

**INVESTIGACION DE SOFTWARE LIBRE PARA LA SEGURIDAD
INFORMATICA EN LAS INSTITUCIONES EDUCATIVAS PÚBLICAS DEL
MUNICIPIO DE DOSQUEBRADAS - RISARALDA**



JORGE MAURICIO RIVERA BUITRAGO

PAULA ANDREA ARIAS CÁRDENAS

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
DOSQUEBRADAS - RISARALDA**

2015

**INVESTIGACION DE SOFTWARE LIBRE PARA LA SEGURIDAD
INFORMATICA EN LAS INSTITUCIONES EDUCATIVAS PÚBLICAS DEL
MUNICIPIO DE DOSQUEBRADAS - RISARALDA**

JORGE MAURICIO RIVERA BUITRAGO

PAULA ANDREA ARIAS CÁRDENAS

**Proyecto de Grado para optar al Título de
ESPECIALISTA EN SEGURIDAD INFORMATICA**

DIRECTOR

DEIVIS EDUARD RAMIREZ MARTINEZ

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
DOSQUEBRADAS - RISARALDA**

2015

Nota de Aceptación:

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Dosquebradas, 26 de Septiembre de 2015

DEDICATORIA

Dedico este Proyecto de Grado a...

***Dios**, porque ha estado conmigo en cada paso que doy, cuidándome y dándome la fe, fortaleza, salud y confianza para terminar este proyecto de investigación.*

***Mis Padres**, Henry Rivera y María Elcy Buitrago quienes a lo largo de mi vida han velado por mi bienestar y educación, siendo mi apoyo en todo momento y depositando su entera confianza en cada reto que se me ha presentado, sin dudar ni un solo momento de mis capacidades. Mi triunfo es el de ustedes, ¡Los Amo!*

***Mi Hermana**, Sandra Milena Rivera por siempre haberme brindado su apoyo, fuerza y compañía incondicional, que me han ayudado y motivado a salir adelante.*

***Mi Esposa**, Eliana Marcela Palacio quien me brindó su amor, cariño, apoyo y ayuda constante, así como también soportó con paciencia mis ausencias y me motivó siempre en los momentos difíciles. ¡Gracias mi Amor!*

Jorge Mauricio Rivera Buitrago

AGRADECIMIENTOS

Los Autores de este Proyecto de Investigación, deseamos expresar nuestros más sincero agradecimientos a...

***La Universidad**, por el apoyo a nuestro Proyecto de Grado a través de los Tutores, Directivos y personal de la Especialización.*

***El Director de Proyecto**, Deivis Eduard Ramírez Martínez, por su valiosa colaboración, asesoría y orientación, que enriquecieron ampliamente el desarrollo del Proyecto de Investigación.*

***Al personal de la Institución Educativa Eduardo Correa Uribe - Sede la Palma Dosquebradas (Risaralda)**, quienes nos proporcionaron el tiempo y la documentación necesaria para la consecución de este proyecto.*

***Nuestras Familias...** Padres, Hermanos, Esposos e Hijo, por su inmenso amor, colaboración, paciencia y por su invaluable apoyo.*

***Y primordialmente a Dios**, a quien debemos y agradecemos todo lo que somos y todo lo que tenemos. Ese ser que esta siempre de manera incondicional y con el cual todo es posible.*

Jorge Mauricio Rivera Buitrago

Paula Andrea Arias Cárdenas

RESUMEN

Actualmente, el mundo se enfrenta a constantes cambios por el uso frecuente de las tecnologías, las cuales se han convertido en herramientas esenciales para nuestras vidas.

Debido a la importancia de la información y al acelerado crecimiento de las tecnologías, surge la necesidad de identificar los riesgos informáticos que se puedan presentar, con el fin de establecer políticas y herramientas que regulen la seguridad y ayuden a mitigar los riesgos a los que se puede estar expuesto. De igual forma, el constante progreso tecnológico, puede conllevar a una evolución en las formas de delinquir, surgiendo de esta forma los delitos informáticos que son actos dirigidos contra la Confidencialidad, Integridad y Disponibilidad de sistemas, redes y datos.

Ante el panorama de riesgo, surge la seguridad informática como el área que se enfoca en la protección de la infraestructura computacional, conformada por estándares, protocolos, normas, procedimientos y herramientas, creadas para minimizar los posibles riesgos.

Por todo lo anterior, el Gobierno Nacional de Colombia ha establecido como reto para la educación de los niños y el beneficio de la comunidad, la masificación de Internet en las Instituciones Educativas públicas de todo el país, diseñando el Programa Vive Digital.

El municipio de Dosquebradas (Risaralda), ha sido beneficiado con el Programa Vive Digital, sin embargo, se ha identificado que no cuenta con una correcta implementación de Seguridad Informática que controle el uso del Internet, para proteger la integridad de los usuarios y prevenir los daños en los equipos, de ahí la importancia de la investigación de un software libre para el control de contenidos, la protección de los activos y para la continuidad del Programa Vive Digital, reconocido como la mejor política TIC del mundo.

Palabras clave: *Programa Vive Digital, Internet, Seguridad informática, Políticas de seguridad, Delitos informáticos, Software libre.*

ABSTRACT

Currently, the world is facing constant changes by the frequent use of the technologies, which have become essential tools for our lives.

Due to the importance of information and the rapid growth of technologies, there is a need to identify the computer risks that may occur, in order to establish policies and tools that govern the safety and help mitigate the risks that can be exposed. Similarly, the constant technological progress, may lead to an evolution in the forms of crime, thus emerging cybercrime that are directed against the confidentiality, integrity and availability of systems, networks and data.

Against the background of risk, arises the computer security as the area that focuses on the protection of the computational infrastructure, comprised of standards, protocols, standards, procedures and tools, created to minimize possible risks.

For all of the above, the Government of Colombia has established as a challenge for the education of children and the benefit of the community, the massification of Internet in public educational institutions around the country, designing the program live Digital.

The municipality of Dosquebradas (Risaralda), has been benefited with the *Vive Digital* program, however, has been identified that do not have a correct implementation of computer security that controls the use of the Internet, to protect the integrity of the users and prevent damage to the equipment, hence the importance of the investigation of a software free for control of content , protection of assets and for the continuity of the Digital lives program, recognized as the best ICT (*Information and Communications Technology*) policy in the world.

Keywords: *Vive Digital program, Internet, Informatic security, Security policies, Cybercrime, Free software.*

CONTENIDO

	pág.
INTRODUCCIÓN	20
1. ALCANCE Y DELIMITACIÓN DEL TEMA DE INVESTIGACIÓN.....	23
1.1. ALCANCE	23
1.2. DELIMITACIÓN	23
1.3. PERTINENCIA Y RELEVANCIA.....	23
1.4. RIESGOS.....	24
2. PROBLEMA DE INVESTIGACIÓN.....	25
3. OBJETIVOS DE LA INVESTIGACIÓN	26
3.1. Objetivo General.....	26
3.2. Objetivos Específicos	26
4. JUSTIFICACIÓN DE LA INVESTIGACIÓN	27
5. MARCO REFERENCIAL DE LA INVESTIGACIÓN	29
5.1. MARCO TEÓRICO - CONCEPTUAL.....	29
5.1.1. Programa Vive Digital	29
5.1.1.1. Objetivos y Aspiraciones del Programa Vive Digital.....	30
5.1.1.2. Principios básicos del Programa Vive Digital	30
5.1.1.3. Masificación de Internet en el Extranjero.....	31
5.1.1.4. Barreras que Impiden la Masificación de Internet.....	33
5.1.2. Ecosistema Digital	35
5.1.2.1. Puntos Vive Digital.....	35
5.1.2.1.1. Fases del Proyecto.....	37

5.1.2.1.2.	Resumen.....	39
5.1.2.2.	Kioscos Vive Digital.....	39
5.1.2.2.1.	Fases Kioscos Vive Digital.....	40
5.1.2.2.2.	Nuevos Kioscos.....	41
5.1.2.2.3.	Requisitos para un Kiosco Vive Digital.....	41
5.1.2.2.4.	Inversión del Programa Vive Digital	42
5.1.3.	Internet	42
5.1.3.1.	Breve Reseña Histórica.....	43
5.1.3.2.	Ventajas y Desventajas del Internet.....	45
5.1.3.2.1.	Ventajas.....	46
5.1.3.2.2.	Desventajas	47
5.1.3.3.	Internet y la Educación	49
5.1.3.4.	La Internet en el desarrollo profesional del docente.....	51
5.1.4.	Seguridad Informática	51
5.1.4.1.	Principios de Seguridad Informática.....	52
5.1.4.2.	Factores de Riesgo	53
5.1.4.3.	Elementos Vulnerables	54
5.1.5.	Delitos Informáticos	54
5.1.5.1.	Características Principales de los Delitos Informáticos.....	55
5.1.5.2.	Tipos de Delitos Informáticos reconocidos por la ONU	56
5.1.5.3.	Tipos de Amenazas y Ataques Informáticos	58
5.1.5.4.	Técnicas de Seguridad Informática.....	59
5.1.6.	Software Libre	60
5.1.6.1.	Tipos de Licencias de Software Libre	61

5.1.6.2.	Ventajas del Software Libre en la Seguridad.....	62
5.1.6.3.	Desventajas del Software Libre	63
5.2.	MARCO CONTEXTUAL.....	64
5.2.1.	Institución Educativa Eduardo Correa Uribe.....	72
5.2.1.1.	Generalidades.....	72
5.2.1.2.	Reseña Histórica de la Sede Educativa Eduardo Correa Uribe	72
5.2.1.3.	Misión	74
5.2.1.4.	Visión.....	74
5.2.1.5.	Ubicación Geográfica y Características.....	75
5.2.1.6.	Aspectos Físicos	79
5.2.1.7.	Procedencia de los Alumnos.....	79
5.2.1.8.	Vías de Acceso.....	79
5.2.1.9.	Sede Principal Vereda El Estanquillo.....	80
5.2.1.10.	Subsede Vereda La Palma	81
6.	HIPÓTESIS	82
7.	METODOLOGÍA DE LA INVESTIGACIÓN.....	83
7.1.	Población o Universo.....	83
7.2.	Muestra	86
7.3.	Delimitación del Estudio	89
7.4.	Variables e Indicadores.....	89
7.5.	Métodos e Instrumentos de Recolección de Información.....	91
7.6.	Procesamiento y análisis de la información.....	91
7.6.1.	Encuesta.....	91
7.6.1.1.	Kiosco Encuestado.....	92

7.6.1.2.	Género.....	93
7.6.1.3.	Edad	94
7.6.1.4.	Grupo al que pertenece	95
7.6.1.5.	Acompañamiento	96
7.6.1.6.	Actividades	97
7.6.1.7.	Frecuencia de Acceso	98
7.6.1.8.	Tiempo de Conexión.....	99
7.6.1.9.	Normas o Pautas	100
7.6.1.10.	Algunas Normas	101
7.6.1.11.	Páginas Web	102
7.6.1.12.	Redes Sociales	104
7.6.1.13.	Contraseñas en Redes Sociales	105
7.6.1.14.	Cuenta de Correo	106
7.6.1.15.	Acciones frente a Correos Electrónicos.....	107
7.6.1.16.	Términos	108
7.6.2.	Lista de Chequeo	110
7.6.2.1.	Género.....	110
7.6.2.2.	Edad	111
7.6.2.3.	Cargo que Desempeña	111
7.6.2.4.	Cantidad de Computadores.....	112
7.6.2.5.	Dispositivo de Conexión a Internet	113
7.6.2.6.	Dispositivo de Distribución del Internet.....	114
7.6.2.7.	Tipo de Conexión a Internet	115
7.6.2.8.	Control de Instalación.....	116

7.6.2.9.	Sistema Operativo.....	117
7.6.2.10.	Licenciamiento.....	118
7.6.2.11.	Antivirus	119
7.6.2.12.	Actualización del Antivirus	120
7.6.2.13.	Descarga de Ficheros	121
7.6.2.14.	Conexiones externas vía Internet.....	122
7.6.2.15.	Conexión Inalámbrica.....	123
7.6.2.16.	Medidas de Seguridad Conexión Inalámbrica	124
7.6.2.17.	Navegador utilizado.....	125
7.6.2.18.	Influencia de Seguridad del Navegador.....	126
7.6.2.19.	Cortafuegos.....	127
7.6.2.20.	Cortafuegos utilizados	128
7.6.2.21.	Sistema de Control Parental.....	129
7.6.2.22.	Contenido consultado	130
8.	HERRAMIENTAS DE SOFTWARE LIBRE	131
8.1.	PfSense	132
8.1.1.	Características Principales de PfSense	134
8.1.2.	Características Avanzadas de PfSense.....	136
8.1.3.	Diagrama PfSense.....	137
8.2.	Zentyal	138
8.2.1	Características Principales de Zentyal.....	139
8.2.2	Diagrama Zentyal	143
8.3.	IPCop.....	144
8.3.1	Características Principales de IPCop.....	145

8.3.2 Características Avanzadas de IPCop	147
8.3.3 Funcionalidad de IPCop	148
8.3.4 Diagrama IPCop	149
9. HERRAMIENTA DE SOFTWARE LIBRE SELECCIONADA PFSense	150
9.1. Instalación de la Herramienta PfSense	151
9.2. Configuración y Pruebas de la Herramienta PfSense	160
10. PROPUESTA DE IMPLEMENTACIÓN	178
10.1. Criterios de Selección de la Herramientas PfSense.....	179
11. CRONOGRAMA.....	182
12. RECURSOS Y PRESUPUESTO.....	183
12.1 Talento Humano	183
12.1.1 Perfil Ingenieros	183
12.1.2 Perfil Técnicos.....	183
12.1.3 Perfil Tabulador.....	183
12.2 Materiales y Equipos	184
12.3 Transporte.....	185
12.4 Recursos Financieros	185
12.5 Fuentes de financiación	186
12.6 Análisis Costo-beneficio:.....	187
CONCLUSIONES	188
BIBLIOGRAFÍA	191
ANEXOS	196

LISTA DE TABLAS

	pág.
Tabla 1. <i>Variables e Indicadores</i>	90
Tabla 2. <i>Cronograma de Actividades por Mes</i>	182
Tabla 3. <i>Presupuesto Financiero Personal</i>	185
Tabla 4. <i>Presupuesto Financiero Equipos</i>	186
Tabla 5. <i>Total Presupuestos</i>	186

LISTA DE FIGURAS

	pág.
Figura 1. <i>Penetración de Internet Fijo, Internet Móvil y PCs en países seleccionados</i>	33
Figura 2. <i>Barreras que Impiden la Masificación de Internet</i>	35
Figura 3. <i>Áreas del Punto Vive Digital</i>	36
Figura 4. <i>Puntos Vive Digital en Fase 1</i>	38
Figura 5. <i>Tipos de KVD (Kioscos Vive Digital) en Fase 1</i>	40
Figura 6. <i>Fraudes cometidos mediante Manipulación de Computadoras</i>	56
Figura 7. <i>Falsificaciones Informáticas</i>	56
Figura 8. <i>Daños o Modificaciones de Programas o Datos Computarizados</i>	57
Figura 9. <i>PVD (Puntos Vive Digital) asignados</i>	66
Figura 10. <i>Regionalización de los PVD (Puntos Vive Digital) asignados</i>	67
Figura 11. <i>Nuevos PVD (Puntos Vive Digital) asignados</i>	68
Figura 12. <i>Listado de PVD (Puntos Vive Digital) Beneficiados en Risaralda</i>	69
Figura 13. <i>Servicio de Puntos Vive Digital</i>	70
Figura 14. <i>Listado de KVD (Kioscos Vive Digital) en Dosquebradas</i>	71
Figura 15. <i>Ubicación Geográfica Municipio de Dosquebradas – Risaralda</i>	76
Figura 16. <i>Mapa Municipio de Dosquebradas – Risaralda</i>	77
Figura 17. <i>Mapa de las Veredas en el Municipio de Dosquebradas – Risaralda</i>	78
Figura 18. <i>Veredas beneficiadas con los Kioscos Vive Digital (KVD) en Dosquebradas...</i>	83
Figura 19. <i>Población proyectada con base en el censo DANE de 2005</i>	84
Figura 20. <i>Total Población de las Veredas con KVD Rango de Edades (0 a + de 80)</i>	84
Figura 21. <i>Total Población de las Veredas con KVD Rango de Edades (5 a 64)</i>	85
Figura 22. <i>Población o Universo Rango de Edades (5 a 64)</i>	86
Figura 23. <i>Fórmula de Muestreo Aleatorio Simple para población finita</i>	86
Figura 24. <i>Resultado Formula Muestreo Aleatorio Simple (Población finita)</i>	87
Figura 25. <i>Muestreo de Población x Vereda con KVD</i>	88
Figura 26. <i>Consolidado de Muestreo de Población x Vereda con KVD</i>	88

Figura 27. Encuesta / Kiosco Encuestado.....	92
Figura 28. Encuesta / Género.....	93
Figura 29. Encuesta / Edad.....	94
Figura 30. Encuesta / Grupo al que pertenece.....	95
Figura 31. Encuesta / Acompañamiento.....	96
Figura 32. Encuesta / Actividades.....	97
Figura 33. Encuesta / Frecuencia de Acceso.....	98
Figura 34. Encuesta / Tiempo de Conexión.....	99
Figura 35. Encuesta / Normas o Pautas.....	100
Figura 36. Encuesta / Algunas Normas.....	101
Figura 37. Encuesta / Páginas Web.....	102
Figura 38. Encuesta / Redes Sociales.....	104
Figura 39. Encuesta / Contraseñas en Redes Sociales.....	105
Figura 40. Encuesta / Cuenta de Correo.....	106
Figura 41. Encuesta / Acciones frente a Correos Electrónicos.....	107
Figura 42. Encuesta / Términos.....	108
Figura 43. Lista de Chequeo / Género.....	110
Figura 44. Lista de Chequeo / Edad.....	111
Figura 45. Lista de Chequeo / Cargo que Desempeña.....	111
Figura 46. Lista de Chequeo / Cantidad de Computadores.....	112
Figura 47. Lista de Chequeo / Dispositivo de Conexión a Internet.....	113
Figura 48. Lista de Chequeo / Dispositivo de Distribución del Internet.....	114
Figura 49. Lista de Chequeo / Tipo de Conexión a Internet.....	115
Figura 50. Lista de Chequeo / Control de Instalación.....	116
Figura 51. Lista de Chequeo / Sistema Operativo.....	117
Figura 52. Lista de Chequeo / Licenciamiento.....	118
Figura 53. Lista de Chequeo / Antivirus.....	119
Figura 54. Lista de Chequeo / Actualización del Antivirus.....	120
Figura 55. Lista de Chequeo / Descarga de Ficheros.....	121
Figura 56. Lista de Chequeo / Conexiones externas vía Internet.....	122

Figura 57. <i>Lista de Chequeo / Conexión Inalámbrica</i>	123
Figura 58. <i>Lista de Chequeo / Medidas de Seguridad Conexión Inalámbrica</i>	124
Figura 59. <i>Lista de Chequeo / Navegador utilizado</i>	125
Figura 60. <i>Lista de Chequeo / Influencia de Seguridad del Navegador</i>	126
Figura 61. <i>Lista de Chequeo / Cortafuegos</i>	127
Figura 62. <i>Lista de Chequeo / Cortafuegos utilizados</i>	128
Figura 63. <i>Lista de Chequeo / Sistema de Control Parental</i>	129
Figura 64. <i>Lista de Chequeo / Contenido consultado</i>	130
Figura 65. <i>Logo PfSense</i>	132
Figura 66. <i>Diagrama PfSense</i>	137
Figura 67. <i>Logo Zentyal</i>	138
Figura 68. <i>Diagrama Zentyal</i>	143
Figura 69. <i>Logo IPCop</i>	144
Figura 70. <i>Diagrama IPCop</i>	149
Figura 71. <i>Instalación PfSense / Configuración de VLANs</i>	151
Figura 72. <i>Instalación PfSense / Conexión de la Interface WAN - LAN</i>	152
Figura 73. <i>Instalación PfSense / Interfaces asignadas WAN – LAN</i>	153
Figura 74. <i>Instalación PfSense / Ventana de Bienvenida de PfSense</i>	154
Figura 75. <i>Instalación PfSense / Configuración de la Consola</i>	155
Figura 76. <i>Instalación PfSense / Tarea a Realizar</i>	156
Figura 77. <i>Instalación PfSense / Ejecución de Comandos</i>	156
Figura 78. <i>Instalación PfSense / Ventana de Confirmación</i>	157
Figura 79. <i>Instalación PfSense / Reinicio</i>	158
Figura 80. <i>Instalación PfSense / Secuencia de Reinicio</i>	159
Figura 81. <i>Configuración PfSense / Interface: LAN</i>	160
Figura 82. <i>Configuración PfSense / Servicios: Servidor DHCP</i>	161
Figura 83. <i>Configuración PfSense / Información del Sistema - Interfaces</i>	162
Figura 84. <i>Configuración PfSense / Selección de Paquete Squid</i>	163
Figura 85. <i>Configuración PfSense / Instalación Paquete Squid</i>	164
Figura 86. <i>Configuración PfSense / Selección de Bloqueo Listas Negras</i>	166

Figura 87. Configuración PfSense / Inicio Actualización Listas Negras.....	167
Figura 88. Configuración PfSense / Acceso de Servicios	168
Figura 89. Configuración PfSense / Prueba de acceso a una página de porno	169
Figura 90. Configuración PfSense / Herramientas adicionales: HAVP Antivirus	170
Figura 91. Configuración PfSense / Instalación del paquete HAVP Antivirus.....	171
Figura 92. Configuración PfSense / Página General de HAVP Antivirus.....	172
Figura 93. Configuración PfSense / Herramientas adicionales: MailScanner	173
Figura 94. Configuración PfSense / Instalación del paquete MailScanner.....	174
Figura 95. Configuración PfSense / Instalación del paquete Dansguardian.....	175
Figura 96. Configuración PfSense / Algunas reglas dentro del Firewall Pfsense.....	176
Figura 97. Configuración PfSense / Prueba de acceso a facebook	177
Figura 98. Configuración PfSense / Herramientas adicionales de PfSense 01	178
Figura 99. Configuración PfSense / Herramientas adicionales de PfSense 02	178

LISTA DE ANEXOS

	pág.
ANEXO A ENCUESTA.....	197
ANEXO B LISTA DE CHEQUEO.....	202

INTRODUCCIÓN

En la actualidad, el mundo se enfrenta a constantes cambios que influyen en gran parte en la evolución e innovación de su entorno y en la transformación de su propio estilo de vida; estos cambios obedecen al uso cada vez más frecuente de las tecnologías, las cuales se han convertido en el medio apropiado e indispensable para el desarrollo de la vida, como lo es trabajar y la necesidad imperiosa de aprender.

Debido a la importancia de la información, ya sea personal, institucional o corporativa, y al acelerado crecimiento de las tecnologías, surge la necesidad de protegerla, pues el éxito de cualquier proyecto depende de qué tan segura se encuentre la información; a pesar de los riesgos que se puedan presentar.

Es importante valorar la información como un activo fundamental, sea cual sea su origen o finalidad, puesto que la seguridad de la misma es un componente crítico que hace parte de la estrategia planteada para alcanzar el logro de objetivos en una organización, y el tema se vuelve más interesante si se parte de la consideración que día a día aumenta el número de usuarios en Internet, más aún cuando algunos de éstos cuentan con la experticia para violentar los esquemas de seguridad, lo que permite de una manera directa el incremento de vulnerabilidades en las redes; por esta razón, es indispensable la gestión e identificación correcta de los riesgos internos y externos, para establecer políticas y/o herramientas de software que regulen la seguridad a implementar y a la vez ayuden a mitigar los riesgos a los que se puede estar expuesto, o por lo menos que permita que el impacto, por materialización de los riesgos, sea el mínimo tolerable.

De igual forma, el constante progreso tecnológico que experimenta actualmente la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de las amenazas tradicionales, como al surgimiento de nuevos actos ilícitos surgiendo de esta forma los delitos informáticos entendiéndolos como los actos dirigidos

contra la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos, así como también el abuso de los mismos.

Ante el panorama de riesgo, surge la **seguridad informática** como el área que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta en una organización (incluyendo los datos contenidos, material informático y programas), existiendo para ello una serie de estándares, protocolos, métodos, reglas, normas, procedimientos, herramientas, aspectos éticos y legales, concebidos para minimizar los posibles riesgos a la infraestructura o a la información. Igualmente la seguridad informática comprende tanto software, bases de datos, metadatos, archivos, como todo lo que se considere o valore activo y signifique un riesgo si ésta llega a manos inescrupulosas; siendo este tipo de información *privilegiada y/o confidencial*.

Asimismo, la seguridad informática busca confirmar que los recursos de los sistemas de información, sean utilizados de la mejor manera y que el acceso o modificación de la misma, sólo sea posible a través de las personas idóneas, que se encuentran acreditadas y dentro de los permisos y límites de su autorización, primando ante todo su ética profesional; de ahí que las nuevas tecnologías de seguridad se presenten como un elemento indispensable para visualizar, controlar y gestionar de forma eficiente todos los recursos que se utilizan.

Por todo lo anterior, en estos momentos la seguridad informática se debe considerar como un tema de dominio obligado por cualquier persona que hace uso de Internet, todo con el fin de no permitir que la información sea expuesta y comprometida; tal es el caso de las instituciones educativas del municipio de Dosquebradas (Risaralda) que han sido beneficiadas dentro del **Plan Vive Digital**, proyecto del Gobierno Nacional de Colombia, que consiste en la donación de una sala de acceso a Internet con computadores, puestos de trabajo, sala de capacitación con tablero digital, consolas de videojuegos, televisores en la zona de entretenimiento y computadores adicionales para realizar trámites y servicios con el Estado Colombiano, todo con el fin de brindar herramientas para la educación de los

niños y la comunidad, pero que a la fecha se ha identificado que dicho proyecto carece de sistemas de protección y no cuenta en su totalidad con un análisis e implementación de seguridad informática que permita salvaguardar la información y controlar el uso que se le da al Internet, para así prevenir la afectación de los equipos, pero principalmente la integridad de los usuarios, de ahí la importancia de la investigación de un software libre para el control de contenidos, la protección de los activos que les han sido asignados y para la continuidad del Plan Vive Digital, que ha sido reconocido internacionalmente como la mejor política TIC del mundo.

Teniendo en cuenta los factores anteriormente explicados es posible determinar que este proyecto de investigación pretende justificar la necesidad de implementar una propuesta de seguridad informática, para este caso se delimitará al uso de software libre, que contenga los elementos necesarios que permitan disminuir en un grado significativo la inseguridad informática a la cual están expuestas las redes de datos de los Kioscos VIVE DIGITAL en el municipio de Dosquebradas (Risaralda).

1. ALCANCE Y DELIMITACIÓN DEL TEMA DE INVESTIGACIÓN

1.1. ALCANCE

El Proyecto de Investigación llegará hasta la implementación de Políticas de Seguridad a través de una Herramienta de Software Libre, que permita mejorar y prevenir el mal uso del Internet, convirtiéndose en instrumento de control y medida de Seguridad Informática, en la Institución Educativa Eduardo Correa Uribe - Sede La Palma del Municipio de Dosquebradas (Risaralda), como prueba piloto para ser aplicado en otras Instituciones Educativas Públicas beneficiadas con el programa VIVE DIGITAL en este municipio.

1.2. DELIMITACIÓN

Una de las limitaciones es el tiempo que pueda proporcionar la Institución Educativa Eduardo Correa Uribe, para facilitar la información necesaria en la Investigación, así como también para la realización de las pruebas requeridas en la búsqueda de la Herramienta de Software Libre como medida de Seguridad Informática para prevenir el mal uso del Internet; de igual forma otra de las limitaciones es la ubicación de la Institución, ya que se encuentra en la zona rural del Municipio de Dosquebradas (Risaralda).

1.3. PERTINENCIA Y RELEVANCIA

La Investigación tiene como base la vulnerabilidad de los Kioscos VIVE DIGITAL de las Instituciones Educativas beneficiadas del municipio de Dosquebradas (Risaralda), al no contar con un análisis e implementación de Seguridad Informática que controle el uso del Internet, para prevenir la afectación de los equipos con Software malicioso y/o dañino, que tendría un impacto directo en los recursos financieros de las instituciones. Además, se limitan las posibilidades para que los estudiantes y otros usuarios de este programa ingresen y consulten páginas o sitios web que generen distracción o riesgos para su integridad.

1.4. RIESGOS

La realización del Proyecto de Investigación, no implica riesgos para la seguridad de los investigadores, debido a que se fundamenta en la búsqueda de alternativas de Software Libre que se conviertan en herramientas de control y medidas de seguridad informática para proteger los activos que le han sido asignados a la Institución Educativa Eduardo Correa Uribe a través del Programa VIVE DIGITAL; de igual forma poder dar continuidad al mismo, protegiendo la integridad de todos y cada uno de los usuarios que utilizan dichas herramientas tecnológicas.

2. PROBLEMA DE INVESTIGACIÓN

¿Puede la implementación de Políticas de Seguridad a través de Herramientas de Software Libre, mejorar y prevenir el mal uso del Internet, en las Instituciones Educativas Públicas beneficiadas con el Programa **VIVE DIGITAL** direccionado por el Gobierno Nacional en el Municipio de Dosquebradas?

3. OBJETIVOS DE LA INVESTIGACIÓN

3.1. Objetivo General

- Especificar las Herramientas de Software Libre que pueden ser usadas como medidas de Seguridad Informática para prevenir el mal uso del Internet en las Instituciones Educativas Públicas del Municipio de Dosquebradas beneficiadas con el Programa **VIVE DIGITAL**.

3.2. Objetivos Específicos

Para el logro del Objetivo general, se establecen los siguientes objetivos específicos:

- Determinar el nivel actual de seguridad con el uso de internet en las Instituciones Educativas Públicas del Municipio de Dosquebradas beneficiadas con el Programa **VIVE DIGITAL**.
- Definir las Herramientas de Software Libre que puedan ser implementadas en las Instituciones Educativas Públicas para prevenir el mal uso del Internet.
- Realizar una propuesta de implementación de Herramientas de Software Libre como medida de Seguridad Informática para las Instituciones Educativas Públicas del Municipio de Dosquebradas.
- Implementar la Herramienta de Software Libre como medida de Seguridad Informática propuesta en la Institución Educativa **Eduardo Correa Uribe** - Sede La Palma del Municipio de Dosquebradas Risaralda, como prueba piloto para ser aplicado posteriormente en otras Instituciones Educativas Públicas beneficiadas con el Programa **VIVE DIGITAL** en el mismo municipio.

4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

El Gobierno Nacional de Colombia se ha establecido como reto que el país dé un gran salto tecnológico mediante la masificación de Internet y el desarrollo del ecosistema digital nacional, con el fin de alcanzar la prosperidad democrática, gracias a la apropiación y el uso de la tecnología; para ello ha diseñado el Programa **Vive Digital**, ya que está demostrado que hay una correlación directa entre la penetración de internet, la apropiación de las tecnologías de la información y las comunicaciones (TIC), la generación de empleo y la reducción de la pobreza. Por lo tanto, el Programa VIVE DIGITAL, conlleva entonces a importantes beneficios sociales y económicos¹.

Una de las fases de este Plan, es la donación de una sala de acceso a Internet con computadores, puestos de trabajo, sala de capacitación con tablero digital, consolas de videojuegos, televisores en la zona de entretenimiento y computadores adicionales para realizar trámites y servicios con el Estado Colombiano, todo lo anterior para las Instituciones Educativas públicas de diferentes regiones del país, con el fin de brindar herramientas para la educación de los niños y la comunidad.

El municipio de Dosquebradas (Risaralda) ha sido beneficiado dentro de este programa y ha empezado a implementarse en sus Instituciones Educativas públicas el uso de estas tecnologías². Sin embargo, se ha identificado que dicho proyecto no cuenta en su totalidad con un análisis e implementación de Seguridad Informática que controlen el uso que se le da al Internet, para así proteger la integridad de los usuarios y prevenir la afectación de los equipos con Software maliciosos que tendrían un impacto directo en los recursos financieros de las instituciones para la reparación de estos daños. Además, se limitan las

¹ Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Vive Digital Colombia. *El Plan Vive Digital*. Recuperado de: <http://www.mintic.gov.co/portal/vivedigital/612/w3-article-1510.html>

² Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (29 de diciembre de 2012). *Dosquebradas ya cuenta con Punto Vive Digital*. Sala de Prensa. Noticias. Recuperado de: <http://mintic.gov.co/portal/604/w3-article-1310.html>

posibilidades para que los estudiantes y otros usuarios de este programa ingresen y consulten páginas o sitios web que generen distracción o riesgos para su integridad.

Por todo lo anterior, se considera importante el desarrollo de este Proyecto, para proponer a dichas instituciones, alternativas de Software Libre, para las cuales no requiera realizar inversiones económicas que seguramente no están contempladas dentro de su presupuesto y que se conviertan en herramientas de control y medidas de seguridad informática para proteger los activos que les han sido asignados y poder dar continuidad al Programa **VIVE DIGITAL**, que ha sido merecedor de reconocimientos internacionales como la mejor política TIC del mundo.

5. MARCO REFERENCIAL DE LA INVESTIGACIÓN

5.1. MARCO TEÓRICO - CONCEPTUAL

Para llevar a cabo la presente investigación, se tomará como referente los siguientes soportes teóricos:

5.1.1. Programa Vive Digital

Vive Digital, es un plan de tecnología de carácter nacional, que busca que el país dé un gran salto tecnológico mediante la masificación de Internet y el desarrollo del ecosistema digital nacional. Se diseñó como estrategia del gobierno para alcanzar la prosperidad democrática gracias a la apropiación y el uso de la tecnología, apostando principalmente a la masificación de Internet. El gobierno tiene la firme convicción de que hay una correlación directa entre la penetración de Internet, la apropiación de las Tecnologías de la Información y las Comunicaciones (TIC), la generación de empleo y la reducción de la pobreza, generando de esta manera importantes beneficios sociales y económicos.

El promotor de esta iniciativa es el Ministerio de Tecnologías de la Información y las Comunicaciones, quienes entre los años 2011 y 2012 estructuraron el Documento de Planeación Estratégica del Subsistema de Innovación³ y el Marco Jurídico del Sistema de Investigación, Desarrollo e Innovación - Subsistema de Innovación para el uso y apropiación de TIC en el Gobierno, documentos en los cuales se amplía toda la información sobre el Programa VIVE DIGITAL y servirán como base para el desarrollo del presente trabajo.

³ Ministerio de Tecnologías de la Información y las Comunicaciones. *Documento de Planeación Estratégica del Subsistema de Innovación*. República de Colombia. Recuperado de: http://www.mintic.gov.co/portal/604/articles-6116_recurso_2.pdf

5.1.1.1. Objetivos y Aspiraciones del Programa Vive Digital

El objetivo principal del Programa VIVE DIGITAL es promover la masificación del uso de Internet, la apropiación de tecnología, y la creación de empleos TIC directos e indirectos; buscando con todo lo anterior, reducir el desempleo, la pobreza, para poder aumentar la competitividad del país y dar un salto hacia la Prosperidad Democrática.

5.1.1.2. Principios básicos del Programa Vive Digital

Para asegurar que las intervenciones estatales sean adecuadas e integrales y logren optimizar el uso de los recursos, el Programa VIVE DIGITAL sigue cinco principios básicos⁴:

- 1. "El mercado hasta donde sea posible, el Estado hasta donde sea necesario" La Tercera Vía, 1999, Dr. Juan Manuel Santos. Promover el desarrollo del sector privado para expandir infraestructura y ofrecer servicios.*
- 2. Incentivar de forma integral la oferta y la demanda de servicios digitales para alcanzar una masa crítica.*
- 3. Reducir barreras normativas e impositivas para facilitar el despliegue de infraestructura y oferta de servicios de telecomunicaciones.*
- 4. Priorizar los recursos del Estado en inversiones de capital.*
- 5. El Gobierno va a dar ejemplo.*

⁴ Ministerio de Tecnologías de la Información y las Comunicaciones. Plan Vive Digital. *Principios básicos del Plan Vive Digital*. Recuperado de: <http://www.mintic.gov.co/portal/vivedigital/612/w3-article-1512.html>

5.1.1.3. Masificación de Internet en el Extranjero

Muchos países como Corea del Sur, Japón, Hong Kong y los países nórdicos, entre otros, en donde los niveles de penetración son mucho mayores que el promedio mundial, han diseñado e implementado en los últimos años, planes similares de masificación de Internet con distintos niveles de éxito. Al evaluar los planes de éstos y otros países, contrastándolos con las características particulares del caso Colombiano, en términos de recursos disponibles, geografía, densidad poblacional, infraestructura actual y régimen normativo; se encontró que el nivel de efectividad que lograron éstas iniciativas dependen de muchos factores, los cuales suelen estar presentes en los casos más exitosos. Los factores que incrementan la posibilidad de éxito de un programa como VIVE DIGITAL son⁵:

- **Visión País:** *Integrar dentro de la visión del país que tiene el gobierno y la industria privada, la promoción al despliegue de infraestructura, ya sea de fibra óptica o inalámbrica, como uno de los componentes esenciales.*
- **Agenda Regulatoria:** *Es importante que la normatividad esté enmarcada en una agenda regulatoria clara alineada con los objetivos del plan.*
- **Asistencia Financiera:** *Por parte del Gobierno es necesario definir el alcance de la asistencia financiera pública para apoyar el despliegue de las redes con subsidios directos o indirectos.*

⁵ Ministerio de Tecnologías de la Información y las Comunicaciones. Plan Vive Digital. *Experiencias Internacionales en la Masificación de Internet*. Recuperado de:
<http://www.mintic.gov.co/portal/vivedigital/612/w3-article-1512.html>

- ***Estimular la Demanda:*** *Contar con una serie de medidas encaminadas a promover la demanda de las TIC por parte de la población general, la empresa privada y el Gobierno.*
- ***Despliegue de Infraestructura:*** *Definir claramente las acciones a seguir para aumentar la cobertura de las redes de fibra óptica e inalámbricas en el país, asegurando la participación de los operadores.*

Es importante hacer referencia que Colombia tiene un importante atraso en cuanto a la masificación del Internet, así como también en el uso de equipos de cómputo frente a otros países de la región; este rezago es mayor cuando se le compara con países desarrollados, y más notorio aún, en el caso de los países latinoamericanos, ya que hay varios que le llevan la delantera a Colombia, como es el caso de Chile, México y Brasil.

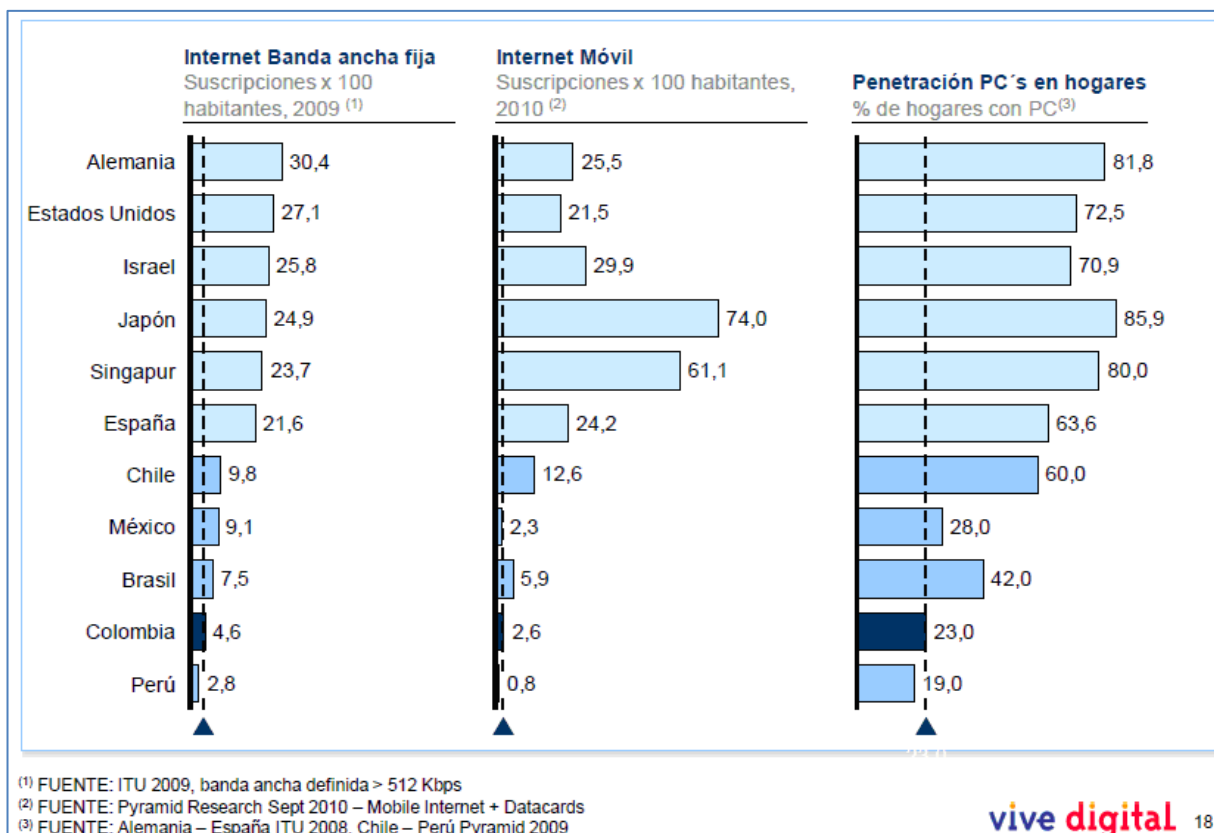


Figura 1. Penetración de Internet Fijo, Internet Móvil y PCs en países seleccionados
Fuente: Orduz, R. (07 de Diciembre de 2010). *Plan Vive Digital Colombia (II)*. Colombia Digital.
Recuperado de: <http://colombiadigital.net/opinion/columnistas/los-numeros-de-las-tic/item/458-plan-vive-digital-colombia-ii.html>

5.1.1.4. Barreras que Impiden la Masificación de Internet

Se ha identificado que en Colombia existen cuatro grandes barreras que dificultan la masificación del uso de Internet⁶.

⁶ Ministerio de Tecnologías de la Información y las Comunicaciones. Plan Vive Digital. *Barreras que Impiden la Masificación de Internet*. Recuperado de: <http://www.mintic.gov.co/portal/vivedigital/612/w3-article-1519.html>

- **Ciudadanos y Microempresas no ven la utilidad.** Como muestran las encuestas, una de las grandes razones para no tener Internet, tanto para los ciudadanos como para las microempresas, es que no encuentran la necesidad o utilidad del servicio de Internet. Esto se debe en parte a la falta de contenidos y aplicaciones locales útiles para el ciudadano o microempresa nacional, así como a la falta de apropiación de la tecnología.
- **Bajo Poder Adquisitivo del Ciudadano.** El costo de los terminales y el servicio de Internet sigue siendo relativamente alto para los ingresos de la mayoría de ciudadanos, por lo que muchos de estos no tienen posibilidad económica de acceder a ellos.
- **Altos Costos de Desplegar Infraestructura.** En el país actualmente sólo alrededor de 200 municipios de los 1.102 están conectados a través de la red de fibra óptica. Las características geográficas y de dispersión han limitado el despliegue de las redes de telecomunicaciones. También, existen dificultades administrativas tanto en los territorios como en la última milla para el despliegue de infraestructura.
- **Recursos.** La realidad colombiana hace que los recursos con los que cuenta el estado para invertir en infraestructura sean limitados, por lo que es importante encontrar la mejor manera de invertirlos. En el Programa VIVE DIGITAL planteamos diversas iniciativas para superarlas.



Figura 2. Barreras que Impiden la Masificación de Internet

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. Plan Vive Digital.

Barreras que Impiden la Masificación de Internet. Recuperado de:

<http://www.mintic.gov.co/portal/vivedigital/612/w3-article-1519.html>

5.1.2. Ecosistema Digital

5.1.2.1. Puntos Vive Digital

Promueve el uso y aprovechamiento de las TIC, a través de la disposición del acceso comunitario a zonas funcionales para el uso de internet, entretenimiento, capacitación, y trámites de Gobierno en Línea.

En el marco del Programa VIVE DIGITAL, el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Conectividad, promueve la creación de 800 Puntos Vive Digital (*centros comunitarios de acceso a Internet*) en cabeceras municipales y en zonas de estratos 1, 2 y 3, donde haya un manifiesto interés de actores regionales por participar y que además cuenten con conexión a redes de transporte terrestre de Banda Ancha tales como Fibra Óptica, redes DSL, cable, entre otras.

El Punto Vive Digital es un espacio que garantiza el acceso a las Tecnologías de la Información y las Comunicaciones que permite integrar a la comunidad en escenarios de acceso, capacitación, entretenimiento y otras alternativas de servicios TIC en un mismo lugar, con el fin de contribuir al desarrollo social y económico de la población y al mejoramiento de la calidad de vida de cada Colombiano.

La siguiente figura muestra las áreas mínimas requeridas para el funcionamiento de los PVD:

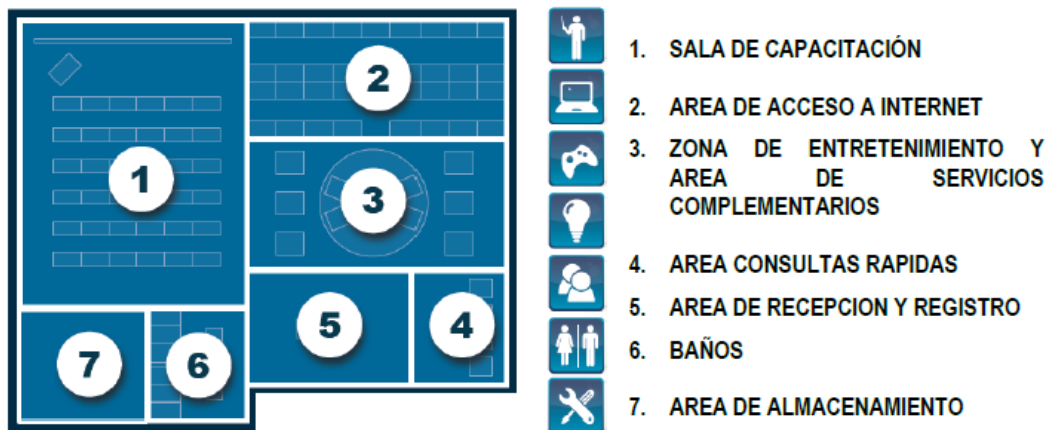


Figura 3. Áreas del Punto Vive Digital

Fuente: FONADE, Fondo Financiero de Proyectos de Desarrollo. (Abril de 2013).

Dotación, Instalación y puesta en funcionamiento de la Infraestructura técnica de los Puntos Vive Digital Fase 1. Bogotá D.C. Recuperado de:

http://www.fonade.gov.co/Contratos/Documentos/3767__2013041910380819%20ANEXO%20No%202-%20DOC%20TECNICO%20PROVEEDOR%20FASE%201.pdf

5.1.2.1.1. Fases del Proyecto

Fase 0

Durante esta fase, se instalaron 71 Puntos Vive Digital en 67 municipios del país, en articulación con entidades territoriales y operadores, en donde el Ministerio TIC aporta la infraestructura tecnológica y equipos, y paga la operación; el operador suministra la conectividad, el mantenimiento de equipos y contrata al administrador, y la Alcaldía pone el sitio y su adecuación, provee los servicios públicos y vigilancia.

Fase 1

En septiembre del año 2012 se convocó a los entes territoriales para participar de la convocatoria de la Fase 1 de PVD (*Punto Vive Digital*) y en septiembre del año 2013 se adjudicaron los operadores para la dotación, instalación y puesta en funcionamiento.

En esta fase la Dirección de Conectividad se propuso instalar 341 PVD en 245 municipios de 25 departamentos del país durante el primer semestre del 2014, con los que se contribuyendo a la reducción de la brecha digital y transformando la vida de cada colombiano. Municipios como Don Matías en Antioquia, Jerusalén en Cundinamarca y La Victoria en el Valle del Cauca contarían con Puntos Vive Digital.



Figura 4. *Puntos Vive Digital en Fase 1*

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. Ecosistema Digital. Usuarios. *Puntos Vive Digital*. Recuperado de: <http://www.mintic.gov.co/portal/vivedigital/612/w3-article-4312.html>

Fase Plus

En diciembre del 2013 se inauguró el primer Punto Vive Digital Plus, ubicado en la localidad de Suba, en la ciudad de Bogotá. En mayo del 2014, el país contó con 16 Puntos Vive Digital Plus, y al término del 2014, los colombianos contaron con cerca de 200 puntos adicionales.

Con talleres de creación de aplicaciones, animaciones y desarrollo de software, los PVD Plus incentivan que los estudiantes sean emprendedores y generadores de nuevos conocimientos; gracias a esto, los jóvenes de nuestro país tendrán la oportunidad de hacerse técnicos en TI. La Isla de San Andrés, Riohacha, Neiva, Viotá y Valledupar son algunos de los municipios que contarán con Puntos Vive Digital Plus.

5.1.2.1.2. Resumen

En mayo del 2012, en el marco del Día Mundial de Internet, se inauguraron simultáneamente los primeros cuatro (4) PVD de la Fase 0 en los municipios de Caloto y Popayán (Cauca), Galapa (Atlántico) y Ventaquemada (Boyacá), contando con la masiva asistencia de la población local que buscaba aprender y capacitarse en TIC. A partir de este momento siguieron las inauguraciones de los demás Puntos, hasta el 1er semestre del 2013.

En septiembre del año 2012 se convocó a los entes territoriales para participar de la convocatoria de la Fase 1 de PVD y en septiembre del año pasado se adjudicaron los operadores para la dotación, instalación y puesta en funcionamiento de los mismos.

En diciembre del 2013 se inauguró el primer Punto Vive Digital Plus, ubicado en la localidad de Suba, en la ciudad de Bogotá. En febrero del 2014, el país tendrá 16 Puntos Vive Digital Plus, y al término del 2014, los Colombianos contarán con cerca de 200 puntos adicionales.

Con referencia a la apropiación TIC, en la actualidad se han capacitado 100.771 personas en los Puntos Vive Digital que se encuentran operando, en temas como alfabetización digital, competencias específicas y como parte de las alianzas con entidades como el Sena, universidades, alcaldías y líderes Comunitarios.

5.1.2.2. Kioscos Vive Digital

Los Kioscos Vive Digital son puntos de acceso comunitario a Internet con los niños, jóvenes y adultos de 5300 centros poblados (veredas y corregimientos)

de más de 100 habitantes, donde pueden conectarse a internet y recibir capacitaciones gratuitas en uso y apropiación de las TIC.

Los Kioscos Vive Digital son de la comunidad y para la comunidad, instalados en lugares comunes como casas de familia, salones comunales, droguerías y colegios, donde los usuarios podrán acceder también a otros servicios como telefonía, fax, escáner y fotocopias.

5.1.2.2.1. Fases Kioscos Vive Digital

Fase 1 - Tipos

TIPO	EQUIPOS	SERVICIOS
TIPO A	Dos (2) Computadores Una (1) Línea Telefónica	Internet Telefonía
TIPO B	Cuatro (4) Computadores Dos (2) Líneas Telefónicas Una (1) Impresora Multifuncional Monocromática	Internet Telefonía Fax Escaneado Fotocopias
TIPO C	Seis (6) Computadores Dos (2) Líneas Telefónicas Una (1) Impresora Multifuncional Color Televisor/DVD	Internet Telefonía Fax Escaneado Fotocopias

Figura 5. Tipos de KVD (Kioscos Vive Digital) en Fase 1

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. Plan Vive Digital. *Tipos de Kioscos Vive Digital*. Recuperado de: <http://www.mintic.gov.co/portal/vivedigital/612/w3-article-5277.html>

Los criterios de elegibilidad de los centros beneficiados con los KVD son:

- Ser reconocidos por el DANE
- Tener una Población igual o mayor a 100 habitantes
- No contar con establecimientos de acceso público a Internet a una distancia menor de dos (2) kilómetros

Fase 2

Serán espacios ubicados en establecimientos y sedes educativas, donde los docentes y estudiantes de las zonas rurales y apartadas del país se beneficiarán del servicio de conectividad a Internet, y en horario extracurricular, todos los habitantes de estas zonas, además podrán acceder a servicios de telefonía, alfabetizarse digitalmente, realizar trámites y servicios con el Estado y optimizar sus actividades económicas.

5.1.2.2.2. Nuevos Kioscos

Ante el éxito de la iniciativa y su impacto positivo en las comunidades el gobierno decidió ampliar el número de kioscos a 5.300 en todo el país, con una inversión de 551.527'489.698 de pesos. Entrando en funcionamiento desde el 2014.

Adicionalmente, 200 Kioscos se ubicaron en resguardos y comunidades indígenas, bases militares, parques nacionales naturales y sitios de frontera.

¡Vive Digital promueve la tecnología en la vida de cada colombiano!

5.1.2.2.3. Requisitos para un Kiosco Vive Digital

- Estar ubicada en centros poblados reconocidos por el DANE con una población mayor o igual que 100 habitantes.
- El centro poblado no podrá tener un sitio de acceso público a Internet.

- Comprometerse a abrir al público en general, como mínimo 20 horas a la semana (incluyendo fines de semana), inclusive en los periodos de vacaciones.
- Garantizar el servicio de energía eléctrica, durante el periodo de servicio del Kiosco Vive Digital.
- Contar con computadores.
- No contar con servicio de Internet en la sede educativa.

5.1.2.2.4. Inversión del Programa Vive Digital

Con una inversión de hasta \$551.527.489.698 de pesos, la Licitación Pública No. 008 de 2013 seleccionará uno o más proponentes que tendrán la misión de diseñar, planear, instalar, poner en servicio, administrar, operar y realizar mantenimiento de 4.200 Kioscos Vive Digital que se suman a los 1.144 ya implementados por el Ministerio TIC.

5.1.3. Internet

Se puede definir como una "red de redes", es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí.

Para contextualizar, una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos.

De esta manera, *Internet sirve de enlace entre redes más pequeñas y permite ampliar su cobertura al hacerlas parte de una "red global". Esta red global tiene la*

característica de que utiliza un lenguaje común que garantiza la intercomunicación de los diferentes participantes; este lenguaje común o protocolo (un protocolo es el lenguaje que utilizan las computadoras al compartir recursos) se conoce como TCP/IP⁷.

Resumiendo, Internet es la "red de redes" que utiliza TCP/IP como su protocolo de comunicación; es un acrónimo de INTERconnected NETworks (Redes interconectadas); para otros, Internet es un acrónimo del inglés INTERnational NET, que traducido al español sería Red Mundial.

5.1.3.1. Breve Reseña Histórica⁸

Los inicios de Internet se remontan a los años 60's. Mientras transcurría la guerra fría, Estados Unidos crea una red exclusivamente militar, con el objetivo de que, en el hipotético caso de un ataque ruso, se pudiera tener acceso a la información militar desde cualquier punto del país.

Esta red se creó en 1969 y se llamó **ARPANET**. En principio, la red contaba con 4 ordenadores distribuidos entre distintas universidades del país. Dos años después, ya contaba con unos 40 ordenadores conectados; tanto fue el crecimiento de la red que su sistema de comunicación se quedó obsoleto. Por lo anterior, dos investigadores crearon el Protocolo TCP/IP, que se convirtió en el estándar de comunicaciones dentro de las redes informáticas (actualmente seguimos utilizando dicho protocolo).

⁷ Club Planeta. *¿Qué es Internet?*. Computación Aplicada al Desarrollo SA de CV. Adelfa 213-A, Villa de las Flores, León Guanajuato. Recuperado de: http://www.cad.com.mx/que_es_internet.htm

⁸ Club Planeta. *Historia del Internet*. Computación Aplicada al Desarrollo SA de CV. Adelfa 213-A, Villa de las Flores, León Guanajuato. Recuperado de: http://www.cad.com.mx/historia_del_internet.htm

ARPANET siguió creciendo y abriéndose al mundo, y cualquier persona con fines académicos o de investigación podía tener acceso a la red.

Las funciones militares se desligaron de ARPANET y fueron a parar a MILNET, una nueva red creada por los Estados Unidos.

La NSF (National Science Foundation) crea su propia red informática llamada NSFNET, que más tarde absorbe a ARPANET, creando así una red con propósitos científicos y académicos.

El desarrollo de las redes fue abismal, y se crean nuevas redes de libre acceso que más tarde se unen a NSFNET, formando el embrión de lo que hoy conocemos como INTERNET.

En 1985 la Internet ya era una tecnología establecida, aunque conocida por unos pocos. El desarrollo de NSFNET fue tal que hacia el año 1990 ya contaba con alrededor de 100.000 servidores.

En el Centro Europeo de Investigaciones Nucleares (CERN), Tim Berners Lee dirigía la búsqueda de un sistema de almacenamiento y recuperación de datos. Berners Lee retomó la idea de Ted Nelson (un proyecto llamado "Xanadú") de usar hipervínculos. Robert Caillau quien cooperó con el proyecto, cuenta que en 1990 deciden ponerle un nombre al sistema y lo llamarón World Wide Web (WWW) o telaraña mundial.

La nueva fórmula permitía vincular información en forma lógica y a través de las redes. El contenido se programaba en un lenguaje de hipertexto con "etiquetas" que asignaban una función a cada parte del contenido. Luego, un programa de computación, un intérprete, eran capaz de leer esas etiquetas para

desplegar la información. Ese intérprete sería conocido como "navegador" o "browser".

En 1993 Marc Andreessen produjo la primera versión del navegador "Mosaic", que permitió acceder con mayor naturalidad a la WWW.

La interfaz gráfica iba más allá de lo previsto y la facilidad con la que podía manejarse el programa abrió la red a los legos. Poco después Andreessen encabezó la creación del programa Netscape. A partir de entonces Internet comenzó a crecer más rápido que otro medio de comunicación, convirtiéndose en lo que hoy todos conocemos.

Algunos de los servicios disponibles en Internet aparte de la WEB son el acceso remoto a otras máquinas (SSH y telnet), transferencia de archivos (FTP), correo electrónico (SMTP), conversaciones en línea (IMSN MESSENGER, ICQ, YIM, AOL, jabber), transmisión de archivos (P2P, P2M, descarga directa), etc.

5.1.3.2. Ventajas y Desventajas del Internet⁹

La evolución del Internet ha crecido enormemente y hoy en día hay mucha gente que utiliza este gran medio, especialmente las nuevas generaciones que han nacido con esto, y en el futuro será esencial y no se podrá detener su crecimiento continuo por todo el mundo.

El Internet ha hecho que muchas cosas se mejoren, pero de igual forma ha contribuido a que las personas tengan más acceso a todo tipo de información,

⁹Bautista, D. (18 de Febrero de 2013) *Ventajas y desventajas del Internet*. Taringa. Recuperado de: <http://www.taringa.net/post/info/16403479/Ventajas-y-desventajas-del-Internet.html>

incluyendo la personal, empresarial, documental, financiera y hasta privada e inapropiada.

Por todo lo anterior, se enumerarán algunas ventajas y desventajas del Internet:

5.1.3.2.1. Ventajas

- *Es la fuente de información más grande que haya existido en de todo el mundo. En Internet hay muchísima información, todo lo que se pueda preguntar simplemente se escribe en Google (o en cualquier otro motor de búsqueda) y en menos de un segundo se obtendrán miles de respuestas la cual es la mayor ventaja de todas.*
- *Nos ofrece varias redes sociales como Facebook, Twitter o MySpace, entre otras, las cuales permiten siempre estar conectados con el resto del mundo.*
- *Podemos estar en contacto con todas las personas que queremos todo el tiempo mediante el uso del mail, redes sociales, etcétera.*
- *Internet nos brinda una variedad de juegos online de diferentes tipos; pero se recuerda que hay que hacerlo moderadamente porque se puede crear una adicción.*
- *Podemos participar de Internet creándonos algún sitio web y/o participando en sitios web escribiendo nuestra opinión sobre algún tema en general o específico.*

- *Internet nos ofrece la posibilidad de ganar dinero online por diferentes medios.*
- *Internet nos da la posibilidad de estar todo el tiempo informados porque nos brinda noticias de último momento.*
- *Internet nos permite ver videos online. Esto anteriormente era algo impensable ya que no existía la globalización de la información.*
- *Una gran ventaja de Internet es que si no entendemos un texto que está en otro idioma simplemente lo colocamos en algún traductor y nos efectúa la tarea.*

5.1.3.2.2. Desventajas

- *Hay muchas personas que se crean perfiles falsos en las redes sociales. Por eso, en Facebook por ejemplo, hay que saber cómo identificarlos. Es complicado, pero no es imposible detectarlos. Esta es una clara desventaja de Internet. También, hay que saber por qué las personas se crean perfiles falsos en Facebook. Menciono a Facebook y no a Twitter por ejemplo porque en la primera red social hay más riesgos que pueden surgir.*
- *Hay mucha gente que coloca información falsa en Internet para confundir a los lectores. Hay que tener cuidado con este tipo de información porque hay que saber si la fuente es confiable. Esta es otra gran desventaja de Internet.*

- *Hay una posibilidad de que nos volvamos dependientes de Internet, es decir, que nos veamos obligados a entrar muy seguido para ver actualizaciones de algo en especial, por ejemplo, saber si alguien nos “twitteó”. Todo en exceso es malo.*
- *Las personas empiezan a pensar más superficialmente cuando leen algo en Internet porque no se especifican en lo que están leyendo, simplemente leen ideas básicas y no se enfocan en estudiar más lo leído porque con ello ya están satisfechos.*
- *Internet puede resultar muy inseguro ya que nos pueden robar datos, por ejemplo cuando utilizamos Facebook sin privacidad, o cuando alguien se infiltra en nuestro ordenador. Esta es quizá la peor desventaja.*
- *En Internet hay muchísimo uso del spam, y esto puede generar inconvenientes en una persona utilizando la web, porque por ejemplo aquel usuario puede hacer clic en alguna ventana emergente y le puede infectar la computadora con malware.*
- *En Internet hay que tener cuidado con las Páginas Web en las que entramos porque puede haber malware que se dirija a nuestras computadoras. Esta es otra clara desventaja.*

5.1.3.3. Internet y la Educación¹⁰

La Internet es utilizada por millones de personas diariamente. Entre ellas hay no sólo profesores, investigadores y estudiantes universitarios o empresas y particulares, sino también maestros y alumnos de primaria y secundaria (que la usan individual y colectivamente), autoridades educativas, etc.

Algunas de las áreas en las que puede utilizarse la Internet en educación son:

- **La Internet en la clase**

Cada día más escuelas están conectadas a la Internet. Lo profesores y los alumnos utilizan esta conexión al mundo de diversas formas. En primer lugar, la Internet es una fuente inagotable de información y datos de primera mano. Como red originariamente científica, en la Internet puede encontrarse gran cantidad de información útil para la clase, desde imágenes de satélites meteorológicos recién tomadas a documentos históricos pasando por conjuntos de datos sobre ecología o el último 'paper' no publicado todavía sobre física.

Estudiantes de clases distantes físicamente utilizan la red como medio de comunicación para realizar proyectos colectivos, recoger e intercambiar datos sobre aspectos diferentes de su medio ambiente o estudiar las diferencias y semejanzas culturales entre comunidades de diferentes países. En un 'revival' sorprendente, una especie de "Freinet electrónico" se apodera de las aulas conectadas a la red: los estudiantes se enzarzan en

¹⁰ Adell, J. *Educación en la Internet*. serie IV. Extraordinari XX Setmana Pedagógica (ISSN 0211-3368), págs. 207-214. Publicado en: Universitat de Tarragona. Recuperado de: <http://nti.uji.es/docs/nti/tarragona.html>

correspondencias escolares electrónicas y multi-mediáticas con compañeros de la otra parte del mundo.

- **La Internet y la administración educativa**

La administración educativa produce, difunde y consume una enorme cantidad de información. Es más, el creciente flujo de información entre los centros docentes y entre estos y la administración podría beneficiarse de la rapidez y reducción de costes que supone su transmisión digital por la red.

Uno de los aspectos en los que se están realizando experiencias, es en la informatización y gestión descentralizada de los expedientes de los alumnos.

Algunas instituciones han comenzado a difundir por la Internet todo tipo de documentos y materiales sobre educación. Un ejemplo de este uso puede verse en el servidor WWW del Departamento de Educación de los EE.UU. (el equivalente a nuestro Ministerio de Educación y Ciencia).

Las ventajas respecto a los canales de distribución tradicionales pueden resumirse en una mayor rapidez a menor coste y en la posibilidad de gestionar grandes cantidades de información con las facilidades de la informática (bases de datos, por ejemplo). A medida que aumente el número de centros docentes conectados y de maestros y alumnos usuarios habituales, este tipo de canales de distribución sustituirán a los actualmente dominantes. El coste de la duplicación y envío por correo.

5.1.3.4. La Internet en el desarrollo profesional del docente

Uno de los principales problemas en la formación continua del profesorado es su dispersión geográfica y el consiguiente aislamiento. Los centros de profesores, la formación de grupos de trabajo, los centros de recursos, etc. son iniciativas que intentan introducir dinámicas de comunicación y formación continua a través del intercambio de experiencias. Un medio de comunicación como la Internet puede utilizarse provechosamente para interconectar dicha población dispersa, minimizando los gastos de desplazamiento. Iniciativas de este tipo, en las que los maestros pueden intercambiar información y experiencias, consultar a expertos o acceder a grandes cantidades de materiales curriculares, se están realizando ya en los países en los que la cultura de la red está más desarrollada.

5.1.4. Seguridad Informática

Se entiende por **seguridad informática** al conjunto de elementos, que tienen como objetivo garantizar la confidencialidad, integridad, disponibilidad y buen uso de la información que reside en un sistema de información. La seguridad informática surge como el área que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta en una organización (incluyendo los datos contenidos, material informático y programas), existiendo para ello una serie de estándares, protocolos, métodos, reglas, normas, procedimientos, herramientas, aspectos éticos y legales, concebidos para minimizar los posibles riesgos a la infraestructura o a la información. Igualmente la seguridad informática comprende tanto software, bases de datos, metadatos, archivos, como todo lo que se considere o valore activo y signifique un riesgo si ésta llega a manos inescrupulosas; siendo este tipo de información privilegiada y/o confidencial.

Asimismo, la seguridad informática busca confirmar que los recursos de los sistemas de información, sean utilizados de la mejor manera y que el acceso o modificación de la misma, sólo sea posible a través de las personas idóneas, que se encuentran acreditadas y dentro de los permisos y límites de su autorización, primando ante todo su ética profesional; de ahí que las nuevas tecnologías de seguridad se presenten como un elemento indispensable para visualizar, controlar y gestionar de forma eficiente todos los recursos que se utilizan.

Por todo lo anterior, en estos momentos la seguridad informática se debe considerar como un tema de dominio obligado por cualquier persona que hace uso de Internet, todo con el fin de no permitir que la información sea expuesta y comprometida.

5.1.4.1. Principios de Seguridad Informática¹¹

Para lograr sus objetivos la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

Confidencialidad: *Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.*

¹¹ Ríos, J. Monografía. Seguridad Informática. Recuperado de: <http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml>

Integridad: *Se refiere a la validez y consistencia de los elementos de información almacenados y procesador en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios , computadores y procesos comparten la misma información.*

Disponibilidad: *Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deber reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente.*

5.1.4.2. Factores de Riesgo¹²

Ambientales/Físicos: *Factores externos, lluvias, inundaciones, terremotos, tormentas, rayos, humedad, calor entre otros.*

Tecnológicos: *Fallas de hardware y/o software, fallas en el aire acondicionado, falla en el servicio eléctrico, ataque por virus informático, etc.*

¹² Ríos, J. Monografía. Seguridad Informática. Recuperado de: <http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml>

Humanos: hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, alteraciones etc.

5.1.4.3. Elementos Vulnerables¹³

*Los 3 elementos principales a proteger en cualquier sistema informático son el **Hardware**, el **Software** y los **Datos**.*

*Por **Hardware** se entiende el conjunto de todos los elementos físicos de un sistema informático como CPU, terminales, cableados, medios de almacenamiento secundarios, tarjeta de red, etc... **Software** se le llama al conjunto de programas lógicos que hacen funcionar tanto el hardware, sistemas operativos, como aplicaciones, y por último los **Datos** que se entienden como el conjunto de información lógica.*

5.1.5. Delitos Informáticos¹⁴

El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos.

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos

¹³ Navarro Martín, S. Seguridad Informática SMR. Tema 1: Seguridad Informática. Wiki sobre Seguridad Informática. Segundo curso de Sistemas Microinformáticos y Redes. Recuperado de: <http://seguridadinformaticasmr.wikispaces.com/TEMA+1+-+SEGURIDAD+IFORM%C3%81TICA>

¹⁴ Recovery Labs. Delitos Informáticos. Computer Forensic. Departamento de Peritaje Informático. España. Recuperado de: http://www.delitosinformaticos.info/delitos_informaticos/definicion.html

consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que, según éstos se trata de los mismos delitos, cometidos a través de otros medios.

Partiendo de esta compleja situación y tomando como referencia el “Convenio de Ciber-delincuencia del Consejo de Europa”, se puede definir los delitos informáticos como:

“Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos”.

5.1.5.1. Características Principales de los Delitos Informáticos

- Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
- Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.
- Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.

5.1.5.2. Tipos de Delitos Informáticos reconocidos por la ONU

Clasificación según la Actividad Informática

DELITO	CARACTERISTICAS
Fraudes cometidos mediante manipulación de computadoras.	
Manipulación de los datos de entrada	Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
La manipulación de programas	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
Manipulación de los datos de salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
Fraude efectuado por manipulación informática	aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Figura 6. *Fraudes cometidos mediante Manipulación de Computadoras*

Fuente: El Rincón del Vago. *Delitos Informáticos*. Recuperado de:

http://html.rincondelvago.com/delitos-informaticos_1.html

Falsificaciones informáticas.	
Como objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada.
Como instrumentos	Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Figura 7. *Falsificaciones Informáticas*

Fuente: El Rincón del Vago. *Delitos Informáticos*. Recuperado de:

http://html.rincondelvago.com/delitos-informaticos_1.html

Daños o modificaciones de programas o datos computarizados.	
Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.
Acceso no autorizado a servicios y sistemas informáticos	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
Piratas informáticos o hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
Reproducción no autorizada de programas informáticos de protección legal	Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un <i>delito informático</i> debido a que el bien jurídico a tutelar es la propiedad intelectual.

Figura 8. *Daños o Modificaciones de Programas o Datos Computarizados*

Fuente: El Rincón del Vago. *Delitos Informáticos*. Recuperado de:

http://html.rincondelvago.com/delitos-informaticos_1.html

5.1.5.3. Tipos de Amenazas y Ataques Informáticos

Los diferentes tipos de ataques existentes, pueden ser realizados sobre cualquier tipo de red o sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica; los Insiders (operadores, programadores) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando un password válida. A través de los años se han desarrollado formas cada vez más sofisticadas de ataques para explotar "agujeros" en el diseño, configuración y operación de los sistemas.

Dentro de las amenazas y ataques más conocidos, se tienen:

- Ingeniería Social | Ingeniería Social Inversa
- Ataque de Monitorización | Autenticación | Contraseñas
- Phishing
- Malwares
- Grayware
- Escaneo de Puertos
- Wardialers
- Código Malicioso
- Control Remoto de Equipos
- Eavesdropping
- VLAN hopping
- STP manipulation
- Man-in-the-middle
- Defacement
- IP Spoofing | MAC Address Spoofing
- Repetición de Transacción
- Backdoors
- DHCP Starvation
- Trashing (Cartoneo)
- Denegación de Servicio (DoS) | Denegación de Servicio Distribuida
- Fraude Informático
- Software ilegal
- Acceso a Información Confidencial Impresa
- Daños Físicos al Equipamiento

5.1.5.4. Técnicas de Seguridad Informática

Una vez conocidas las vulnerabilidades y ataques a las que podrá estar expuesto un sistema informático o de información, es necesario conocer los recursos disponibles para protegerlo.

Muchas de las vulnerabilidades existentes son el resultado de implementaciones incorrectas de tecnologías, otras son consecuencias de la falta de planeamiento de las mismas, pero la mayoría de los agujeros de seguridad son ocasionados por los usuarios de dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

Por todo lo anterior, existen técnicas de seguridad informática que buscan implementar y mantener cualquier sistema seguro; siendo conscientes que ninguna de las técnicas a mencionar, representan el 100% de la seguridad deseada, aunque muchas parezcan ser la solución, será la suma de algunas de ellas las que convertirán un sistema en confiable.

Dentro de las técnicas de seguridad más conocidos, se tienen:

- Firewalls (Cortafuegos)
- Wrappers
- Detección de Intrusos en Tiempo Real
- Sistemas Anti-Sniffers
- Gestión de Contraseñas seguras
- Seguridad en Protocolos y Servicios
- Criptografía
- Backups de datos
- Acceso físico (Keyloggers, Sniffers, Escritorio remoto, Backdoors)
- Seguridad en Internet (Redes Sociales, Correo Electrónico, Mensajería Instantánea, etc.)
- Antivirus
- Actualizaciones y Parches de Seguridad
- Capacitación
- Uso de Software Legal o de Software Libre (GNU/Linux)

5.1.6. Software Libre

Es aquel programa o conjunto de ellos de los que el usuario puede disponer del código fuente sin restricciones, y el cual puede modificar y redistribuir también sin limitaciones. Estas libertades garantizadas al usuario del software (o a aquel que lo recibe), no son contrarias a los derechos legítimos del autor del programa, es decir, éste no tiene por qué perder sus derechos sobre el mismo.

De una manera más precisa, el Software Libre se refiere a cuatro libertades de los usuarios del software¹⁵:

1. **Libertad 0** / *La libertad de usar el programa, con cualquier propósito.*
2. **Libertad 1** / *La libertad de estudiar cómo funciona el programa y modificarlo, adaptándolo a las propias necesidades.*
3. **Libertad 2** / *La libertad de distribuir copias del programa, con lo cual se puede ayudar a otros usuario.*
4. **Libertad 3** / *La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie.*

Las libertades 1 y 3 requieren acceso al código fuente, porque estudiar y modificar el software sin su código es muy poco viable.

¹⁵ HispaLinux. Hacia la sociedad del conocimiento libre. *¿Qué es el Software Libre?*. Recuperado de: <http://hispalinux.es/SoftwareLibre>

5.1.6.1. Tipos de Licencias de Software Libre¹⁶

Una licencia es aquella autorización formal con carácter contractual que un autor de un software da a un interesado para ejercer "actos de explotación legales". Pueden existir tantas licencias como acuerdos concretos se den entre el autor y el licenciataria. Desde el punto de vista del software libre, existen distintas variantes del concepto o grupos de licencias:

- ✓ **Licencias GPL** | Licencia Pública General de GNU (GNU GPL).
- ✓ **Licencias AGPL** | Licencia Pública General de Affero (Affero General Public License, también Affero GPL o AGPL)
- ✓ **Licencias Estilo BSD** | Licencia utilizada en gran cantidad de software distribuido junto a los sistemas operativos BSD.
- ✓ **Licencias Estilo MPL y derivadas** | La MPL es Software Libre y promueve eficazmente la colaboración.
- ✓ **Licencia Copyleft**

¹⁶ Wikipedia. La enciclopedia libre. *Software Libre*. Modificada por última vez el 13 de marzo de 2015. Recuperado de: http://es.wikipedia.org/wiki/Software_libre

5.1.6.2. Ventajas del Software Libre en la Seguridad

El uso de Software Libre deriva una serie de ventajas, algunas de las cuales están relacionadas directamente con la seguridad. A saber¹⁷:

- *Al disponer del código fuente de los programas en su totalidad, éste puede ser analizado por terceras personas ajenas a sus autores en busca de fallos de diseño o de implementación; es decir, cualquiera con los conocimientos necesarios puede realizar una auditoría del código del programa.*
- *La posibilidad de realizar modificaciones libremente al código fuente y distribuirlos permite que cualquiera pueda ofrecer mejoras sobre éste. Estas mejoras podrán ser nuevas funcionalidades que se incorporen al mismo o parches que corrijan problemas detectados anteriormente.*
- *Las características del software libre hacen que no sea lógico que tengan un costo, lo que permite que este tipo de software pueda ser utilizado por organizaciones y personas con menos recursos económicos. El software libre pone en manos de cualquier persona, el tipo de tecnología que, hoy por hoy, sólo podían tener grandes organizaciones.*
- *De igual forma, la posibilidad de modificar libremente el software permite a las organizaciones que lo adapten a sus propias necesidades, pudiendo eliminar funcionalidades que no le sean de interés. En el mundo de la seguridad existe la máxima de “lo más sencillo es más seguro” por ello poder eliminar funciones innecesarias de las herramientas las puede convertir de forma inmediata en más seguras (porque no podrán ser utilizadas estas funcionalidades para subvertirlas).*

¹⁷ Ferrer, J., & Fernández-Sanguino, J. *Seguridad informática y Software Libre*. Estructura de Hispalinux. Recuperado de: <http://es.tldp.org/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf>

5.1.6.3. Desventajas del Software Libre

El uso de software libre no está exento de desventajas. Así se podrían enumerar las siguientes¹⁸:

- *La posibilidad de una generación más fácil de troyanos, dado que el código fuente también puede ser modificado con intenciones maliciosas. Si el troyano logra confundirse con la versión original puede haber problemas graves. La fuente del programa, en realidad, será el método de distribución de software, que, de no ser seguro, permitirá que un tercer agente lo manipule. La distribución de software se asegura añadiendo posibilidad de firmado de hashes de la información distribuida.*
- *El método de generación de software libre suele seguir, en la mayoría de los casos, el modelo bazar, es decir, muchas personas trabajan sobre partes concretas e integrando sus cambios o personas desde el exterior contribuyen mejoras al proyecto global. Esto puede dar lugar a que se realice una mala gestión del código fuente del software por no seguir métodos formales de seguimiento, la consecuencia final es que falten piezas clave (que nadie ha contribuido) como es el caso de la documentación.*
- *Al no tener un respaldo directo, la evolución futura de los componentes software no está asegurada o se hace demasiado despacio.*

Por todo lo anterior, si bien el software libre en la actualidad tiene una cobertura desigual de las distintas necesidades de seguridad de una empresa o institución, éste es, definitivamente, una apuesta de futuro provechosa en aquellas áreas aún no desarrolladas y

¹⁸ Ferrer, J., & Fernández-Sanguino, J. *Seguridad informática y Software Libre*. Estructura de Hispalinux. Recuperado de: <http://es.tldp.org/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf>

una oportunidad real e inmediata en las demás áreas para utilizar soluciones equivalentes a las propietarias con:

- ✓ Menor coste.
- ✓ Mayores garantías de seguridad, por la posibilidad de auditar el código.
- ✓ Mayor flexibilidad (adaptación e integración), por la posibilidad de modificar su código.

5.2. MARCO CONTEXTUAL

El presente Proyecto de Investigación se enmarca y desarrolla en el siguiente contexto geográfico:

Para poner en contexto, los Puntos Vive Digital, son espacios que garantizan el acceso a las Tecnologías de la Información y las Comunicaciones (TIC), con el fin de contribuir a la reducción de la pobreza y a minimizar la brecha digital de los colombianos; iniciativa que hace parte del Programa VIVE DIGITAL del Ministerio TIC, liderada por el programa social Compartel.

El Ministerio TIC desde su programa social Compartel instaló hasta el año 2014, 800 Puntos Vive Digital en todo el país, pero en la actualidad es un proyecto que aún sigue creciendo.

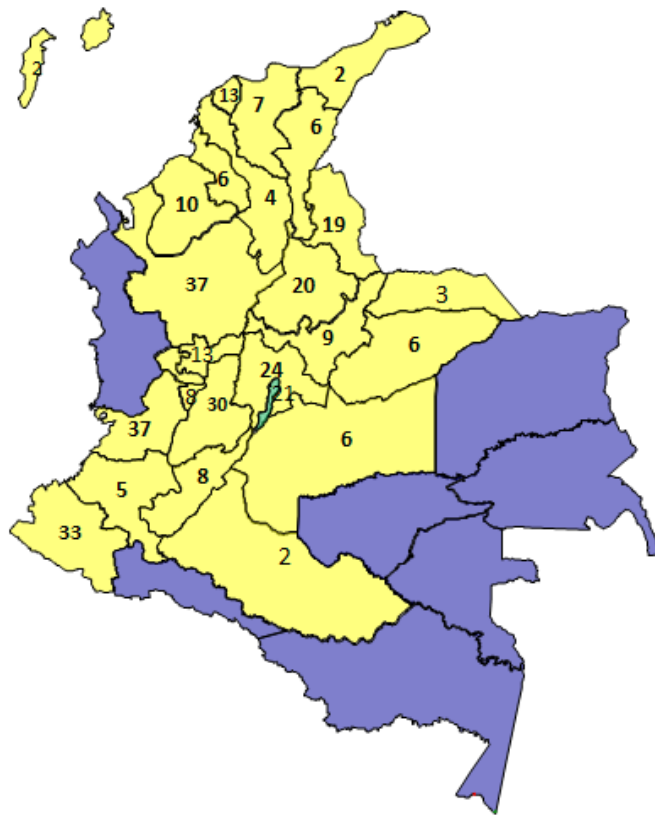
Dentro de los múltiples servicios que presta un Punto Vive Digital, con equipos de última tecnología, están:

- **Acceso a Internet:** Niños, jóvenes y adultos podrán explorar el mundo, acortar distancias, ahorrar tiempo, y mucho más accediendo a Internet.

- **Sala de capacitaciones:** La comunidad podrá participar en diferentes procesos de formación para el aprovechamiento y uso productivo de las TIC.
- **Actividades de entretenimiento y cultura:** Lo más innovador en materia de entretenimiento y otras actividades culturales estarán al alcance de todos.
- **Trámites y servicios de Gobierno en línea:** El Estado colombiano estará a un solo clic a través de los diferentes trámites y servicios que ofrece Gobierno en Línea.
- **Servicios complementarios** de acuerdo a las necesidades de la comunidad.

De acuerdo a la distribución de los PVD (Puntos Vive Digital) implementados según los resultados de la convocatoria pública de PVD en su fase 1, en donde se solicitaron **896** Puntos Vive Digital para **556** municipios de Colombia, aplicando la metodología de escogencia de los Puntos Vive Digital basada en criterios de equidad, maximización de usuarios beneficiados y haciendo especial énfasis en los municipios que tuvieran conectividad de Fibra Óptica y/o que estuvieran dentro del proyecto nacional de Fibra Óptica Nacional; se logró así una sinergia entre los proyectos para optimizar el uso de los bienes y servicios a desarrollar.

Como resultado, se obtuvo que de las 896 solicitudes de PVD, fueron seleccionados 341 PVD asignados en 25 departamentos comprendidos en 245 municipios, de la siguiente manera:



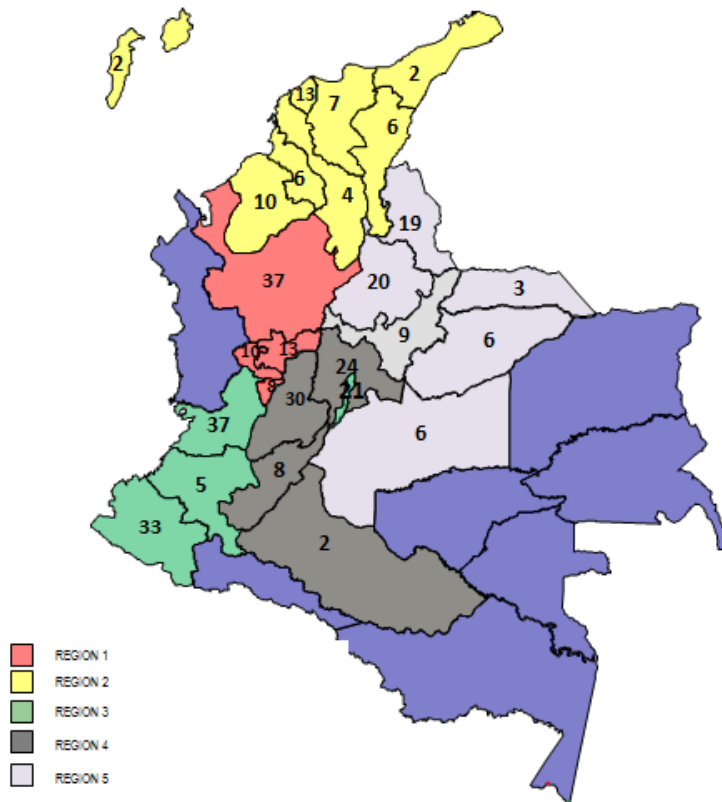
DEPARTAMENTO	No. MUNICIPIO	No.PVD
ANTIOQUIA	36	37
ARAUCA	3	3
ATLANTICO	8	13
BOLIVAR	2	4
BOYACA	6	9
CALDAS	11	13
CAQUETA	1	2
CASANARE	4	6
CAUCA	3	5
CESAR	1	6
CORDOBA	7	10
CUNDINAMARCA	25	45
HUILA	5	8
LA GUAJIRA	1	2
MAGDALENA	4	7
META	4	6
NARIÑO	30	33
NORTE DE SANTANDER	18	19
QUINDIO	5	8
RISARALDA	7	10
SAN ANDRES	2	2
SANTANDER	14	20
SUCRE	6	6
TOLIMA	27	30
VALLE DEL CAUCA	15	37
TOTAL PVD	245	341

Figura 9. PVD (Puntos Vive Digital) asignados

Fuente: FONADE, Fondo Financiero de Proyectos de Desarrollo. (Abril de 2013). *Dotación, Instalación y puesta en funcionamiento de la Infraestructura técnica de los Puntos Vive Digital Fase 1.* Bogotá D.C. Recuperado de:

http://www.fonade.gov.co/Contratos/Documentos/3767__2013041910380819%20ANEXO%20No%202-%20DOC%20TECNICO%20PROVEEDOR%20FASE%201.pdf

La distribución de los departamentos se hará en 5 regiones donde se detallan a continuación, así como el número total de Puntos Vive Digital por cada región:



REGION	DEPARTAMENTO	No. MUNICIPIO	No. PVD
1	ANTIOQUIA	36	37
	CALDAS	11	13
	QUINDIO	5	8
	RISARALDA	7	10
TOTAL		59	68
2	ATLANTICO	8	13
	BOLIVAR	2	4
	CESAR	1	6
	CORDOBA	7	10
	LA GUAJIRA	1	2
	MAGDALENA	4	7
	SAN ANDRES	2	2
SUCRE	6	6	
TOTAL		31	50
3	CAUCA	3	5
	NARIÑO	30	33
	VALLE DEL CAUCA	15	37
TOTAL		48	75
4	CAQUETA	1	2
	CUNDINAMARCA	25	45
	HUILA	5	8
	TOLIMA	27	30
TOTAL		58	85
5	NORTE DE SANTANDER	18	19
	SANTANDER	14	20
	ARAUCA	3	3
	BOYACA	6	9
	CASANARE	4	6
META	4	6	
TOTAL		49	63
TOTAL PVD ASIGNADOS		245	341

Figura 10. Regionalización de los PVD (Puntos Vive Digital) asignados

Fuente: FONADE, Fondo Financiero de Proyectos de Desarrollo. (Abril de 2013). *Dotación, Instalación y puesta en funcionamiento de la Infraestructura técnica de los Puntos Vive Digital Fase 1.* Bogotá D.C. Recuperado de:

http://www.fonade.gov.co/Contratos/Documentos/3767__2013041910380819%20ANEXO%20No%202-%20DOC%20TECNICO%20PROVEEDOR%20FASE%201.pdf

Adicional a lo anterior, El Ministerio TIC con el ánimo de llegar a más municipios en el país asignará 231 nuevos PVD en 20 departamentos, de la siguiente manera:

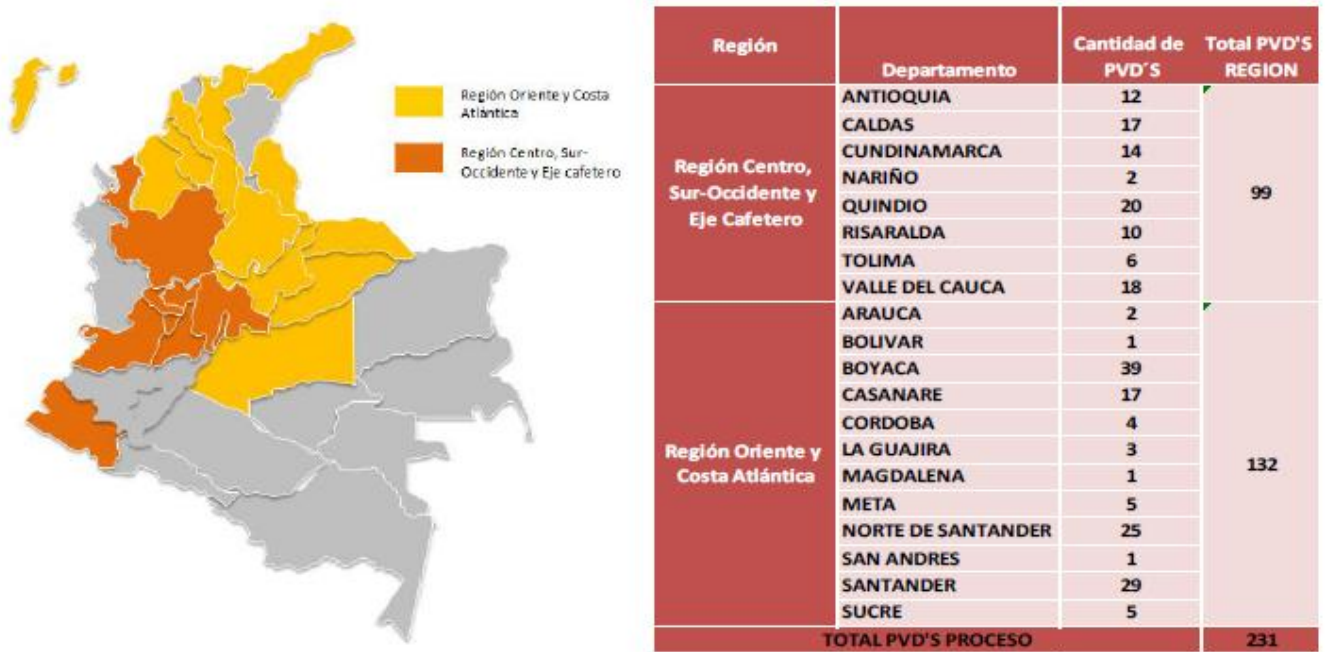


Figura 11. Nuevos PVD (Puntos Vive Digital) asignados

Fuente: FONADE, Fondo Financiero de Proyectos de Desarrollo. (Junio de 2014). *Dotación, Instalación y puesta en funcionamiento de la Infraestructura técnica de los Puntos Vive Digital Fase 1 en una segunda Etapa.* Bogotá D.C. Recuperado de:

http://www.fonade.gov.co/Contratos/Documentos/4382__2014062006500208%20DOCUMENTO%20TECNICO%20PROVEEDOR%20FASE%201.pdf

Ahora bien, partiendo de la distribución y regionalización del Programa Vive Digital por parte del Ministerio TIC en todo el territorio Colombiano; el presente Proyecto de Investigación se enmarca y desarrolla en el **Departamento de Risaralda**, específicamente en el **Municipio de Dosquebradas**, tal y como se evidencia en la siguiente figura con el listado de los *Puntos Vive Digital* en cada uno de los municipios beneficiados:

LISTADO DE PUNTOS VIVE DIGITAL BENEFICIADOS

REGION	DANE MUNICIPIO	DEPARTAMENTO	MUNICIPIO	TIPOLOGIA	CANTIDAD
1	66075	RISARALDA	BALBOA	D	1
	66088	RISARALDA	BELEN DE UMBRIA	D	1
	66170	RISARALDA	DOSQUEBRADAS	D	1
	66383	RISARALDA	LA CELIA	C	1
	66001	RISARALDA	PEREIRA	C	1
	66001	RISARALDA	PEREIRA	C	1
	66001	RISARALDA	PEREIRA	B	1
	66001	RISARALDA	PEREIRA	A	1
	66400	RISARALDA	LA VIRGINIA	A	1
	66682	RISARALDA	SANTA ROSA DE CABAL	B	1

Figura 12. Listado de PVD (Puntos Vive Digital) Beneficiados en Risaralda

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones. *Listado de Puntos Vive Digital Beneficiados*. Recuperado de: http://www.mintic.gov.co/portal/vivedigital/612/articulos-4312_recurso_1.pdf

Como se mencionó a lo largo del documento, el presente Proyecto de Investigación se desarrollará en base a **1 de los 7 Kioscos Vive Digital** que hacen parte del Punto Vive Digital instalado en el municipio de Dosquebradas, ubicado exactamente en la Diagonal 23A # 21T- 31, Barrio La Pradera, y cuya información de interés se muestra en la siguiente figura.

DEPARTAMENTO	MUNICIPIO	OPERADOR	DATOS ATENCION	DATOS CONTACTO
RISARALDA	Dosquebradas	EMTEL	<p>Dirección Diagonal 23 21T - 31</p> <p>Horario de Atención 8 am a 12 pm 2 pm a 6 pm</p>	<p>Nombre de Contacto MONICA ANDREA LOAIZA GUTIERREZ - WILLIAN DE JESUS LOPEZ</p> <p>Telefono de contacto 3302371-3205933224 - 311-3897385</p> <p>Correo personal o el utilizado para Facebook monika2010_loaiza@hotmail.com vivewilly@hotmail.com</p>

Figura 13. *Servicio de Puntos Vive Digital*

Fuente: Gobierno en Línea. *Tu punto de acceso oficial a la información, trámites y servicios del Estado Colombiano*. Servicio de Puntos Vive Digital. Recuperado de: <https://www.gobiernoenlinea.gov.co/web/guest/puntos-vive-digital>

Las 7 sedes educativas beneficiadas con Kioscos Vive Digital en el municipio de Dosquebradas (Risaralda), tuvieron dentro de sus requisitos para su escogencia, las siguientes pautas:

- Estar ubicada en centros poblados reconocidos por el DANE con una población mayor o igual que 100 habitantes.
- El centro poblado no podrá tener un sitio de acceso público a Internet.
- Comprometerse a abrir al público en general, como mínimo 20 horas a la semana (incluyendo fines de semana), inclusive en los periodos de vacaciones.
- Garantizar el servicio de energía eléctrica, durante el periodo de servicio del KVD.
- No contar con servicio de Internet en la sede.

Por lo anterior, se presenta el listado de las 7 sedes del Municipio de Dosquebradas, beneficiadas con KVD, resaltando aquella Institución Educativa objeto del presente Proyecto de Investigación:

A	B	C	D	E	F	G
CONTRATISTA	DEPARTAMENTO	MUNICIPIO	DIRECCION SEDE	ESTABLECIMIENTO EDUCATIVO	NOMBRE SEDE	NOMBRE GESTOR
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA LAS HORTENCIAS	I.E.	LAS HORTENCIAS	N/A
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA NUEVA INDEPENDENCIA	I.E.	NUEVA INDEPENDENCIA	DIANA PAOLA OSORIO CIFUENTES
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA LA PALMA	I.E. EDUARDO CORREA URIBE	LA PALMA	MAITER YEIN GARCIA ARBELAEZ
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA AGUAZUL	I.E BOQUERON	BOQUERONCITO	YENNY TATIANA RAMIREZ VALENCIA
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA LA RIVERA	I.E. CARTAGENA	LA RIVERA	BEATRIZ ELENA ALZATE VANEGAS
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA BUENA VISTA	I.E. ENRIQUE MILLAN RUBIO	ENRIQUE MILLAN RUBIO	YAMILET CUSTODIA CARDONA LOPEZ
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA NARANJALES	I.E FABIO VASQUEZ BOTERO	NARANJALES	JULIANA DUQUE HENAO

Figura 14. Listado de KVD (Kioscos Vive Digital) en Dosquebradas

Fuente: Autoría Propia

Como información complementaria, los Kioscos son liderados por miembros de la misma comunidad, personas comprometidas con capacidad de comunicación y convocatoria que contribuyen desde sus competencias al progreso de sus comunidades. Estos líderes son conocidos como **Gestores Locales** de los Kioscos y están encargados de garantizar el óptimo funcionamiento de los equipos y la capacitación de las personas respecto al uso y apropiación de las TIC. Para lograr esta meta, los Gestores contarán con asesoría y acompañamiento por parte de la Institución Universitaria ESCOLME, aliado de la UT NEC de Colombia S.A. – Hispasat S.A. para el componente de Apropiación del Proyecto Kioscos Vive Digital, relacionado con los procesos de sensibilización y cultura digital, capacitación en alfabetización TIC y cursos Especializados desarrollados a partir de los intereses de las poblaciones, todo con el fin de promover y difundir los logros sociales y casos de éxito que se generen en el día a día en cada uno de estos kioscos.

Retomando la figura anterior con el listado de KVD (Kioscos Vive Digital) beneficiados en el Municipio de Dosquebradas, se muestra resaltada la **Institución Educativa Eduardo Correa Uribe** objeto de estudio del presente Proyecto de Investigación y de la cual se presenta la siguiente información relevante:

5.2.1. Institución Educativa Eduardo Correa Uribe

5.2.1.1. Generalidades

El establecimiento Educativo Eduardo Correa Uribe, comenzó a funcionar a partir de 1930; fue conformado como Asociación mediante resolución N° 701 del 1° de octubre de 2003, asociada técnica, administrativa y financieramente con los centros de: Miralindo, la Palma; Nueva Independencia, las Hortensias, Argentina y Chaquiro.

En febrero del año de 2004 la Secretaria de Educación nombra a la Licenciada Magda Córdoba Mosquera como Directora de la Institución, la cual ofrecía hasta grado noveno (9°), y en el año 2006, se gradúan los primeros bachilleres, ya que fue reconocida como Institución Educativa Eduardo Correa Uribe mediante resolución 224 de Marzo 14 de 2005.

5.2.1.2. Reseña Histórica de la Sede Educativa Eduardo Correa Uribe

El señor Juan Bautista Molina, dueño de grandes extensiones de tierra, donó una cuadra de terreno para la construcción de la escuela. En este terreno existía un palo de aguacate inmenso, el cual fue derrumbado por diez familias habitantes del sector, y así adecuaron el terreno para la edificación. Después de trasladados los materiales de construcción a lomo de mula, fue levantada la primera escuela del sector, la comunidad de la vereda la fría, como se conocía en aquella época, comenzó a estudiar la posibilidad de contratar una maestra para iniciar labores, ya que no fue posible por nombramiento oficial.

Al paso de los de los años, la población fue aumentando y llegaron a la escuela otros profesores: Rosario Mejía, Teresa Delgado, Ana Félix Ocampo, y se

recuerda muy especialmente a la señora Rosa María Sepúlveda, quien enseñó durante 17 años. En el año de 1930 la escuela fue oficializada con el nombre de Escuela la Fría, en razón a la vereda.

En el período comprendido entre 1930 y 1966, se destacan personajes como: Hernán Rendón, quien trabajó por la electrificación que hoy disfruta la vereda; Eduardo Correa a quien se le debe gran parte del progreso de la comunidad, por hacer posible la apertura de la carretera, y los profesores Zulia Marín, Nidia Ospina, Helena López y Alicia Marulanda, quienes lucharon por la creación de las plazas docentes de este centro educativo. También se recuerda el estanquillo la Fría, situado al frente de la escuela, por lo cual esta se empezó a llamar “*Escuela Estanquillo La Fría*”, aunque oficialmente su nombre era “Escuela La Fría”. En el año 1967, la señora Gladis de Vélez se empeñó en la construcción de una nueva escuela. Organizó actividades en compañía de los integrantes de la junta de acción comunal y profesores, logrando su propósito con la vinculación del Comité de Cafeteros, el ICCE y el Departamento; así construyeron la escuela que hoy se posee.

Siendo Gobernador Mario Jiménez Correa, sobrino de Eduardo Correa Uribe, las profesoras Ana Marina Duque y Mariela Cuartas, solicitaron por medio de un oficio sustentado, con firmas de miembros de la comunidad, que se cambiara el nombre de “*Escuela La Fría*”, por el de “*Escuela Eduardo Correa Uribe*”, en memoria y reconocimiento a quien hizo tanto bien, no solo a la vereda, sino también al sector educativo. El 12 de Mayo de 1973 se colocó la placa con el respectivo nombre; la cual fue bendecida por Monseñor Baltasar Álvarez Restrepo, obispo de la ciudad de Pereira.

5.2.1.3. Misión

La Institución Educativa Eduardo Correa Uribe, brinda a su comunidad los ciclos de preescolar primaria, básica secundaria y media académica haciendo uso del modelo pedagógico escuela activa en sus estrategias metodológicas “Escuela Nueva”, post-primaria rural con metodología Escuela Nueva, SAT y CAFAM; desarrolla planes y estrategias educativas, visibiliza proyectos pedagógicos, construye proyectos de formación integral favoreciendo el aprendizaje en los estudiantes, a la vez promueve los valores humanos como la tolerancia, el respeto, la laboriosidad, la identidad y la espiritualidad vinculando la infancia y la juventud a una cultura de sostenibilidad mediante proyectos productivos que proponen por el mejoramiento de la calidad de vida de los egresado y sus familias.

5.2.1.4. Visión

La Institución Educativa Eduardo Correa Uribe, ofrecerá la educación pre-escolar, básica y media, desarrollará el modelo pedagógico Escuela Activa que responderá a las necesidades educativas de su sector de influencia, tomando para ello los aportes de las estrategias “Escuela Nueva” SAT y CAFAM, post-primaria rural con metodología “Escuela Nueva”. Asumirá la educación por competencias garantizando la formación de personas responsables, respetuosas, tolerantes, laboriosas, espirituales con identidad y con capacidad para proponer y ejecutar proyectos productivos y de desarrollo social y humano.

5.2.1.5. Ubicación Geográfica y Características

Las veredas que conforman el sector de influencia de la Institución, tuvieron como pobladores a colonos llegados de los departamentos de Antioquia, el viejo Caldas y el norte del Valle.

Entre los iniciadores o fundadores de estas veredas, se encuentran: Inés Cuervo y Carlos Benítez de la vereda el Estanquillo; Dagoberto Pineda, Pedro Narváez y Rafael Quirama de la vereda la Palma; Don Gustavo Osorio y Bernardo Osorio de la vereda la Nueva Independencia; Don Emiro Montoya, José Antonio Villegas de la vereda las Hortensias y Mercedes Martínez y María de Jesús Montoya de la vereda la Fría, la Argentina y el Chaquiro.

La gran mayoría de los habitantes de esta Asociación son todos trabajadores, hospitalarios, de buenas costumbres y en su mayoría católicos, dedicados a la agricultura. Las mujeres son dedicadas al hogar, a los oficios católicos y a la crianza de sus hijos; las relaciones son buenas y se manifiestan a través del buen trato entre los mismos.





Figura 15. *Ubicación Geográfica Municipio de Dosquebradas – Risaralda*
Fuente: Wikipedia. La enciclopedia libre. *Dosquebradas*. Modificada por última vez el 11 de marzo de 2015. Recuperado de: <http://es.wikipedia.org/wiki/Dosquebradas>

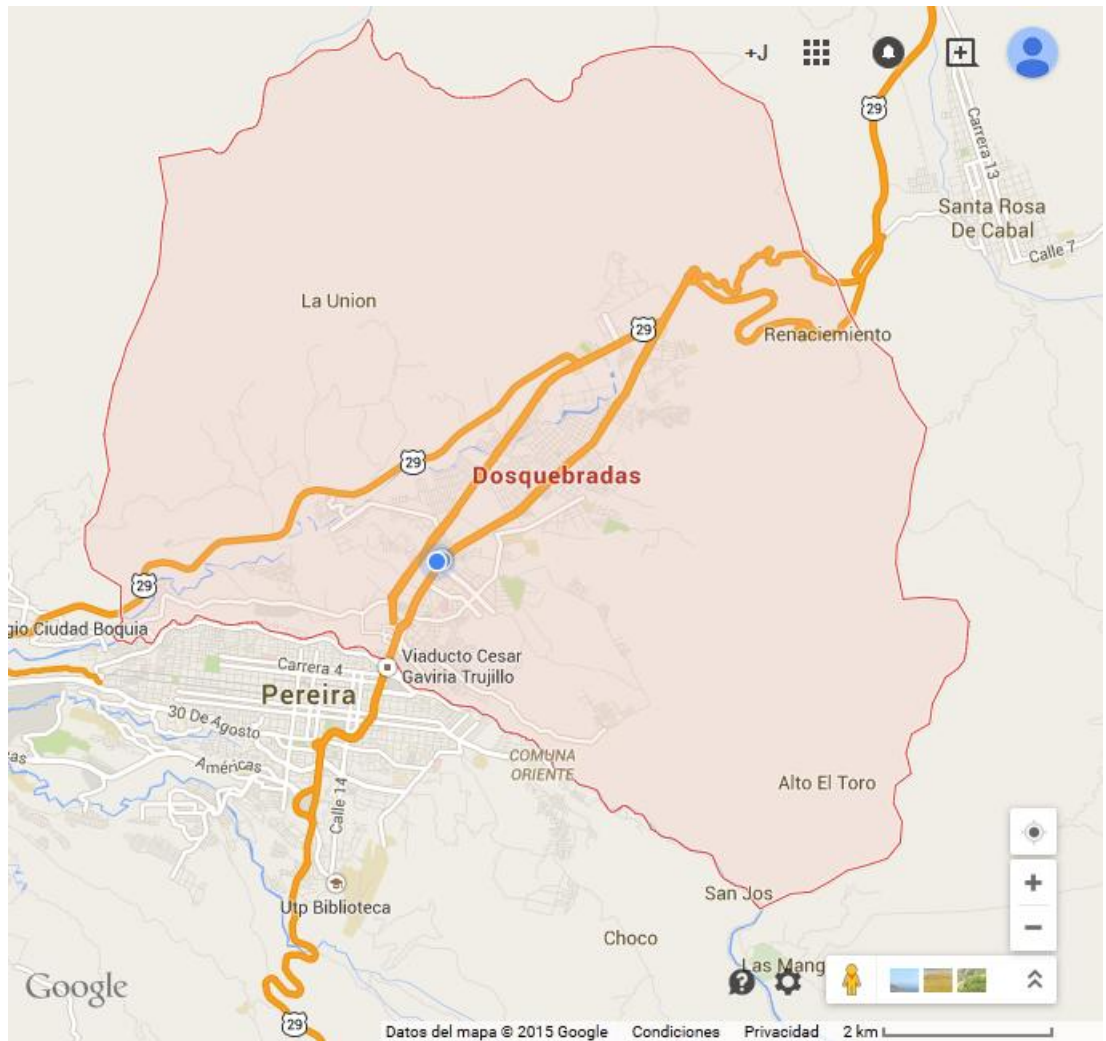


Figura 16. *Mapa Municipio de Dosquebradas – Risaralda*

Fuente: Google. Maps. (2015). *Dosquebradas, Risaralda, Colombia*. Modo Básico.

Recuperado de:

<https://www.google.com/maps/place/Dosquebradas,+Risaralda,+Colombia/@4.838985,-75.671235,13z/data=!3m1!4b1!4m2!3m1!1s0x8e3880c45cd78303:0xeb0625cf082593fe>

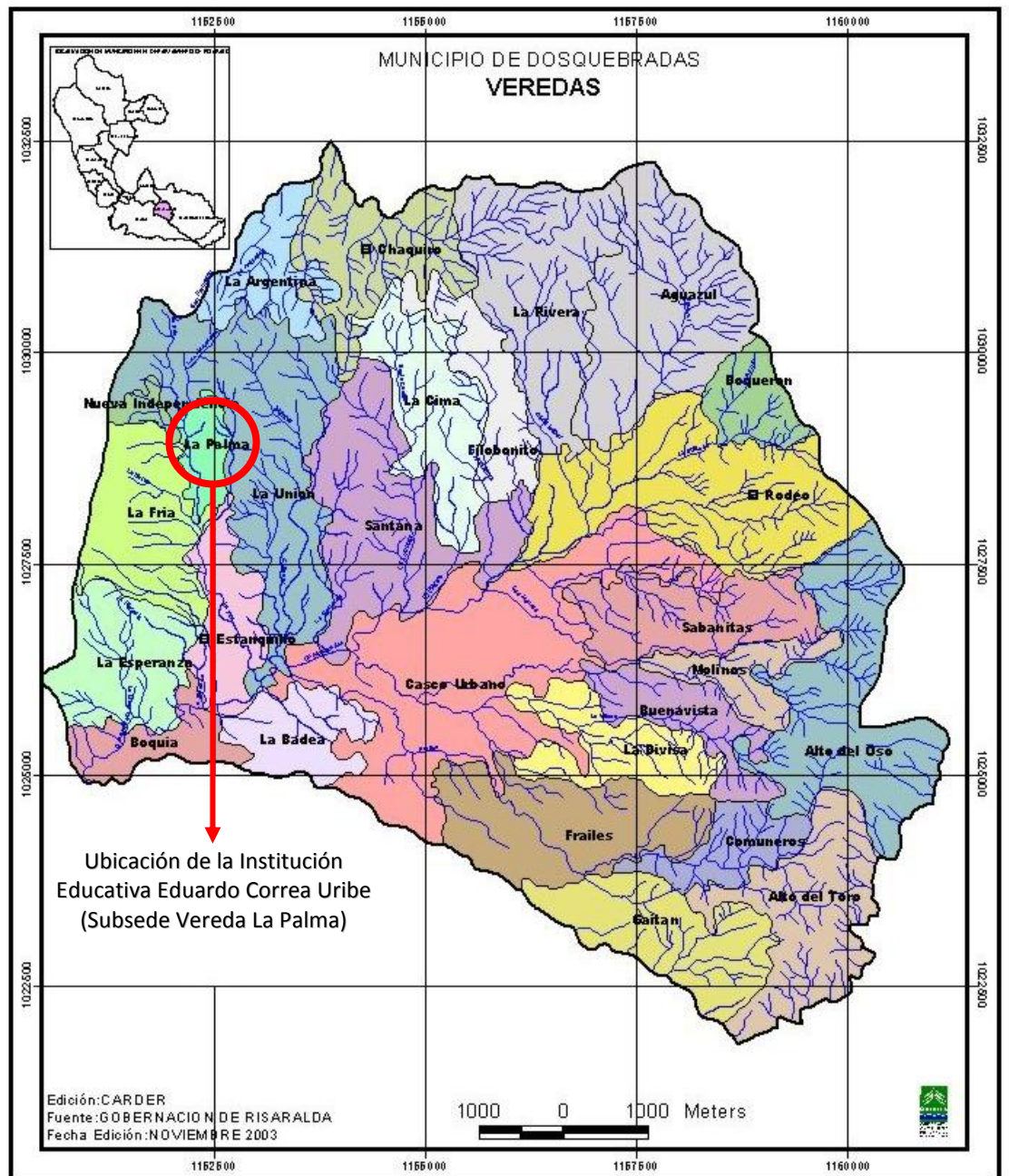


Figura 17. Mapa de las Veredas en el Municipio de Dosquebradas – Risaralda
Fuente: CARDER, Corporación Autónoma Regional de Risaralda. (Julio 04 de 2013).
Mapas del Departamento de Risaralda. Mapa de las Veredas Dosquebradas. Documento.
Recuperado de: <http://www.carder.gov.co/intradocuments/webExplorer/mapas-del-departamento-de-r-da-0/page:4>

5.2.1.6. Aspectos Físicos

Con respecto a la cabecera municipal, la vereda las Hortensias que es la más distante de la Asociación, tiene aproximadamente 18 Km. y su altura está en un promedio de 1.550 mts a 2.200 mts sobre el nivel del mar.

El clima oscila entre 17° a 25° C, su mayor altura es el alto del nudo, su topografía es semi-quebrada.

Los límites de la Asociación son los siguientes:

Norte: Veredas la Argentina, el Chaquiro y partes de Santa Ana alta.

Sur: Avenida del pollo y Vereda la Esperanza.

Occidente: Vereda Minas del Socorro (Municipio de Pereira) alto del Nudo de Marsella y la reserva natural del nudo.

Oriente: Vereda la Unión.

5.2.1.7. Procedencia de los Alumnos

La mayoría de los estudiantes que asisten a la Institución Eduardo Correa Uribe, pertenecen a las diferentes veredas que la conforman y son hijos de agregados de otras partes.

5.2.1.8. Vías de Acceso

Por carretera, saliendo del Municipio de Dosquebradas o por Pereira y se realiza a través de los recorridos pasando por las veredas la Fría, la nueva Independencia, las Hortensias, ó por Santa Ana baja, Santa Ana alta, el Chaquiro.

El transporte lo presta la empresa transportes Dosquebradas y transportes florida con horario promedio de dos horas entre turnos.

Los suelos son francos arcillados, franco arenosos, con buen grado de fertilidad y vegetación.

Dentro de la Institución Eduardo Correa Uribe se encuentra la reserva natural el Alto el Nudo que en la actualidad es administrada por la CARDER y sitio turístico destinado por la alcaldía municipal.

5.2.1.9. Sede Principal Vereda El Estanquillo

Nombre de la Institución:	Eduardo Correa Uribe
Dirección:	Vereda el Estanquillo
Municipio:	Dosquebradas
Departamento:	Risaralda
Niveles:	Pre-escolar Primaria Secundaria
Programa:	Escuela nueva Post-primaria SAT
Jornadas:	Mañana Tarde Sábados
Naturaleza:	Oficial
Calendario:	A
Núcleo:	4
Propietario:	El Municipio
Directora:	Magda Córdoba Mosquera
Identificación Dane Sede:	26617000085401
Año de fundación:	1930

5.2.1.10. Subsede Vereda La Palma

Nombre de la Institución:	Eduardo Correa Uribe
Dirección:	Vereda la palma
Municipio:	Dosquebradas
Departamento:	Risaralda
Niveles:	Primaria
Programas:	Escuela Nueva
Jornadas:	Mañana
Naturaleza:	Oficial
Calendario:	A
Núcleo:	4
Propietario:	El Municipio
Directora:	Maury Edelmira Bedoya Poloche
Identificación Dane Sede:	26617000087102
Año de fundación:	1972

6. HIPÓTESIS

Como posible solución se plantea la siguiente hipótesis:

De no implementarse Políticas de Seguridad a través de Herramientas de Software libre como medidas informáticas para prevenir la afectación de los equipos y proteger la estabilidad de los usuarios por el mal uso del Internet, en las Instituciones Educativas Públicas beneficiadas con el Programa Vive Digital, éstas serán vulnerables a posibles daños parciales o totales en la infraestructura de los activos que les han sido asignados, teniendo un impacto directo en los recursos financieros de las instituciones, así como también en los posibles riesgos para la integridad de las personas, afectando en general la continuidad del programa.

7. METODOLOGÍA DE LA INVESTIGACIÓN

7.1. Población o Universo

Este Proyecto de Investigación se realizó tomando como población o universo, los 7 Kioscos Vive Digital instalados en las diferentes Instituciones Educativas Públicas de las veredas del Municipio de Dosquebradas, Departamento de Risaralda, beneficiadas con el Programa VIVE DIGITAL.

El siguiente es el listado de las 7 veredas de Dosquebradas, beneficiadas con KVD:

A	B	C	D	E	F	G
CONTRATISTA	DEPARTAMENT	MUNICIPIO	DIRECCION SEDE	ESTABLECIMIENTO EDUCATI	NOMBRE SEDE	NOMBRE GESTOR
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA LAS HORTENCIAS	I.E.	LAS HORTENCIAS	N/A
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA NUEVA INDEPENDENCIA	I.E.	NUEVA INDEPENDENCIA	DIANA PAOLA OSORIO CIFUENTES
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA LA PALMA	I.E. EDUARDO CORREA URIBE	LA PALMA	MAITER YEIN GARCIA ARBELAEZ
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA AGUAZUL	I.E. BOQUERON	BOQUERONCITO	YENNY TATIANA RAMIREZ VALENCIA
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA LA RIVERA	I.E. CARTAGENA	LA RIVERA	BEATRIZ ELENA ALZATE VANEGAS
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA BUENA VISTA	I.E. ENRIQUE MILLAN RUBIO	ENRIQUE MILLAN RUBIO	YAMILET CUSTODIA CARDONA LOPEZ
U.T NEC-HISPASAT	RISARALDA	DOSQUEBRADAS	VEREDA NARANJALES	I.E FABIO VASQUEZ BOTERO	NARANJALES	JULIANA DUQUE HENAO

Figura 18. Veredas beneficiadas con los Kioscos Vive Digital (KVD) en Dosquebradas
Fuente: Autoría propia

Partiendo de los datos suministrados por el DANE (Departamento Administrativo Nacional de Estadística) y proyectados con base en el Censo de 2005; para el año 2015 la Población total de las 7 Veredas (Las Hortensias, Nueva Independencia, La Palma, Aguazul, La Rivera, Buena Vista y Naranjales) beneficiadas con los 7 Kioscos Vive Digital instalados en las respectivas Instituciones Educativas Públicas del Municipio de Dosquebradas (Risaralda) es de **1663** personas, dentro de un rango de edades entre los Cero (0) años y más de Ochenta (80) años, tal y como se evidencia en las siguientes dos figuras:

edades entre los Cinco (5) y Sesenta y Cuatro (64) años, obteniendo un total de **1396** personas, cifra que se sustenta a partir de la siguiente imagen:

Total de la Población por Rango de Edades (5 a 64)
Veredas Municipio Dosquebradas

198874

RANGOS DE EDADES	TOTAL MUNICIPIO	POBLACION CENTRO POBLADO	LA RIVERA	BUENAVISTA	NARANJALES	LAS HORTENSIAS	LA PALMA	LA NUEVA INDEPENDENCIA	AGUAZUL	
			448	318	251	122	195	103	227	
5 - 9	15282	7.68%	34	24	19	9	15	8	17	
10-14	15868	7.98%	36	25	20	10	16	8	18	
15-19	17096	8.60%	39	27	22	10	17	9	20	
20-24	18132	9.12%	41	29	23	11	18	9	21	
25-29	16085	8.09%	36	26	20	10	16	8	18	
30-34	14915	7.50%	34	24	19	9	15	8	17	
35-39	13231	6.65%	30	21	17	8	13	7	15	
40-44	11676	5.87%	26	19	15	7	11	6	13	
45-49	12805	6.44%	29	20	16	8	13	7	15	
50-54	12449	6.26%	28	20	16	8	12	6	14	
55-59	10734	5.40%	24	17	14	7	11	6	12	
60-64	8619	4.33%	19	14	11	5	8	4	10	
Total			376	267	210	102	164	86	191	1396

Figura 21. Total Población de las Veredas con KVD / Rango de Edades (5 a 64)

Fuente: Autoría propia

En resumen, para este Proyecto de Investigación se tomó como Población o Universo, un total de **1396** personas, entre los Cinco (5) y Sesenta y Cuatro (64) años de edad, pertenecientes a los 7 Kioscos Vive Digital instalados en las diferentes Instituciones Educativas Públicas de las veredas del Municipio de Dosquebradas (Risaralda) beneficiadas con el Programa VIVE DIGITAL direccionado por el Gobierno Nacional; tal y como se muestra en la siguiente figura:

RANGOS DE EDADES	LA RIVERA	BUENAVISTA	NARANJALES	LAS HORTENSIAS	LA PALMA	LA NUEVA INDEPENDENCIA	AGUAZUL	
5 - 9	34	24	19	9	15	8	17	
10-14	36	25	20	10	16	8	18	
15-19	39	27	22	10	17	9	20	
20-24	41	29	23	11	18	9	21	
25-29	36	26	20	10	16	8	18	
30-34	34	24	19	9	15	8	17	
35-39	30	21	17	8	13	7	15	
40-44	26	19	15	7	11	6	13	
45-49	29	20	16	8	13	7	15	
50-54	28	20	16	8	12	6	14	
55-59	24	17	14	7	11	6	12	
60-64	19	14	11	5	8	4	10	
Total	376	267	210	102	164	86	191	1396

Figura 22. Población o Universo | Rango de Edades (5 a 64)
Fuente: Autoría propia

7.2. Muestra

Para dar cumplimiento al primer objetivo específico de este Proyecto de Investigación, el cual consistía en determinar el nivel actual de seguridad con el uso de internet en las Instituciones Educativas Públicas del Municipio de Dosquebradas beneficiadas con el Programa **VIVE DIGITAL**; se aplicó un **Muestreo Aleatorio Simple** a la Población o Universo, previamente definida (**1396** personas), obteniéndose una **muestra** de **227** personas.

Como se mencionó anteriormente, la muestra de **227** personas, se obtuvo mediante la **Fórmula de Muestreo Aleatorio Simple para una población Finita**

$$n = \frac{Z^2_{\alpha} \cdot N \cdot p \cdot q}{e^2(N-1) + Z^2_{\alpha} \cdot p \cdot q}$$

Figura 23. Fórmula de Muestreo Aleatorio Simple para población finita
Fuente: Autoría propia

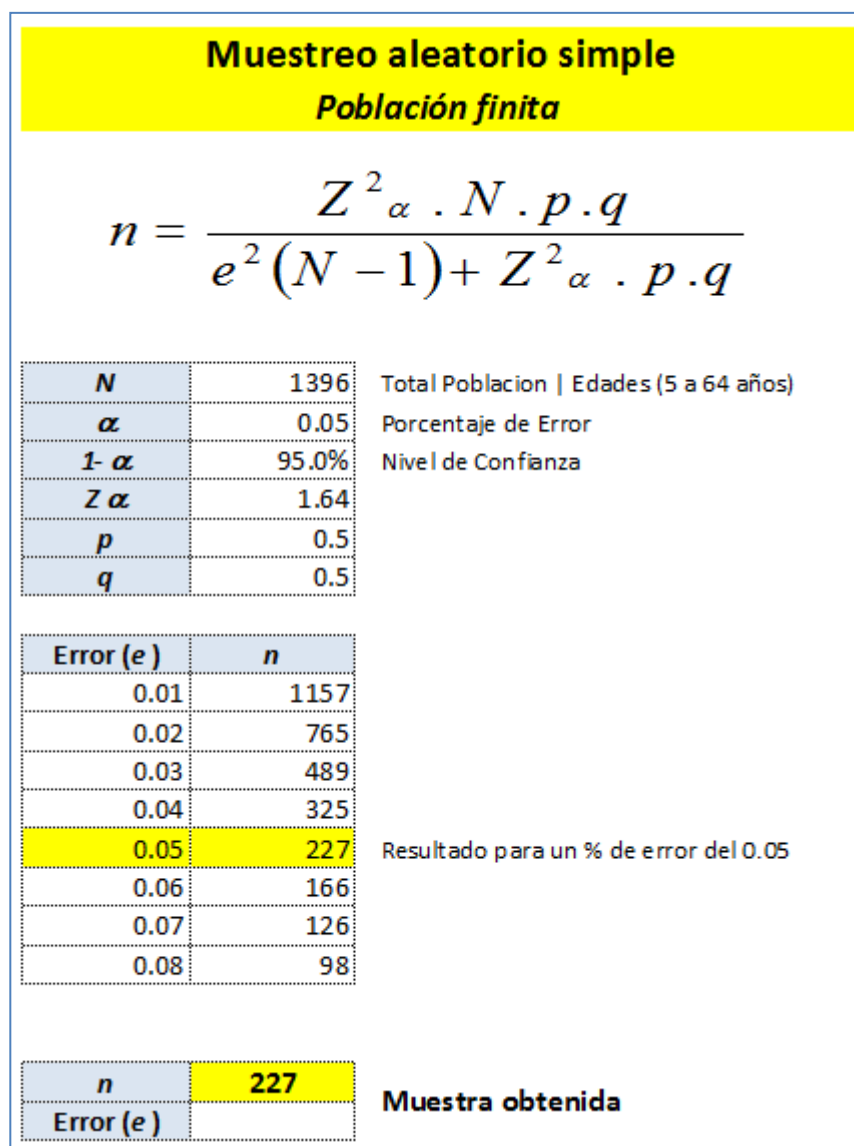


Figura 24. Resultado Formula Muestreo Aleatorio Simple (Población finita)

Fuente: Autoría propia

En base al muestreo obtenido de **227** personas, se procedió a conocer el número de población equivalente en cada una de las 7 veredas del Municipio de Dosquebradas (Risaralda) beneficiadas con el Programa VIVE DIGITAL, de acuerdo al total de la población de cada una de ellas en el rango de edades entre los Cinco (5) y Sesenta y Cuatro (64) años, utilizando para ello la *Regla de Tres*.

VEREDAS	LA RIVERA	BUENAVISTA	NARANJALES	LAS HORTENSIAS	LA PALMA	LA NUEVA INDEPENDENCIA	AGUAZUL	TOTAL	MUESTREO
Total Población por Vereda (Edades 5 a 64)	376	267	210	102	164	86	191	1396	227
Porcentaje (%) de Población en base al total (1396)	27	19	15	7	12	6	14	100 %	
Muestreo de Población x Vereda en base al total (227)	61	43	34	17	27	14	31	227	

Figura 25. *Muestreo de Población x Vereda con KVD*

Fuente: Autoría propia

VEREDA	Muestreo x Vereda
LA RIVERA	61
BUENAVISTA	43
NARANJALES	34
LAS HORTENSIAS	17
LA PALMA	27
LA NUEVA INDEPENDENCIA	14
AGUAZUL	31
Total Muestreo	227

Figura 26. *Consolidado de Muestreo de Población x Vereda con KVD*

Fuente: Autoría propia

7.3. Delimitación del Estudio

- **Tipo de Investigación:** Proyecto basado en Investigación, que buscó unir la investigación con la práctica a través de la aplicación.
- **Tipo de Estudio:** Cualitativo.

7.4. Variables e Indicadores

De conformidad con la hipótesis seleccionada y los objetivos definidos, las siguientes son las variables e indicadores del estudio utilizados:

Variable: Información CLAVE a ser recolectada y procesada.

Indicador: Forma en que se precisa la variable para obtener la información deseada a través de los Instrumentos o técnicas de recolección de información.

Tabla 1. Variables e Indicadores

OBJETIVOS ESPECÍFICO	VARIABLES	DEFINICIÓN DE LA VARIABLE	INDICADORES
Determinar el nivel actual de seguridad con el uso de internet en las Instituciones Educativas Públicas del Municipio de Dosquebradas beneficiadas con el Programa VIVE DIGITAL.	Nivel de Vulnerabilidad Informática	Errores y problemas en la configuración del hardware o software de los equipos de cómputo usados para Internet.	Diagnóstico realizado sobre la vulnerabilidad de los equipos de cómputo.
Definir las Herramientas de Software Libre que puedan ser implementadas en las Instituciones Educativas Públicas para prevenir el mal uso del Internet.	Herramientas Evaluadas	Posibles herramientas de software libre que pueden aplicarse para reducir el nivel de vulnerabilidad en los equipos de cómputo.	Comparativo de Herramientas de Software Libre evaluadas.
Realizar una propuesta de implementación de Herramientas de Software Libre como medida de Seguridad Informática para las Instituciones Educativas Públicas del Municipio de Dosquebradas.	Propuestas de Intervención	Conjunto de acciones a establecer como medida de Seguridad Informática.	Procedimientos, modelos y propuesta.
Implementar la Herramienta de Software Libre como medida de Seguridad Informática propuesta en la Institución Educativa Eduardo Correa Uribe - Sede La Palma del Municipio de Dosquebradas Risaralda, como prueba piloto para ser aplicado posteriormente en otras Instituciones Educativas Públicas beneficiadas con el Programa VIVE DIGITAL.	Informe de Implementación	Resultados implementación de la herramienta en la Institución Educativa.	Informe sobre la aplicación de la herramienta de Software Libre.

Fuente: Autoría propia

7.5. Métodos e Instrumentos de Recolección de Información

La información requerida para dar cumplimiento a los objetivos del Proyecto de investigación, se recolectó a través de los siguientes medios:

Información primaria

- ✓ Encuestas a docentes, estudiantes, administrativos y comunidad de los 7 Kioscos Vive Digital instalados en las Instituciones Educativas Públicas del Municipio de Dosquebradas, beneficiadas con el Programa VIVE DIGITAL, con el objetivo de evaluar la seguridad en el uso de Internet en estos mismos Kioscos.

- ✓ Lista de Chequeo por parte del encargado del Kiosco Vive Digital de la Institución Educativa Eduardo Correa Uribe – Sede la Palma Dosquebradas, con el objetivo de conocer el nivel de seguridad de la infraestructura (Hardware - Software) del Programa VIVE DIGITAL en la Institución Educativa en mención.

7.6. Procesamiento y análisis de la información

7.6.1. Encuesta

Para la realización de la *Encuesta* a los docentes, estudiantes, administrativos y comunidad de los 7 Kioscos Vive Digital instalados en las Instituciones Educativas Públicas del Municipio de Dosquebradas, beneficiadas con el Programa VIVE DIGITAL, se partió de la muestra de 227 personas, previamente obtenida mediante la Fórmula de Muestreo Aleatorio Simple para una población finita, aplicada en el rango de edades entre los Cinco (5) y Sesenta y Cuatro (64) años.

De acuerdo a los datos obtenidos, se presenta el siguiente análisis de la información de cada uno de los ítems de la encuesta:

DATOS GENERALES

7.6.1.1. Kiosco Encuestado

Seleccione el Kiosco Vive Digital al cual visita.

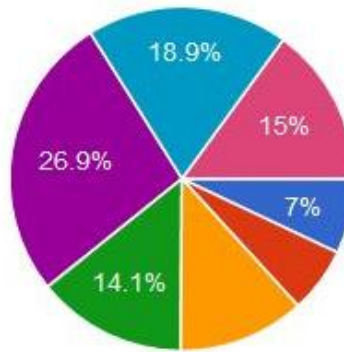


Figura 27. Encuesta / Kiosco Encuestado

Fuente: Autoría propia

Instituto Educativo Vereda las Hortencias	16	7%
Instituto Educativo Vereda Nueva Independencia	14	6.2%
Instituto Educativo Vereda La Palma	27	11.9%
Instituto Educativo Vereda Agua Azul	32	14.1%
Instituto Educativo Vereda La Rivera	61	26.9%
Instituto Educativo Vereda Buena Vista	43	18.9%
Instituto Educativo Vereda Naranjales	34	15%

Según los datos obtenidos en el primer ítem sobre el Kiosco Vive Digital al cual visita, se confirma el número de encuestas aplicadas según el muestreo de población de cada una de las **7 Veredas** beneficiadas con el Kiosco Vive Digital, previamente obtenido mediante Muestreo Aleatorio Simple para una población finita de 1396 personas en el rango de edades entre los Cinco (5) y Sesenta y Cuatro (64) años, sumando entre todas un total de 227 encuestas cubriendo el 100% de la Población o Universo.

7.6.1.2. Género

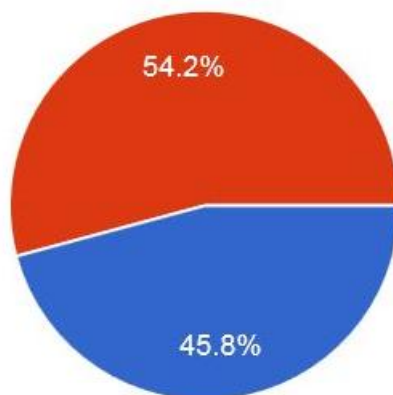


Figura 28. Encuesta / Género

Fuente: Autoría propia

Masculino	104	45.8%
Femenino	123	54.2%

Según el resultado de este ítem, se confirma que el mayor porcentaje de las personas encuestadas de las 7 Veredas beneficiadas con el Kiosco Vive Digital en el Municipio de Dosquebradas (Risaralda), pertenecen al género **Femenino**, con un total de 123 personas equivalente al 54.2%, comparado con el género **Masculino**, el cual obtuvo un total de 104 personas, correspondiente al 45.8%, sumando entre todos un total de 227 encuestas cubriendo el 100% del Muestreo Aleatorio Simple.

7.6.1.3. Edad

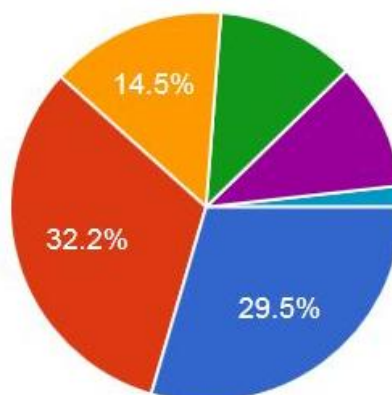


Figura 29. Encuesta / Edad

Fuente: Autoría propia

Entre 5 y 14	67	29.5%
Entre 15 y 24	73	32.2%
Entre 25 y 34	33	14.5%
Entre 35 y 44	26	11.5%
Entre 45 y 54	24	10.6%
Entre 55 y 64	4	1.8%

De acuerdo al rango de Edades encuestadas que hacen uso de Internet en los diferentes Kioscos Vive Digital en el Municipio de Dosquebradas, se evidencia que el mayor número de personas a las cuales se les aplicó el cuestionario, pertenecen al grupo entre **15 y 24** años con un total de 73 encuestas, correspondiente al 32.2%, seguido del rango de edades entre **5 y 14** años, sumando 67 encuestas que equivalen al 29.5%; como tercer grupo con mayor número de encuestados, se encuentran los pertenecientes al rango entre los **25 y 34** años, con un total de 33 encuestas correspondiente al 14.5%. Dentro de los últimos tres rangos de edades, se evidencian las del grupo entre **35 y 44** años con un total de 26 encuestas y un porcentaje de 11.5%, continuando con el rango entre **45 y 54** años que suman 24 encuestas equivalentes al 10.6% y por último el grupo de **55 a 64** años con un total muy bajo de 4 encuestas equivalentes al 1.8%.

7.6.1.4. Grupo al que pertenece

Seleccione a qué grupo pertenece:

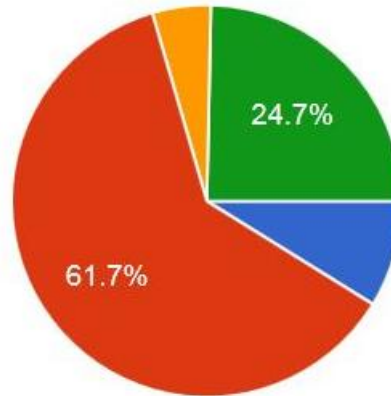


Figura 30. Encuesta / Grupo al que pertenece
Fuente: Autoría propia

Docente	20	8.8%
Estudiante	140	61.7%
Administrativo	11	4.8%
Comunidad	56	24.7%

En base al resultado obtenido en cuanto al grupo que se pertenece, la opción de **Estudiante** ocupa el mayor porcentaje con un valor de 61.7%, representados en 140 personas, lo que evidencia que más de la mitad de los encuestados del Muestreo pertenecen a este grupo, los cuales hacen uso de Internet en los diferentes Kioscos Vive Digital de las 7 Veredas beneficiadas en el Municipio de Dosquebradas (Risaralda). Como segundo grupo, se encuentra la opción de **Comunidad**, con un total de 56 personas, equivalentes al 24.7%, casi la cuarta parte del total de los encuestados, seguidos de la opción **Docente**, con un valor de 20 encuestados, correspondientes al 8.8%, y por último se encuentra el grupo **Administrativo**, con un pequeño porcentaje de 4.8%, equivalente a 11 personas, sumando entre todos un total de 227 encuestas cubriendo el 100% de la Muestra.

DATOS DE OPINIÓN

7.6.1.5. Acompañamiento

Responder esta pregunta solamente en el caso de ser Estudiante: Cuando utiliza Internet desde los computadores del Kiosco Vive Digital, ¿Se hace en presencia de un adulto o docente que lo supervise?

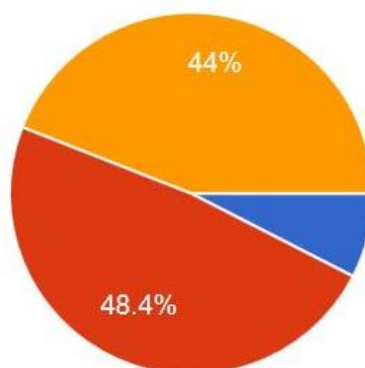


Figura 31. Encuesta / Acompañamiento

Fuente: Autoría propia

Si	12	7.5%
No	77	48.4%
A veces	70	44%

Según los datos obtenidos en base al cuestionamiento anterior, en el caso de pertenecer al grupo *Estudiante*, se evidencia que el alto porcentaje de 48.4% de los encuestados, reflejados en un total de 77 estudiantes, *No* utilizan el Internet bajo la supervisión de un adulto o docente, en ninguno de los diferentes Kioscos Vive Digital de las 7 Veredas en el Municipio de Dosquebradas. De igual forma, el otro gran porcentaje de 44%, equivalente a 70 estudiantes, manifiestan que *A veces* hacen uso del Internet en presencia de un adulto o docente, y por último el 7.5%, de este mismo grupo de encuestados, representados en 12 estudiantes, revelan que *Si* utilizan el Internet en presencia de un adulto o docente que lo supervise; demostrándose de esta forma la gran libertad a la hora de acceder y consultar contenido en Internet sin ningún acompañamiento.

7.6.1.6. Actividades

Si utiliza Internet desde los computadores del Kiosco Vive Digital, señale
¿Cuáles de estas actividades realiza?

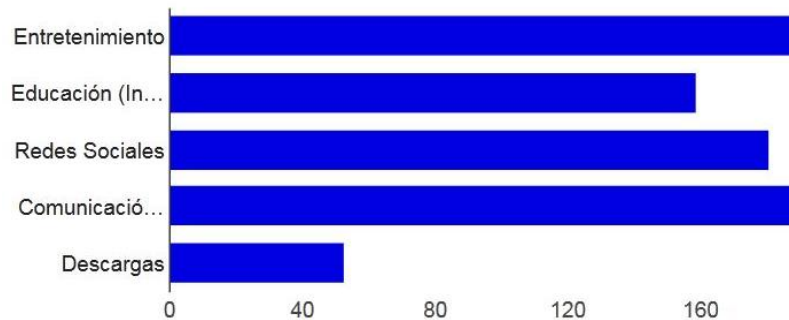


Figura 32. Encuesta / Actividades
Fuente: Autoría propia

Entretenimiento	189	83.3%
Educación (Investigación)	159	70%
Redes Sociales	181	79.7%
Comunicación (Correo, Foros, Chats, etc)	189	83.3%
Descargas	53	23.3%

De acuerdo a la pregunta anterior, acerca de las actividades que más se realizan durante el uso del Internet en los computadores del Kiosco Vive Digital, se evidencia que las dos actividades con mayor frecuencia son **Entretenimiento** y **Comunicación (Correos, Foros, Chats, etc)**, las dos con un total de 189 encuestas, equivalentes al 83.3%; seguidos por **Redes Sociales** con un total de encuestas también alto de 181, correspondiente al 79.7%, y por la actividad de **Educación (Investigación)** con 159 encuestas, representando el 70%; por último se encuentra la actividad de **Descargas** con un total de 53 encuestas, iguales al 23.3%.

7.6.1.7. Frecuencia de Acceso

Con qué frecuencia accede a Internet desde los computadores del Kiosco Vive Digital?

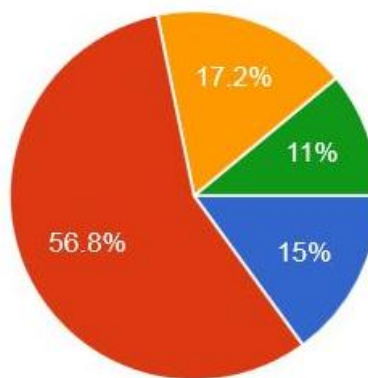


Figura 33. Encuesta / Frecuencia de Acceso
Fuente: Autoría propia

Todos los Días	34	15%
Varios Días a la Semana	129	56.8%
Una vez a la Semana	39	17.2%
Solo Fines de Semana	25	11%

En base al acceso a Internet desde los computadores del Kiosco Vive Digital en el Municipio de Dosquebradas, se muestra que la mayor frecuencia de uso de Internet se realiza durante **Varios Días a la Semana**, con un gran total de 129 encuestas, equivalentes al 56.8%, más de la mitad de los encuestados, seguidos de las siguientes frecuencias de acceso con valores muy similares, como lo son **Una vez a la Semana** con un total de 39 encuestas, correspondientes al 17.2% y **Todos los Días** con 34 encuestas igual al 15%; por último se encuentra la opción de **Solo fines de Semana** con un total de 25 encuestas, representando el 11%.

7.6.1.8. Tiempo de Conexión

Cuánto tiempo se conecta a internet a la semana, desde los computadores del Kiosco Vive Digital?

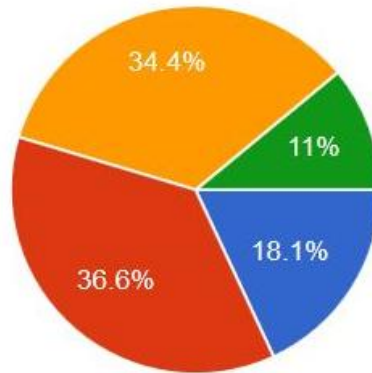


Figura 34. Encuesta / Tiempo de Conexión

Fuente: Autoría propia

Menos de 1 hora	41	18.1%
De 1 a 5 horas	83	36.6%
De 5 a 10 horas	78	34.4%
De 10 a 20 horas	25	11%
Más de 20 horas	0	0%

De acuerdo al tiempo de conexión a Internet a la semana desde los computadores del Kiosco Vive Digital, se evidencia que los dos rangos con mayor frecuencia son **De 1 a 5 horas** con un total de 83 encuestas (36.6%) y **De 5 a 10 horas** con 78 encuestas (34.4%), seguidos de la opción **Menos de 1 hora** con un total de 41 encuestas, equivalentes al 18.1%, continuando con el rango **De 10 a 20 horas** con 25 encuestas (11%) y por último con la opción de **Más de 20 horas**, la cual no fue seleccionada por ninguno de los encuestados.

7.6.1.9. Normas o Pautas

Le han sugerido normas o pautas para seguir durante el uso de Internet en los computadores del Kiosco Vive digital?

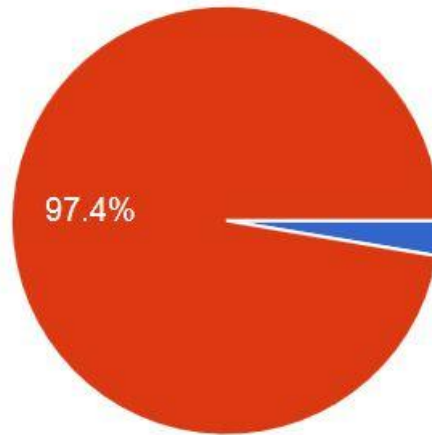


Figura 35. Encuesta / Normas o Pautas

Fuente: Autoría propia

Si	6	2.6%
No	221	97.4%

Según los resultados obtenidos en base al cuestionamiento anterior sobre normas o pautas para el uso de Internet en los computadores del Kiosco Vive digital, se evidencia en un alto porcentaje de 97.4% de los encuestados, reflejados en un total de 221 estudiantes, casi el total de la Muestra, que **No** le han sugerido normas o pautas para seguir durante el uso de Internet, en ninguno de los diferentes Kioscos Vive Digital de las 7 Veredas en el Municipio de Dosquebradas, quedando un mínimo porcentaje de 2.6%, de este mismo grupo de encuestados, representados en 6 estudiantes, revelando que **Si** le han sugerido normas o pautas para el uso de Internet; demostrándose de esta forma la gran falencia de seguridad al no contar con los parámetros y cuidados necesarios sugeridos por el personal encargado de dichos Kiosco Vive digital, a la hora de acceder y consultar contenido en Internet.

7.6.1.10. Algunas Normas

Si la respuesta fue Si en la pregunta anterior, menciona alguna de las Normas

No consumir alimentos cerca a los equipos
No comer cerca de los equipos
Mantener limpios los Equipos
No descargar programas
No comer cerca a los equipos
No descargar ningun programa

Figura 36. Encuesta / Algunas Normas
Fuente: Autoría propia

Según los datos obtenidos en base al cuestionamiento anterior, en el caso puntual de que *Si* le han sugerido normas o pautas para seguir durante el uso de Internet en los computadores del Kiosco Vive digital, se relaciona a continuación las pocas medidas propuestas por el personal encargado de los Kiosco Vive digital, resumidas en tres respuestas generales: ***No consumir alimentos cerca a los equipos***, ***Mantener limpios los equipos*** y por último ***No descargar ningún programa***. Las normas o pautas mencionadas por los encuestados, no reflejan parámetros ni criterios de control de Seguridad suficientemente fuertes a la hora de utilizar Internet en los diferentes Kioscos Vive Digital de las 7 Veredas beneficiadas en el Municipio de Dosquebradas (Risaralda), evidenciándose una gran falencia de Seguridad Informática.

7.6.1.11. Páginas Web

Dentro de las siguientes categorías de páginas web, cuáles ha visitado alguna vez desde los equipos del Kiosco Vive Digital?

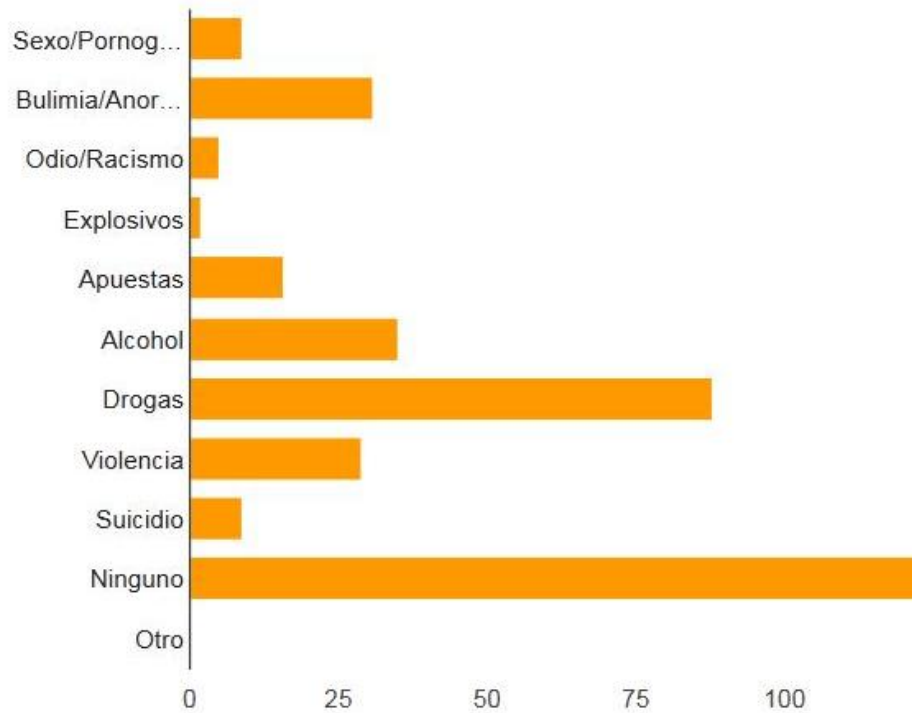


Figura 37. Encuesta / Páginas Web

Fuente: Autoría propia

Sexo/Pornografía/Desnudos	9	4%
Bulimia/Anorexia	31	13.7%
Odio/Racismo	5	2.2%
Explosivos	2	0.9%
Apuestas	16	7%
Alcohol	35	15.4%
Drogas	88	38.8%
Violencia	29	12.8%
Suicidio	9	4%
Ninguno	123	54.2%
Otro	0	0%

De acuerdo a la pregunta anterior, acerca de las páginas web visitadas alguna vez desde los computadores del Kiosco Vive Digital en el Municipio de Dosquebradas (Risaralda), se evidencia que más de la mitad del Muestreo de los encuestados con un total de 123, equivalentes al 54.2%, no han visitado *Ninguna* de las categorías de páginas web relacionadas en la pregunta; como segundo resultado se encuentra la opción *Drogas*, con un total de 88 encuestas, correspondientes al 38.8%, seguido de la categoría *Alcohol* con un porcentaje de 15.4%, igual a 35 encuestas.

En cuarta posición se encuentra la opción de *Bulimia/Anorexia* con un total de 31 encuestas, equivalentes al 13.7%, continuando la categoría *Violencia* con 29 encuestados, representando el 12.8%, y seguido de *Apuestas* con un porcentaje de 7%; ya dentro de las categorías de páginas web con totales y porcentajes bajos, se encuentran las opciones de *Sexo/Pornografía/Desnudos* y *Suicidio*, *ambas* con un total de 9 encuestas, equivalentes al 4%, pasando por la categoría de *Odio/Racismo* con un porcentaje de 2.2%, igual a 5 encuestas, y por último la opción de *Explosivos* con sólo 2 encuestas, correspondientes al 0.9%.

7.6.1.12. Redes Sociales

A cuál de las siguientes Redes Sociales, accedes desde los computadores del Kiosco Vive Digital?

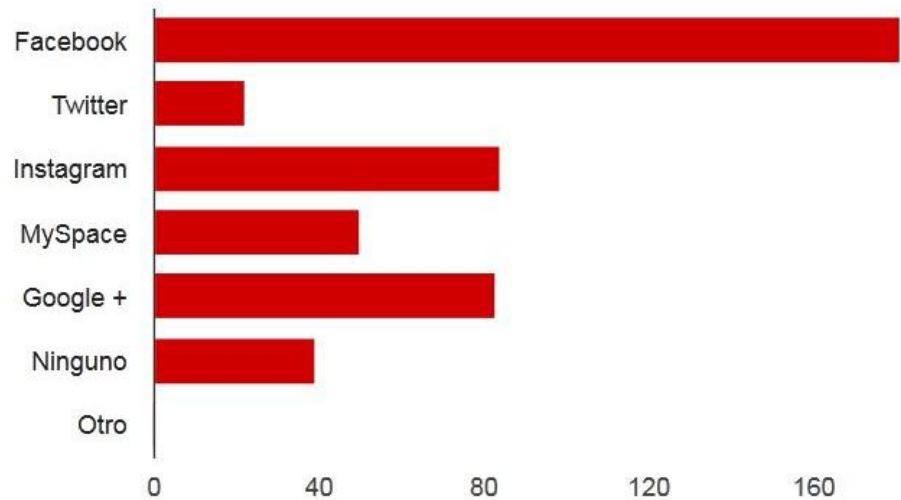


Figura 38. Encuesta / Redes Sociales

Fuente: Autoría propia

Facebook	181	79.7%
Twitter	22	9.7%
Instagram	84	37%
MySpace	50	22%
Google +	83	36.6%
Ninguno	39	17.2%
Otro	0	0%

Según los datos obtenidos sobre Redes Sociales, se muestra que la principal opción seleccionada es **Facebook**, con un altísimo porcentaje de 79.7%, representados en 181 encuestas, seguido de la opción **Instagram**, con un total de 84, equivalentes al 37%, en tercer lugar la Red Social **Google +** con 83 encuestas, correspondiente al 36.6%, como cuarta opción, **MySpace**, con un resultado de 50 encuestas, que representa al 22%, y por último las opciones de **Ninguno** con un total de 39 encuestas, igual al 17.2% y la Red Social **Twitter** con 22 encuestas, equivalentes al modesto 9.7%.

7.6.1.13. Contraseñas en Redes Sociales

Si tiene alguno o varias perfiles en Redes sociales, las contraseñas empleadas para ingresar a estos sitios son:

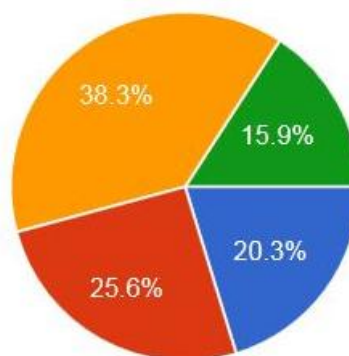


Figura 39. Encuesta / Contraseñas en Redes Sociales
Fuente: Autoría propia

Todas Iguales	46	20.3%
Todas Diferentes	58	25.6%
Utiliza la misma para varios sitios	87	38.3%
No tengo Perfil en Redes sociales	36	15.9%

En base a las contraseñas empleadas para ingresar a los perfiles en Redes Sociales, se evidencia un grupo de porcentajes muy parejos, liderada por la opción *Utiliza la misma para varios sitios* con un total de 87 encuestas, correspondientes al 38.3%, seguida de la respuesta *Todas Diferentes* con un porcentaje del 25.6%, igual a 58 encuestas, continuando con la elección de *Todas Iguales* con un total de 46, equivalentes al 20.3% y por último la opción de *No tengo Perfil en Redes Sociales*, la cual obtuvo el inesperado resultado de 36 encuestas, que representan el 15.9%, sumando entre todos un total de 227 encuestas cubriendo el 100% de la Muestra.

7.6.1.14. Cuenta de Correo

Tiene Cuenta de Correo Electrónico?

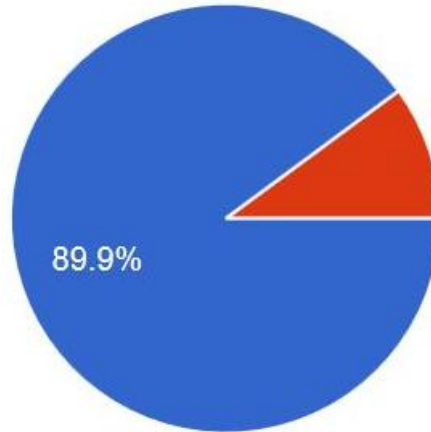


Figura 40. Encuesta / Cuenta de Correo
Fuente: Autoría propia

Si	204	89.9%
No	23	10.1%

Según los resultados obtenidos en base al cuestionamiento anterior, se evidencia que el altísimo porcentaje de 89.9%, equivalentes a 204 encuestas, casi el total de la Muestra, corresponden a la opción *Si* se dispone de una Cuenta de Correo Electrónico, por parte de los usuarios de los diferentes Kioscos Vive Digital de las 7 Veredas en el Municipio de Dosquebradas, quedando un pequeño porcentaje de 10.1%, de este mismo grupo, representados en 23 encuestados que revelan el *No* disponer de alguna Cuenta de Correo Electrónico; lo que da a entender que casi el total de los encuestados tienen la posibilidad de recibir correos de todo tipo, incluyendo aquellos de procedencia desconocida, maliciosa o dañina que de no conocerse sus alcances, pueden afectar considerablemente la infraestructura de los Kioscos Vive Digital.

7.6.1.15. Acciones frente a Correos Electrónicos

Si la respuesta fue Si en la pregunta anterior conteste: Si recibe correos electrónicos extraños mientras utilizan los computadores del Kiosco Vive Digital, Qué acción realizas?

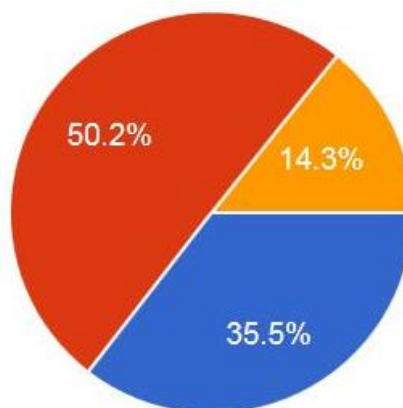


Figura 41. Encuesta / Acciones frente a Correos Electrónicos
Fuente: Autoría propia

Abrirlos y revisar su contenido	72	35.5%
Borrarlos sin abrirlos	102	50.2%
Preguntarle a alguien si se debe abrir	29	14.3%

Según los datos obtenidos en base a la pregunta anterior, en el caso de aquellos encuestados que *Si* disponen de una Cuenta de Correo Electrónico, se evidencia que un poco más de la mitad de los encuestados, representados en un 50.2% equivalentes a 102 personas, realizan la buen practica de **Borrar sin Abrir** los correos electrónicos extraños, recibidos mientras utilizan los computadores del Kiosco Vive Digital, seguidos de otro gran porcentaje de 35.5%, correspondientes a 72 encuestados, que por el contrario incurren en la arriesgada acción de **Abrir y revisar su contenido** exponiendo a posibles daños la infraestructura de los Kioscos Vive Digital, y por último se muestra un pequeño porcentaje del 14.3%, representados en 29 encuestados, que ante la duda de un Correo Electrónico recibido, optan por la opción de **Preguntarle a alguien si se debe abrir**.

7.6.1.16. Términos

Señale cuál de los siguientes términos conoce:

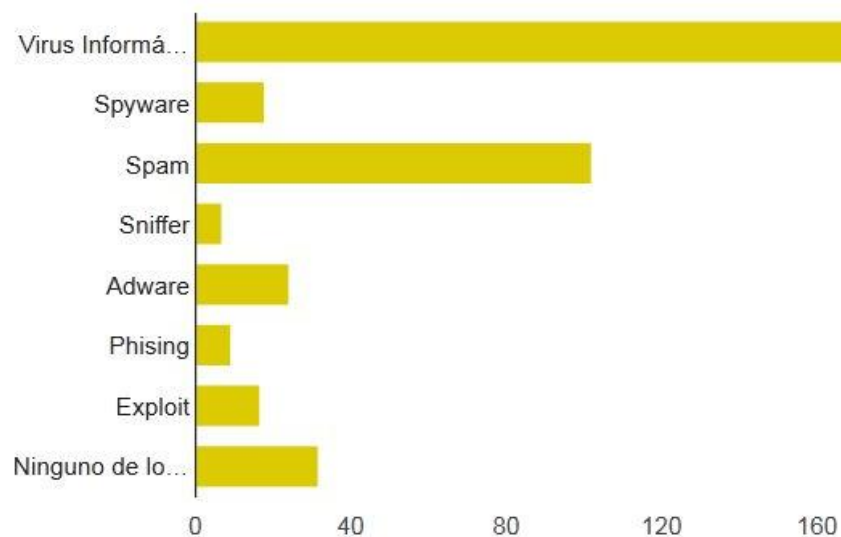


Figura 42. Encuesta / Términos

Fuente: Autoría propia

Virus Informático	184	81.1%
Spyware	18	7.9%
Spam	102	44.9%
Sniffer	7	3.1%
Adware	24	10.6%
Phising	9	4%
Exploit	17	7.5%
Ninguno de los Anteriores	32	14.1%

De acuerdo a la última pregunta de la encuesta, acerca de aquellos términos que conocen los usuarios de los diferentes Kioscos Vive Digital del Municipio de Dosquebradas (Risaralda), se evidencia que 123 encuestados, equivalente al 81.1%, casi el total del Muestreo, conoce el término *Virus Informático*; como segundo resultado se encuentra el término *Spam*, con un total de 102 encuestas, correspondientes al 44.9%, seguido de la opción *Ninguno de los Anteriores*

con un porcentaje de 14.1%, igual a 32 encuestas, y en cuarta posición se encuentra el término *Adware* con un total de 24 encuestas, equivalentes al 10.6%.

Dentro de los términos con totales y porcentajes bajos, se encuentran las opciones de *Spyware* con 18 encuestados, representando el 7.9%, seguido de *Exploit* con un porcentaje de 7.5%, igual a 17 encuestas; *Phising* con un total de 9 encuestas, equivalentes al 4%, y por último el término de *Sniffer* con un porcentaje de 3.1%, igual a 7 encuestas; lo que da a entender que casi el total de los encuestados desconocen el significado de la mayoría de los términos que representan un alto riesgo para la Seguridad Informática de la infraestructura (Software - Hardware) de los Kioscos Vive Digital de las diferentes veredas del Municipio de Dosquebradas (Risaralda), beneficiadas dentro del Programa Vive Digital direccionado por el Gobierno Nacional.

7.6.2. Lista de Chequeo

Para la realización de la *Lista de Chequeo*, por parte del encargado(a) del Kiosco Vive Digital, instalado en la **Institución Educativa Pública Eduardo Correa Uribe** – Sede la Palma Dosquebradas, beneficiada con el Programa VIVE DIGITAL, se optó por aplicarse en sólo una sede para conocer el nivel de seguridad de la infraestructura (Hardware - Software) instalados.

De acuerdo a los datos obtenidos, se presenta el siguiente análisis de la información de cada uno de los ítems de la encuesta:

DATOS GENERALES

7.6.2.1. Género

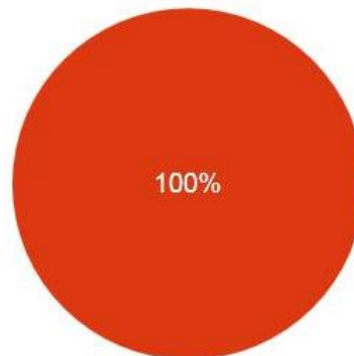


Figura 43. *Lista de Chequeo / Género*

Fuente: Autoría propia

Masculino	0	0%
Femenino	1	100%

Según los datos obtenidos en el primer ítem de la lista de chequeo, se confirma que el encargado(a) del Kiosco Vive Digital, instalado en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), pertenece al Género ***Femenino***.

7.6.2.2. Edad



Figura 44. *Lista de Chequeo / Edad*

Fuente: Autoría propia

Entre 18 y 30	1	100%
Entre 31 y 40	0	0%
Entre 41 y 50	0	0%
Entre 51 y 60	0	0%
Entre 61 y Más	0	0%

De acuerdo al rango de Edades establecidas, se establece que la persona encargada del Kiosco Vive Digital, en la Institución Educativa Eduardo Correa Uribe – Sede la Palma Dosquebradas, se encuentra en el rango de **18 y 30** años.

7.6.2.3. Cargo que Desempeña

Cargo que desempeña en el Kiosco Vive Digital

Gestora Social

Figura 45. *Lista de Chequeo / Cargo que Desempeña*

Fuente: Autoría propia

Según el dato obtenido, se conoce que el cargo que desempeña la persona encargada del Kiosco Vive Digital, en la Institución mencionada, es el de **Gestora Social**.

LISTA DE CHEQUEO

HARDWARE

7.6.2.4. Cantidad de Computadores

De cuántos computadores dispone el Kiosco Vive Digital?

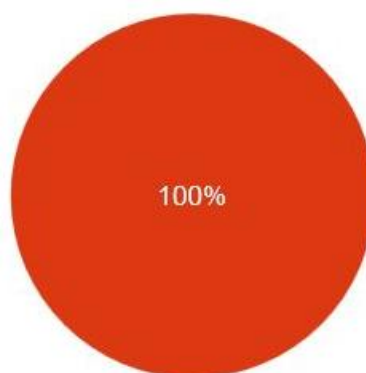


Figura 46. *Lista de Chequeo | Cantidad de Computadores*

Fuente: Autoría propia

De 1 a 5 Computadores	0	0%
De 5 a 10 Computadores	1	100%
Más de 10 Computadores	0	0%

En base a lo contestado por la persona encargada del Kiosco Vive Digital, instalado en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), con respecto a la cantidad de computadores con que dispone el Kiosco Vive Digital en mención, se conoce que cuenta con un total de equipos dentro del rango de **5 a 10 Computadores**.

7.6.2.5. Dispositivo de Conexión a Internet

Con qué dispositivo de conexión se cuenta para el acceso a Internet en los computadores del Kiosco Vive Digital?

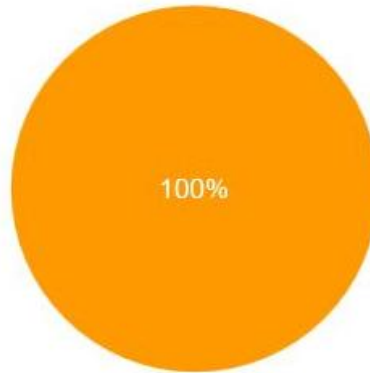


Figura 47. Lista de Chequeo / Dispositivo de Conexión a Internet
Fuente: Autoría propia

Línea Telefónica (RTB, RDSI, ADSL)	0	0%
Cable (Fibra Óptica, Cable Coaxial)	0	0%
Satélite (Antena Parabólica)	1	100%
Inalámbrica (Wi-Fi, WiMax)	0	0%
Telefonía Movil (3G, 4G)	0	0%
Radio (LMSD)	0	0%

Según la respuesta obtenida, en base a los diferentes dispositivos de conexión existentes para el acceso a de Internet en los computadores del Kiosco Vive Digital instalado en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se conoce que dicho Kiosco cuenta con un Dispositivo de tipo *Satélite (Antena Parabólica)* para tal fin.

7.6.2.6. Dispositivo de Distribución del Internet

Con que dispositivo se cuenta para la distribución de Internet en los computadores del Kiosco Vive Digital?

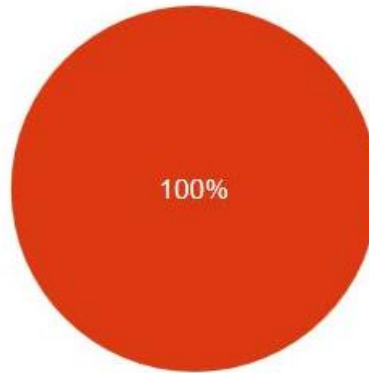


Figura 48. Lista de Chequeo / Dispositivo de Distribución del Internet

Fuente: Autoría propia

Servidor de Internet	0	0%
Router	1	100%
Firewall	0	0%
Otro	0	0%

De acuerdo a la pregunta anterior, acerca de los diferentes dispositivos de distribución de Internet en los computadores del Kiosco Vive Digital instalados en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se revela por parte de la encargada del Kiosco en mención, que se dispone de un Dispositivo tipo **Router** para la distribución de Internet.

7.6.2.7. Tipo de Conexión a Internet

De qué forma se conectan los computadores del Kiosco Vive Digital a Internet?

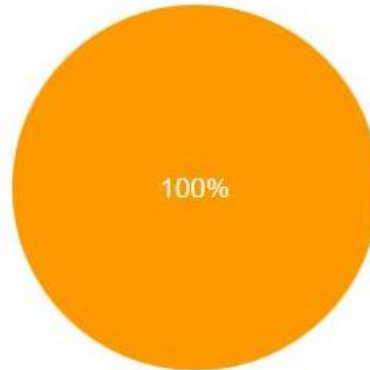


Figura 49. Lista de Chequeo | Tipo de Conexión a Internet

Fuente: Autoría propia

Cableado (UTP)	0	0%
Inalámbrico	0	0%
Cableado e Inalámbrico	1	100%

En base a lo contestado por la persona encargada del Kiosco Vive Digital, instalado en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), con respecto a la forma en que se encuentran conectados los computadores del Kiosco en mención a Internet, se conoce que se dispone de dos tipos de conexión, tanto **Cableado** como **Inalámbrico**, abarcando de esta forma la totalidad de los computadores instalados para tal fin.

7.6.2.8. Control de Instalación

Se controla que los usuarios puedan instalar aplicaciones en los equipos del Kiosco Vive Digital?

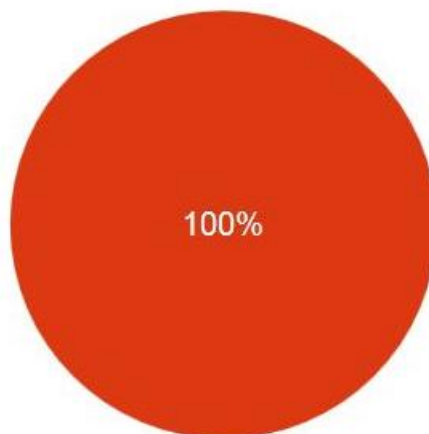


Figura 50. Lista de Chequeo / Control de Instalación

Fuente: Autoría propia

Si	0	0%
No	1	100%
Ns/Nr	0	0%

De acuerdo a la pregunta anterior, acerca del control para la instalación de aplicaciones por parte de los usuarios, en los computadores del Kiosco Vive Digital, instalados en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se conoce por parte de la encargada del Kiosco en mención, que **No** se dispone de dichos controles para tal acción, evidenciándose una gran falencia de Seguridad Informática.

SOFTWARE

7.6.2.9. Sistema Operativo

Qué Sistema Operativo tienen instalados los computadores del Kiosco Vive Digital?



Figura 51. *Lista de Chequeo / Sistema Operativo*

Fuente: Autoría propia

Windows (Cualquier Distribución)	1	100%
Mac (Cualquier Distribución)	0	0%
Linux (Cualquier Distribución)	0	0%

En base a la respuesta dada por la persona encargada del Kiosco Vive Digital, instalado en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), con respecto al Sistema Operativo instalado en los computadores del Kiosco Vive Digital mencionado, se conoce que cuentan con un S.O *Windows (Cualquier Distribución)*.

7.6.2.10. Licenciamiento

El Software de los computadores del Kiosco Vive Digital, cuentan con sus respectivas licencias de instalación?



Figura 52. *Lista de Chequeo / Licenciamiento*
Fuente: Autoría propia

Si	1	100%
No	0	0%
Ns/Nr	0	0%

De acuerdo a la pregunta anterior, acerca de las licencias del Software instalado en los computadores del Kiosco Vive Digital en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se confirma por parte de la encargada del Kiosco en mención, que *Si* se dispone de licenciamiento de instalación, lo que permite en primera instancia tener tranquilidad por contar con software original.

7.6.2.11. Antivirus

Los computadores del Kiosco Vive Digital tienen instalado antivirus?

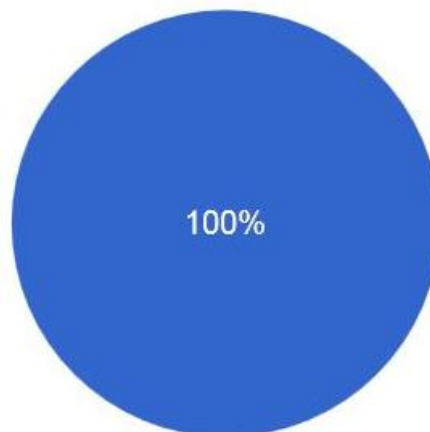


Figura 53. Lista de Chequeo / Antivirus

Fuente: Autoría propia

Si	1	100%
No	0	0%
Ns/Nr	0	0%

Según el dato obtenido, se conoce que los computadores del Kiosco Vive Digital, instalados en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), *Sí* cuentan con software Antivirus, permitiendo proteger un poco esa gran falencia de Seguridad Informática expuesta durante la Lista de Chequeo.

7.6.2.12. Actualización del Antivirus

Si la respuesta fue Si en la pregunta anterior, El antivirus instalado permanece actualizado?



Figura 54. Lista de Chequeo / Actualización del Antivirus

Fuente: Autoría propia

Si	1	100%
No	0	0%
Ns/Nr	0	0%

En base a lo contestado por la persona encargada del Kiosco Vive Digital, en el caso de que *Si* se contara con Antivirus instalado en los computadores del Kiosco Vive Digital de la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se evidencia que este tipo de Software *Si* cuenta con las actualizaciones pertinentes, permitiendo mejorar la Seguridad Informática de los equipos.

7.6.2.13. Descarga de Ficheros

Se utilizan programas de descarga de ficheros? (música, películas, programas, documentos, etc)



Figura 55. Lista de Chequeo / Descarga de Ficheros

Fuente: Autoría propia

Si	1	100%
No	0	0%
Ns/Nr	0	0%

De acuerdo a la pregunta anterior, acerca del uso de programas para la descarga de ficheros, en los computadores del Kiosco Vive Digital, instalados en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se conoce por parte de la encargada del Kiosco en mención, que *Si* se utilizan dichos programas de descargas, evidenciándose una gran vulnerabilidad de Seguridad Informática, por la falta de control.

7.6.2.14. Conexiones externas vía Internet

Se realizan conexiones externas por vía Internet a los computadores del Kiosco Vive Digital?

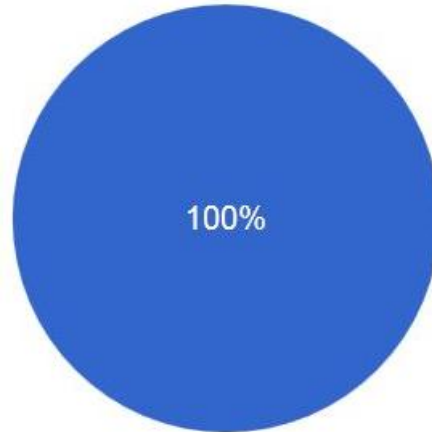


Figura 56. *Lista de Chequeo | Conexiones externas vía Internet*
Fuente: Autoría propia

Si	1	100%
No	0	0%
Ns/Nr	0	0%

En base a la respuesta anterior, referente a la existencia de conexiones externas por vía Internet a los computadores del Kiosco Vive Digital, instalados en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se conoce por parte de la encargada del mismo, que **Si** se realizan conexiones de este tipo, demostrándose el gran riesgo de Seguridad Informática, así como también la vulnerabilidad a la que podría quedar expuesta la infraestructura, por el permitir dicho acceso remoto sin los debidos controles, políticas y protocolos de seguridad.

7.6.2.15. Conexión Inalámbrica

Ofrece el Kiosco Vive Digital conexión inalámbrica (WIFI) a sus usuarios?

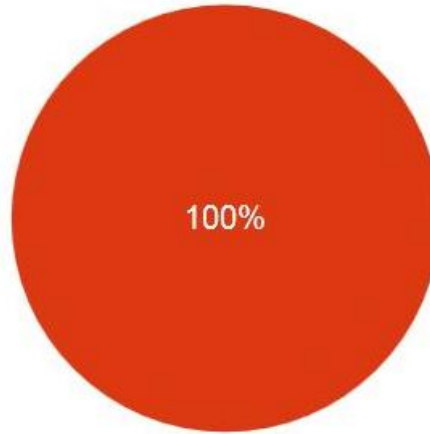


Figura 57. Lista de Chequeo / Conexión Inalámbrica

Fuente: Autoría propia

Si	0	0%
No	1	100%
Ns/Nr	0	0%

De acuerdo a lo contestado por la persona encargada del Kiosco Vive Digital, instalado en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), con respecto al servicio de Conexión Inalámbrica (Wifi), se conoce que dicho Kiosco Vive Digital **No** ofrece a sus usuarios acceso de este tipo, limitándose sólo a la conexión a Internet por cable.

7.6.2.16. Medidas de Seguridad Conexión Inalámbrica

Si la respuesta fue Si en la pregunta anterior, Se cuentan con medidas de seguridad para proteger dicha conexión?

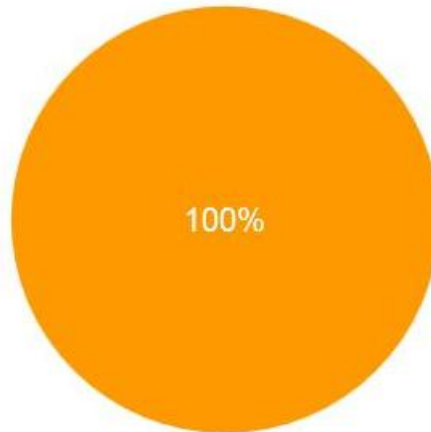


Figura 58. Lista de Chequeo / Medidas de Seguridad Conexión Inalámbrica
Fuente: Autoría propia

Si	0	0%
No	0	0%
Ns/Nr	1	100%

En base a la respuesta Negativa en la pregunta anterior, en cuanto a que no se ofrece a sus usuarios el servicio de Conexión Inalámbrica (Wifi) en el Kiosco Vive Digital de la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se da por entendido que **No** se cuentan con medidas de seguridad para proteger dicha conexión.

7.6.2.17. Navegador utilizado

Qué Navegador se utiliza en los computadores del Kiosco Vive Digital para navegar en Internet?

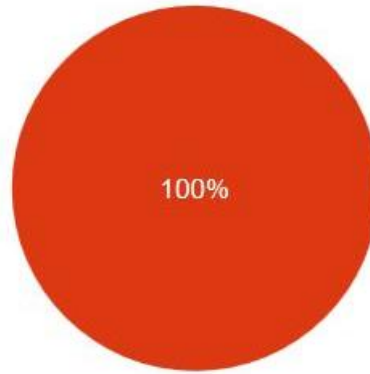


Figura 59. *Lista de Chequeo / Navegador utilizado*
Fuente: Autoría propia

Mozilla Firefox	0	0%
Chrome	1	100%
Internet Explorer	0	0%
Safari	0	0%
Opera	0	0%
Otro	0	0%

Según el dato obtenido por la persona encargada del Kiosco Vive Digital, instalado en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se conoce que el Navegador **Chrome** es el instalado y utilizado para el uso de Internet en todos los computadores del Kiosco en mención.

7.6.2.18. Influencia de Seguridad del Navegador

Considera que el navegador influye en la seguridad a la hora de navegar por Internet?

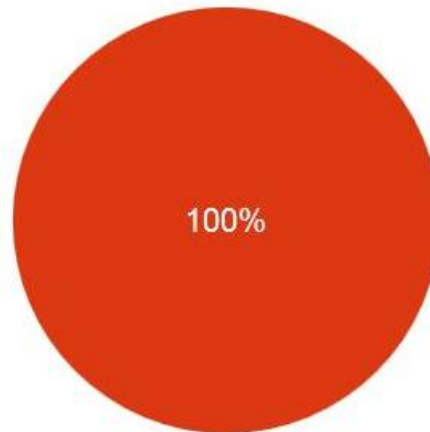


Figura 60. *Lista de Chequeo / Influencia de Seguridad del Navegador*
Fuente: Autoría propia

Si	0	0%
No	1	100%
Ns/Nr	0	0%

De acuerdo a la opinión y punto de vista de la persona encargada del Kiosco Vive Digital, instalado en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), en cuanto al papel del Navegador como herramienta que también permite el control para la Seguridad Informática, se conoce que ésta *No* considera que el navegador influye en la seguridad a la hora de navegar por Internet.

7.6.2.19. Cortafuegos

Se cuenta con algún Software como Cortafuegos para los computadores del Kiosco Vive Digital?

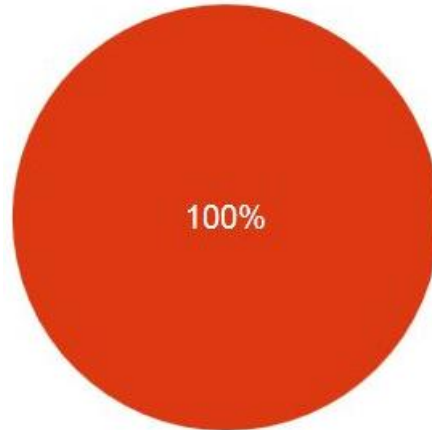


Figura 61. *Lista de Chequeo / Cortafuegos*
Fuente: Autoría propia

Si	0	0%
No	1	100%
Ns/Nr	0	0%

Con el fin de conocer el nivel de seguridad actual con que cuentan los computadores del Kiosco Vive Digital, instalados en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se conoce en base a la respuesta obtenida por la encargada del Kiosco mencionado, que *No* se cuenta con algún Software como Cortafuegos para los equipos del Kiosco Vive Digital, demostrándose el gran riesgo de Seguridad Informática en que se ven expuestos, así como también la vulnerabilidad en la que podría quedar dicha infraestructura, por la falta de controles, políticas y protocolos de seguridad.

7.6.2.20. Cortafuegos utilizados

Si la respuesta fue Si en la pregunta anterior, Que Software como Cortafuegos se utiliza?

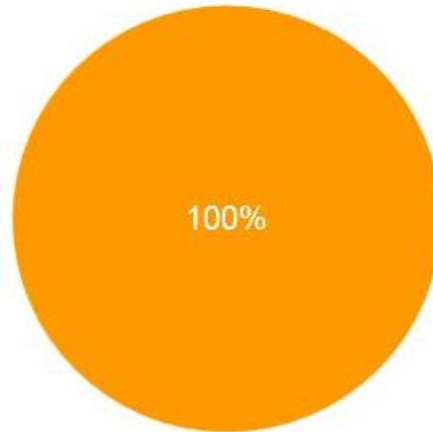


Figura 62. Lista de Chequeo / Cortafuegos utilizados

Fuente: Autoría propia

El que viene con el Sistema Operativo	0	0%
El que viene con el Antivirus	0	0%
No se utiliza	1	100%
Otro	0	0%

En base a la respuesta Negativa en la pregunta anterior, en cuanto a que no se cuenta con algún Software como Cortafuegos para los computadores del Kiosco Vive Digital de la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se da por entendido que *No* se utiliza software alguno con dichas características como medida de seguridad para proteger el uso de Internet.

7.6.2.21. Sistema de Control Parental

Se tiene instalado algún tipo de Sistema de Control Parental y/o Control de Usuarios en los computadores del Kiosco Vive Digital?

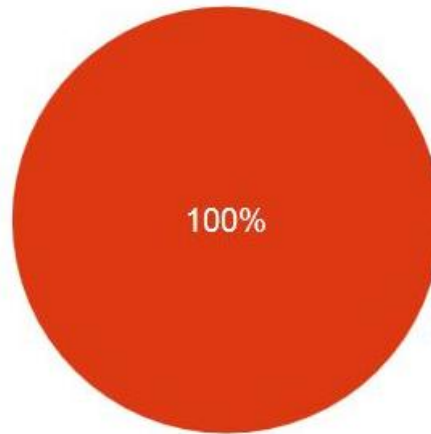


Figura 63. Lista de Chequeo / Sistema de Control Parental

Fuente: Autoría propia

Si	0	0%
No	1	100%
Ns/Nr	0	0%

Continuando con la necesidad de conocer el nivel de seguridad actual con que cuentan los computadores del Kiosco Vive Digital, instalados en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se confirma de acuerdo a la respuesta obtenida por la encargada del Kiosco mencionado, que *No* se tiene instalado ningún tipo de Sistema de Control Parental y/o Control de Usuarios, demostrándose de igual forma la gran vulnerabilidad en cuanto a la Seguridad Informática, así como también el riesgo en el que se podría ver expuesta la infraestructura, por la falta de controles, políticas y protocolos de seguridad.

7.6.2.22. Contenido consultado

Se Controla o supervisa el contenido que consultan las personas en Internet en los computadores del Kiosco Vive Digital?

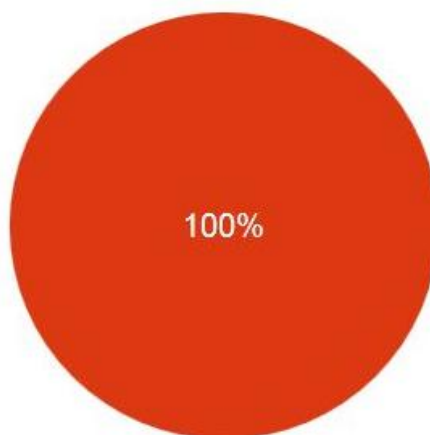


Figura 64. *Lista de Chequeo / Contenido consultado*
Fuente: Autoría propia

Si	0	0%
No	1	100%
Ns/Nr	0	0%

Por último y continuando con la idea de conocer el nivel de seguridad actual con que cuentan los computadores del Kiosco Vive Digital, instalados en la Institución Educativa Pública Eduardo Correa Uribe – Sede la Palma Dosquebradas (Risaralda), se conoce en base a la respuesta de la encargada del Kiosco en mención, que **No** se controla o supervisa el contenido que consultan las personas en Internet, evidenciándose nuevamente el gran riesgo en cuanto a la Seguridad Informática, así como también la vulnerabilidad en la que podría quedar expuesta la infraestructura, por la falta de controles, políticas y protocolos de seguridad.

8. HERRAMIENTAS DE SOFTWARE LIBRE

En la actualidad, existen productos, tecnologías, dispositivos, y Herramientas de Software Libre que se utilizan como Políticas de seguridad Informática para la protección de la infraestructura computacional y todo lo relacionado con esta; tal es el caso puntual de la Información como el bien o activo máspreciado de cualquier entidad, sea cual sea su tipo o característica de funcionamiento.

Por lo anterior y en base a las respuestas analizadas durante el capítulo *Metodología de la Investigación*, obtenidas a través de la Encuesta y Lista de Chequeo, aplicados en los diferentes Kioscos Vive Digital de las Instituciones Educativas Públicas del Municipio de Dosquebradas (Risaralda), beneficiadas con el Programa Vive Digital direccionado por el Gobierno Nacional; se evidencia la falta de estándares, protocolos y políticas de seguridad que son vitales para minimizar aquellos riesgos informáticos que vulneran la infraestructura y/o la información de aquellas instituciones educativas, por el mal uso del Internet; por esta razón, el presente Proyecto de Investigación se enfocó en la implementación de Políticas de Seguridad a través de una Herramienta de Software Libre, para mejorar y prevenir la problemática identificada, para lo cual se seleccionaron 3 de las múltiples opciones existentes en la actualidad, que a nuestro criterio cumplieran con las expectativas y requerimientos de seguridad buscados.

Dichas herramientas fueron elegidas para ser analizadas en base a la documentación existente, para finalmente seleccionar la más idónea, que permita proteger la integridad de los usuarios, prevenir los daños en la infraestructura computacional y salvaguardar la información, todo lo anterior como instrumento de control y medida de Seguridad Informática.

Las 3 Herramientas de Software Libre seleccionadas son:

pfSense | *Zentyal* | *IPCop*

8.1. PfSense



Figura 65. Logo PfSense

Fuente: IRONTEC, Internet y Sistemas sobre GNU/Linux. Sistemas e Infraestructuras. Firewall pfSense. Recuperado de: <https://www.irontec.com/sistemas-linux>

PfSense es una distribución personalizada de FreeBSD (abreviatura de Berkeley Software Distribution, que traducido al español es llamado *Distribución libre de Software Berkeley*, el cual es un sistema operativo derivado de Unix nacido a partir de un proyecto de la universidad de California en Berkeley) que cuenta con un software explícito para seguridad informática, adaptado para su uso como Firewall, Router, Servidor de Balanceo de Carga, entre otras, para usarlo en servicios de redes LAN y WAN.

Contextualizando un poco, un Firewall es aquel elemento de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. De igual forma, se trata de un dispositivo o conjunto de dispositivos configurados para limitar, permitir, cifrar, descifrar, el tráfico entre los diferentes entornos sobre la base de un conjunto de normas y otros criterios.

El modelo de desarrollo de la Herramienta de Software Libre *PfSense* es de código abierto, por tal motivo ha tenido desde su creación más de un millón de descargas, las cuales han sido instaladas con éxito en diferentes entornos, desde redes domésticas hasta grandes empresas.

Dentro de las características que ofrece *PfSense*, además de tratarse de una solución muy completa, licenciada bajo BSD (libre distribución), se destaca la de contar con un gestor de paquetes desde su interfaz gráfica, accedida remotamente para ampliar sus funcionalidades, ya que al elegir el paquete deseado el mismo sistema lo descarga y lo instala automáticamente. Otra de las particularidades de dicha herramienta, es la de no requerir o necesitar conocimientos avanzados acerca de líneas de comandos de BSD para manejar *PfSense*.

Como característica adicional, *PfSense* puede ser instalado en cualquier tipo de Computador personal o Servidor, independientemente de su arquitectura, pero con la necesidad de que se cuente con un mínimo de 2 tarjetas de red; su proceso de instalación es similar a FreeBSD, y para resumirlo, una vez copiados los archivos del sistema al disco duro, se procede a configurar las direcciones IP de las tarjetas de red, al concluir lo anterior, se puede acceder al sistema desde un explorador web. El portal de administración está basado en PHP y teóricamente todas las configuraciones y administración se pueden realizar desde allí, por lo tanto no es indispensable contar con conocimientos avanzados sobre la línea de comandos UNIX para su manejo.

Para la instalación de la Herramienta de Software Libre *PfSense* sobre una arquitectura i386 (32 bits), los requerimientos de hardware mínimos son los siguientes:

1. Procesador Intel Pentium III, hasta un Intel Xeon. (No AMD)
2. Memoria RAM desde 256 Mb hasta 3 Gb.
3. Disco Duro de 2 Gb hasta 80 Gb, IDE, SCSI, SATA y SAS-SATA.
4. Tarjetas de red.

8.1.1. Características Principales de PfSense

PfSense al igual que un Sistema Operativo, es una aplicación que se instala de una forma muy similar, ya que dispone de varias funcionalidades, dentro los cuales se encuentran servicios de redes LAN y WAN como los siguientes:

Firewall: *PfSense* se puede configurar como un cortafuego, permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a partir de una dirección ya sea de red o de host de origen y de destino, también haciendo filtrado avanzado de paquetes por protocolo y puerto.

Servidor VPN: *PfSense* se puede configurar como un servidor VPN, usando protocolos de tunneling tales como IPSec, PPTP, entre otras.

Servidor de Balanceo de Carga: *PfSense* puede ser configurado como servidor de balanceo de carga, tanto entrante como saliente; esta característica es usada comúnmente en servidores web, correo, DNS. También para proveer estabilidad y redundancia en el envío de tráfico a través del enlace WAN evitando los embotellamientos.

Portal Cautivo: Este servicio consiste en forzar la autenticación de usuarios redirigiéndolos a una página especial de autenticación y/o para aceptar los términos de uso, realizar un pago etc. para poder tener acceso a la red. El portal cautivo es usado comúnmente para control de accesos a la red en los puntos de accesos inalámbricos de los hoteles, restaurantes, parques y kioscos.

Tabla de Estado: *Pfsense* es un stateful firewall, el cual como característica principal guarda el estado de las conexiones abiertas en una tabla. La mayoría de los firewall no tienen la capacidad de controlar con precisión la tabla de estado.

Servidor DNS: *PfSense* se puede configurar como un servidor DNS primario.

Servidor DHCP: También funciona como servidor de DHCP, se puede también implementar VLAN desde *PfSense*.

Servidor PPPoE: Este servicio es usado por los ISP para la autenticación de usuarios que puedan ingresar a internet, por una base local o vía radius (Protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP).

Enrutamiento Estático: *PfSense* funciona como un enrutador ya que entrega direccionamiento IP y hace el NATEO (Network Address Translation) hacia afuera.

Redundancia: *PfSense* permite configurar dos o más cortafuegos a través del protocolo CARP (Common Address Redundancy Protocol) por si uno de los cortafuegos se cae el otro se declara como cortafuegos primario.

Reportes y Monitoreo: A través de los gráficos RRD, *PfSense* muestra el estado de los siguientes componentes:

- Utilización de CPU

- Rendimiento Total
- Estado del Firewall
- Rendimiento individual por cada interface
- Paquetes enviados y recibidos por cada interface
- Manejo de tráfico y ancho de banda.

8.1.2. Características Avanzadas de PfSense

PfSense en la actualidad, compite contra productos tradicionales, orientados al mismo segmento de Seguridad Informática tipo cortafuegos y enrutadores, bajo un esquema Open Source (Codigo abierto) de licenciamiento sin costo.

Además de las funciones de servidor, *PfSense* incorpora herramientas para controlar el tráfico de la red, ya sea a nivel interno o externo. De igual forma, incluye funciones de Firewall y de Gateway que complementan la labor del servidor de servicios de red, por lo tanto se trata de una distribución robusta adecuada para un entorno de servidor, en donde son críticos los servicios de red e información.

PfSense, cuenta con las siguientes funcionalidades avanzadas:

- Escaneo de virus y spam a través de la pasarela de paso para tráfico http así como imap, pop y smtp.
- Filtrado y caché de contenidos/protocolos a través de proxy con Squid (y otros proxys más ligeros) y DNSguardian de una manera realmente bien amplia y con la funcionalidad de poder actualizar las reglas de forma automática y gratuita. Los productos convencionales requieren una licencia (en dólares) para realizar esta tarea. *PfSense* no tiene costos de licenciamiento.

- Servicio de detección de intrusiones (IDS), con la posibilidad de poder actualizar las reglas provistas de forma comunitaria y gratuita.
- Servidor LDAP (OpenLDAP) con autenticación de SAMBA como PDT.
- Sistema de backup de configuración del servidor.
- Sistema VPN (Virtual Private Network) con soporte IPSEC, OpenVPN y PPTP.
- Proxy inverso para balanceo de carga entre varios webservers de la red interna.
- Alta latencia, útil para enlaces con alta latencia, como conexiones satelitales, expira conexiones idle (ociosas) después de lo normal.

8.1.3. Diagrama PfSense

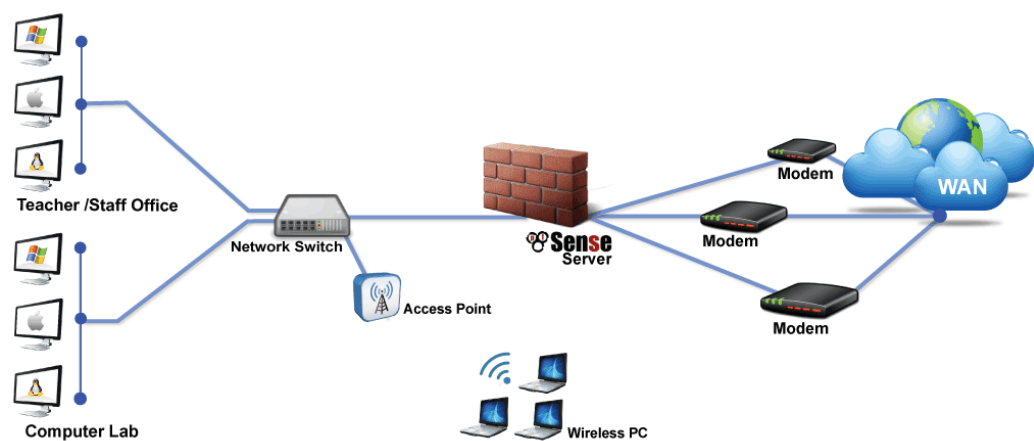


Figura 66. Diagrama PfSense

Fuente: CST. UTM Firewall PfSense. *Funcionalidades Avanzadas*. Recuperado de: <http://www.cstonline.com.ar/productos/firewall-y-router-pfsense/>

8.2. Zentyal



Figura 67. *Logo Zentyal*

Fuente: ZENTYAL. eBox Technologies S.L. *Zentyal para Administradores de Redes*. Versión 2.2. CEEI Aragon, Nave 19. C/María de Luna 11. Zaragoza. Recuperado de: http://www.zentyal.com/wp-content/uploads/2012/06/Zentyal_for_Network_Administrators_book_sample_ES.pdf

Zentyal (conocido anteriormente como *eBox*) es una solución integral de tecnología de la información, que permite a profesionales TIC administrar todos los servicios de una red informática, tales como el acceso a Internet, la seguridad de la red, la compartición de recursos, la infraestructura de la red o las comunicaciones, de forma sencilla y a través de una única plataforma. De igual forma, esta herramienta actúa como Gateway, Servidor de seguridad (UTM), Servidor de oficina, Servidor de infraestructura de red y Servidor de comunicaciones.

El código fuente de esta Herramienta de Software Libre, está disponible bajo los términos de la Licencia Pública General de GNU, así como también bajo varias licencias privativas. Es de aclarar, que la empresa Española eBox Technologies S.L. es el propietario y patrocinador de Zentyal y posee el copyright del código fuente.

Zentyal es un producto español que equivale a un Small Business Server. Este servidor se basa en Ubuntu Server 10.04 y proporciona una forma sencilla de configurar un servidor GNU/Linux, o varios, para que actúen como Gateway, servidor DNS, DHCP, firewall, backup, servidor VoIP, samba, correo, proxy, etc. Durante su programación se hizo énfasis en la usabilidad, creando una interfaz amigable que incluye únicamente aquellas opciones de uso más frecuente.

Otra de las características importantes de *Zentyal* es que todas sus funcionalidades están integradas entre sí, automatizando la mayoría de tareas y ahorrando tiempo en la administración de sistemas, mejorando la seguridad y disponibilidad de los servicios en donde se encuentra instalada.

Dentro de las generalidades de la herramienta *Zentya*, se puede mencionar el hecho de que se usa principalmente en pymes, pero también en otros entornos como Centros Educativos, Administraciones Públicas, Hospitales, entre otros.

Por último, el servidor *Zentyal* es un servidor Linux completo que se puede usar de forma gratuita sin soporte técnico y actualizaciones, o con soporte completo por una cuota mensual muy asequible.

8.2.1 Características Principales de Zentyal

ZENTYAL GATEWAY

Zentyal Gateway permite que la red sea más fiable, optimiza el ancho de banda así como ayuda a controlar lo que entra a la red.

- **Caché Transparente**

Conexión más rápida, si se visitan los mismos sitios web, los datos se descargarán una sola vez y la conexión estará disponible para tareas más importantes.

- **Control de Tráfico**

No presenta una conexión de Internet sobrecargada.

- **Balaceo de Carga y Disponibilidad**

Si se cuenta con más de una conexión a Internet, Zentyal puede distribuir los clientes de forma transparente y asegurar que estén conectados, aunque una de las conexiones esté inactiva.

- **Filtrado de Contenido**

Restringe el acceso a determinados sitios, o permite sólo a sitios específicos. Esta característica permite restringir la navegación inapropiada y ayuda a cumplir las políticas de uso de Internet en tu organización.

ZENTYAL UTM

Protege la red informática contra ataques externo, internos e intrusos.

- **Filtrado de Contenido**

Deja el malware fuera. Existen miles de amenazas como spam, virus, phishing, etc. El filtrado de contenido actúa sobre el e-mail, páginas web y ficheros compartidos para que se obtenga sólo el contenido que interesa.

- **Cortafuegos**

Dispone de distintos niveles de seguridad, permitiendo sólo el tráfico necesario contra intrusos no deseados.

- **Detección de Intrusos**

El IDS informará de cualquier intento sospechoso y dejará analizarlos para evaluar los potenciales daños.

ZENTYAL INFRASTRUCTURE

Gestiona y optimiza el tráfico interno de la red, incluyendo la configuración del servidor de dominio, la gestión de máquinas y de los certificados digitales.

- **Objetos de Red**

Puede cambiar la configuración de toda la red, de un departamento o de un solo computador.

- **Servidor DNS**

Puede asignar una dirección y un nombre fijo a cada computador de la red para facilitar la navegación por Intranet. Es más fácil recordar el nombre de un equipo que su dirección IP.

- **Servidor Web**

Zentyal viene con el servidor web Apache.

- **SSL Profesional**

Permite crear los propios certificados SSL y usarlos para correo electrónico o sitios web internos.

ZENTYAL OFFICE

Permite gestionar y compartir recursos de oficina, incluyendo perfiles de usuarios y grupos, ficheros, impresoras, calendarios, contactos, tareas y backup de datos.

- **Servicio de Directorio**

Permite la gestión de todos los usuarios y recursos desde un punto central. De igual forma permite determinar quién tiene acceso y a qué datos.

- **Calendarios, Contactos, Ficheros, Impresoras y Tareas**

Zentyal permite compartir calendarios, contactos y tareas entre los miembros del mismo equipo, así como también archivos e impresora, que pueden ser utilizados independientemente del sistema operativo.

- **Backup de Datos**

Ofrece automatizar los backups de datos para no tener que preocuparse de discos que fallan o de usuarios que borran ficheros por accidente.

ZENTYAL UNIFIED COMMUNICATIONS

Zentyal servidor de comunicaciones unificadas gestiona todas las comunicaciones, incluyendo correo electrónico, mensajería instantánea y Voz IP.

- **Gestión de Usuarios**

Gestiona todos los usuarios y recursos desde un punto central.

- **Correo electrónico**

Zentyal trae consigo una solución de correo electrónico integrado, con tecnologías antispam y antivirus.

- **Mensajería Instantánea**

Ofrece mensajería instantánea basada en el protocolo Jabber/XMPP.

8.2.2 Diagrama Zentyal

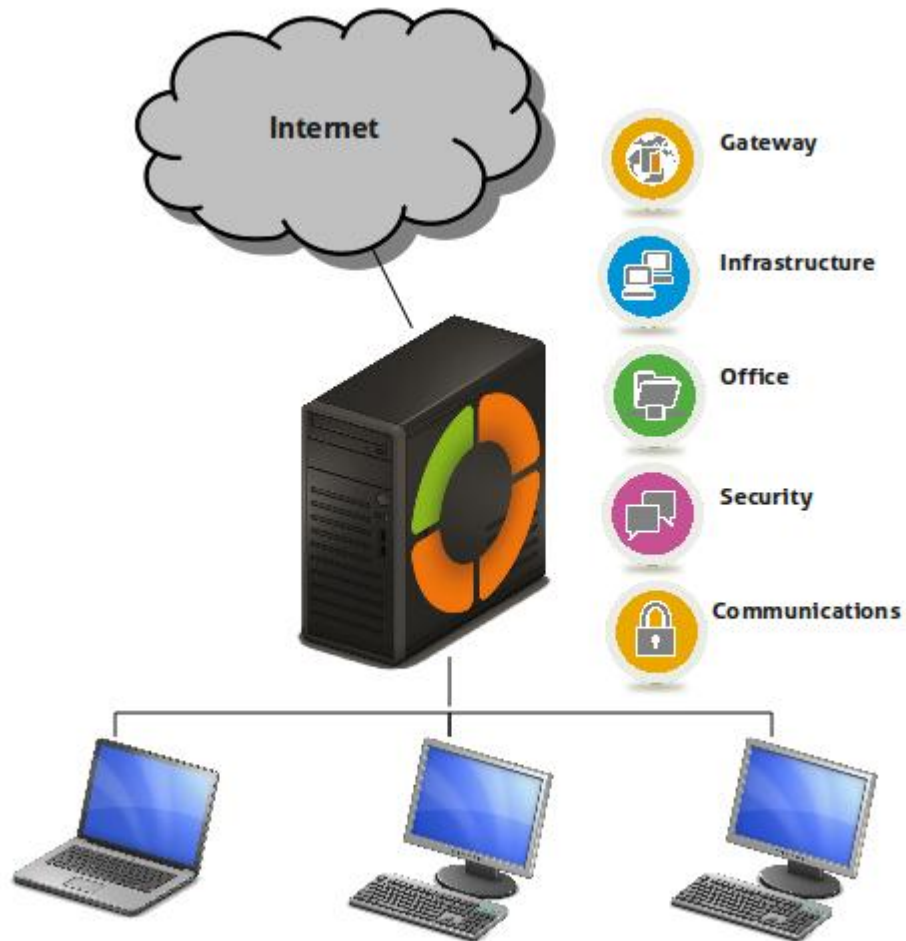


Figura 68. *Diagrama Zentyal*

Fuente: VGS Global. (28 de Septiembre de 2011). *Zentyal una opción al Windows Small Business Server*. Recuperado de: <http://www.vgsglobal.com.ar/blog/2011/09/zentyal-una-opcion-al-windows-small-business-server/>

8.3. IPCop



Figura 69. Logo IPCop

Fuente: Ezquieta, J. (16 de junio de 2013). *Manual del Administrador de IPCop v2.0.0*. Recuperado de: <http://www.ipcop.org/2.0.0/es/admin/html/>

IPCop es un proyecto GNU/GPL o distribución basada en Linux que implementa un cortafuego (o firewall), cuyo único propósito es el de proteger las redes en que está instalado, lo anterior mediante la puesta en marcha como un Cortafuegos, el cual puede ser configurado gracias a la interfaz web que proporciona.

La Herramienta de Software Libre *IPCop*, surge a partir de un grupo de usuarios y desarrolladores, quienes decidieron que implementando tecnología ya existente con nueva tecnología sobresaliente y práctica de programación segura, podría hacer el mejor trabajo para mantener los sistemas seguros.

IPCop tiene como principal objetivo, ser un cortafuego sencillo, administrado a través de una interfaz web, con funcionalidades básicas y avanzadas, como lo es el simple filtrado de paquetes, la asignación de ancho de banda fija a cada equipo de computo y/o la configuración de redes virtuales VPN, entre otras; de igual forma, el administrador podrá instalar módulos adicionales (add-on) que le ofrecerán mayor versatilidad, siendo esto un valor agregado a tener en cuenta.

Dentro de las generalidades de la herramienta, *IPCop* se encuentra limitada en la instalación, debido a que solo trae por defecto las opciones básicas para su función como firewall, limitándose la protección frente a los daños que se podrían presentar; por otra parte permite la implementación de diferentes topologías de red, desde la LAN (Red de área local) que sale a internet, hasta la creación de una Zona Desmilitarizada (DMZ), soportando también la inclusión de una red inalámbrica.

8.3.1 Características Principales de IPCop

IPCop permite gestionar el acceso a Internet, la seguridad y la interacción de hasta cuatro redes distintas que, en la idioma del *IPCop*, se denominan *GREEN*, *BLUE*, *ORANGE* y *RED*, las cuales presentan las siguientes características:

- **GREEN:** *Esta es la interface de red LAN o red de área local, en donde se conectan todos los equipos que necesiten mayor protección, como servidores que no requieren tener presencia en Internet y puestos de trabajo. En otras palabras, estarán protegidos del exterior, en el sentido que no son accesibles desde Internet.*
- **BLUE:** *Es la interface que se asigna normalmente para conectar un access point de modo que se puedan conectar dispositivos inalámbricos. De igual forma se puede utilizar para conectar cualquier otra red que se necesite sea esta inalámbrica o no. No es necesario activar esta interface en una instalación de *IPCop* si no se cuenta con más de una red, o no se va a utilizar un router inalámbrico.*

- **ORANGE:** *Esta es la interface que se utilizará para montar una DMZ o zona desmilitarizada. Principalmente se utiliza para montar servidores web, de correo, de ftp, etc. que deban tener presencia en Internet; o sea que sean accesibles desde Internet, pero que en el caso que se produzca alguna intrusión a algún equipo de esta red, eso no comprometa la seguridad de nuestra red interna (GREEN). No es necesario activar esta interface en una instalación de IPCop si no se piensa utilizar una DMZ.*

- **RED:** *Es la interface de red que permite conectar directamente al proveedor de Internet. Puede ser una conexión ADSL, cable-modem, una línea dedicada o hasta inclusive un modem telefónico común. Por razones de ancho de banda esta última opción es **desaconsejable**, pero es perfectamente factible tenerla configurada para una contingencia en la cual el proveedor de Internet tenga inconvenientes para brindar el vínculo habitual. Cualquier instalación de IPCop contará con esta interface habilitada. En el caso de contar con un router wifi, si bien es conveniente, no es obligatorio que se encuentre conectado a la interface BLUE, ya que se podrá conectar sin problemas a la interface GREEN.*

Las características antes mencionadas de cada interface son las políticas de seguridad que IPCop implementa por defecto, pero no es necesario utilizar las cuatro, ya que se puede configurar de diferentes maneras dependiendo de las necesidades que se tengan.

8.3.2 Características Avanzadas de IPCop

- **USABILIDAD**

Diseño de la Interfaz

La interfaz es muy sencilla en cuanto a diseño, ya que se enfoca más en el cuidado de los datos y la facilidad de acceso que el aspecto.

El diseño de esta interfaz web, está basada en formularios, y su uso de listas desplegadas evita que el usuario deba memorizarlas.

Por último, la representación de los tipos de interfaces mediante colores hace más intuitiva la identificación de una interfaz con su tipo asociado. Además, estos colores van directamente asociados con el riesgo que se asume en cada uno de los tipos, siendo el color rojo para la de mayor riesgo y el verde para la de más confianza.

Facilidad de uso

La administración y configuración de este cortafuego requiere de unos conocimientos más que básicos sobre seguridad informática.

Accesibilidad

Esta herramienta no dispone de herramientas de accesibilidad propias, recurriendo a las incorporadas por el sistema operativo; sin embargo, la representación que se hace de los datos mediante formularios facilita el uso de la interfaz con la ayuda de herramientas de tecnología asistida.

- **PORTABILIDAD / ADAPTABILIDAD**

Plataformas disponibles

La funcionalidad de IPCop está basada en IPTables, incorporado en el framework Netfilter, disponible en todas las plataformas GNU/Linux.

Plugins

IPCop permite ampliar su funcionalidad mediante la inclusión de add-ons o plugins, además de dar la posibilidad a los usuarios de crear los suyos propios y empaquetarlos.

- **RENDIMIENTO**

Requisitos hardware

- ✓ Sistema operativo: IPCop 2.0.4
- ✓ Procesador: 486 o superior
- ✓ Memoria RAM: 64 MB o superior
- ✓ Espacio en disco: 512 MB o superior

8.3.3 Funcionalidad de IPCop

IPCop ofrece una amplia gama de funcionalidades que van más allá de las que ofrecen algunos firewalls comerciales, dentro de las cuales se tienen:

- Acceso seguro por SSL a la interface de administración web
- DHCP cliente / servidor
- DNS dinámico
- Lista de hosts seteable desde la interfase web
- HTTP / FTP proxy (squid)
- IDS (snort) en todas las interfases

- Log local o remoto
- NTP cliente / servidor
- servidor SSH (PSK o con password)
- Traffic shaping (en la interfase RED)
- “Statefull” Firewall
- Módulos “nat helper” para h323, irc, mms, pptp, proto-gre, quake3
- Port forwarding (redireccionamiento de puertos)
- DMZ pin holes
- Activar o desactivar ping en todas las interfases
- VPN (IPSEC)
- Gráficos de monitoreo de CPU, RAM, swap, HD, tráfico de RED, etc.

Dentro de los fallos y/o carencias importantes de ésta Herramienta de Software Libre IPCop, se puede mencionar que la configuración y administración de este cortafuego requiere de conocimientos un poco avanzados, debido a que los menús y opciones que ofrece, no son triviales por la complejidad de los conceptos de seguridad informática utilizados en este.

8.3.4 Diagrama IPCop

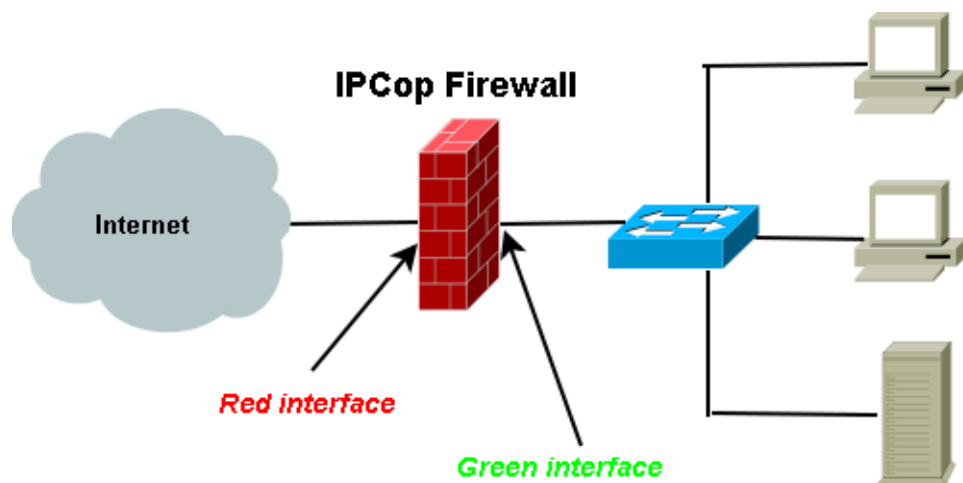


Figura 70. Diagrama IPCop

Fuente: Vazquez, J. (03 de Septiembre de 2008). *IPCop firewall part I: installation*. Recuperado de: <http://pctechtips.org/ipcop-firewall-part-i-installation/>

9. HERRAMIENTA DE SOFTWARE LIBRE SELECCIONADA | PFSense

En base a todo lo relacionado a través de este Proyecto de Investigación, cuyo enfoque se base en una propuesta de implementación de Políticas de Seguridad a través de una Herramienta de Software Libre como instrumento de control y medida informática, que permita mejorar y prevenir el mal uso del Internet, en el Kiosco Vive Digital de la Institución Educativa Eduardo Correa Uribe - Sede La Palma del Municipio de Dosquebradas Risaralda; se pudo determinar en base al capítulo 8 (*Herramientas de Software Libre*), que la mejor opción es *PfSense*, la cual se devela como un instrumento de control y medida de Seguridad Informática que ofrece soluciones para problemas de red y seguridad, permitiendo salvaguardar la información y controlar el uso que se le da al Internet, para así prevenir la afectación de la infraestructura computacional, pero principalmente proteger la integridad de sus usuarios, ya sean niños, adolescentes o la misma comunidad. Además, *PfSense* posee una comunidad activa y en línea que ayuda a resolver las dudas que puedan surgir y contribuir en revisiones constantes; de ahí la importancia de ésta herramienta para el control de contenidos, la protección de los activos que les han sido asignados y para la continuidad del Programa VIVE DIGITAL, que ha sido reconocido internacionalmente como la mejor política TIC del mundo.

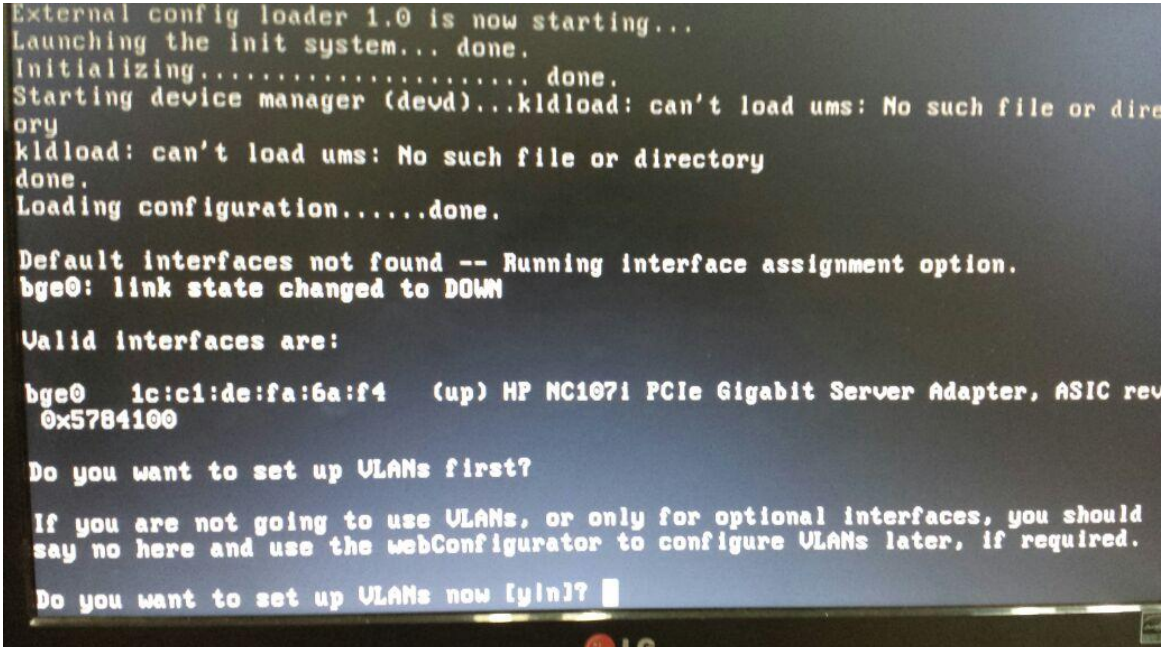
Por último y teniendo en cuenta los factores anteriormente mencionados, se determina que a través de la herramienta *PfSense*, se puede justificar la necesidad de implementar esta propuesta de seguridad informática, ya que no solo contiene los elementos necesarios que permiten disminuir en un grado significativo la falta de seguridad informática a la cual se ven expuestas las redes de datos de los Kioscos VIVE DIGITAL en el municipio de Dosquebradas (Risaralda), sino que también, ofrece el beneficio de no requerirse inversión económica alguna, por ser una herramienta de software libre que cuenta con un modelo de desarrollo y distribución de tipo “*Código Abierto*”, ya que en las Instituciones Educativas Públicas mencionadas no se tienen contempladas inversiones de este tipo dentro de sus presupuestos.

9.1. Instalación de la Herramienta PfSense

El proceso de instalación de la Herramienta de Software Libre *PfSense*, se realizó de la siguiente manera:

- Se arranca el Computador principal o el Servidor desde la unidad de CD, con el fin de que se inicie la secuencia de “Booteo” para la instalación de la Herramienta de Software Libre *PfSense*; visualizándose luego el respectivo menú, en el cual se seleccionó la opción **1**: "*Boot PfSense [Default]*".

Después se muestra un pantallazo como el siguiente, señalando que identificador se le da a las tarjetas de red que se encuentran instaladas y reconocidas por el *PfSense*, las cuales se referencian por el fabricante; al final se pregunta si se desea configurar la VLAN para la red LAN, a lo que se contestó "*No*".



```
External config loader 1.0 is now starting...
Launching the init system... done.
Initializing..... done.
Starting device manager (devd)...kldload: can't load ums: No such file or directory
kldload: can't load ums: No such file or directory
done.
Loading configuration.....done.

Default interfaces not found -- Running interface assignment option.
bge0: link state changed to DOWN

Valid interfaces are:

bge0  1c:c1:de:fa:6a:f4  (up) HP NC1071 PCIe Gigabit Server Adapter, ASIC rev
0x5784100

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]? 
```

Figura 71. Instalación *PfSense* / Configuración de VLANs
Fuente: Autoría propia

- Se continúa con el identificador de las tarjetas de red para diferenciar cual será WAN y LAN respectivamente. Los identificadores pueden varias dependiendo del fabricante de las tarjetas de red.

```
hitting 'a' to initiate auto detection.
Enter the WAN interface name or 'a' for auto-detection: wa
Invalid interface name 'wa'
Enter the WAN interface name or 'a' for auto-detection: wan
Invalid interface name 'wan'
Enter the WAN interface name or 'a' for auto-detection: a
Connect the WAN interface now and make sure that the link is up.
Then press ENTER to continue.
bge0: link state changed to UP
Detected link-up on interface bge0.
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): a
Connect the LAN interface now and make sure that the link is up.
Then press ENTER to continue.
```

Figura 72. *Instalación PfSense | Conexión de la Interface WAN - LAN*

Fuente: Autoría propia

- Luego de configurar el identificador de las tarjetas de red, el sistema confirma si la configuración es correcta, con el fin de poder proceder con la carga de archivos de instalación del *PfSense*, a lo que se contestó "Si".

```
Detected link-up on interface bge0.  
  
Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/NAT mode.  
(or nothing if finished): a  
  
Connect the LAN interface now and make sure that the link is up.  
Then press ENTER to continue.  
ste0: link state changed to UP  
  
Detected link-up on interface ste0.  
  
Enter the Optional 1 interface name or 'a' for auto-detection  
(or nothing if finished):  
  
The interfaces will be assigned as follows:  
  
WAN -> bge0  
LAN -> ste0  
  
Do you want to proceed [y/n]?
```

Figura 73. *Instalación PfSense / Interfaces asignadas WAN – LAN*
Fuente: Autoría propia

- En este paso de la instalación, se muestra la siguiente pantalla con las 17 opciones de la Herramienta PfSense, en la cual se seleccionó la opción **7** (*Ping host*), y se realizó un ping a la dirección www.google.com para verificar que se tuviera acceso a Internet.

```
Starting syslog...done.
Starting CRON... done.
Jul 10 10:10:58 php-fpm[6674]: /rc.start_packages: Restarting/Starting all packa
ges.
pfSense (pfSense) 2.2.2-RELEASE amd64 Mon Apr 13 20:10:22 CDT 2015
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.2-RELEASE-pfSense (amd64) on pfSense ***

WAN (wan)      -> bge0      -> v4/DHCP4: 192.168.1.77/24
LAN (lan)      -> ste0      -> v4: 192.168.1.1/24
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) pfSense Developer Shell
4) Reset to factory defaults  13) Upgrade from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Figura 74. *Instalación PfSense / Ventana de Bienvenida de PfSense*
Fuente: Autoría propia

- En la siguiente figura se muestra el inicio de la instalación de *PfSense* en el Disco Duro; en la cual se seleccionó la opción “*Accept these Settings*”, comenzando inmediatamente el formateo del disco duro y la copia de los archivos del sistema.

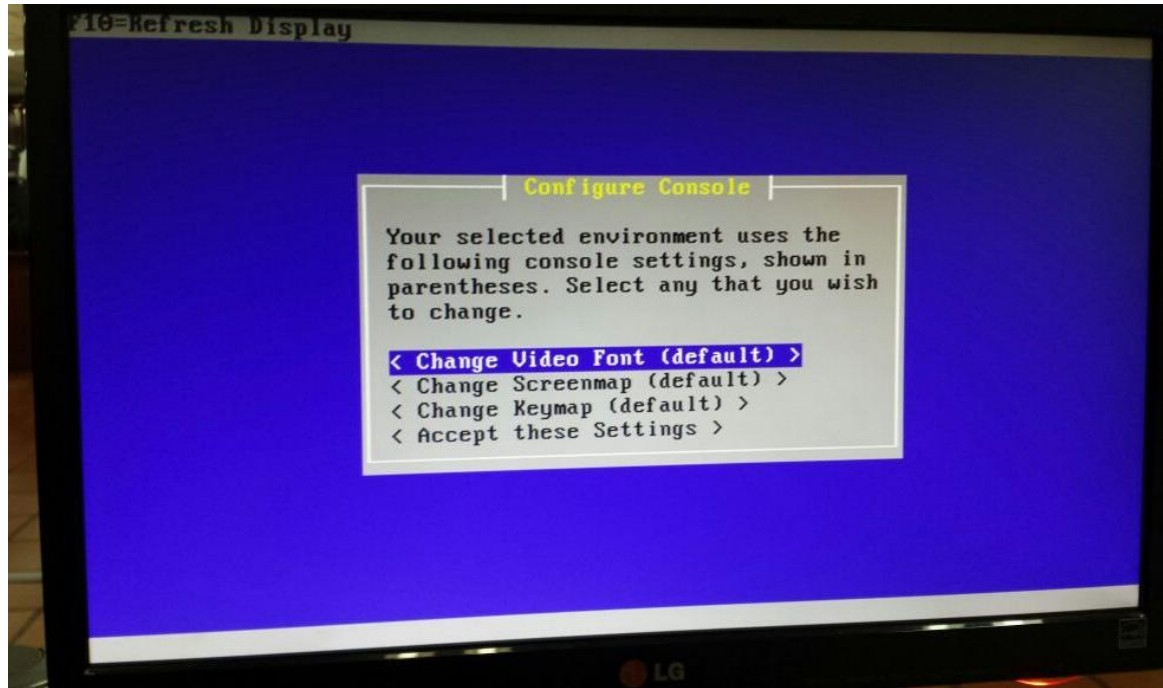


Figura 75. *Instalación PfSense / Configuración de la Consola*
Fuente: Autoría propia

- Luego saldrá la siguiente pantalla, en donde se pregunta qué tipo de instalación se quiere aplicar al Computador o Servidor, a lo cual se selecciona la opción “Quick/Easy Install”.

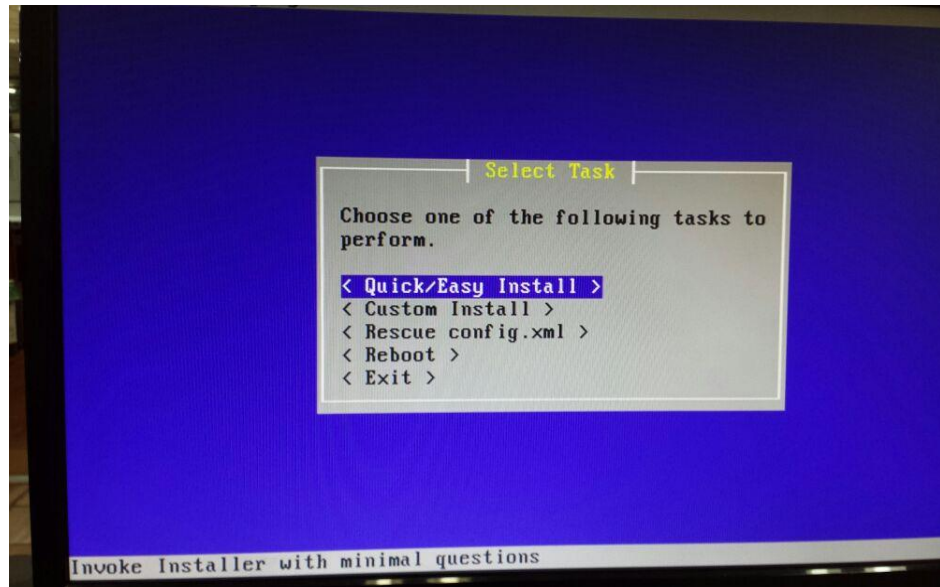


Figura 76. Instalación PfSense / Tarea a Realizar
Fuente: Autoría propia

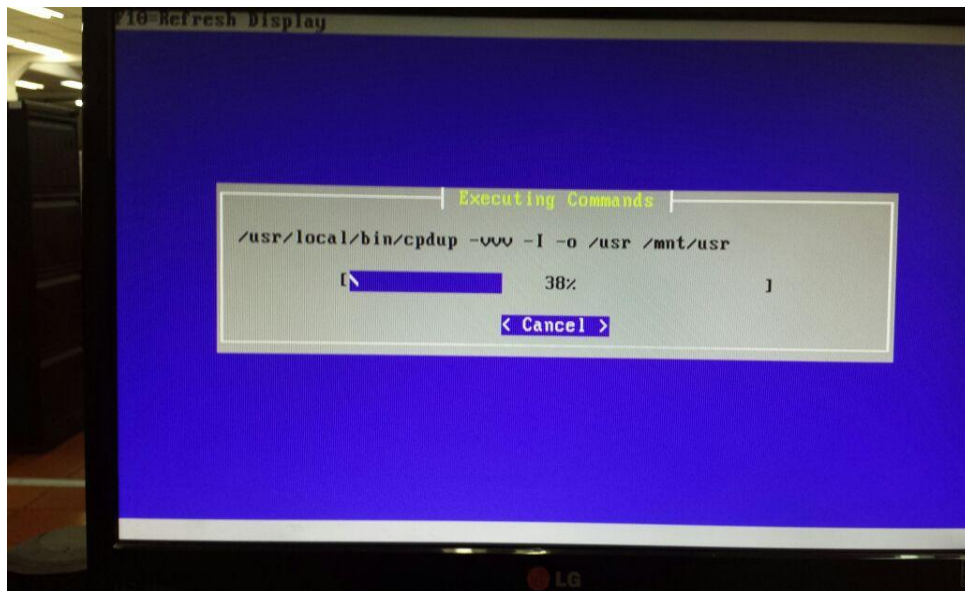


Figura 77. Instalación PfSense / Ejecución de Comandos
Fuente: Autoría propia

- Se continúa con la selección de la opción “OK”, como se muestra en la siguiente figura, para dar por terminado el proceso de instalación del *PfSense* en el Computador o Servidor destinado.

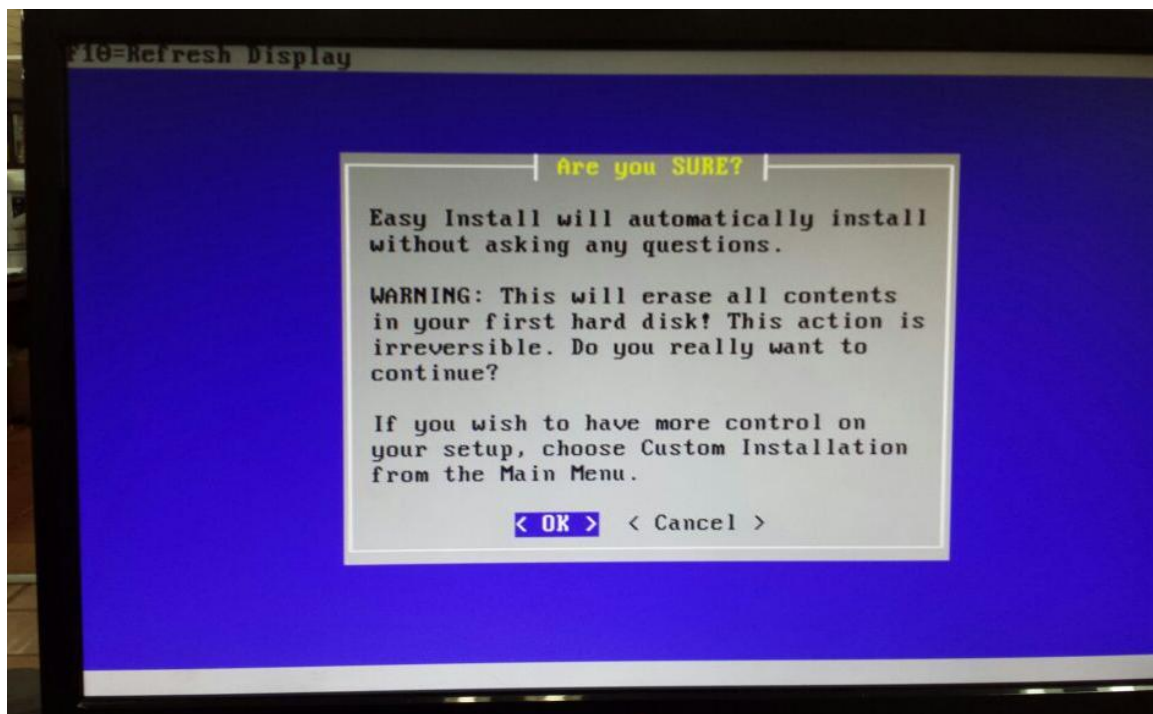


Figura 78. *Instalación Pfsense / Ventana de Confirmación*
Fuente: Autoría propia

- Por último, se seleccionó la opción “*Reboot*”, para reiniciar el Computador.

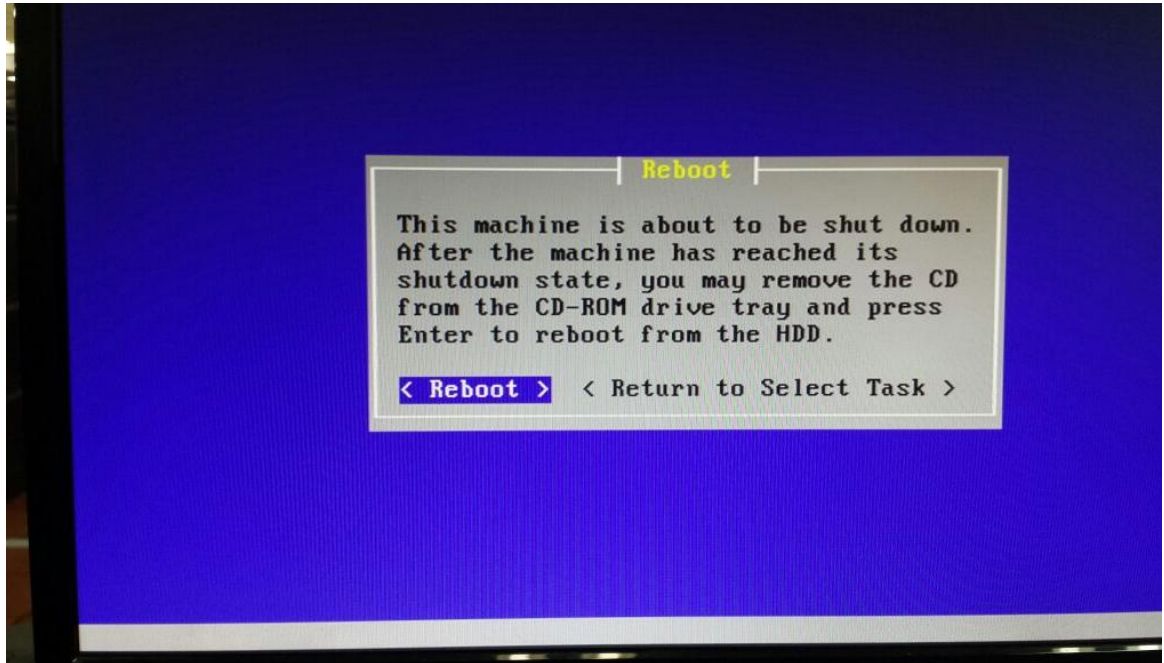


Figura 79. *Instalación PfSense / Reinicio*
Fuente: Autoría propia

- Hasta este punto, se evidencia la Instalación en el Disco Duro, reiniciándose el Computador con el *Usuario: admin* y la *Clave: pfsense* por defecto, como lo muestra la siguiente figura.

```
After the reboot is complete, open a web browser and
enter https://192.168.1.1 (or the LAN IP Address) in the
location bar.

You might need to acknowledge the HTTPS certificate if
your browser reports it as untrusted. This is normal
as a self-signed certificate is used by default.

•DEFAULT Username=: admin
•DEFAULT Password=: pfsense

Rebooting in 5 seconds. CTRL-C to abort.
Rebooting in 4 seconds. CTRL-C to abort.
Rebooting in 3 seconds. CTRL-C to abort.
Rebooting in 2 seconds. CTRL-C to abort.
Rebooting in 1 second.. CTRL-C to abort.

pfSense is now rebooting.

Waiting (max 60 seconds) for system process `valra' to stop...done
Waiting (max 60 seconds) for system process `bfd daemon' to stop...done
Waiting (max 60 seconds) for system process `syncer' to stop...
```

Figura 80. *Instalación PfSense / Secuencia de Reinicio*
Fuente: Autoría propia

9.2. Configuración y Pruebas de la Herramienta PfSense

- En este paso se conecta desde otro equipo a la red LAN, para administrar gráficamente el web configurator del *PfSense*.

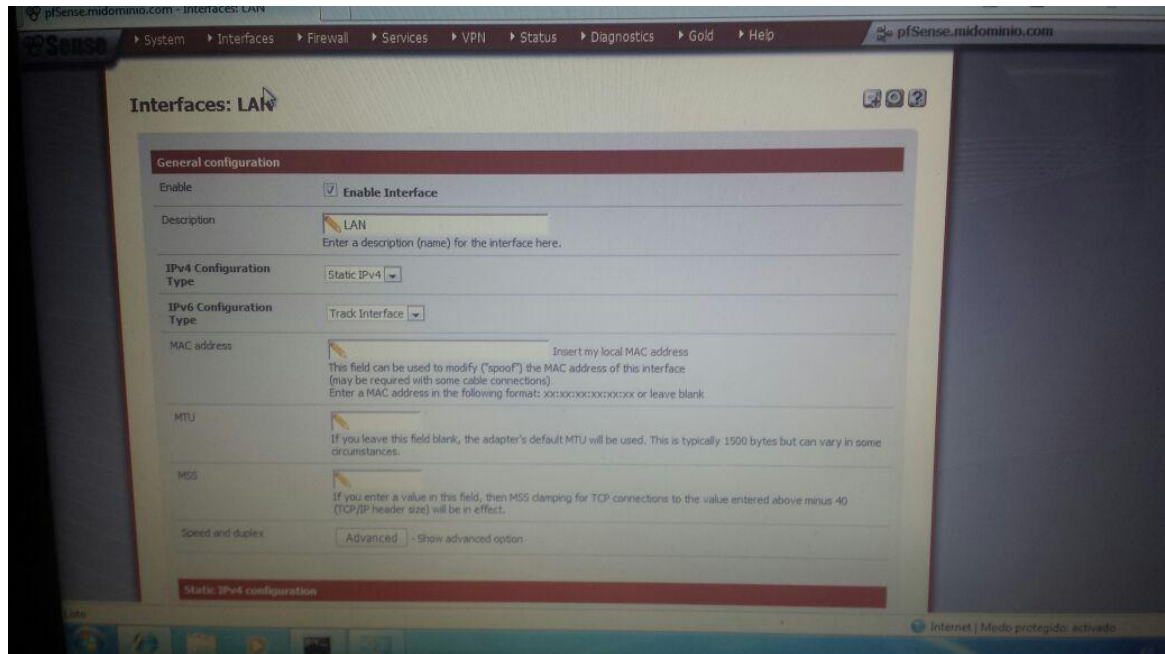


Figura 81. Configuración PfSense / Interface: LAN

Fuente: Autoría propia

- En la siguiente figura, se evidencia que el Servidor está entregando dinámicamente las direcciones IP en un rango de 192.168.2.10 a 192.168.2.145.

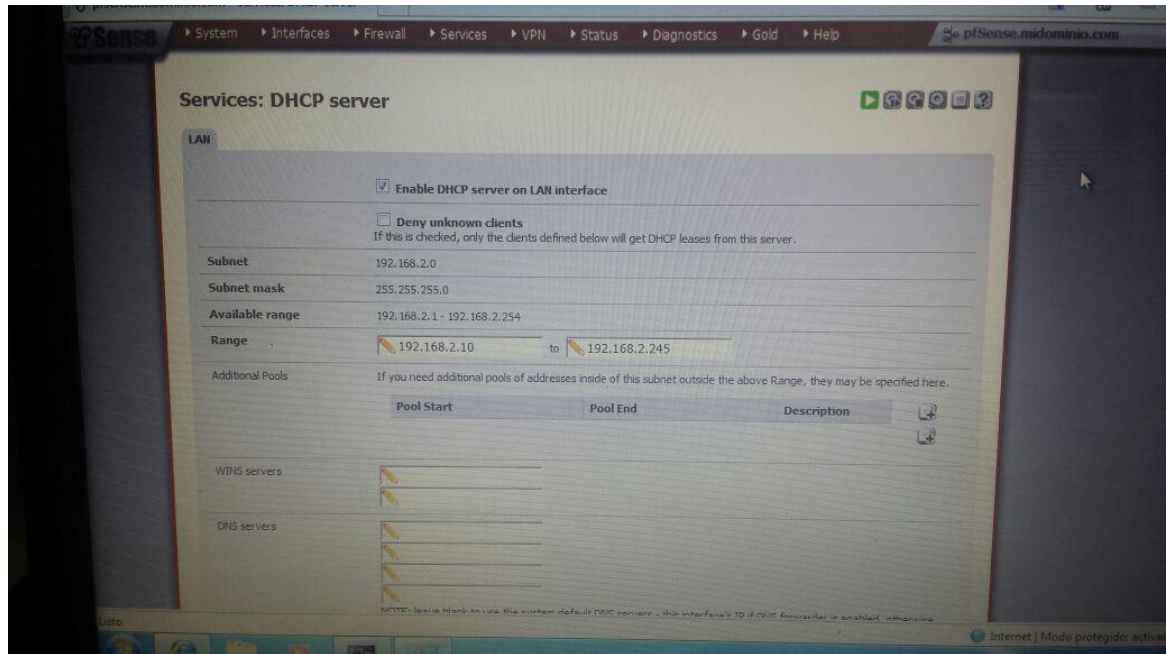


Figura 82. Configuración PfSense / Servicios: Servidor DHCP
Fuente: Autoría propia

- En este paso, se ve gráficamente la configuración del Servidor, la configuración de las Interfaces y del *PfSense*, como por ejemplo la versión instalada.

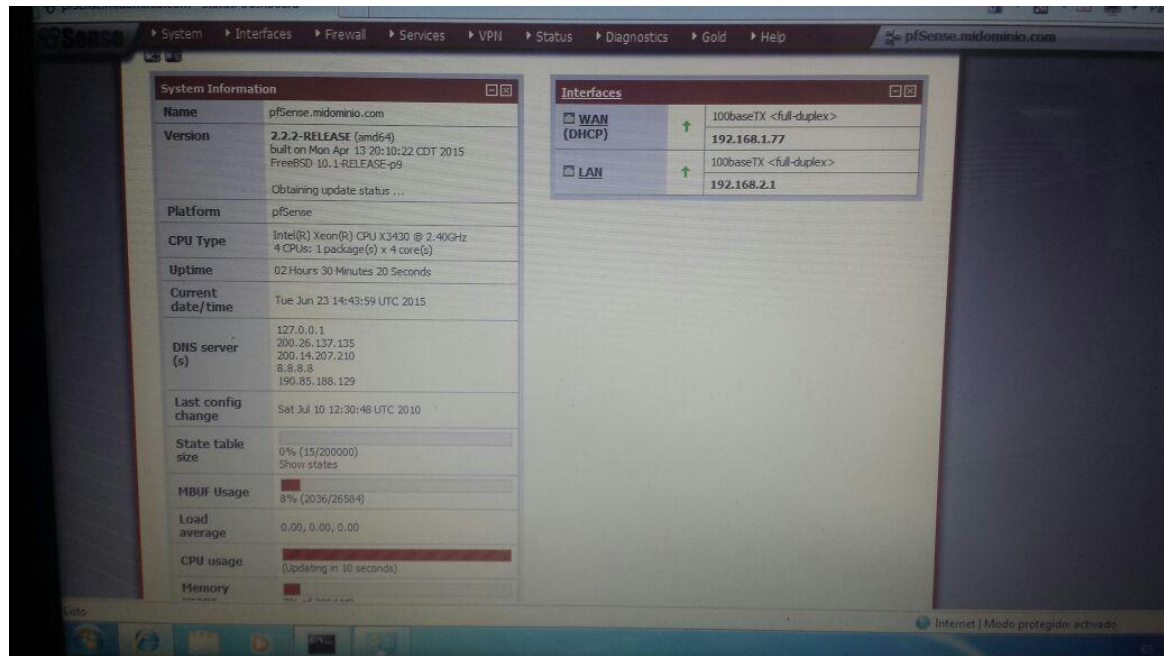


Figura 83. Configuración PfSense / Información del Sistema - Interfaces
Fuente: Autoría propia

- Como se evidencia en la siguiente figura, se muestran algunos paquetes con los que cuenta *PfSense*, los cuales se recomienda ser instalados, según las necesidades puntuales que se tengan; en este caso se seleccionó instalar el “*Squid*” y el “*SquidGuard*”.

Squid: Es un paquete que ofrece *PfSense*, el cual se instala para configurar los acceso desde las diferentes paginas. Entre sus utilidades está la de mejorar el rendimiento de las conexiones a Internet guardando en caché peticiones recurrentes a servidores web y DNS, acelerar el acceso a un servidor web determinado o añadir seguridad realizando filtrados de tráfico.

SquidGuard: Es un redirector URL utilizada para utilizar Listas Negras con el proxy software *Squid* . Cuenta con dos grandes ventajas, es rápido y es gratis. *SquidGuard* se presenta bajo licencia pública GNU.

spamd	Services	Beta 1.1.2 platform: 2.2 2.2.999	<p>network interface or by reading a packet capture file. These flows may be reported via NetFlow to a collecting host or summarised within softflowd itself. Softflowd supports Netflow versions 1, 5 and 9 and is fully IPv6-capable - it can track IPv6 flows and send export datagrams via IPv6. It also supports export to multicast groups, allowing for redundant flow collectors.</p> <p>No package info, check the forum</p> <p>Tarbits like spamd are fake SMTP servers, which accept connections but don't deliver mail. Instead, they keep the connections open and reply very slowly. If the peer is patient enough to actually complete the SMTP dialogue (which will take ten minutes or more), the tarbit returns a 'temporary error' code (4xx), which indicates that the mail could not be delivered successfully and that the sender should keep the mail in their queue and retry again later.</p>
squid	Network	Stable 2.7.9 pkg v.4.3.6 platform: 2.2 2.2.999	<p>No package info, check the forum</p> <p>High performance web proxy cache.</p> <p>No package info, check the forum</p>
squid3	Network	beta 0.2.8 platform: 2.2	<p>High performance web proxy cache. It combines squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, ssl filtering and antivirus integration via i-cap</p> <p>Package info</p>
squidGuard	Network Management	Beta 1.9.14 platform: 2.2	<p>High performance web proxy URL filter. Works with both Squid 2.x and Squid 3.x.</p> <p>No package info, check the forum</p>
squidGuard-devel	Network Management	Beta 1.5_beta pkg v.1.5.6 platform: 2.2 2.2.999	<p>High performance web proxy URL filter. Requires proxy Squid 2.x package.</p> <p>No package info, check the forum</p>

Figura 84. Configuración *PfSense* / Selección de Paquete *Squid*

Fuente: Autoría propia

- En la siguiente figura, se muestra el proceso de instalación del paquete de *Squid* y su versión 2.7.9_4-amd64.pbi, con el fin de bloquear listas negras.

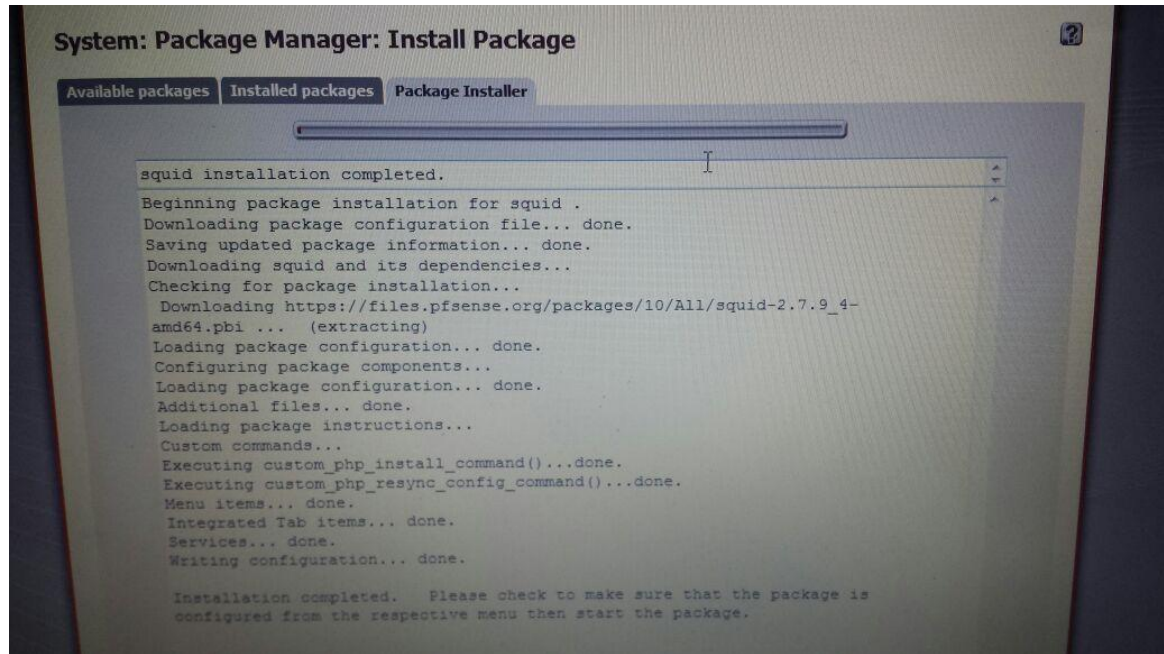


Figura 85. Configuración PfSense / Instalación Paquete Squid
Fuente: Autoría propia

- El siguiente paso realizado, fue el de adicionar la Herramienta ***Shalla Secure Services***, el cual es una colección de Listas Negras agrupadas por categoría para ser utilizadas dentro del paquete *SquidGuard*. Esta herramienta nos presenta 74 categorías de bloqueo en diferentes campos como:
 - ✓ ***Agresivo***: Sitios de contenido agresivo obvio y explicito. Se encuentran discursos de odio, insultos, agresiones y todo tipo de racismo.
 - ✓ ***Alcohol***: Sitios de cervecerías, bodegas, distribuidores y destilerías. Esta categoría incluye los sitios que explican cómo se hace la cerveza, vinos y licores.
 - ✓ ***Jugar***: Sitios que ofrecen la posibilidad de ganar dinero, pero solo para mayores de edad, como Póker, Casino, Bingo y otros juegos de azar, así como los sitios de apuestas. Se diferencia de la opción de *manía / juegos* en el aspecto de ganar o perder dinero o ser atraídos a hacerlo.
 - ✓ ***Pornografía/Pedofilia***: Sitios sobre todo tipo de contenido sexual que van desde los desnudos parciales o totales, hasta la pornografía, pedofilia, hardcore, Sex Movies, entre muchos otros contenidos.
 - ✓ ***Sexo / Ropa interior***: Sitios de venta y presentación de ropa interior sexy o lencería de una manera atractiva, pero que de cierta forma incitan de forma directa el Sexo.
 - ✓ ***Violencia***: Sitios sobre homicidios, suicidios, accidentes violentos y daños a personas.

- ✓ **Armas:** Sitios que ofrecen todo tipo de armas, accesorios para las mismas, y todo lo relacionado a este entorno, tales como: Cuchillos, Espadas, Armas de fuego, Arcos, Tiendas, Armería, así como los sitios que contienen información general sobre su fabricación y uso.

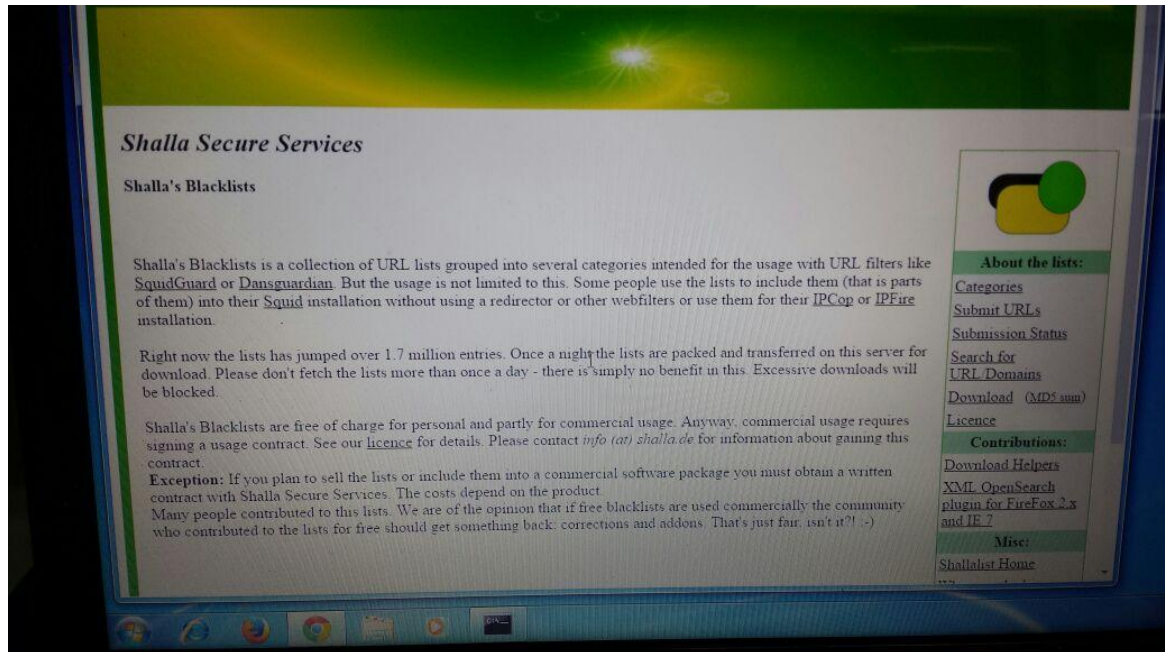


Figura 86. Configuración PfSense / Selección de Bloqueo Listas Negras
Fuente: Autoría propia

- Con la siguiente figura, se evidencia cómo fue la instalación del paquete de *shallalist.tar.gz* al *SquidGuard*.

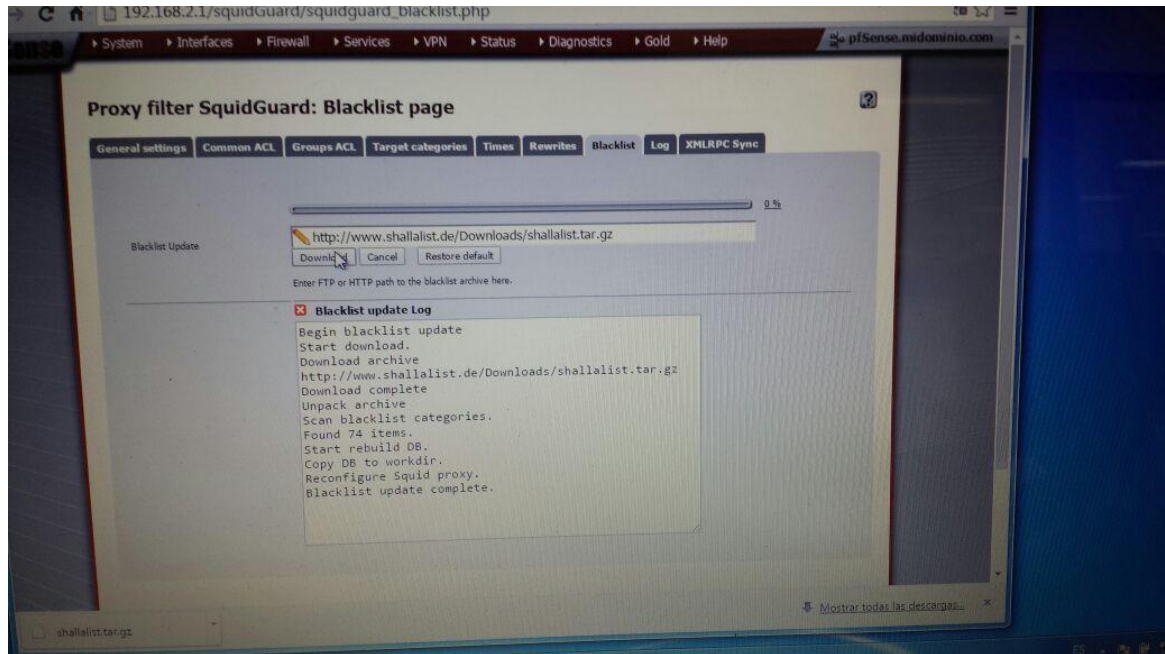


Figura 87. Configuración PfSense | Inicio Actualización Listas Negras
Fuente: Autoría propia

- En esta gráfica se pueden ver las categorías que ofrece el *Shalla*, para ser seleccionadas la que se desean bloquear.

Como ejemplo se muestra el bloquea que se le realiza a una categoría de Porno:
[blk_BL_porn] ... Access deny

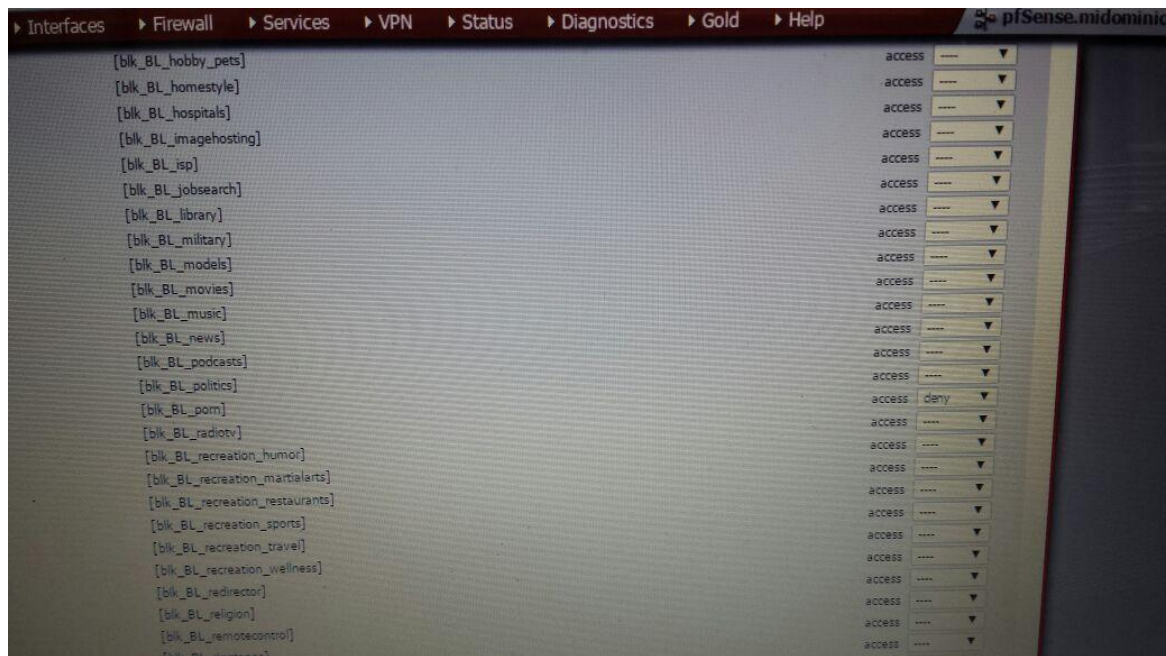


Figura 88. Configuración PfSense / Acceso de Servicios
Fuente: Autoría propia

- Como evidencia del paso anterior, se muestra en la siguiente figura cómo fue bloqueado el acceso a la página www.youporn.com

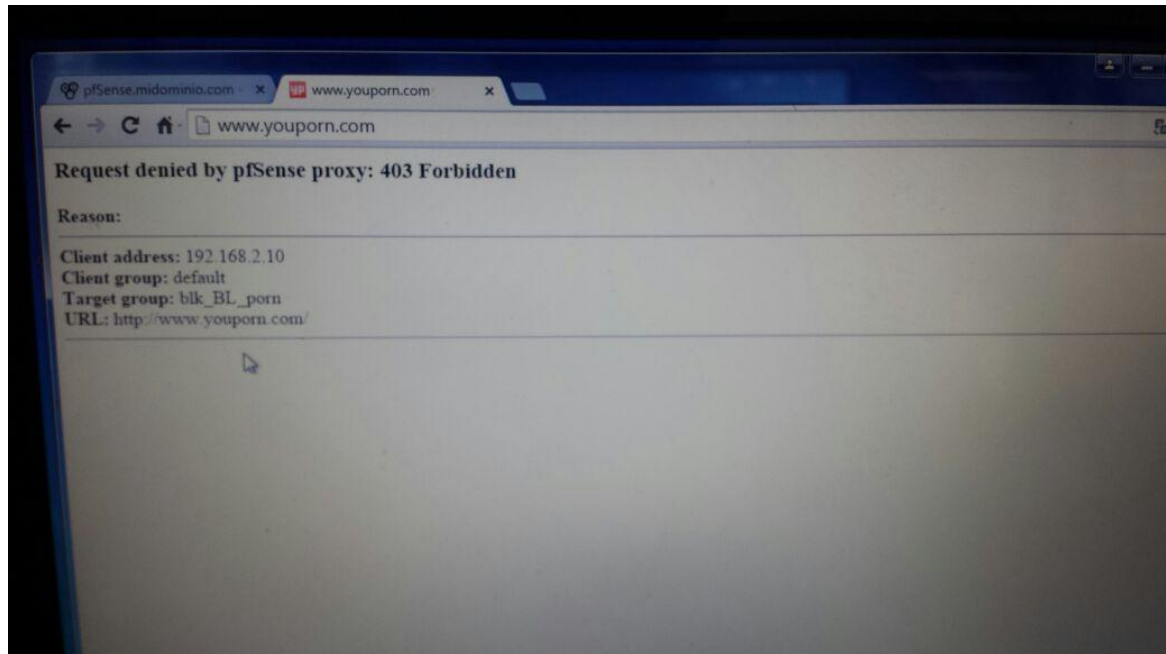


Figura 89. Configuración PfSense / Prueba de acceso a una página de porno
Fuente: Autoría propia

- Dentro de las Herramientas adicionales para configurar Pfsense, se encuentra **HAVP Antivirus**, tal y como se evidencia en la siguiente figura, que combinado con Antivirus gratuitos para Linux, reduce el riesgo de ser víctimas de ataques al navegar por Internet en un PC con Windows.

Package Name	Category	Version	Description
haproxy	Services	platform: 2.2	haproxy. Supports ACLs for smart backend switching. Package info
haproxy-devel	Services	Release 0.24 platform: 2.2	The Reliable, High Performance TCP/HTTP(S) Load Balancer This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Supports ACLs for smart backend switching. Package info
HAVP antivirus	Network Management	BETA 0.91_3 pkg v1.05_1 platform: 2.2 2.2.999	Antivirus: HAVP (HTTP Antivirus Proxy) is a proxy with a ClamAV anti-virus scanner. The main aims are continuous, non-blocking downloads and smooth scanning of dynamic and password protected HTTP traffic. Havn antivirus proxy has a parent and transparent proxy mode. It can be used with squid or standalone. And File Scanner for local files. No package info, check the forum
iftop	Services	Beta 0.17 platform: 2.2	Realtime interface monitor (console/shell only) Package info
inspector	Network Management	BETA 0.3.2 platform: 2.2 2.2.999	IMInspector is an Instant Messenger transparent proxy with logging capabilities. Currently it supports MSN, AIM, ICQ, Yahoo and IRC to different degrees. Package info
iperf	Network Management	Beta	Iperf is a tool for testing network throughput, loss, and jitter.

Figura 90. Configuración PfSense / Herramientas adicionales: HAVP Antivirus
Fuente: Autoría propia

- En la siguiente figura, se muestra el proceso de instalación del paquete de HAVP Antivirus.

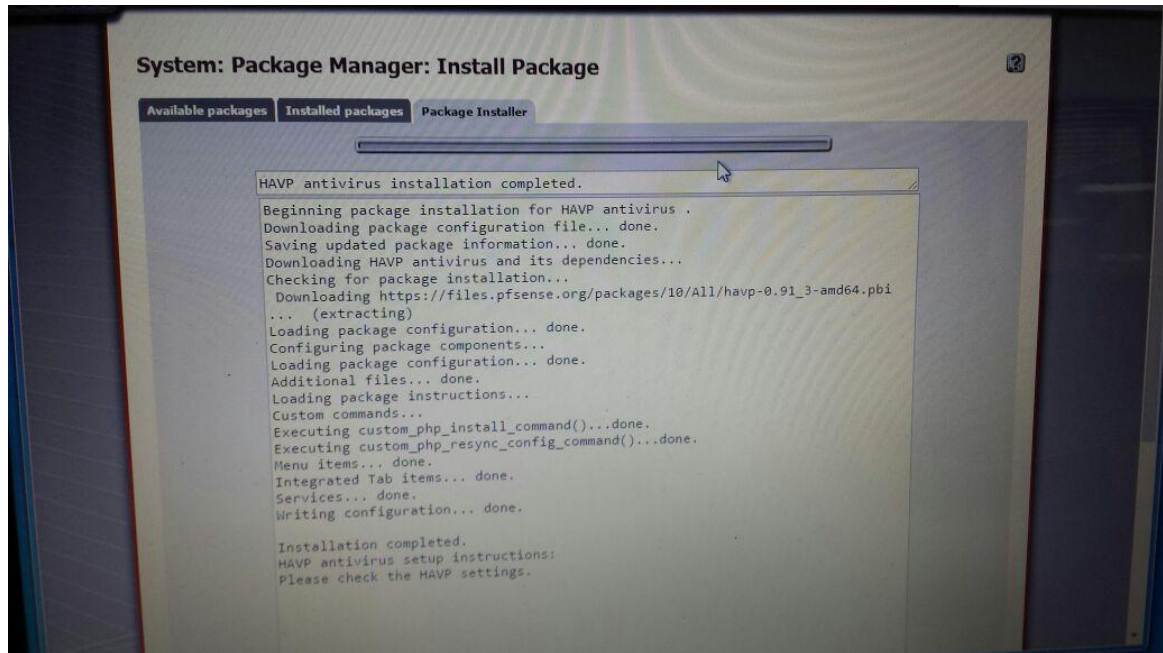


Figura 91. Configuración PfSense / Instalación del paquete HAVP Antivirus
Fuente: Autoría propia

- Después de la instalación de la herramienta HAVP Antivirus, se procede a la configuración, activación y actualización del mismo, como se muestra en la siguiente figura.

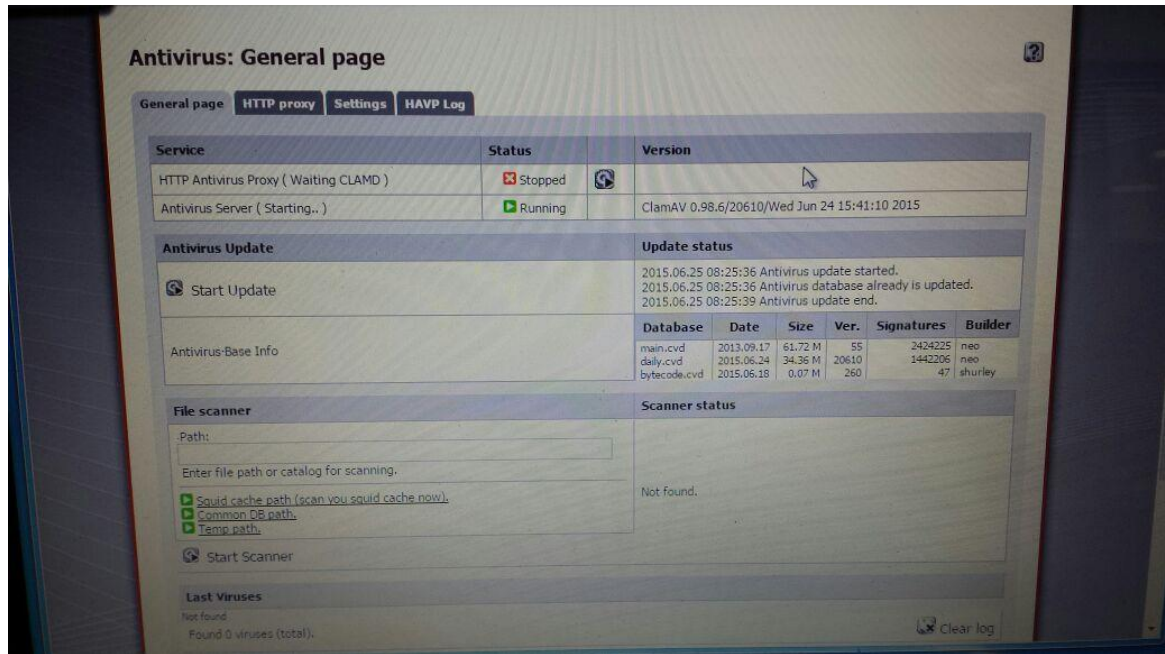


Figura 92. Configuración PfSense | Página General de HAVP Antivirus
Fuente: Autoría propia

- Otra herramienta seleccionada para las pruebas, fue **MailScanner**, la cual escanea correo electrónico en busca de virus, spam, phishing, malware y otros ataques contra las vulnerabilidades de seguridad, desempeñando un papel importante en la seguridad de una red.

		platform: 2.2 2.2.999	Package info
Lightsquid	Network Report	RC1 2.41 platform: 2.2	High performance web proxy report (LightSquid). Proxy realtime stat (SQStat). Requires squid HTTP proxy. No package info, check the forum
mailreport	Network Management	Stable 2.3 platform: 2.2	Allows you to setup periodic e-mail reports containing command output, log file contents, and RRD graphs. No package info, check the forum
mailscanner	Services	beta 0.2.12 platform: 2.2 2.2.999	MailScanner is an e-mail security and anti-spam package for e-mail gateway systems. This is a level3 mail scanning tool with high CPU load. Package info
mtr-nox11	Network Management	Stable 0.85_2 platform: 2.2	Enhanced traceroute replacement No package info, check the forum
netio	Network Management	ALPHA 1.26 platform: 2.2 2.2.999	This is a network benchmark for DOS, OS/2 2.x, Windows NT/2000 and Unix. It measures the net throughput of a network via NetBIOS and/or TCP/IP protocols (Unix and DOS only support TCP/IP) using various different packet sizes. No package info, check the forum
nmap	Security	Stable 1.3 platform: 2.2	NMap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques (determine what services the hosts are offering), version detection (determine what application/service is running on a port), and TCP/IP fingerprinting (remote host OS or device identification). It also offers flexible target and port specification, decoy/stealth scanning, SunRPC scanning, and

Figura 93. Configuración PfSense / Herramientas adicionales: MailScanner
Fuente: Autoría propia

- Con la siguiente figura, se evidencia la instalación del paquete de *MailScanner*

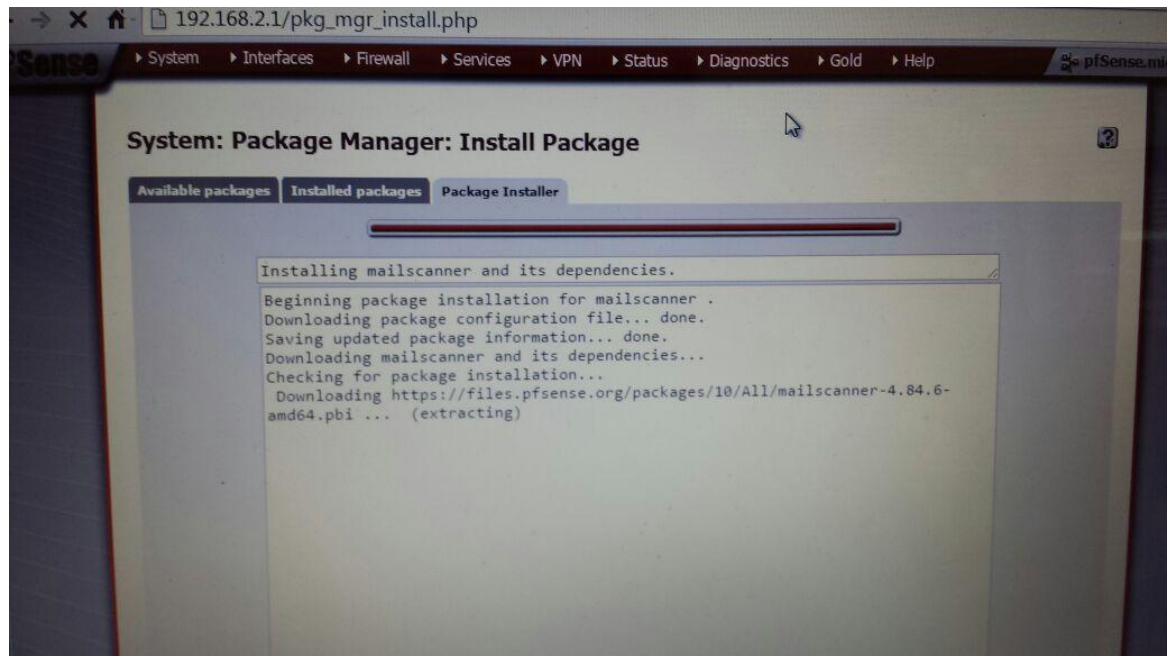


Figura 94. Configuración PfSense | Instalación del paquete MailScanner
Fuente: Autoría propia

- Continuando con las pruebas, se seleccionó la herramienta *Dansguardian*, la cual es un software de filtro de contenido, diseñado para controlar el acceso a sitios web, como es el caso de Facebook.

Dansguardian incluye un filtro de virus, importante en Sistemas Operativos Windows, usado principalmente en instituciones de educación, gobierno y empresas.

Con la siguiente figura, se evidencia la instalación del paquete *Dansguardian*.

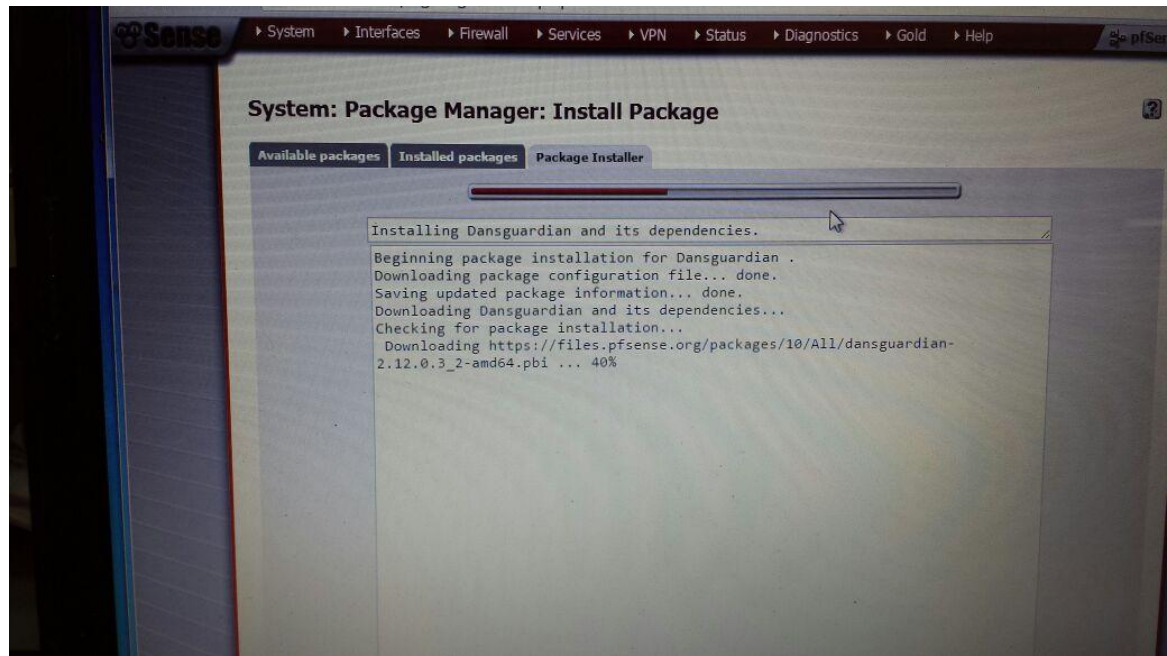


Figura 95. Configuración PfSense / Instalación del paquete Dansguardian
Fuente: Autoría propia

- En la siguiente figura se muestran algunas reglas configuradas dentro del Firewall *PfSense*, como el bloque de Facebook.

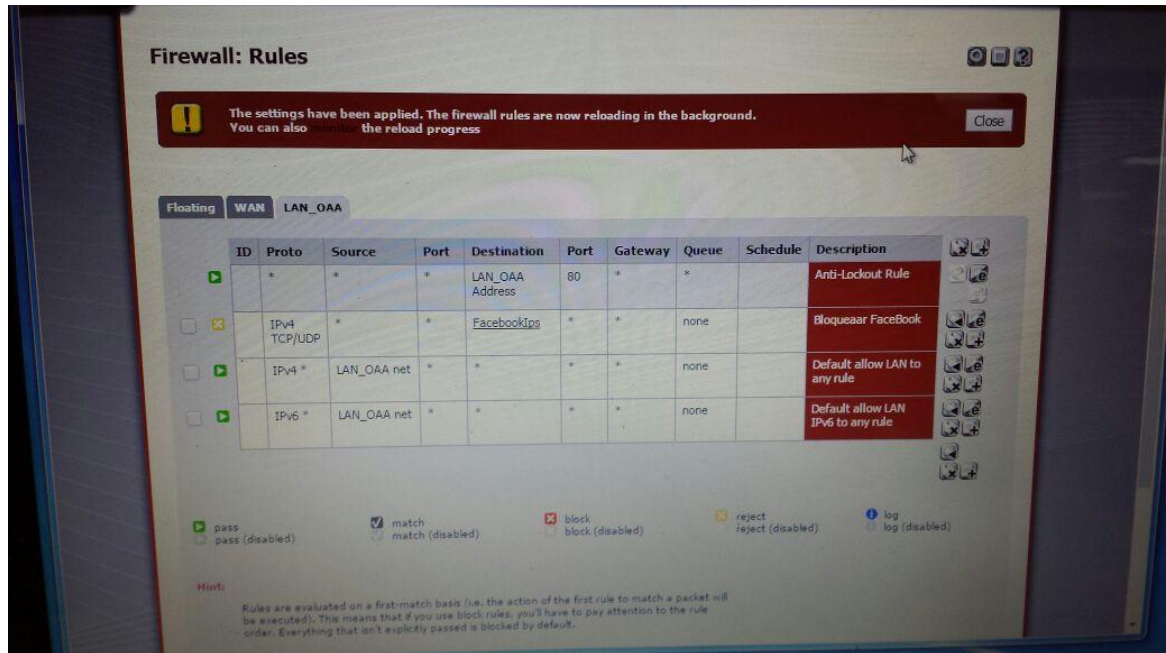


Figura 96. Configuración PfSense / Algunas reglas dentro del Firewall Pfsense
Fuente: Autoría propia

- Como evidencia del paso anterior, se muestra en la siguiente figura cómo fue bloqueado el acceso a la página www.facebook.com

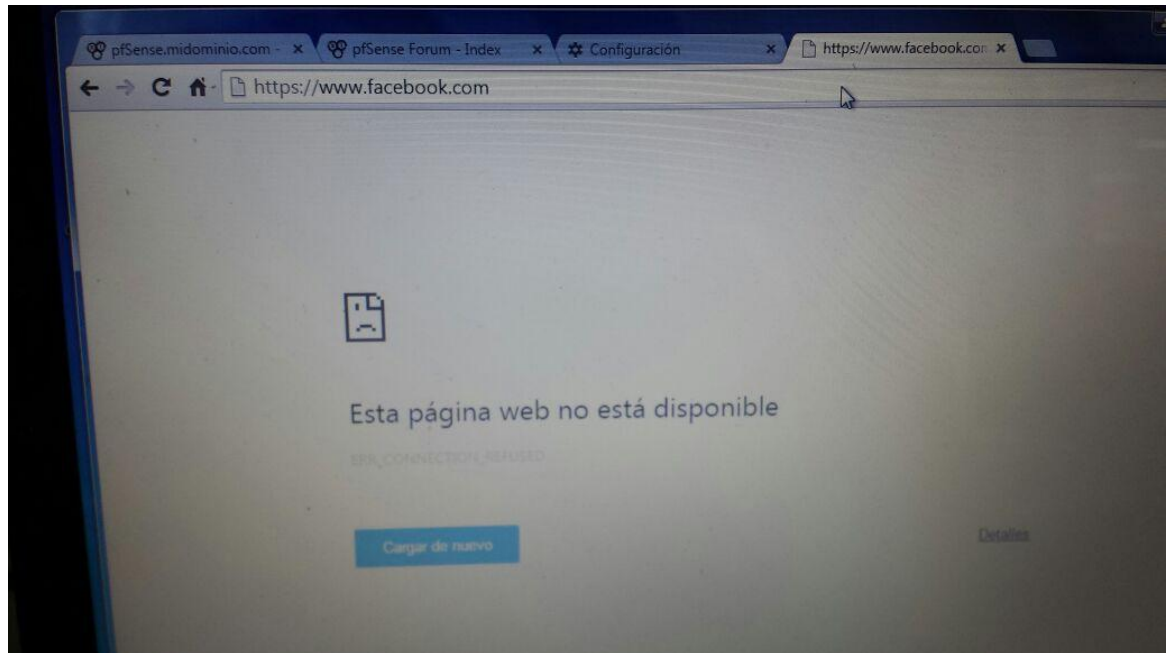


Figura 97. Configuración PfSense / Prueba de acceso a facebook
Fuente: Autoría propia

- Para finalizar, se muestran en la siguientes figuras, algunos de los diferentes servicios que también ofrece la herramienta **Pfsense**, los cuales pueden ser instalados si se requieren.

Package Name	Category	Version	Description
OpenBGPD	NET	STABLE 0.9.3_3 platform: 2.2	OpenBGPD is a FREE implementation of the Border Gateway Protocol, Version 4. It allows ordinary machines to be used as routers exchanging routes with other systems speaking the BGP protocol. -- WARNING! Installs files to the same place as Quagga OSPF. Installing both will result in a broken state, remove this package before installing Quagga OSPF.
OpenVPN Client Export Utility	Security	RELEASE 1.2.16 platform: 2.2	Allows a pre-configured OpenVPN Windows Client or Mac OSX's Viscosity configuration bundle to be exported directly from pfSense. No package info, check the forum
pfBlockerNG	Firewall	Stable 1.09 platform: 2.2	pfBlockerNG is the Next Generation of pfBlocker. Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. Country Blocking Database by MaxMind Inc. (GeoLite Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Emerging Threats IQRisk IP Reputation Threat Sources.
pfflowd	Network Management	Stable 1.0.3 platform: 2.2	pfflowd converts OpenBSD PF status messages (sent via the pfsync interface) to Cisco NetFlow datagrams. These datagrams may be sent (via UDP) to a host of one's choice. Utilising the OpenBSD stateful packet filter infrastructure means that flow tracking is very fast and accurate. No package info, check the forum
PHPService	Services	Beta 0.4.2 platform: 2.2.999	PHP run as a service it can do anything PHP can do including but not limited to monitoring files, CPU, RAM, and send alerts to the syslog.

Figura 98. Configuración PfSense / Herramientas adicionales de PfSense 01
Fuente: Autoría propia

Package Name	Category	Version	Description
Service Watchdog	Services	Release 1.6 platform: 2.2	Monitors for stopped services and restarts them. No package info, check the forum
Shellcmd	Services	Beta 0.6 platform: 2.2	The shellcmd utility is used to manage commands on system startup. No package info, check the forum
siproxd	Services	Beta 1.0.3 platform: 2.2	Proxy for handling NAT of multiple SIP devices to a single public IP.
snort	Security	Stable 3.2.5 platform: 2.2	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
softflowd	Network Management	Beta 1.1 platform: 2.2	Softflowd is flow-based network traffic analyser capable of Cisco NetFlow data export. Softflowd semi-statefully tracks traffic flows recorded by listening on a network interface or by reading a packet capture file. These flows may be reported via NetFlow to a collecting host or summarised within softflowd itself. Softflowd supports Netflow versions 1, 5 and 9 and is fully IPv6-capable - it can track IPv6 flows and send export datagrams via IPv6. It also supports export to multicast groups, allowing for redundant flow collectors. No package info, check the forum

Figura 99. Configuración PfSense / Herramientas adicionales de PfSense 02
Fuente: Autoría propia

10. PROPUESTA DE IMPLEMENTACIÓN

Con el fin de poder realizar la propuesta de implementación, en base a todo lo expuesto durante el desarrollo de este Proyecto de Investigación; se relacionan a continuación los siguientes criterios con los cuales se seleccionó la Herramienta *PfSense*, como Software Libre que proporcionará Políticas de Seguridad informática para el Kiosco Vive Digital de la Institución Educativa Eduardo Correa Uribe - Sede La Palma del Municipio de Dosquebradas Risaralda.

10.1. Criterios de Selección de la Herramientas PfSense

Los criterios por los cuales fue seleccionada *PfSense* como Política de Seguridad Informática a través de esta Herramienta de Software Libre, son:

- *PfSense* es una distribución personalizada de FreeBSD el cual se deriva de Unix que funciona como Firewall, Router, Servidor de Balanceo de Carga, Portal Cautivo, Servidor VPN, DDNS, DHCP, entre otras, que cuenta con un software explícito para seguridad informática, adaptado para ser usado en servicios de redes LAN y WAN.
- *PfSense* está soportado comercialmente por BSD Perimeter INC; el cual ofrece, de ser requerido, acompañamiento y asesoría especializada, como solución de Seguridad Informática para redes LAN y WAN.
- No se requieren conocimientos avanzados, en cuanto a líneas de comandos de BSD para poder manejar la Herramienta *PfSense*.

- Cuenta con un gestor de paquetes desde su interfaz gráfica, para ampliar sus funcionalidades, el cual sólo requiere la elección el paquete deseado, puesto que el mismo sistema lo descarga y lo instala automáticamente.
- Se puede acceder a la GUI (*Interfaz Gráfica de Usuario*) de Pfsense a través de cualquier explorador de internet (IE, Mozilla, Chrome etc.)
- *PfSense* se puede instalar sobre cualquier arquitectura de PC o Servidor, ya que cuenta con dos versiones de arquitectura, la **i386** que es compatible con computadores de 32 bits y la **amd64** la cual funciona a 64 bits, pero esta última puede necesitar más memoria, aunque dará mejor rendimientos.
- Es una solución de seguridad de código abierto, es decir que cualquier desarrollador puede añadir mejoras al S.O bajo ciertas condiciones legales.
- *PfSense* cuenta con reglas de Nateo (*Network Address Translation*) que permiten redireccionar el tráfico entrante y enmascaramiento de Ip. Existen dos tipos de reglas para nateo que son : PREROUTING que son las que me permitir el redireccionamiento del trafico entrante y POSTROUTING que son las que permiten enmascarar la red LAN con la dirección Ip publica y así poder salir a internet.
- *PfSense* como firewall, puede controlar todo el tráfico que se va a trasmitir de una red a otra red, mediante reglas que permiten o deniegan servicios.

- Al implementar un elemento de red como lo es *PfSense*, se brinda más seguridad en la LAN/WAN al momento de utilizar Internet, debido a que puede controlar el tráfico, restringir el uso de Internet por Ip, filtrar y bloquear contenido de páginas, entre otros; de esta forma serán menos las posibilidades de ataques hacia la red.
- *PfSense* cuenta con dos plataformas: **Live-Cd**, el cual se puede ejecutar directamente desde el CD, aunque también permite ser instalado en el disco duro del computador. La otra es **Embedded**, diseñada específicamente para su uso con cualquier memoria de flash en lugar de disco duro, pero tiene la desventaja que no se pueden añadir paquetes adicionales.
- Existen más de 1 millón de implementaciones de *PfSense* a nivel mundial que han mostrado resultados exitosos.

11. CRONOGRAMA

El tiempo estimado fue de 6 meses distribuidos de la siguiente manera:

- | | |
|---|----------------------------------|
| 1. Diagnostico de los 7 Kioscos Vive Digital (Seguridad en Internet) | (Primer Mes) |
| 2. Elaboración y Diligencia de encuestas | (Primer Mes Últimos 15 días) |
| 3. Tabulación de encuestas | (Segundo Mes Primeros 15 días) |
| 4. Investigación y análisis de las herramientas de seguridad | (Segundo Mes) |
| 5. Prueba y selección de la herramienta más idónea | (Tercer y Cuarto Mes) |
| 6. Propuesta de Implementación y documentación de la herramienta seleccionada | (Quinto Mes) |
| 7. Documentación y Publicación de Resultados (Documento final) | (Sexto Mes) |

Tabla 2. Cronograma de Actividades por Mes

ETAPAS		CRONOGRAMA DE ACTIVIDADES (Por Mes)					
		1	2	3	4	5	6
1	Diagnostico Instituciones Educativas de Dosquebradas beneficiadas con el Programa VIVE DIGITAL. (7 Kioscos Vive Digital)	■					
2	Elaboración y Diligencia de encuestas	■	■	■	■	■	■
3	Tabulación de encuestas		■	■			
4	Investigación y análisis de las herramientas de seguridad	■	■	■	■	■	■
5	Prueba y selección de la herramienta más idónea			■	■	■	
6	Propuesta de Implementación de la herramienta seleccionada	■	■	■	■	■	■
7	Documentación y Publicación de Resultados (Documento final)						■

Fuente: Autoría propia

12. RECURSOS Y PRESUPUESTO

12.1 Talento Humano

- Dos Ingenieros de Sistemas
- Dos Técnicos en Sistema para realizar las encuestas
- Un Tabulador de Encuestas

12.1.1 Perfil Ingenieros

- **Paula Andrea Arias Cárdenas**, Ingeniera de Sistemas de la Universidad Nacional Abierta y a Distancia (UNAD), con capacidad de trabajo en equipo, fortaleza para tomar decisiones con objetividad, disposición para el aprendizaje y el conocimiento, hábil para la planeación, gestión y ejecución de proyectos.
- **Jorge Mauricio Rivera Buitrago**, Ingeniero de Sistemas de la Universidad Nacional Abierta y a Distancia (UNAD), capaz de formular y poner en marcha planes informáticos según los objetivos de la empresa a corto, mediano y largo plazo, así como supervisar proyectos, diseñar planes de formación tecnológica y perfeccionamiento de planes logísticos, habilidades para obtener y analizar información, capacidad de síntesis.

12.1.2 Perfil Técnicos

- Dos Técnicos en sistemas, con habilidades para el trato de personas, ya que las encuestas se le harán a jóvenes y niños en su mayoría, por ello deben tener disposición y buena actitud para aclarar inquietudes que se puedan presentar.

12.1.3 Perfil Tabulador

- Persona responsable, con experiencia en el proceso de tabulación de encuestas.

12.2 Materiales y Equipos

Para el desarrollo de este proyecto de investigación, se dispuso de dos computadores, para la investigación de las Herramientas de Software Libre diseñadas como medidas de Seguridad Informática.

El primer equipo se estableció como servidor y contó con dos tarjetas de red como elementos principales; la primera tarjeta se utilizó para acceder a internet y la segunda sirvió para el filtrado de información que entra y sale de la red. El segundo equipo fue el cliente para navegar por internet y hacer las pruebas de conexión y validación. Adicional a los elementos mencionados, se requirió de un switch para conectar los dos computadores y establecer una red de prueba.

El software instalado, cumple con los requisitos de la GNU (Licencia Pública General), ya que éste se basa en programas libres, el cual se permitió descargar, configurar y modificar al gusto del cliente, al ser libre permitió que fuese trabajado sin licencia, lo cual no representó ningún gasto.

Por todo lo anterior, si bien el software libre en la actualidad tiene una cobertura desigual de las distintas necesidades de seguridad de una empresa o en este caso Institución Educativa, éste es, definitivamente, una solución provechosa en aquellas áreas aún no exploradas y una oportunidad real e inmediata en aquellas otras para utilizar soluciones equivalentes a las propietarias, con los siguientes beneficios:

- Menor coste
- Mayor garantía de seguridad, debido a la posibilidad de auditar el código en uso.
- Mayor flexibilidad en la adaptación e integración por la posibilidad de modificar dicho código.
- Posibilidad del mantenimiento asegurado con independencia del origen del producto en sí.

12.3 Transporte

Se requirió realizar visitas a los 7 Kioscos Vive Digital instalados en las diferentes Instituciones Educativas Públicas del Municipio de Dosquebradas (Risaralda), beneficiadas con el Programa VIVE DIGITAL, para diagnosticar la seguridad en el uso de internet, encuestas, pruebas e implementación de la Herramienta de Software Libre en la Institución Educativa **Eduardo Correa Uribe** - Sede La Palma Dosquebradas.

12.4 Recursos Financieros

Tabla 3. *Presupuesto Financiero Personal*

1 PRESUPUESTO FINANCIERO PERSONAL						
Actividad	Personal	Cantidad Personal	Tiempo en Horas x Persona	Base Mes x Persona	Valor Hora x Persona	Total
Visita Diagnóstico Instituciones Educativas de Dosquebradas beneficiadas con el Programa VIVE DIGITAL. (7 Kioscos Vive Digital)	Ingeniero	2	20	2.500.000	10.417	416.680
Elaboración y Diligencia de Encuestas	Técnico	2	8	1.200.000	5.000	80.000
Tabulación de Encuestas	Tabulador	1	40	500.000	2.083	83.320
Investigación y Análisis de Herramientas de Software Libre (Seguridad)	Ingeniero	2	60	2.500.000	10.417	1.250.040
Prueba y Selección de la Herramienta más idónea	Ingeniero	2	120	2.500.000	10.417	2.500.080
Implementación de la Herramienta Seleccionada	Ingeniero	2	30	2.500.000	10.417	625.020
Materiales y suministros (DVD, CD, Papelería, Lapiceros, Fotocopias)	N/A	N/A	N/A	N/A	N/A	400.000
Gastos Varios (Imprevistos)	N/A	N/A	N/A	N/A	N/A	600.000
Documentación y Publicación (Documento Final)	Ingeniero	2	30	2.500.000	10.417	625.020
						6.580.160

Fuente: Autoría propia

Tabla 4. *Presupuesto Financiero Equipos*

2 PRESUPUESTO FINANCIERO EQUIPOS			
Descripción	Cantidad	Valor	Total
Computadores Argon Core i5 con Sistema Operativo Linux y tarjeta de red integrada	2	1.218.000	2.436.000
Tarjeta de Red adicional	1	30.000	30.000
Switch	1	60.000	60.000
			2.526.000

Fuente: Autoría propia

Tabla 5. *Total Presupuestos*

TOTAL PRESUPUESTO	
Descripción	Total
1 Presupuesto Financiero Personal	6.580.160
2 Presupuesto Financiero Equipos	2.526.000
9.106.160	

Fuente: Autoría propia

12.5 Fuentes de financiación

Este proyecto se financió con recursos propios.

12.6 Análisis Costo-beneficio:

En este caso el mayor beneficio fue para la Institución Educativa **Eduardo Correa Uribe – Sede la Palma Dosquebradas**, como prueba piloto, para ser aplicado posteriormente en las demás Instituciones Educativas Públicas beneficiadas con el programa VIVE DIGITAL, ya que se estaría protegiendo la infraestructura asignada y de igual forma la integridad de cada uno de los usuarios que acceden y utilizan internet a través de éste programa.

En cuanto al beneficio propio, éste se reflejó en el aprendizaje mismo, por la puesta en práctica de aquellos conocimientos adquiridos durante la Especialización, así como también por el mismo desarrollo de nuestro Proyecto de Investigación en Seguridad Informática.

CONCLUSIONES

Partiendo de la base de que en la actualidad, son muchos los productos, tecnologías, dispositivos y herramientas de software libre que se utilizan como estándares, protocolos y políticas de seguridad, vitales para minimizar aquellos riesgos informáticos que vulneran la infraestructura computacional y/o la información de las organizaciones, así como también la integridad de sus usuarios; surgió la idea de este Proyecto de Investigación, en el cual se pudo determinar el nivel actual de seguridad informática al momento de utilizar Internet en los 7 Kioscos Vive Digital de las Instituciones Educativas Públicas del Municipio de Dosquebradas (Risaralda), beneficiadas con el Programa VIVE DIGITAL direccionado por el Gobierno Nacional; en base a lo anterior, se realizó el análisis de 3 opciones, dentro de las muchas existentes: *PfSense* | *Zentyal* | *IPCop*, determinándose que la mejor elección de herramienta de software libre para su implementación como Política de Seguridad, en cuanto al mal uso del Internet, para el caso puntual de la Institución Educativa **Eduardo Correa Uribe – Sede la Palma Dosquebradas**, como prueba piloto, para ser aplicado posteriormente en las demás Instituciones mencionadas... es la herramienta *pfSense*.

Después de comparar las 3 Herramientas de Software Libre mencionadas, y seleccionar *PfSense* como la opción más idónea en cuanto a Política de Seguridad Informática para el caso que nos ocupa, se puede concluir:

- Como el mal uso a internet representa el punto más débil de la seguridad en los Kioscos Vive Digital de las Instituciones Educativas Públicas del Municipio de Dosquebradas (Risaralda) por parte de los usuarios de los mismos; surge *Pfsense* como Firewall, para proporcionar una gran variedad de herramientas que complementan la estructura de la red, mediante la configuración de Políticas de Seguridad Informática, tales como:

- ✓ La eliminación de acceso a Redes Sociales, como Facebook, Twitter, MySpace, entre otros.
 - ✓ El bloqueo de chats, mensajería instantánea, video conferencias, etc.
 - ✓ El bloqueo de descargas desde Internet.
 - ✓ La eliminación de archivos adjuntos que no sean habitualmente utilizadas en los Kioscos Vive Digital.
 - ✓ La restricción de términos y palabras clave utilizadas en la web, como por ejemplo: *sexo, chat, pornografía, pedofilia, redes sociales*, entre muchos otros.
- ***PfSense*** como Software Libre, se trata de una muy buena opción frente a las demás soluciones, incluyendo las comerciales que suponen un gran esfuerzo económico para la Institución Educativa en mención; ya que ofrece soluciones para problemas de red y seguridad muy distintas y concretas como es el caso del uso de Internet. Además, posee una comunidad activa que ayuda a resolver las posibles dudas que puedan surgir y contribuir en revisiones constantes de *PfSense*.
 - ***PfSense*** fue elegida como el instrumento de control y medida de Seguridad Informática más idónea, en base a la documentación existente y confirmada mediante su instalación y pruebas de rendimiento, que permitieron develar la posible protección de la integridad de los usuarios, prevenir los daños en la infraestructura computacional y salvaguardar la información.
 - La metodología de la Herramienta de Software Libre ***PfSense***, cambia el concepto de software como producto, por el de software como servicio de valor añadido, permitiendo que programas como VIVE DIGITAL, puedan asegurar su continuidad, debido a que se fundamenta como un plan de tecnología que busca la masificación de Internet, en el cual la infraestructura computacional, la información y la integridad de sus usuarios, se convierten en aspectos fundamentales relacionados con el aumento del conocimiento.

- Para el Programa VIVE DIGITAL, el Internet es su principal recurso tecnológico, el cual complementa más no sustituye los métodos tradicionales de comunicación, aprendizaje e investigación, pese a los riesgos que también conlleva el uso del mismo; de ahí la importancia de que los 7 Kioscos Vive Digital instalados en las Instituciones Educativas del Municipio de Dosquebradas (Risaralda) beneficiadas con este programa, cuenten con *PfSense* como Herramienta de Software Libre para proteger la integridad de los usuarios y mantener la continuidad del Programa.
- *PfSense* como Firewall, por sí solo no es la solución final a la implementación de seguridad para el mal uso del Internet en los Kioscos Vive Digital mencionados durante el Proyecto de Investigación, ya que se requiere de un control y una vigilancia constante, y para ello se necesita de instrumentos y protocolos de seguridad adicionales que faciliten la Confidencialidad, Integridad y Disponibilidad del mismo sistema y de la información. De igual forma, *PfSense* es un mecanismo que permite cumplir con las políticas de seguridad deseadas y configuradas, como filtrado de contenido, denegación de accesos a sitios no autorizados, control del ancho de banda asignado a cada segmento de la red, mecanismo para evitar virus, gusanos, troyanos, entre otras.

Por último y en vista del estudio y de los resultados obtenidos durante este Proyecto de Investigación, en el que se han expuesto las distintas capacidades, ventajas y desventajas del *Software Libre* frente al *Software Propietario*, se puede confirmar que este primero, a pesar de que en determinadas áreas compite frente a frente con las soluciones propietarias existentes; la situación ha ido cambiando para el Software Libre, ya que ha demostrado ser competitiva y aceptada por el público general, aprobación que ha dado lugar a un desarrollo exponencial en el que posiblemente llegue a igualarse o incluso sobrepasar el Software Propietario con el transcurrir de los días.

BIBLIOGRAFÍA

Ortegón, E., Pacheco, J. F., & Prieto, A. (julio de 2005). *Metodología del marco lógico para la planificación, el seguimiento y la evaluación de proyectos y programas*. Instituto Latinoamericano y del Caribe de Planificación Económica y Social (ILPES). Área de proyectos y programación de inversiones. Santiago de Chile. Recuperado de: <http://www.eclac.org/publicaciones/xml/9/22239/manual42.pdf>

Secretaría de Educación de Dosquebradas. *Directorio de Establecimientos Educativos Oficiales del Municipio de Dosquebradas*. Centro Administrativo Municipal (CAM). Recuperado de: <http://www.sem Dosquebradas.gov.co/archivos/DIRECTORIO%20OFICIALES%202015.pdf>

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (08 de noviembre de 2010). Video: *¿Qué es el Plan Vive Digital?*. Recuperado de: <https://www.youtube.com/watch?v=-x8DFRnJHm8>

Orduz, R. (07 de Diciembre de 2010). *Plan Vive Digital Colombia (II)*. Los números de las Tic. Colombia Digital. Recuperado de: <http://colombiadigital.net/opinion/columnistas/los-numeros-de-las-tic/item/458-plan-vive-digital-colombia-ii.html>

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Vive Digital Colombia. *El Plan Vive Digital*. Recuperado de: <http://www.mintic.gov.co/portal/vivedigital/612/w3-article-1510.html>

Ministerio de Tecnologías de la Información y las Comunicaciones. *Documento de Planeación Estratégica del Subsistema de Innovación*. República de Colombia. Recuperado de: http://www.mintic.gov.co/portal/604/articles-6116_recurso_2.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Vive Digital Colombia. Video: *El Plan Vive Digital*. Recuperado de: <http://www.mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-6106.html>

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (29 de diciembre de 2012). *Dosquebradas ya cuenta con Punto Vive Digital*. Sala de Prensa. Noticias. Recuperado de: <http://mintic.gov.co/portal/604/w3-article-1310.html>

Club Planeta. ¿Qué es Internet?. Computación Aplicada al Desarrollo SA de CV. Adelfa 213-A, Villa de las Flores, León Guanajuato. Recuperado de:
http://www.cad.com.mx/que_es_internet.htm

Club Planeta. Historia del Internet. Computación Aplicada al Desarrollo SA de CV. Adelfa 213-A, Villa de las Flores, León Guanajuato. Recuperado de:
http://www.cad.com.mx/historia_del_internet.htm

Falla Aroche, S. (14 de febrero de 2006). *La historia de Internet*. Recuperado de:
<http://www.maestrosdelweb.com/internethis/>

Bautista, D. (18 de Febrero de 2013) Ventajas y Desventajas del Internet. Taringa. Recuperado de: <http://www.taringa.net/post/info/16403479/Ventajas-y-desventajas-del-Internet.html>

Pérez Hernández, A. J. *Internet, Ventaja o Desventaja*. Comalcalco, Tabasco (México). Recuperado de: <http://alvarojesus.galeon.com/>

Adell, J. Educacion en la Internet. serie IV. Extraordinari XX Setmana Pedagògica (ISSN 0211-3368), págs. 207-214. Publicado en: Universitas Tarraconensis. Recuperado de:
<http://nti.uji.es/docs/nti/tarragona.html>

Yusneidher. (25 de noviembre de 2012). Informática Aplicada a la Educación Superior. *Ventajas y Desventajas del Internet para la Educación*. Recuperado de:
<http://yusneidher.blogspot.com/2012/11/ventajas-y-desventajas-del-internet.html>

Erb, M. Gestión de Riesgo en la Seguridad Informática. *Facilitando el manejo seguro de la información en organizaciones sociales*. Recuperado de:
https://protejete.wordpress.com/gdr_principal/definicion_si/

Ríos, J. Monografía. *Seguridad Informática*. Recuperado de:
<http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml>

Navarro Martín, S. Seguridad Informática SMR. Tema 1: *Seguridad Informática*. Wiki sobre Seguridad Informática. Segundo curso de Sistemas Microinformáticos y Redes. Recuperado de: <http://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA>

Recovery Labs. *Delitos Informáticos*. Computer Forensic. Departamento de Peritaje Informático. España. Recuperado de: http://www.delitosinformaticos.info/delitos_informaticos/definicion.html

Borghello, C. *Protección*. Segu-Info. Seguridad de la Información. Recuperado de: <http://www.segu-info.com.ar/proteccion/proteccion.htm>

Asamblea del Hacklab. *Seguridad Informática: Recomendaciones básicas para los usuarios*. Recuperado de: https://we.riseup.net/hacklab+asamblea/seguridad_informatica

CSIRTCV. Centre de Seguretat TIC de la Comunitat Valenciana. *12 medidas básicas para la seguridad Informática*. Cardenal Benlloch, 69 Entlo – 46010 Valencia. Recuperado de: <http://www.csirtcv.gva.es/sites/all/files/downloads/12%20medidas%20b%C3%A1sicas%20para%20la%20seguridad%20Inform%C3%A1tica.pdf>

HispaLinux. Hacia la sociedad del conocimiento libre. *¿Qué es el Software Libre?*. Recuperado de: <http://hispalinux.es/SoftwareLibre>

FONADE, Fondo Financiero de Proyectos de Desarrollo. (Abril de 2013). Dotación, Instalación y puesta en funcionamiento de la Infraestructura técnica de los Puntos Vive Digital Fase 1. Bogotá D.C. Recuperado de: http://www.fonade.gov.co/Contratos/Documentos/3767__2013041910380819%20ANEXO%20No%202-%20DOC%20TECNICO%20PROVEEDOR%20FASE%201.pdf

FONADE, Fondo Financiero de Proyectos de Desarrollo. (Junio de 2014). Dotación, Instalación y puesta en funcionamiento de la Infraestructura técnica de los Puntos Vive Digital Fase 1 en una segunda Etapa. Bogotá D.C. Recuperado de: http://www.fonade.gov.co/Contratos/Documentos/4382__2014062006500208%20DOCUMENTO%20TECNICO%20PROVEEDOR%20FASE%201.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. Listado de Puntos Vive Digital beneficiados. Recuperado de:
http://www.mintic.gov.co/portal/vivedigital/612/articles-4312_recurso_1.pdf

Gobierno en Línea. Tu punto de acceso oficial a la información, trámites y servicios del Estado Colombiano. Servicio de Puntos Vive Digital. Recuperado de:
<https://www.gobiernoenlinea.gov.co/web/guest/puntos-vive-digital>

Google. Maps. (2015). *Dosquebradas, Risaralda, Colombia*. Recuperado de:
<https://www.google.com/maps/place/Dosquebradas,+Risaralda,+Colombia/@4.838985,-75.671235,13z/data=!3m1!4b1!4m2!3m1!1s0x8e3880c45cd78303:0xeb0625cf082593fe>

CARDER, Corporación Autónoma Regional de Risaralda. (04 de Julio de 2013). Mapas del Departamento de Risaralda. Mapa de las Veredas Dosquebradas. Documento. Recuperado de: <http://www.carder.gov.co/intradocuments/webExplorer/mapas-del-departamento-de-r-da-0/page:4>

Ferrer, J., & Fernández-Sanguino, J. *Seguridad informática y Software Libre*. Estructura de Hispalinux. Recuperado de: <http://es.tldp.org/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf>

DragonJar. (03 de Julio de 2009). Comunidad de Seguridad Informática. Videos: *Seguridad Informática con Software Libre*. Recuperado de:
<http://www.dragonjar.org/seguridad-informatica-con-software-libre.xhtml>

MuyComputer. (19 de Mayo de 2014). *50 herramientas de software libre para la seguridad informática*. Tecnologías de Software Libre. Recuperado de:
<http://www.somoslibres.org/modules.php?name=News&file=article&sid=3473>

Pujadas, J. (2007). *Tutorial sobre pfsense*. Recuperado de:
http://www.bellera.cat/josep/pfsense/installacio_cs.html

Canal de armgasa123. (21 de mayo de 2010). Video: *pfsense parte 1*. Recuperado de:
<https://www.youtube.com/watch?v=EdRJ035hoq8>

Canal de armgasa123. (22 de mayo de 2010). Video: *pfsense parte 2*. Recuperado de: <https://www.youtube.com/watch?v=mFwWfq-i6JE>

May, G. (28 de abril de 2014). Video: *¿cómo instalar pfsense, bloquear redes sociales, y tener dos redes*. Recuperado de: <https://www.youtube.com/watch?v=XAorp-IGLiw>

Zentyal. (22 de septiembre de 2014). *Zentyal 3.5 Documentación Oficial*. Recuperado de: https://wiki.zentyal.org/wiki/Es/3.5/Zentyal_3.5_Documentacion_Oficial

Taringa. (21 de diciembre de 2010). *Manual completo Instalación de Zentyal Firewall de Linux*. Recuperado de: <http://www.taringa.net/posts/linux/8450763/Manual-completo-Instalacion-de-Zentyal-Firewall-de-Linux.html>

Aliaga, A. Linux Zone. *Tutorial sobre IP COP*. Recuperado de: <http://linuxzone.es/tutorial-sobre-ip-cop/>

Ezquieta, J. (16 de junio de 2013). *Manual del Administrador de IPCop v2.0.0*. Recuperado de: <http://www.ipcop.org/2.0.0/es/admin/html/>

Alfárez Sánchez, J. A. *Instalación de un Router/Appliance con funciones de Firewall, Vpn, Protección de Ataques, Antispam y Antivirus perimetral con IPCop*. Recuperado de: http://www.alferez.es/documentos/Instalacion_IPCOP.pdf

ANEXOS

ANEXO A | ENCUESTA

Evaluar la Seguridad con el uso de Internet en las Instituciones Educativas Públicas del Municipio de Dosquebradas beneficiadas con el Programa VIVE DIGITAL



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA | ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

Objetivo: "Evaluar la Seguridad con el uso de Internet en las Instituciones Educativas Públicas del Municipio de Dosquebradas beneficiadas con el Programa VIVE DIGITAL"

Aviso: La información que se suministre al diligenciar esta encuesta, tiene como objetivo únicamente fines investigativos y académicos, por lo tanto no se hará pública de forma particular. Nadie más a excepción de quien realiza la encuesta, tendrá acceso a la información puntual acá suministrada. Todos los hallazgos serán presentados de manera general en el informe final de un Proyecto de Investigación, sin que esto afecte la privacidad de la misma. Adicionalmente esta encuesta, no debe ser marcada con su nombre o número de identificación para garantizar su confidencialidad.

Datos Generales

Fecha

Mes	Día	2015	31
-----	-----	------	----

Seleccione el Kiosko Vive Digital al cual visita

- Instituto Educativo Vereda las Hortencias
- Instituto Educativo Vereda Nueva Independencia
- Instituto Educativo Vereda La Palma
- Instituto Educativo Vereda Agua Azul
- Instituto Educativo Vereda La Rivera
- Instituto Educativo Vereda Buena Vista
- Instituto Educativo Vereda Naranjales

Genero

- Masculino
- Femenino

Edad

- Entre 5 y 14
- Entre 15 y 24
- Entre 25 y 34
- Entre 35 y 44
- Entre 45 y 54
- Entre 55 y 64

Seleccione a que grupo pertenece

- Docente
- Estudiante
- Administrativo
- Comunidad

Datos de Opinión

Responder esta pregunta solamente en el caso de ser Estudiante: Cuando utiliza Internet desde los computadores del Kiosco Vive Digital, ¿Se hace en presencia de un adulto o docente que lo supervise?

- Si
- No
- A veces

Si utiliza Internet desde los computadores del Kiosco Vive Digital, señale ¿Cuáles de estas actividades realiza?

- Entretenimiento
- Educación (Investigación)
- Redes Sociales
- Comunicación (Correo, Foros, Chats, etc)
- Descargas

Con qué frecuencia accede a Internet desde los computadores del Kiosco Vive Digital?

- Todos los Días
- Varios Días a la Semana
- Una vez a la Semana
- Solo Fines de Semana

Cuánto tiempo se conecta a internet a la semana, desde los computadores del Kiosco Vive Digital?

- Menos de 1 hora
- De 1 a 5 horas
- De 5 a 10 horas
- De 10 a 20 horas
- Más de 20 horas

Le han sugerido normas o pautas para seguir durante el uso de Internet en los computadores del Kiosco Vive digital?

- Si
- No

Si la respuesta fue Si en la pregunta anterior, menciona alguna de las Normas

Dentro de las siguientes categorías de páginas web, cuáles ha visitado alguna vez desde los equipos del Kiosco Vive Digital?

- Sexo/Pornografía/Desnudos
- Bulimia/Anorexia
- Odio/Racismo
- Explosivos
- Apuestas
- Alcohol
- Drogas
- Violencia
- Suicidio
- Ninguno
- Otros:

A cuál de las siguientes Redes Sociales, accedes desde los computadores del Kiosco Vive Digital?

- Facebook
- Twitter
- Instagram
- MySpace
- Google +
- Ninguno
- Otros:

Si tiene alguno o varias perfiles en Redes sociales, las contraseñas empleadas para ingresar a estos sitios son:

- Todas Iguales
- Todas Diferentes
- Utiliza la misma para varios sitios

Tiene Cuenta de Correo Electrónico?

- Si
- No

Si la respuesta fue Si en la pregunta anterior conteste: Si recibe correos electrónicos extraños mientras utilizan los computadores del Kiosco Vive Digital, Qué acción realizas?

- Abrirlos y revisar su contenido
- Borrarlos sin abrirlos
- Preguntarle a alguien si se debe abrir


Señale cuál de los siguientes términos conoce

- Virus Informático
- Spyware
- Spam

- Sniffer
- Adware
- Phising
- Exploit
- Ninguno de los Anteriores

ANEXO B | LISTA DE CHEQUEO

Seguridad de la infraestructura (Hardware - Software) del Programa VIVE DIGITAL en la Institución Educativa Eduardo Correa Uribe – Sede la Palma Dosquebradas




UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA | ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA

Lista de Chequeo: "Seguridad de la infraestructura (Hardware - Software) del Programa VIVE DIGITAL en la Institución Educativa Eduardo Correa Uribe – Sede la Palma Dosquebradas"

Aviso: La información que se suministre al diligenciar esta encuesta, tiene como objetivo únicamente fines investigativos y académicos, por lo tanto no se hará pública de forma particular. Nadie más a excepción de quien realiza la encuesta, tendrá acceso a la información puntual acá suministrada. Todos los hallazgos serán presentados de manera general en el informe final de un Proyecto de Investigación, sin que esto afecte la privacidad de la misma. Adicionalmente esta lista de chequeo, no debe ser marcada con su nombre o número de identificación para garantizar su confidencialidad.

Datos Generales

Fecha

Mes ▼ Día ▼ 2015 ▼ 

Genero

- Masculino
- Femenino

Edad

- Entre 18 y 30
- Entre 31 y 40
- Entre 41 y 50
- Entre 51 y 60
- Entre 61 y Más

Cargo que desempeña en el Kiosco Vive Digital

Lista de Chequeo

Hardware

De cuántos computadores dispone el Kiosco Vive Digital?

- De 1 a 5 Computadores
- De 5 a 10 Computadores
- Más de 10 Computadores

Con qué dispositivo de conexión se cuenta para la distribución de Internet en los computadores del Kiosco Vive Digital?

- Línea Telefónica (RTB, RDSI, ADSL)
- Cable (Fibra Óptica, Cable Coaxial)
- Satélite (Antena Parabólica)
- Inalámbrica (Wi-Fi, WiMax)
- Telefonía Movil (3G, 4G)
- Radio (LMSD)

Con que dispositivo se cuenta para la distribución de Internet en los computadores del Kiosco Vive Digital?

- Servidor de Internet
- Router
- Firewall
- Otros:

De qué forma se conectan los computadores del Kiosco Vive Digital a Internet?

- Cableado (UTP)
- Inalámbrico
- Cableado e Inalámbrico

Se controla que los usuarios puedan instalar aplicaciones en los equipos del Kiosco Vive Digital?

- Si
- No
- Ns/Nr

Software

Qué Sistema Operativo tienen instalados los computadores del Kiosco Vive Digital?

- Windows (Cualquier Distribución)
- Mac (Cualquier Distribución)
- Linux (Cualquier Distribución)

El Software de los computadores del Kiosco Vive Digital, cuentan con sus respectivas licencias de instalación?

- Si
- No
- Ns/Nr

Los computadores del Kiosco Vive Digital tienen instalado antivirus?

- Si
- No
- Ns/Nr

Si la respuesta fue Si en la pregunta anterior, El antivirus instalado permanece actualizado?

- Si
- No
- Ns/Nr

Se utilizan programas de descarga de ficheros? (música, películas, programas, documentos, etc)

- Si
- No
- Ns/Nr

Se realizan conexiones externas por vía Internet a los computadores del Kiosco Vive Digital?

- Si
- No
- Ns/Nr

Ofrece el Kiosco Vive Digital conexión inalámbrica (WIFI) a sus usuarios?

- Si
- No
- Ns/Nr

Si la respuesta fue Si en la pregunta anterior, Se cuentan con medidas de seguridad para proteger dicha conexión?

- Si
- No
- Ns/Nr

Qué Navegador se utiliza en los computadores del Kiosco Vive Digital para navegar en Internet?

- Mozilla Firefox
- Chrome
- Internet Explorer
- Safari
- Opera
- Otros:

Considera que el navegador influye en la seguridad a la hora de navegar por Internet?

- Si
- No
- Ns/Nr

Se cuenta con algún Software como Cortafuegos para los computadores del Kiosco Vive Digital?

- Si
- No
- Ns/Nr

Si la respuesta fue Si en la pregunta anterior, Que Software como Cortafuegos se utiliza?

- El que viene con el Sistema Operativo
- El que viene con el Antivirus
- No se utiliza
- Otros:

Se tiene instalado algún tipo de Sistema de Control Parental y/o Control de Usuarios en los computadores del Kiosco Vive Digital?

- Si
- No
- Ns/Nr

Se Controla o supervisa el contenido que consultan las personas en Internet en los computadores del Kiosco Vive Digital?

- Si
- No
- Ns/Nr