PA263&dq=que+es+vlans&hl=es&sa=X&ei=2E8GVYCHDsmoNoDQg4gJ&ved=0CEoQ6AEwCA#v=onepage&q=que%20es%20vlans&f=false>

9. ¿Con qué tipo de seguridad cuentan dichas aplicaciones?

El Gobierno Autónomo Descentralizado del Cantón Guaranda para la protección de las aplicaciones utilizan el equipo Gateprotect “es un firewall que utiliza la tecnología eGUI que hace más fácil la operación del sistema, aumenta significativamente la productividad de la empresa y elimina las reglas y provee visualizaciones gráficas, reduciendo costos, tiempo y aumentando la productividad del personal operativo”

10. ¿Con cuántos servidores cuentan y que funcionalidad tienen?

En la estructura física de la red el Gobierno Autónomo Descentralizado del Cantón Guaranda cuentan con cuatro servidores los cuales cumplen con las siguientes funciones:

- Almacenar Base de Datos.
- Respaldo de Base de Datos.
- Correo Electrónico.
- Telefonía IP.

11. ¿De qué tipo de clase de subred tiene la infraestructura de red alámbrica e inalámbrica?

En el Gobierno Autónomo Descentralizado del Cantón Guaranda utilizan una estructura de red tipo B, su rango es 127 hasta la 191, distribuido para 65534 hosts y 16384 redes.

12. ¿Con qué frecuencia realiza un chequeo de los puertos de conectividad de red?

- Diario
- Mensual
- Anual
- Otros

Especifique:.....

En el departamento de Sistemas del Gobierno Autónomo Descentralizado del Cantón Guaranda realizan un chequeo de puertos mensualmente que se emplea para designar la acción de analizar por medio de un programa (programa) el estado de los puertos de una maquina conectada a una red de comunicaciones, detectando si los puertos se encuentran abiertos, cerrados o protegidos por un cortafuegos.

13. ¿Controla el acceso a redes sociales?

- Si
- No

En el Gobierno Autónomo Descentralizado del Cantón Guaranda el control de acceso a redes sociales se realiza mediante el equipo Gateprotect el cual proporciona la funcionalidad de realizar dicha operación.

14. ¿Controla el ancho de banda para cada una de las oficinas?

- Si
- No

En el Gobierno Autónomo Descentralizado del Cantón Guaranda el control de Ancho de Banda (Es la capacidad de información de datos que se puede enviar a través de una conexión de red en un periodo de tiempo dado. El ancho de banda se indica generalmente en bits por segundo (bps). Kilobits por segundo (kbps), o megabits por segundo (Mbps).) La cual se realiza mediante el equipo Gateprotect el cual proporciona la funcionalidad de realizar dicha operación.

15. ¿Cuenta con IP públicas para alguna oficina?

- Si
- No

En el Gobierno Autónomo Descentralizado del Cantón Guaranda el departamento de Sistemas cuenta con una IP pública “Es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet”

16. ¿Cuentan con equipos que soporta IPV6?

- Si
- No

En el Gobierno Autónomo Descentralizado del Cantón Guaranda en el departamento de Sistemas por el momento no cuentan con equipos que soporten la tecnología IPV6.

17. ¿Cómo está distribuida la estructura IPV6?

No cuentan con una estructura IPV6.

18. ¿Cómo se dan cuenta de los problemas que presenta la red?

En el Gobierno Autónomo Descentralizado del Cantón Guaranda verifican el correcto funcionamiento mediante el monitoreo de la Red Interna a través del CMD con el comando bntstat -a y el número de IP asignada a cada equipo.

19. ¿Qué medida de seguridad está utilizando en la intranet para evitar el acceso de usuarios no autorizados a la información?

En la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda al momento no cuentan con una medida de seguridad que les permita tener el control de todos sus usuarios y a que información deben acceder provocando desconfianza en la información compartida a los diferentes usuarios.

20. ¿Qué medida de seguridad está utilizando para prevenir el desperdicio de recursos en la intranet de la Institución?

En la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda se presenta el problema de mala utilización de recursos por ciertos usuarios que ingresan a páginas de entretenimiento entre otras creando inestabilidad para el personal debido a que no pueden llevar a cabo sus funciones laborales en su totalidad.

21. ¿Qué medida de seguridad en la red está utilizando para prevenir ataques informáticos provenientes de internet?

En la Red del Gobierno Autónomo Descentralizado del Cantón Guaranda cuentan con un equipo Gateprotect que opera como firewall bloqueando el acceso no autorizado a cualquier ataque proveniente de internet, permitiendo al mismo tiempo realizar conexiones autorizadas dentro de la Institución.

22. ¿Cuál es la forma de organización de Equipos en la Red?

- Grupo de Trabajo.
- Grupo en el Hogar.
- Dominio (Active Directory).

La forma de organización de los equipos en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda es de un Grupo de Trabajo que permite que todos los equipos se encuentren en el mismo nivel, ninguno tiene el control sobre otro, no se

encuentra protegido con contraseña y todos los equipos deben encontrarse en la misma red local o subred.

23. ¿Estaría usted de acuerdo con la implementación de un Directorio Activo para brindar protección a la Intranet?

- Si
- No

En el Gobierno Autónomo Descentralizado del Cantón Guaranda están de acuerdo con la implementación del Directorio Activo (Active Directory) ya que permite simplificar y centralizar la administración de los usuarios y equipos mejorando el acceso a los recursos de una red de ordenadores. El Directorio Activo utiliza distintos protocolos como (LDAP, DNS, DHCP Y KERBEROS). Para almacenar información sobre los usuarios, grupos y servicios relacionados, se utiliza una base de datos, pero la utilidad del Directorio Activo es mayor ya que, además de la información sobre los usuarios, mantiene información sobre los servidores, equipos, directivas de seguridad, etc.³⁴

³⁴ Ramos, M. García, A. (2011). Sistemas Operativos en Red. Madrid. Paraninfo.

**FICHA DE OBSERVACIÓN DIRECTA DE SEGURIDADES INFORMÁTICAS
GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA
(UNIDAD DE SISTEMAS)**

FECHA: 23 de Febrero del 2015.

OBSERVADORAS: Karla Barragán, Jessica Rea.

Se observó la infraestructura de red del Gobierno Autónomo Descentralizado del Cantón Guaranda determinando los equipos de red con los cuales está estructurado el rack que se encuentra en la Unidad de Sistemas, verificando las medidas de seguridad implementadas en dicha estructura llegando a establecer al equipo firewall Gateprotect como medida de protección para comunicaciones externas, a la vez se realizó el diagrama de funcionamiento de seguridad perimetral que realiza el equipo utilizando como requerimiento para la Implementación de la Solución de Seguridad Informática.

En la infraestructura física de la red distribuida en los diferentes departamentos de la Institución se encontró problemas de conflictos IP, debido al manejo indebido de la configuración de la red en el equipo perteneciente a cada uno de los usuarios.

Conclusiones:

Mediante la observación directa se pudo determinar que el proceso de dar solución a los problemas es tedioso y demoroso debido a que deben realizar un seguimiento de las causas que ocasionaron dicho problema.

2.4 DIAGRAMAS

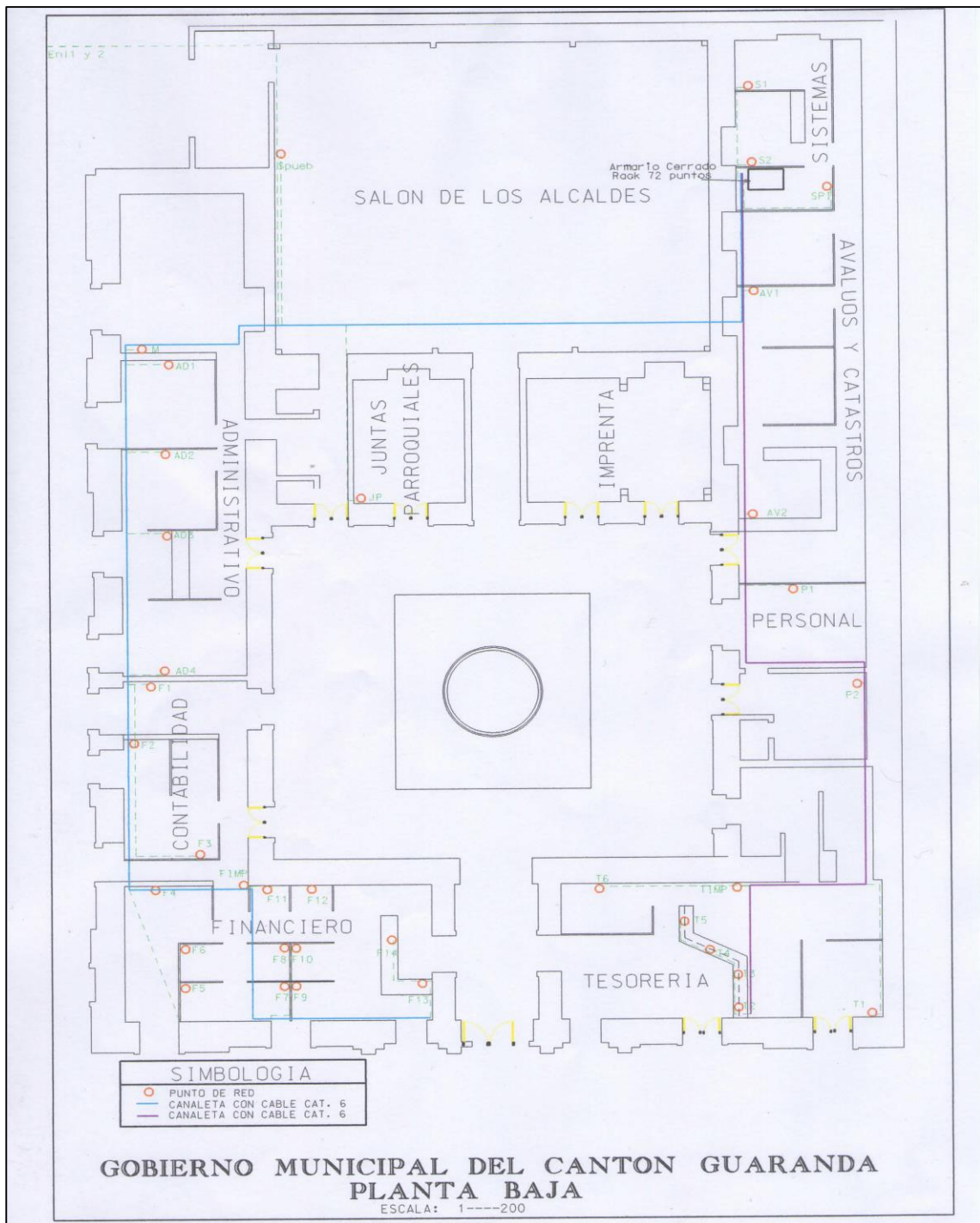


Gráfico 6 Plano de la Planta Baja del GAD Municipal.

Fuente: Gobierno Autónomo Descentralizado del Cantón Guaranda.

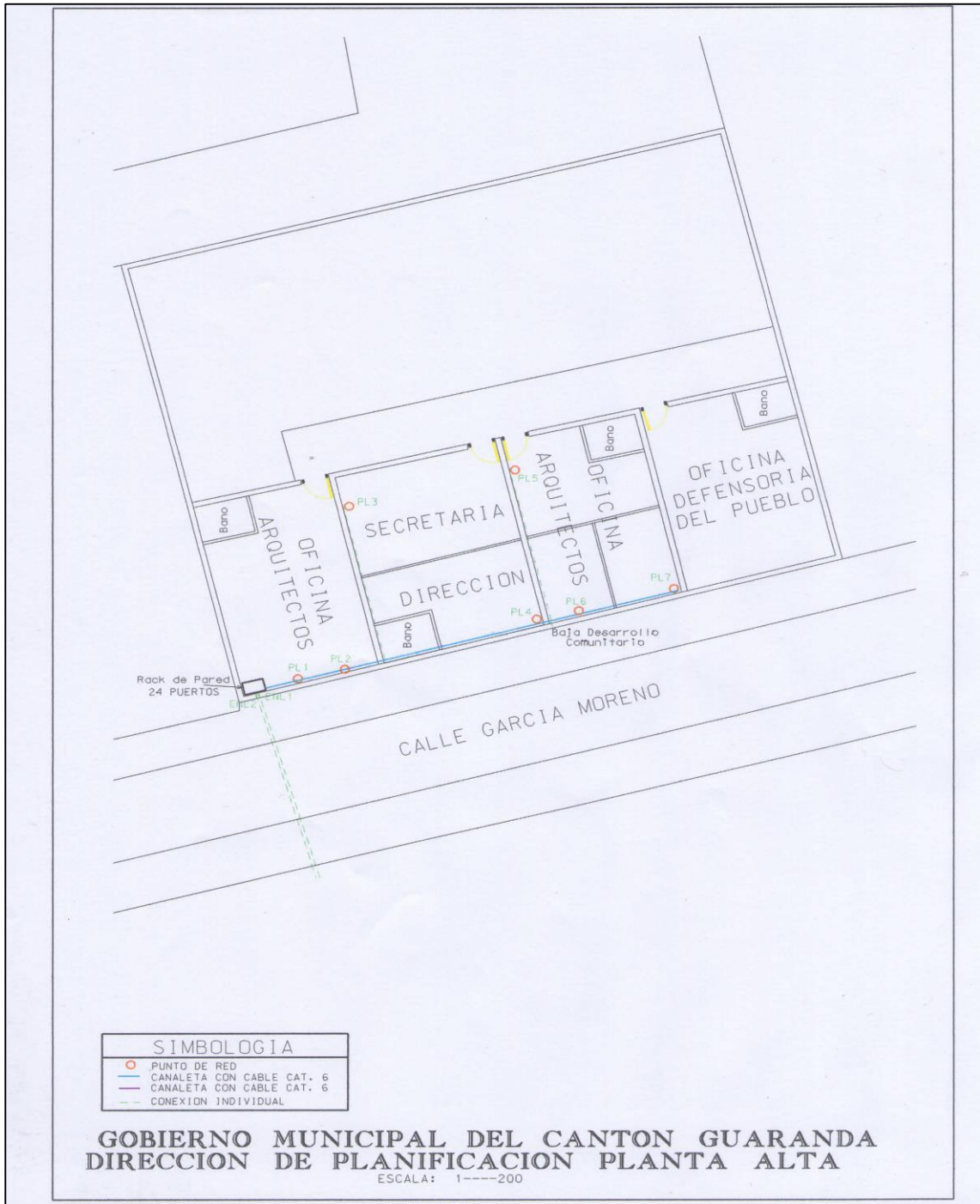


Gráfico 7 Plano de la Planta Alta del GAD Municipal.

Fuente: Gobierno Autónomo Descentralizado del Cantón Guaranda.

2.5 REQUISITOS TECNICOS

- El servidor requerido para la implementación del Directorio Activo debe cumplir las siguientes características:
 - Servidor no virtual o virtualizado con sistema de virtualización por blades.
 - Procesador Xeon, Intel Core i5 o compatible con al menos 2 núcleos y 2.8 GHz
 - Memoria RAM de 8 GBytes o superior.
 - Sistema operativo del servidor: Windows 2008 Server R2 o Superior.
- Licencia Windows Server 2012 Estándar 64.

2.6 RELACIÓN BENEFICIO / COSTO

La Implementación del Directorio Activo como Solución de Seguridad Informática para fortalecer la confidencialidad de la información en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda, trae como beneficio una serie de mejoras, tanto en el proceso de centralización de los recursos y de gestión así como también en la autenticación y autorización de usuarios con el objetivo de estandarizar, asegurar y facilitar la administración de toda la tecnología, permitiendo tener un control de las actividades que deben realizar cada uno de los usuarios de la Institución a través del Departamento de Sistemas.

Los costos empleados en la Implementación del Directorio Activo son bajos en relación a los beneficios obtenidos nombrados anteriormente, por lo cual la ejecución del proyecto de investigación es factible económicamente para la Institución.

BENEFICIOS	COSTOS	
<ul style="list-style-type: none"> ▪ Capacidad de controlar a los usuarios mediante directivas de grupo, servicios de red y aplicaciones. ▪ Control centralizado de los recursos de la red. ▪ Un único inicio de sesión. ▪ Creación de estructuras jerárquicas de dominios y subdominios. ▪ Mayor Seguridad. ▪ Mejoras en el rendimiento y la confiabilidad. ▪ Autenticación y autorización de usuarios. 	Servidor con el que cuenta la Institución.	\$00.00
	Instalación del Servidor del controlador del dominio.	\$800.00
	Unión de los Equipos al Dominio.	\$2000.00
	Pruebas de Seguridad y Funcionamiento.	\$400.00
	Licencia de Windows Server 2012.	\$1185.00
	TOTAL	\$4385.00

Tabla 8 Relación Beneficio \ Costo.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

De los costos expuestos en la Tabla. **\$2385.00** incluido IVA, es la inversión por parte de la Institución los **\$2000.00** dólares es la parte que se cubrió con el trabajo que es unir todos los equipos al dominio realizado por las autoras del trabajo de investigación.

Siendo una gran ventaja para la Institución directamente para la Unidad de Sistemas Informáticos debido a que ellos se beneficiaran ya que cuentan con una herramienta para realizar su trabajo obteniendo así un mayor control de la tecnología.

Los responsables de la Unidad de Sistemas Informáticos al no resolver algunos de problemas que se daban anteriormente como conflictos de direccionamiento IP, dispondrán de su tiempo restante para realizar otro tipo de actividades en mejoramiento del Gobierno Autónomo Descentralizado del Cantón Guaranda.

2.6.1 Detalle de Costos.

ESTRUCTURA DE COSTOS (VALORES ANUALES)			
RUBROS	COSTOS FIJOS	COSTO VARIABLE	COSTO TOTAL
Costo de Producción			\$ 48.000,00
Depreciación	\$ 48.000,00		
Costo de Administración			\$ 27.165,28
Útiles de aseo	\$ 200,00		
Sueldos y salarios	\$ 25.367,28		
Beneficios Sociales	\$ 638,00		
Servicios básicos	\$ 960,00		
Costo de Venta			\$ 60.867,28
Sueldos y salarios	\$ 25.367,28		
Equipos de Computo		\$ 35.000,00	
Útiles de oficina		\$ 500,00	
Costos Financieros			\$ 0,00
Intereses	\$ 0,00		
COSTO TOTAL	\$ 99.894,56	\$ 35.500,00	\$ 136.032,56

Tabla 9 Estructura de Costos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

El riesgo empleado es del 5% por cualquier falla o problema que pueda presentarse en el Sistema implementado, porcentaje expuesto por las responsables del trabajo de investigación.

La inflación es del 4.05% a nivel del país.

$$TMAR = i + f + if$$

$$TMAR = 0.05 + 0.0405 + 0.05 * 0.0405$$

$$TMAR = 0.093$$

$$i = \frac{1}{1 + i^n} = \frac{1}{1 + (0.093)^1} = 0.91$$

$$Costos Actualizados = Costos Totales * i$$

$$CA = \$136.032,56 (0.91)$$

$$CA = \$123.789,62$$

2.6.2 Detalle de Ingresos

INGRESOS DE LA INSTITUCIÓN	
DETALLE	VALOR
Impuesto Urbano	\$ 4.561.490,03
Impuesto Rural	\$ 282.605,93
Patentes	\$ 92.789,80
Activos Totales	\$ 36.016,12
Licencia Anual de Funcionamiento	\$ 6.012,70
Mercado 10 de Noviembre	\$ 44.249,58
Mercado 24 de Mayo	\$ 17.228,75
Contribución Especial de Mejoras	\$ 28.446,03
Alcabalas	\$ 167.387,36
Utilidad a los Predios	\$ 243.309,84
TOTAL	\$ 5.479.536,14

Tabla 10 Detalle de Ingresos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

No se utilizó los ingresos totales de la Institución debido a que solo nos basamos en los costos totales de la Unidad de Sistemas Informáticos. Los Ingresos destinados para la Unidad de Sistemas Informáticos son de **\$150.000** los cuales utilizamos como base de referencia puesto que son los beneficiados directos de la Implementación de una Solución de Seguridad Informática: Active Directory.

$$\mathbf{Ingresos Actualizados} = \mathbf{Ingresos Totales} * i$$

$$\mathbf{Ingresos Actualizados} = 150.000 * 0.91$$

$$\mathbf{Ingresos Actualizados} = \$136.500$$

$$R B/C = \frac{INGRESOS ACTUALIZADOS}{COSTOS ACTUALIZADOS + INVERSIÓN}$$

$$R B/C = \frac{\$136.500}{\$123.789.62 + \$2529.00} = \mathbf{\$1.08}$$

La razón costo beneficio da como resultado \$1.08, es decir por cada \$1 dólar invertido se obtendrá 0.8 ctvs. de dólar, obteniendo como rédito económico para la Unidad de Sistemas Informáticos los beneficios que se detallan a continuación:

- Administración de los recursos de la red.
- Políticas de seguridad.
- Autenticación y autorización de usuarios.
- Reducción de conflictos IP.
- Mayor control de usuarios.

Entre otros beneficios que serán implementados mediante las necesidades y la aceptación de los responsables de la Unidad de Sistemas Informáticos debido a que dentro del servicio de directorio Active Directory implementado se pueden incrementar una serie de políticas de seguridad a más de las que se encuentran creadas, para fortalecer la seguridad en la intranet y al mismo tiempo mejorando el rendimiento laboral en la Institución.

2.7 CONCLUSIONES Y RECOMENDACIONES

2.7.1 CONCLUSIONES

En la presente investigación se ha realizado el estudio de la infraestructura existente de la red del Gobierno Autónomo Descentralizado del Cantón Guaranda y se ha llegado a lograr lo siguiente:

Utilizar Active Directory como medida de seguridad en la Intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda es de gran importancia debido a las facilidades que nos presenta para tener a todos los usuarios dentro de un mismo dominio y poder administrarlos.

- Se logró determinar los problemas que afectaban el correcto funcionamiento, consiguiendo así la Solución de Seguridad Informática.
- Con el análisis realizado se logró encontrar la Solución de Seguridad Informática para fortalecer la confidencialidad de la información en la intranet de la Institución obteniendo grandes beneficios con su implementación.
- Con la implementación de Active Directory como Solución de Seguridad Informática se logró obtener un mayor control de los problemas ocasionados en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda.
- Se logró realizar el análisis Beneficio/Costo, dando a conocer las grandes ventajas que tiene la implementación del Directorio Activo ante sus costos que no son muy altos, proporcionando a los técnicos de la Institución una forma de administración segura y confiable de los usuarios y sus labores.
- En la ejecución de la Fase de Pruebas se comprueba que los técnicos de la Institución tengan un mayor control de los usuarios convirtiendo en un método rápido y eficaz la administración de la red.

2.7.2 RECOMENDACIONES

En relación a los resultados obtenidos en la presente investigación, y con el fin de dar protección a toda la información con la cual la Institución realiza su trabajo diariamente se presenta las siguientes recomendaciones.

Para obtener mejor seguridad y por ende mayores beneficios de Active Directory se debería aplicar las políticas de seguridad acorde a las necesidades que se vayan presentando.

- Dar seguimiento a los problemas ocasionados en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda, para emplear las directivas de grupo que controlen los mismos.
- Utilizar Active Directory como medida de seguridad para obtener una mejor administración de la tecnología y recursos de la red.
- Comprometer a los usuarios del dominio que utilicen contraseñas seguras para mantener la confidencialidad de su información.
- Se debería realizar estudios de Beneficio/Costo para sustentar la importancia que tiene la implementación de tecnología en la Unidad de Sistemas Informáticos constituyéndose en un beneficio general para toda la Institución.
- Realizar pruebas periódicas para corroborar que el funcionamiento del controlador de dominio implementado sea el correcto.

CAPITULO III

3.1 APORTE TEORICO Y / O PRÁCTICO

3.1.1 Comparación entre un Grupo de Trabajo y Controlador de Dominio

3.1.1.1 Grupo de Trabajo

Es un tipo de Agrupación más básico, diseñado únicamente para los usuarios ayudar a encontrar objetos como impresoras y carpetas compartidas en ese grupo. Cuando se une a un grupo de trabajo, hay que asignar el nombre del grupo de trabajo a la computadora.³⁵

3.1.1.2 Dominio

Es el elemento fundamental que agrupa todos los objetos como equipos y usuarios. Todos estos objetos se administraran de forma estructurada y jerárquica.³⁶

3.1.1.3 Controlador de Dominio

Su función es almacenar objetos del Directorio Activo (Active Directory) como, por ejemplo, las unidades organizativas o las cuentas de usuario.³⁷

En un Grupo de Trabajo todos los usuarios trabajan a un mismo nivel sin restricciones, es decir ninguno tiene el control sobre otro, la información es compartida entre todos los usuarios, no cuentan con políticas de seguridad, si se realiza algún cambio en uno de los equipos se debe realizar en todos porque de lo contrario los otros equipos tendrán problemas al conectarse, compartir recursos y servicios además la red no es muy segura ya que puede ser vulnerada al suplantar identidades y accesos. Esta forma organizativa de trabajo presenta un nivel de seguridad inadecuado, debido a que su configuración es fácilmente manipulable por los usuarios que lo conforman.

³⁵ Cutipa, S. (2013). Instalación y Configuración de una Red LAN con Windows Server 2003 e Internet. Recuperado de https://books.google.com.ec/books?id=Ffk9AAwAAQBAJ&dq=que+es+un+grupo+de+trabajo+de+windows&hl=es&source=gbs_navlinks_s

³⁶ Niño, J. (2011). Sistemas Operativos en Red. Recuperado de <https://books.google.com.ec/books?id=A9vJAAwAAQBAJ&pg=PA84&dq=active+directory+como+funciona&hl=es&sa=X&ei=2McBVdyQCsK6ggSn6oHIBA&ved=0CEkQ6AEwBw#v=onepage&q=active%20directory%20como%20funciona&f=false>

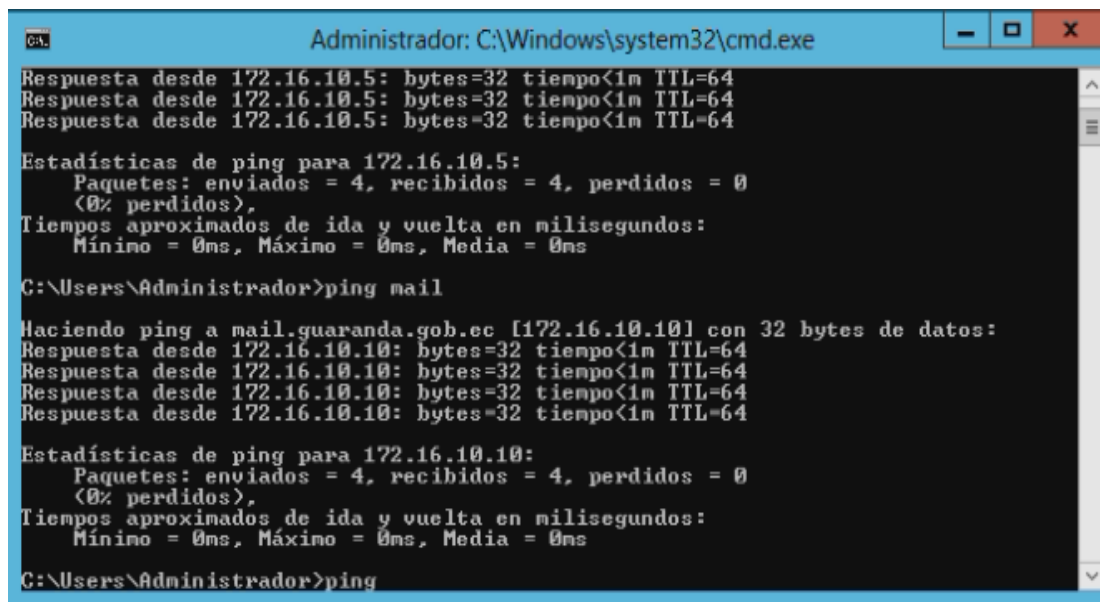
³⁷ Niño, J. (2011). Sistemas Operativos en Red. Recuperado de <https://books.google.com.ec/books?id=A9vJAAwAAQBAJ&pg=PA84&dq=active+directory+como+funciona&hl=es&sa=X&ei=2McBVdyQCsK6ggSn6oHIBA&ved=0CEkQ6AEwBw#v=onepage&q=active%20directory%20como%20funciona&f=false>

Un Dominio es más seguro que un grupo de trabajo debido a que sus contraseñas son cifradas y monitoreadas constantemente por el servidor de dominio, el cual se encarga de centralizar la seguridad y la administración de los recursos de la red. Además permite la autenticación y autorización de usuarios. Estableciendo así un mejor nivel de seguridad en relación al grupo de trabajo que es con el que trabajan en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda.

3.2 FASE 1: LEVANTAMIENTO DE INFORMACIÓN, ANALISIS.

3.2.1 Comprobación de la topología de red y conectividad actual.

En esta fase se realizarón las pruebas de conectividad remotamente hacia el servidor y a las diferentes terminales de la Institución mediante el símbolo del sistema a través del comando ping y todas su combinaciones según los requerimientos que se necesita para verificar que exista conexión en los diferentes puntos de red.



```
Administrador: C:\Windows\system32\cmd.exe
Respuesta desde 172.16.10.5: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.10.5: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.10.5: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 172.16.10.5:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>ping mail

Haciendo ping a mail.guaranda.gob.ec [172.16.10.10] con 32 bytes de datos:
Respuesta desde 172.16.10.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.10.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.10.10: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.10.10: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 172.16.10.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>ping
```

Gráfico 8 Pruebas de conectividad.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

3.2.2 Analizar las seguridades perimetrales con las que cuenta la red.

En la seguridad perimetral la red del Gobierno Autónomo Descentralizado del Cantón Guaranda cuentan con equipo firewall como se muestra en el siguiente gráfico.

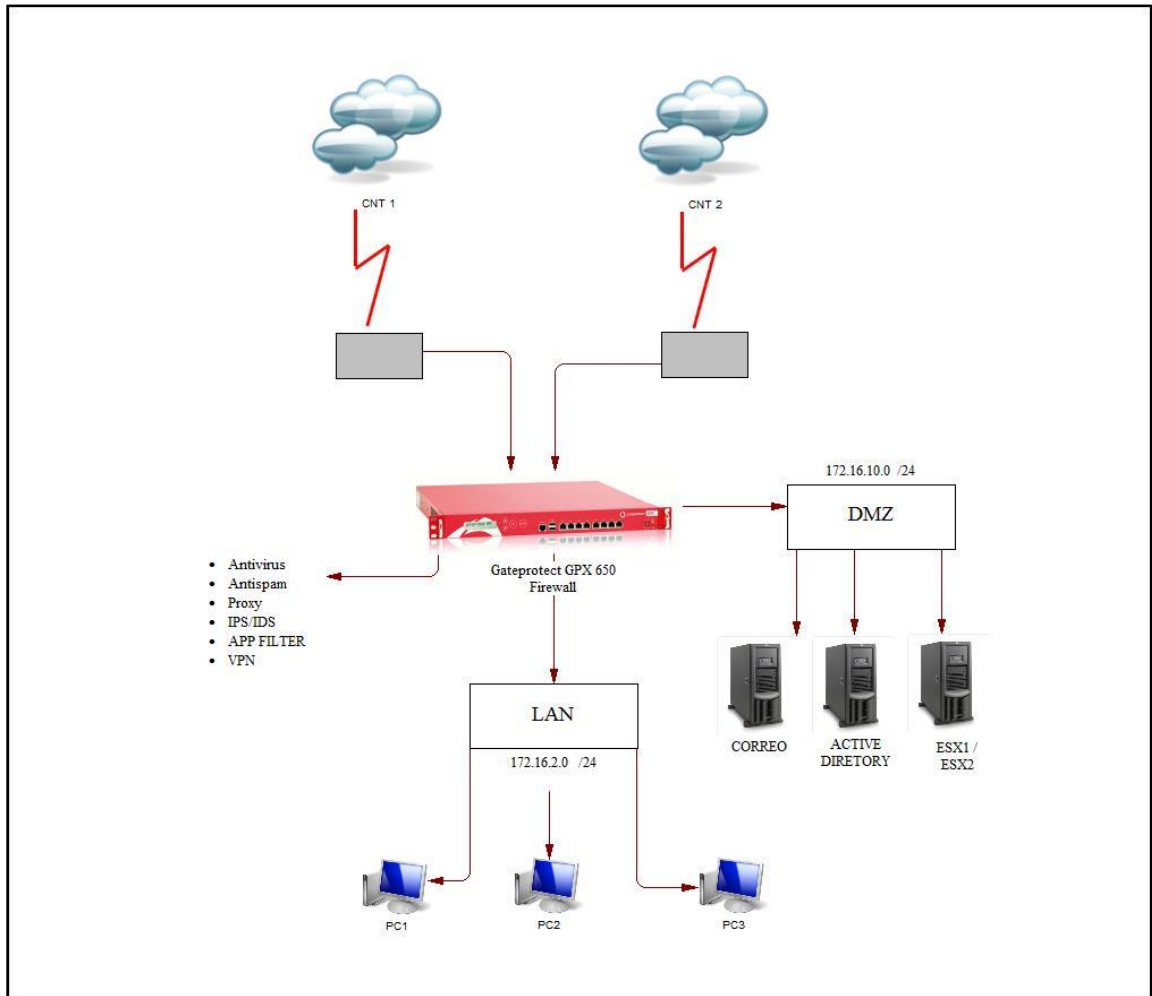


Gráfico 9 Diagrama de la Seguridad Perimetral.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

3.2.3 Definir estándares para la creación de usuarios.

Estructura de permisos y políticas que serán implementadas en el directorio activo. La definición de políticas de seguridad se ha establecido de acuerdo a las Unidades Organizativas.

CONFIGURACIÓN DE SEGURIDAD Y POLÍTICAS A NIVEL DE DOMINIO			
USUARIO	CONFIGURACIÓN (SEGURIDAD)	VALOR ESTABLECIDO	
Usuario	Horas de Inicio de Sesión	07H00 - 21H00	
Usuario	Iniciar sesión desde	gaddc01 (Servidor)	
Usuario	Contraseña nunca expira	Habilitado	
POLITICAS DE GRUPO APLICADAS			
D / OU	TIPO DE POLITICA	VALOR ESTABLECIDO	E / U
Administración General	Complejidad de la Contraseña	N/A	Equipo
Administración General	Caducidad de la Contraseña de los usuarios	N/A	Equipo
Administración General	Umbral de Bloqueo de Cuenta	3 intentos	Equipo
Administración General	Tiempo de Bloqueo de Cuenta	10 minutos	Equipo
Administración General	Tiempo de Protector de Pantalla	5 minutos	Usuario
Administración General	Protección por contraseña del protector de pantalla	N/A	Usuario
Administración General	Impedir cambios en el fondo de escritorio	N/A	Usuario
Administración General	Fondo de escritorio	\\192.168.10.11\Wallpapers\fondo.bmp	Usuario
Administración General	Cambio de la Hora del sistema	Admins. del Dominio / Grupo-Sistemas	Equipo
Administración General	Cambio de la zona horaria del sistema	Admins. del Dominio / Grupo-Sistemas	Equipo

Tabla 11 Estándares para la creación de usuarios.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

POLÍTICAS DE GRUPO ADICIONALES RECOMENDADAS			
D / OU	TIPO DE POLITICA	VALOR ESTABLECIDO	E / U
gadguaranda.local	Impedir cambio de dirección IP	N/A	Usuario
Administración General	Configuración personalizada de Internet Explorer	N/A	Usuario
gadguaranda.local	Ocultar determinados elementos del panel de control	N/A	Usuario

Tabla 12 Políticas de Grupo.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

CONFIGURACIÓN DE SEGURIDAD Y POLÍTICAS A NIVEL DE DOMINIO			
USUARIO	CONFIGURACIÓN (SEGURIDAD)	VALOR ESTABLECIDO	
Usuario	Horas de Inicio de Sesión	07H00 - 21H00	
Usuario	Iniciar sesión desde	gaddc01 (Servidor)	
Usuario	Contraseña nunca expira	Habilitado	
POLITICAS DE GRUPO APLICADAS			
D / OU	TIPO DE POLITICA	VALOR ESTABLECIDO	E / U
Tecnología	Complejidad de la Contraseña	N/A	Equipo
Tecnología	Caducidad de la Contraseña de los usuarios	N/A	Equipo
Tecnología	Umbral de Bloqueo de Cuenta	3 intentos	Equipo
Tecnología	Tiempo de Bloqueo de Cuenta	10 minutos	Equipo
Tecnología	Tiempo de Protector de Pantalla	5 minutos	Usuario
Tecnología	Protección por contraseña del protector de pantalla	N/A	Usuario
Tecnología	Impedir cambios en el fondo de escritorio	N/A	Usuario
Tecnología	Fondo de escritorio	\\192.168.10.11\Wallpapers\fondo.bmp	Usuario
Tecnología	Cambio de la Hora del sistema	Admins. del Dominio / Grupo-Sistemas	Equipo
Tecnología	Cambio de la zona horaria del sistema	Admins. del Dominio / Grupo-Sistemas	Equipo

Tabla 13 Políticas de Grupo para Sistemas Informáticos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

POLÍTICAS DE GRUPO ADICIONALES RECOMENDADAS			
D / OU	TIPO DE POLITICA	VALOR ESTABLECIDO	E / U
gadguaranda.local	Impedir cambio de dirección IP	Inhabilitado	Usuario
Administración General	Configuración personalizada de Internet Explorer	Inhabilitado	Usuario
gadguaranda.local	Ocultar determinados elementos del panel de control	Inhabilitado	Usuario

Tabla N° 1 Políticas de Grupo para Sistemas Informáticos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

3.2.3.1 Matrices para el levantamiento de información de los usuarios del Gobierno Autónomo Descentralizado del Cantón Guaranda.

3.2.3.1.1 Dirección de Administración General

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Administración General			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono/Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Ramsses	Torres	Alcalde	Alcaldía	2 981 643 IP 3048	guaranda.gob.ec	RAMSSESTORRES	g123	AGAL01
María	García	Secretaria-Alcaldía	Alcaldía		guaranda.gob.ec	MARIAGARCIA	g123	AGAL02
María	Pazmiño	Secretaria-General	Alcaldía	IP 3055	guaranda.gob.ec	MARIAPAZMIÑO	g123	AGAL03
Ángela	García	Conmutador	Alcaldía	IP 3000-3050- 3051	guaranda.gob.ec	ANGELAGARCIA	g123	AGAL04
German	Ramos	Pro-secretario	Alcaldía		guaranda.gob.ec	GERMANRAMOS	g123	AGAL05

Tabla 14 Usuarios de Administración General.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

3.2.3.1.2 Dirección de Comunicación

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Dirección de Comunicación			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Emilio	Sánchez	Director	Dirección de Comunicación	2 985 425	guaranda.gob.ec	EMILIOSANCHEZ	g123	DC01
Ángela	García	Secretaria	Dirección de Comunicación	IP 3032	guaranda.gob.ec	ANGELAGARCIA	g123	DC02
Víctor	Poma	Asistente de periodismo	Dirección de Comunicación		guaranda.gob.ec	VICTORPOMA	g123	DC03
Cristian	Gutiérrez	Asistente de periodismo	Dirección de Comunicación		guaranda.gob.ec	CRISTIANGUTIERREZ	g123	DC04
Mario	Arias	Diseñador	Dirección de Comunicación		guaranda.gob.ec	MARIOARIAS	g123	DC05
Carolina	Carrillo	Reportera	Dirección de Comunicación		guaranda.gob.ec	CAROLINACARRILLO	g123	DC06
Javier	Lumbi	Reportera	Dirección de Comunicación		guaranda.gob.ec	JAVIERLUMBI	g123	DC07
Wilmer	Curí	Camarógrafo	Dirección de Comunicación		guaranda.gob.ec	WILMERCURI	g123	DC08
Andrea	Vasconez	Productora	Dirección de Comunicación		guaranda.gob.ec	ANDREAVASCONEZ	g123	DC09

Tabla 15 Usuarios de la Dirección de Comunicación.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.3 Secretaría de Concejo

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Secretaría de Concejo			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Miguel	León	Secretario	Secretaria de Concejo	2 985 423	guaranda.gob.ec	MIGUELLEON	g123	SC01
Mercedes	Aluisa	Redacción de actas	Secretaria de Concejo	IP 3002	guaranda.gob.ec	MERCEDESALUISA	g123	SC02

Tabla 16 Usuarios de Secretaría de Concejo.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.4 Dirección Procuraduría Sindica

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Procuraduría Sindica			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname e equipo
Aníbal	García	Procurador Sindico	Procuraduría Sindica	2 980 352 IP3005	guaranda.gob.ec	ANIBALGARCIA	g123	PS01
Patricia	Chávez	Secretaria	Procuraduría Sindica	IP 3043	guaranda.gob.ec	PATRICIACHAVEZ	g123	PS02
Álvaro	Escobar	Abogado	Procuraduría Sindica		guaranda.gob.ec	ALVAROESCOBAR	g123	PS03
David	García	Asistente de Abogacía	Procuraduría Sindica		guaranda.gob.ec	DAVIDGARCÍA	g123	PS04

Tabla 17 Usuarios de la Dirección Procuraduría Sindica.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.5 Auditoría Interna

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Auditoría Interna			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Nancy	Tariz	Auditora Interna	Auditoría Interna	IP 3052	guaranda.gob.ec	NANCYTARIS	g123	AI01

Tabla 18 Usuarios de Auditoría Interna.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.6 C.C. Tambo del Libertador

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	C.C. Tambo del Libertador			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Miguel	Vizcaíno	Administrador	C.C. Tambo del Libertador	2980 634	guaranda.gob.ec	MIGUELVISCAINO	g123	TL01

Tabla 19 Usuarios de C.C. Tambo del Libertador.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.7 Dirección Administrativa

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Dirección Administrativa			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
María	Ozorio	Director	D.A y Servicios Generales	IP 3053	guaranda.gob.ec	MARIAOZORIO	g123	DA01
Blanca	Purcachi	Secretaria	D.A y Servicios Generales	IP 3038	guaranda.gob.ec	BLANCAPURCACHI	g123	DA02
Marisol	Manobanda	Secretaria	D.A y Servicios Generales		guaranda.gob.ec	MARISOLMANOBANDA	g123	DA03
Marco	Gutiérrez	Jefe de Servicios	Servicios Inst. y Municipales	IP 3025	guaranda.gob.ec	MARCOGUTIERREZ	g123	DASI04
Segundo	Llumiguano	Administrador cementerio	Cementerio	2 985 876	guaranda.gob.ec	SEGUNDOLLUMIGUANO	g123	DACG05
Alex	Silva	Administrador	Terminal Terrestre	2 980 173 IP 3028	guaranda.gob.ec	ALEXSILVA	g123	DATT06
Eugenia	Chávez	Secretaria	Terminal Terrestre		guaranda.gob.ec	EUGENIACHAVEZ	g123	DATT07
Jaime	Gaïbor	Jefe de Sistemas	Sistemas I.	IP 3014	guaranda.gob.ec	JAIMEGAIBOR	g123	DASIFS08
Jaime	Gaïbor	Jefe de Sistemas	Sistemas I.		guaranda.gob.ec	JAIMEGAIBOR	g123	DASIFS09
Jaime	Gaïbor	Jefe de Sistemas	Sistemas I.		guaranda.gob.ec	JAIMEGAIBOR	g123	DASIFS10
Jaime	Gaïbor	Jefe de Sistemas	Sistemas I.		guaranda.gob.ec	JAIMEGAIBOR	g123	DASIFS11

Nerio Roi	Olalla	Asistente de Tecnología de Información	Sistemas I.		guaranda.gob.ec	ROIOLALLA	g123	DASI12
Steve	Naranjo	Asistente de Tecnología de Información	Sistemas I.		guaranda.gob.ec	STEVENARANJO	g123	DASI13
Steve	Naranjo	Asistente de Tecnología de Información	Sistemas I.		guaranda.gob.ec	STEVENARANJO	g123	DASIFS14
Roberto	Mejía	Administrador	Plaza Comercial Animales	2207 029	guaranda.gob.ec	ROBERTOMEJIA	g123	DASI15
Javier	Ballesteros	Director	Adquisiciones		guaranda.gob.ec	JAVIERBALLESTEROS	g123	DAA16
Napoleón	Cunalata	Asistente de adquisiciones	Adquisiciones	2985 940	guaranda.gob.ec	NAPOLEONCUNALATA	g123	DAA17
Darío	Albán	Asistente de adquisiciones	Adquisiciones		guaranda.gob.ec	DARIOALBAN	g123	DAA18
Martha	Rea	Secretaria Adquisiciones	Adquisiciones		guaranda.gob.ec	MARTHAREA	g123	DAA19
Diana	Alarcón	Secretaria	Compras Públicas	2985 661	guaranda.gob.ec	DIANAALARCON	g123	DACP20
Hernán	Ramos	Comisario	Comisaría Municipal	2980 635	guaranda.gob.ec	HERNANRAMOS	g123	DACM21
Lilian	Pazmiño	Secretaria Comisaria	Comisaría Municipal		guaranda.gob.ec	LILIANPAZMIÑO	g123	DACM22
Policía	Municipal	Policías	Comisaría Municipal		guaranda.gob.ec	POLICIA	g123	DACM0123
Ramiro	Pazos	Jefe de Guarda Almacén	Guarda Almacén	2980 690 IP 3034	guaranda.gob.ec	RAMIROPAZOS	g123	DAGA24
Klever	Pachala	Asistente de Guarda almacén	Guarda Almacén		guaranda.gob.ec	KLEVERPACHALA	g123	DAGA25

Tabla 20 Usuarios de la Dirección Administrativa.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.8 Dirección de Talento Humano

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Dirección de Talento Humano			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Luis	Mediavilla	Director	Dirección de Talento Humano	IP 3033	guaranda.gob.ec	LUISMEDIAVILLA	g123	DTH01
Katuska	Ribadeneira	Asistente del Director	Dirección de Talento Humano	IP 3039	guaranda.gob.ec	KATIUSKARIBADENEIRA	g123	DTH02
Narcisa	Ulloa	Secretaria	Dirección de Talento Humano	IP 3016	guaranda.gob.ec	NARCISAULLOA	g123	DTH03
Deysi	Sánchez	Secretaria	Dirección de Talento Humano	2980 180	guaranda.gob.ec	DEYSISANCHEZ	g123	DTH04
Oscar	González	Analista de recursos	Dirección de Talento Humano		guaranda.gob.ec	OSCARGONZALEZ	g123	DTH05
Alfonso	Hurtado	Secretario	Dirección de Talento Humano		guaranda.gob.ec	ALFONSOHURTADO	g123	DTH06
Angélica	Núñez	Secretaria	Dirección de Talento Humano		guaranda.gob.ec	ANGELICANUNEZ	g123	DTH07

Tabla 21 Usuarios de la Dirección de Talento Humano.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.9 Dirección de Desarrollo Comunitario y Gestión Social

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Dirección de Desarrollo Comunitario y Gestión Social.			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Pablo	Escorza	Director	D. de Desarrollo Comunitario y Gestión Social	2 980 327 IP 3047	guaranda.gob.ec	PABLOESCORZ	g123	DDC01
Mónica	Muñoz	Jefa de Cultura	Cultura	IP 3006	guaranda.gob.ec	MONICAMUÑOZ	g123	DDCCU02
Carlos	Ninabanda	Promotor Cultural	Cultura		guaranda.gob.ec	CARLONINABANDA	g123	DDCCU03
Rosa	Velasco	Secretaria	Cultura		guaranda.gob.ec	ROSAVELASCO	g123	DDCCU04
Gonzalo	Aucatoma	Administrador	Coliseo	2 982 133	guaranda.gob.ec	GONZALO AUCATOMA	g123	DDCO05
Verónica	Flores	Secretaria	Desarrollo Comunitario		guaranda.gob.ec	VERONICAFLORES	g123	DDCDC06
José	Chela	Promotor	Desarrollo Comunitario		guaranda.gob.ec	JOSECHELA	g123	DDCDC07
Freddy	Flores	Promotor	Desarrollo Comunitario	2985 424	guaranda.gob.ec	FREDYFLORES	g123	DDCDC08
Esther	Yumbay	Promotora	Desarrollo Comunitario		guaranda.gob.ec	ESTHERYUMBAY	g123	DDCDC09
Nancy Cecilia	Recalde	Secretaría Gestión Turística	Gestión Turística	IP 3019	guaranda.gob.ec	CECILIARECALDE	g123	DDCGT10

José	Vizcaíno	Inspector de Servicios Municipales	Gestión Turística		guaranda.gob.ec	JOSEVISCAINO	g123	DDCGT11
Mario	Barrionuevo	Oficinista	Gestión Turística		guaranda.gob.ec	MARIOBARRIONUEVO	g123	DDCGT12
Marisol	Arellano	Secretaría	C.C Indio Guaranda	2980 757	guaranda.gob.ec	MARISOLARELLANO	g123	DDCIG13
Zoila	Analuisa	Promotora Social	Concejo de Niñez y Adolescencia	2985 629	guaranda.gob.ec	ZOILAANALUISA	g123	DDCCN14
Leticia	Fierro	Secretaria	C. de Niñez y Adolescencia		guaranda.gob.ec	LETICIAFIERRO	g123	DDCCN15
Nelly	Aucatoma	Secretaria	C. de Niñez y Adolescencia		guaranda.gob.ec	NELLYAUCATOMA	g123	DDCCN16
Mónica	Aroca	Secretaria	C. de Niñez y Adolescencia		guaranda.gob.ec	MONICAROCA	g123	DDCCN17
Luis	Lucio	Asesor Jurídico	C. de Niñez y Adolescencia		guaranda.gob.ec	LUISLUCIO	g123	DDCCN18
Alexandra	Andrade	Secretaria	C. de Niñez y Adolescencia		guaranda.gob.ec	ALEXANDRAANDRADE	g123	DDCCN19

Tabla 22 Usuarios de la Dirección de Desarrollo Comunitario y Gestión Social.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.10 Dirección de Gestión Ambiental

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Dirección de Gestión Ambiental			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Marcelo	Borja	Director	D. de Gestión Ambiental	2982 808	guaranda.gob.ec	MARCELOBORJA	g123	DGA01
Gabriela	Lara	Secretaría	Dirección de Gestión Ambiental	IP 3030	guaranda.gob.ec	GABRIELALARA	g123	DGA02
Rolando	Manobanda	Administrador	Centro de Faenamiento	2980 756 IP 3029	guaranda.gob.ec	ROLANDOMANOBA NDA	g123	DGACF03
Washington	Manobanda	Veterinario	Centro de Faenamiento		guaranda.gob.ec	WASHINGTONMAN OBANDA	g123	DGACF04
Iván	Mora	Administrador	Mercado 10 de Noviembre	IP 3018	guaranda.gob.ec	IVANMORA	g123	DGAMN05
Ruth	Villena	Secretaria	Mercado 10 de Noviembre		guaranda.gob.ec	RUTHVILLENA	g123	DGAMN06
Segundo	Jiménez	Administrador	Mercado 24 de Mayo	2980 976	guaranda.gob.ec	SEGUNDOJIMENEZ	g123	DGAMM07
Washington	Naranjo	Secretario	Mercado 24 de Mayo		guaranda.gob.ec	WASHINGTONNARANJO	g123	DGAMM08
Paulina	Naranjo	Jefa de Medio Ambiental	Medio Ambiente		guaranda.gob.ec	PAULINANARANJO	g123	DGAMA09
Neicer	Caspi	Promotores	Medio Ambiente		guaranda.gob.ec	NEICERCASPI	g123	DGAMA10
Ángel	Murillo	Asistente de control Sanitario	Medio Ambiente		guaranda.gob.ec	ANGELMURILLO	g123	DGAMA11

Diana	Noboa	Promotora Ambiental	Medio Ambiente		guaranda.gob.ec	DIANANOBOA	g123	DGAMA12
Gabriela	López	Secretaria	Medio Ambiente		guaranda.gob.ec	GABRIELALOPEZ	g123	DGAMA13

Tabla 23 Usuarios de la Dirección de Gestión Ambiental.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.11 Dirección de Planificación Territorial

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Dirección de Planificación Territorial			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Vicente	López	Director	Dirección de Planificación Territorial	2980 759 IP 3022	guaranda.gob.ec	VICENTELOPEZ	g123	DPT01
José	Camacho	Atención al Cliente	Dirección de Planificación Territorial	IP 3008	guaranda.gob.ec	JOSECAMACHO	g123	DPT02
Javier	Zurita	Administrador	Esmart-G		guaranda.gob.ec	JAVIERZURITA	g123	DPTEG03
Joffre	Naranjo	Comisario de Construcciones	Comisaria de Construcciones	IP 3010	guaranda.gob.ec	JOFFRENARANJO	g123	DPTCC04
Fausto	Agualongo	Asistente de Abogacía	Comisaria de Construcciones		guaranda.gob.ec	FAUSTOAGUALONGO	g123	DPTCC05
Paulina	González	Secretaria	Comisaria de Construcciones	IP 3024	guaranda.gob.ec	PAULINAGONZALEZ	g123	DPTCC06

Fernando	Vásconez	Técnico de Planificación Personal	Urbanismo	IP 3020	guaranda.gob.ec	FERNANDOVASCONEZ	g123	DPTUR07
Silvia	Meza	Jefe de Avalúos y Catastros	Avalúos y Catastros	IP 3015	guaranda.gob.ec	SILVIAMEZA	g123	DPTAC08
Carmen	Chimbo	Secretaria	Avalúos y Catastros	IP 3031	guaranda.gob.ec	CARMENCHIMBO	g123	DPTAC09
Mauro	Orozco	Asistente de Avalúos	Avalúos y Catastros		guaranda.gob.ec	MAUROOROZCO	g123	DPTAC10
Javier	Navarrete	Asistente de Avalúos	Avalúos y Catastros		guaranda.gob.ec	JAVIERNAVARRETE	g123	DPTAC11
Marcelo	Collaguazo	Asistente de Avalúos	Avalúos y Catastros		guaranda.gob.ec	MARCELOCOLLAGUAZO	g123	DPTAC12
Margoth	Pazmiño	Secretaria	Avalúos y Catastros		guaranda.gob.ec	MARGOTHPAZMIÑO	g123	DPTAC13
Blanca	Chamorro	Secretaria	Planificación		guaranda.gob.ec	BLANCACHAMORRO	g123	DPTP14
María Augusta	Valdiviezo	Analista Av. y catastros	Avalúos y Catastros		guaranda.gob.ec	MARIAVALDIVIEZO	g123	DPTAC15
Gonzalo	Sisalema	Asistente de Planificación	Planificación		guaranda.gob.ec	GONZALOSISALEMA	g123	DPTP16
Laura	Carrasco	Asistente de Planificación	Planificación		guaranda.gob.ec	LAURACARRASCO	g123	DPTP17
Patricio	Medina	Técnico de riesgos	Planificación		guaranda.gob.ec	PATRICIOMEDINA	g123	DPTP18
Ramiro	Alegría	Arquitecto	Planificación		guaranda.gob.ec	RAMIROALEGRIA	g123	DPTP19
Jimmi	Mena	Técnico en Planificación	Planificación		guaranda.gob.ec	JIMMIMENA	g123	DPTP20
Ángel	Ruiz	Técnico en Planificación	Planificación		guaranda.gob.ec	ANGELRUIZ	g123	DPTP21
Josué	Mestanza	Dibujante	Planificación		guaranda.gob.ec	JOSUEMESTANZA	g123	DPTP22

Tabla 24 Usuarios de la Dirección de Planificación Territorial.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.12 Dirección de Obras Públicas

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Dirección de Obras Públicas			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Rolando	Terán	Director	Dirección de Obras Públicas	IP 3045	guaranda.gob.ec	ROLANDOTERAN	g123	DOP01
Laura	Salto	Secretaría	Dirección de Obras Públicas	IP 3032	guaranda.gob.ec	LAURASALTOS	g123	DOP02
Jaime	Chimbo	Asistente	Obras Publicas		guaranda.gob.ec	JAIMECHIMBO	g123	DOP03
David	Peñaloza	Ingeniero en Obras Públicas	Dirección de Obras Públicas		guaranda.gob.ec	DAVIDPENALOZA	g123	DOP04
Carlos	Orozco	Técnico de Obras Públicas	Dirección de Obras Públicas		guaranda.gob.ec	CARLOSOROZCO	g123	DOP05
Manuel	Yáñez	Técnico de Obras Públicas	Dirección de Obras Públicas		guaranda.gob.ec	MANUELYANEZ	g123	DOP06
Guillermo	Escobar	Técnico de Obras Públicas	Dirección de Obras Públicas		guaranda.gob.ec	GUILLERMOESCOBAR	g123	DOP07
Fabián	Chimbo	Asistente	Dirección de Obras Públicas		guaranda.gob.ec	FBIANCHIMBO	g123	DOP08
Luis	Chacán	Técnico de Obras Públicas	Dirección de Obras Públicas		guaranda.gob.ec	LUISCHACAN	g123	DOP09

Tabla 25 Usuarios de la Dirección de Obras Públicas.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.13 Unidad Municipal de Tránsito

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Unidad Municipal de Tránsito			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Garita	Poliocia	Seguridad y Vigilancia	Unidad Municipal de Tránsito		guaranda.gob.ec	GARITAPOLIOCIA	g123	UMT01
María	Moncayo	Secretaria	Unidad Municipal de Tránsito		guaranda.gob.ec	MARIAMONCAYO	g123	UMT02
Juan Carlos	Arroba	Asistente	Unidad Municipal de Tránsito		guaranda.gob.ec	JUANARROBA	g123	UMT03
Wilson	Cárdenas	Asistente	Unidad Municipal de Tránsito		guaranda.gob.ec	WILSONCARDENAS	g123	UMT04

Tabla 26 Usuarios de la Unidad Municipal de Tránsito.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.2.3.1.14 Registro de la Propiedad

LISTA DE USUARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA								
Elaborado por :	Karla Barragán, Jessica Rea			Autorizado por :	Departamento de Sistemas			
Departamento :	Registro de la Propiedad			Fecha de revisión :	24/03/2015			
Fecha :	19/03/2015							
Nombres	Apellidos	Cargo	Departamento	Teléfono / Fax / Ext	Nombre de dominio	Nombre de usuario	Password temporal	Hostname equipo
Alfonso	Bonilla	Registrador	Registro Propiedad	2986 250	guaranda.gob.ec	ALFONSOBONILLA	g123	RP01
Iván	Naranjo	Asistente	Registro Propiedad		guaranda.gob.ec	IVANNARANJO	g123	RP02
Mercedes	García	Asistente	Registro Propiedad		guaranda.gob.ec	MERCEDESGARCIA	g123	RP03
Karina	Urbina	Asistente	Registro Propiedad		guaranda.gob.ec	KARINAURBINA	g123	RP04
Lorena	Velasco	Asistente	Registro Propiedad		guaranda.gob.ec	LORENAVELASCO	g123	RP05
Raúl	González	Asistente	Registro Propiedad		guaranda.gob.ec	RAULGONZALEZ	g123	RP06
Mercy	Gavilánez	Asistente	Registro Propiedad		guaranda.gob.ec	MERCYGAVILANEZ	g123	RP07

Tabla 27 Usuarios de Registro de la Propiedad.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.3 FASE 2: IMPLEMENTACIÓN DEL DIRECTORIO ACTIVO

3.3.1 Instalación del Servidor.

3.3.1.1 Windows Server 2012

Windows Server 2012 es el sucesor de Windows Server 2008 R2. En esta versión trae consigo funcionalidades como crear un Dominio de Active Directory, así como gestionar funcionalidades críticas de una red empresarial tales como DHCP o DNS. Unos de los principales añadidos es la gestión de cloud privadas. Este sistema operativo facilita las infraestructuras virtuales.³⁸

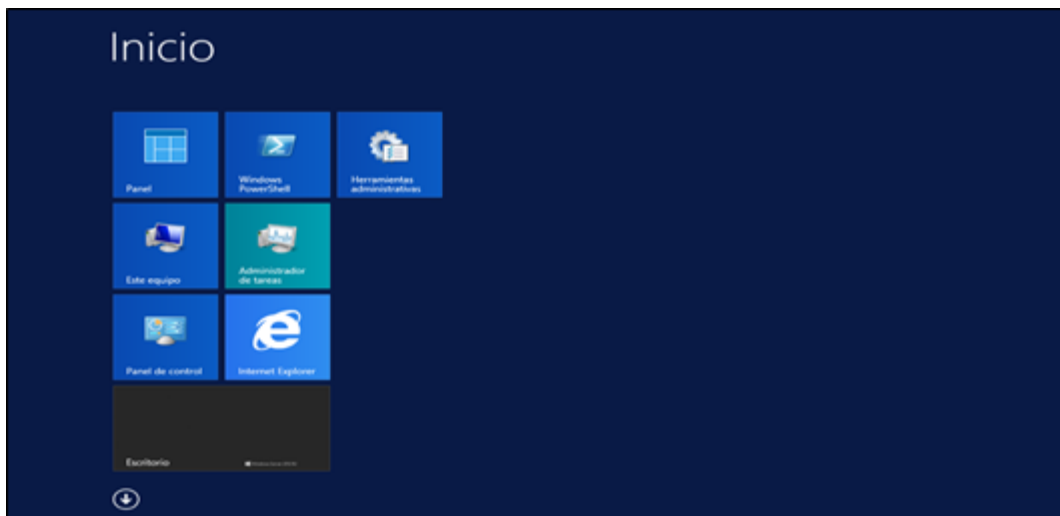


Gráfico 10 Panel de Inicio de Windows Server 2012.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

La Instalación del Servidor de Controlador de dominio se realizó en uno de los servidores de correo, el cual se encuentra virtualizado.

³⁸ Paiola, P. (2013). Windows 8 Instalación y Configuración. Barcelona. Ediciones Eni

3.3.2 Instalación del Servidor de Dominio

Antes de empezar se debe cambiar el Nombre de Equipo (Servidor). Equipo – Propiedades – Cambiar Configuración – Cambiar – Nombre del Equipo.

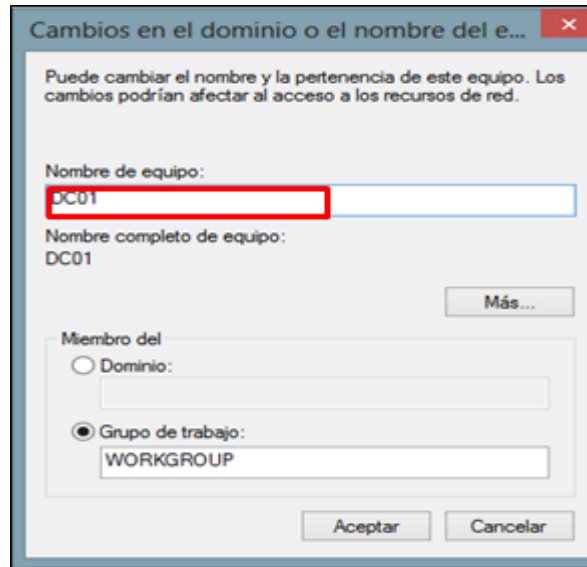


Gráfico 11 Cambiar Nombre de Equipo.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Inicio – Herramientas Administrativas – Administrador del Servidor.

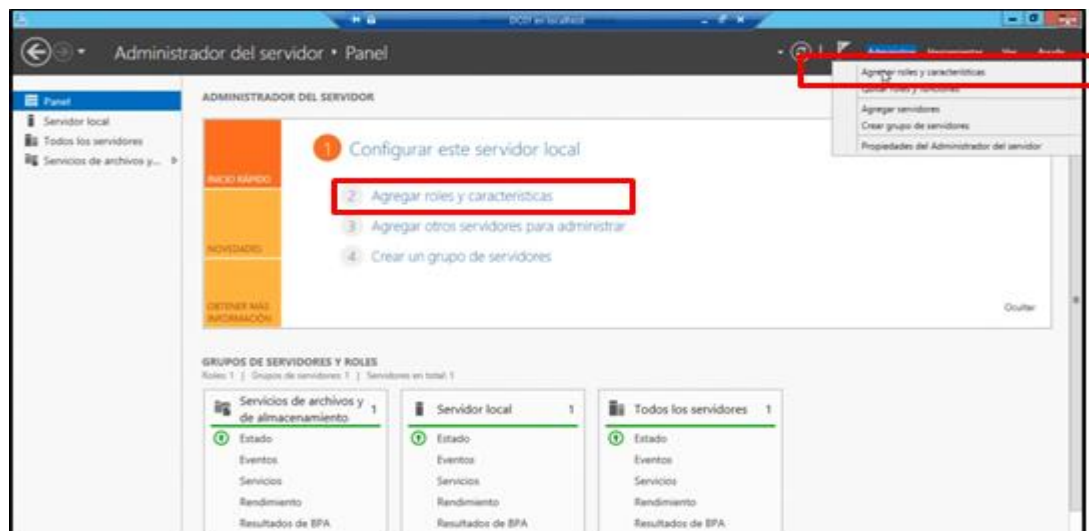


Gráfico 12 Administrador del Servidor.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Agregar roles y características – Instalación basada en características o roles – Seleccionar un servidor del grupo de servidores.

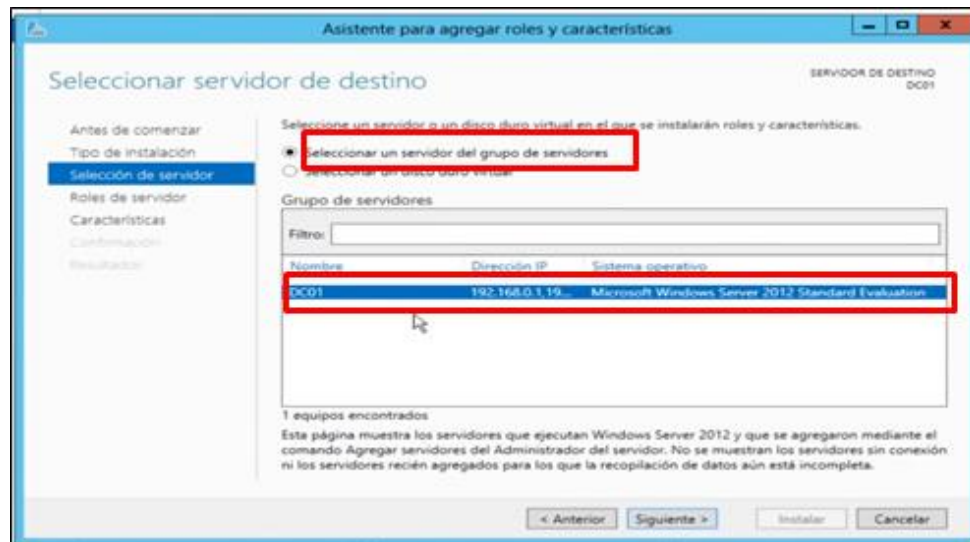


Gráfico 13 Servidor Destino.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Servicios de Dominio de Active Directory – Agregar características. Las características se agregan automáticamente para proceder a instalarse.

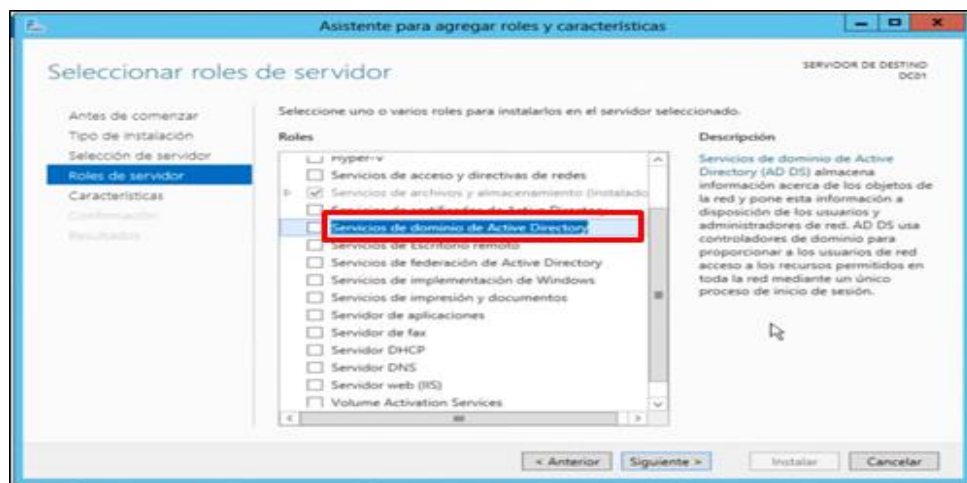


Gráfico 14 Roles de Servidor.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Lista de todas la características del Controlador de dominio – Instalar.

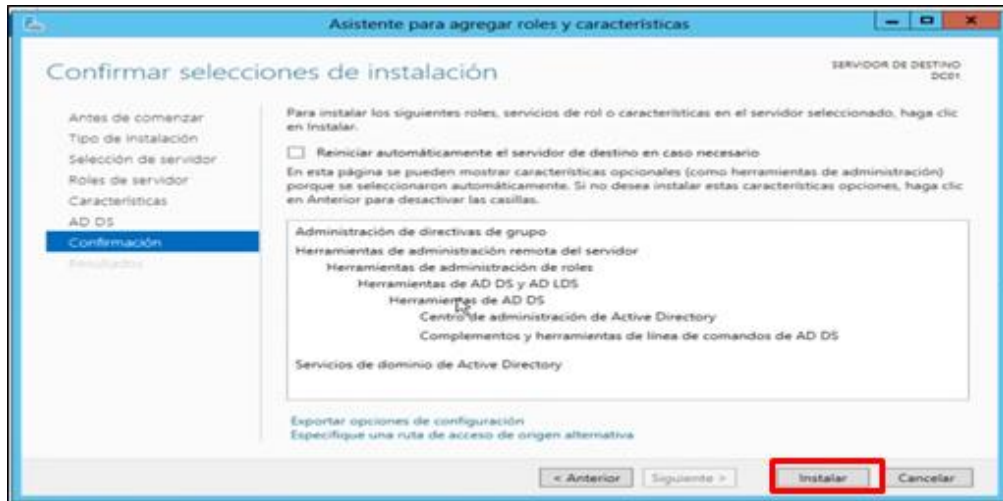


Gráfico 15 Selecciones de Instalación.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Una vez instalado los roles y las diferentes características procedemos a: Para que la maquina sea un controlador de dominio se requiere lo siguiente:

Promover este servidor a controlador de dominio, utilizando el enlace al asistente.

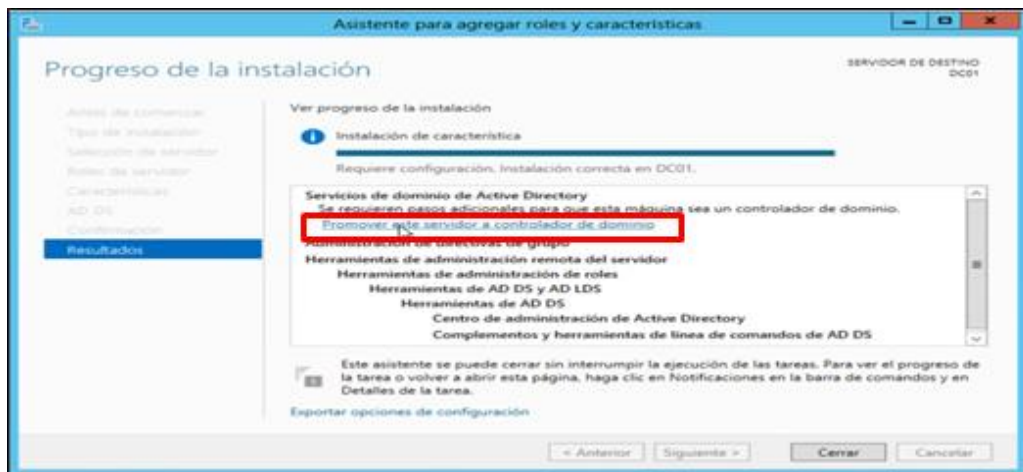


Gráfico 16 Promover a controlador de dominio.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Se despliega el asistente de configuración de Servicios de Active Directory para seguir con la instalación.

Agregar un bosque nuevo – Digitar el Nombre del dominio raíz – guaranda.gob.ec.

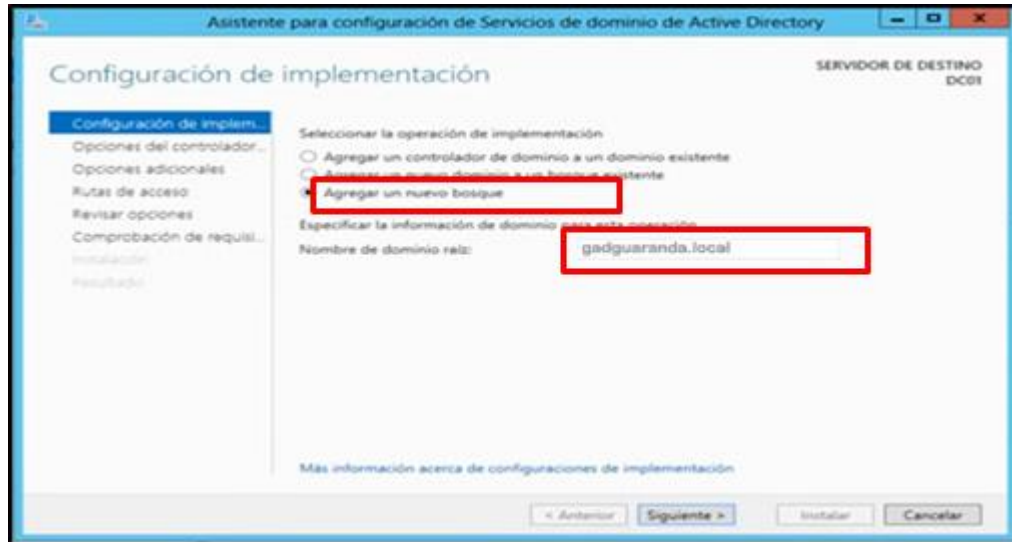


Gráfico 17 Configuración de Implementación.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Opciones de controlador de dominio.

Establecemos una contraseña con un nivel de seguridad alto utilizando caracteres especiales como por ejemplo: @, ?, ¡, \$, ..., etc. También mayúsculas y minúsculas.

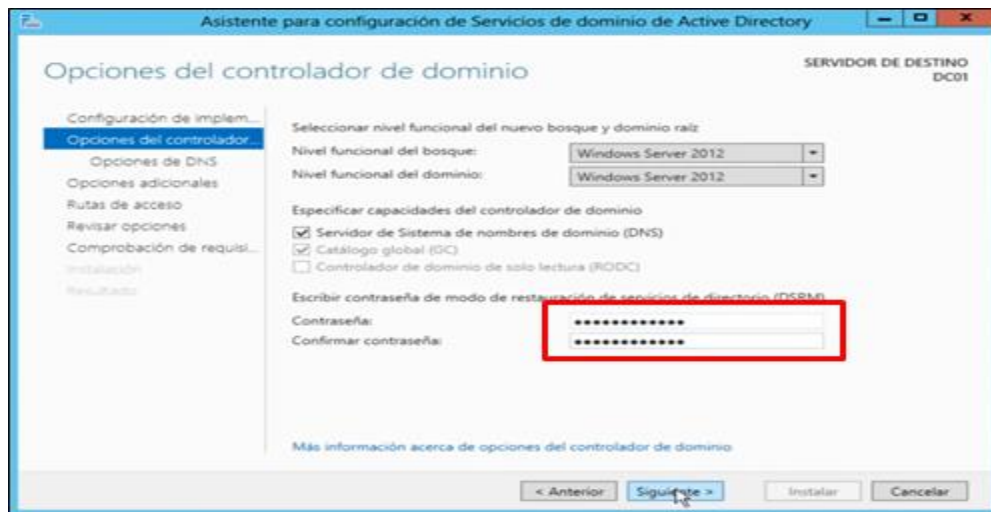


Gráfico 18 Opciones de Controlador de Dominio.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

No se puede crear una delegación DNS, omitimos para luego configurarlo, pasamos al proceso que continua.

Opciones Adicionales, se genera automáticamente del nombre de dominio raíz.

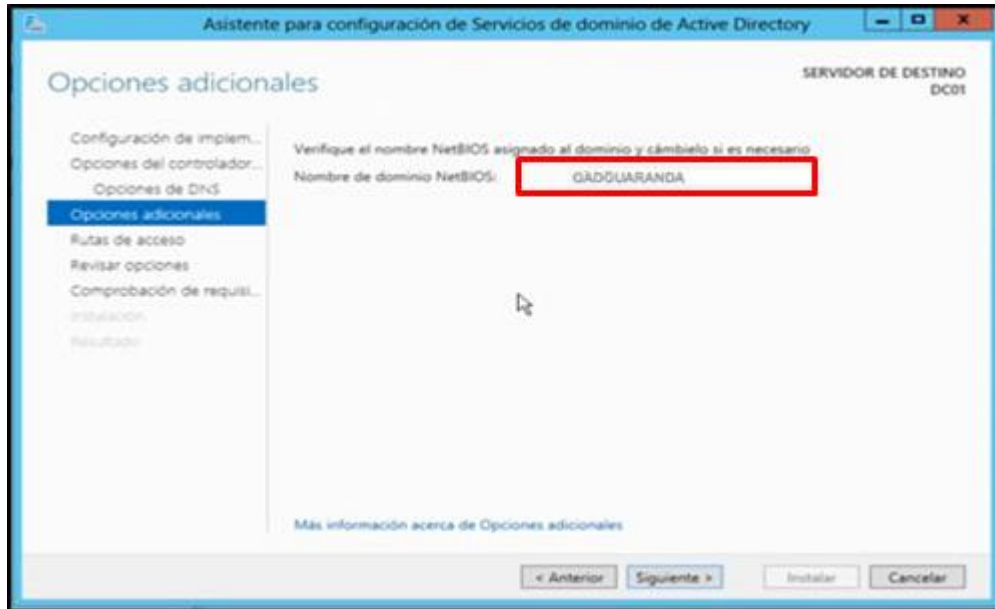


Gráfico 19 Opciones Adicionales.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Rutas de acceso – Para especificar la ubicación de la base de datos de Active Directory.

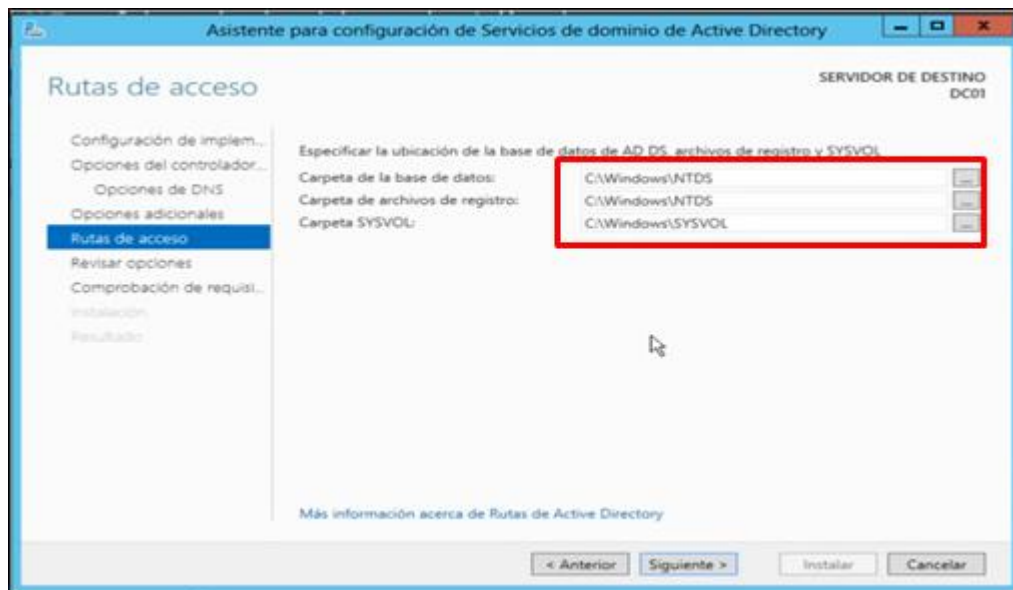


Gráfico 20 Rutas de Acceso.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Revisar Opciones – Resumen de las opciones a configurar.

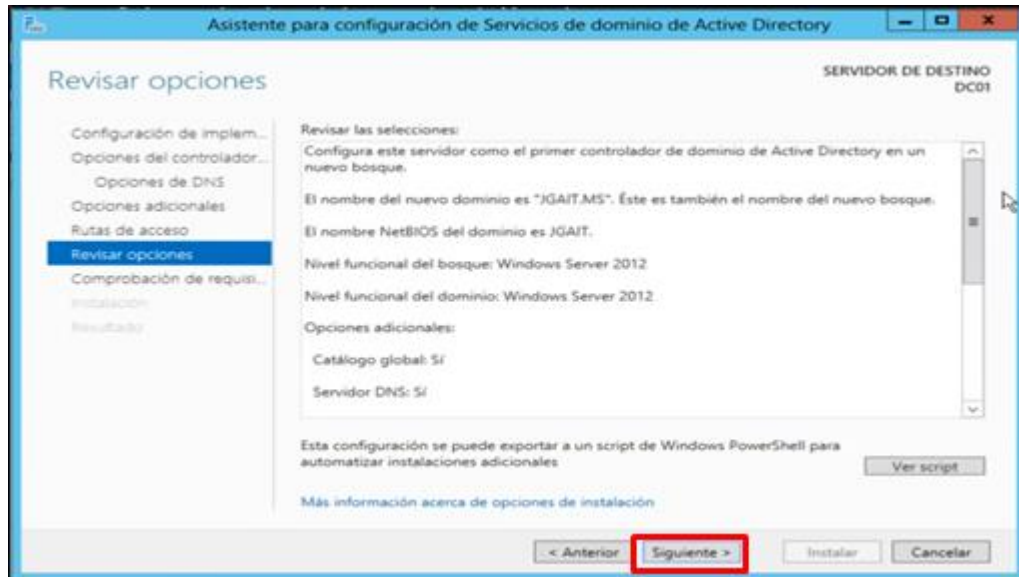


Gráfico 21 Opciones a configurar.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Comprobación de requisitos previos y valoración de una serie de servicios que debe tener el controlador de dominio, para la instalación.

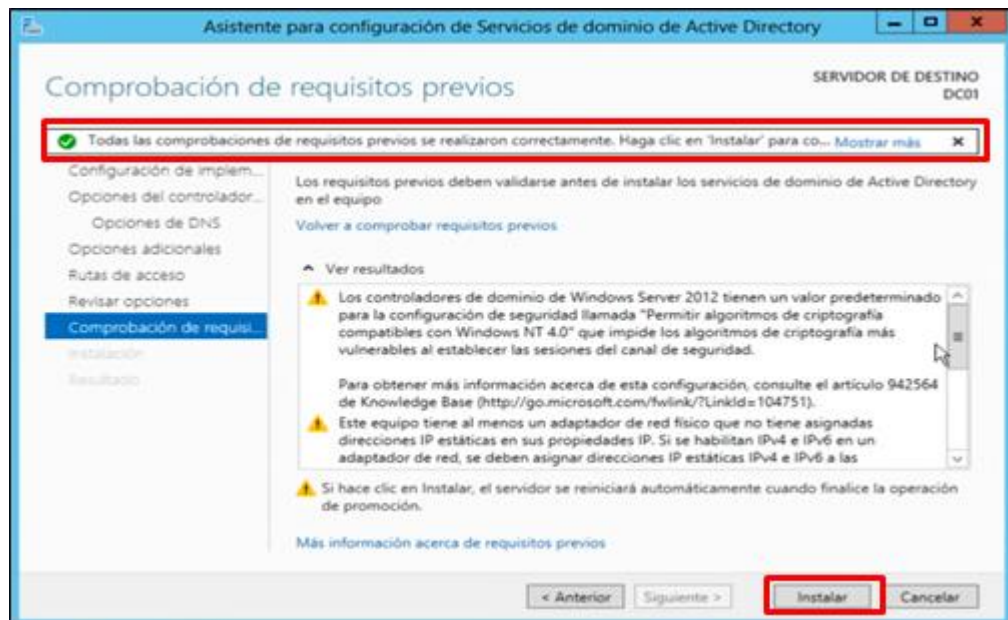


Gráfico 22 Requisitos Previos de Instalación.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Completada la instalación se mostrara el siguiente mensaje: el servidor se ha configurado correctamente como controlador de dominio. Una vez terminada la instalación del controlador de dominio la maquina se reiniciara para establecer los cambios o configuraciones efectuadas.

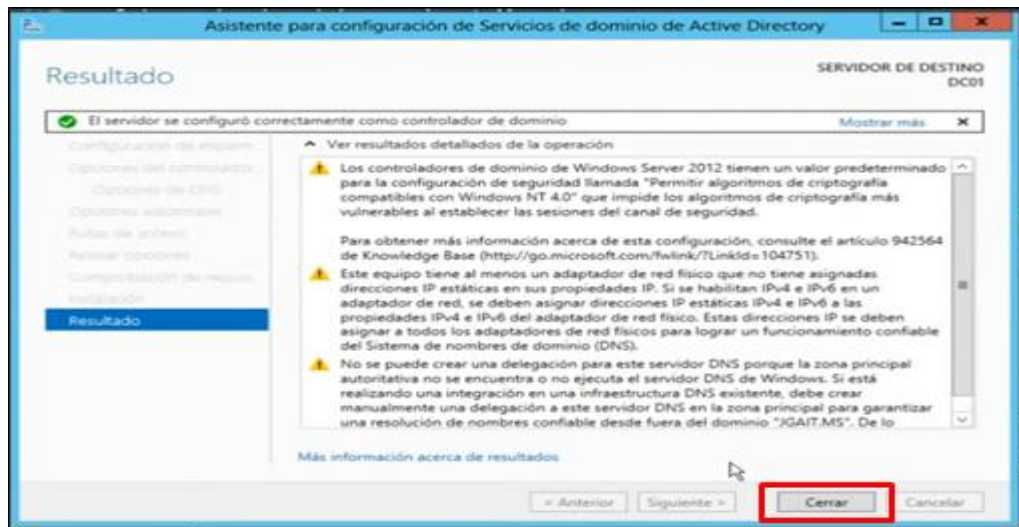


Gráfico 23 Instalación Completada.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Una vez instalado el controlador de dominio se reinicia el equipo para establecer todas las configuraciones realizadas, iniciando como controlador de dominio GADGUARANDA\Administrador.

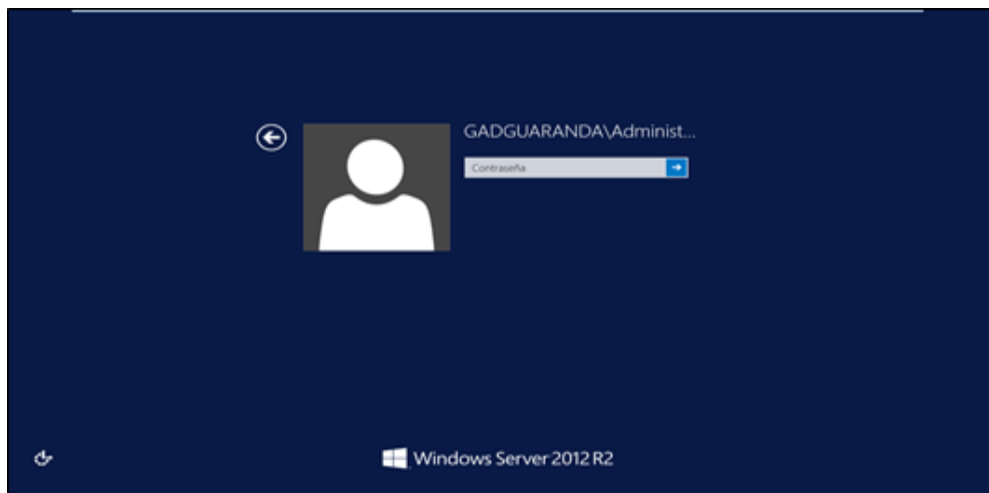


Gráfico 24 Inicio de Sesión del Controlador de Dominio.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Panel Administrador del Servidor, instalado y configurado el rol de Active Directory y el rol de DNS.

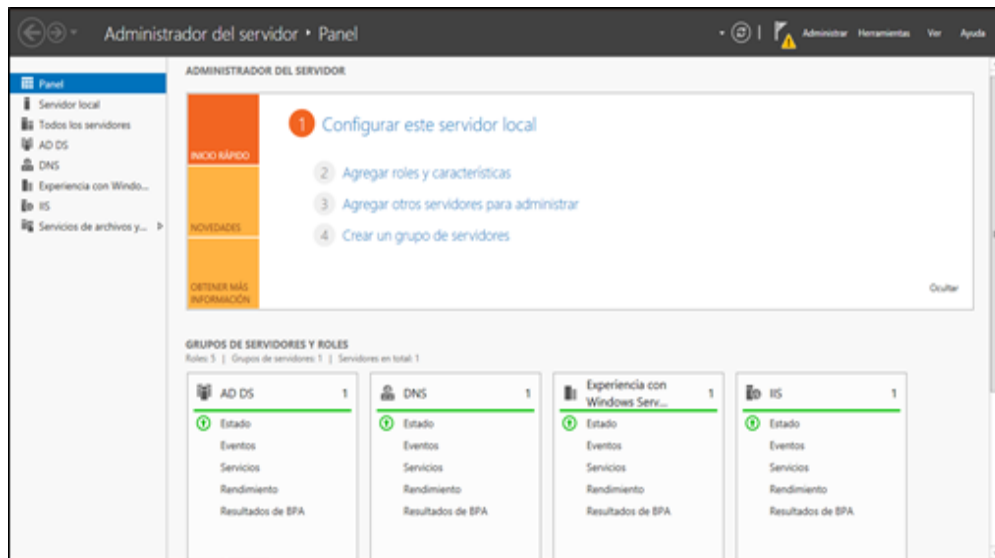


Gráfico 25 Administrador del Servidor.

Fuente: Elaborado por las autora, en base a los resultados obtenidos en la investigación

Rol de servicios de dominio de Active Directory. (Activado)

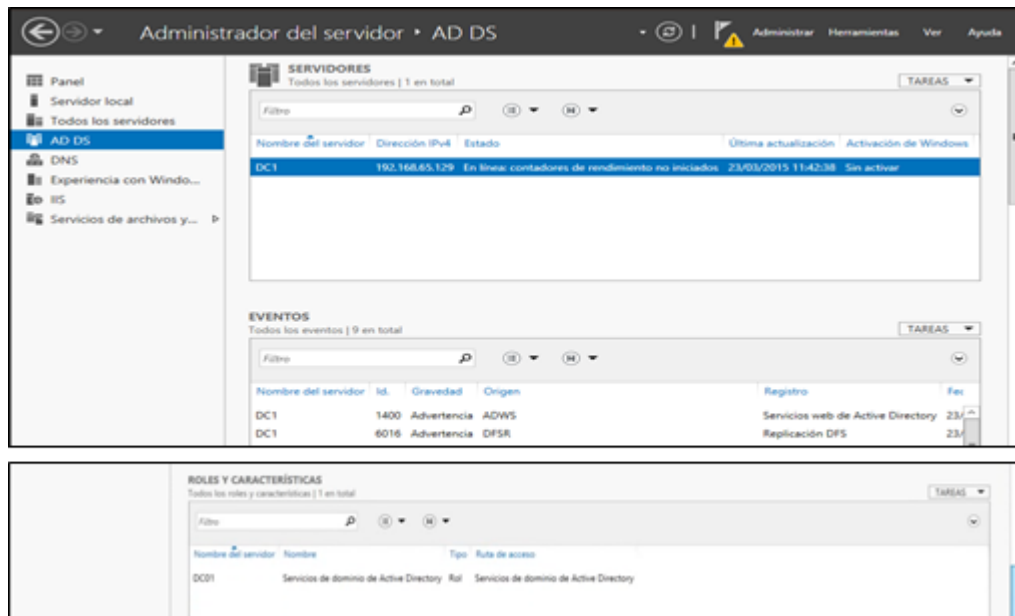


Gráfico 26 Roles de Active Directory activados.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Configuración del dominio en Windows PowerShell a través del comando (Get-ADDomain). Para detallar toda la configuración del controlador de dominio

```

PS C:\Users\Administrador.JGAI1-DC2012X> Get-ADDomain
AllowedDNSSuffixes           : <>
ChildDomains                 : <>
ComputersContainer           : CN=Computers,DC=JGAI1,DC=MS
DeletedObjectsContainer      : CN=Deleted Objects,DC=JGAI1,DC=MS
DistinguishedName           : DC=JGAI1,DC=MS
DNSRoot                      : JGAI1.MS
DomainControllersContainer   : OU=Domain Controllers,DC=JGAI1,DC=MS
DomainMode                   : Windows2012Domain
DomainSID                    : S-1-5-21-3872886611-2487998563-2247278886
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=JGAI1,DC=MS
Forest                       : JGAI1.MS
InfrastructureMaster         : DC01.JGAI1.MS
LastLogonReplicationInterval : <>
LinkedGroupPolicyObjects     : <CN=(31B2F348-816D-11D2-945F-8BC84FB984F9),CN=Policies,DC=LostAndFound,DC=JGAI1,DC=MS>
LostAndFoundContainer        : <>
ManagedBy                   : <>
Name                         : JGAI1
NetBIOSName                  : JGAI1
ObjectClass                   : domainDNS
ObjectGUID                   : 75af4aee-fb8c-4f87-9a84-eb671f8d93eb
ParentDomain                  : <>
PDCEmulator                  : DC01.JGAI1.MS
QuotasContainer              : CN=NTDS Quotas,DC=JGAI1,DC=MS
ReadOnlyReplicaDirectoryServers : <>
ReplicaDirectoryServers      : <DC01.JGAI1.MS>
RIDMaster                     : DC01.JGAI1.MS
SubordinateReferences        : <DC=ForestDnsZones,DC=JGAI1,DC=MS,DC=DomainDnsZones,DC=JGAI1,DC=MS>
SystemContainer              : CN=System,DC=JGAI1,DC=MS
UsersContainer                : CN=Users,DC=JGAI1,DC=MS
  
```

Gráfico 27 Detalle de la configuración de controlador de dominio.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Prueba de consola de Usuario y Equipos de Active Directory.

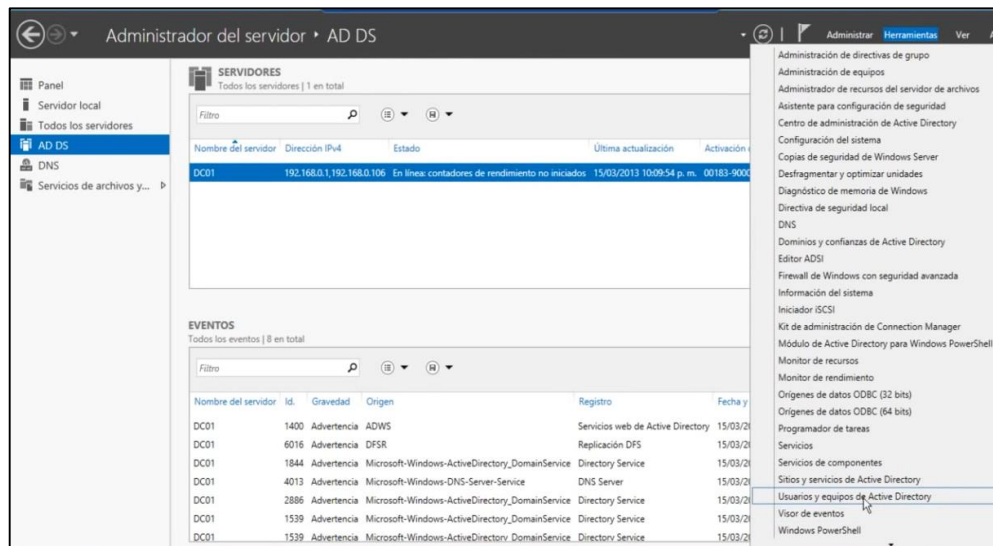


Gráfico 28 Opción Usuarios y características de A.D.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Panel de Usuarios y equipos de Active Directory. Con el Controlador de Dominio creado.



Gráfico 29 Controlador de Dominio, usuarios y equipos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.3.3 Configuración del Servidor DNS.

Panel de inicio de Windows Server 2012 - Administrador de DNS.

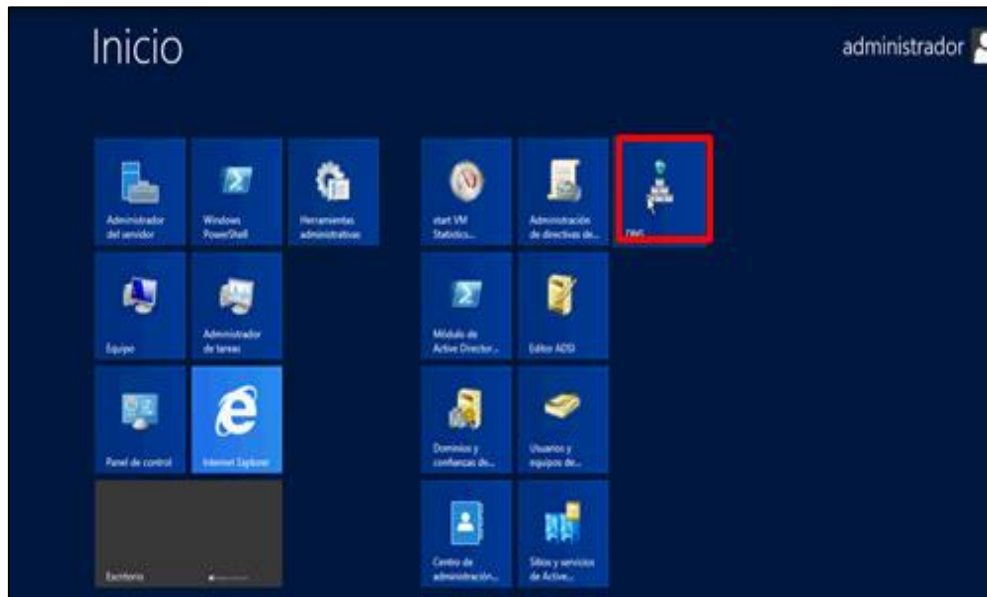


Gráfico 30 Pantalla de Panel de Control Windows Server 2012.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Administrador DNS - Zonas de Búsqueda Directa

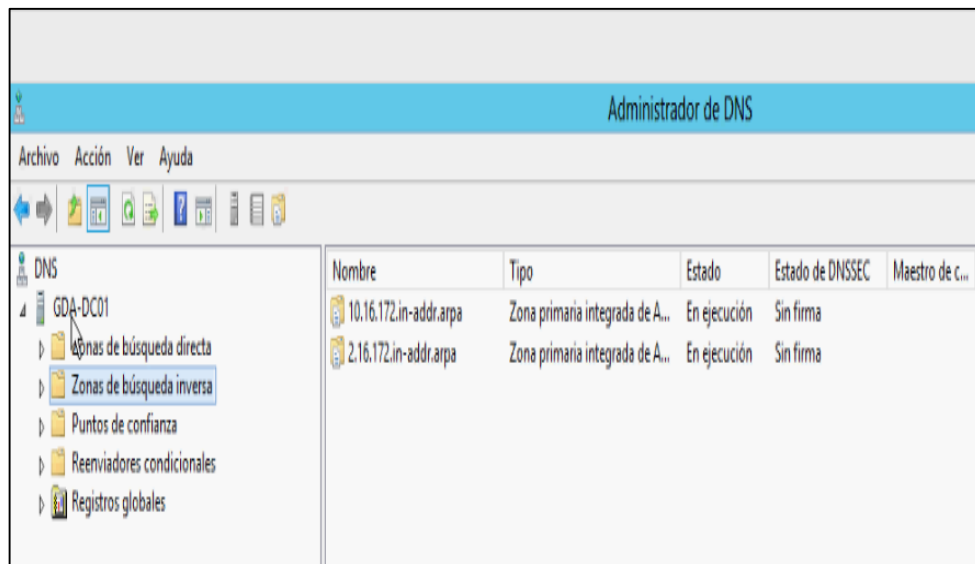


Gráfico 31 Pantalla del Administrador DNS

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Propiedades de GDA-DC01 – Zona Directa – guaranda.gob.ec.

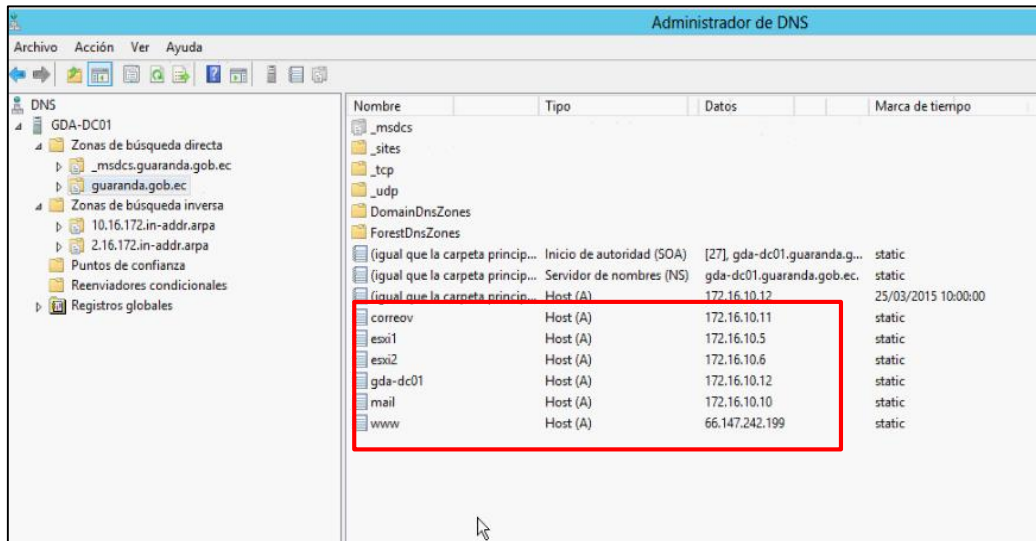


Gráfico 32 Configuración Zona Directa.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Establecer caducidad /borrado para todas las zonas.

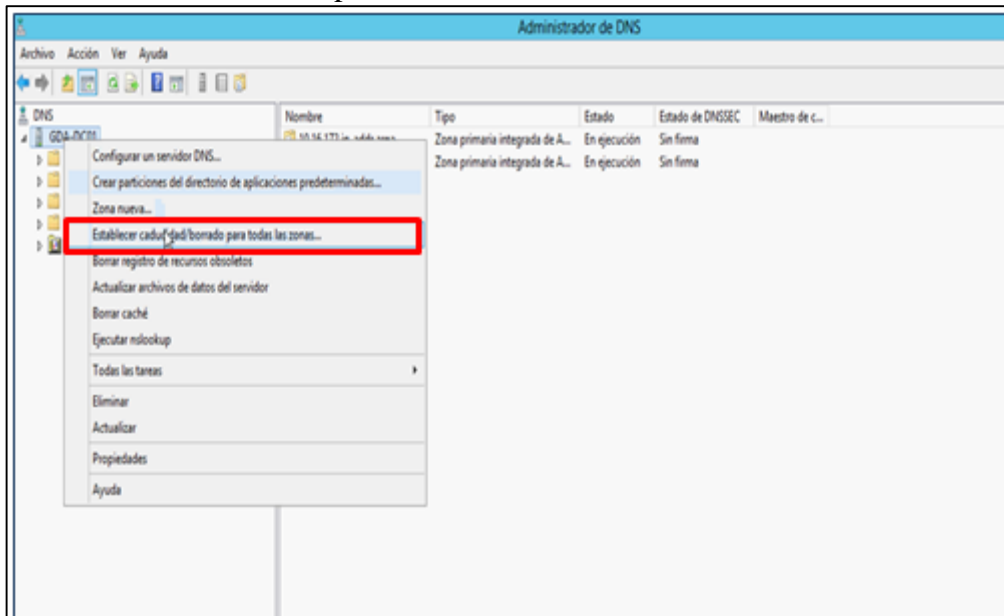


Gráfico 33 Política de Caducidad Zonas.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Configuración de Caducidad – Borrar registro de los recursos obtenidos.

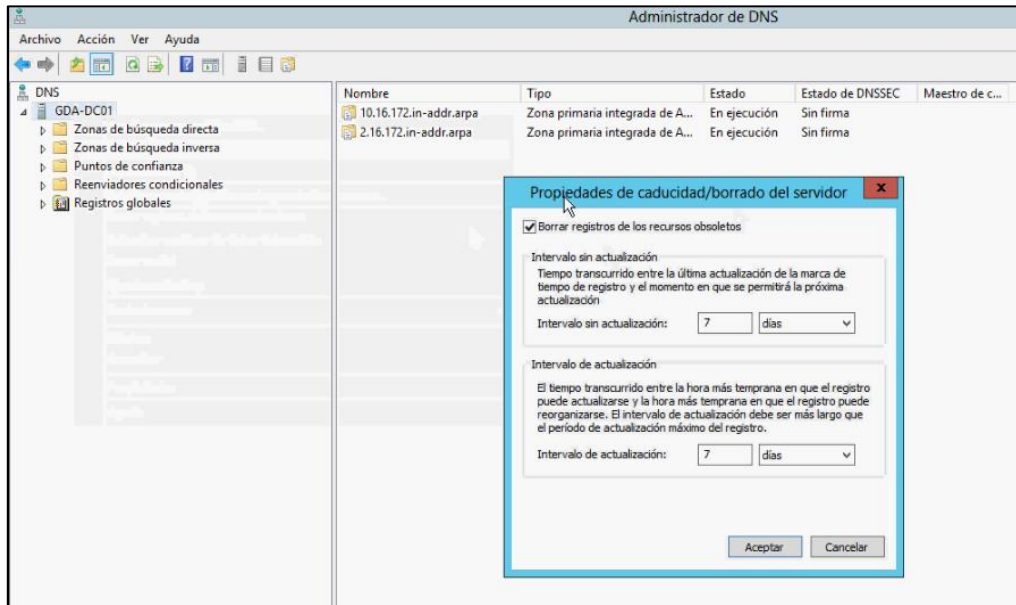


Gráfico 34 Configuración de Caducidad.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Propiedades de GDA-DC01 – Reenviadores.

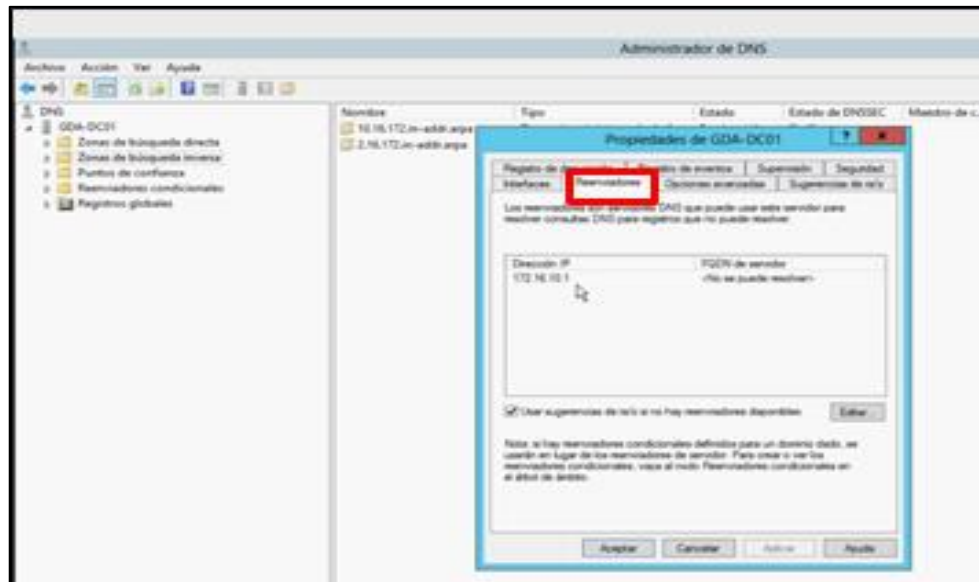


Gráfico 35 Reenviadores.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Propiedades de GDA-DC01 – Reenviadores – Editar.

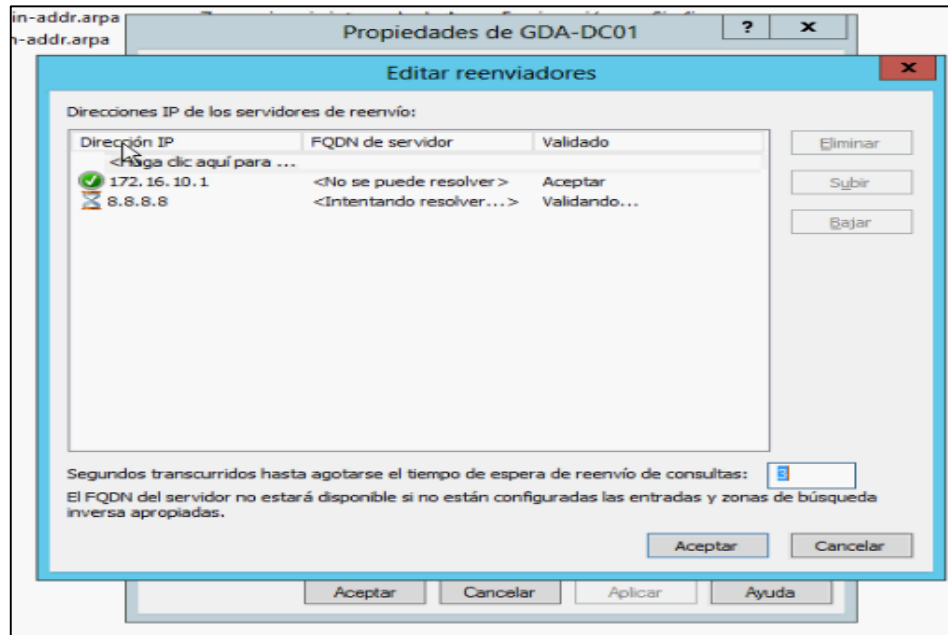


Gráfico 36 Editar Reenviadores.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Propiedades de GDA-DC01 – Opciones avanzadas – Habilitar limpieza automática.

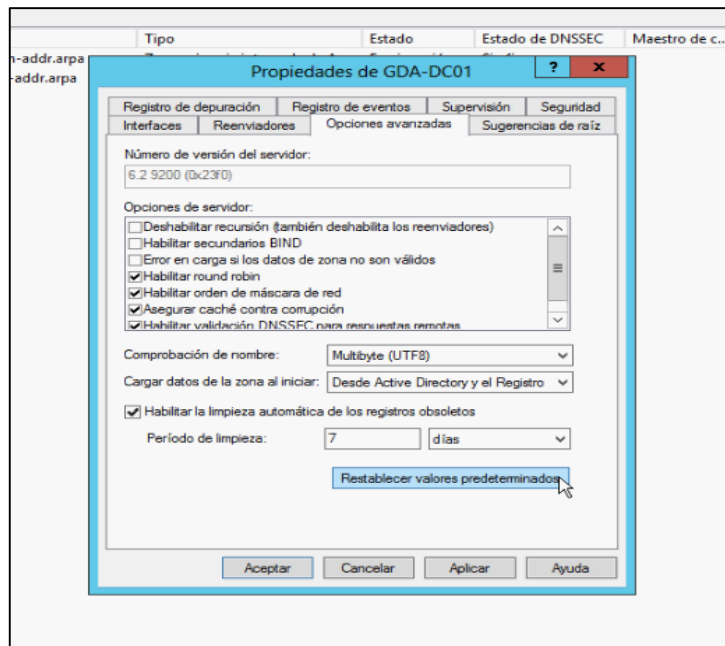


Gráfico 37 Habilitar Limpieza de registros obsoletos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Propiedades de GDA-DC01 – Seguridad.

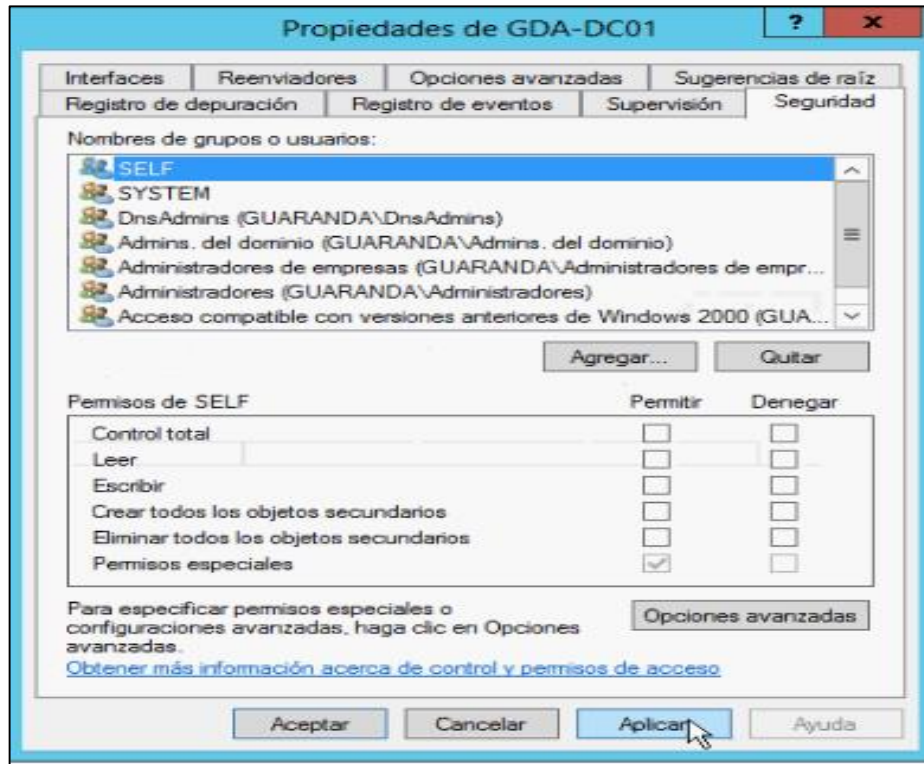


Gráfico 38 Seguridad.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.3.4 Configuración inicial del directorio activo.

3.3.4.1 Estructura Lógica de Active Directory.

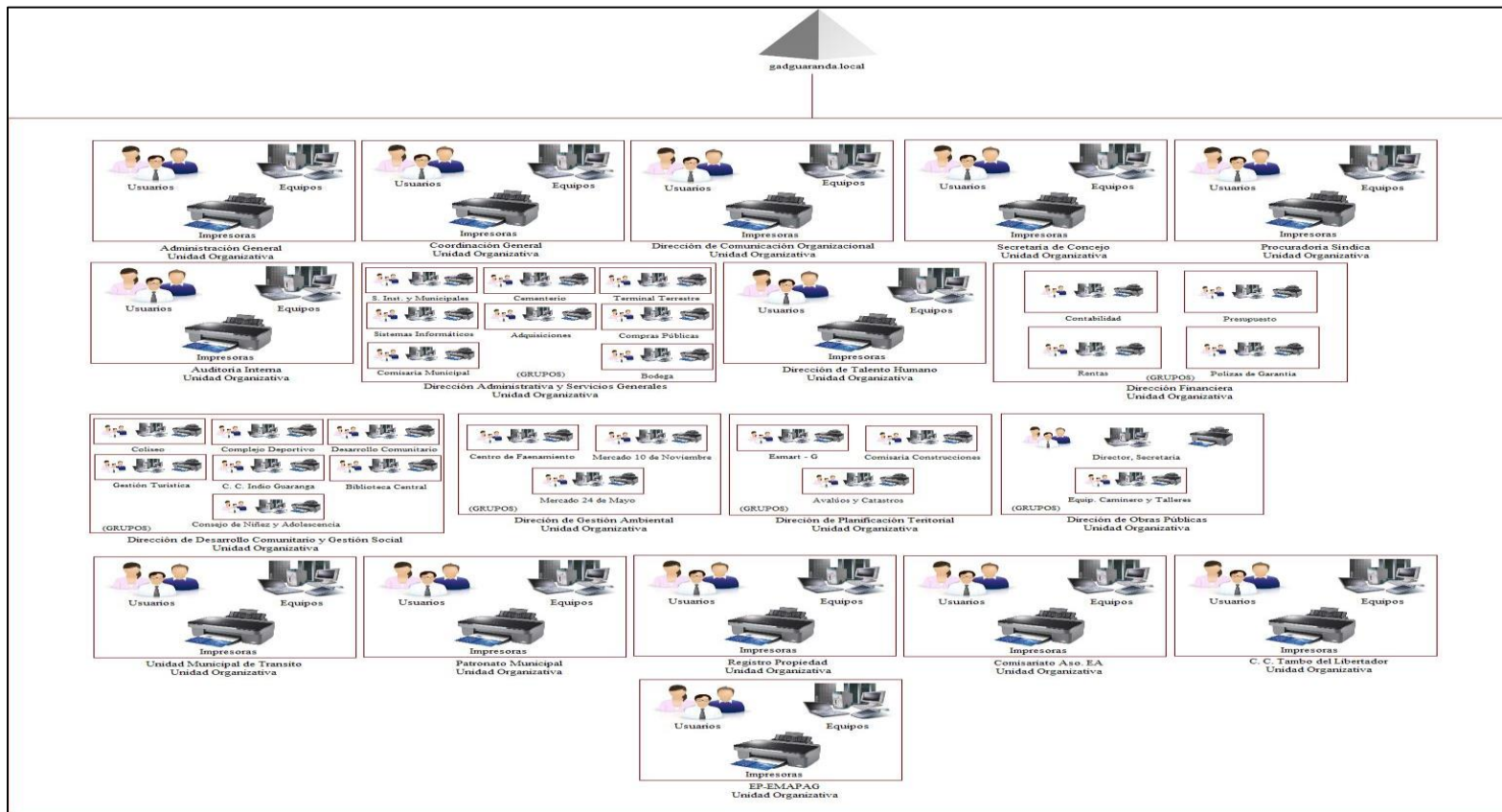


Gráfico 39 Diagrama de la estructura lógica de Active Directory.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.3.5 Creación de usuarios y políticas de acuerdo al diseño original.

3.3.5.1 Creación de Usuarios, Unidades Organizativas, Grupos

Administrador del servidor – Usuarios y equipos de Active Directory.

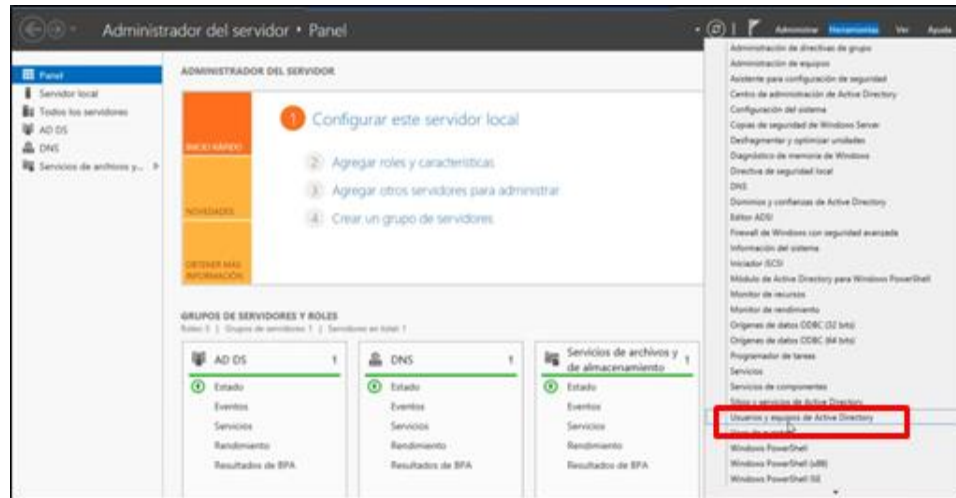


Gráfico 40 Panel del Administrador del servidor.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Panel de Usuarios de Active Directory con el dominio gadguaranda.local

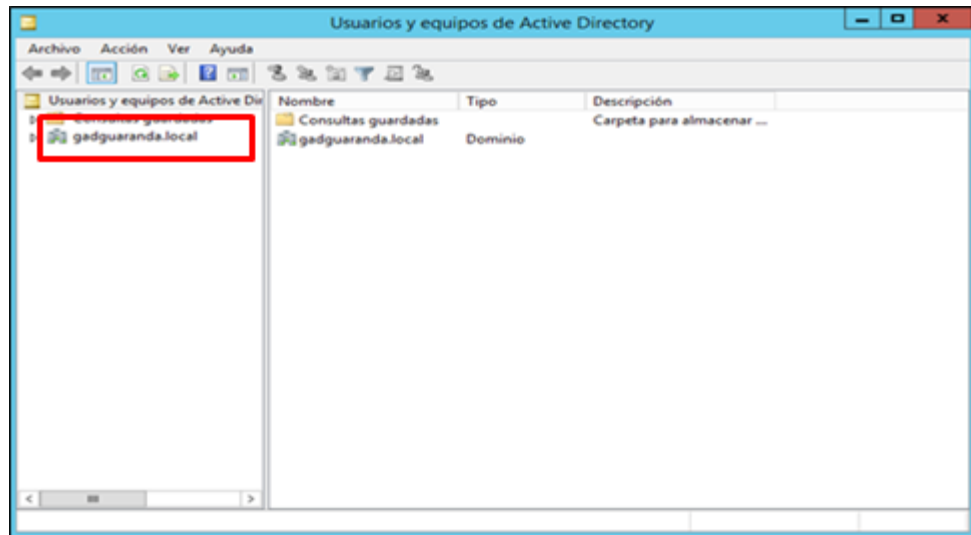


Gráfico 41 Controlador del Dominio.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Creación de Unidades Organizativas – Dirección Administrativa y Servicios Generales.

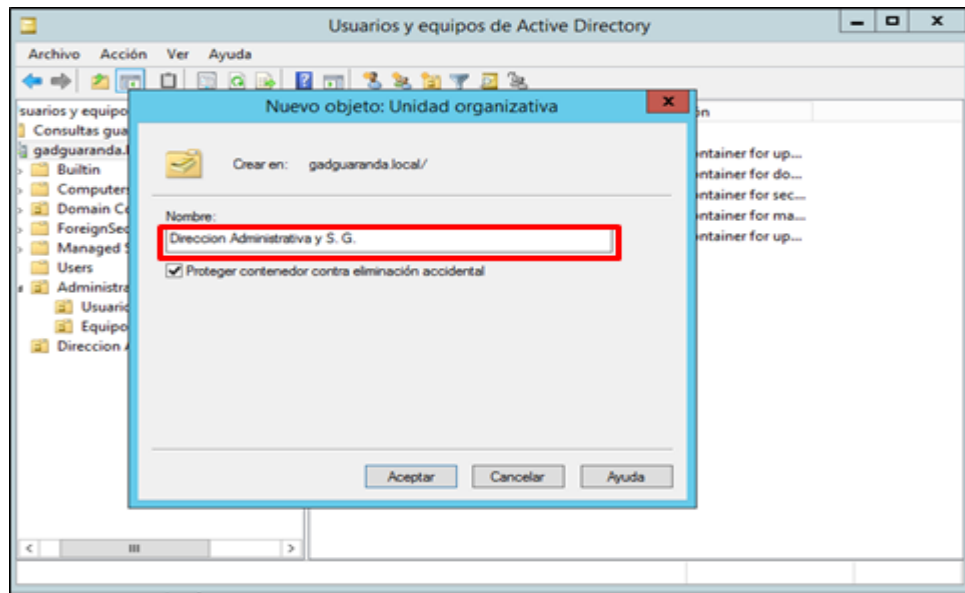


Gráfico 42 Unidades Organizativas.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Creación de Grupos en la Unidad Organizativa Dirección Administrativa y Servicios Generales – Sistemas Informáticos.

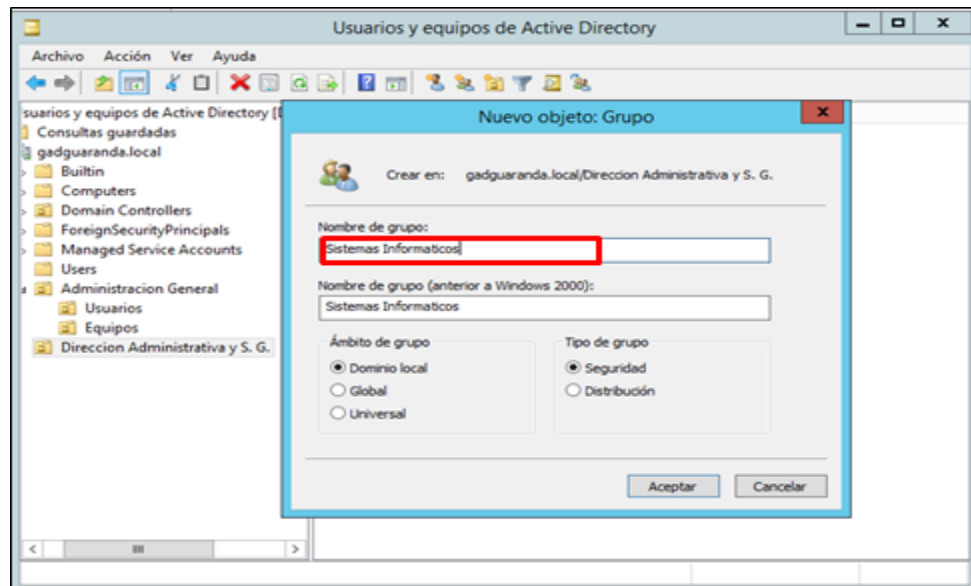


Gráfico 43 Creación de grupos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Creación de usuarios – Grupo Sistemas Informáticos – Usuario (Jaime Gaibor).

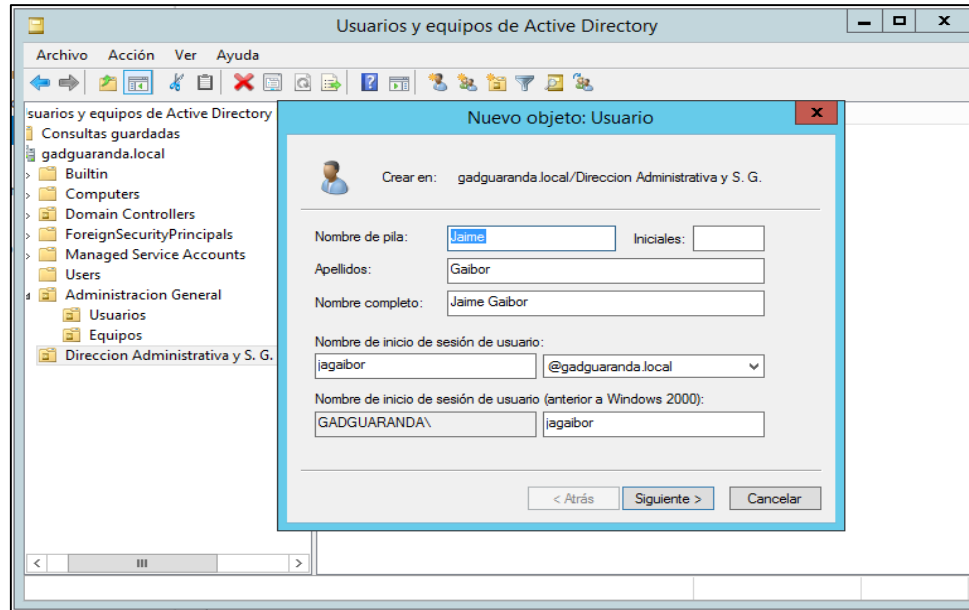


Gráfico 44 Creación de usuarios.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Creación de Equipos, unión al dominio guaranda.gob.ec y al usuario encargado del equipo.

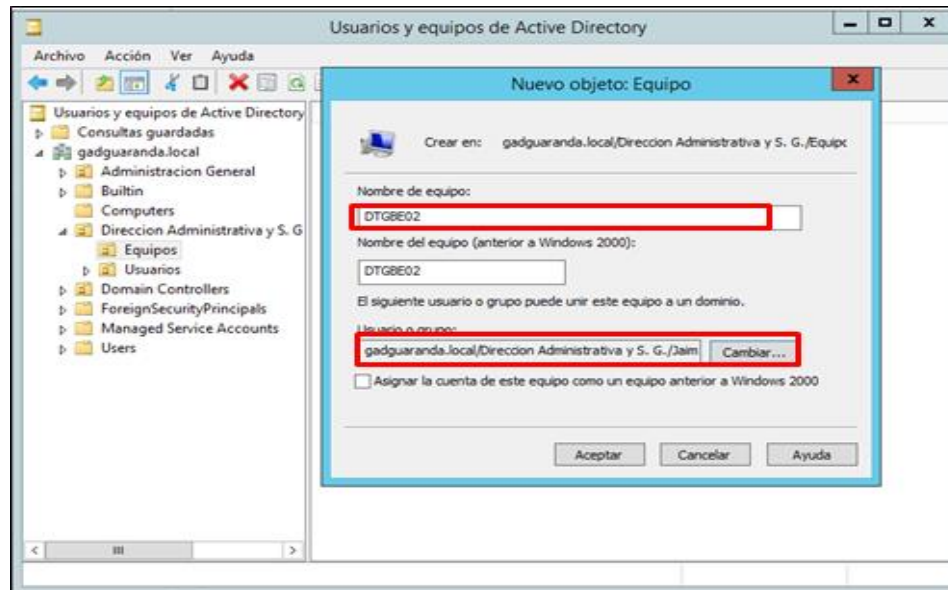


Gráfico 45 Unión de equipos al dominio.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.3.6 Creación de Políticas de Grupo de Active Directory.

Active Directory tiene la herramienta de administración de directivas de grupo, en esta sección se puede crear las políticas de acuerdo a las necesidades establecidas por la Unidad de Sistemas Informáticos para tener un mayor control de la tecnología de la Institución.

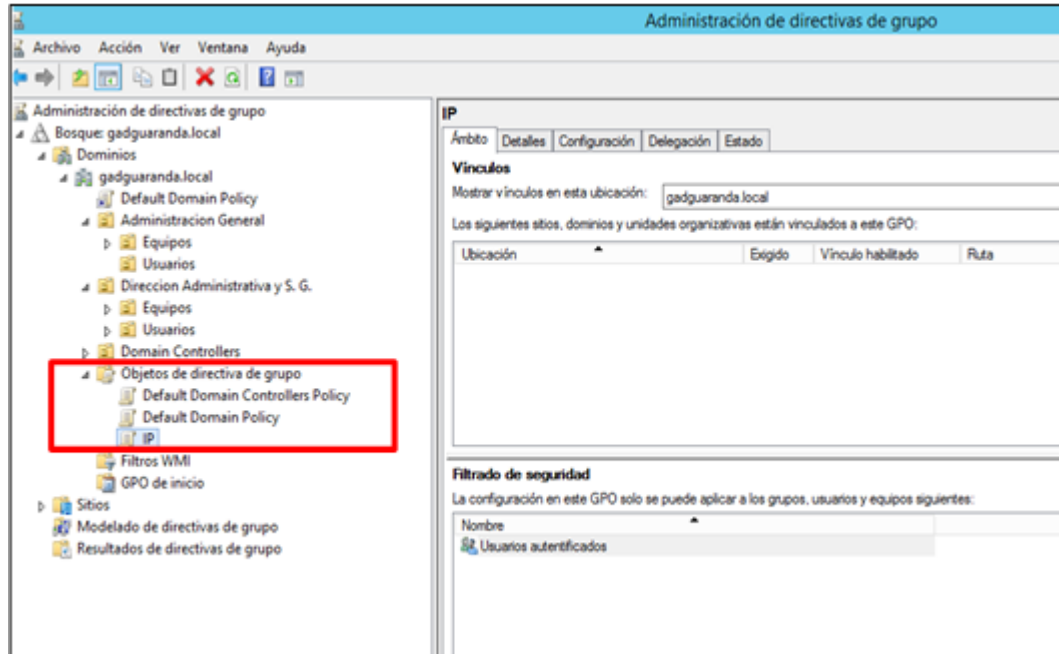


Gráfico 46 Administración de directivas de grupo.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Se da a conocer algunas de las directivas de grupo creadas como son:

Para evitar el cambio de IP por los usuarios se habilito la opción de Prohibir el acceso a las propiedades de componentes de una conexión LAN.

Editor de administración de directivas de grupo – Configuración de usuario – Plantillas administrativas: definiciones de directivas – Red – Conexiones de red.

Prohibir la eliminación de conexiones de acceso remoto	No configurada	No
Prohibir el acceso al elemento Preferencias de acceso remoto en el menú ...	No configurada	No
Habilitar la configuración de conexiones de red de Windows 2000 para ad...	No configurada	No
Desactivar notificaciones cuando una conexión tenga conectividad limita...	No configurada	No
Prohibir el acceso a las propiedades de componentes de una conexión LAN	No configurada	No
Capacidad para habilitar o deshabilitar una conexión LAN	No configurada	No
Prohibir el acceso a las propiedades de una conexión LAN	No configurada	No
Prohibir el acceso al Asistente para nueva conexión	No configurada	No

Gráfico 47 Prohibir propiedades de una conexión LAN.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación

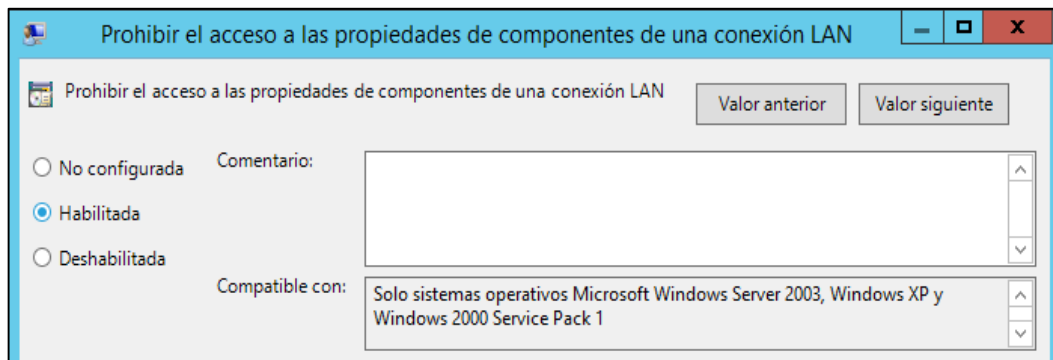


Gráfico 48 Opciones de Configuración.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Se estableció un único inicio de sesión para todos los usuarios, desde las 07:00am hasta las 21:00pm .

Panel de inicio de Windows Server 2012 – Usuarios y Equipos de Active Directory.

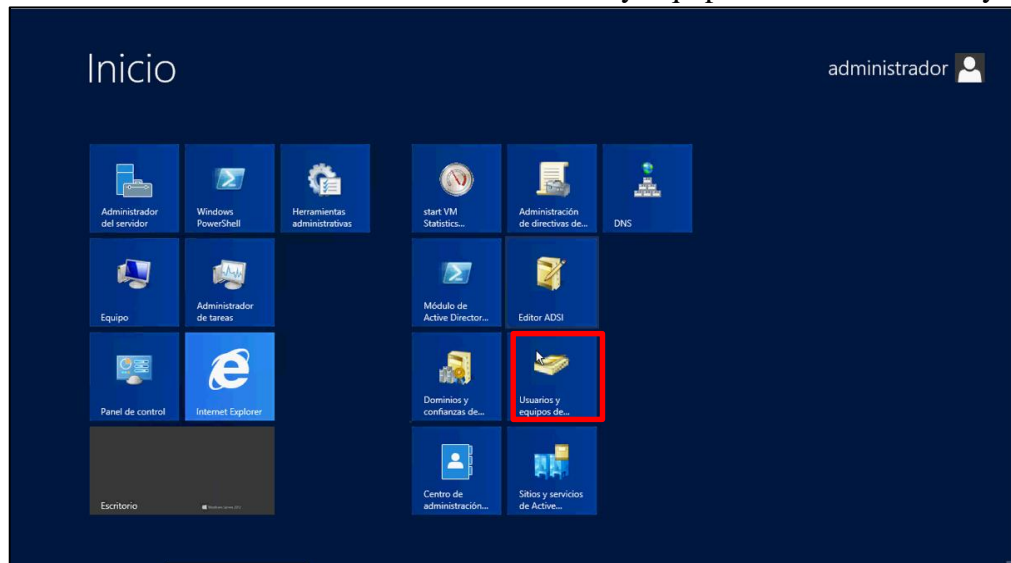


Gráfico 49 Panel de inicio de Windows Server 2012 – Usuarios y Equipos.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Usuarios y equipos de Active Directory – (OU) TECNOLOGIA – Usuario (JoseArellano).

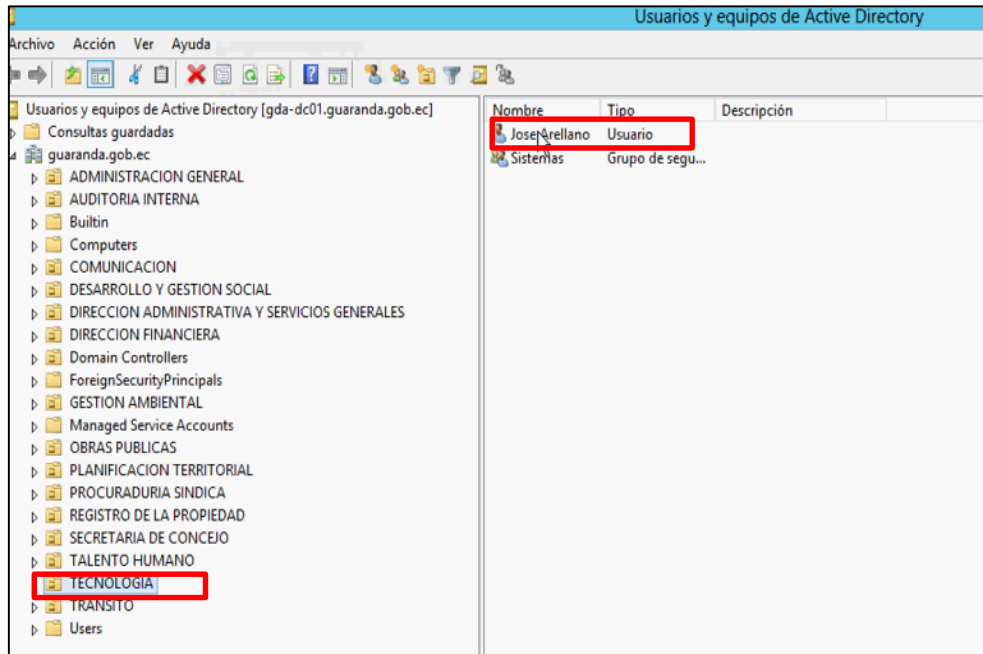


Gráfico 50 Usuario Administrador.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Propiedades del Usuario – Cuenta - Horas de Inicio de Sesión.

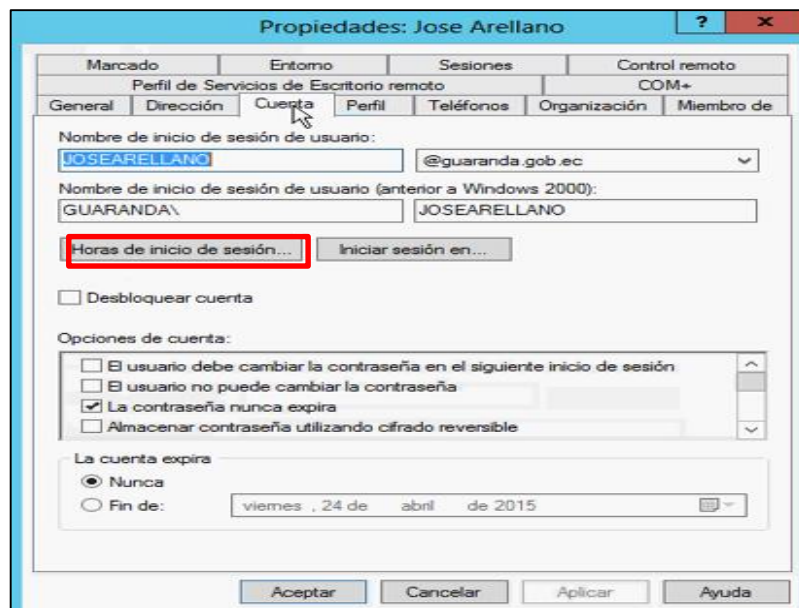


Gráfico 51 Configuración de Hora de Inicio de Sesión.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Usuarios y Equipos de Active Directory – Unidad Organizativa – TECNOLOGIA – Usuario (Administrador) - Hora de Inicio.

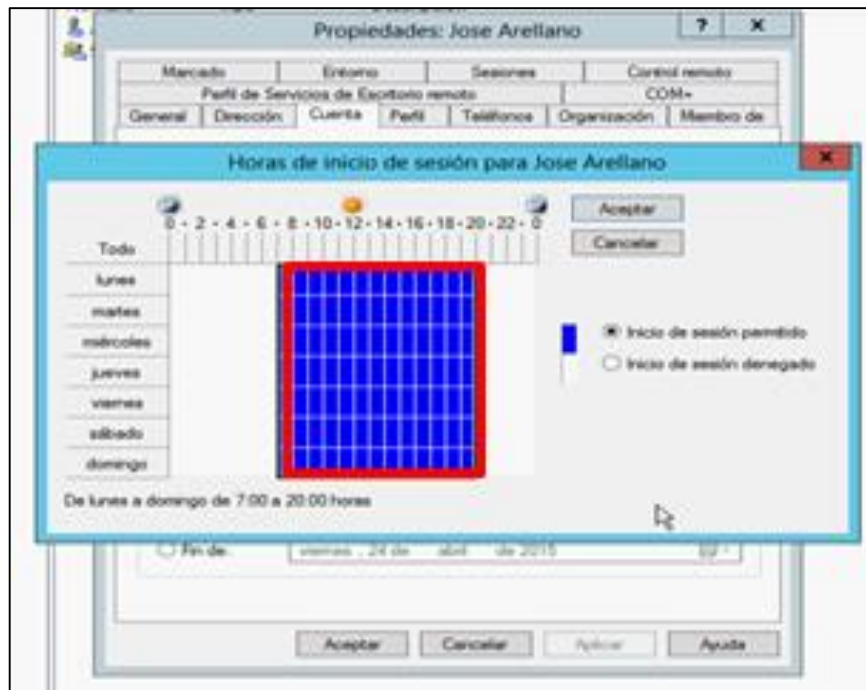


Gráfico 52 Horas de Inicio de Sesión.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.3.7 Incorporación de computadores al directorio activo.

Para incorporar los equipos al directorio activo se procede a realizar lo siguiente: Equipo – Propiedades – Cambiar Configuración – Cambiar. Digitar el nombre del Equipo (debe ser único) y en la opción de Dominio: gadguarda.local.

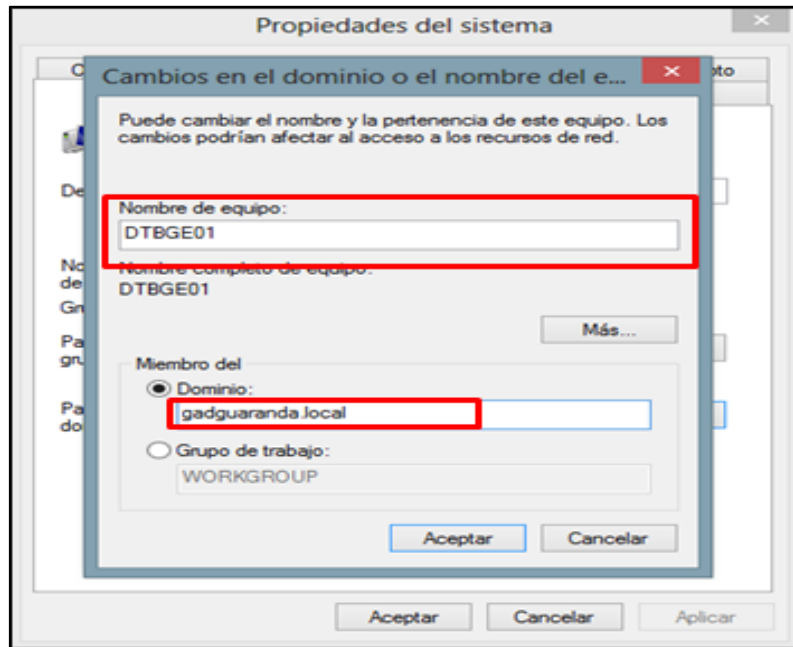


Gráfico 53 Cambio del nombre de equipo.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

Asignación del servidor DNS Preferido para acceder al mismo Servidor DNS del Servidor del Directorio Activo en este caso: 172.16.10.2 este será el mismo para todos los equipos.

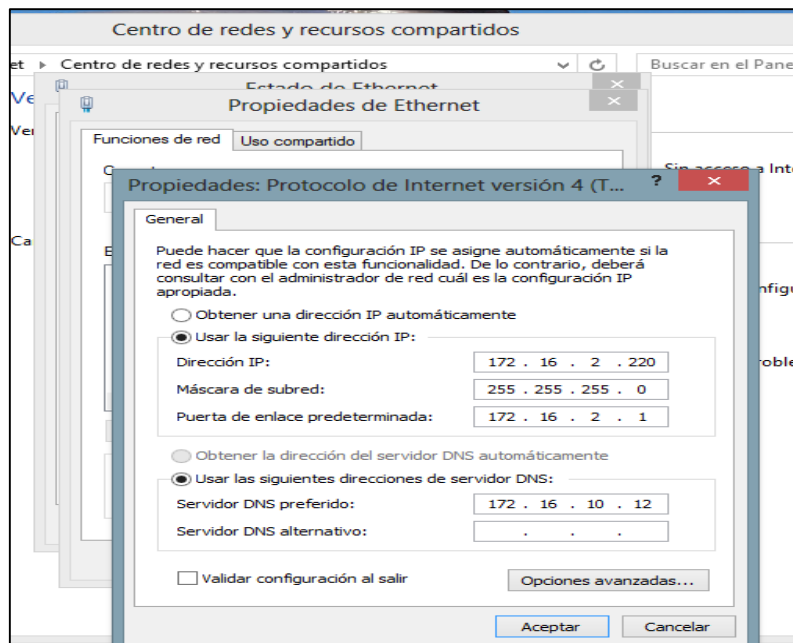


Gráfico 54 IP para el DNS Preferido.

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación

3.3.8 Migración de perfiles de usuarios a la nueva estructura de dominio.

Para migrar un perfil de usuario al dominio guaranda.gob.ec se empleó las siguientes configuraciones en cada uno de los equipos del Gobierno Autónomo Descentralizado del Cantón Guaranda.

CONFIGURACIONES PARA UNIR AL DOMINIO			
#	Paso	Valor de Configuración	Explicación
1	Cambiar configuración DNS	172.16.10.12	El DNS único debe ser el indicado para la operación correcta en el dominio
2	Habilita administrador local y establecer contraseñas	Sistemas *.*	Por razones de seguridad, uso de sistemas y buena práctica
3	Cambio del Hostname según el estándar	-	Estándar de nombramiento aprobado por sistemas
4	Habilitar el primer nivel de UAC en Windows 7 superior.	Nivel 1	Habilita la solicitud de credenciales cuando el sistema requiera elevación
5	Fundir el equipo al dominio	Guaranda.gob.ec	Proceso de unión al dominio
6	Reiniciar el equipo	-	Proceso requerido luego de unir al dominio
7	Iniciar sesión con el usuario del dominio	Guaranda/(usuario)	Esto permite que se cree la carpeta con el perfil del usuario
8	Iniciar sesión como administrador de sistema	-	Se requiere de una cuenta de administrador para migrar la cuenta del usuario
9	Copiar la información del perfil antiguo al nuevo	-	Proceso de migración de la información

			(escritorio/documentos/descargas/imágenes)
10	Copiar carpetas de configuración del perfil antiguo	-	Verificar carpetas APP Data y LocalAPPData para copiar
11	Iniciar sesión con el usuario del dominio	Guaranda/(usuario)	
12	Ordenar la información copiada	-	Ubicar la información en su lugar respectivo
13	Configurar parámetros adicionales para el equipo	ODBC/correo/etc.	Configuraciones específicas para las aplicaciones de la institución
14	Realizar pruebas equitativas	-	Probar correos, impresoras, (permisos), navegadores, etc.
15	Enseñar al usuario la nueva forma de inicio de sesión	-	Resolver todas las dudas que se presentan al momento que se inicia sesión
16	Enseñar al usuario el nuevo estándar de contraseña	-	El nuevo estándar de contraseñas es más seguro y exigente

Tabla 28 Lista de configuraciones.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación

CAPITULO IV

4.1 PRUEBAS DE FUNCIONAMIENTO Y SEGURIDAD

El propósito de realizar las pruebas es la de verificar el funcionamiento correcto de la medida de seguridad implementada, con el cual se puede realizar varias simulaciones que permitan obtener resultados validos e incorrectos del servicio de directorio cuya finalidad es la de analizar el comportamiento de Active Directory en ejecución.

La fase de pruebas tiene como objetivo verificar las políticas de grupo que se implementó para tener un mayor control de los usuarios.

Dentro del Servicio de Directorio (Active Directory) que se implementó, se pueden aplicar varias políticas de seguridad según las necesidades que tenga la Institución. Con el propósito de tener un mayor control de usuarios, administrar los recursos de la red y aún más la Institución implementaría un servidor de archivos para tener la información centralizada, protegida y confidencial.

4.1.1 Pruebas de conectividad hacia y desde el servidor de directorio activo.

Desde las diferentes dependencias del Gobierno Autónomo Descentralizado del Cantón Guaranda. En esta fase se procede a verificar en cada usuario del dominio que funcionen correctamente las políticas de seguridad que se implementó.

Inicio de Sesión fuera del horario laboral establecido. No podrá ingresar debido a que se encuentra fuera del lapso de tiempo de sesión que se fijó previamente en una de las políticas de seguridad.



Gráfico 55 Inicio de Sesión.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación

Pantalla de Sesión Iniciada – Fondo de Escritorio. Política de grupo fondo para el directorio activo.



Gráfico 56 Fondo de Escritorio.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación

Propiedades de Ethernet. Para prevenir el conflicto de direcciones IP se creó una política de seguridad que impida que el usuario modifique la dirección IP asignada al Equipo.

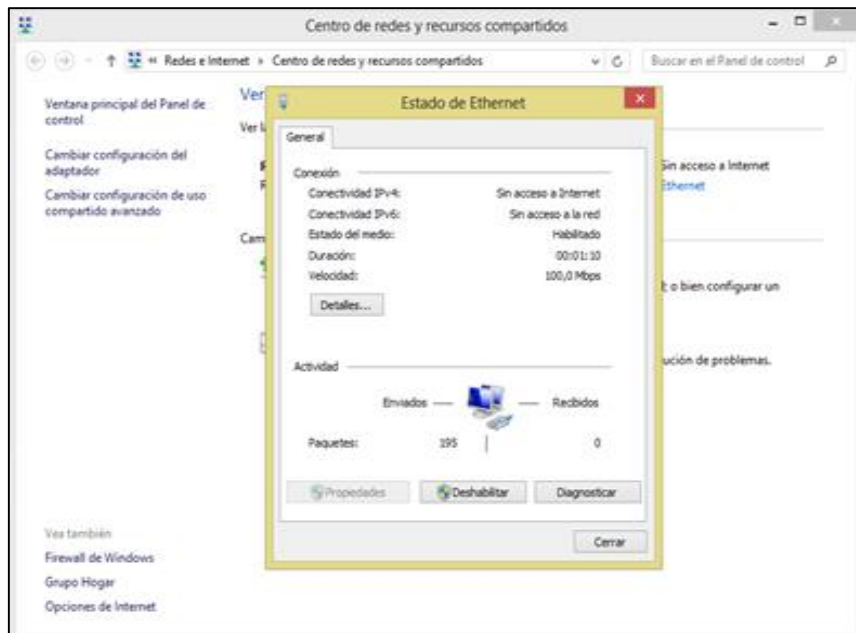


Gráfico 57 Propiedades de Ethernet.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación

4.2 COMPROBACIÓN DE HIPÓTESIS

En el estudio realizado para la Implementación de una Solución de Seguridad Informática para fortalecer la confidencialidad de la información en la Intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda se determinó que cuentan con un Equipo Firewall para la protección de comunicaciones externas provenientes de internet, pero al mismo tiempo carecen de una medida de seguridad en la organización, gestión y control de todos los recursos de la red. Por lo que se han ido generando algunos problemas de conflictos IP en los últimos años.

El siguiente gráfico muestra el número de conflictos IP que se han dado entre el periodo comprendido por los años 2010 al 2014.

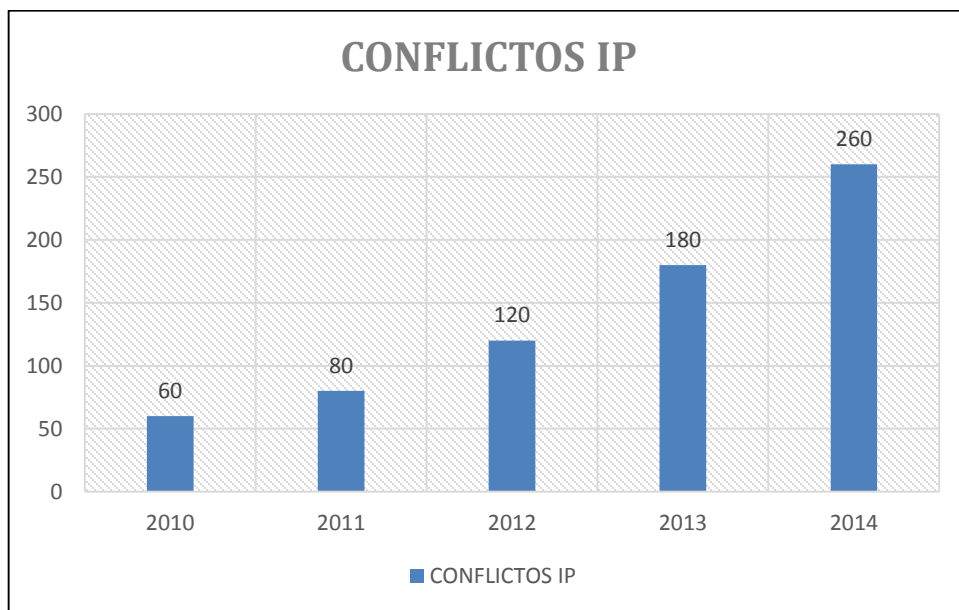


Gráfico 58 Número de conflictos IP.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación

Con la implementación de Active Directory se fortaleció la confidencialidad de la información accediendo a un mayor control de los usuarios que se encuentran dentro del mismo dominio, alcanzando el objetivo planteado: mantener seguro y protegido los procesos que se realicen dentro de la Institución, al permitir el desarrollo de un plan de operación preventiva para proteger sus datos y comunicaciones, evitando la pérdida de privacidad, robo de información e incluso responsabilidad legal.

Comparación entre el Control Manual y la Implementación de Active Directory.

CONTROL MANUAL			ACTIVE DIRECTORY	
N°	Problema	Tiempo/Min	Solución	Tiempo/Min
1	Conflictos IP	2880min	Prohibir el acceso a las propiedades de componentes de una conexión LAN (Política de Seguridad).	0min
2	Infección de Virus	60min	Control de Cuentas de Usuario	10min
3	Instalación de Programas no autorizados	30min	Control de Cuentas de Usuario	10min
4	Manipulación indebida de configuración del equipo.	1440min	Política de Seguridad.	0min
TOTAL		4410min		20min

Tabla 29 Control manual y Active Directory.

Fuente: Elaborado por las autoras, en base a los resultados obtenidos en la investigación

$$TOTAL = 4410 \text{ min}(100\%)$$

$$TOTAL = (20 * 100)/4410$$

$$TOTAL = 0.45\%$$

$$TOTAL = 100\% - 0.45\%$$

$$TOTAL = 99.55\%$$

Una vez aplicados los instrumentos de investigación e implementada la solución, procedemos a verificar la hipótesis **“Con la Implementación de una Solución de Seguridad Informática se logrará fortalecer la confidencialidad de la información en la intranet del Gobierno Autónomo Descentralizado del Cantón Guaranda”**.

Se establece comparaciones para resolver problemas entre el control manual empleando un tiempo de 4410min e implementando la Solución de Seguridad Informática Active Directory reduciendo tiempo\recursos en 20min obteniendo un mayor control de los usuarios de la Institución en un porcentaje de 99.55% fortaleciendo la confidencialidad de la información.

4.3 CONCLUSIONES Y RECOMENDACIONES

4.3.1 CONCLUSIONES

- Se elaboró los planes generales de migración para la plataforma de Active Directory tomando en cuenta las necesidades de la Institución para definir las políticas a utilizar.

- Se aplicaron las características definidas por los administradores de la Institución para la implementación de políticas de grupo, que permiten asegurar, estandarizar y controlar de mejor manera el ambiente de trabajo de los usuarios; con la finalidad de optimizar su productividad.

- La integración de los usuarios a un Servicio de Directorio en el Gobierno Autónomo Descentralizado del Cantón Guaranda evitará los problemas de conflictos IP que se ha dado en la Institución en los últimos años.

4.3.2 RECOMENDACIONES

- Integrar los servicios de correo electrónico a Active Directory.
- Para una mayor seguridad en la utilización de Active Directory se recomienda a los administradores cumplir con los requerimientos de complejidad para contraseñas.
- Una de las medidas de seguridad básicas para una Institución que cuenta con varios usuarios son las políticas de caducidad de contraseña ya que ayuda a evitar accesos no autorizados permitiendo mantener de manera confidencial la información de los mismos.
- Para un mejor desempeño en las funciones institucionales es necesario tener la información de manera ordenada y actualizada de los diferentes activos de la institución.
- Para realizar de forma rápida los respaldos de la información de los usuarios es recomendable centralizar la información en un File Server (Servidor de archivos).
- Es recomendable implementar políticas de caducidad o eliminación de cuentas de usuarios para mantener segura la información cumpliendo con la regla de que la información es propiedad de la Institución y no debe ser utilizada fuera de ella.
- Mantener las aplicaciones virtualizadas para un mejor aprovechamiento de servidores, escalabilidad de sistemas y recuperaciones rápidas de información y de aplicaciones en caso de desastres.

4.4 BIBLIOGRAFÍA:

- Albadalejo, A. Hernández, A. (2008). Administración de Servicios de Internet. Murcia. Compobell.
- Alegre, M. García, A. (2011). Sistemas Operativos en Red. Madrid. Paraninfo.
- Anderruthy, J. Gaumé, S. (2011). Mantenimiento y Reparación de un Pc en red. Barcelona. ENI
- Área de Libre Comercio de las Américas. (2015). Área de Libre Comercio de las Américas. Recuperado de: <http://www.ftaa-alca.org/intprop/natleg/ecuador/L320b.asp#11t1c1s5>
- Barbancho, J. Benjumea, J. Rivera, O. Romero, M. Roper, J. Sanchez, G. Sivianes, F. (2014). Redes Locales. España. Paraninfo.
- Cutipa, S. (2013). Instalación y Configuración de una Red LAN con Windows Server 2003
- E Internet. Recuperado de
- https://books.google.com.ec/books?id=Ffk9AAwAAQBAJ&dq=que+es+un+grupo+de+trabajo+de+windows&hl=es&source=gbs_navlinks_s
- Daburon B. (2010). Windows 7. España: Ediciones ENI
- Garrido Herrera, P.M; López Caballero, M.E; Zarandieta Morán, F. (2009). Tipos de redes de ordenadores. Redes LAN, MAN y WAN. Clasificación. Tecnología Interactiva 3 E.S.O. Recuperado de http://contenidos.educarex.es/mci/2009/43/TEMA7/tipos_de_redes_de_ordenadores_redes_lan_man_y_wan_clasificacin.html
- Jara, H. Pacheco, F. (2013). Ethical Hacking 2.0. Recuperado de <https://books.google.com.ec/books?id=joMIAU4seLYC&pg=PA263&dq=que+es+vllans&hl=es&sa=X&ei=2E8GVYCHDsmoNoDQg4gJ&ved=0CEoQ6AEwCA#v=onepage&q=que%20es%20vllans&f=false>
- Maciá, F. Mora, F. Gil, J. Iglesias, V. Jorquera, D. Berná, J. Monllor, J. Ramos, H.
- Niño, J. (2011). Sistemas Operativos en Red. Recuperado de <https://books.google.com.ec/books?id=A9vJAAwAAQBAJ&pg=PA84&dq=active>

+directory+como+funciona&hl=es&sa=X&ei=2McBVdyQC6ggSn6oHIBA&ved=0CEkQ6AEwBw#v=onepage&q=active%20directory%20como%20funciona&f=false.

- Olifer, N. y Olifer, V. (2009). Redes de Computadoras. México. Litográfica Ingramex
- Paiola, P. (2013). Windows 8 Instalación y Configuración. Barcelona. Ediciones
- Perez M. (2009). Windows Server 2008: Instalación, Configuración y Administración. Recuperado de <https://books.google.com.ec/books?id=4FcuYxCbPioC&pg=PA441&dq=que+es+el+protocolo+dhcp&hl=es&sa=X&ei=848EVcisHMWvvgSF04PgBw&ved=0CEsQ6AEwCQ#v=onepage&q=que%20es%20el%20protocolo%20dhcp&f=false>
- Pérez, A. G. (2011). Internet lo Básico que debe saber. España. StarkBook Editorial
- Van den Bent, J. Van der Steeg, M. (2012). EXIN Cloud Computing Foundation. Recuperado de https://books.google.com.ec/books?id=8VVeAgAAQBAJ&dq=que+es+protocolo+kerberos&hl=es&source=gbs_navlinks_s
- The Stationery Office. (2010). Operación del Servicio. Recuperado de <https://books.google.com.ec/books?id=htb2mp3A2WAC&pg=PA108&dq=servicios+de+directorio&hl=es&sa=X&ei=A-UKVeWHHfb7sAT3kYDwBA&ved=0CDIQ6AEwBA#v=onepage&q=servicios%20de%20directorio&f=false>
- Ramos, M. García, A. (2011). Sistemas Operativos en Red. Madrid. Paraninfo.
- Raymond McLeod, Jr. (2010). Sistema de información gerencial. México. Printed
- Reinoso, E. J; Maldonado, C. A; Muñoz, R. Damiano, L. E y Abrutsky, M. A. (2012). Base de Datos. Argentina. AlfaOmega Grupo Editor Argentina S.A
- Romero, M. Barbancho, J. Benjumea, J. Rivera, O. Roper, J. Sanchez, G. Sivianes, F. (2010). Redes Locales. Madrid. Paraninfo
- Roldán Santana, C. (2012, 09 de Septiembre). Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo?. [CODEJOBS Aprende a

programar].Recuperado de:

<http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#sthash.y6IIwI9F.dpbs>

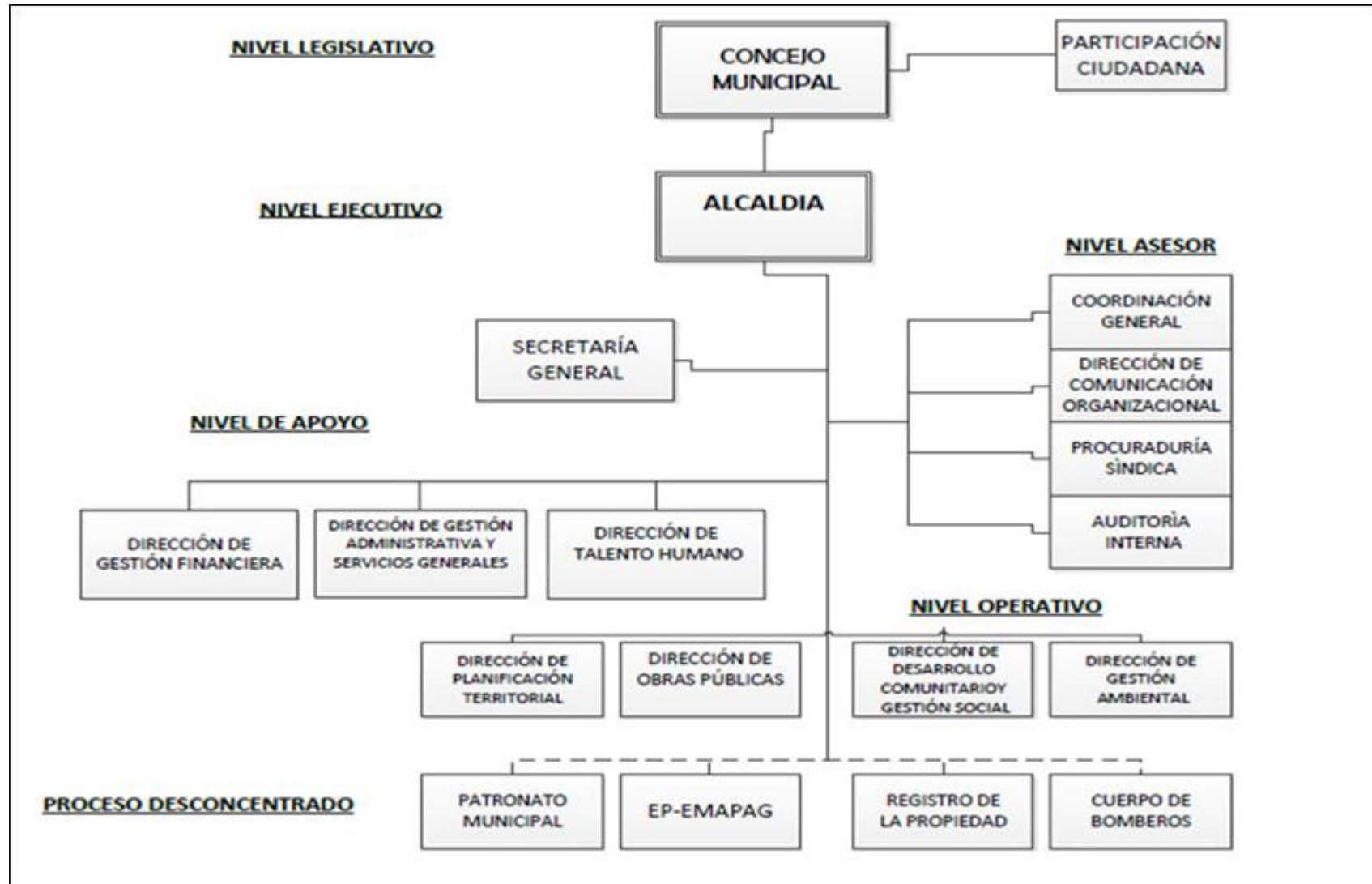
- Sánchez Estella, O. y Herrero Domingo, R. (2014). Aplicaciones básicas de ofimática. España. Paraninfo
- Vieites Gómez, A. (2011). Enciclopedia de la Seguridad Informática. México. AlfaOmega

WEBGRAFÍA

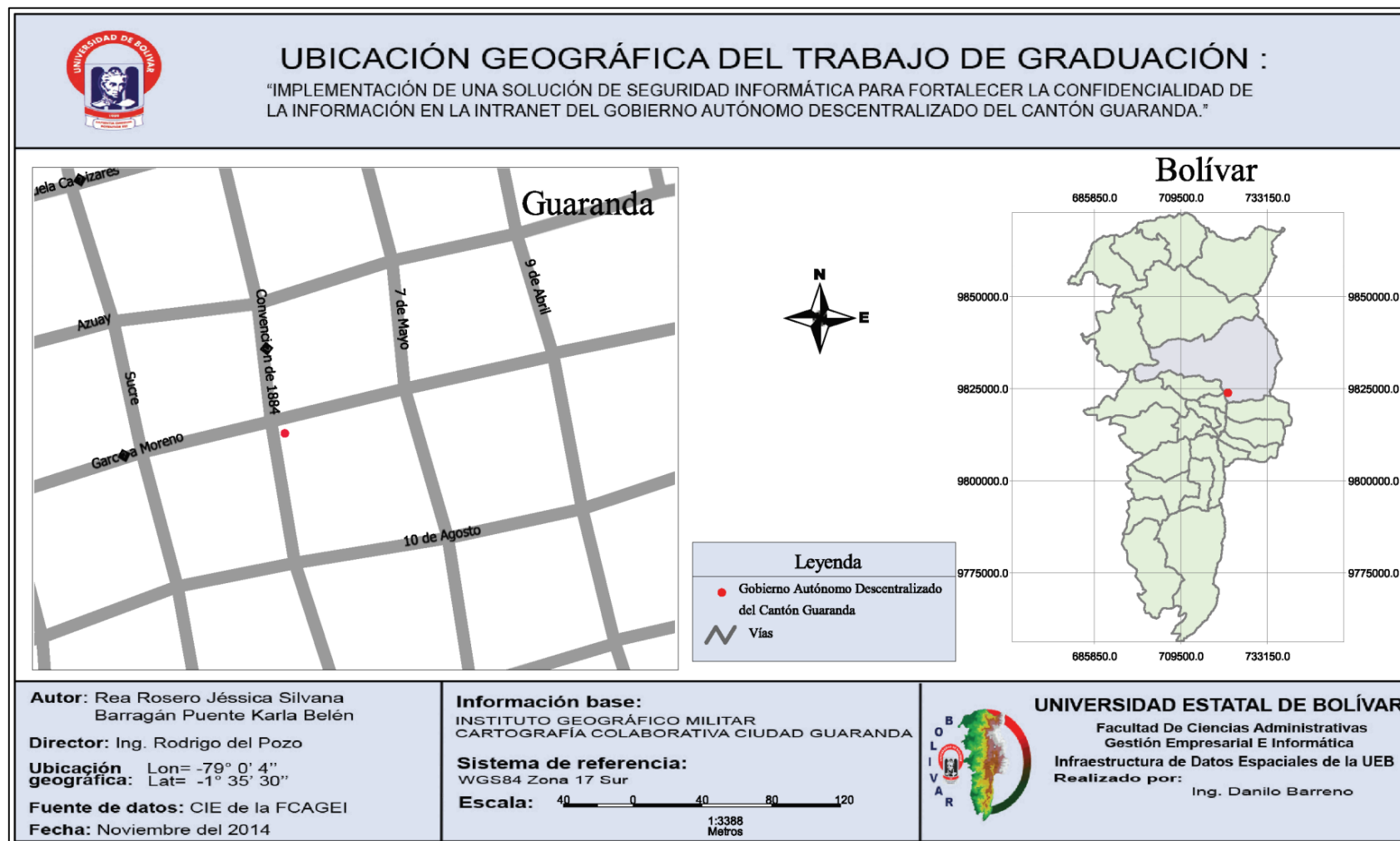
- Roldán Santana, C. (2012, 09 de Septiembre). Seguridad Informática: ¿Qué es una vulnerabilidad, una amenaza y un riesgo? [CODEJOBS Aprende a programar].Recuperado de:
<http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo#sthash.y6IIwI9F.dpbs>

ANEXOS

ANEXO N° 1 ESTRUCTURA ORGANIZACIONAL.



ANEXO N° 2 MAPA GEOREFERENCIADO.



ANEXO N° 3 ENTREVISTA DE SEGURIDADES INFORMÁTICAS.
GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA
(DEPARTAMENTO DE SISTEMAS)

NOMBRE:..... **FECHA:**.....

1. ¿Qué tipo de red utilizan?

.....
.....

2. ¿Cuál es el medio de conexión que utiliza?

.....
.....

3. ¿Con qué tipo de equipos cuentan en su infraestructura de red?

- Capa Dos (Capa Física- No Programables)
- Capa Tres (Capa de Aplicación- Programables)

4. ¿Qué conflictos o caídas de sistema ha sufrido su red?

- Ataques ilegales
- Ataques de IP
- Ataques de Hackers

5. ¿Qué problemas se han presentado en la administración de la Intranet?

.....
.....

6. Si usted cuenta con una red inalámbrica ¿qué tipo de seguridad tiene?

- Solo clave
- Clave y configuración

7. ¿Su infraestructura de red cuenta con subredes o VLANS?

.....
.....

8. ¿Cuentan ustedes con algún tipo de Aplicación informática?

- Si
- No

9. ¿Con qué tipo de seguridad cuentan dichas aplicaciones?

.....
.....

10. ¿Con cuántos servidores cuentan y que funcionalidad tienen?

.....
.....

11. ¿De qué tipo de clase de subred tiene la infraestructura de red alámbrica e inalámbrica?

.....
.....

12. ¿Con qué frecuencia realiza un chequeo de los puertos de conectividad de red?

- Diario
- Mensual
- Anual
- Otros

Especifique:.....

13. ¿Controla el acceso a redes sociales?

- Si
- No

14. ¿Controla el ancho de banda para cada una de las oficinas?

- Si
- No

15. ¿Cuenta con IP públicas para alguna oficina?

- Si
- No

16. ¿Cuentan con equipos que soporta IPV6?

- Si
- No

17. ¿Cómo está distribuida la estructura IPV6?

.....
.....

18. ¿Cuenta con un equipo para la administración de red?

- Si
- No

19. ¿Cómo se dan cuenta los problemas que presenta la red?

.....
.....

20. ¿Qué medida de seguridad está utilizando en la intranet para evitar el acceso de usuarios no autorizados a la información?

.....
.....

21. ¿Qué medida de seguridad está utilizando para prevenir el desperdicio de recursos en la intranet de la Institución?

.....
.....

22. ¿Qué medida de seguridad en la red está utilizando para prevenir ataques informáticos provenientes de internet?

.....
.....

23. ¿Cuál es la forma de organización de Equipos en la Red?

- Grupo de Trabajo.
- Grupo en el Hogar.
- Dominio (Active Directory).

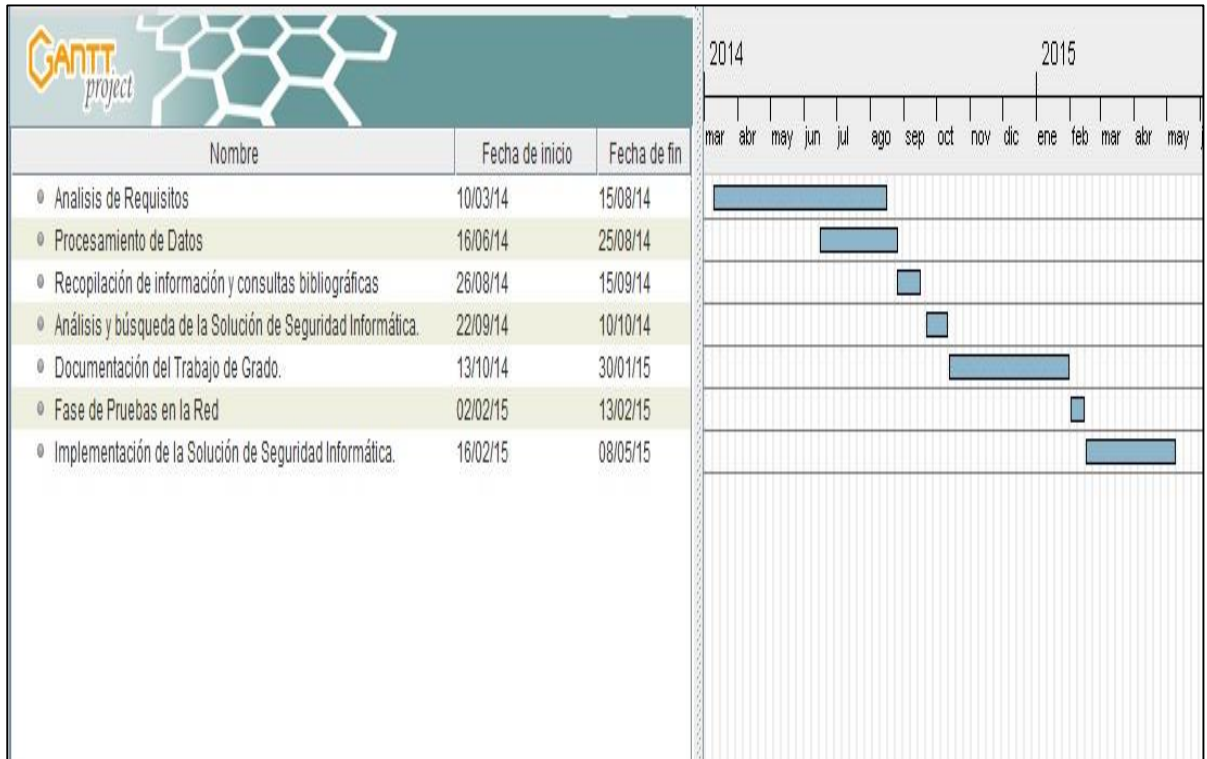
24. ¿Estaría usted de acuerdo con la implementación de un Directorio Activo para brindar protección a la Intranet?

- Si
- No

ANEXO N° 4 FICHA DE OBSERVACIÓN DIRECTA.

Localidad:		Ficha N°:	
Informante:		Fecha:	
Clasificación:			
Investigador:			
TÍTULO: Infraestructura de Red			
Columna Marginal	Columna Matriz		
Aspectos a observarse.			
RED	Tipo	Extensión	Tipo de Seguridad
Alámbrica			
Inalámbrica			
	Cable de Subred	Clase de Ip (Pública / Privada)	
TOPOLOGÍA DE RED	Tipo:		
	Descripción:		
TIPO DE CABLE	Categoría	Rendimiento	Velocidad de
Coaxial			
UTP			
Fibra Óptica			
EQUIPOS	Cantidad	Marca	Descripción
Switch			
Router			
Hub			
Puente o Bridges			
Impresoras			
Ordenadores			
SERVIDORES	Tipo	Marca	Funcionalidad
APLICACIONES	Nombre	Seguridad	Ubicación (Servidor)
ADMINISTRACIÓN DE LA RED	Programas	Accesos a Redes Sociales	Ancho de banda

ANEXO N° 5 CRONOGRAMA DE ACTIVIDADES.



ANEXO N° 6 DETALLE DE COSTOS DE LA UNIDAD DE SISTEMAS INFORMÁTICOS.

SUELDOS Y SALARIOS						
CANT.	DESCRIPCIÓN	UNIDAD MEDIDA	SUELDO MENSUAL	APORTE PATRONAL 11.15%	APORTE PERSONAL 9.45%	VALOR TOTAL
1	Jefe departamental	Dólares	1086	120.98	102.53	862.49
1	Asistente	Dólares	901	100.46	85.14	715.40
1	Asistente	Dólares	675	75.26	63.78	535.96
Total						\$2113.94

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

UTILES DE OFICINA				
CANTIDAD	DESCRIPCION	UNIDAD MEDIDA	PRECIO UNITARIO	VALOR TOTAL
56	Resmas de papel boom A4	Resma	4,5	250
400	Carpetas	Docenas	0,2	80
5	Archivadores	Docenas	3	15,5
10	Caja de esferos	Caja	5,25	50
5	Sello	Unidad	7	35
5	Engrampadora	Unidad	2	10
9	Perforadora	Unidad	3,5	30
10	Caja de clips	Caja	0,35	3,5
2	Calculadora	Unidad	13	26
Total				\$ 500

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

SERVICIOS BÁSICOS				
CANTIDAD	DESCRIPCIÓN	UNIDAD/MEDIDA	PRECIO UNITARIO	VALOR TOTAL
10625	Luz	kw	0,08	850
733	agua	Metro cúbico	0.15	110
Total				\$960

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

CALCULO DE DEPRECIACIÓN									
Rubros	Valor I.	Vida. Útil.	%	1	2	3	4	5	V. residual
Equipos De Oficina	3000	5	20%	600	600	600	600	600	600
Equipos De Computo	1440	3	33.33%	321,35	321,35	321,35			321,35
Herramientas	560	2	50%	280	280				280
Total	\$4000			921,35	921,35	921,35	600	600	1201,35

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

EQUIPOS DE COMPUTO		
Cantidad	Detalle	Valor
4	Servidores	\$ 10.000
2	PCS	\$ 2.000
1	Servidor Cisco Telefonía IP.	\$ 14.000
2	Router Microtick	\$ 2.000
1	Switch Catalust 2960 Series	\$ 800
1	Switch 3com	\$ 700
8	Convertidores TPLink	\$ 2.500
2	Modem Cisco Series	\$ 3.000
TOTAL		\$ 35.000

Fuente: Elaborado por las autoras en base a los resultados obtenidos en la investigación.

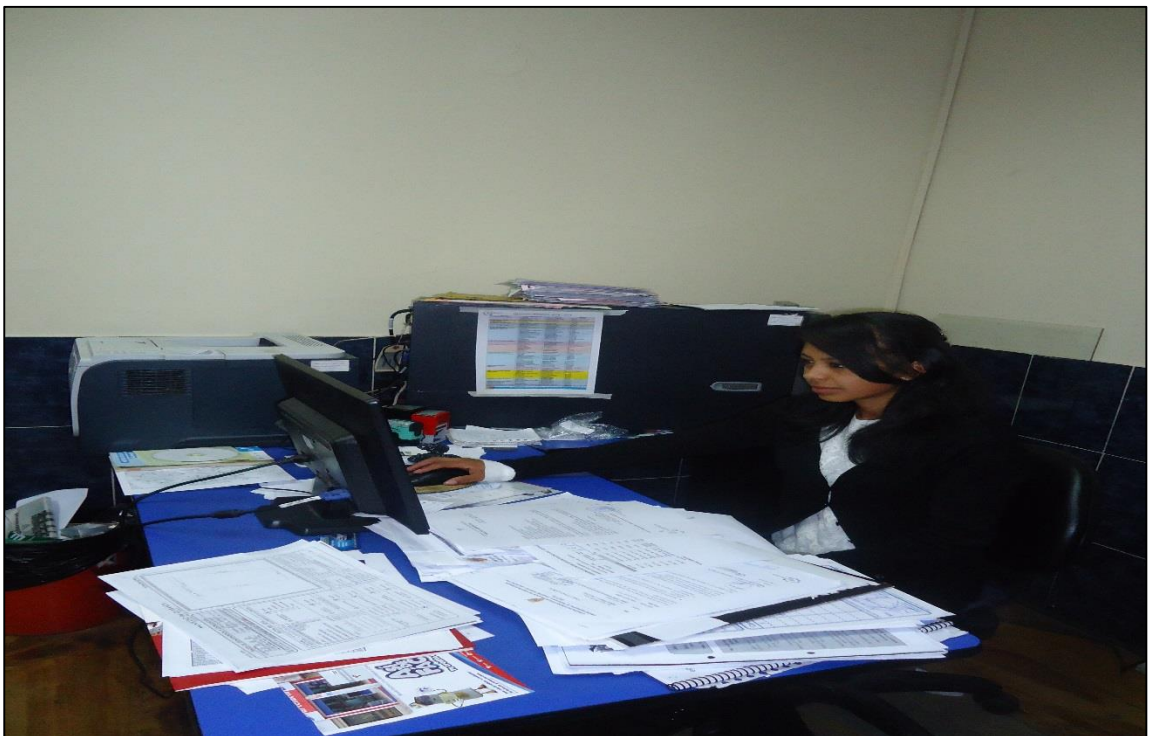
ANEXO N° 7 ESTUDIO DEL LOS EQUIPOS DEL RACK.



ANEXO N° 8 CONFIGURACIÓN DEL SERVIDOR.



ANEXO N° 9 UNIÓN DE EQUIPOS AL DOMINIO.





Gobierno Autónomo Descentralizado
UNIDAD DE SISTEMAS

ING. JAIME GAIBOR, JEFE DE LA UNIDAD DE SISTEMAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA, A PETICIÓN DE LA PARTE INTERESADA.

CERTIFICO:

Que por medio de la presente dejo constancia que las Srtas. BARRAGÁN PUENTE KARLA BELÉN, con cedula de ciudadanía N° 0202134185 y REA ROSERO JESSICA SILVANA, con cedula de ciudadanía N° 0202095899, estudiantes de la Carrera de Sistemas de la Facultad de Ciencias Administrativas Gestión Empresarial e Informática de la Universidad Estatal de Bolívar, han realizado como Trabajo de Graduación el tema: **“IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA PARA FORTALECER LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN LA INTRANET”**, en el Gobierno Autónomo Descentralizado del Cantón Guaranda.

Guaranda, 16 de junio de 2015

Ing. Jaime Gaibor
JEFE UNIDAD DE SISTEMAS



Dirección: Convención de 1884 y García Moreno
Teléfonos: (03) 2980321 – (03) 2981643
E-mail: alcaldiaagda@gmail.com

www.guaranda.gob.ec

URKUND rdelpozo (rdelpozo)

Document [TRABAJO DE GRADO CAPI. II, III, IV.pdf](#) (D14160692)

Submitted 2015-04-30 15:14 (-05:00)

Submitted by jesmar201991@hotmail.com

Receiver rdelpozo.ueb@analysis.orkund.com

Message [Show full message](#)

6% of this approx. 48 pages long document consists of text present in 7 sources.

List of sources

Rank	Path/Filename
	Proyecto de InvestigaciónACTUALIZADO 11 DE AGOSTO.docx
	http://misticadiciplina.blogspot.com/
	http://www.cetid.abogados.ec/archivos/7.ppt
	https://carolinacols.files.wordpress.com/2011/11/ataquesinformaticos.pdf
	anteproyecto2.docx
	http://gnu2801.blogspot.com/2010/11/tipos-de-intrusos-informaticos.html

UNIVERSIDAD ESTATAL DE BOLÍVAR FACULTAD DE CIENCIAS ADMINISTRATIVAS GESTIÓN EMPRESARIAL E INFORMÁTICA ESCUELA DE SISTEMAS CARRERA DE SISTEMAS TRABAJO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS COMPUTACIONALES TEMA: "IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD INFORMÁTICA PARA FORTALECER LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN LA INTRANET DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN GUARANDA" AUTORAS: BARRAGÁN PUENTE KARLA BELÉN REA ROSERO JESSICA SILVANA DIRECTOR ING. RODRIGO DEL POZO DURANGO PARES ACADEMICOS ING. DARWIN CARRIÓN LIC. JUAN MANUEL GALARZA GUARANDA, 2015. III. DEDICATORIA Dedico este trabajo de graduación a Dios por guiar mis pasos, por estar conmigo en todos los momentos buenos y malos y por haberme dado a mi familia quienes son la base fundamental en mi vida, demostrándome su altruismo, amor, paciencia, comprensión, tolerancia incondicional y su apoyo tanto emocional como económico para lograr cumplir con uno de los objetivos de mi vida. Barragán Karla Dedico este trabajo de graduación a Dios por mostrarme día a día con humildad, paciencia y sabiduría los pasos que debería seguir para cumplir con mis metas, permitiéndome haber llegado hasta este momento muy importante de mi formación profesional. A mis padres por haberme dado la vida, amor, comprensión y por ser las personas que me apoyaron incondicionalmente en toda mi vida académica dándome una carrera para mi futuro, proporcionándome sus palabras de aliento en los momentos más difíciles de mi vida y mi trayecto estudiantil. A toda mi familia por darme sus valiosos consejos fomentando mi educación y valores. Rea Jessica. III. AGRADECIMIENTO Agradecemos a Dios por habernos acompañado espiritualmente a lo largo de nuestra carrera, por ser nuestra fortaleza en los momentos de debilidad ayudándonos a culminar una meta en nuestra vida A nuestros padres por ser los pilares fundamentales de nuestra vida ya que son las personas que nos impulsaron a seguir adelante con sus buenos consejos y sabidurías brindándonos su apoyo para tener una excelente educación. Gracias por habernos

Handwritten signature in blue ink, possibly reading 'J. Barragán' or similar, with the date '08-05-15' and '10/16/15' written below it.